Architecture d'un réseau pour la sécurité

Fred Hémery

IUT Béthune
Département
Réseaux &
Télécommunications

TRC8 Sécurité Avancée — 07/08

Plan

Introduction

- Sécuriser l'environnement physique
  - accès aux salles
  - stockage des sauvegardes dans un lieu différent
- Sécuriser les systèmes d'exploitations
  - Mettre à jour les versions du système d'exploitation
- Sécuriser les applications
  - Garantir le bon fonctionnement de l'application quelques soient les utilisations (vérification des données saisies par l'utilisateur)
- Sécuriser l'accès aux données
  - Accès protegé par une identification et gestion des droits en fonction du rôle de l'utilisaeur

Introduction

- Une entreprise qui veut être connectée au réseau doit garantir la sécurité de son réseau interne, et en particulier :
  - La confidentialité (données de l'entreprise) ;
  - L'intégrité (modifications involontaires) ;
  - La réputation de l'entreprise
- Identification de la menace
  - Les failles
  - Les virus
  - Stupidité, accidents

Failles

Elles sont exploitées par les pirates (hackers, crackers)

- Failles de programmation
  - le pirate transforme le programme exécuté par le processus (buffer overflow)
  - Les données saisies par l'utilisateur dans un formulaire
  - Requête SQL
  - Forums de discussion
- Quelques chiffres du NIST (*National Institute of Standards and Technology*)
  - 17 vulnérabilités / jour en moyenne
  - 12 failles critiques pour les 3 premiers mois 2006

Virus

- Programme informatique qui en modifie un autre pour pouvoir se reproduire (programme auto propageant)
- Type
  - Vers : se propagent au travers du réseau
  - Troyens : Création d'une faille dans le système
  - Bombes logiques : virus qui va se déclencher suite à un événement (date, utilisation particulière d'un logiciel)
  - Spyware : programme collectant des données privées pour les renvoyant vers son créateur
  - Pishing : imitation plus ou moins fidèle d'un site officiel
  - Mail spam (publicité) et HOAX(faux mail)
- Protection
  - Pare-feu contre les vers
  - Antivirus qui analyse les courriers et les exécutables
- Evolution
  - 1980 : 20 virus recencés
  - 2003 : 65000 virus
  - 2004 : 79000 virus

Introduction

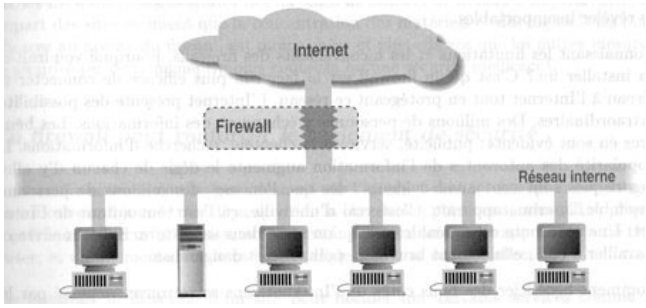
- Les types d'attaques
  - Intrusions ;
  - Refus de service
  - Vols d'informations
- Les outils
  - Le pare-feu
  - Logiciels anti-virus
  - Logiciels d'audit
  - Les IDS (Instruction Detection System)
  - Les Honeypots (pots à miel)
- Stratégies de sécurité
  - Le moindre privilège
  - Le goulot d'étranglement

Plan

Les pares-feu : Introduction

- Un pare-feu, garde-barrière, firewall est là pour éviter qu'un danger qui vient du monde Internet entre dans votre réseau interne.
- Ses fonctions sont :
  - Restreindre l'accès de votre réseau à un seul point précis ;
  - Empêcher les menaces de s'approcher de vos autres défenses
  - Restreindre les sorties à un seul point précis
- De manière logique un pare-feu est
  - Un séparateur
  - Un limitateur
  - Un analyseur
- Son implémentation physique est réalisée par un ensemble de composants matériels comme : un routeur, un ordinateur hôte ou une combinaison d'ordinateurs.

