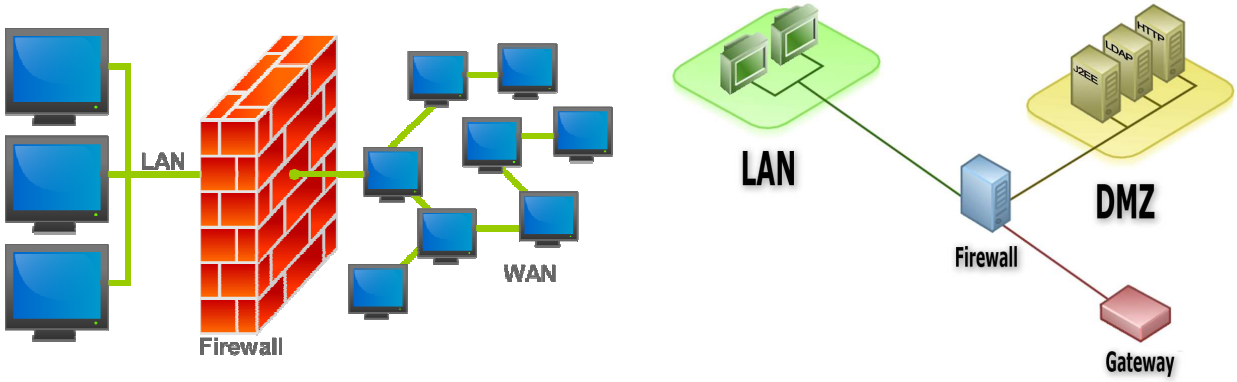
LES DÉFENSES MATÉRIELLES



Objectifs du COURS :

Ce cours traitera essentiellement les points suivants :

- les firewalls
- la traduction d'adresse (DNAT, SNAT)
- les DMZ (simple et en « sandwich »)
- les proxys
- les VPNs
- QCM et exercices d'applications

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).

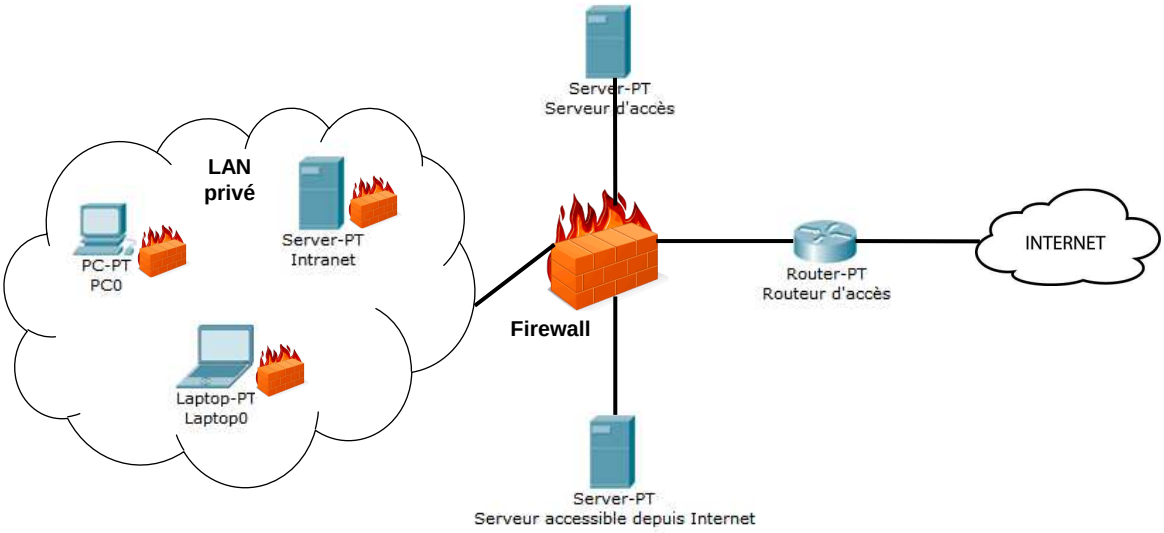
Par ailleurs, quelques principes de base doivent être respectés pour assurer l'efficacité des défenses :

- **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.

