

Plan

1. Qu'est-ce que la sécurité ?
2. Sécurité des systèmes et des réseaux
 1. Sécurité d'un système isolé
 2. Sécurité d'un système appartenant à un réseau
 1. Le NAT statique
 2. Le NAT dynamique
 3. Sécurité d'un ensemble de réseaux
3. Techniques
 1. Le chiffrement
 2. Des protocoles sécurisés

Qu'est-ce que la sécurité ?

s'assurer que

- aucune entité n'effectue une action non autorisée
- aucune entité ne dénie avoir effectué une action qu'elle a effectuée

garantir

- l'intégrité et éventuellement la confidentialité des informations mémorisées
- l'intégrité et éventuellement la confidentialité des informations transmises
- la disponibilité des services pour les parties autorisées

4 mots clés en sécurité et un concept:

- Authenticité, confidentialité, intégrité, disponibilité et non répudiation

Rappel

L'exécution d'actions ne peut se faire que dans un système qui autorise ces actions.

Objectifs, moyens, techniques

objectifs de la sécurité

- sécuriser les systèmes
- sécuriser tout ou partie du réseau
 - pour protéger les systèmes
 - pour protéger les informations transmises

techniques pour la sécurité

- chiffrement
- protocoles sécurisés
- restreindre les accès
- etc...

moyens

- définir une politique de sécurité
 - identifier les entités
 - définir quelle entité a le droit de faire quoi
 - définir ce qui est interdit
- installer la politique définie
- surveiller les systèmes
- participer à la surveillance des réseaux

Pb : les failles de sécurité proviennent à 80% de l'intérieur de l'entreprise

Sécurité d'un système isolé

Objectifs

- éviter que des entités effectuent des actions non autorisées
 - éviter les processus interdits
 - éviter que des processus autorisés n'effectuent des opérations interdites

Définir une politique de sécurité et la valider

- qu'est ce qui est autorisé / interdit à chaque entité ?

Installer la politique définie

- identifier qui tente de faire quoi
- spécifier les autorisations et les interdictions
- dans un système d'exploitation qui le permet

**attribuer des comptes
droits sur les programmes
droits sur les données**

Vérifier la politique installée

- journaliser
- alerter

niveau de sécurité d'un système

Common Criteria (CC)

voir ANSSI

www.ssi.gouv.fr

Sécurité d'un système appartenant à un réseau

Rappel : un système ne peut être attaqué que s'il a un processus serveur en attente de demande (*port en état listen*).

Configuration des services

- quels services sont nécessaires ? pour quels clients ?
- droits des services (UID, GID, chroot...)
- choix des implémentations

Contrôle des services actifs

- à partir de la configuration du système
- en examinant les services en attente, de l'intérieur (`netstat`) ou de l'extérieur du système (`nmap`)

Contrôle des demandes de service

- filtrage des demandes avant de les livrer aux entités serveurs
- journalisation des demandes
- alertes en cas de demandes interdites
- remonter les tentatives malveillantes

CERT

Computer Emergency Response Team

www.cert.org

Sécurité d'un réseau (1)

Au niveau Réseau (pour un réseau isolé par un équipement)

