



# Les mécanismes de filtrage et de NAT

Licence Pro SEICOM – Module 37





# SOMMAIRE

- Les firewalls
  - Filtrage de paquets simple
  - Relai d'applications
    - Proxies applicatifs
    - Reverse-proxies
  - Filtrage statefull inspection
  - Conclusion
- NAT (Network Address Translation)
  - Introduction par l'exemple
  - Implémentation
  - NAT statique
  - NAT dynamique
  - Récapitulatif
- Exercices



# LES FIREWALLS



# Les firewalls

- **Un firewall occupe une place importante dans la sécurité des réseaux :**
  - Portail entre un réseau sécurisé et non-sécurisé
  - Minimum de deux interfaces logiques
  - Système logicielle (parfois sur plateforme matérielle propriétaire)
  - Mise en œuvre de restrictions d'entrées/sorties
  - Permettre de se connecter à Internet
  - Permettre l'ouverture de son réseau à ses partenaires ainsi qu'à ses employés itinérants
  - Suivre l'activité du réseau (logs)
- **3 règles de base :**
  - ACCEPT : autoriser une connexion
  - REJECT : rejeter une connexion
  - DROP : bloquer une connexion de façon silencieuse
- **Un firewall doit :**
  - Etre lui-même sécurisé
  - Etre performant en fonction du trafic

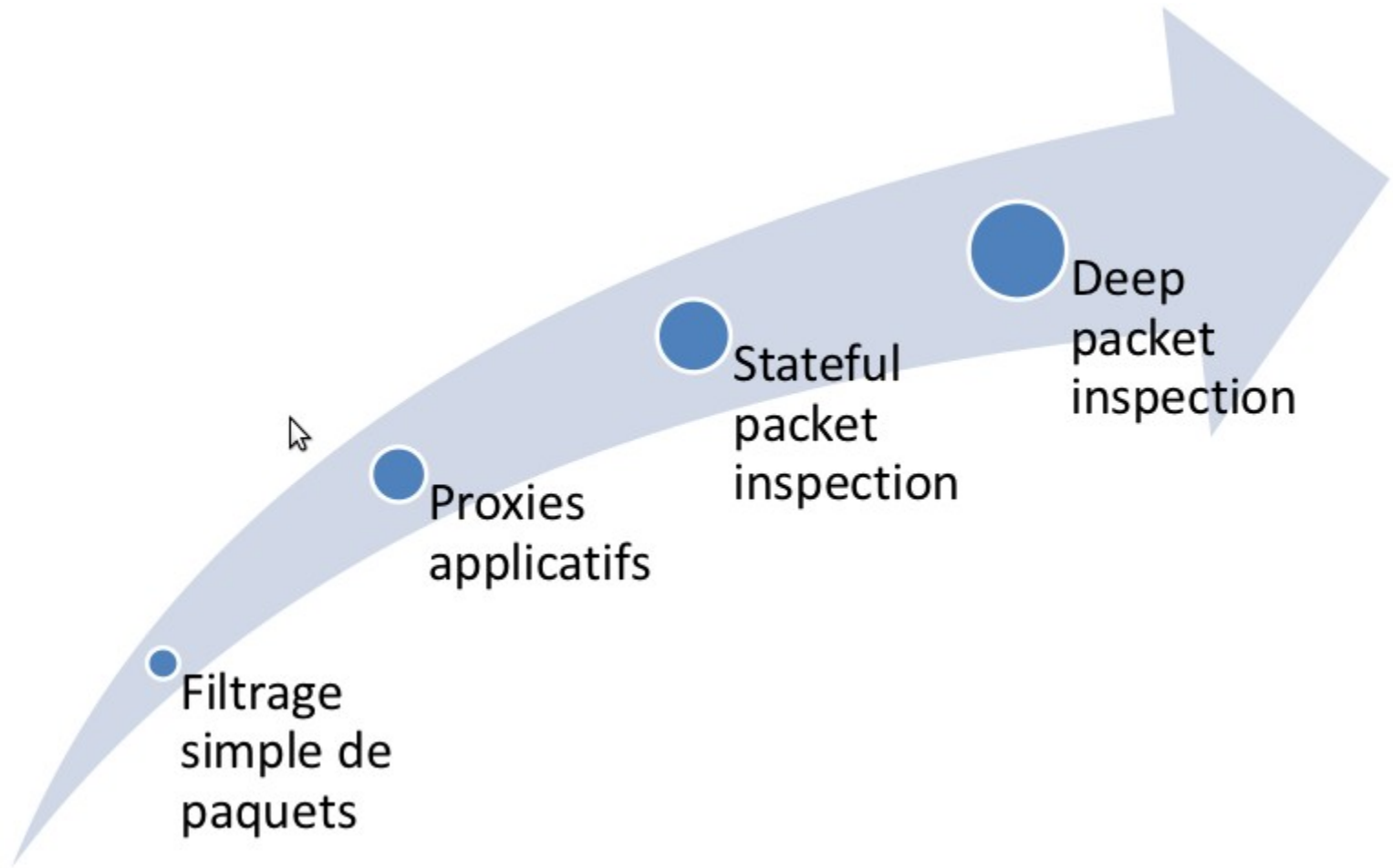


## Un firewall : pour quelle politique ?

- Deux politiques de base possibles :
  - Tout ce qui n'est pas interdit est autorisé
  - Tout ce qui n'est pas autorisé est interdit
- Pour se protéger :
  - Des connexions indésirables et de l'inconnu
  - Des attaques sur les points faibles des OS
  - Des attaques DoS sur les réseaux internes
- Mais qui ne protège pas :
  - De ce qui ne passe pas par lui (attaques internes, AP pirates...)
  - Des virus
  - Des attaques sur ses propres faiblesses
  - D'une mauvaise administration



