Pare-feu

Présentation

Un **Pare-feu** [appelé aussi Coupe-feu, Garde-barrière ou **Firewall**], 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 (cartes réseau) suivantes :

- Une interface pour le réseau à protéger (réseau interne),
- Une interface pour le réseau externe.

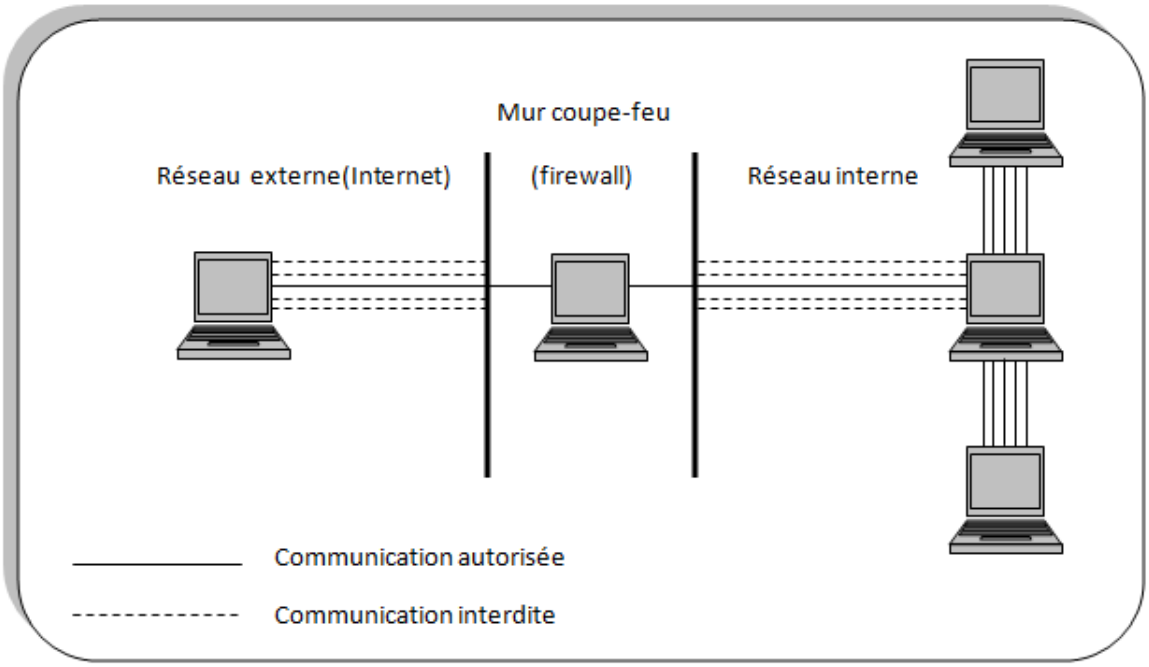

Figure I.1: Pare-feu

La configuration du Firewall est telle que les données arrivant sur l'une des cartes ne soient pas transmises directement sur l'autre mais de manière sélective, selon des critères de filtrage déterminés lors de sa configuration.

Le filtrage réalisé par le Pare-feu constitue le premier rempart de la protection du système d'information.

Le système Pare-feu est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local [ou la machine local] et un ou plusieurs

réseaux externes. Il est possible de mettre un système Pare-feu sur n'importe qu'elle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic,
- 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**.

Selon la nature de l'analyse et de traitements effectués par un Firewall, différents types de Firewalls existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent : niveau 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP, etc.) du modèle OSI. Dans le cas de la fonction du routeur (Firewall routeur), il analyse chaque paquet de données selon les informations contenant dans le paquet (adresses IP, numéro de port, type de paquet).

Les Pare-feu de base opèrent sur un faible nombre de couches du modèle TCP/IP, tandis que les plus sophistiqués en couvrent un plus grand nombre et sont ainsi plus efficaces

Indépendamment ou en complément d'une architecture utilisant ces dispositifs, il existe des services additionnels tels : la traduction d'adresse réseau (NAT) et les réseaux privés virtuels (VPN).

Principe de fonctionnement

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 : « tout ce qui n'est pas explicitement autorisé est interdit »,
- Soit d'empêcher les échanges qui ont été explicitement interdites.

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

Les différents types de filtrage

• Filtrage simple de paquets

Un système Pare-feu fonctionne sur le principe du **filtrage simple de paquets** (stateless packet filtring). 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 échangés 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.

• 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 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 client.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir des 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 anglosaxon est **stateful inspection** ou stateful paket filtring, se traduit en français par « 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 coté du Pare-feu. L'ensemble des paquets transitant dans le cadre de cette connexion sont implicitement acceptés par le Pare-feu.

- **Filtrage applicatif**

Le filtrage applicatif permet comme son nom l'indique de filtrer les communications application par application. Ce filtrage opère donc au niveau 7 (couche application) du modèle OSI. Le filtrage applicatif suppose donc, une connaissance des applications présentes sur le réseau, et notamment de la manière dont les données sont 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 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.

