La sécurité des réseaux

Table des matières

Les attaques visant à pirater un système en réseau dans le but de récupérer des informations sensibles ou d'altérer les services existent à tous les niveaux. La majorité des entreprises a connu une attaque, même mineure. Google a annoncé en janvier 2010 qu'elle a été la victime d'une attaque pirate ciblée. Chez un particulier, un PC non protégé et connecté à l'Internet peut être infecté en moins de 24 heures (la durée dépend du trafic généré et de l'OS). Les points d'entrée les plus vulnérables sont les navigateurs (lien malveillant) et les clients de messagerie (faux lien intégré et pièces jointes). Par ailleurs, ces derniers reçoivent souvent davantage de spam que de vrais courriers !

1. Introduction

Quelle que soit leur place ou leur rôle dans une architecture de réseau local ou sur Internet, les systèmes (serveurs, PC, routeurs, systèmes de stockage, …) sont donc tous vulnérables à un certain niveau pour différentes raisons :

- émergence en permanence des nouveaux usages et de nouvelles technologies, et donc de nouvelles vulnérabilités (réseaux sociaux, P2P, messagerie instantanée, réseaux sans fil, smartphones connectés en WiFi ou en 3G, téléphonie sur IP, stockage sur clé USB, …) ;
- les politiques de sécurité sont complexes car elles doivent opérer simultanément sur tous les éléments d'une architecture réseau et pour différents types d'utilisateurs (firewall sur les routeurs d'accès et sur les serveurs d'extrémité, cryptage de certains fichiers, droits accrus pour les administrateurs sur certaines ressources, …) ;
- les politiques de sécurité mises en place sont basées sur des jugements humains qui doivent de plus être révisés en permanence pour s'adapter aux nouvelles attaques ;
- la sécurisation est coûteuse en moyens, en temps et surtout en ressources humaines. Pour limiter ces vulnérabilités (quelles que soient les solutions, un système reste toujours vulnérable), la sécurité informatique vise généralement trois objectifs principaux :
- l'intégrité consiste à garantir que les données n'ont pas été altérées sur la machine ou durant la communication (sécurité du support et sécurité du transport) ;
- la confidentialité consiste à assurer que seules les personnes autorisées ont accès aux ressources ;
- la disponibilité consiste à garantir à tout moment l'accès à un service ou à des ressources.

Un quatrième objectif peut être rajouté, il s'agit de la non-répudiation qui permet de garantir qu'aucun des correspondants ne pourra nier la transaction. L'authentification est un moyen de garantir la confidentialité. Elle consiste à s'assurer de l'identité d'un utilisateur ; un contrôle d'accès (nom d'utilisateur et mot de passe crypté) permet de limiter l'accès à certaines ressources (lecture seule sur tel dossier, accès interdit à tel fichier, …).

2. Les attaques

Les attaques peuvent être classées en deux grandes catégories : les techniques d'intrusion dont l'objectif principal est de s'introduire sur un réseau pour découvrir ou modifier des données et les dénis de service (DoS : Denial of Service attack) qui ont pour but d'empêcher une application ou un service de fonctionner normalement.

Cette deuxième catégorie agit donc sur la disponibilité de l'information tandis que la première concerne essentiellement la confidentialité et l'intégrité.

2.1. Les techniques d'intrusion

Ces techniques peuvent être classées suivant le niveau d'intervention :

- les accès physiques vont du vol de disque dur ou de portable à l'écoute du trafic sur le réseau (sniffing) ;
- l'ingénierie sociale permet de retrouver ou de récupérer directement des couples

identifiant/mot de passe en envoyant par exemple des messages falsifiés (phishing) ;

- l'interception de communication permet l'usurpation d'identité, le vol de session (hijacking), le détournement ou l'altération de messages (spoofing) ;
- les intrusions sur le réseau comprennent le balayage de ports (port scan), l'élévation de privilèges (passage du mode utilisateur au mode administrateur) et surtout les logiciels malveillants ou malwares (virus, vers et chevaux de Troie).

2.1.1. Le sniffing

Sur la plupart des réseaux, les trames sont diffusées sur tout le support (câble Ethernet, transmission radio WiFi, …). En fonctionnement normal, seul le destinataire reconnaît son adresse et lit le message. La carte Ethernet ou WiFi d'un PC peut être reprogrammée pour lire tous les messages qui traversent le réseau (promiscuous mode).

Exemple d'activation du promiscuous mode (sous GNU/Linux) :

```
ifconfig eth0 promisc ou ip link set wlan0 promisc on
```

Pour la désactivation :

```
ifconfig eth0 -promisc ou ifconfig eth0 promisc off
```

La limite dans ce cas est le dispositif d'interconnexion utilisé sur le LAN ou le segment de LAN (switch, routeur). Les hackers utilisent des sniffers ou analyseurs réseau qui scannent tous les messages qui circulent sur le réseau et recherchent ainsi des identités et des mots de passe. La commande « tcpdump » sous GNU/Linux (bien entendu !) et le logiciel « Wireshark », par exemple permettent le sniffing.

2.1.2. Le « craquage » de mot de passe

Le pirate utilise un dictionnaire de mots de noms propres construit à partir d'informations personnelles et privées qui ont été collectées (social engineering).

Ces chaînes de caractère sont essayées une à une à l'aide de programmes spécifiques qui peuvent tester des milliers de mots de passe à la seconde (exemple : John the ripper).

Toutes les variations sur les mots peuvent être testées : mots écrits à l'envers, lettres majuscules et minuscules, ajout de chiffres et de symboles. Ce type d'attaque est souvent nommé « attaque par force brute » car le mot de passe est deviné grâce à des milliers d'essais successifs à partir d'un dictionnaire, et non pas retrouvé à l'aide d'un programme capable de décrypter une chaîne de caractère.

2.1.3. Le phishing

Ce mot anglais provient de la contraction de fishing (pêcher) et de phreaking (pirater le réseau téléphonique). Il s'agit de conduire des internautes à divulguer des informations confidentielles, notamment bancaires, en usant d'un hameçon fait de mensonge et de contrefaçon électronique (identité visuelle d'un site connu, en-têtes, logo, …). Le cas le plus classique est celui d'un mail usurpant l'identité de votre banque et contenant un lien vers un faux site où l'on vous demandera de confirmer votre numéro de carte bleue par exemple.

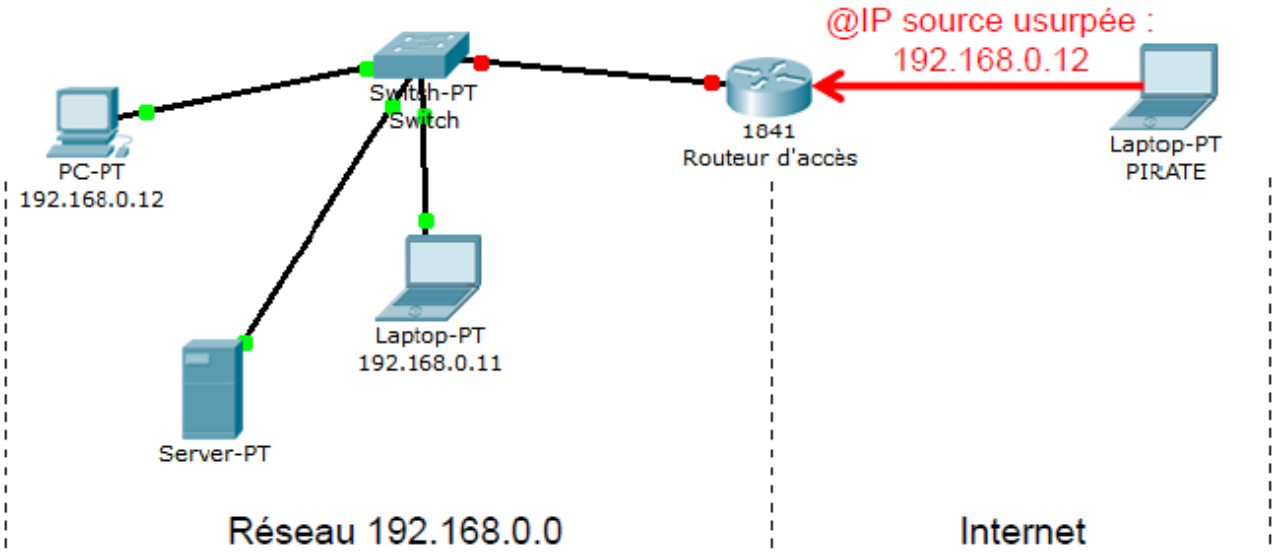
Le phishing utilise également des virus qui installent des programmes espions afin d'intercepter la frappe des données confidentielles sur le clavier (keyloggers) pour les transmettre ensuite sur un site

où le « phisher » pourra les récupérer.