LES FIREWALLS

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



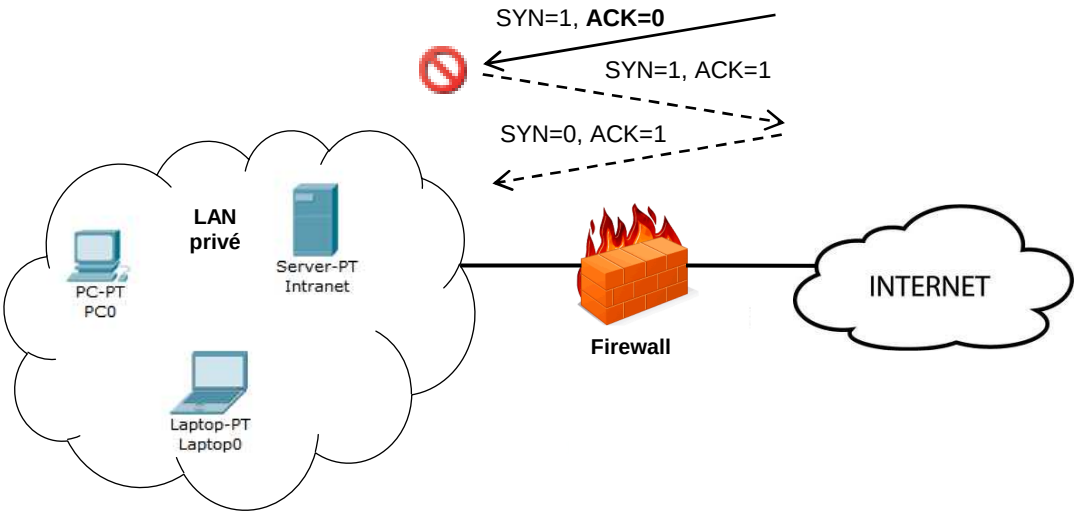
Rôle et situation du firewall

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 correspondant 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.



Blocage des connexions entrantes

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.	Action
A	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	80	Autorisé
B	Entrant	0.0.0.0	192.168.0.0	TCP	80	>1023	Autorisé
C	Sortant	192.168.0.0	0.0.0.0	TCP	>1023	25	Autorisé
D	Entrant	0.0.0.0	192.168.0.0	TCP	25	>1023	Autorisé
E	Toutes	0.0.0.0	0.0.0.0	Tous	Tous	Tous	Refusé

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 (bien sûr !) ; utilisation du programme iptables pour les firewalls Linux (of course !) ; …

LA TRADUCTION D'ADRESSE

Remarque :

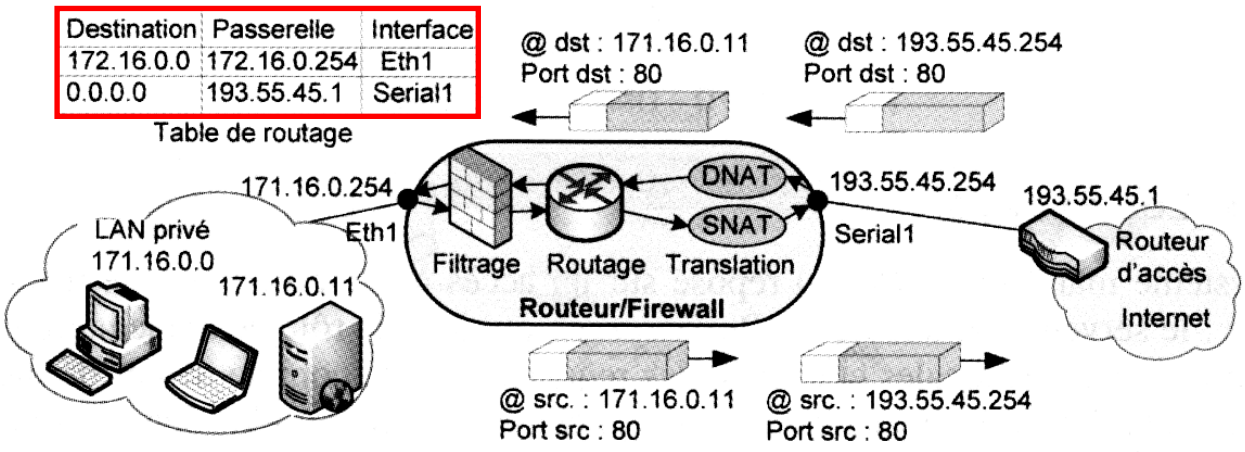
Voir cours sur le mécanisme de la NAT et de la PAT.