Pare-feu personnel

Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le firewall est installé on parle de Firewall personnel (pare-feu personnel).

Ainsi, un Firewall personnel permet de contrôler l'accès au réseau des applications installées sur la machine, et notamment empêcher les attaques du type cheval de Troie, c'est-à- dire des

programmes nuisibles ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un pirate informatique.

Le Firewall personnel permet en effet de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées à se connecter.

Zone démilitarisée (DMZ)

Les systèmes 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-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de cloisonnement des réseaux (le terme isolation est parfois également utilisé).

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie, 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 démilitarisée (notée DMZ, Demilitarised 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.

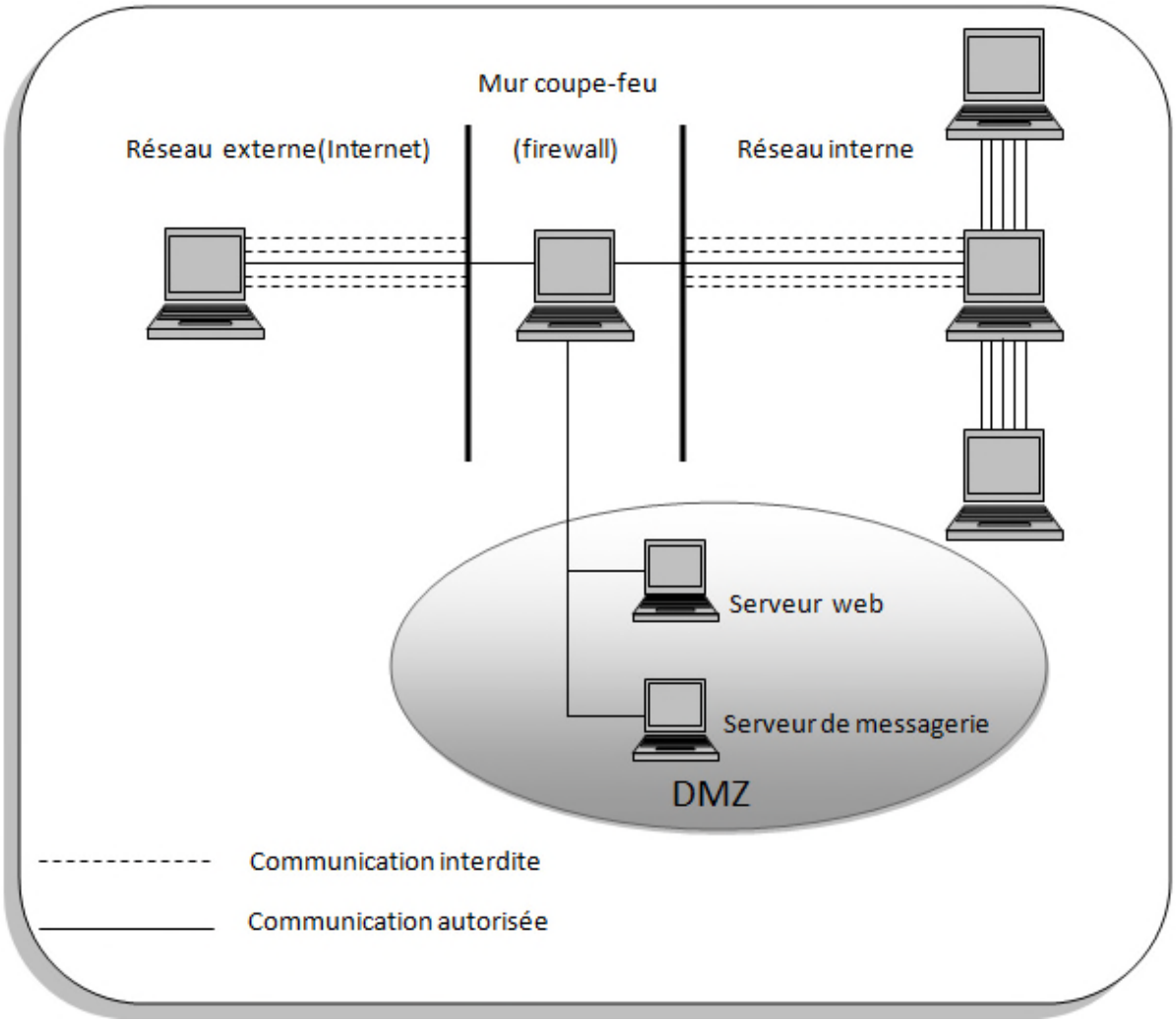

Figure I.2: Exemple d'une zone démilitarisée (DMZ)

La politique de sécurité mise en oeuvre sur la DMZ est généralement la suivante :

- trafic du réseau externe vers la DMZ autorisé,
- trafic du réseau externe vers le réseau interne interdit,
- trafic du réseau interne vers la DMZ autorisé,
- trafic du réseau interne vers le réseau externe autorisé,
- trafic de la DMZ vers le réseau interne interdit,
- trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques de l'entreprise.