# Evolutions des technologies de firewalls





# Filtrage simple de paquets

Première génération de firewall, le filtrage simple de paquets examinent les paquets au niveau de la couche réseau et sont indépendants des applications, ce qui offre de bonnes performances et évolutivités.

## Fonction

- **Implémentés sur les routeurs**
- **Filtrage basé sur :**
  - **L'adresse IP source ou destination**
  - **Le port source ou destination**
  - **Le flag acknowledge**
- **La décision de rejet se prend uniquement sur la base du paquet examiné (pas de notions de sessions)**
- **Incompatible avec des applications aux ports dynamiques (VoIP) ou UDP**

## Avantages

Pas cher et performant

## Inconvénients

Faible niveau de sécurité, sensibles aux attaques (flooding, sniffing), difficile à administrer



## Filtrage simple de paquets

- Filtrage de la messagerie

- Politique : toute machine interne peut envoyer des emails vers l'extérieur

Source	Destination	Port source	Port destination	Action	Commentaire
ANY	ANY	*	tcp/25	Accept	SMTP sortant

- Problème : le sens du paquet n'est pas renseigné
- Solution : n'autoriser que le trafic sortant et en entrée, les réponses qui en découlent (flag ack)

Source	Destination	Port source	Port destination	Action	Flag	Commentaire
MON RESEAU	ANY	*	tcp/25	Accept		SMTP entrant
ANY	ANY	tcp/25	*	Accept	Ack	Réponses





# Les proxies applicatifs

Seconde génération de firewall, les proxies applicatifs fonctionnent sur serveurs réseaux dédiés.

## Fonction

- **Améliore la sécurité en examinant toutes les couches applicatives**
- **Fonctionne sur des serveurs qui requièrent un système d'exploitation**
- **Logiciel s'intercalant entre les clients et des serveurs tiers**
- **Rôles :**
  - **Assurer une authentification pour un service**
  - **Relayer les dialogues entre les clients et les serveurs en centralisant les accès**
  - **Journaliser les actions**
  - **Modifier les informations qui transitent**
  - **Doit comprendre le protocole sous-jacent mais reste**
  - **Moins complexe que le protocole qu'elle sert**
  - **Peut déceler un protocole non-conforme**

## Avantages

Plus sécurisé que le filtrage simple de paquets

## Inconvénients

- Casse le modèle client / serveur
- Analyse les paquets uniquement au niveau de la couche application (L7)
- Nécessite de nombreuses tâches administratives
- Lent et complexe (Charge CPU)
- Incompatibles avec de nouveaux protocoles

# Les proxies applicatifs

- Les protocoles communément relayés : DNS, SMTP, HTTP, FTP, Telnet
- Exemple :
  - Une machine du réseau privé veut se connecter sur internet sur un serveur web
  - La machine du réseau privé initie une connexion TCP sur le proxy en se connectant sur un port destiné au service concerné
  - Le proxy établit alors une connexion TCP sur le serveur web en modifiant dans le paquet l'adresse IP source pour y mettre son adresse publique et le port de destination par le port du service concerné
  - Le serveur proxy sait trouver le port de destination en regardant sur quel port s'est effectuée la connexion TCP avec la machine du réseau privé.
  - Le serveur proxy transmet la réponse à la machine