Les pares-feu



Les pares-feu

- Les possibilités d'un pare-feu
  - Il est au centre des décisions de sécurité (plus efficace qu'une décision diffuse)
  - Il peut renforcer le règlement de sécurité. Il peut en particulier interdire l'utilisation de données partagées (NFS, NIS, ...)
  - Il enregistre toutes les activités vers ou en provenance d'Internet
- Ce qu'il ne peut prendre en charge
  - Il ne protège pas des utilisateurs malveillants qui se trouvent dans le réseau interne
  - Il ne protège pas contre les connexions qui ne passent pas par lui
  - Il ne protège pas directement des virus

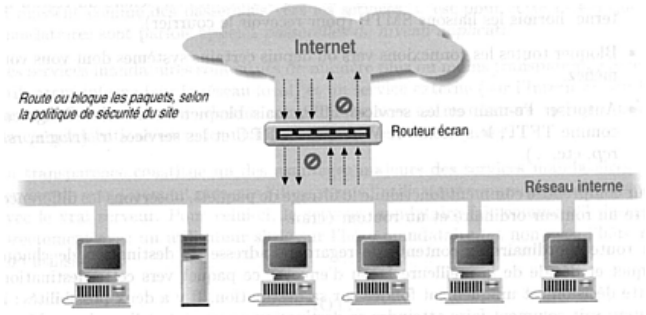
Les pares-feu

- Le filtrage de paquets
  - Le filtrage de paquets est l'action qui permet de contrôler le flux de données depuis et vers un réseau.
  - Les filtres autorisent ou bloquent les paquets et cela en fonction de règles
- Le filtrage applicatif(proxy) ou service mandataire
  - Le service mandataire (proxy) analyse le trafic au niveau applicatif(HTTP, FTP, . . .)
  - Un service mandataire est un service qui communique avec les serveurs externes à la demande de clients internes.
  - Les clients envoient leurs requêtes au serveur mandataire (proxy) qui relaie les requêtes approuvées vers les serveurs externes et ensuite relaie les réponses vers les clients.

Plan

Le filtrage

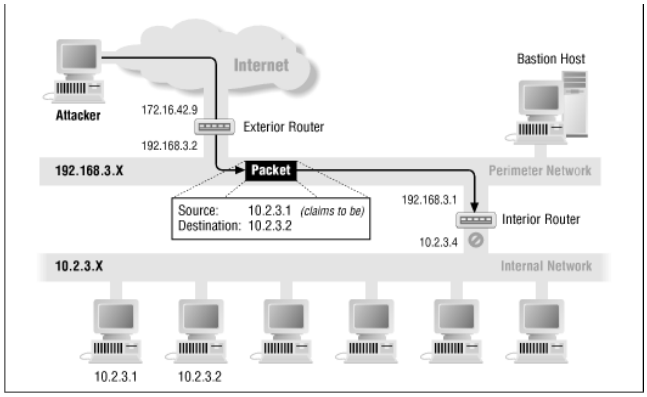
- Les systèmes de filtrage de paquets routent les paquets entre hôtes internes et externes, mais de façon sélective,
- Ils autorisent ou bloquent certains types de paquets au regard de règles qui ont été élaborées pour mettre en place une politique de sécurité.



Le filtrage

- Le filtrage se fait en fonction de
  - L'adresse IP source
  - L'adresse IP destination
  - Le type de protocole TCP, UDP, ICMP, ...
  - Le Port TCP, UDP source et/ou destination
  - Le type de message ICMP
  - Le type de message dans le suivi de session (Syn)
  - L'interface sur laquelle le paquet arrive (sens de communication)
  - L'interface sur laquelle le paquet va sortir
- Certains protocoles sont difficiles à traiter : le protocole RPC qui utilise le protocole UDP de la couche transport, n'a pas de numéro de port connu à l'avance.