La parade proposée par la plupart des banques est une saisie à la souris du numéro de compte et de code d'entrée.

2.1.4. Le spoofing

L'attaque basique de ce type est la falsification d'adresse IP : l'agresseur prétend provenir d'une machine interne pour pénétrer sur le réseau privé. Cette attaque peut être simplement bloquée avec un firewall au niveau du routeur d'accès qui éliminera les paquets entrants avec une IP source interne.



Le mail spoofing : les courriers électroniques sur Internet sont également exposés à la falsification. Une adresse d'expéditeur peut être falsifiée simplement dans la mesure où elle ne comporte pas de signature numérique. Le protocole d'envoi de messages SMTP n'est pas sécurisé.

Le DNS spoofing : le pirate utilise les faiblesses du protocole DNS et de son implémentation sur les serveurs de noms de domaine pour rediriger les internautes vers des sites falsifiés. Le but du pirate est donc de faire correspondre l'adresse IP d'une machine qu'il contrôle à l'URL réel d'une machine publique. On peut distinguer deux attaques de type DNS spoofing :

- le DNS ID spoofing basé sur la récupération et l'exploitation dans une fausse réponse du numéro d'identification contenu dans une requête DNS ;
- le DNS cache poisoning qui corrompt (empoisonne) avec de fausses adresses le cache des serveurs DNS.

Le web spoofing est une version élaborée de l'IP spoofing : il s'agit de remplacer un site par une version pirate du même site. Cette technique est notamment utilisée dans la dernière étape du phishing. La falsification se déroule en plusieurs temps :

- amener la victime à entrer dans le faux site web (grâce à l'utilisation du DNS spoofing par exemple) ;
- intercepter les requêtes HTTP ;
- récupérer les vraies pages web et modifier ces pages ;
- envoyer de fausses pages aux victimes.

2.1.5. Les malwares

Le terme « virus » est souvent employé abusivement pour désigner toutes sortes de logiciels malveillants (les virus ont été historiquement les premiers malwares). Un logiciel antivirus devrait logiquement s'appeler anti-malwares puisqu'il permet aussi de détecter les vers et les chevaux de Troie. Le spam est l'un des vecteurs les plus importants de propagation des malwares.

Un virus est un programme qui se propage à l'aide d'autres programmes ou de fichiers. Il est souvent simple et facile à détecter à partir de son code (signature) mais néanmoins efficace lorsqu'il se propage plus rapidement que la mise à jour des antivirus. Un virus passe le plus souvent par la messagerie et est activé par la sélection d'un lien sur le message ou l'ouverture d'un fichier attaché. Les conséquences de l'exécution du virus peuvent aller de la simple modification des paramètres d'une application (page par défaut du navigateur) ou de la base de registre du système (exécution automatique d'un programme commercial à chaque démarrage) à l'effacement de données ou de fichiers essentiels à l'OS.

Un ver (worm) est un programme plus sophistiqué capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque, ni d'une action d'une personne. La particularité des vers ne réside pas forcément dans leur capacité immédiate de nuire mais dans leur facilité de se propager grâce par exemple aux listes de contacts présentes sur les PC ou les smartphones. Le premier ver introduit sur l'iPhone change le fond d'écran : en avril 2009, le ver « StalkDaily » a exploité une faille de sécurité sur le site Twitter pour envoyer des milliers de messages de spam en utilisant des comptes de membres Twitter.

Un cheval de Troie (trojan) est un programme caché dans un autre programme qui s'exécute au démarrage du programme. Il permet donc de s'introduire sur le système à l'insu de la victime (ouverture d'une porte dérobée ou backdoor) ; le cheval de Troie devient alors autonome et peut agir comme un virus en infectant des données ou des programmes.

2.2. Déni de service

Ce type d'attaque (Denial Of Service ou DOS) empêche par saturation un service de fonctionner correctement sur une machine. Par exemple « Ping of the death » qui est la plus ancienne des attaques de type DOS : un ping continu avec une taille de paquet maximum est lancé vers la machine cible.

Une variante connu sou le nom de « smarfing » est basée sur l'envoi d'un « echo request » ICMP avec comme adresse source celle de la victime et une adresse de destination de broadcast. Les réponses « echo reply » provenant de toutes les machines du réseau vers la machine de la victime saturent celle-ci.

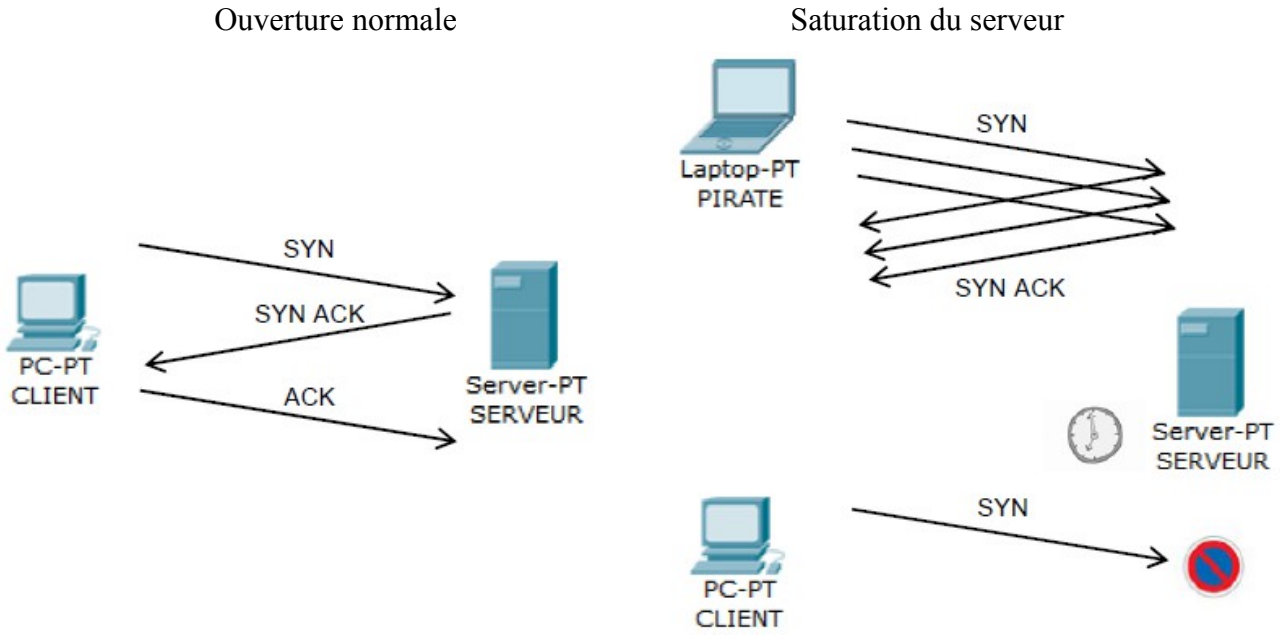
2.2.1. SYN Flood

Cette attaque consiste à inonder (flooding) la cible à l'aide de demandes successives d'ouverture de connexion TCP. Lors d'une ouverture normale :

- le premier segment TCP est transmis par le client avec le bit SYN à 1 pour demander l'ouverture ;
- le serveur répond avec dans son segment TCP les bits SYN et ACK à 1 ;
- le client demandeur conclut la phase avec le bit ACK à 1.

Les abus interviennent au moment où le serveur a renvoyé un accusé de réception (SYN ACK) au

client mais n'a pas reçu le « ACK » du client. C'est alors une connexion a semi-ouverte et l'agresseur peut saturer la structure de données du serveur victime en créant un maximum de connexions partiellement ouvertes. Le client autorisé ne pourra plus ouvrir de connexion.