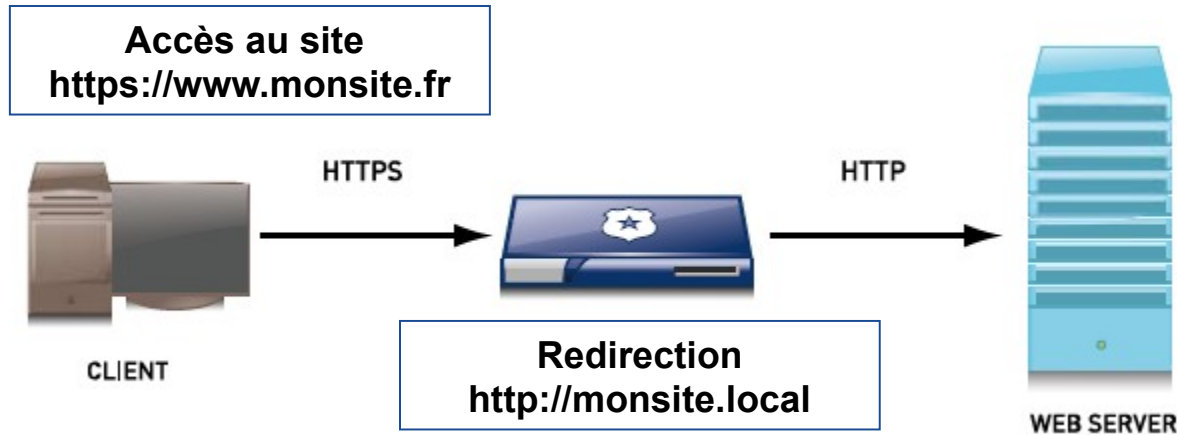




## Les reverse-proxies

- Principalement utilisés pour les serveurs web : toutes les connexions depuis internet vers les serveurs web sont routées vers le serveur proxy :
  - Traite la demande lui-même (authentification cache...)
  - Transmet la requête complète ou partielle aux serveurs web
- Présente une seule interface à l'émetteur
- Distribue le trafic entrant à différents serveurs avec la possibilité de faire du load-balancing

# Les reverse-proxies



## • Pourquoi installer un reverse-proxy ?

- Cryptage / Accélération SSL : les serveurs web n'ont pas besoin d'assurer eux-mêmes le cryptage, un reverse proxy peut le faire avec du matériel d'accélération SSL
- Partage de charge : le trafic peut être distribué sur différents serveurs
- Possibilité de réécriture d'url (les adresses internes ne sont pas visibles)
- Cache du contenu statique (html, images) pour réduire la charge des serveurs web
- Compression : optimisation et compression des flux



# Stateful Packet Inspection

Troisième génération de firewall, les firewalls Stateful Inspection surmontent les faiblesses des solutions de filtrage simple de paquets et de proxies en fournissant une solution analysant l'ensemble des couches du modèle OSI sans casser le modèle client / serveur.

## Fonction

- **Technologie inventée par Checkpoint**
- **Intercepte les packets au niveau de la couche réseau**
- **Extrait l'information sur l'état d'une session pour pouvoir statuer sur la décision (ACCEPT/REJECT/DENY) au niveau de toutes les couches OSI**
- **Maintient cette information dans une table dynamique des état pour évaluer les connexions qui suivent**
- **Offre une solution qui offre : sécurité, performance, évolutivité**

## Avantages

Très sécurisé  
Plus rapide que les proxies  
Standard  
Pas de modification des applications  
Transparent pour les utilisateurs  
Compatible avec des applications aux ports dynamiques (VoIP) ou UDP

## Inconvénients



# Stateful Packet Inspection

- Exemple de politique de filtrage (Checkpoint NGX)

DMZ_to_INTERNET (Rules 64-68)							
64	DMZ - WAN	DMZ_H_SRV-SU	* Any	TCP smtp TCP pop-3 ICMP echo-request ICMP echo-reply	accept	- None	SRV-FIREWALL
65	DMZ - WAN	DMZ_N_SUPERV	* Any	DMZ_to_WAN PPTP TCP Remote_Desktop	accept	Log	SRV-FIREWALL
66	DMZ - WAN	G_DMZ_FORMAT	<del>G_PENTASONIC</del> <del>G_DMZ</del> <del>G_VPN_CLIENTS</del>	DMZ_to_WAN	accept	Log	SRV-FIREWALL
67	DMZ - WAN	DMZ_N_EXTERN	<del>G_PENTASONIC</del> <del>G_VPN_CLIENTS</del> <del>G_DMZ</del>	DMZ_to_WAN	accept	Log	SRV-FIREWALL
68	DMZ - WAN	DMZ_N_MOCS	<del>G_PENTASONIC</del> <del>G_VPN_CLIENTS</del> <del>G_DMZ</del>	DMZ_to_WAN	accept	Log	SRV-FIREWALL
INTERNAL_NETWORKS (Rules 69-72)							
69	PROTECTION SMTP	* Any	* Any	TCP smtp	drop	Log	SRV-FIREWALL
70	LAN - DMZ	G_LAN	G_DMZ	LAN_to_DMZ	accept	- None	SRV-FIREWALL
71	LAN - WAN	G_LAN	<del>G_DMZ</del> <del>G_VPN_CLIENTS</del>	LAN_to_WAN	accept	- None	SRV-FIREWALL
72	LAN - WAN	LAN_N_SAV	<del>G_DMZ</del> <del>G_VPN_CLIENTS</del>	SAV_to_WAN	accept	- None	SRV-FIREWALL



## Deep Packet Inspection

- Combine IDS et IPS avec un parefeu
  - Analyse des entêtes / données des paquets
  - Détection de la non-conformité protocoles (virus, spams, intrusions)
    - Achemine le paquet
    - Redirige le paquet (statistiques, analyses)
    - Classe le paquet (CoS)
- Différent de SPI qui analyse uniquement les entêtes