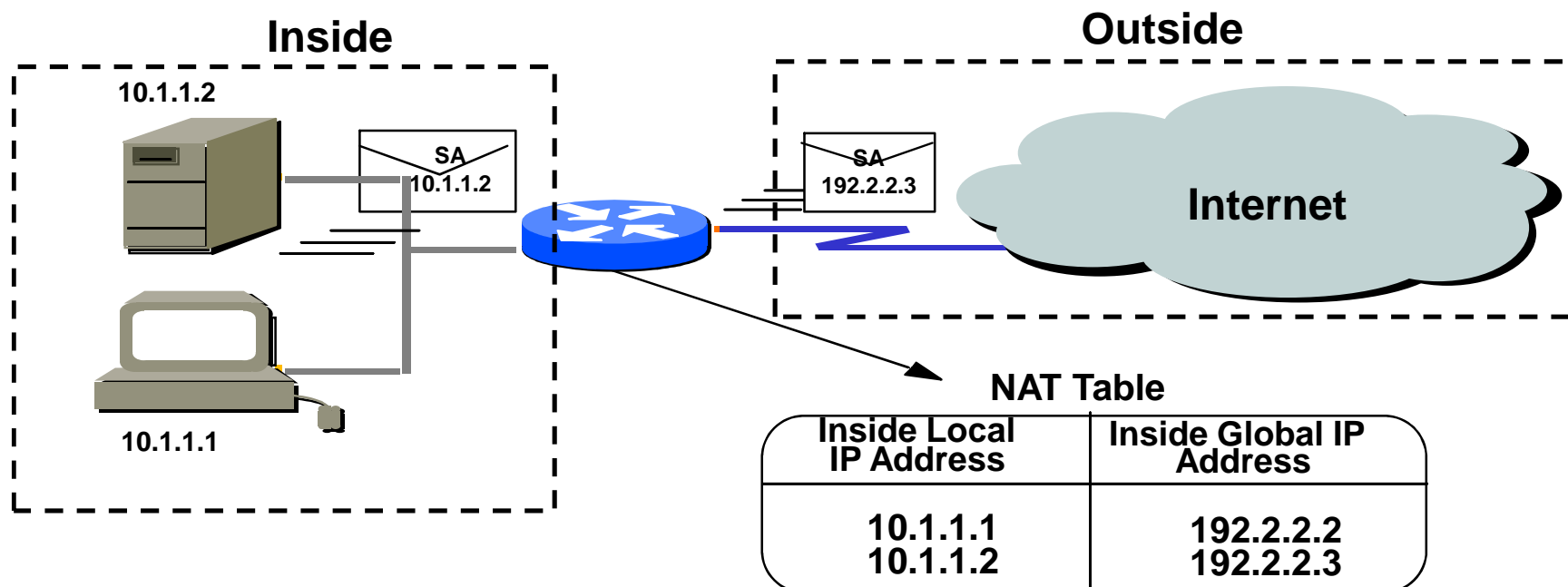
- identification du réseau et des systèmes qui le composent
 - adresses privées (RFC 1918)
 - Classe A : 10.0.0.0
 - Classe B : 172.16.0.0 à 172.31.0.0
 - Classe C : 192.168.0.0 à 192.168.255.0
- protection par le routeur
 - règles de filtrage sur la source, la destination ou les deux (fonction pare-feu)
 - traduction d'adresses
 - IP-masquerading,
 - Network Address Translation (statique ou dynamique),
 - Port Address Translation,
 - » Attention, il peut être nécessaire de réécrire le message du fait du changement d '@IP.
 - » Pas de chiffrement
 - » Pas de journaux (performances...)

Sécurité d'un réseau (2)

Le NAT statique = association de n adresses avec n adresses.

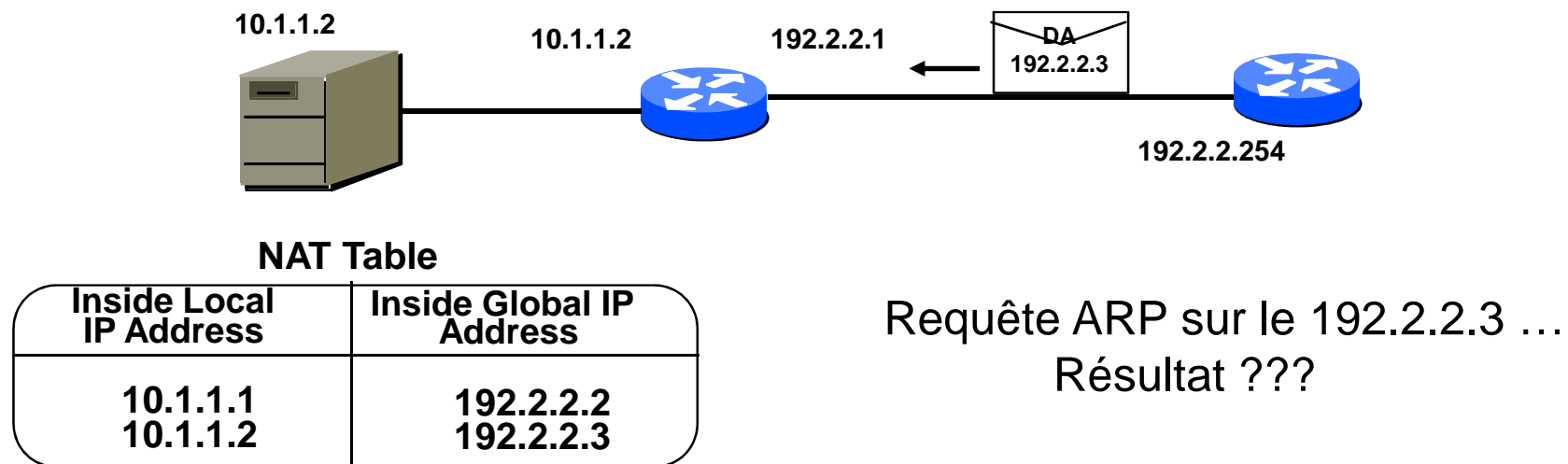
C'est à dire qu'à une adresse IP interne, on associe une adresse IP externe.