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).



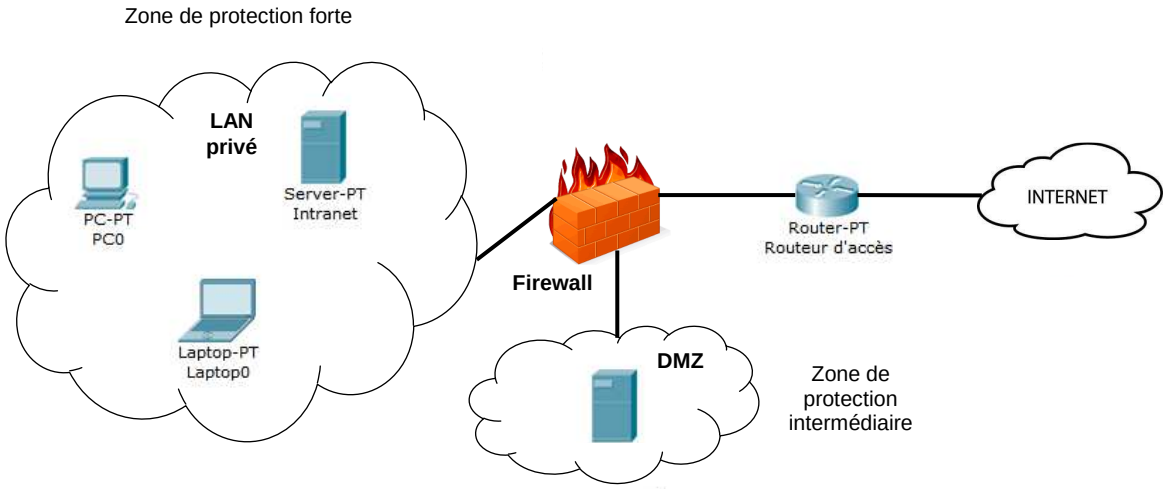
Règles de filtrage

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

Exemple : NAT, routage et firewall

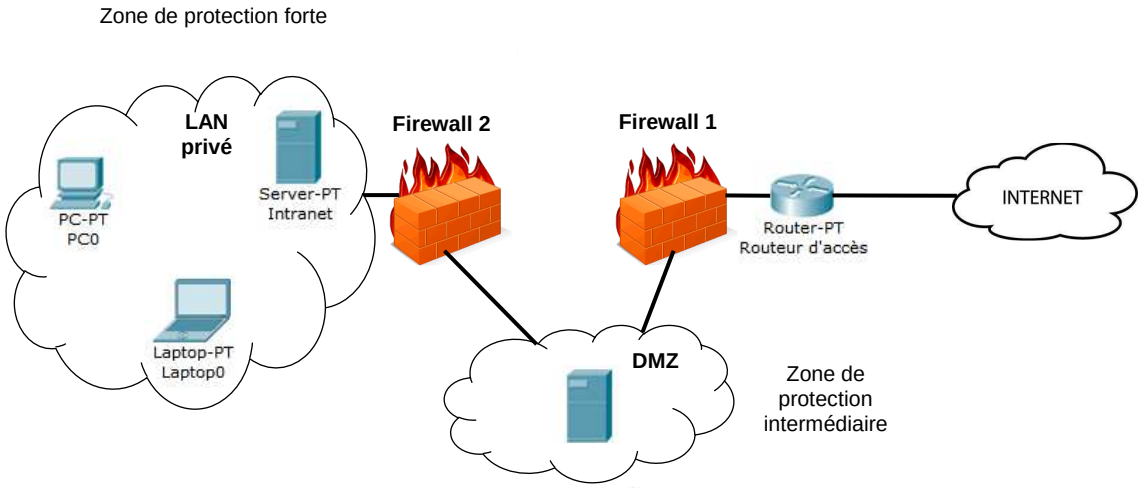
LES DMZ

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

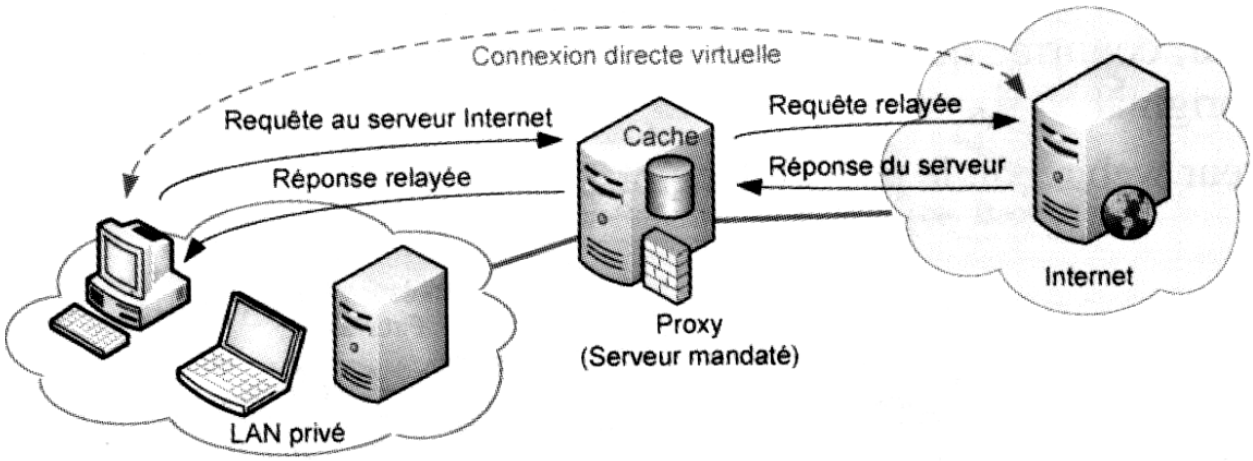
Un niveau supplémentaire de sécurité peut être introduit avec un deuxième firewall. Les règles d'accès sur le firewall du LAN privé sont plus restrictives. La DMZ est située entre deux firewalls (DMZ « en sandwich ») avec des règles moins restrictives introduites par le premier firewall.



DMZ en sandwich

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).