# Deep Packet Inspection

- Applications dans une entreprise
  - Avant : Protection du périmètre
    - Protection contre internet
  - Maintenant : Améliore la sécurité à tous les niveaux y compris l'application et l'utilisateur
    - Développement des portables dans l'entreprise
    - Développement des accès nomades
- Applications pour les FAI
  - Conformité vis-à-vis des lois
  - SLA et analyse des emails, sites web, P2P
  - Ciblage comportemental des systèmes de publicité
- Applications pour les gouvernements
  - USA : National Security Agency et Narus (Semantic Traffic Analyzer sur des liens 10 Gbits) en collaboration avec AT&T (plus gros fournisseur de services téléphonique et internet xDSL des USA)
  - Chine : censure (pornographie, religion, politique)
  - Iran : Nokia Siemens Networks qui permet de d'écouter et de bloquer les communications téléphoniques...
  - Lybie, France : filiale de Bull (Amnesys) avec les projets GLINT/SMINT/EAGLE





## Déploiement d'un firewall de nos jours

- Firewall matériel (appliances, boîtes noires)
  - Plate-forme unique, logiciel pré-installé
  - Peut être utilisé pour la prise en charge des petites entreprises ou des filiales disposant, en interne, de faibles ressources informatiques
- Firewall logiciel
  - Options de déploiement de plate-forme souples
  - Peut évoluer en fonction des besoins de l'entreprise