Rôle du système: remplacer l'adresse de la station du réseau par une adresse externe (publique).



Sécurité d'un réseau (3)

Problème : comment retrouver le chemin de retour ?

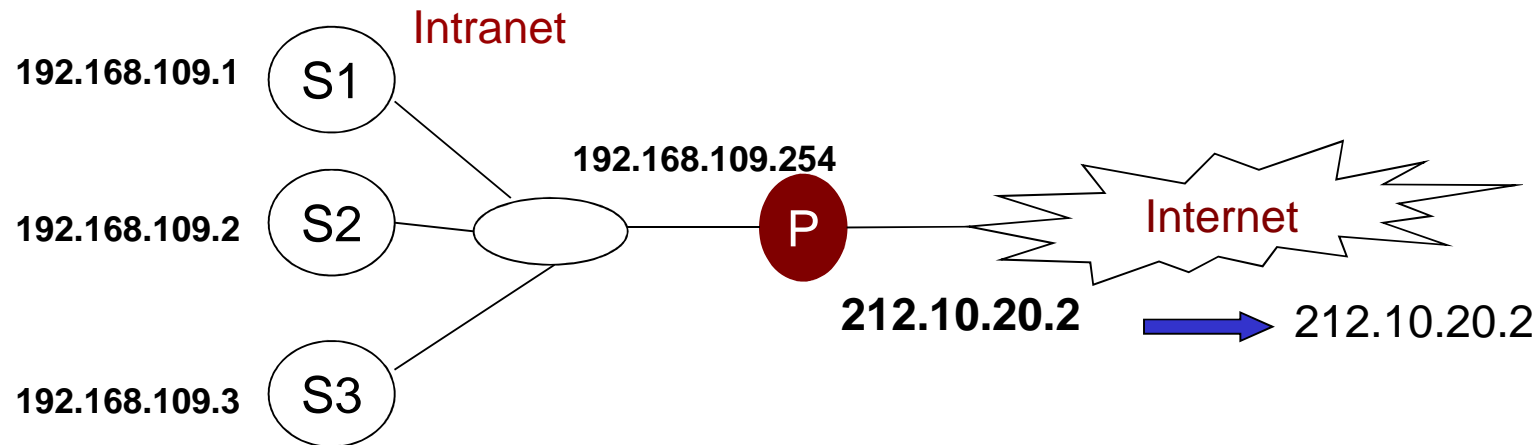


Solution : le Proxy-arp

Le « routeur » renvoie son adresse MAC pour toutes les adresses contenues dans la table NAT.

En général, les pare-feux ou les routeurs ont cette fonctionnalité

Sécurité d'un réseau (4)



1 seule adresse est disponible pour envoyer des paquets IP vers Internet (ex: adsl)

Pb: Si plusieurs stations appartiennent au réseau local, comment peuvent-elles envoyer des PDU-IP vers l'internet et comment les différencier ?