Il existe plusieurs méthodes simples pour parer cette attaque :

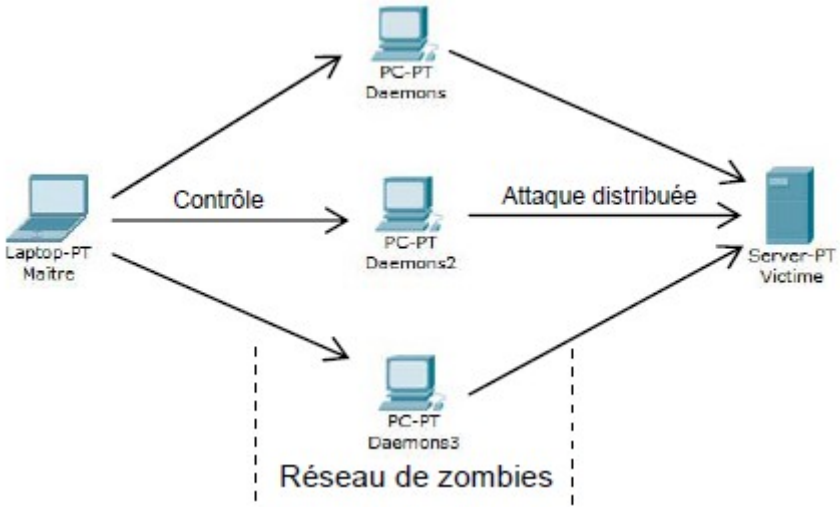
- la limitation du nombre de connexions depuis la même source ou la même plage d'adresses IP ;
- la libération des connexions semi-ouvertes selon un choix de client et un délai aléatoire ;
- la réorganisation de la gestion des ressources allouées aux clients en évitant d'allouer des ressources tant que la connexion n'est pas complètement établie.

2.2.2. DDOS

Le déni de service distribué ou DDOS (Distributed Denial Of Service) a les mêmes effets que le DOS traditionnel excepté que ce n'est plus une seule machine qui attaque les autres mais une multitude de machines nommées zombies contrôlées par un maître unique. L'attaque se déroule en plusieurs étapes :

- recherche sur Internet d'un maximum de machines vulnérables qui deviendront des complices involontaires, des « zombies ». Les réseaux de zombies (botnet) ainsi formés sont une ressource précieuse pour les hackers ;
- installation sur ces machines de programmes dormants (daemons) et suppression des traces éventuelles. Les daemons sont basés sur les attaques DOS classiques (paquets UDP multiples, SYN Flood, …) ;
- activation du dispositif à l'heure et au jour programmé.

Parmi les attaques DDOS très populaires, on connaît l'attaque sur les sites Yahoo, CNN et eBay qui ont subi une inondation de leur réseau.



3. Les défenses matérielles

3.1. Introduction

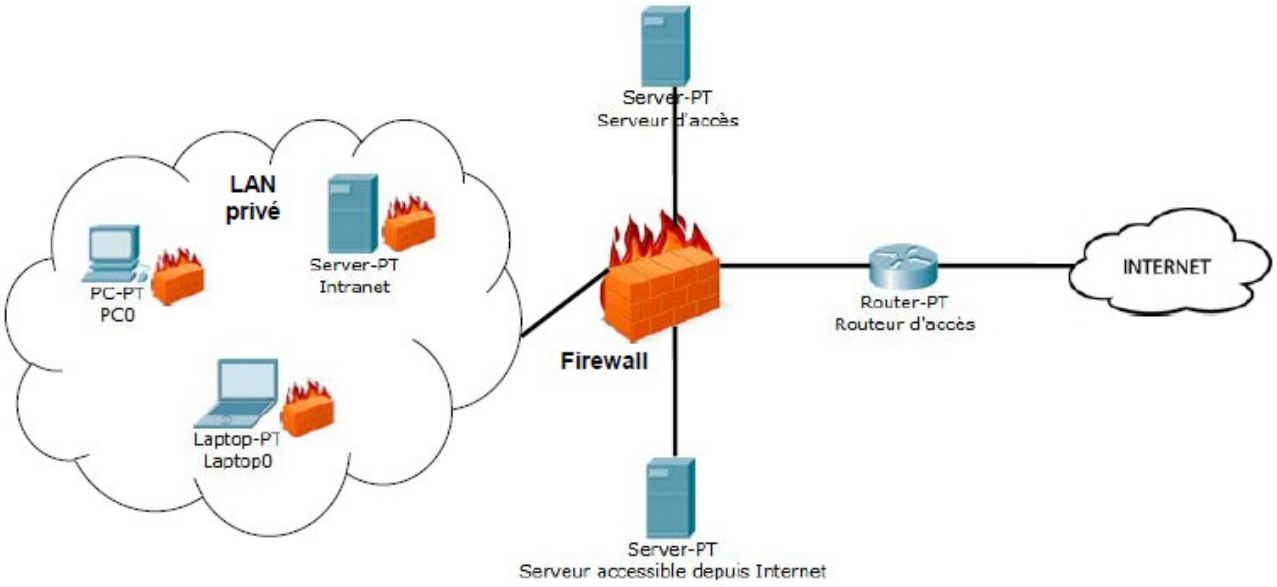
Les défenses matérielles interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de données centralisée sur le disque dur d'un serveur par exemple), sur les médias servant à transporter cette information (sécurisation du réseau sans fil) et sur les équipements intermédiaires traversés lors du transport (utilisation d'un firewall installé sur le routeur d'accès).

Par ailleurs, quelques principes de base doivent être respectés pour assurer l'efficacité des défenses :

- principe du moindre privilège : chaque élément du système (utilisateur, logiciel) ne doit avoir que le minimum de privilèges nécessaires pour accomplir sa tâche (les utilisateurs ne doivent pas être administrateurs, une session sur un serveur web est ouverte par défaut sur un compte utilisateur …).
- défense en profondeur : plusieurs mesures de sécurité valent mieux qu'une (antispam sur les postes de messagerie et sur les postes de travail, firewall sur le routeur d'accès et sur les machines d'extrémité …).
- interdiction par défaut : dans la mesure où toutes les menaces ne peuvent être connues à l'avance, il est mieux d'interdire tout ce qui n'est pas explicitement permis que de permettre tout ce qui n'est pas explicitement interdit (sur un firewall, il vaut mieux commencer par fermer tous les ports pour n'ouvrir ensuite que ceux nécessaires).
- participation des utilisateurs : un système de protection n'est efficace que si tous les utilisateurs le supportent, un système trop restrictif pousse les utilisateurs à devenir créatifs.
- simplicité : la plupart des problèmes de sécurité ont leur origine dans une erreur humaine. Dans un système simple, le risque d'erreur est plus faible et les analyses sont plus rapides.

3.2. Les firewalls

Le firewall ou pare-feu est chargé de filtrer les accès entre l'Internet et le LAN ou entre deux LAN.



La localisation du firewall (avant ou après le routeur, avant ou après la NAT) est stratégique. Le firewall, qui est souvent un routeur intégrant des fonctionnalités de filtrage, possède autant d'interfaces que de réseaux connectés. Suivant la politique de sécurité, le filtrage est appliqué différemment pour chacune des interfaces d'entrée et de sortie : blocage des adresses IP privées entrantes, autorisation des accès entrants vers le serveur d'identification ou le serveur web institutionnel, blocage des accès entrants vers l'Internet…

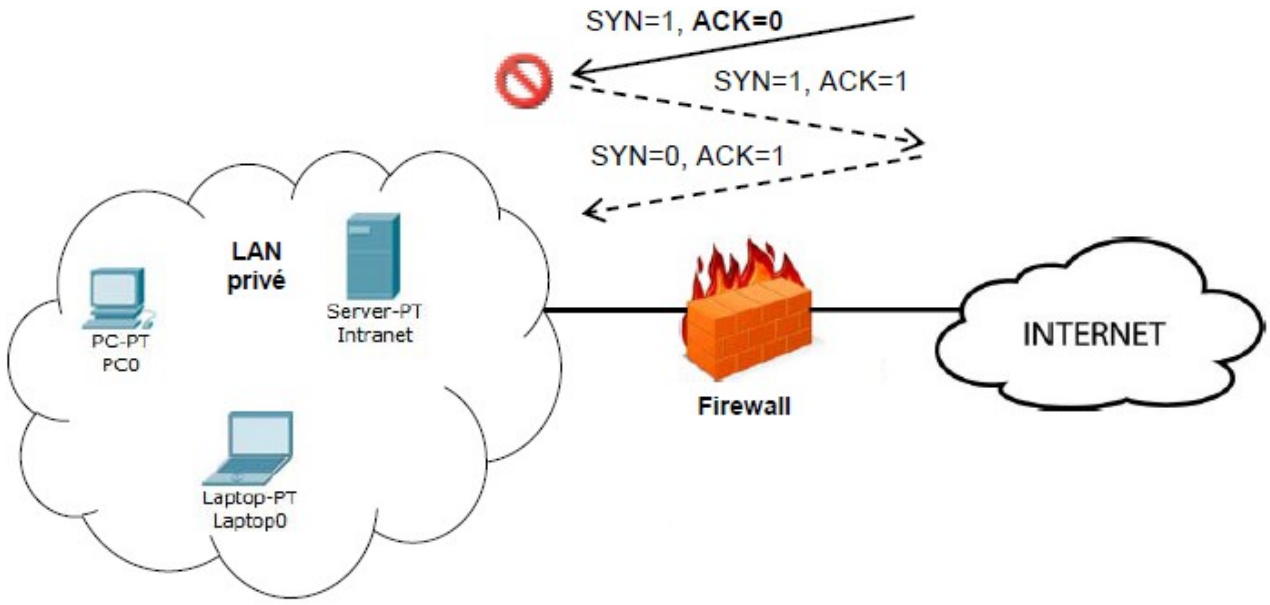
Les machines d'extrémités possèdent également un firewall mais celui-ci est logiciel (pare-feu Windows ou iptables sous Linux par exemple) et sert à protéger les machines du trafic entrant si le firewall à l'entrée du LAN n'a pas été suffisamment sélectif.