# NETWORK ADDRESS TRANSLATION

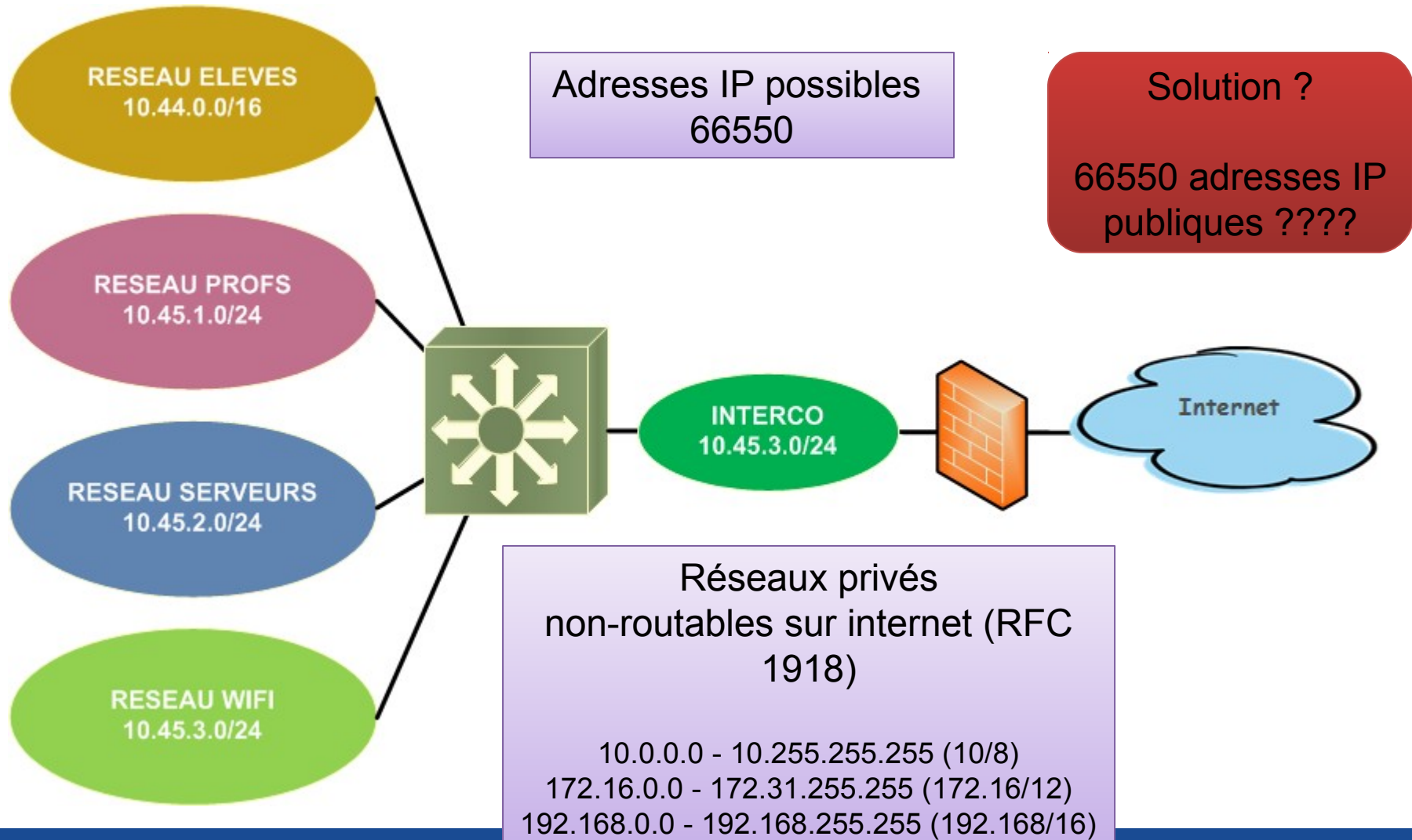


## Définition

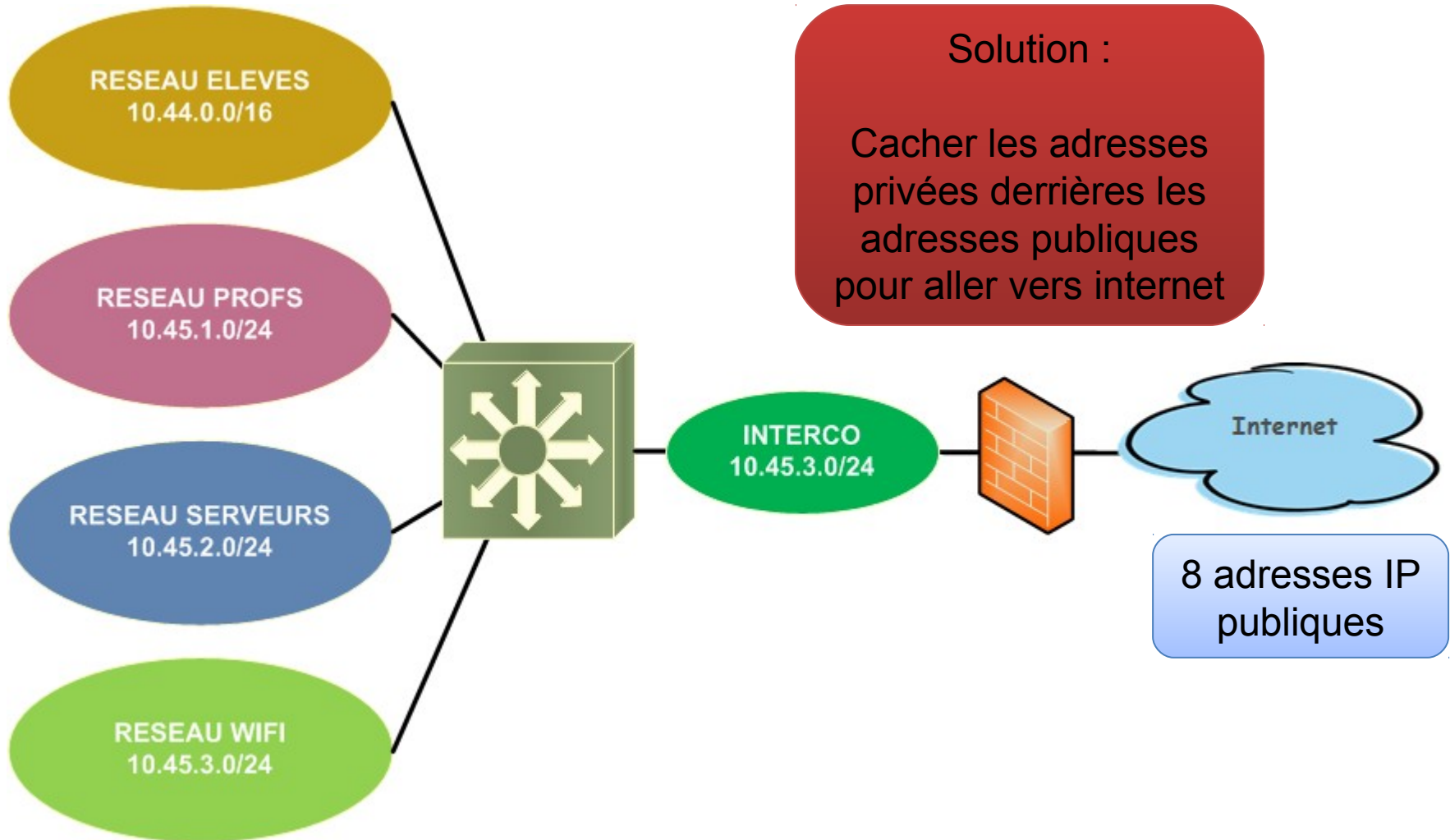
- **Network Address Translation (NAT)**, « traduction d'adresse réseau » en français.
- Mécanisme qui permet de faire correspondre les adresses IP internes non-unique et souvent non routables d'un domaine vers un ensemble d'adresses externes uniques et routables.
- Permet de pallier la carence d'adresses IPv4 sur Internet, le protocole IPv6 dispose d'un espace d'adressage plus important.
- La traduction d'adresse est souvent utilisée pour partager une connexion internet.



## Introduction par l'exemple



## Introduction par l'exemple



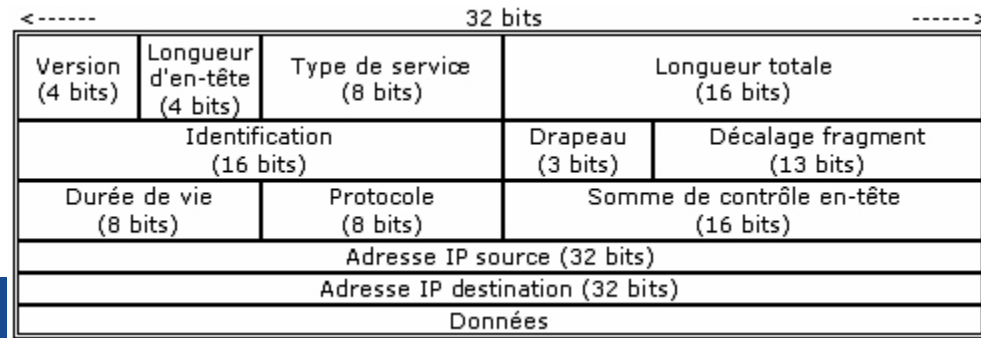


# NAT STATIQUE

- Table de translation fonctionnant par paire

SOURCE		DESTINATION	
Originale	Translatée	Originale	Translatée
IP INTERNE	IP EXTERNE	*	ORIGINALE

