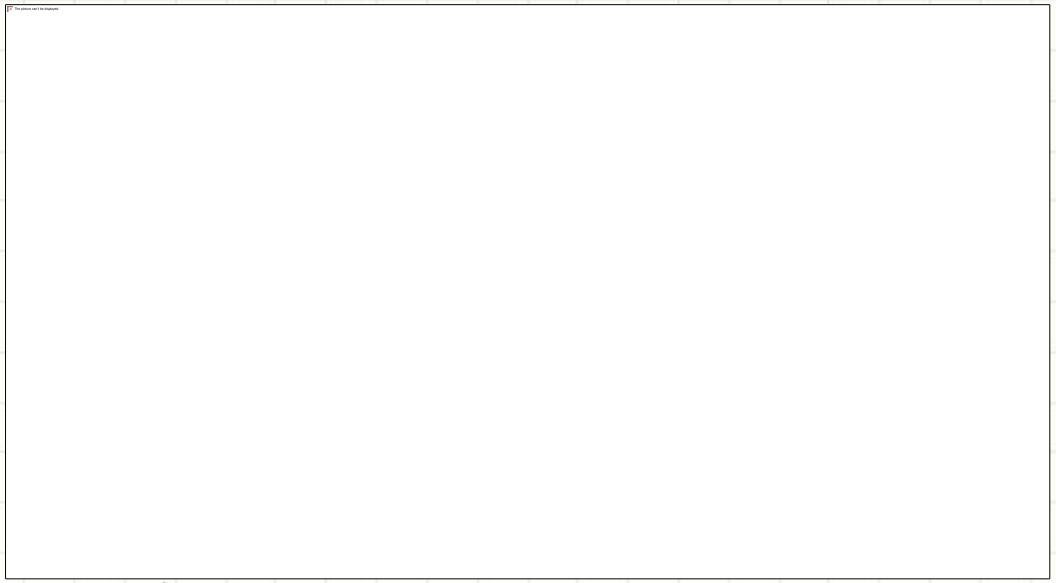
FIREWALL

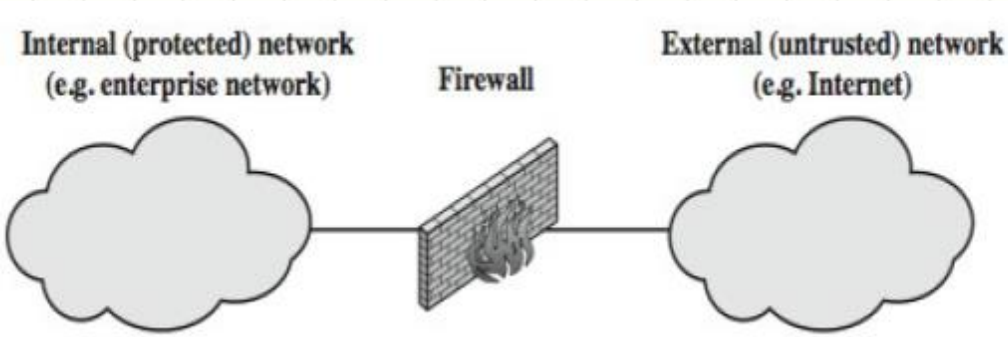


SAOUDI Lalia

2020-2021

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

- ➢ Un point de contrôle du trafic
  - Interconnecte des réseaux avec des niveaux de confiance différents
- Travaille au niveau IP ou au dessus
- En se référant à la définition de Cheswick et Bellovin, un pare-feu est un ensemble de composants placés entre deux réseaux ayant les propriétés suivantes :
  - tout le trafic transitant entre les deux réseaux passe nécessairement par le pare-feu ;
  - seul le trafic explicitement autorisé par la politique de sécurité appliquée localement est autorisé à passer au travers du pare-feu
  - le pare-feu est immunisé contre toute intrusion.



1) Un domaine à protéger : un réseau ‘interne’.

Un réseau d’entreprise/personnel que l’on veut protéger Vis à vis d’un réseau ‘externe’ d’ou des intrus sont susceptibles de conduire des attaques.

2) Un pare-feu

Installé en un point de passage obligatoire entre le réseau à protéger (interne) et un réseau non sécuritaire (externe).

C’est un ensemble de différents composants matériels et logiciels qui contrôlent le traffic intérieur/extérieur selon une politique de sécurité.

Pare-feu : le possible et l'impossible

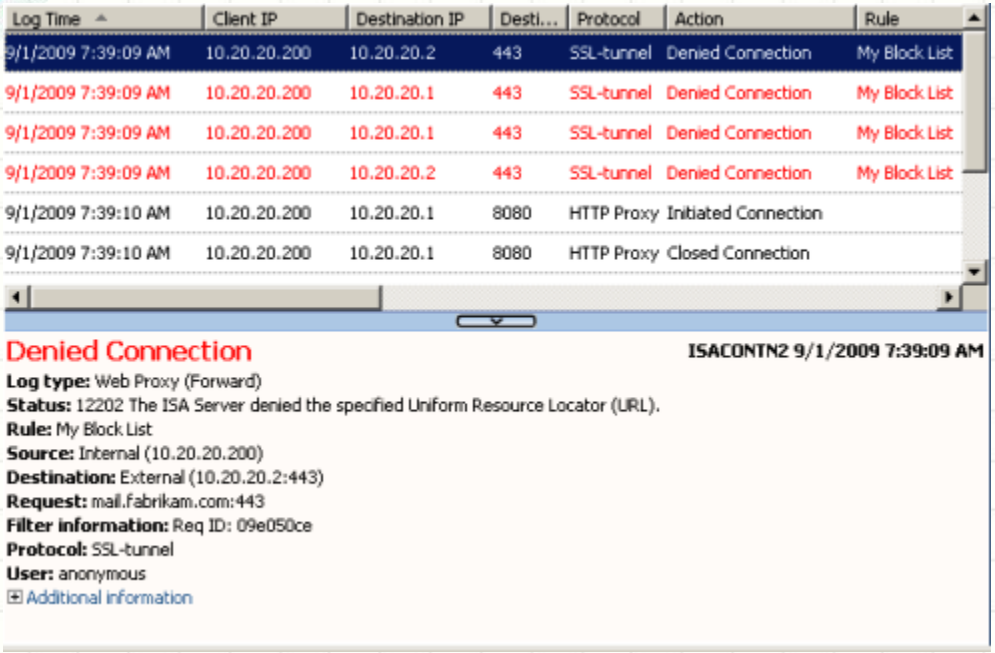
Ce que peut faire un pare-feu :

1) Etre un guichet de sécurité: un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs.
2) Appliquer une politique de contrôle d'accès.
3) Enregistrer le trafic: construire des journaux de sécurité.