=> Utilisation du NAT dynamique

Sécurité d'un réseau (5)

2 cas possibles :

- 1 seule adresse IP de sortie -> **PAT**
- n adresses de sortie pour m ordinateurs ($m > n$)
-> **IP masquerading ou PAT**

Fonctionnement :

- *En Masquerading*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy)
- *En PAT*, traduction automatique de l'adresse IP de la station émettrice avec l'adresse IP de la Passerelle (routeur, proxy) et translation du port.
La translation du port permet de différencier les stations qui utilisent la même adresse IP Passerelle.

Application possible : mini-réseau derrière un routeur ADSL ➔ pb : adresse IP statique/dynamique

Sécurité d'un réseau (6)

Au niveau Transport

- filtrage sur les numéros de port -> quelles communications client-serveur sont autorisées ?
- suivi de communication client-serveur

Au niveau Application

- contrôle de contenu applicatif -> autorisations, authentications, contenus
 - par un proxy applicatif

Utilisation d'un pare-feu / garde-barrière / *firewall*

- ensemble des moyens mis en œuvre pour sécuriser un réseau
- filtrage transport et applicatif

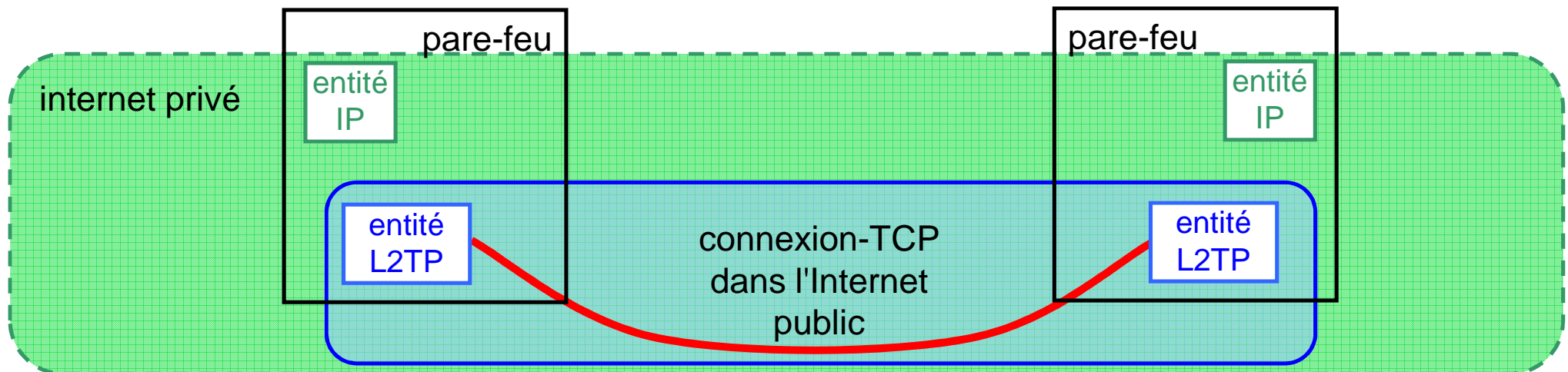
Sécurité d'un ensemble de réseaux

Contexte

- une organisation possède plusieurs réseaux distants les uns des autres
 - interconnexion par un médium "privé" : cher, mais sûr
 - interconnexion par l'Internet public : économique, mais non sûr

une solution : le *tunnelling ou VPN (Virtual Private Network)*

- les PDU sont transportées chiffrées entre 2 réseaux grâce à un Service "On intègre la machine distante dans le réseau de l'entreprise"
- les extrémités sont identifiées
- Protocole utilisée : L2TP *Layer 2 Tunnelling Protocol* -> IETF



Chiffrement - Définitions

source : <http://fr.wikipedia.org/wiki/Cryptologie>

Cryptologie (cryptology)

- C'est l'étude scientifique de la cryptographie et de la cryptanalyse.

Cryptographie (cryptography)

- C'est l'étude du chiffrement et du déchiffrement, ainsi que des procédés permettant d'assurer l'intégrité, l'authentification et la signature.

Cryptanalyse (cryptanalysis)

- C'est l'étude des procédés de décryptage. Son utilisation est illégale.

Chiffrement (encryption)

- C'est transformer une information pour assurer son secret.