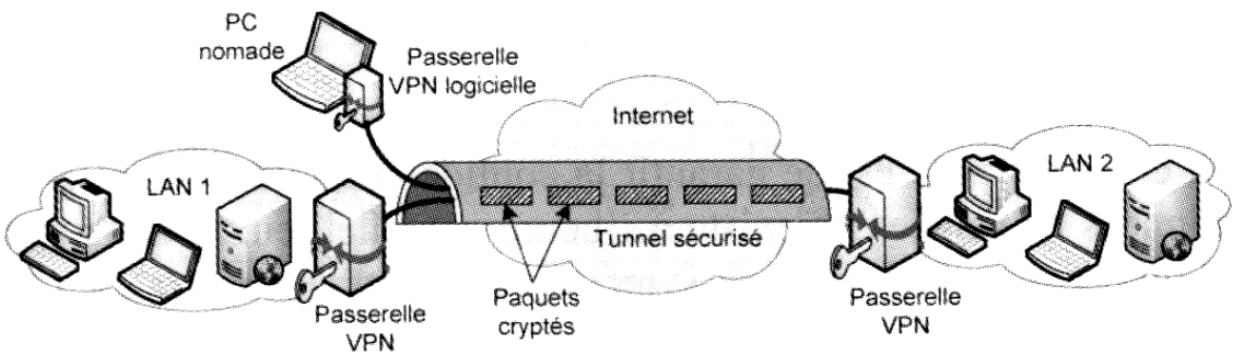


Serveur mandataire

LES VPNs

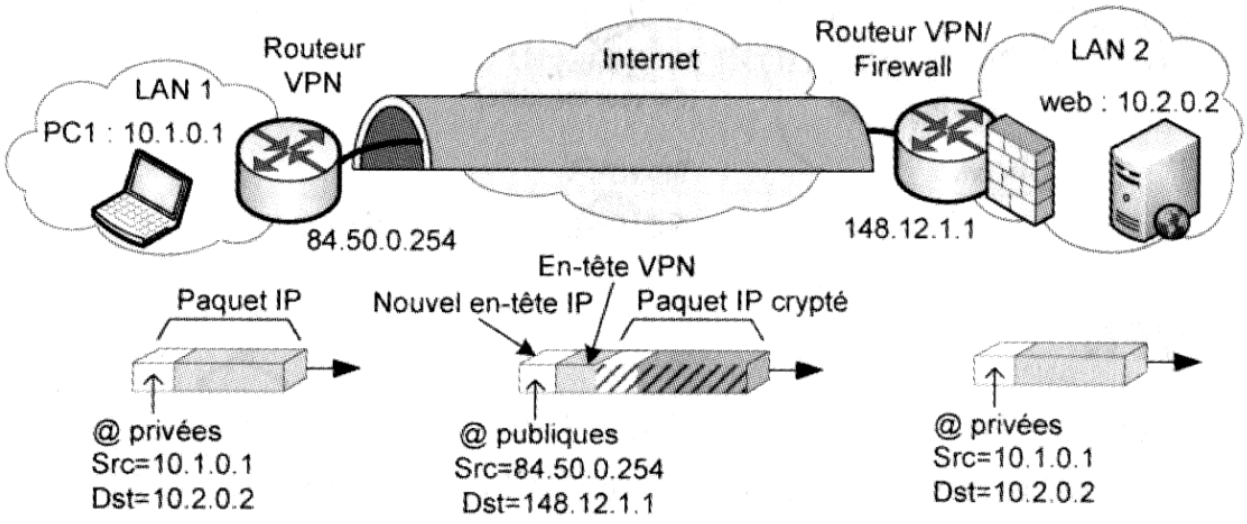
Le réseau privé virtuel (VPN, Virtual Private Network) est un élément essentiel dans les architectures modernes de sécurité. Un VPN est constitué d'un ensemble de LAN privés reliés à travers Internet par un « tunnel » sécurisé dans lequel les données sont cryptées. Les postes distants faisant partie 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 œuvre, 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 LANs 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. Nous étudierons ces protocoles dans un prochain cours concernant « les défenses logicielles ».

QCM ET EXERCICES D'APPLICATION

QCM

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	Action
A	Entrant	Externe	Interne	TCP	>1023	21		Autorisé
B	Sortant	Interne	Externe	TCP	21	>1023		Autorisé
C	Sortant	Interne	Externe	TCP	>1023	21		Autorisé
D	Entrant	Externe	Interne	TCP	21	>1023	Oui	Autorisé
E	Toutes	Toutes	Toutes	Tous	Tous	Tous		Refusé

Question 1 :

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

Réponse : oui

Question 2 :

Les transferts FTP vers un serveur interne sont autorisés seulement si la connexion est initiée de l'extérieur.

Réponse : non

Question 3 :

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

Réponse : non

Question 4 :

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

Réponse : oui

Question 5 :

Sur les routeurs Cisco, les ACL (Access Control Lists) 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.

Réponse : b

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.

Réponse(s) : a

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.

Réponse(s) : a et d

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.

Réponse(s) : a, b et d

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.

Réponses : a et d

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.

Réponse(s) : a, b et c

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

Réponses : b, c et e

EXERCICE

Question :

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

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

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