Ce que ne peut pas faire un pare-feu :

1) Protéger contre les utilisateurs internes (selon leurs droits).
2) Protéger un réseau d'un trafic qui ne passe pas par le pare-feu (exemple de modems additionnels)
3) Protéger contre les virus.
4) Protéger contre des menaces imprévues (hors politique).

Pare-feu : le Log



Log Time	Client IP	Destination IP	Desti...	Protocol	Action	Rule
9/1/2009 7:39:09 AM	10.20.20.200	10.20.20.2	443	SSL-tunnel	Denied Connection	My Block List
9/1/2009 7:39:09 AM	10.20.20.200	10.20.20.1	443	SSL-tunnel	Denied Connection	My Block List
9/1/2009 7:39:09 AM	10.20.20.200	10.20.20.1	443	SSL-tunnel	Denied Connection	My Block List
9/1/2009 7:39:09 AM	10.20.20.200	10.20.20.2	443	SSL-tunnel	Denied Connection	My Block List
9/1/2009 7:39:10 AM	10.20.20.200	10.20.20.1	8080	HTTP Proxy	Initiated Connection	
9/1/2009 7:39:10 AM	10.20.20.200	10.20.20.1	8080	HTTP Proxy	Closed Connection	

Denied Connection

ISACONTN2 9/1/2009 7:39:09 AM

Log type: Web Proxy (Forward)
Status: 12202 The ISA Server denied the specified Uniform Resource Locator (URL).
Rule: My Block List
Source: Internal (10.20.20.200)
Destination: External (10.20.20.2:443)
Request: mail.fabrikam.com:443
Filter information: Req ID: 09e050ce
Protocol: SSL-tunnel
User: anonymous
Additional information

Politique de sécurité

-La **politique de sécurité définit l'ensemble des règles de filtrage** à implémenter sur le pare-feu.

- Cela consiste à spécifier l'ensemble des services et protocoles TCP/IP pouvant être accessibles par des utilisateurs internes ou externes au site
- 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.

Un langage de définition de la politique de sécurité

Il offre l'avantage de présenter clairement le rôle des règles de filtrage. En effet, les règles de filtrage ont la forme suivante : si <condition> alors <action>

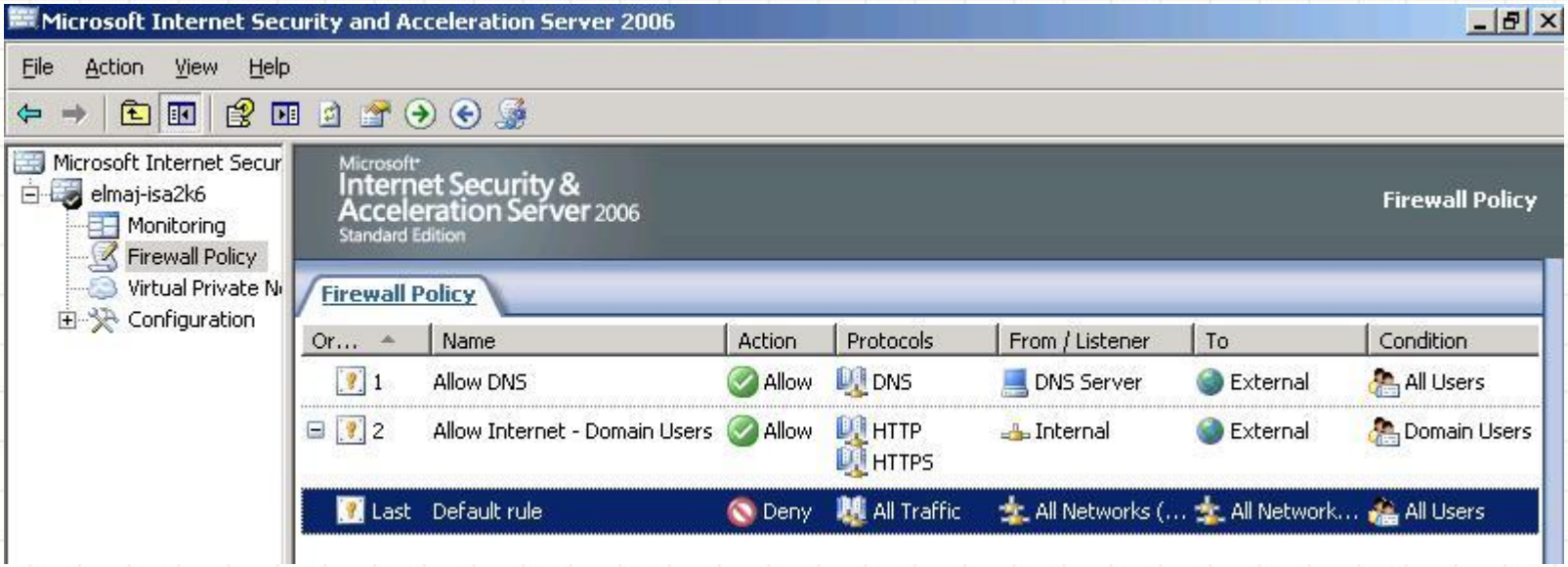
action entreprise pour un filtrage est classiquement : <action>=PERMIT, DENY.

Deux stratégies de configuration de pare-feu existent :

— tout ce qui n'est pas explicitement interdit est autorisé ;

— tout ce qui n'est pas explicitement permis est interdit.

Politique de sécurité : ISA server



Les différentes catégories de firewall

1. Firewall sans états (stateless)
2. Firewall à états (stateful)
3. Firewall applicatif

Les différentes catégories de firewall:

Firewall sans états (stateless)

- Ce sont les firewalls les plus anciens mais surtout les plus basiques qui existent
- Ils font un contrôle de chaque paquets indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control Lists).
- La plupart des routeurs incluent un filtrage de paquet statique

- Ces firewalls interviennent sur les couches réseau et transport.
- Les règles de filtrages s'appliquent par rapport à une adresses IP sources ou destination, mais aussi par rapport à un port source ou destination.