Les limites de système Pare-feu

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.

Introduction

Les réseaux locaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseaux avec le développement des commutateurs.

En effet, dans un réseau local, la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels, il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole).

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel, les protocoles de transport et les protocoles d'administration et de gestion des réseaux locaux virtuels, mais avant tout, nous commencerons par un rappel sur le principe de la commutation.

Rappels sur la commutation

Les commutateurs ne sont rien d'autre que des ponts filtrants, certes équipés de fonctions plus nombreuses et de performances qui n'ont rien de comparable aux ponts que nous utilisons depuis plusieurs années.

Le travail de base d'un commutateur est de gérer des tables d'adressage : savoir sur quel port se trouve une adresse MAC afin d'éviter de diffuser le trafic inutile sur les segments des autres machines. Le nombre d'adresses MAC par port fait partie des caractéristiques du produit auxquelles l'administrateur du réseau doit s'intéresser afin de choisir le switch approprié.

Lorsque le réseau n'est pas bouclé (c'est-à-dire que pour aller d'un point à un autre du réseau il y a un et un seul chemin), cette gestion de table d'adresses MAC est suffisante. Lorsqu'il peut y avoir plusieurs chemins pour aller d'un point à un autre du réseau il est nécessaire d'utiliser en plus des arbres de recouvrement (spanning-tree en anglais).

Spanning-Tree

Le protocole STP est un protocole de couche 2 qui permet de construire des structures de réseau redondantes dans lesquelles les commutateurs sont interconnectés dans plus d'un endroit, afin de maintenir une tolérance aux pannes. Traditionnellement, cette conception peut entraîner la mise en boucle infinie du trafic broadcast et de quelques autres paquets, tout en provoquant une chute significative des performances du réseau car les données reçues sur une interface et transmises à une autre rebondissent en effet vers l'expéditeur.

Lors de la conception d'un réseau, il est souvent difficile d'éviter les boucles broadcast accidentelles. Il est également parfois souhaitable de concevoir des architectures avec de boucles

potentielles (dans lesquelles un commutateur se connecte à deux commutateurs ou plus), car ce type de conception a une meilleure tolérance aux pannes et permet qu'un seul périphérique ou un seul lien soit retiré sans scinder l'ensemble du réseau en deux parties totalement isolées. Pour permettre la création de boucles et d'autres architectures complexes sans entraîner de sérieux problèmes de performances, le protocole STP implémente un mécanisme d'élection afin de choisir un noeud de commutation "racine". En fonction du résultat de cette élection, une hiérarchie arborescente du trafic est établie à partir de ce noeud et les liens qui pourraient provoquer une inversion de la propagation du trafic broadcast sont temporairement bloqués.

Domaine de Collision

Un domaine de collision est un ensemble d'entités (cartes réseaux) qui partagent le même média de communication. Tous les environnements à supports partagés, notamment ceux que vous créez au moyen de concentrateurs, sont des domaines de collision (Figure 2.1). Plus il y a de stations connectées par le biais d'un appareil fonctionnant au niveau 1 du modèle OSI, plus il y a de risques de collision.

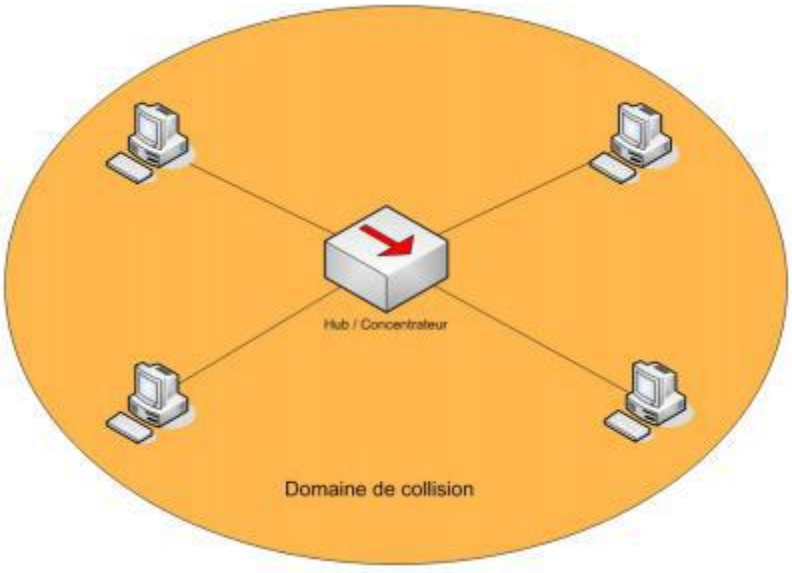

Figure 2.1 : Domaine de Collision avec un Hub.

Pour résoudre ce problème nous devons alors remplacer le hub par un commutateur (voir la figure 2.2), lequel crée une connexion réseau dédiée. Cette connexion est interprétée comme un domaine de collision individuel puisque le trafic reste indépendant de toutes les autres formes de trafic informatique, autrement dit il y aura alors un domaine de collision par port du Switch, et le fait que le port du Switch soit branché sur une unique carte réseau, élimine le risque de collision.