- Quand un paquet traverse l'équipement opérant le NAT, l'adresse IP source du paquet est remplacée dans l'en-tête TCP/IP par l'adresse externe.
- 2 interfaces réseaux logiques minimum pour le NAT





# NAT STATIQUE

- Association entre une adresse interne et son homologue externe.
- L'équipement maintient une table de nat « un pour un » basé sur l'adresse IP uniquement.
- Utilisation principale : accès depuis internet à des serveurs d'un réseau privé.
- Le routeur NAT modifie :
  - l'adresse source dans l'en-tête IP du paquet pour mettre une adresse valide en sortie vers internet
  - l'adresse destination dans l'en-tête IP du paquet pour mettre une adresse valide en sortie vers un réseau privé
- 3 types de NAT statique :
  - NAT Statique Unidirectionnel : traduction des connexions de l'extérieur vers l'intérieur.
  - NAT Statique Bidirectionnel : traduction des connexions dans les deux sens.
  - NAT Statique PAT : Conjonction d'une NAT *Statique Uni* ou *Bidirectionnelle* et d'une transformation du port tcp/udp de destination.



# NAT STATIQUE

## NAT Statique Unidirectionnelle

SOURCE		DESTINATION	
Originale	Translatée	Originale	Translatée
*	*	<b>IP EXTERNE</b>	<b>IP INTERNE</b>

## NAT Statique Bidirectionnelle

SOURCE		DESTINATION	
Originale	Translatée	Originale	Translatée
*	*	<b>IP EXTERNE</b>	<b>IP INTERNE</b>
<b>IP INTERNE</b>	<b>IP EXTERNE</b>	*	*

## NAT Statique PAT

SOURCE		DESTINATION		PORT SOURCE		PORT DESTINATION	
Originale	Translatée	Originale	Translatée	Original	Translaté	Original	Translaté
*	*	<b>IP EXTERNE</b>	<b>IP INTERNE</b>	*	Original	25	2525
<b>IP INTERNE</b>	<b>IP EXTERNE</b>	*	*	2525	25	*	Original





## NAT statique : Avantages / Inconvénients

Avantages	Inconvénients
Rendre une machine accessible sur Internet en associant une adresse IP publique à une adresse IP privée	Obligation d'avoir une adresse publique par machine voulant accéder à Internet
Permet de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées	Pénurie d'adresses IPv4 non réglée...
	Attention : en cas de réseau multi-vlans, il faut que toutes les routes soient déclarées
	Proxy ARP



## NAT DYNAMIQUE







- Aucune association prédéfinie entre l'IP publique et l'IP privée de la requête qu'il reçoit l'association entre une adresse interne et sa contre-partie externe est créée dynamiquement au moment de l'initiation de la connexion.
- Ce sont les numéros de ports qui vont permettre d'identifier la traduction en place : le numéro du port source (celui de la machine interne) va être modifié par le routeur. Il va servir pour identifier la machine interne.
- **NAT Dynamique PAT** (Port Address Translation du port client/source) : les adresses externes sont indifférentes.
- **Masquerading** : seule l'adresse IP du routeur est utilisée comme adresse externe. (sous cas de la Dynamique PAT)



# NAT DYNAMIQUE

- NAT Dynamique PAT et Masquerading

SOURCE		DESTINATION		PORT SOURCE		PORT DESTINATION	
Originale	Translatée	Originale	Translatée	Original	Translaté	Original	Translaté
<b>RESEAU INTERNE</b>	<b>IP EXTERNE</b>	*	ORIGINAL E	*	<b>Dynamique</b>	80	Original

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
+ NO NAT (Rules 1-4)							
+ NAT - INSIDE (Rules 5-13)							
+ NAT - VPN (Rules 14-53)							
- NAT - OUTSIDE (Rules 54-55)							
54	 G_PENTASONIC	* Any	* Any	 SRV-FIREWALL	= Original	= Original	 SRV-FIREWALL
55	 G_DMZ	* Any	* Any	 SRV-FIREWALL	= Original	= Original	 SRV-FIREWALL



## NAT dynamique : Avantages / Inconvénients

### Avantages

On peut « cacher » un grand nombre de machines derrière une seule adresse publique

Répond à la problématique de pénurie d'adresses IPv4

Aucune machine privée n'est accessible sur internet = un peu de sécurité en +

### Inconvénients

Aucune des machines du réseau privée n'est accessible sur Internet

Certains protocoles supportent très mal le NAT (ftp passif, h323, p2p IRC-DCC, SIP, icmp, traceroute, DNS), pour palier à cela, les routeurs NAT doivent savoir inspecter le contenu des paquets qui les traversent, et remplacer les adresses IP spécifiées par les adresses traduites. Notez que cela implique de recalculer la somme de contrôle et la longueur du paquet.