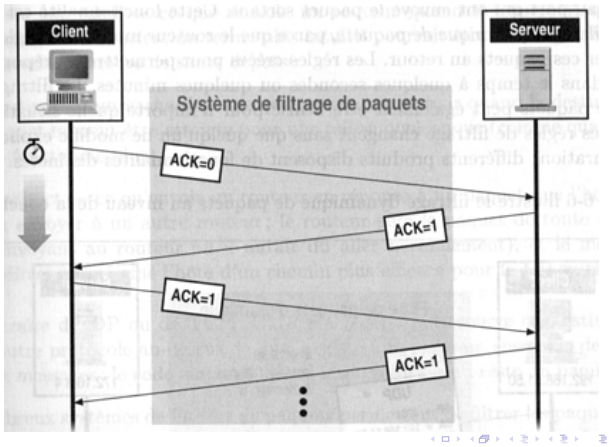
Le filtrage : vol d'adresse IP



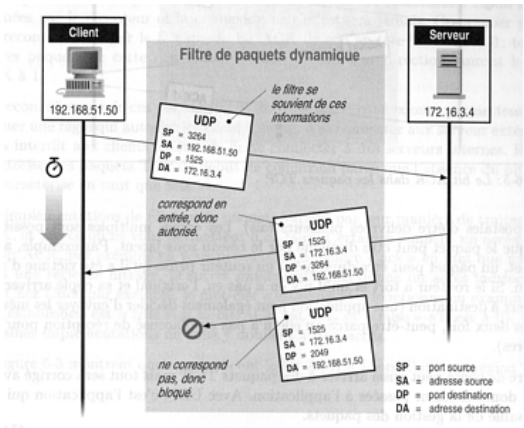
Le filtrage : le protocole TCP

- Le protocole TCP est un protocole qui fonctionne en mode connecté ⇒ avant d'échanger des informations, les deux correspondants doivent établir la connexion.
- Les attaques
  - Vol de session TCP
  - Fragments *overlapping*
  - Fragments *tiny*
- La technique
  - On découpe les paquets avec une taille mini 68 octets en utilisant la fragmentation. Le premier fragment ne contient pas de demande de connexion, il est accepté dans le deuxième.
  - En utilisant l'offset (position du 1er caractère dans le fragment dans le paquet complet) on recouvre le fragment précédent en faisant une demande de connexion cette fois.

Le filtrage : le protocole TCP



Le filtrage : le protocole UDP



Le filtrage

- Avantages
  - Il protège un réseau complet
  - Il est transparent pour l'utilisateur
  - Il est disponible sur de nombreux routeurs
- Inconvénients
  - Les règles sont parfois difficiles à configurer ou encore à tester
  - Certains protocoles ne sont pas adaptés au filtrage comme le protocole RPC (utilisé avec NFSv3, NIS)

Le filtrage par adresse

- Écriture de règles de filtrage
  - Vous voulez autoriser uniquement le trafic IP entre un hôte externe (1172.16.51.50) et les hôtes de votre réseau 193.49.62.0.

Règle	Direction	@ source	@destination	Ack = 1	Action
A	Entrant	172.16.51.50	193.49.62.0/24	-	Ok
B	Sortant	193.49.62.0/24	172.16.51.50	-	Ok
C	Toutes	Toutes	Toutes	-	Refus

la direction s'exprime en fonction du réseau interne

TAB.: filtrage IP

Le filtrage par service

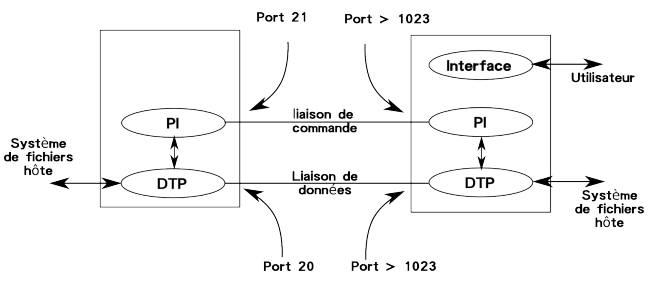
Écriture des règles pour le filtrage du service Telnet en accès client

- Caractéristiques des paquets pour le service Telnet sortant
  - @IP source et une adresse locale
  - Utilise le protocole TCP
  - Le port destinataire doit être **23**, le port source aléatoire doit être supérieur à **1023**
  - Le premier paquet (qui établit la connexion) à le bit **ACK = 0**, les autres l'ont à **1**.
- Caractéristiques des paquets pour le service Telnet entrant
  - @IP source et une adresse distante
  - Le port source doit être **23**, le port destination doit être supérieur à **1023**
  - Tous les paquets auront le bit **ACK = 1**

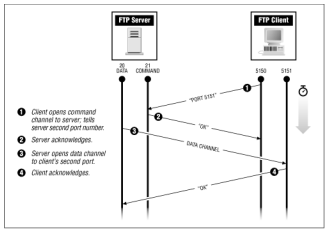
Règle	Direction	@ source	@destination	Protocole	Port Src	Port Dest	Ack = 1	Action
A	Sortant	Interne	Toutes	TCP	> 1023	23	-	Ok
B	Entrant	Toutes	Interne	TCP	23	> 1023	Oui	Ok
C	Toutes	Toutes	Toutes	Tous	Tous	Tous	-	Refus

TAB.: Filtrage du service telnet

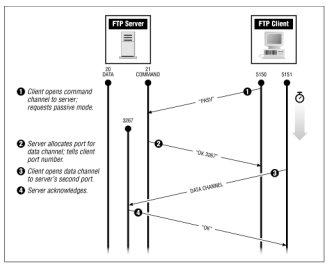
Le filtrage par service : FTP



Le filtrage par service : FTP



Mode actif (défaut)