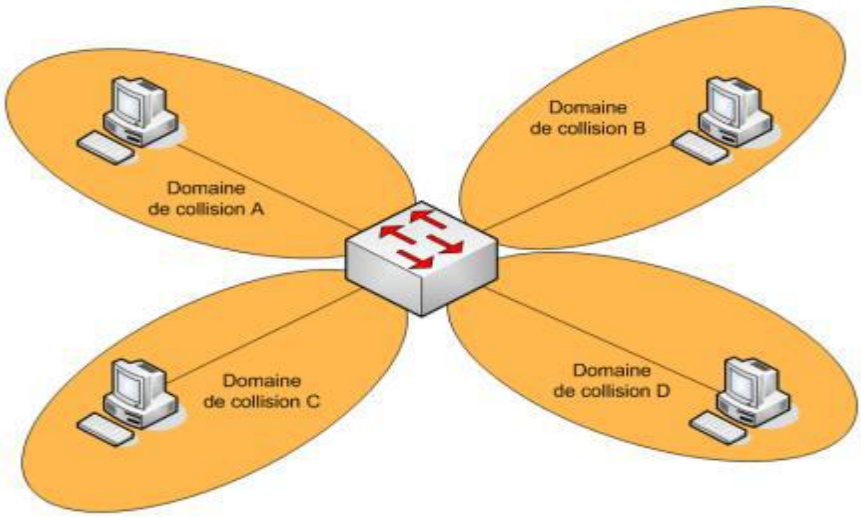

Figure 2.2 : Domaine de collision avec un Switch.

L'étendue et le nombre de domaines de collisions dépendent donc de l'équipement sur lequel les entités sont connectées.

Domaine de diffusion

Le domaine de diffusion sur la couche 2 est désigné par l'expression « domaine de diffusion MAC ». Ce domaine comprend tous les périphériques du réseau local qui reçoivent d'un hôte les trames de diffusion destinées à tous les autres ordinateurs du réseau local, il faut noter aussi qu'un domaine de diffusion englobe plusieurs domaines de collisions.

Quand on parle de domaine de diffusion, on prend l'hypothèse où l'entité émettrice souhaite envoyer une donnée à tout le monde. (Voir la Figure 2.3).

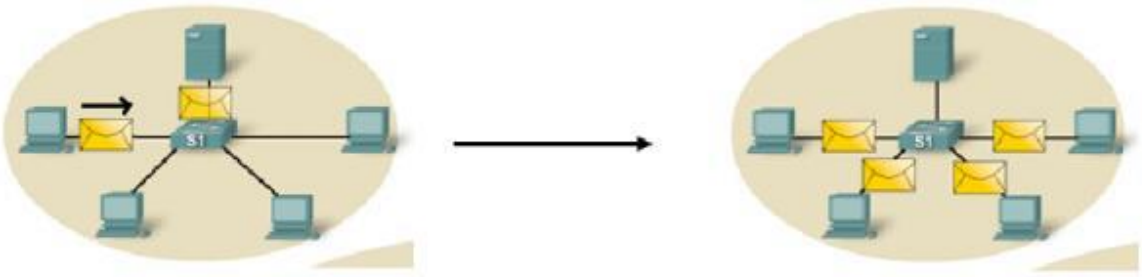

Figure 2.3 : Domaine de diffusion.

Dans le LAN, que ce soit avec un Hub, ou un Switch, la donnée sera propagée sur tous les ports parce que:

- Un hub ne lit pas le niveau 2 donc il transmet la donnée sur tous ses ports.

- Un Switch lit le niveau 2 et comprend que la donnée est à destination de tout le monde (adresse MAC destination = ffff.ffff.ffff) donc il transmet cette donnée sur tous ses ports.

Il faut donc réduire le domaine de broadcast, et pour ce faire nous devons utiliser une fonctionnalité qui existe sur le Switch qui est la possibilité de "découper" le domaine de broadcast en plusieurs domaines de broadcast plus petits pour exploiter au maximum la bande passante de chaque domaine de collision. On ne parle plus alors de LAN mais de VLAN (Virtual LAN).

VLAN (Virtual Local Area Network)

Le développement rapide d'Internet a mené de nombreuses entreprises à étendre leur installation informatique. La technologie VLAN apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances.

Définition d'un VLAN

Ce nom générique désigne un ensemble de méthodes utilisées pour diviser un groupe de ports sur un dispositif physique en un ensemble de réseaux logiques distincts, ce qui isole le trafic sur un groupe de ports et empêche tout type de trafic de se croiser au niveau du commutateur (ce système est le plus souvent implémenté en utilisant la norme IEEE 802.1Q).