Déchiffrement (decryption)

- C'est l'action inverse du chiffrement, qui consiste à retrouver l'information initiale contenue dans le message chiffré.

Décryptage

- C'est l'action qui consiste à "casser" le chiffrement d'une information.

Chiffrement : principes

Définitions

- chiffrement
- déchiffrement

$$\begin{array}{ccc} M & \xrightarrow{E_k} & C \\ C & \xrightarrow{D_{k'}} & M \end{array}$$

E algorithme de chiffrement
D algorithme de déchiffrement
k clé de chiffrement
k' clé de déchiffrement

Propriétés (souhaitées) d'un cryptosystème

- $D_{k'}(E_k(M)) = M$ où les clés k et k' sont associées
- $D_{k'}$ et E_k dépendent totalement ou partiellement d'informations secrètes
- les algorithmes doivent être économiques : processeur, mémoire, taille de code
- le secret doit reposer sur les clés plutôt que sur les algorithmes
 - algorithme public - > qualité meilleure
- la calcul de k' doit être très difficile, même si on connaît C et M
- $D_b(E_a(M))$ doit être une information non valide

Chiffrement : cryptosystèmes

A chiffre symétrique ($k = k'$)

- économique
- problème de la gestion des clés

A chiffre asymétrique ($k \neq k'$)

- $D_{k'}(E_k(M)) = E_k(D_{k'}(M)) = M$
- peu économique

DES (*Data Encryption Standard -fin en 2001*)


Triple-DES

IDEA (*International Data Encryption Algorithm*)

AES (*Advanced Encryption Standard*)

DH (*Diffie-Hellman*)

RSA (*Rivest, Shamir, Adleman*)



$$E_k(M) = M^e \text{ modulo } n \quad k = \{e, n\}$$
$$D_{k'}(C) = C^d \text{ modulo } n \quad k' = \{d, n\}$$
$$n = p * q$$
$$p \text{ et } q \text{ premiers entre eux}$$
$$e \text{ premier avec } (p-1) * (q-1)$$
$$d * e = 1 \text{ modulo } ((p-1) * (q-1))$$

hachage

- pour créer des empreintes d'information (*digest*)
- algorithmes analogues à ceux du chiffrement
- pas de déchiffrement

MD5 (*Message Digest*)

SHA-1 (*Secure Hash Algorithm*)

Chiffrement : utilisations

chiffrement avec une clé secrète partagée entre 2 entités

- seules les 2 entités peuvent déchiffrer

authentification
confidentialité
intégrité
non répudiation

chiffrement avec la clé publique d'une entité

- seule l'entité possédant la clé privée associée à la clé de chiffrement peut déchiffrer

confidentialité

chiffrement avec la clé privée d'une entité

- tout le monde peut déchiffrer avec la clé publique associée
- si la tentative de déchiffrement produit un résultat valide
 - preuve de la source
 - l'information est intègre
 - seule l'entité a pu chiffrer