Filtrage de paquets statique : Les ACL

- Les «Access Control List» sont des listes définissant les règles
- Exemple d'ACL
  - Autoriser uniquement le trafic HTTP sortant

N°	Action	IP destination	Port dest.	IP source	Port src	Commentaires
1	Autorise	172.16.0.0/16	>1023	Toutes	80	WEB vers réseau interne
2	Autorise	Toutes	80	172.16.0.0/16	>1023	Réseau interne vers WEB
3	Bloque	Toutes	Tous	Toutes	Tous	Défaut

«Tout ce qui n'est pas explicitement autorisé est interdit»

Attaques sur les pare-feu niveau paquet

Spoofing adresse IP

- ➢ Adresse source du paquet est une adresse interne
- ➢ Le pare-feu laisse passer
- ➢ Pas de chance, le paquet était un “exploit”

➢ Fragmentation paquet

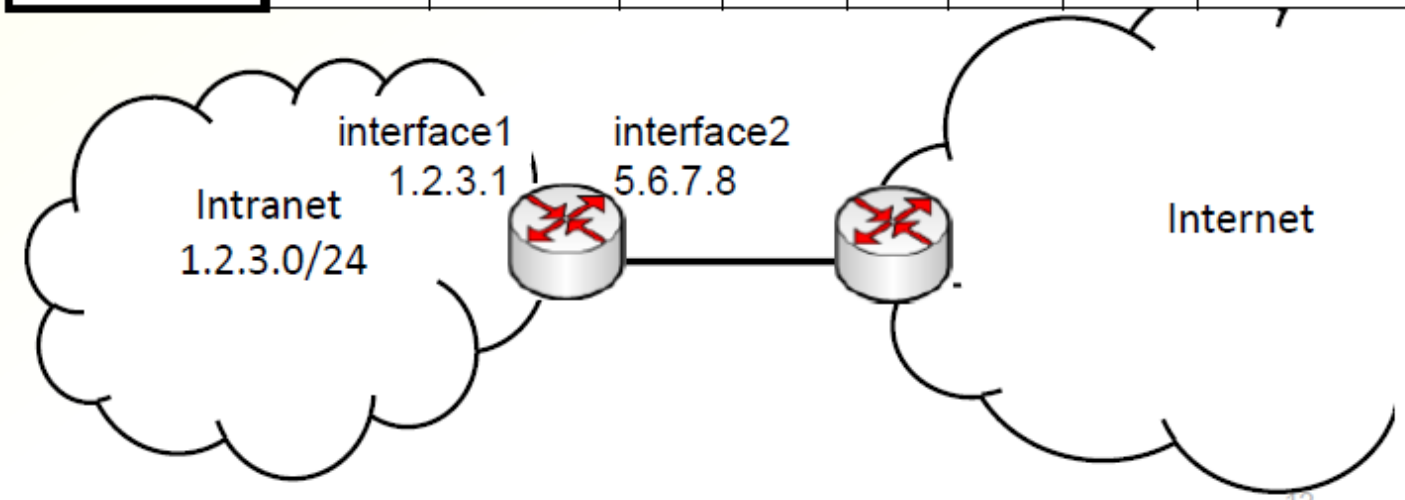
- ➢ Découpage paquet en plein de petits segments
- ➢ L'en-tête TCP n'est plus localisable car ne tient plus dans un paquet
- ➢ Suivant la politique du pare-feu, peut accepter paquet...

- Seul le premier fragment contient les informations TCP/UDP
  - Les fragments suivants ne contiennent pas d’informations sur les ports

Anti-spoofing filter example

- Filter based on input interface (part of the policy shown only):

Input interface	Protocol	Src IP	Port	Dst IP	Port	Flags	Action	Comment
2	*	1.2.3.0/24	*	*	*		Block	Ingress filter
2	*	5.6.7.8	*	*	*		Block	Router address
1	*	1.2.3.1	*	*	*		Block	Router address
1	*	1.2.3.0/24	*	*	*		Allow	Egress filter
1	*	*	*	*	*		Block	Default rule (If1)
...							...	



Les limites

Une limite de ce type de firewall se trouve au niveau des protocoles fonctionnant de manière similaire au FTP.

certains protocoles ont besoin d'ouvrir un autre port que celui dédié . Ce port est choisi aléatoirement avec une valeur supérieure à 1024. Dans le cas du protocole FTP, l'utilisation de deux ports permet d'avoir un flux de contrôle et un flux de données pour les connexions.

Le problème posé viens du fait que ce port est choisi aléatoirement, il n'est donc pas possible de créer des règles pour permettre les connexions FTP avec les firewalls sans états.

Filtrage de paquets dynamique (Stateful)

- Le filtrage dynamique fonctionne comme le filtrage statique au niveau de la couche 3 et 4, mais la différence du filtrage **statique est qu'il implémente des tables d'état pour chaque** connexion établie (State table)

Ce genre de filtre bloque ou autorise les paquets en fonction:

  - De leur contenu actuel
  - Du contenu des paquets précédents

- ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :
  - NEW : Un client envoie sa première requête.
  - ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW.
  - RELATED : Peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
  - INVALID : Correspond à un paquet qui n'est pas valide.
- Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall.

Exemple

- Pour la consultation de l'internet, on n'aura plus, sur un pare-feu dynamique, qu'à spécifier :
- **autoriser <toute source interne:1024-65535> vers <toute source externe>**
- L'effet de cette règle sera dans un premier temps de n'autoriser que des paquets d'initiation de connexion SYN, et ce uniquement s'ils se propagent dans le bon sens. D'autre part, si un paquet SYN autorisé est observé en provenance d'une source interne d'adresse intIP de port intPort vers une destination externe d'adresse extIP, alors le pare-feu va temporairement accepter les paquets compatibles de ces caractéristiques. Un paquet destiné à une autre adresse que intIP ou un autre port que intPort sera rejeté.

Avantages

- protection contre certaines attaques DoS comme par exemple le Syn Flood.
- l'acceptation d'établissement de connexions à la demande. C'est à dire qu'il n'est plus nécessaire d'ouvrir l'ensemble des ports supérieurs à 1024.

Limites

- il existe un coût supplémentaire lors de la modification des règles du firewall. Il faut que les firewalls réinitialisent leurs tables à état.
- ce type de firewall ne protège pas contre l'exploitation des failles applicatives, qui représentent la part la plus importante des risques en terme de sécurité.