Implémenter un réseau local virtuel revient à scinder un seul commutateur en plusieurs périphériques totalement indépendants, à la différence de la solution VLAN, qui est beaucoup plus souple et économique car il est possible de transformer le réseau et de réaffecter les ressources matérielles à volonté. Les administrateurs réseau du monde entier ont accueilli chaleureusement les VLANs car ils offrent un moyen simple mais puissant de construire un ensemble de réseaux distincts sur un seul périphérique ou, par exemple, de séparer les serveurs des postes de travail sans avoir besoin d'acheter un commutateur dédié pour chaque groupe. Un réseau Ethernet avec deux VLANs est présenté comme exemple dans la figure 2.4.

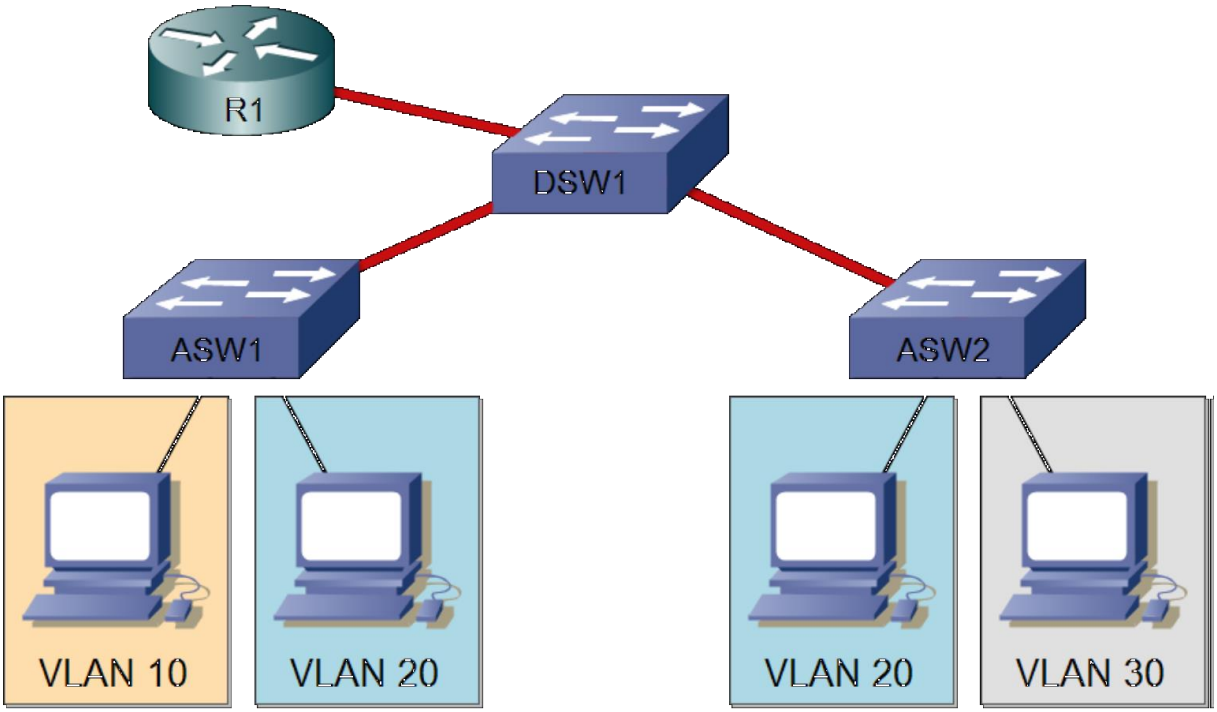

Figure 2.4 : Plusieurs VLANs dans un réseau Ethernet.

Avantages des VLANs

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages et permet de nombreuses applications intéressantes.

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

 Flexibilité de segmentation du réseau : Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en plusieurs VLANs en même temps.

 Simplification de la gestion : L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

 Augmentation considérable des performances du réseau : Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.

 Meilleure utilisation des serveurs réseaux : Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire appartenir le serveur à plusieurs VLANs en même temps. Cette appartenance à de multiples VLANs permet de réduire le trafic qui doit être routé (traité au niveau du protocole de niveau supérieur, par exemple IP) du et vers le serveur, et donc d'optimiser le trafic. Tout comme le découpage d'un disque dur en

plusieurs partitions permet d'augmenter les performances (la fragmentation peut être diminuée) de son ordinateur, le VLAN améliore considérablement l'utilisation du réseau.

 Renforcement de la sécurité du réseau : Les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.

 Technologie évolutive et à faible coût : La simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs.

 Régulation de la bande passante : Un des concepts fondamentaux des réseaux Ethernet est la notion d'émission d'un message réseau vers l'ensemble (broadcast ou multicast) des éléments connectés au même commutateur (hub/Switch). Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic disponible au sein de l'infrastructure.

Applications courantes du VLAN

- deux VLANs regroupant d'une part les périphériques et, d'autre part les utilisateurs.
- création des VLANs dans un bâtiment permet de regrouper les utilisateurs par catégories alors qu'ils sont situés à des endroits différents.
- priorisation des flux en fonction des catégories d'utilisateurs.
- réseau de quarantaine : lorsqu'une station manifeste une activité anormale au lieu de lui couper complètement l'accès au réseau, on la place dans un réseau de quarantaine qui permet de conserver la connectivité réseau tout en limitant la portée de la contamination et en évitant de polluer l'intranet avec du trafic inutile.
- réseau d'administration.