Mode passif

Le filtrage par service : FTP

Règle	Direction	@source	@destination	Protocole	Port Src	Port Dest	Ack=1	Action	Observation
				Serveur FTP					
A	Entrant	Externe	Interne	TCP	> 1023	21	-	Ok	Requête FTP entrante
B	Sortant	Interne	Externe	TCP	21	> 1023	Oui	Ok	Réponse
				mode actif					
C	Sortant	Interne	Externe	TCP	20	> 1023	-	Ok	Création canal données
D	Entrant	Externe	Interne	TCP	> 1023	20	Oui	Ok	Réponse canal données
				mode passif					
E	Entrant	Externe	Interne	TCP	> 1023	> 1023	-	Ok	Création canal données mode passif
F	Sortant	Interne	Externe	TCP	> 1023	> 1023	Oui	Ok	Réponse canal données requête entrante
				client FTP					
G	Sortant	Interne	Externe	TCP	> 1023	21	-	Ok	Requête FTP sortante
H	Entrant	Externe	Interne	TCP	21	> 1023	Oui	Ok	Réponse requête sortante
				mode actif					
I	Entrant	Externe	Interne	TCP	20	> 1023	-	Ok	Création canal données pour la requête ftp sortante
K	Sortant	Interne	Externe	TCP	> 1023	20	Oui	Ok	Réponse canal données requête ftp sortante
				mode passif					
L	Sortant	Interne	Externe	TCP	> 1023	> 1023	-	Ok	Création canal données requête ftp sortante mode passif
M	Entrant	Externe	Interne	TCP	> 1023	> 1023	Oui	Ok	Réponse canal données requête ftp sortante mode passif

TAB.: Protocole FTP

La translation d'adresse

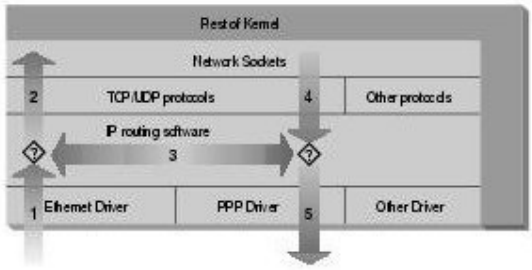
- **NAT** : *Network Address Translation* est un service qui permet de translater un ensemble d'adresses (privées, 10.0.0.0, 172.16.0.0, 192.168.0.0) vers un ensemble d'adresses (publiques)
- Quand une machine transmet un paquet vers l'Internet, le service NAT du firewall translate l'adresse de l'émetteur vers une autre adresse avant de le transmettre sur le réseau. Lorsque la réponse arrive, le firewall translate l'adresse du destinataire vers l'adresse d'origine
- **DNAT** : Desination Network Address Translation est un cas particulier du service NAT. Permet de mettre en place un service Internet avec une adresse privée.
- **SNAT** : Source Network Address Translation est un autre cas particulier du service NAT.

La translation d'adresse

- Masquerading : Est un cas particulier de SNAT avec les différences suivantes :
  - Une adresse source avec l'ensemble des services associés
  - La translation d'adresse n'est effectuée que lorsque le paquet est transmis par l'interface réseau qui est associée à la nouvelle adresse source.
- Le service masquerading est spécifiquement utilisé pour cacher un réseau interne privé derrière une adresse IP officielle.

Plan

Le filtrage sous Linux : `iptables`

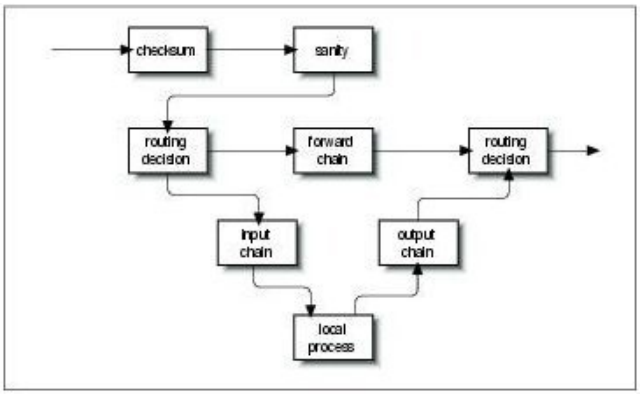


Le filtrage sous Linux : `iptables`

Comment fonctionne un routeur ?