Pour chaque trame ou chaque paquet entrant ou sortant sur une interface donnée, les en-têtes correspondent aux différentes couches sont analysés et le filtrage sélectif est appliqué suivant la stratégie de sécurité définie par l'administrateur réseau.

Le filtrage peut porter sur :

- les adresses MAC source ou destination ;
- les adresses IP source ou destination ;
- les ports TCP ou UDP source ou destination ;
- les flags de l'en-tête TCP (SYN, ACK, …) ;
- le type de message ICMP ;
- le type de message ou le contenu HTTP, SMTP, POP.

Le firewall peut également empêcher les connexions entrantes en analysant la valeur du bit ACK de l'en-tête TCP. Lors d'une demande de connexion, le bit ACK du premier segment TCP est à 0, les bits ACK des segments suivants sont généralement tous à 1. Il suffit donc de bloquer les segments entrants avec le bit ACK à 0, les segments suivants pour cette connexion ne seront pas pris en compte.



La configuration d'un firewall passe par l'écriture d'une suite de règles qui décrivent les actions à effectuer (accepter ou refuser le trafic) suivant les informations contenues dans les en-têtes des paquets. Les caractéristiques de chaque paquet sont comparées aux règles, les unes après les autres. La première règle rencontrée qui correspond aux caractéristiques du paquet analysé est appliquée : l'action décrite dans la règle est effectuée. Pour assurer une sécurité maximum, la seule règle présente par défaut doit être celle qui interdit l'accès à tous les paquets entrants et sortants ; d'autres règles seront ensuite insérées pour ouvrir les accès souhaités. La stratégie appliquée est donc « tout ce qui n'est pas explicitement autorisé est interdit ».

Le tableau ci-dessous donne un exemple de règles d'un firewall muni de deux interfaces : une vers un LAN privé, une autre vers l'extérieur. Les règles précisent l'interface concernée (la direction du trafic), les adresses IP (une valeur à 0 autorise toutes les adresses), le protocole de niveau 4, les services (valeurs des ports) et éventuellement le blocage des connexions entrantes (test du bit ACK).

Règle	**Destination**	**@source**	**@dest.**	**Proto**	**Port src.**	**Port dst.**
A	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	80
B	Entrant	0.0.0.0	192.168.0.0	TCP	80	>1023
C	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	25
D	Entrant	0.0.0.0	192.168.0.0	TCP	25	>1023
E	Toutes	0.0.0.0	0.0.0.0	Tous	Tous	Tous

La stratégie de sécurité est la suivante :

- la règle A permet à toutes les machines situées sur le LAN d'adresse 192.168.0.0 d'ouvrir une connexion TCP vers un serveur web (port 80) externe quelconque (adresse 0.0.0.0) ;
- la règle B autorise le serveur web consulté à répondre aux machines locales ;
- émission (règle C) ou réception (règle D) de courrier SMTP (port 25) avec un serveur

externe ;

- blocage de tout autre trafic (règle E).

Quels que soient l'origine du firewall utilisé et l'OS associé, les règles portent plus ou moins sur les mêmes propriétés des paquets entrants ou sortants. Le degré de filtrage peut cependant varier, certains firewalls permettent un filtrage en travaillant les contenus des messages et peuvent se baser sur les connexions antérieures pour prendre leurs décisions (firewall statefull).

Les syntaxes pour décrire les règles sont également très variables suivant les constructeurs ou les OS : utilisation d'ACL (Access Control List) pour les routeurs/firewall Cisco ; utilisation du programme iptables pour les firewalls GNU/Linux ; …

3.3. La traduction d'adresse

La traduction d'adresse (NAT / PAT) est aussi un dispositif de sécurité complémentaire au filtrage dans la mesure où elle masque les adresses privées qui ne sont par conséquent plus visibles de l'extérieur. Les firewalls étant généralement intégrés aux routeurs qui possèdent de plus des fonctionnalités de traduction, il est nécessaire pour la compréhension des règles de routage et de filtrage de savoir dans quel ordre sont effectuées ces différentes opérations.

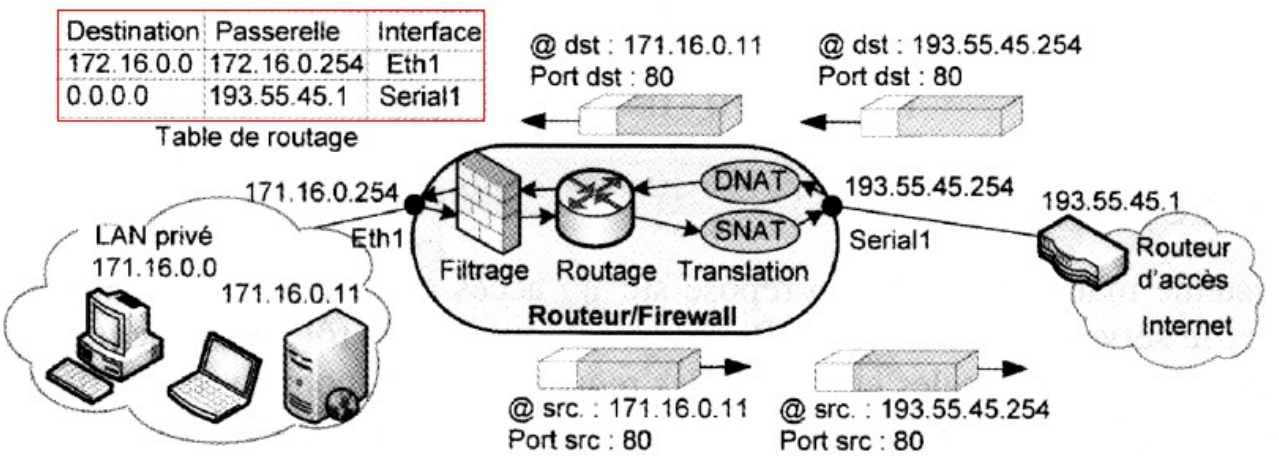
Pour un paquet entrant, la traduction concerne l'adresse de destination (celle qui est masquée) ; cette opération est nommée DNAT (Destination NAT). Il est nécessaire que la traduction soit réalisée avant le processus de routage puisque le routeur doit connaître l'adresse interne pour prendre sa décision.

Dans l'exemple décrit page suivante, le paquet entrant est destiné au serveur web interne.

L'adresse de destination qui est initialement celle du routeur (193.55.45.254), la seule visible de l'extérieur, est traduite vers celle du serveur web (171.16.0.11) grâce à l'indication du numéro de port 80. Le paquet peut ensuite être routé suivant la table et traité par la première règle du firewall, sur l'interface concernée (Eth1).

Pour un paquet sortant, la traduction concerne l'adresse source (celle qui doit être masquée) ; cette opération est nommée SNAT (Source NAT). Dans ce cas, le filtrage est d'abord effectué pour savoir si le paquet est autorisé à sortir. La traduction est ensuite réalisée après le processus de routage, en sortie du routeur.

Dans l'exemple, le paquet sortant provient du serveur web interne, il est autorisé à sortir par la deuxième règle du filtrage. Après routage, son adresse est traduite vers celle de l'interface de sortie du routeur (Serial1).