Passerelles applicatives

- **Passerelles applicatives:**

  Un pare-feu applicatif considère les connexions à la fois au niveau de la couche transport et au niveau applicatif.

  Une passerelle applicative (*application gateway) est un serveur* permettant d'effectuer un contrôle d'accès plus ou moins fin sur les données échangées entre deux réseaux pour un service TCP/IP particulier.
  Plus précisément, dans le modèle client-serveur, une passerelle est un serveur placé entre le client qui demande un service particulier et le serveur rendant ce service

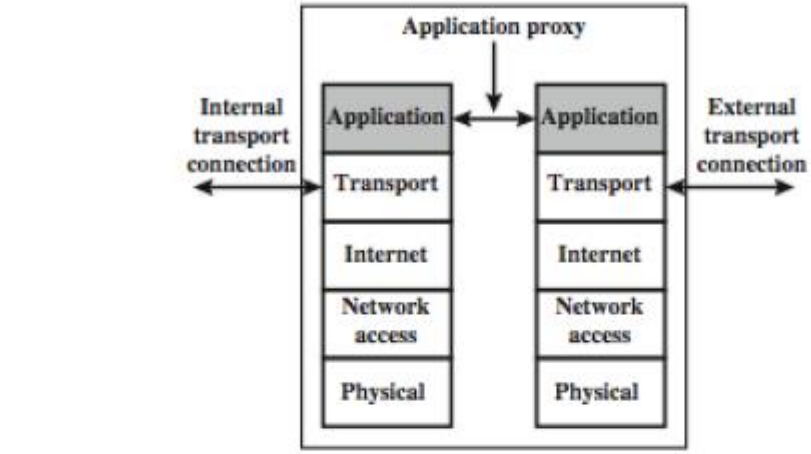
Exemple

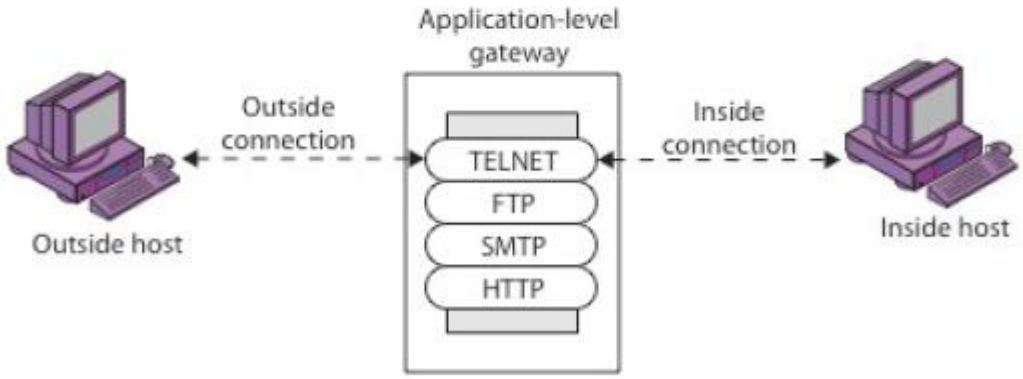
- Le protocole HTTP permet d'accéder en lecture sur un serveur par une commande GET, et en écriture par une commande PUT. Un pare-feu applicatif va être en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

Passerelles applicatives

- **les passerelles de niveau applicatif** , encore appelées proxy ou reverse proxy, permettent de faire un filtrage fin en fonction du service demandé, classiquement : telnet, FTP, SMTP ou HTTP (HyperText Transfer Protocol) ;

PASSERELLE APPLICATIVE





(b) Application-level gateway

Limites

- Complexité/charge pare-feu augmente en fonction du nombre de services en mode proxy et du nombre d'utilisateur: Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7.
- En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles .

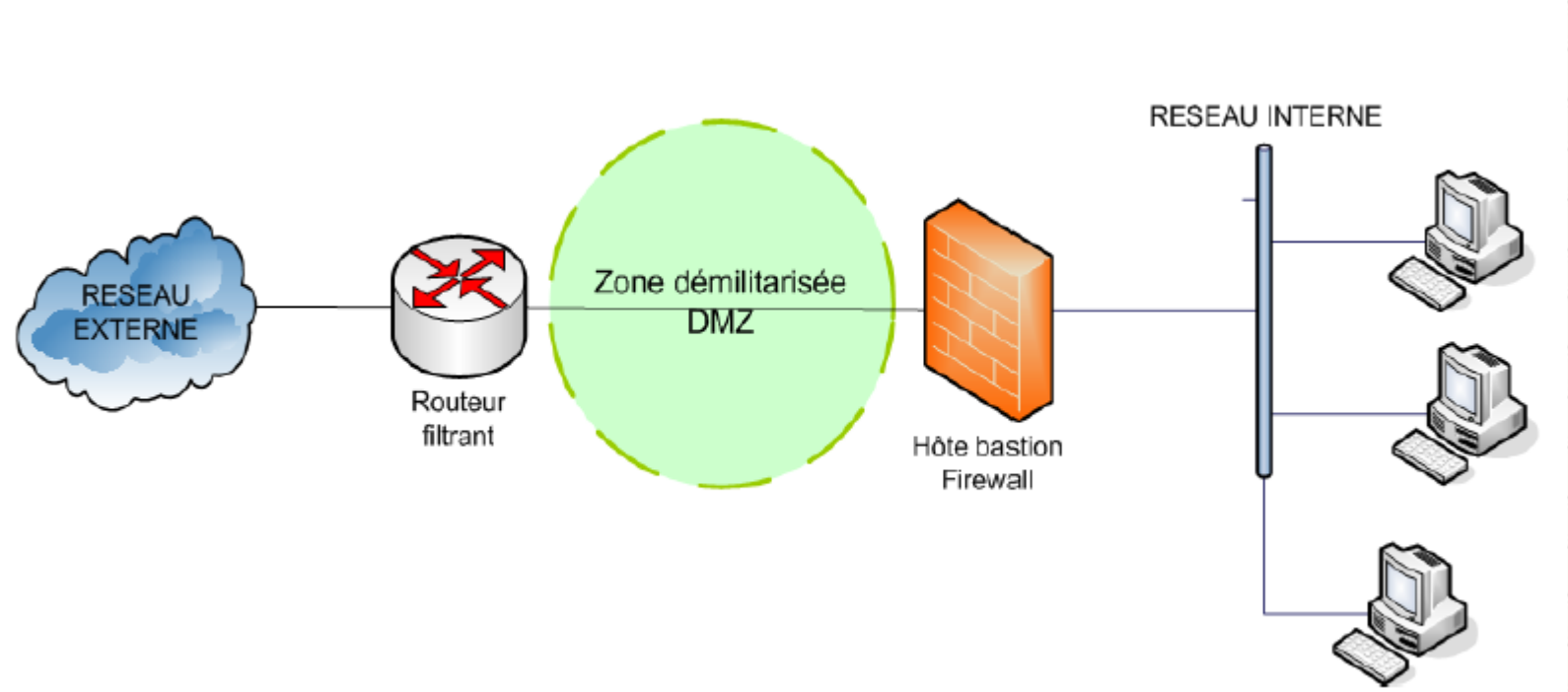
pare-feu personnel

- Pb: utilisateur nomade
- Un pare-feu personnel est un logiciel de sécurité pour les terminaux, qu'ils soient fixes ou mobiles, les terminaux fixes visés ayant un accès Internet, en particulier ADSL (Asymmetric Digital Subscriber Line) ou câble. Un pare-feu personnel est généralement composé d'un système de détection d'intrusion, associé à un parefeu et une protection applicative.

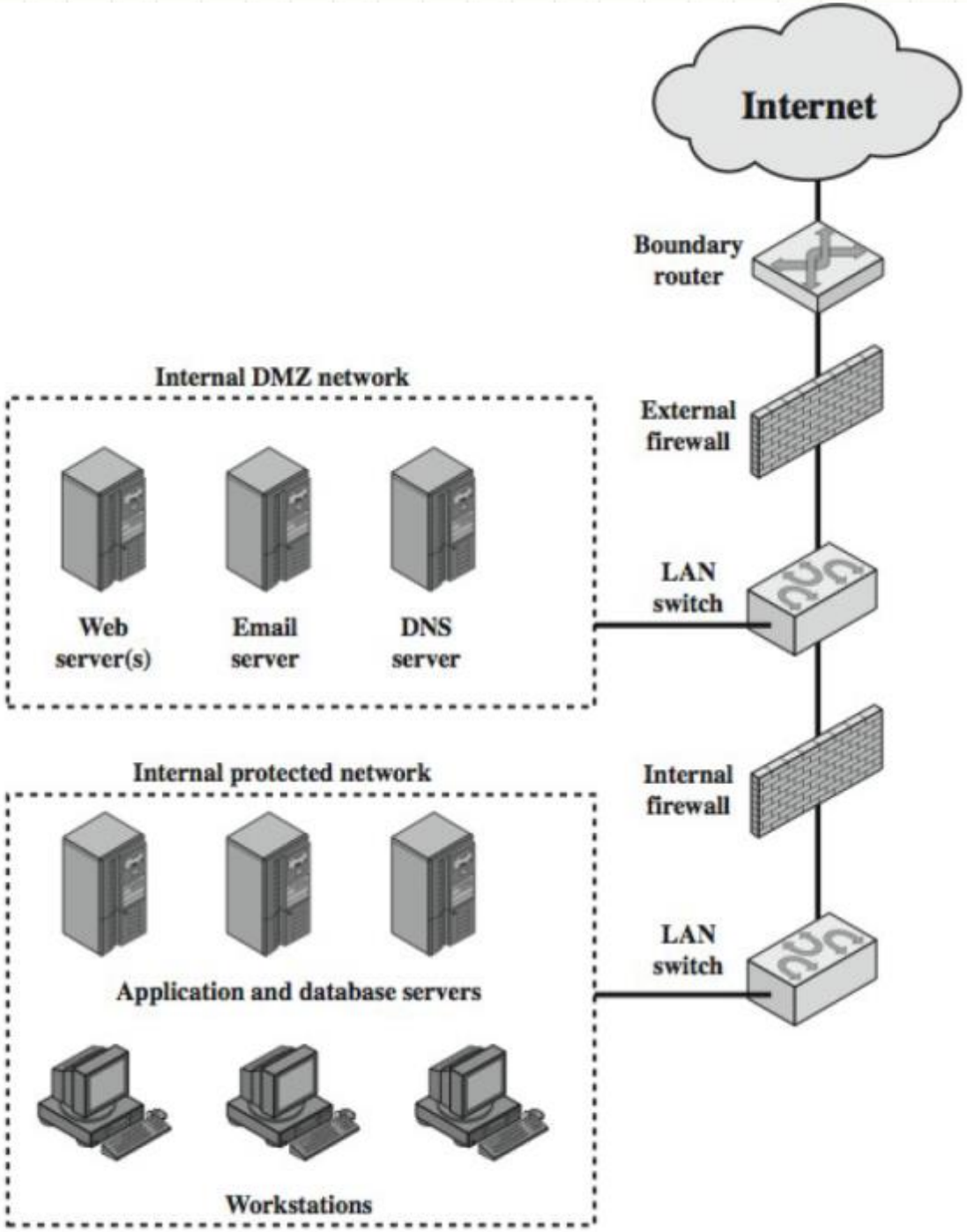
Architectures réseaux et firewalls

- **Les besoins des entreprises sont :**
  - **Le réseau interne doit avoir accès aux services externes: Internet, réseau d'une autre entreprise,**
  - **Le réseau public doit avoir accès à certains services internes: Serveur mail, serveur web de la société, extranet**
- **L'architecture la plus appropriée est l'architecture DMZ(**de l'anglais *demilitarized zone*)
- **Cette approche combine un filtrage statique des paquets et un filtrage dynamique**
  - **Le filtrage statique est assuré par un routeur**
  - **Le filtrage dynamique par un firewall**