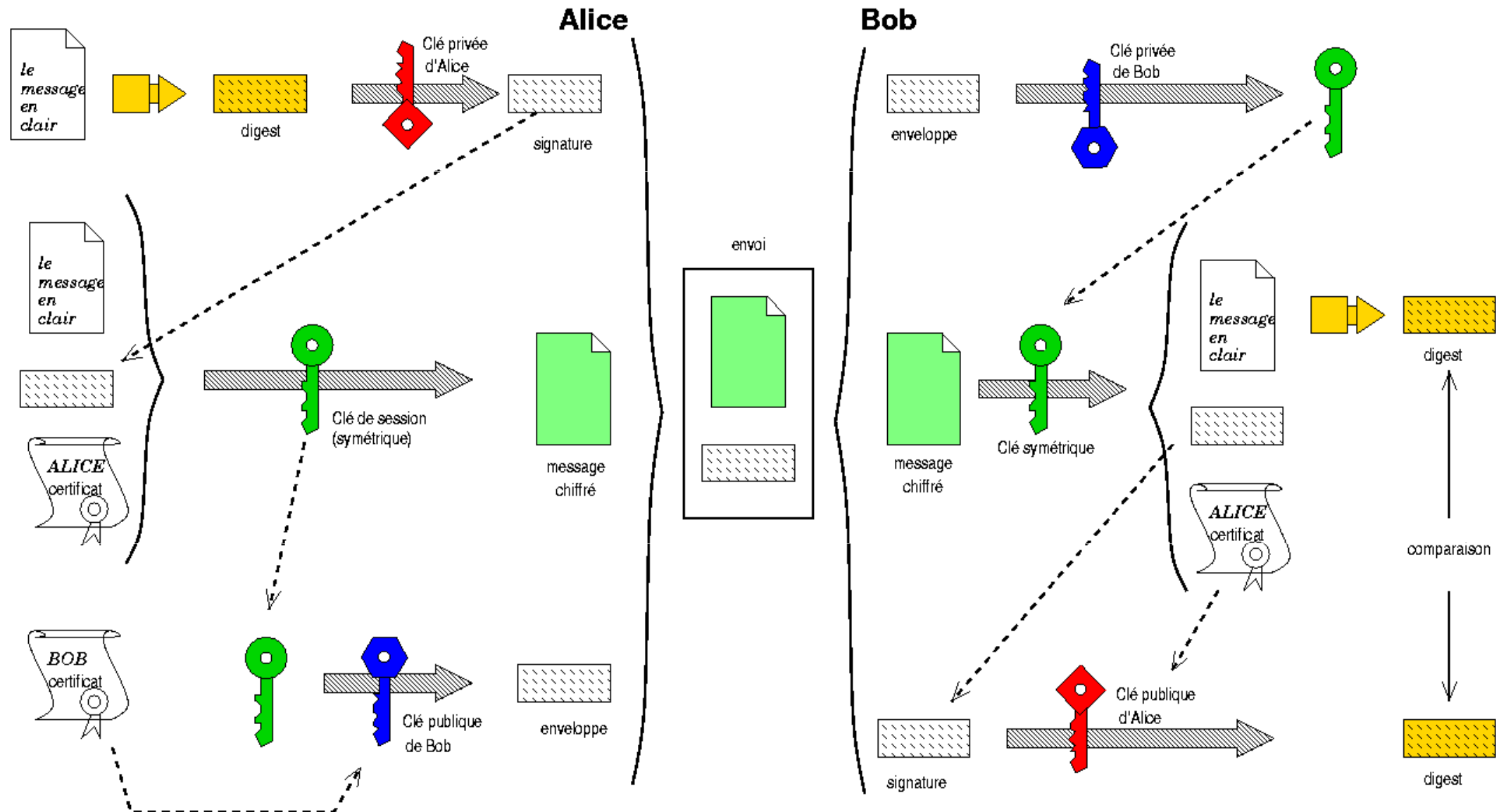
authentification
intégrité
non répudiation

distribution des clés

- certificats
 - preuve de possession
 - contient la clé publique
 - délivré par une autorité de certification