- Le datagramme IP est reçu (1)
- Le datagramme IP est examiné pour savoir si il est destiné à la machine locale
- Si il est destiné à la mlachine locale, il est traité localement (2)
- Sinon, la table de routage est interrogée pour déterminer la bonne route et le datagramme est renvoyé ou supprimé si aucun chemin n'est trouvé (3)
- Le datagramme en provenance des processus locaux est routé et envoyé vers la bonne interface (4)
- Le datagramme prêt à l'envoi est examiné pour savoir si sa route est bonne, et est détruit sinon
- Le datagramme est transmis (5)

Le filtrage sous Linux : `iptables`



Le filtrage sous Linux : `iptables`

- Il y a trois chaînes de règles par défaut : `INPUT`, `OUTPUT`, `FORWARD`
- La commande iptables permet de manipuler les chaînes de règles :
  - Création d'une chaîne (N)
  - Destruction d'une chaîne vide (X)
  - Fixe la politique d'une chaîne (P)
  - Liste les règles d'une chaîne (L)
  - Vide la chaîne (F)
  - Initialise les compteurs de la chaîne (Z)
- La manipulation des règles d'une chaîne
  - Ajouter une règle (A)
  - à une position précise (I)
  - Modification d'une règle (R)
  - suppression d'une règle (D)

Les spécifications de filtrage

- Source (`-s 192.168.37.0/24`), Destination (`-d 192.168.37.9`)
- Protocole (`-p TCP`)
- Le port source (`-sport 22`) ou destinataire (`-dport 80`)
- Interface en entrée (`-i eth0`)
- Fragmentation (`-f`)
- Les drapeaux du protocole TCP (`SYN, ACK,FIN,RST,URG,PSH`)
- Adresse MAC
- Limite de fréquence d'utilisation du filtre par période de temps
- L'état de la connexion

Le résultat du filtrage : cible ou saut

- `DROP` : le paquet est supprimé
- `ACCEPT` : Le paquet est accepté
- Redirection vers une autre chaîne de règles créée par l'utilisateur
- `REDIRECT` le paquet est redirigé vers la même machine sur un port différent
- `REJECT` : le paquet est supprimé, l'émetteur reçoit un message d'erreur
- `RETURN` : les règles suivantes ne sont pas utilisées, la politique par défaut est utilisée
- `QUEUE` : traitement du paquet par une application externe au noyau
- `LOG` : permet de tracer le paquet

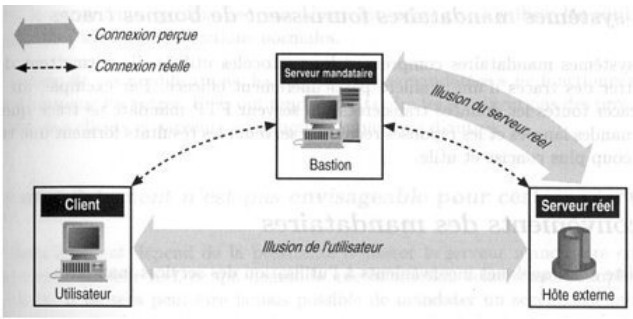
Les tables

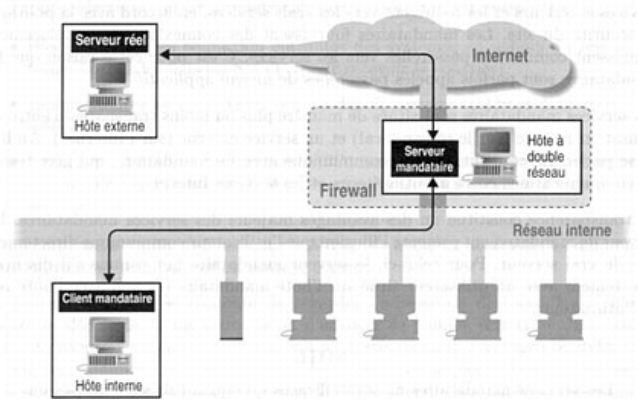
- `mangle` : table utilisée pour marquer les paquets
- `nat` : table utilisée pour faire de la translation d'adresse
- `filter` : table par défaut

La syntaxe complète d'une règle

```
iptables [-t table] commande [correspondance]
                        [cible/saut]
```


- Le mandatement donne accès à l'extérieur du réseau sans être visible de l'extérieur.
- Un serveur mandataire s'exécute sur le pare-feu
  - Il assure le mandatement de un ou plusieurs protocoles
  - Il est accessible des clients et peut communiquer avec l'extérieur
- Le client mandataire dialogue avec le serveur mandataire au lieu du serveur réel (à l'extérieur)
- Le serveur mandataire évalue la requête et décide d'y donner suite ou non
- Si le serveur mandataire autorise la requête, il la communique au serveur réel et renvoie les réponses vers le client.
- Pour l'utilisateur il n'y a aucune différence
- Pour le serveur extérieur, il dialogue avec une application qui s'exécute sur le pare-feu.