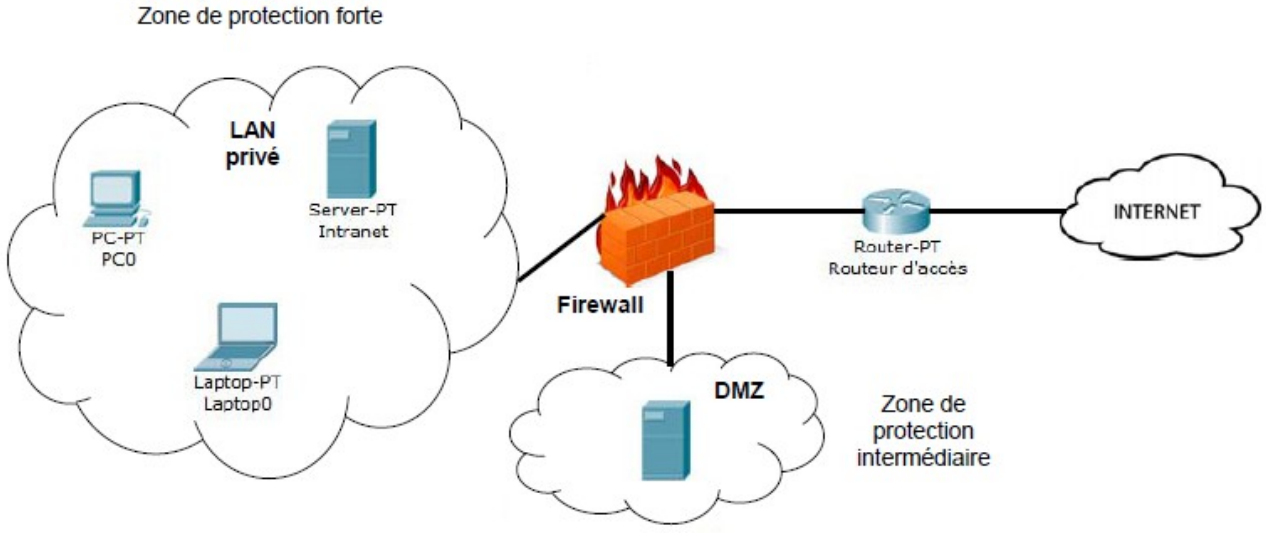


Règles de filtrage

Destination	Interface	@source	@dest.	Port src.	Port dst.
Entrant	Eth1	*	171.16.0.11	*	80
Sortant	Eth1	171.16.0.11	*	80	*

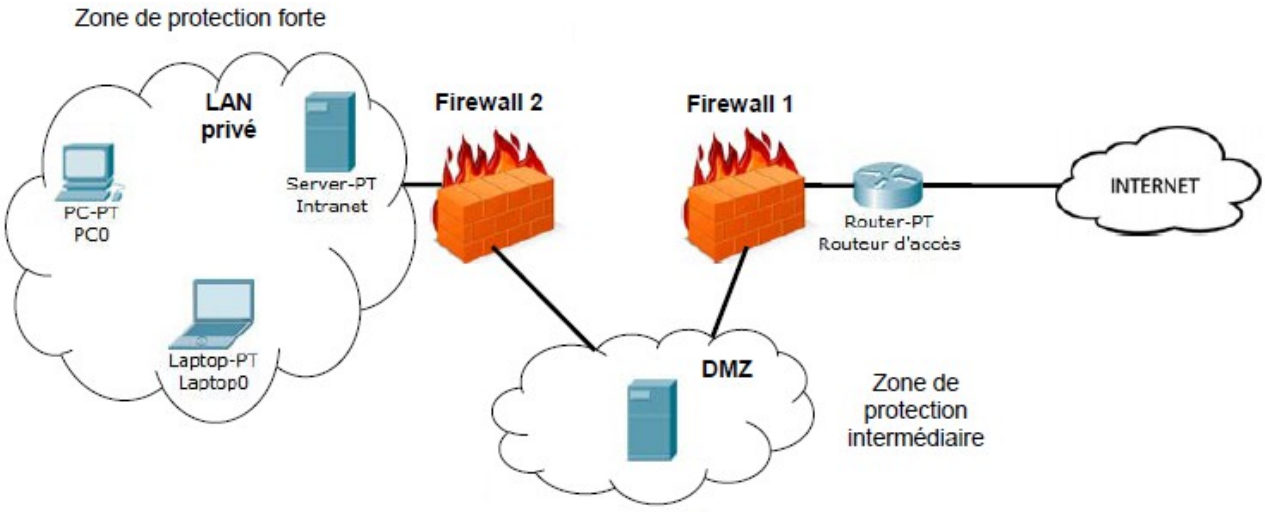
3.4. Les DMZ

Une zone démilitarisée (ou DMZ, DeMilitarized Zone) est une zone de réseau privée ne faisant partie ni du LAN privé ni de l'Internet. À la manière d'une zone franche au-delà de la frontière, la DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes.



DMZ simple

Un niveau supplémentaire de sécurité peut être introduit avec un deuxième firewall. Les règles d'accès sur le firewall du LAN privé sont plus restrictives. La DMZ est située entre deux firewalls (DMZ « en sandwich ») avec des règles moins restrictives introduites par le premier firewall.

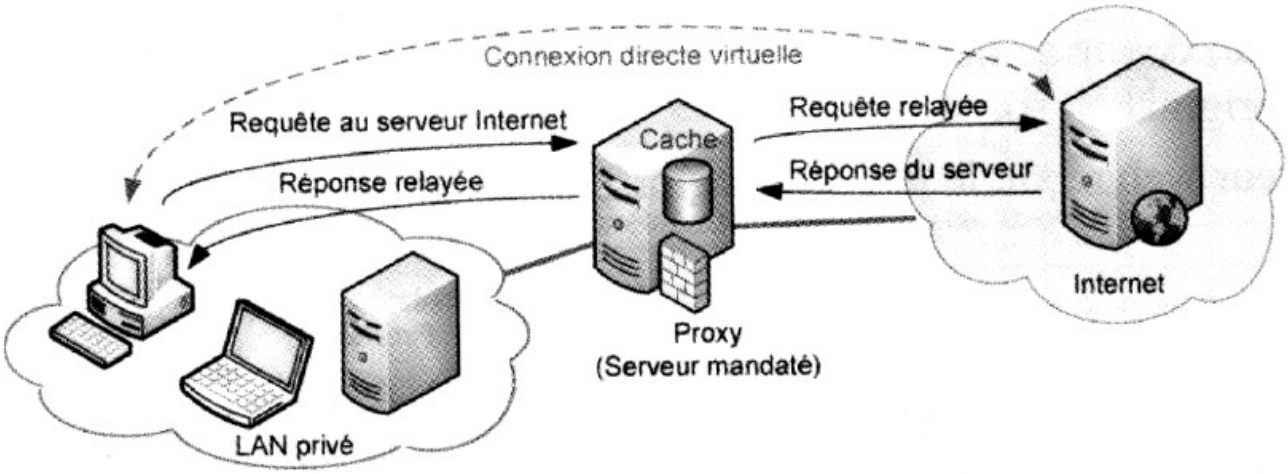


DMZ en sandwich

3.5. Les proxys

Un système mandataire (Proxy) repose sur un accès à l'Internet pour une machine dédiée : le serveur mandataire ou Proxy server, joue le rôle de mandataire pour les autres machines locales et exécute les requêtes pour le compte de ces dernières. Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (HTTP, FTP, SMTP, …) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, …).

Les serveurs mandataires configurés pour HTTP permettent également le stockage des pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés (Proxy cache).

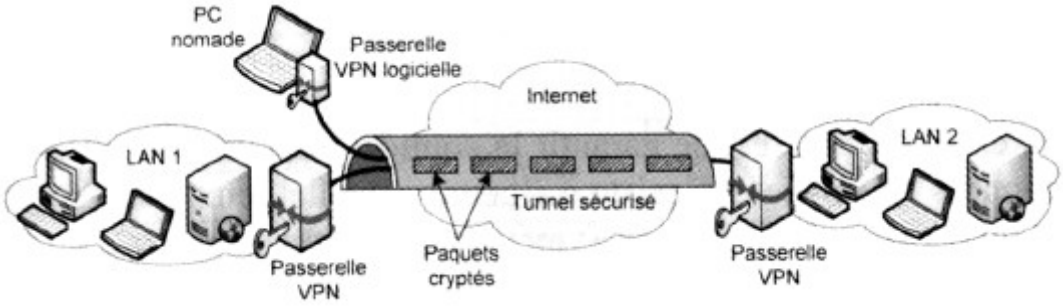


3.6. Les VPN

Le réseau privé virtuel (VPN, Virtual Private Network) est un élément essentiel dans les architectures modernes de sécurité. Un VPN est constitué d'un ensemble de LAN privés reliés à travers Internet par un « tunnel » sécurisé dans lequel les données sont cryptées. Les postes distants faisant partie du même VPN communiquent de manière sécurisée comme s'ils étaient dans le même espace privé, mais celui-ci est virtuel car il ne correspond pas à une réalité physique. Cette solution