Firewall et DMZ

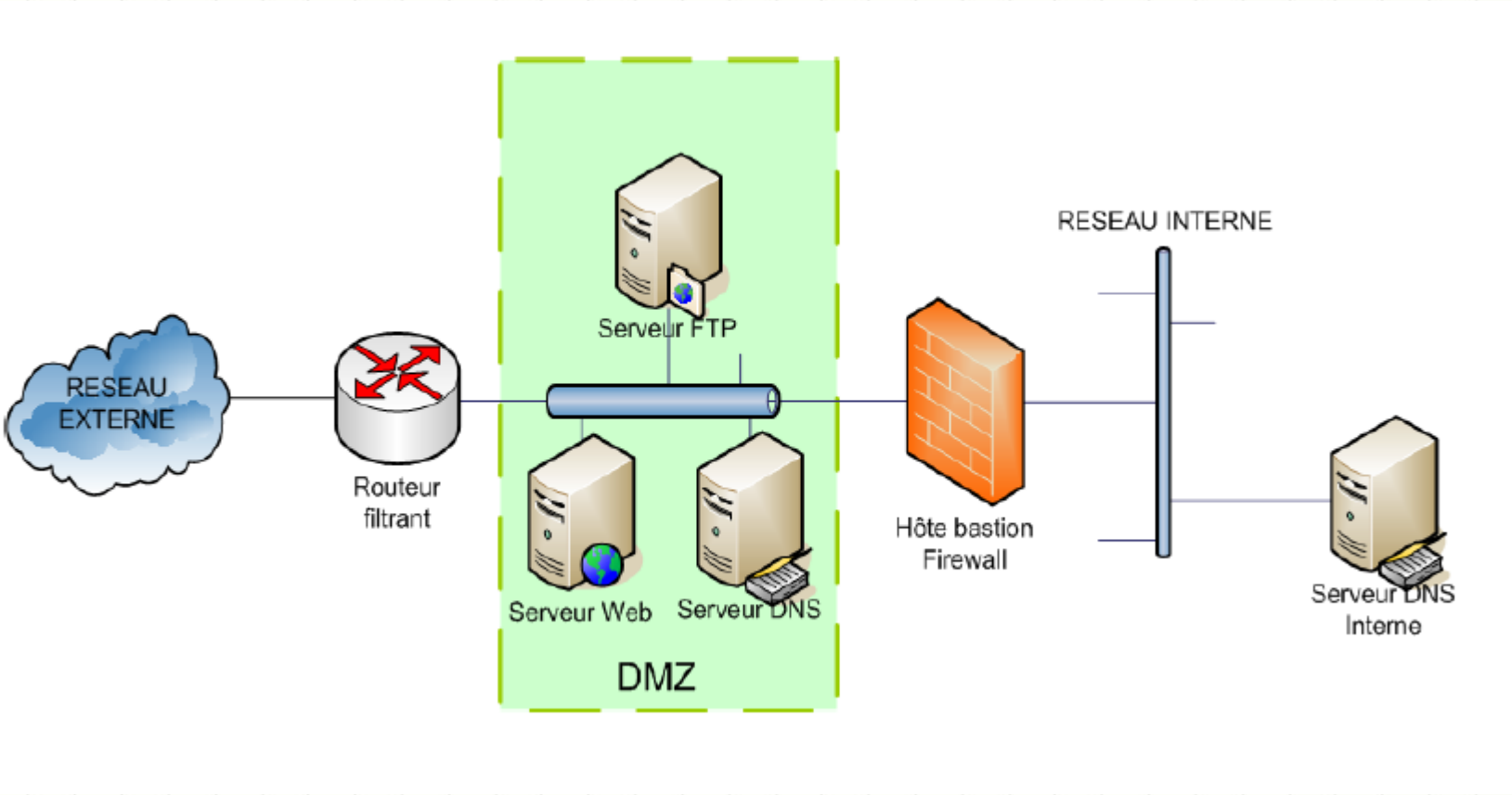


DMZ (De-Militerized Zone)



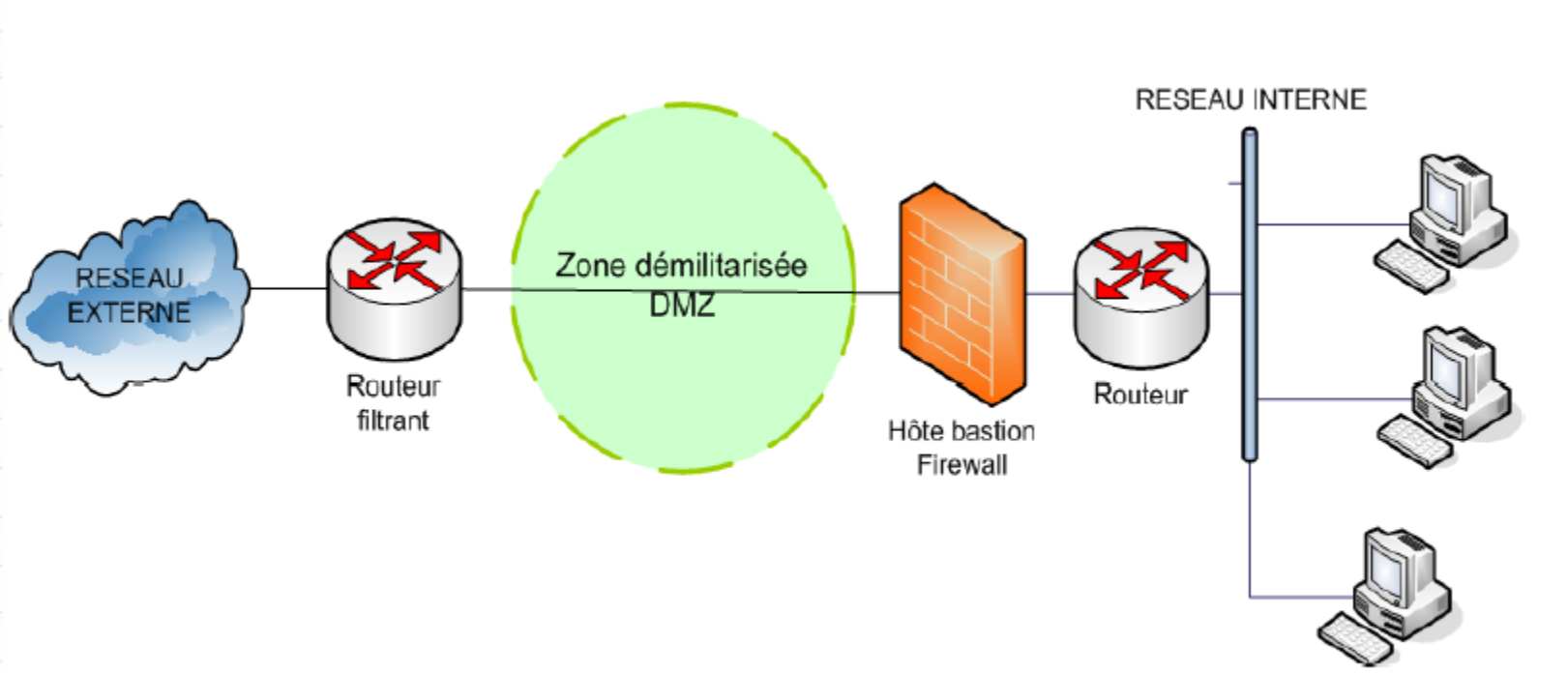
- Il existe 4 topologies principales de firewall associé à une DMZ
  - Topologie classique
  - Topologie «Belt and Brace»
  - Topologie «Belt and Brace» avec un sous-réseau séparé
  - Architecture Chapman