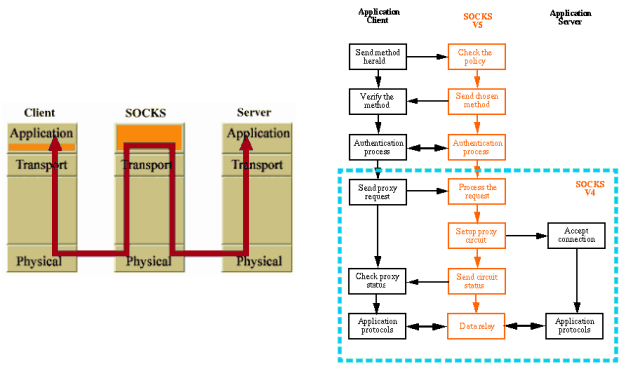




- Avantages du service de mandataire
  - Permet aux utilisateurs d'accéder directement aux services extérieurs
  - Le service mandataire fournit une trace
  - Les utilisateurs n'ont pas besoin d'être enregistrés sur le pare-feu
- Inconvénients
  - Il faut que le client soit adapté aux services mandataires
  - Le mandatement n'est pas toujours possible (application qui craint la gigue)
  - Le mandatement ne protège pas de toutes les faiblesses du protocole (HTTP peut faire exécuter des commandes à distance)
- Terminologie
  - Mandataire au niveau application (connaît les commandes échangées)
  - Mandataire au niveau circuit (`SOCK`)

Le mandatement : filtrage applicatif

Le filtrage applicatif générique



Plan

Système de détection d'intrusions

- Les systèmes de détection d'intrusions **IDS** : (*Intrusion Detection Systems*) utilisent deux principes :
  - **NIDS** (*Network Intrusion Detection System*) qui fonctionnent comme des sondes, interceptant et analysant les paquets à la volée
  - **HIDS** (*Hostbased Intrusion Detection System*) qui analysent les logs –
- Les différentes vérifications
  - Vérification de la pile protocolaire
  - Vérification des protocoles applicatifs
  - Reconnaissance des attaques par "Pattern Matching"
- Les Honeypots sont des machines leurres
  - *Paratonnerre* : protection des autres machines grâce à une machine plus attirante
  - *Canari* : machine représentative du SI mais observée de près pour déduire l'état du SI.
  - *Recherche* : observation des pirates, de leurs outils et de leurs méthodes

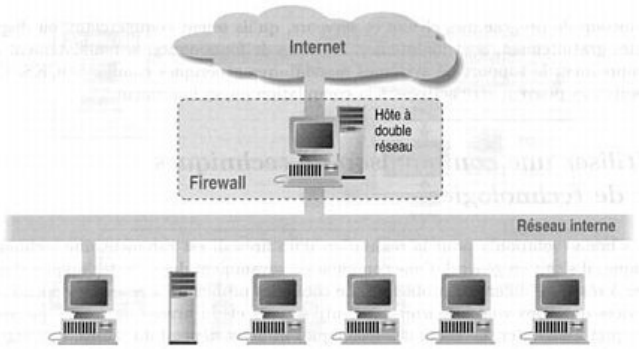
Système de détection d'intrusions

Les actions

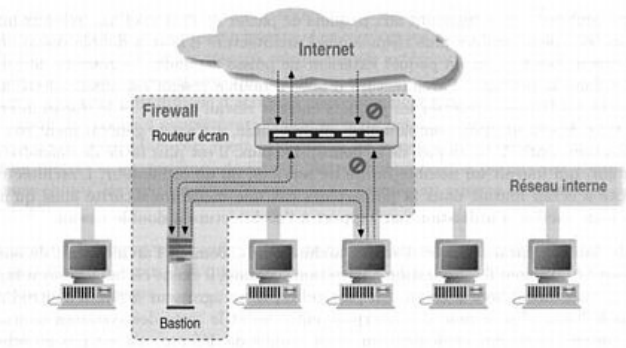
- Reconfiguration d'équipements tierces (firewall, ACL sur routeurs)
- Envoi d'une trap SNMP à un hyperviseur tierce
- Envoi d'un email à un ou plusieurs utilisateurs
- Journalisation (log) de l'attaque
- Sauvegarde des paquets suspicieux
- Démarrage d'une application
- Envoi d'un "ResetKill" (message TCP FIN)
- Notification visuelle de l'alerte