## Double NAT

- Technique de double translation d'adresses et de ports :
  - Modification des paramètres de destination
  - Modification des paramètres de la source
- Le NAT cache les adresses internes vis-à-vis de l'extérieur ainsi que les adresses externes vis-à-vis du réseau privé.
- Utilité : interconnexion de plusieurs réseaux privés sont interconnectés qui ont des conflits et des collisions entre l'adressage IP des réseaux privés.

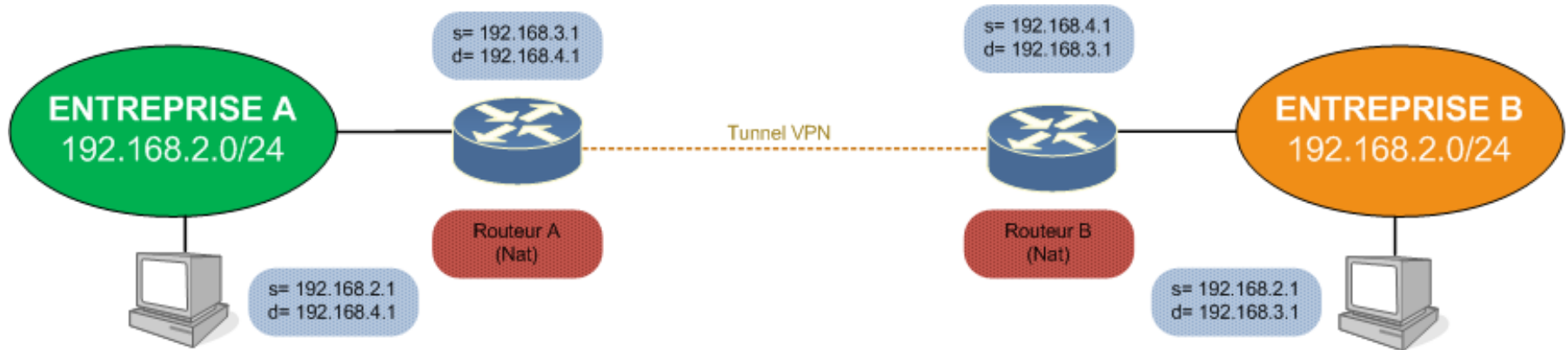
# Double NAT : Exemple

## Routeur A

SOURCE		DESTINATION	
Originale	Translatée	Originale	Translatée
192.168.2.1	192.168.3.1	192.168.4.1	ORIGNALE
192.168.4.1	ORIGNALE	192.168.3.1	192.168.2.1

## Routeur B

SOURCE		DESTINATION	
Originale	Translatée	Originale	Translatée
192.168.2.1	192.168.4.1	192.168.3.1	ORIGNALE
192.168.3.1	ORIGNALE	192.168.4.1	192.168.2.1





# NAT - Récapitulatif

## ● Quand utiliser de la NAT statique ?

Pour rendre disponible une machine (service) sur Internet :

- Serveur FTP
- Serveur HTTP
- Serveur SMTP
- ...

## ● Quand utiliser de la NAT dynamique ?

Le NAT dynamique permet d'une part de donner un accès à Internet à des machines possédant des adresses privées, et d'autre part d'apporter un petit plus en terme de sécurité.

- Economiser les adresse IP publiques
- Donner un accès à Internet à des machines qui n'ont pas besoin d'être joignables de l'extérieur
- Utilisation : entreprise, domicile...



## NAT - Récapitulatif

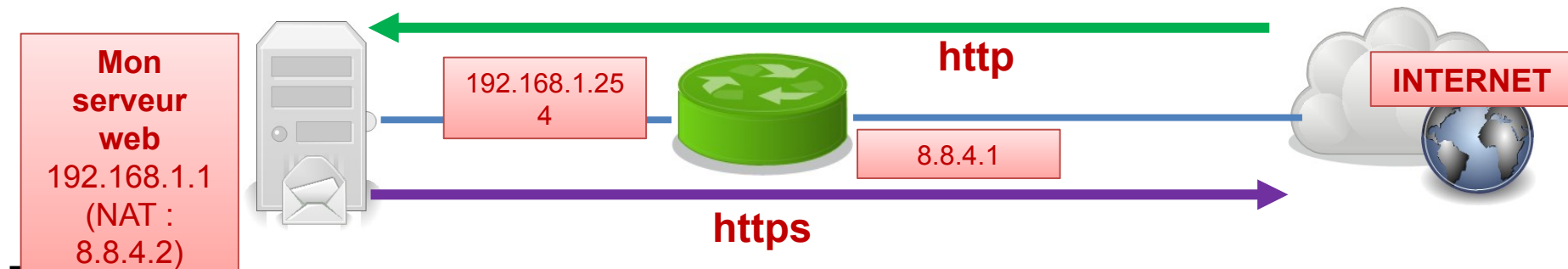
- Quel avenir pour le NAT ? Presque aucun.
  - IPV4 est là pour anticiper la pénurie d'adresse IPV4.
  - Avec IPV6, l'adressage est sur 128 bits, c'est-à-dire que cela revient à attribuer entre 1.564 et 3.911.873.538.269.506.102 adresses par m<sup>2</sup> de surface terrestre (océans inclus).
  - Matériel désormais compatible IPV6 (routeurs, commutateurs, serveurs, postes de travail, etc.)