Classification des VLANs

Les VLANs déployés sur plusieurs commutateurs sont classés suivant deux types:

1) les VLANs implicites : lorsqu'un message Ethernet passe d'un commutateur (Switch). Tout élément connecté à un Switch peut accéder à tout autre élément du même VLAN connecté sur le même Switch. Le mode de transmission du Switch permet de mettre directement en relation deux postes.

2) les VLANs explicites : une étiquette (tag) d'appartenance à un VLAN est ajoutée à chaque Ethernet.

Pour définir des VLANs, il faut que les commutateurs supportent cette extension de la technologie Ethernet (IEEE 802.1q).

Types de VLANs

Les échanges à l'intérieur d'un domaine sont sécurisés et les communications inter domaines sont autorisées et peuvent être contrôlées (autorisation ou interdiction de communiquer avec une ou plusieurs stations d'un autre domaine). L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue:

1) les VLAN de niveau 1 ou VLAN par port (*Port-Based* VLAN) :

Ces VLANs regroupent des stations connectées à un même port du commutateur (figure2.5). La configuration est statique, le déplacement d'une station implique son changement de VLAN. C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN. Un port, donc les stations qui lui sont raccordées, peut appartenir à plusieurs VLANs.

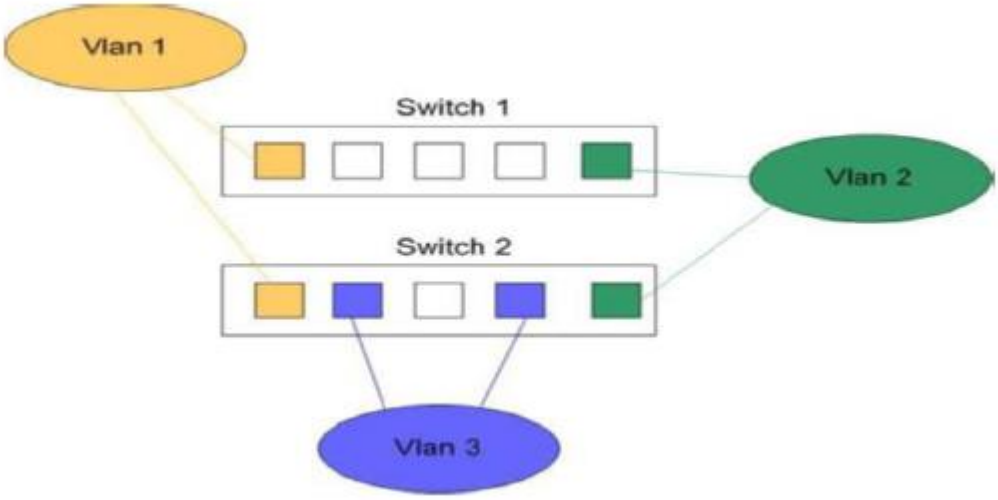

Figure 2.5 : VLAN par port.

2) les VLAN de niveau 2 ou VLAN MAC (*MAC Address-Based VLAN*) :

Ces VLANs associent les stations par leur adresse MAC. De ce fait, deux stations raccordées à un même port (segment) peuvent appartenir à deux VLANs différents, comme présenté dans la figure 2.6. Les tables d'adresses sont introduites par l'administrateur.

Il existe des mécanismes d'apprentissage automatique d'adresses, l'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration (Drag&Drop). Une station peut appartenir à plusieurs VLANs. Les

VLANs de niveau 2 sont indépendants des protocoles supérieurs. La commutation, s'effectuant au niveau MAC autorise un faible temps de latence (commutation très efficace).

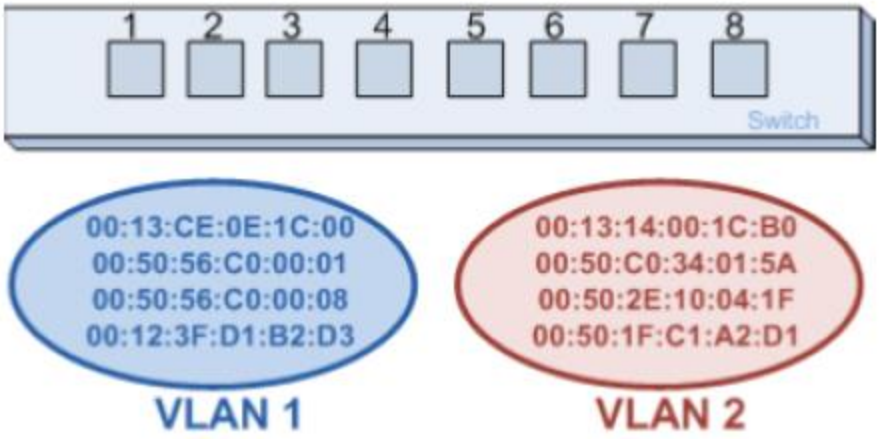

Figure 2.6 : VLAN par adresse MAC.