Plan

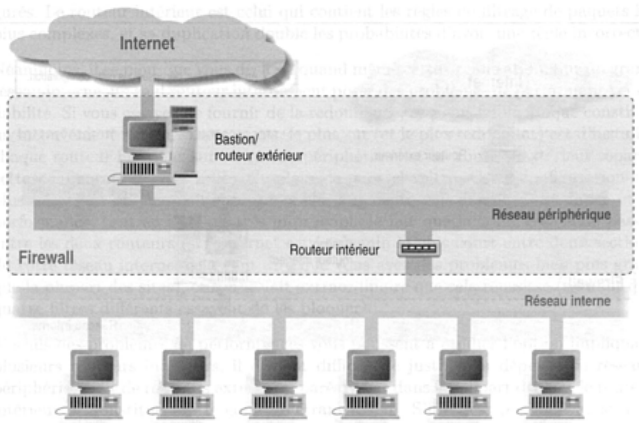
Hôte à double réseaux



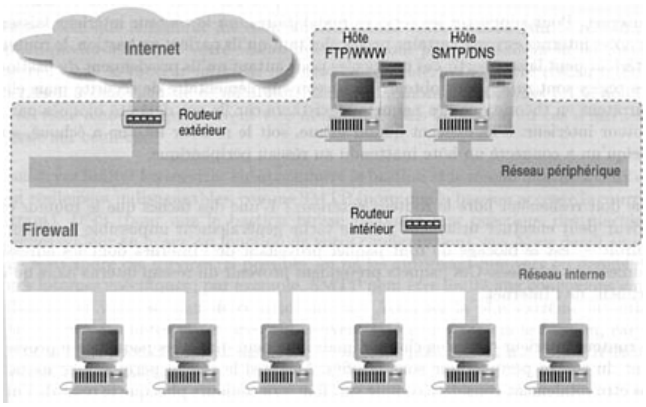
Routeur écran



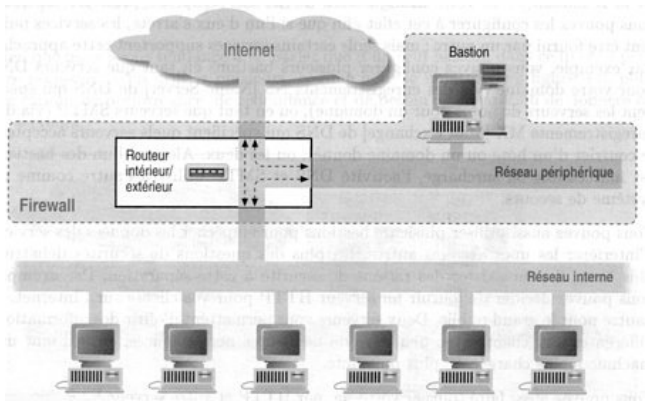
Réseau périphérique



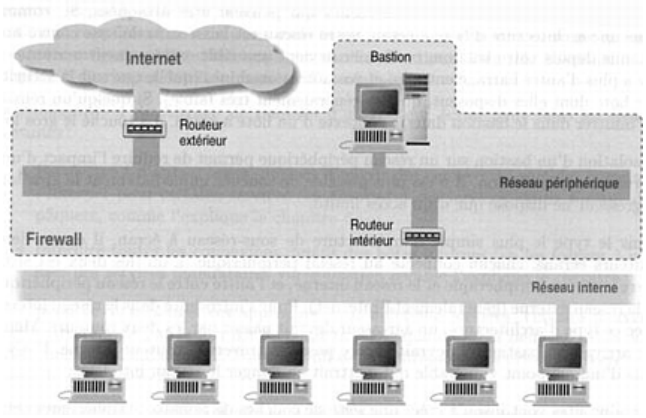
Réseau périphérique avec plusieurs bastions