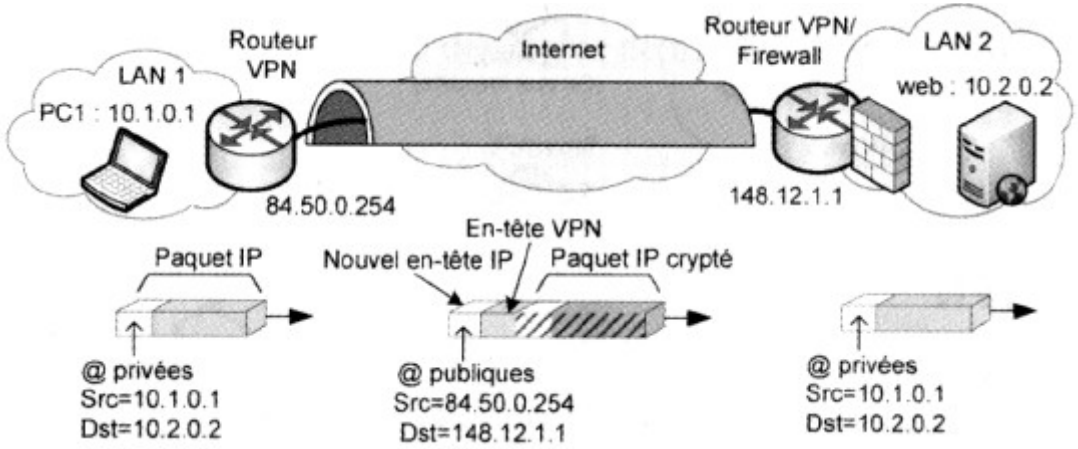
permet d'utiliser les ressources de connexion de l'Internet plutôt que de mettre en oeuvre, comme par le passé, une liaison spécialisée privée entre deux sites qui peut être très coûteuse si les sites sont fortement éloignés. La principale contrainte du VPN est de sécuriser les transmissions, par nature exposées sur les réseaux publics Internet.

Ci-dessous, les PC des deux LAN et le PC nomade font partie du même VPN. Les communications passent par des passerelles matérielles ou logicielles chargées d'identifier les extrémités du tunnel, de crypter les données et de les encapsuler dans un nouveau paquet en gérant un double adressage privé et public.



Principe du VPN

L'exemple ci-dessous permet de mieux comprendre le rôle des passerelles et la gestion des adresses.



Exemple de transfert dans un VPN

- le PC1 (10.1.0.1) envoie un paquet vers le serveur web (10.2.0.2) comme il le ferait si ce dernier était sur le même LAN ;
- le routeur qui joue le rôle de passerelle VPN encrypte le paquet, ajoute l'en-tête VPN et un nouvel en-tête IP avec les adresses publiques et relaie le paquet ;
- à l'autre extrémité, le routeur/firewall reçoit le paquet, confirme l'identité de l'émetteur, confirme que le paquet n'a pas été modifié, décapsule et décrypte le paquet ;
- le serveur web reçoit le paquet décrypté.

Les protocoles utilisés pour crypter les données, encapsuler le paquet et gérer les authentifications sont : PPTP, L2TP, L2F et IPSec.

4. Faille ARP

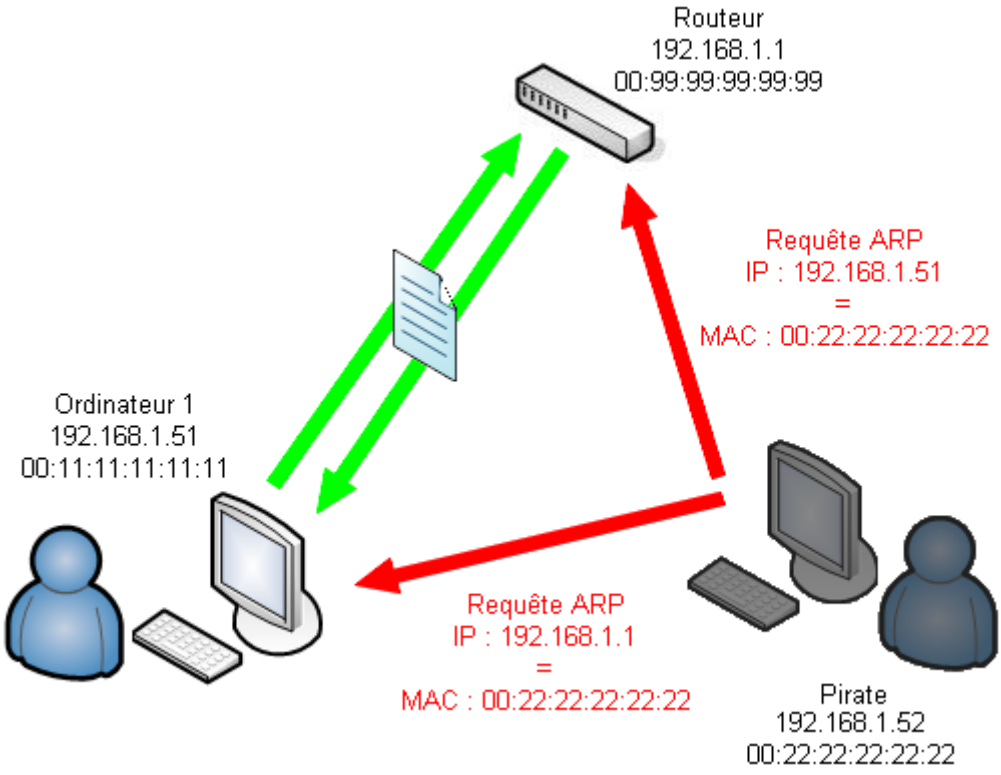
Le protocole ARP (Address Resolution Protocol) est utilisé pour établir une correspondance entre adresses IPv4 et adresses MAC des cartes réseau. On dispose d'un réseau en étoile dont les machines sont caractérisées par leur nom, leur adresse IP, leur adresse MAC :

- Routeur, 192.168.1.1, 00:99:99:99:99:99
- Ordinateur_1, 192.168.1.51, 00:11:11:11:11:11
- Ordinateur_2, 192.168.1.52, 00:22:22:22:22:22

Ordinateur_1 veut communiquer avec Routeur. Il connaît son adresse IP, mais la carte réseau a besoin de son adresse MAC pour lui transmettre le message. Il envoie donc une requête ARP en broadcast. Toutes les machines du réseau vont donc recevoir ce message et normalement, le routeur doit lui répondre. Ordinateur_1 va alors stocker cette information dans une table de correspondance, la table ARP, au cas où il en aurait à nouveau besoin plus tard. On peut visualiser le contenu de cette table en rentrant la commande :

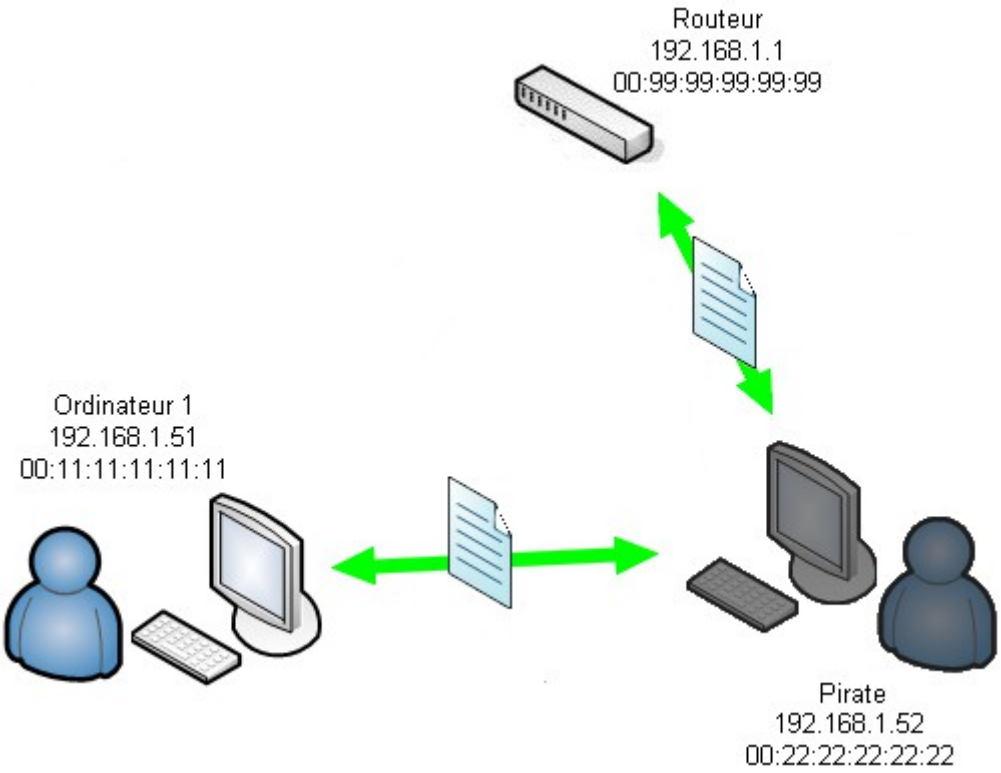
```
arp -a
```

Il est aisé pour une machine d'envoyer une requête ARP, aussi bien pour demander une adresse que pour en fournir une. Normalement, seule la machine dont l'adresse est demandée doit répondre à une requête. Mais en pratique, n'importe quelle machine peut le faire. Le routeur pourrait répondre que son adresse MAC est 00:33:33:33:33:33, Ordinateur_1 l'aurait pris en compte sans sourciller. Ainsi, si Routeur dit à Ordinateur_1 que l'adresse MAC de Ordinateur_2 est 00:55:55:55:55:55, il va prendre en compte cette information. Cela pose un problème : un attaquant peut manipuler les tables ARP des machines présentes sur le réseau et ainsi détourner le trafic : c'est l'attaque de l'homme du milieu (MITM : Man In The Middle).