3) les VLANs de niveau 3 ou VLANs d'adresses réseaux (*Network Address-Based VLAN*) :

Ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (subnet d'IP) comme illustré dans la figure 2.7. Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN. Une station peut appartenir à plusieurs VLANs par affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur doit accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage. L'en-tête n'est pas modifié.

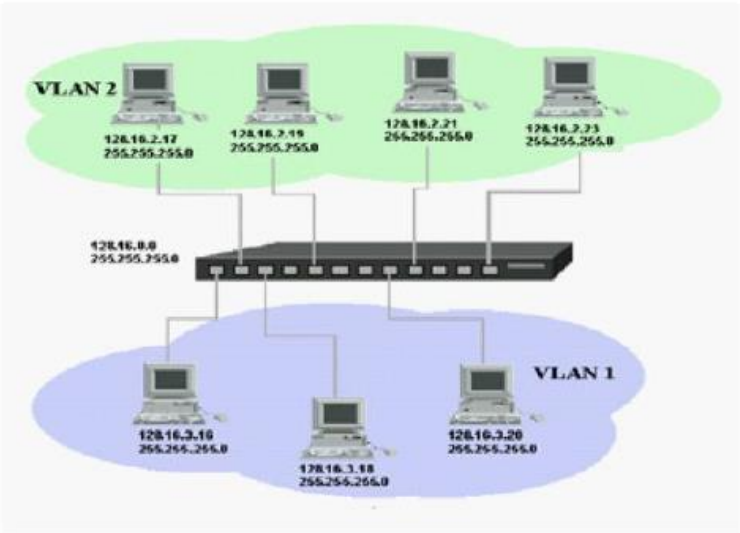

Figure 2.7 : Construction des VLANs par sous réseau.

Il est aussi envisageable de réaliser des VLANs par :

 protocole (IP, IPX...) : la communication ne peut s'établir qu'entre stations utilisant le même protocole.

 application (N◦ de port TCP) : la constitution des VLANs est alors dynamique, un utilisateur peut successivement appartenir à des VLANs différents selon l'application qu'il utilise.

 mot de passe (constitution dynamique des VLANs au login de l'utilisateur).

Les protocoles de transport des VLANs

Afin d'assurer le transport des VLANs, certains protocoles ont été mis en place :

L'identification des VLANs (802.1Q)

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire (filtrage de trafic). Lorsque le réseau est important, les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames (figure 2.8). L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLANs d'appartenance des stations qui lui sont raccordées. La norme IEEE 802.1Q définit l'étiquetage des trames.

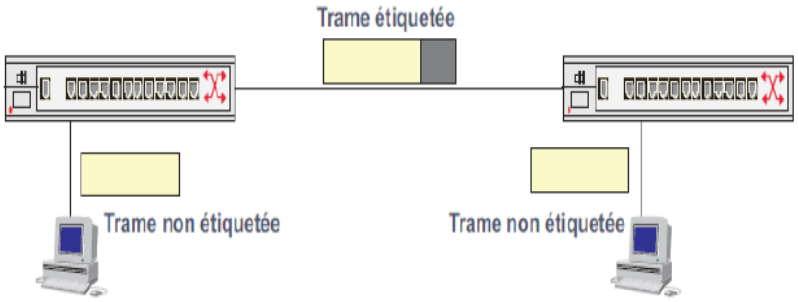

Figure 2.8 : Principe de l'étiquetage des trames dans les VLANs.

La norme IEEE 802.1p/Q

Un VLAN correspond à un domaine de broadcast. Cependant, lorsque plusieurs VLAN sont définis sur un même segment, cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le broadcast en une rafale d'unicasts. La solution adoptée par l'IEEE est toute différente : un seul VLAN peut être déclaré par port, les VLANs sont définis dans les normes 802.1Q et 802.1p qui introduisent quatre octets supplémentaires dans la trame MAC afin d'identifier les VLANs (VLAN tagging) et de gérer 8 niveaux de priorité (Qualité of Service, QoS). La figure 2.9 illustre le format de la trame 802.1p/Q.

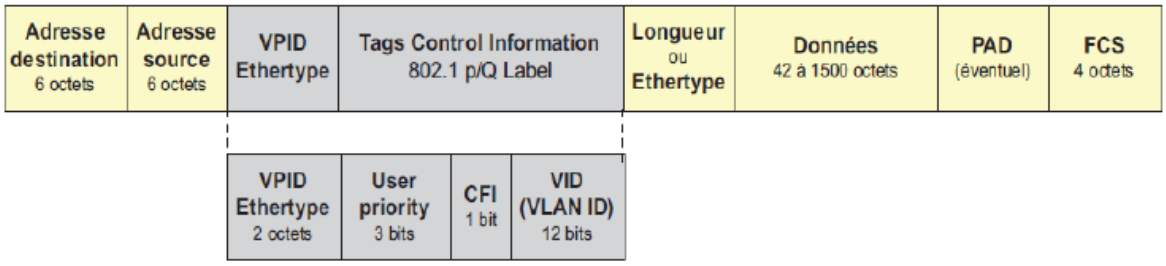

Figure 2.9 : Format de la trame 802.1p/Q.