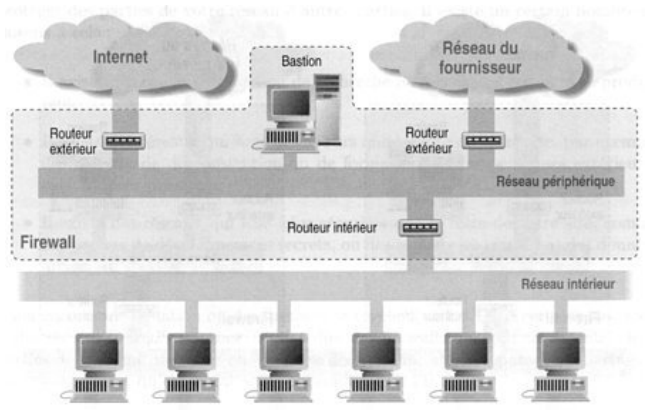
Réseau périphérique avec routeur



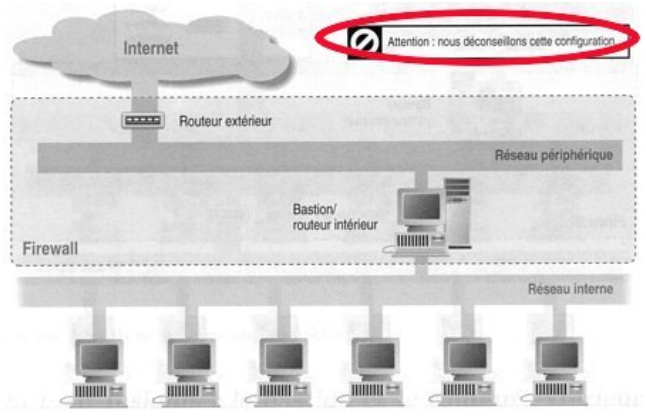
Réseau périphérique avec 2 routeurs



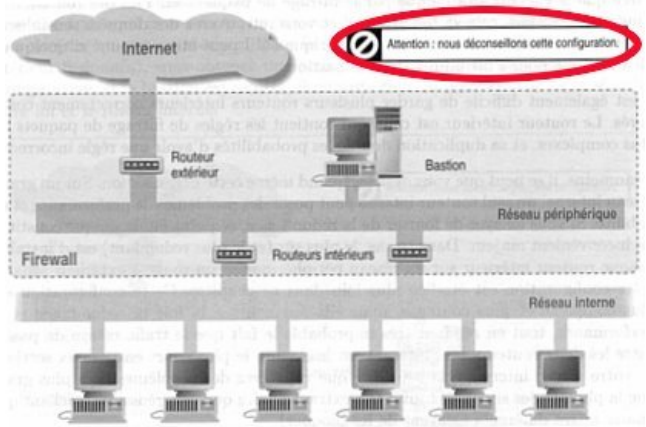
Réseau périphérique + Plusieurs réseaux



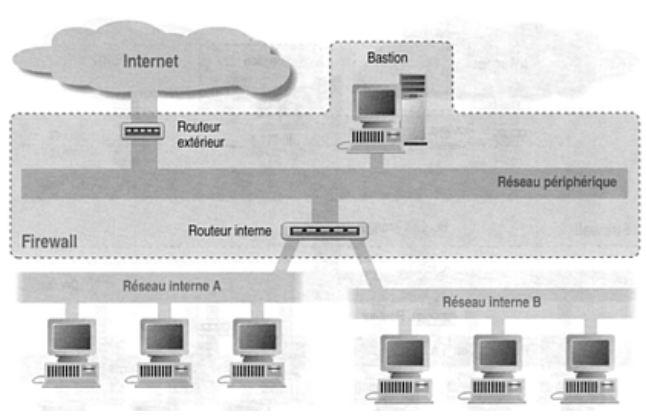
Réseau périphérique avec routeur interne



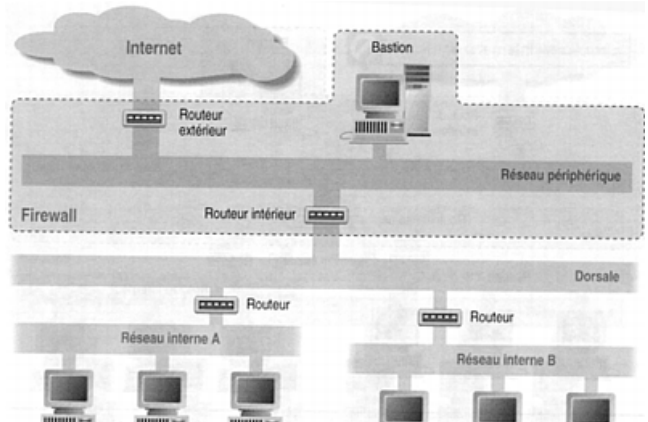
Réseau périphérique avec + routeurs internes



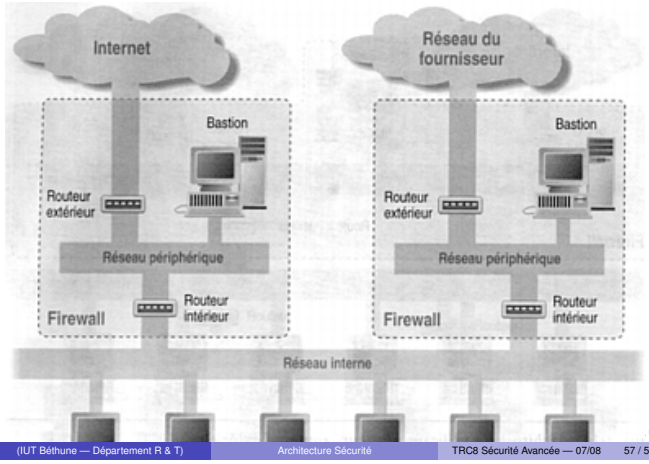
Réseau périphérique avec + réseaux internes



Réseau périphérique et dorsale



Réseau périphérique avec + réseaux externes



Réseaux internes protégés