Topologie classique



- Avantages
- L’accès aux services externes n’a pas d’impact sur le réseau interne
- Le serveur DNS de la DMZ donne un minimum d’informations
- Le serveur DNS interne est isolé des attaques externes
- Les filtres du routeur filtrant doivent restreindre les accès externes à la DMZ
- Autoriser FTP de l’externe vers l’adresse IP du serveur FTP uniquement

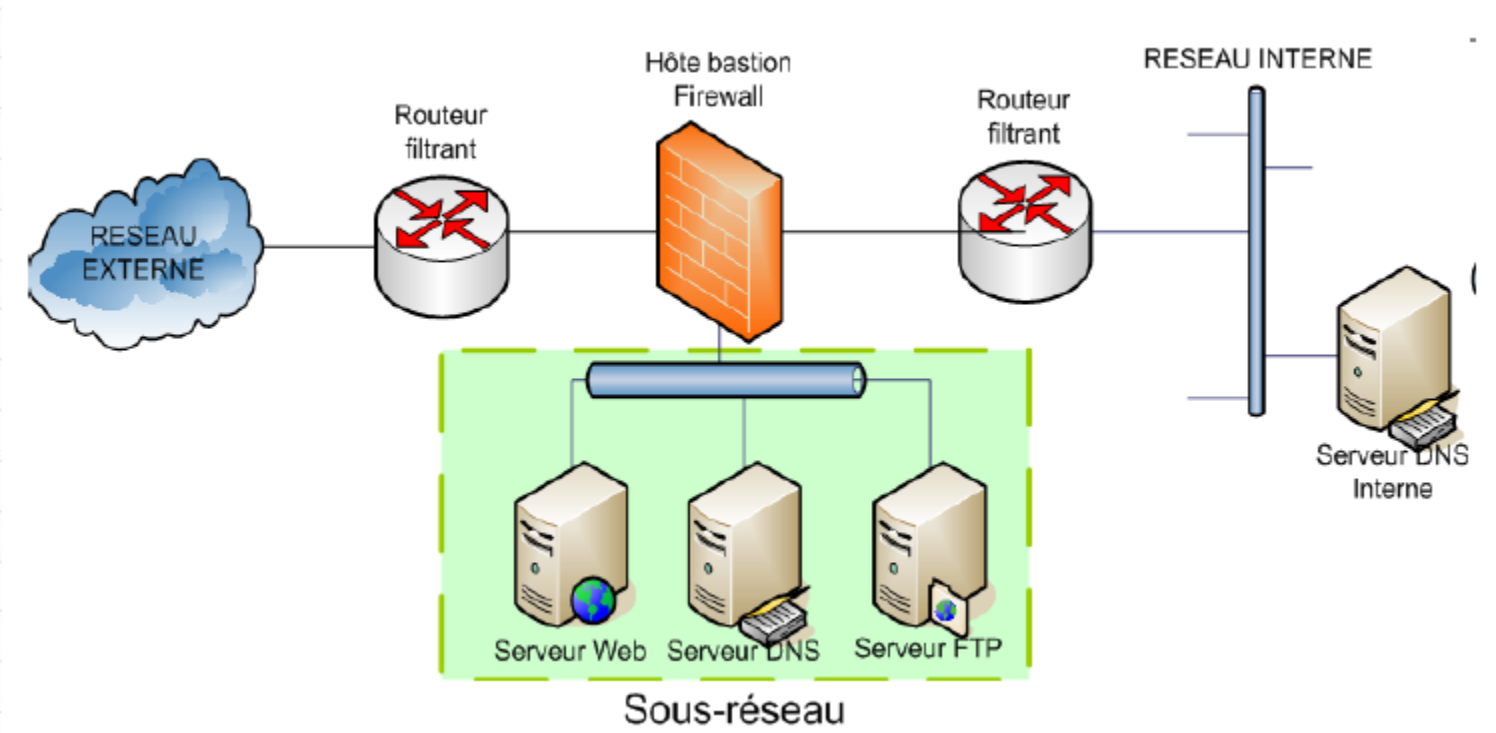
Topologie «Belt and Brace»



Avantages

- Dans la topologie classique, si le firewall est compromis, il peut servir à attaquer le réseau interne
- En ajoutant un 2ème routeur filtrant, on protège le réseau interne
- Trois niveaux de défense