Pour garantir la compatibilité avec l'existant, le marquage des trames est vu comme une encapsulation supplémentaire. Ainsi, le champ **VPID** (*VLAN Protocol ID*) est similaire au champ Ethertype de la trame 802.3, il identifie le format 802.1 p/Q, sa valeur est fixée à 0x8100. Les deux octets suivants permettent de définir huit niveaux de priorité (*User Priority*).

Les commutateurs de dernière génération disposent de plusieurs files d'attente, les trames sont affectées à telle ou telle file suivant leur niveau de priorité.

Le bit **CFI** (*Canonical Format Identifier*) est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0. Dans les réseaux Token Ring, à 1, il indique que les données du champ routage par la source sont au format non canonique.

Le champ **VID** (*VLAN IDentifier*) identifie sur douze bits le VLAN destination. L'introduction de quatre octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS. On commence à trouver des cartes transporteurs capables de supporter le tagging.

Réseaux privés virtuels

Présentation

Il arrive ainsi souvent que les entreprises éprouvent le besoin de communiquer avec les filiales, des clients ou même du personnel géographiquement éloignées via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi, il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La solution consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (tunneling), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données.

Mise en oeuvre de liaisons sécurisées

L'échange de données confidentielles entre les personnels nomades et l'entreprise ou entre différentes entités implique la mise en oeuvre de liaisons sécurisées, physiques (lignes louées spécialisées) ou virtuelles (VPN) en liaison avec un Pare-feu.

Trois types de solutions de VPN existent associées avec un Pare-feu :

- Intégrée comme service du Pare-feu,
- Systèmes autonomes placés devant le Pare-feu,
- Systèmes autonomes placés derrière le Pare-feu (solutions logicielles).

L'échange de données entre sites distants de la même entreprise peut aussi être effectué en utilisant une liaison spécialisée ou dédiée utilisant les services d'un opérateur de

télécommunication. Cette solution permet de s'affranchir de toutes les menaces liées à l'utilisation du réseau Internet, mais elle représente un coût plus important.

Fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling, c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

L'expression tunnel chiffré est utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du coté de l'organisation.

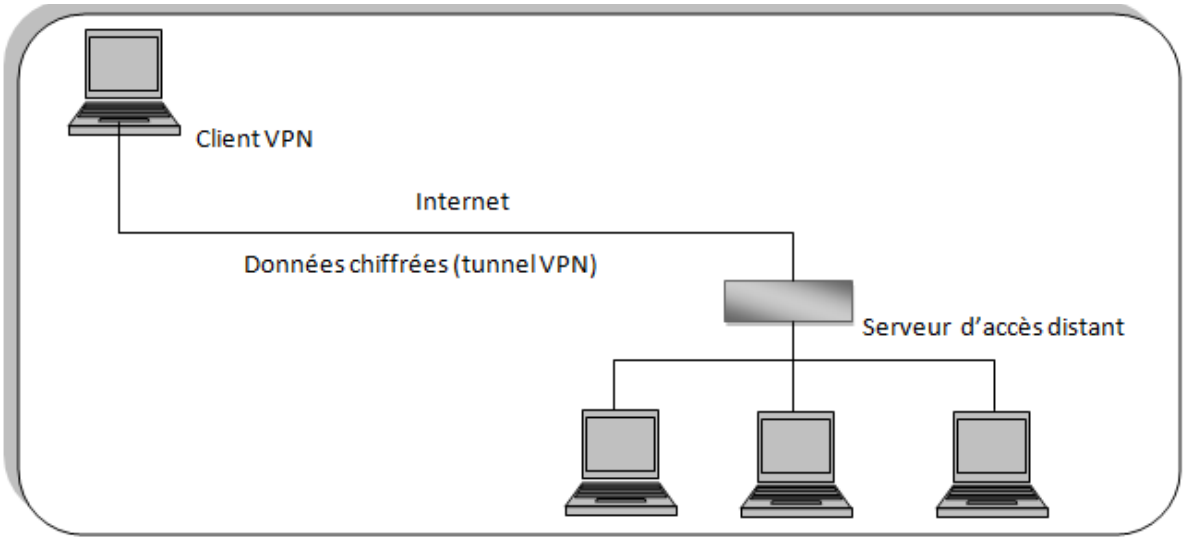

Figure I.1: Réseau privé virtuel (VPN)

De cette façon, lorsqu'un utilisateur a besoin d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée.

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur.

Protocoles de tunneling

Les principaux protocoles de tunneling sont les suivants :

- **PPTP** (point-to-point tunneling protocol) est un protocole de niveau 2 développé par Microsoft, 3 Com, Ascend, US Robotics et ECI Telematics,
- **L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi obsolète,
- **L2TP** (Layer Two Tunneling Protocole) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2,
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP [1].