Supposons que derrière Ordinateur_2 se trouve une personne indiscrète désireuse de savoir ce qui se

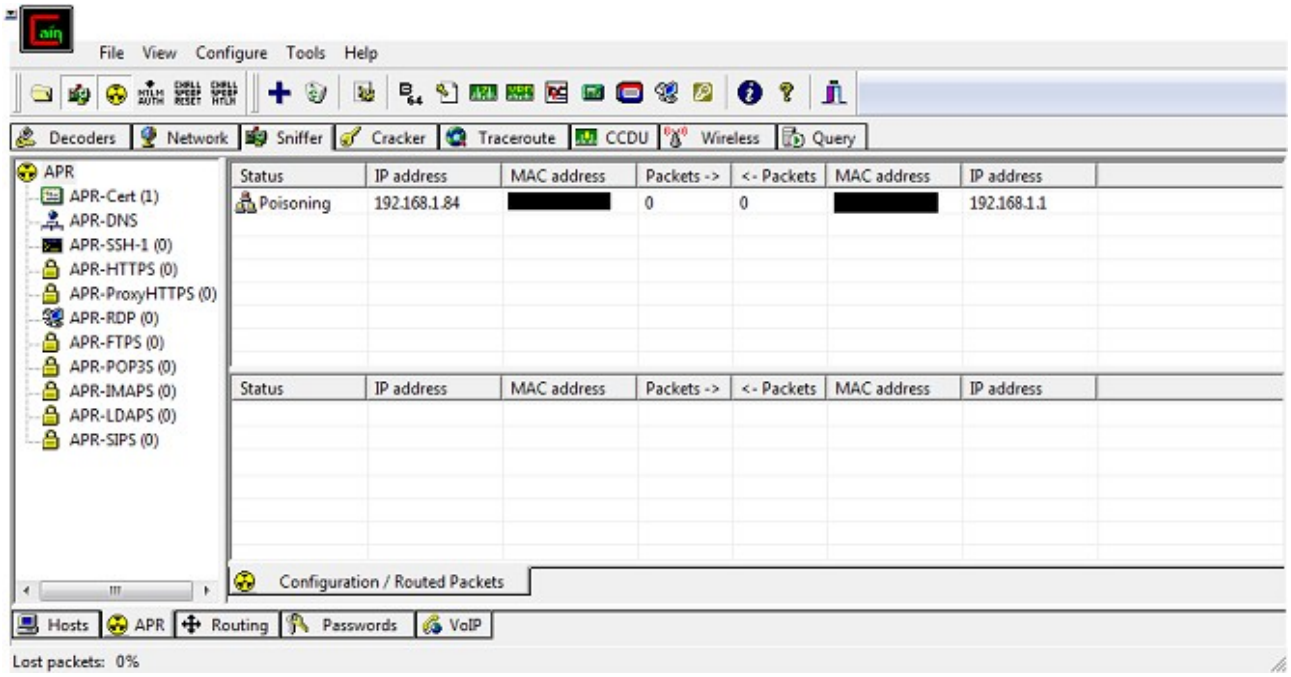
dit entre Ordinateur_1 et Routeur. Il lui suffit d'envoyer une requête ARP à Ordinateur_1 disant que l'adresse MAC associée à 192.168.1.1 (l'IP du routeur) est 00:22:22:22:22:22, et d'envoyer une autre requête à Routeur disant que l'adresse MAC associée à 192.168.1.51 est 00:22:22:22:22:22. De cette manière, tout échange de données entre Ordinateur_1 et Routeur passera par Ordinateur_2 ! Le pirate peut alors analyser le trafic, puisqu'il passe par sa propre carte réseau, mais aussi l'altérer, modifier les informations qui transitent...



Pour réaliser cette attaque, voici quelques logiciels utiles :

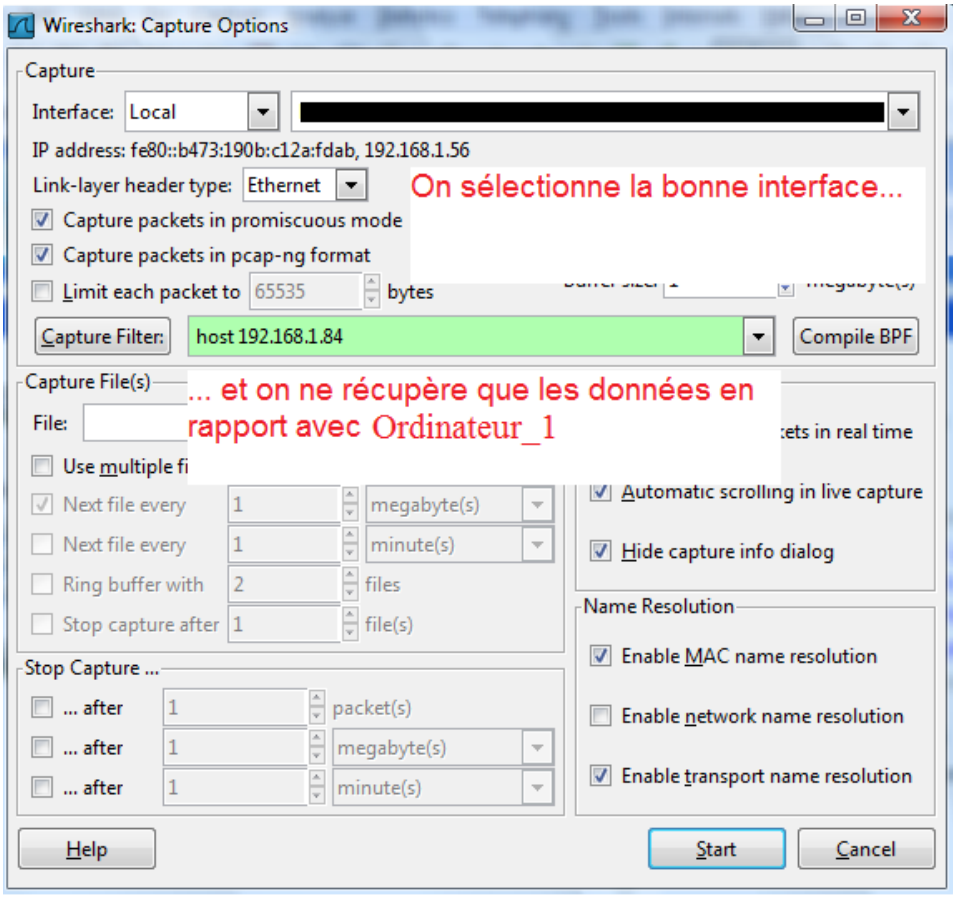
- nemesis, sous GNU/Linux, permet de forger des requêtes ARP, entre autres ;
- scapy, sous GNU/Linux, permet de forger des requêtes ou faire de l'analyse réseau par exemple ;
- Wireshark permet d'analyser les requêtes qui passent par la carte réseau ;
- Cain&Abel, sous Windows, permet de cracker des réseaux Wi-Fi et de mettre en œuvre une attaque MITM.

Exemple : soient 2 hôtes dans le réseau 192.168.1.0 : Ordinateur_2 (192.168.1.56) et Ordinateur_1 (192.168.1.84). Il y a aussi un routeur qui donne accès à Internet (192.168.1.1). Ordinateur_2 lance une attaque MITM entre Ordinateur_1 et le routeur.