Topologie à sous réseau

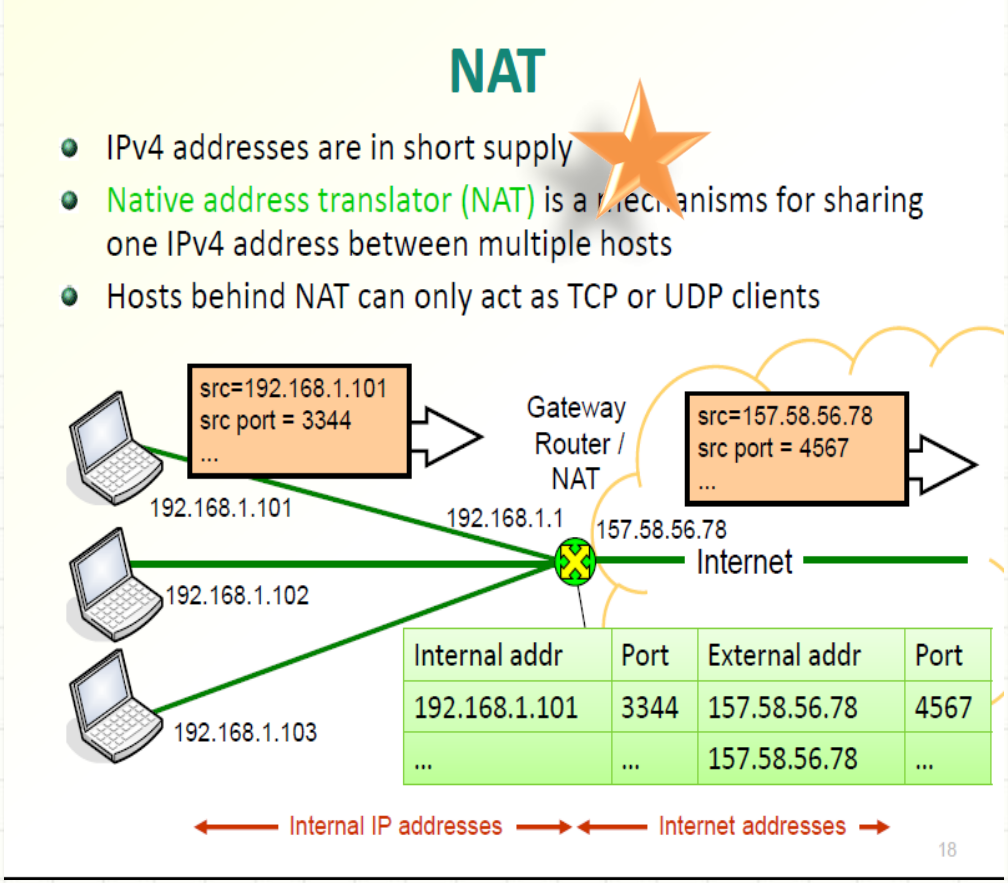


Les serveurs publics sont placés dans un sous-réseau séparé et protégés par un firewall

Firewall NatNAT :Native Adresse Translator

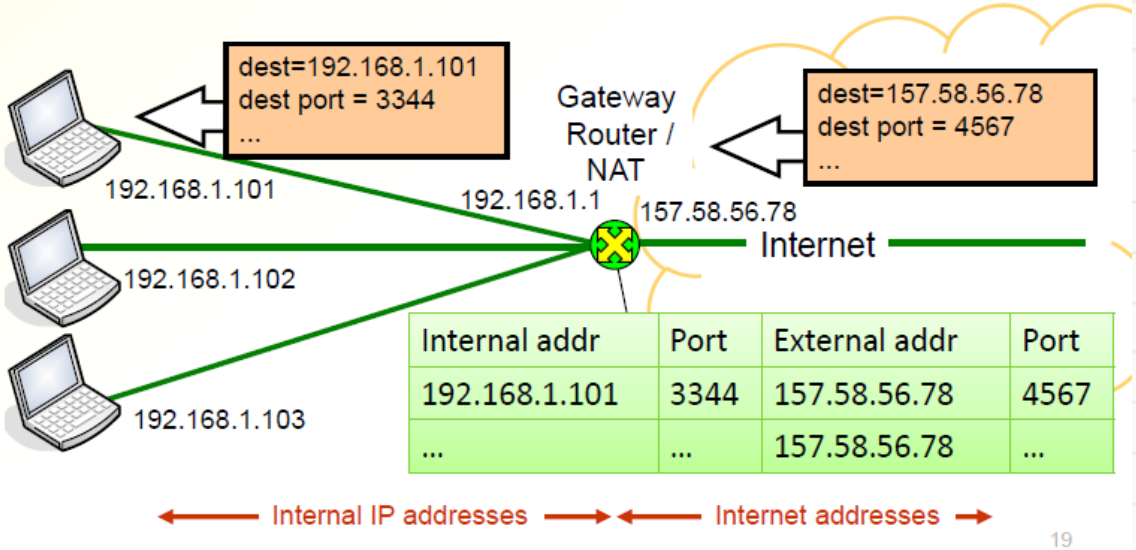
- **Firewall Nat traduit l'adresse** <private IP addr, port> interne à une adresse <public IP addr, port> externe et vice versa.

NAT


NAT
IPv4 addresses are in short supply
Native address translator (NAT) is a mechanisms for sharing one IPv4 address between multiple hosts
Hosts behind NAT can only act as TCP or UDP clients
src=192.168.1.101
src port = 3344
...
Gateway
Router /
NAT
src=157.58.56.78
src port = 4567
...
192.168.1.101
192.168.1.1
157.58.56.78
Internet
192.168.1.102
192.168.1.103
Internal addr
Port
External addr
Port
192.168.1.101
3344
157.58.56.78
4567
...
...
157.58.56.78
...
Internal IP addresses
Internet addresses
18

NAT

- IPv4 addresses are in short supply
- Native address translator (NAT) is a mechanisms for sharing one IPv4 address between multiple hosts
- Hosts behind NAT can only act as TCP or UDP clients



Les différents types de pare-feux.
Les pare-feux bridge

- Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus.
- Leurs interfaces ne possèdent pas d'adresse Ip, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies.
  - cela signifie que le pare-feu est indétectable pour un hacker lambda. En effet, quand une requête ARP estémise sur le câble réseau, le pare-feu ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau,
  - Ces pare-feux se trouvent typiquement sur les Switch.
- **Avantages**
- - Impossible de l'éviter (les paquets passeront par ses interfaces)- Peu coûteux
- **Inconvénients**
- - Possibilité de le contourner (il suffit de passer outre ses règles)- Configuration souvent contraignante- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

Les pare-feux matériels

- Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel.
- **Avantage:**
- leur interaction avec les autres fonctionnalités du routeur est simplifiée
- ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur.
- Son administration est souvent plus aisée que les pare-feu bridges
- Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout pare-feu.
- **Inconvénients:**
- seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un pare-feu d'une autre marque,son utilisation est impossible

Les pare-feux Logiciels

- Présents à la fois dans les serveurs et les routeurs.
- Exemples:
- Iptable (linux)
- IPFire
- Isa server (windows)

- Questions de cours 8
- Q1: Quelles sont les trois caractéristiques clé d’un firewall?
- Q2: Qu'est ce qu’un DMZ
- Q3: Citer les cas non traités par un pare-feu .
- Q4: Qu'est qu’une politique de sécurité d’un parefeu
- Q5: Quelle est la meilleure politique de sécurité et pourquoi
- Q6: Citer les différentes catégories de firewall.