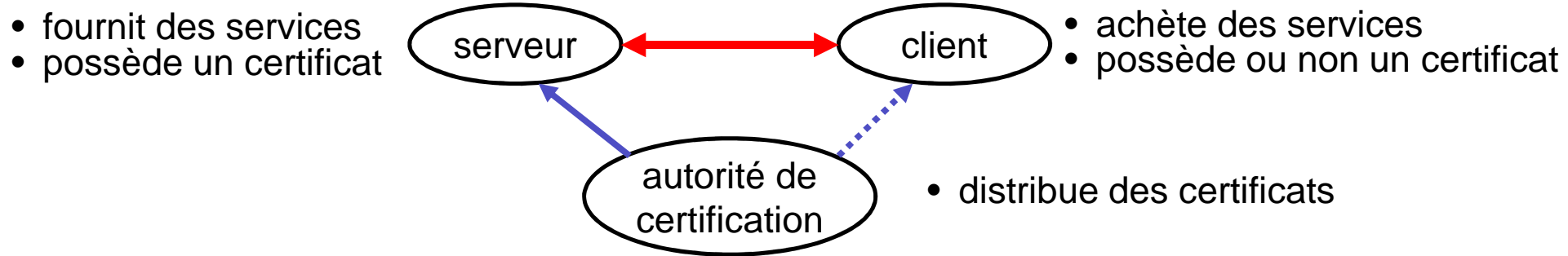
domaine de confiance

Chiffrement : exemple résumé

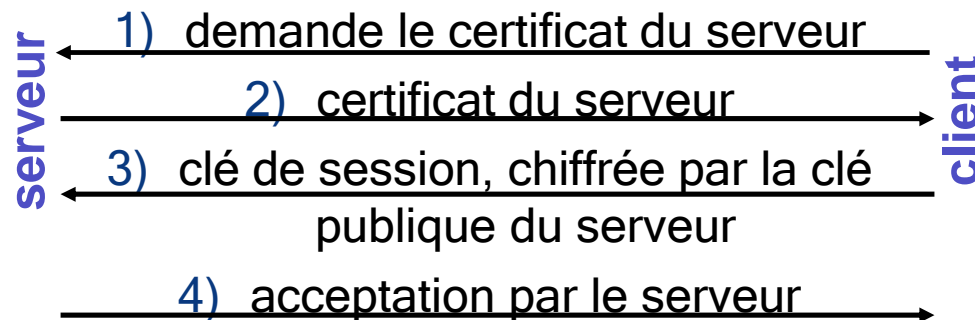


Protocole sécurisé : SSL

Secure Socket Layer (Netscape 1994)



établissement de connexion ssl



transmission d'informations

- non chiffrée
- chiffrée avec la clé publique du serveur
- chiffrée avec la clé de session
- compression éventuelle

problèmes

- le client n'est certifié qu'optionnellement ⇒ risque pour le serveur
- si le client est certifié, il ne peut pas être anonyme ⇒ risque pour le client
- pas de contrôle de validité des certificats entre délivrance et fin de validité
- autorités de certification

Sécurité Wi-Fi

Protection par défaut : le WEP

- Utilise un codage pour les données

- l'implémentation WEP (Wired Equivalent Privacy) (clé sur 40 bits / 104bits) donnée par les utilisateurs auquel est rajouté un vecteur d'initialisation (24 bits).

Fonctionnement : chiffrement RC4 en utilisant la clé + vecteurs d'initialisation (IV)

message envoyé = $(M.c(M)) \text{ xor } RC4(IV . K)$

$c(M)$ = checksum de M et K = clé

le RC4 donne des séquences pseudo-aléatoires

Le vecteur d'initialisation change à chaque trame envoyé, on lui rajoute 1

(assez facilement crackable si on connaît le 1er octet de M et IV)

Pb : faiblesse d'implémentation dans IV commencent à 0 puis
incrémentés de 1 à chaque envoi, vecteurs faibles

Actuellement, quelques dizaines de minutes pour cracker clé WEP

Si utilisation de WEP, alors codage supplémentaire : ssl, Ipsec, ssh,...

Protocole Kerberos (1)

Protocole d'authentification fonctionnant avec DES

pré-requis :

- Un ordinateur jouant le rôle du Tiers de confiance (KDC -Key Distribution Center)
- Un client partageant une clé secrète avec le Tiers de confiance
- Un serveur partageant une clé secrète avec le Tiers de confiance

But :

- Connexion du client au serveur

2 Phases :

- Récupération d'une clé de session après authentification vers le KDC
- Authentification vers le serveur et connexion

Protocole Kerberos (2)

Phase 1 :

- Client envoie vers KDC une demande de connexion vers un serveur en clair
 - identité, nom du serveur, durée prévue
- Vérification des droits du client par KDC
- KDC envoie vers client une réponse cryptée avec clé client en DES
 - clé de session, date d'expiration de cette clé, nom du serveur
 - ticket kerberos (clé de session, date d'expiration) crypté avec clé serveur

Phase 2 :

- Client envoie vers serveur
 - ticket kerberos
 - authentificateur (horodatage, clé optionnelle) crypté avec clé de session
- Serveur déchiffre le ticket kerberos et decode authentificateur
 - Vérification horodatage (protocole NTP)
- Communication en utilisant clé de session