# EXERCICES

# Exercice n°1



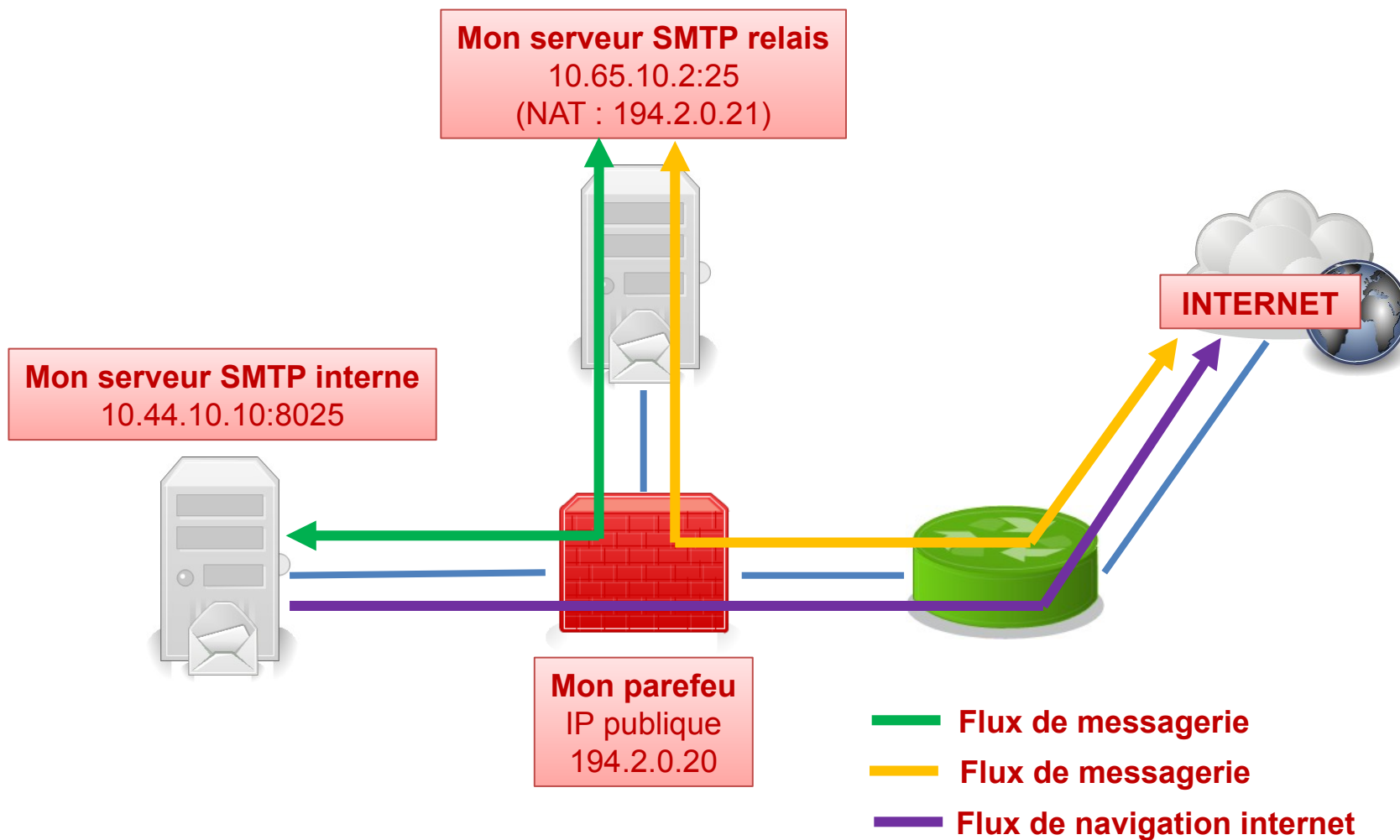
**Filtrage**

Source	Destination	Port source	Port destination	Action
*	*	*	*	DENY

**Translation d'adresse**

SOURCE		DESTINATION		PORT SOURCE		PORT DESTINATION	
Originale	Translatée	Originale	Translatée	Original	Translaté	Original	Translaté

## Exercice n°2





## Exercice n°2

### Filtrage

Source	Destination	Port source	Port destination	Action
*	*	*	*	DENY



## Exercice n°2 (suite)

### Translation d'adresse

SOURCE		DESTINATION		PORT SOURCE		PORT DESTINATION	
Originale	Translatée	Originale	Translatée	Original	Translaté	Original	Translaté