Administration Réseau

Réseaux et sécurité, Principes

McInfo4 - Réseaux

Département d'informatique
IUT Bordeaux 1

Février 09

Pourquoi la sécurité ?

- Maladroits, pirates, plaisantins et autres malveillants
- Protéger ce qu'on a à protéger
- Continuer à fonctionner
- Responsabilité morale et légale

La sécurité n'est pas (seulement) un problème technique

- Les mesures de sécurité amènent des contraintes
- Gêne trop grande pour les utilisateurs ⇒ stratégies de contournement
- Nécessité
  - de sensibiliser les utilisateurs
  - d'établir une politique de sécurité

Les éléments d'une politique

- Ce qui est **obligatoire**
  - Changer de mot de passe, le garder secret
- Ce qui est **interdit**
- Ce qui est **illégal** (évidemment !)
- le reste
  - WEB pendant les heures de travail ? ....

Les éléments d'une politique (suite)

- Ce qui est **autorisé**
- Ce qui est **conseillé**
- ...

Facteurs de succès d'une politique de sécurité

- Une **politique officielle explicite**, correspondant à la réalité
- avec le **soutien** de la hiérarchie
- avec des **moyens** correspondant aux besoins
- l'**adhésion** des utilisateurs

Éléments techniques

- Réseaux interne / externe
- Adresses privées / publiques
- Routeurs, passerelles, filtrage...
- Serveurs, postes-clients, "bastions",...
- Proxy (mandataire, relais)
- Tunnels, réseaux privés virtuels (VPN)
- ...

Un réseau, avec des machines à intérieur, relié à l'extérieur

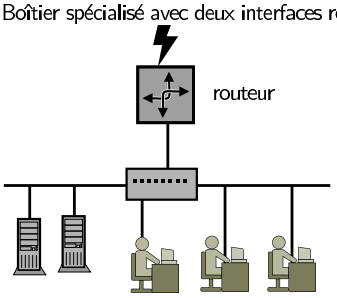
- Permettre l'accès
  - De l'intérieur, à certains services extérieurs
  - De l'extérieur, à certains services hébergés sur des serveurs internes
- Protéger les machines internes

Approche fonctionnelle (suite)

- **Bastions** : les serveurs "exposés" qui doivent être surveillés particulièrement
- En général, on limite l'accès aux services extérieurs (P2P...)
- Rappel : responsabilité des employeurs

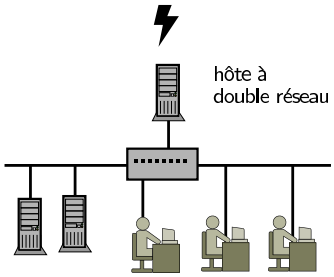
Routeur filtrant

Boîtier spécialisé avec deux interfaces réseau



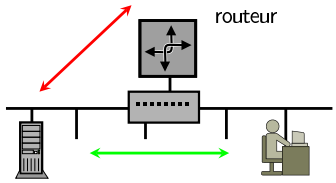
Hôte à double réseau

Ordinateur avec deux interfaces réseau, peut héberger des services.



Exemple

- Routeur non filtrant
- On donne des adresses IP privées aux machines du réseau
  - Exemple : 10.1.1.1, 10.1.1.2
- Les serveurs ont aussi une adresse IP publique



public 147.210.94.100
privé 10.1.1.4

privé
10.1.1.1

Filtrage

Le routeur **laisse passer / interdit** certaines communications, selon

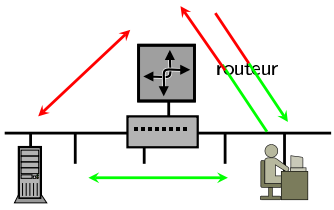
- adresses IP (source /dest)
- protocoles (IP, TCP, ...)
- numéros de ports
- "flags" des paquets IP
- ...

Mandataires, NAT

Les clients ne peuvent pas dialoguer directement avec l'extérieur

- passage par des **mandataires**
  - ok pour certains services (smtp, nntp, web, ftp...)
  - Plus compliqué pour d'autres (sessions telnet, visio,...)
- technique de "**masquerading**"
  - *Network Address Translation* : traduction d'adresse
  - SNAT = source NAT

Masquerading



public 147.210.94.100
privé 10.1.1.4

privé
10.1.1.1

- Le routeur "déguise" les paquets venant du client pour faire croire qu'il en est l'émetteur
- Le serveur distant répond au routeur
- Le routeur fait suivre les réponses au client

Exemple masquerading

Exemple :

1. début de session telnet de 10.1.2.3 en direction de 220.6.7.8 (TCP, port 23)
2. Le routeur remplace l'adresse d'origine (10.1.2.3) par sa propre adresse, et fait suivre à 220.6.7.8
3. Le site extérieur répond au routeur
4. Le routeur remplace l'adresse de destination (la sienne) par celle du demandeur 10.1.2.3 et transmet sur le réseau interne

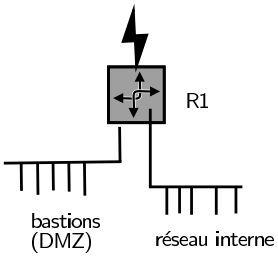
La communication passe entre 10.1.2.3 et 220.6.7.8.

Architecture à "DMZ"

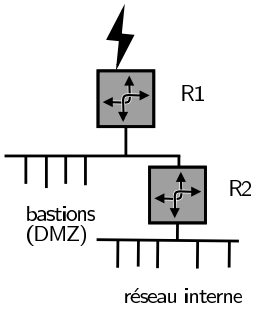
DMZ = zone démilitarisée
Découpage du réseau interne en 2 zones séparées

- la zone démilitarisée contient les bastions (serveurs accessibles de l'extérieur)
- Postes clients inaccessibles de l'extérieur

DMZ à 1 seul routeur



DMZ à 2 routeurs



Conclusion

La sécurité possède des aspects **techniques**, mais aussi "**politiques**".
Compromis entre

- ce qu'on devrait faire
- ce qu'on peut faire
- ce qui est acceptable par les utilisateurs