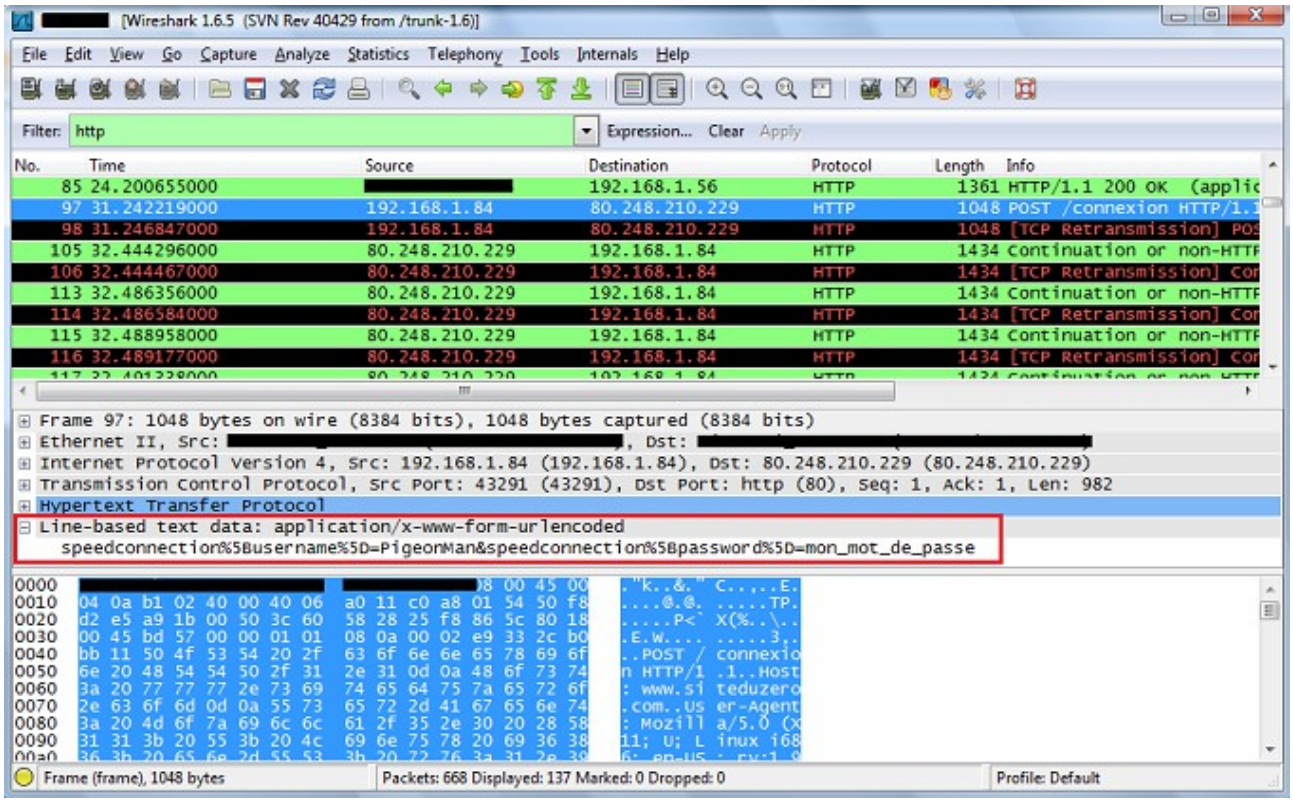
interface CAIN

Puis, sur Ordinateur_2, on lance l'analyseur de trafic Wireshark et on réalise une capture en ne demandant que les paquets en rapport avec Ordinateur_1.



Interface Wireshark

Il est alors possible de récupérer des données confidentielles (mot de passe par exemple)...



5. Exercices d'application

5.1. Énoncé

Le tableau ci-dessous représente un ensemble de règles de filtrage sur un firewall.

Règle	**Destination**	**@source**	**@dest.**	**Proto.**	**Port src.**	**Port dst.**	**ACK=1**
A	Entrant	Externe	Interne	TCP	>1023	21	
B	Sortant	Interne	Externe	TCP	21	>1023	
C	Sortant	Interne	Externe	TCP	>1023	21	
D	Entrant	Externe	Interne	TCP	21	>1023	Oui
E	Toutes	Toutes	Toutes	Tous	Tous	Tous	

Question 1 : Les transferts FTP vers un serveur interne sont-ils toujours autorisés ?

Question 2 : Les transferts FTP vers un serveur interne sont autorisés seulement si la connexion est initiée de l'extérieur ?

Question 3 : Les transferts FTP vers un serveur externe sont-ils toujours autorisés ?

Question 4 : Les transferts de courrier SMTP sont-ils autorisés dans les deux sens ?

Question 5 : Sur les routeurs Cisco, les ACL permettent de filtrer les paquets entrants ou sortants en

fonction des adresses IP source et destination.

Quelle règle de filtrage indique la commande ci-dessous (les adresses sources sont données en premier) ?

Access-list 101 deny ip any host 10.1.1.1

a) Autorisation des paquets IP provenant de n'importe quelle source et à destination de la machine 10.1.1.1.
b) Refus des paquets IP provenant de n'importe quelle source et à destination de la machine 10.1.1.1.
c) Refus des paquets IP provenant de la machine 10.1.1.1.

Question 6 : Sur les machines sous OS Linux, le programme « iptables » permet de réaliser le filtrage des paquets.

Que réalise la commande ci-dessous ?

Iptables -A INPUT -I eth0 -p icmp -j DROP

a) Le rejet de tous les « ping » entrants.
b) Le rejet des connexions entrantes vers un serveur web.
c) Le rejet de toutes les trames entrantes vers l'interface Ethernet 0.

Question 7 : La traduction d'adresse « NAT » permet :

a) D'utiliser davantage d'adresses privées que d'adresses publiques disponibles sur un site.
b) De réaliser le routage des paquets vers le réseau privé.
c) De filtrer les adresses entrantes qui ne correspondent pas à une machine du réseau privé.
d) De masquer les adresses privées à l'Internet.

Question 8 : Le rôle d'un système mandataire « proxy » est :

a) De relayer les requêtes des machines locales pour diverses applications sur Internet.
b) De centraliser les accès extérieurs pour sécuriser en un seul point les communications.
c) De filtrer les paquets en fonction de leur numéro de port.
d) D'enregistrer dans un cache les informations ou les fichiers fréquemment consultés.

Question 9 : Concernant les DMZ, quelles affirmations sont vraies :

a) Une DMZ inclut forcément un firewall.
b) Les serveurs web sont toujours placés à l'extérieur d'une DMZ.
c) Lorsque plusieurs DMZ sont installées, la plus proche du réseau privé est la moins sécurisée.
d) Une DMZ sert de zone intermédiaire entre un LAN et Internet.

Question 10 : Concernant les VPN, quelles affirmations sont vraies :

a) Un tunnel sécurisé est créé entre deux sites distants.
b) Des passerelles sont nécessaires pour isoler les réseaux privés du réseau public.
c) Les paquets qui circulent sur Internet sont cryptés.

d) Les utilisateurs doivent crypter tous les messages qu'ils envoient.

Question 11 : Vous décidez d'installer un VPN entre deux sites distants. Quels sont les protocoles que vous pouvez utiliser ?

a) WEP
b) PPTP
c) IPSec
d) SNMP
e) L2TP

Question 12 : La règle A du firewall (voir ci-dessous) permet aux machines du LAN privé d'accéder à DMZ 2, alors que la règle C devait l'interdire. Comment remédier à cela ?

Règle	**Destination**	**@source**	**@dest.**	**Proto.**	**Port src.**	**Port dst.**
A	Toutes	DMZ	2	TCP	Tous	80
B	LAN	DMZ	1	TCP	Tous	25
C	LAN	Toutes	TCP	Tous	Tous	Autorisé
D	Toutes	Toutes	Tous	Tous	Tous	Refusé

5.2. Correction

Question 1 : oui

Question 2 : non

Question 3 : non

Question 4 : oui

Question 5 : b

Question 6 : a

Question 7 : a et d

Question 8 : a, b et d

Question 9 : a et d

Question 10 : a, b et c

Question 11 : b, c et e

Question 12 : Une solution est de passer la règle A en troisième position :

Règle	**Destination**	**@source**	**@dest.**	**Proto.**	**Port src.**	**Port dst.**
B	LAN	DMZ	1	TCP	Tous	25
C	LAN	Toutes	TCP	Tous	Tous	Autorisé

A	Toutes	DMZ	2	TCP	Tous	80
D	Toutes	Toutes	Tous	Tous	Tous	Refusé

La règle B permet aux machines du LAN d'accéder à DMZ 1. La règle C interdit tout autre trafic en provenance du LAN. La règle A n'a plus d'influence sur le trafic du LAN et permet aux machines externes d'accéder à DMZ 2.