Firewall et IDS

Cours 05

Ahmed Amou El Arby

Firewall

- Un firewall (pare-feu) original empêche la propagation d'un incendie.

- Un firewall dans un réseau doit empêcher la propagation d'une attaque, tout en permettant la circulation du trafic autorisé.

- Un pare-feu se compose d'un ou plusieurs composants.

- Un firewall est inefficace contre les attaques situées du coté intérieur

Firewall
principes de base

- Moindre privilège
- Défense en profondeur
- Goulet d’étranglement
- Interdiction par défaut
- Participation de l'utilisateur
- Simplicité

Firewall

Moindre privilège

Ne pas accorder aux utilisateurs du réseau protégé par le pare feu des droits dont il n'ont pas la nécessité

Exemple:

- Interdire le P2P dans une entreprise
- Les utilisateurs réguliers ne doivent pas être des administrateurs
- Les administrateurs doivent également utiliser des comptes utilisateurs ..etc

Firewall

Défense en profondeur

Utiliser les moyens de protection à tous les niveaux possibles, ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau.

Exemple:

- Installer des Anti virus à plusieurs niveaux.
- Sécuriser les machines même celles qui sont protégées par le pare feu
- ..etc

Firewall

Goulet d’étranglement

Toutes les communications entrant ou sortant du réseau doivent transiter par le pare feu. En effet, il ne faut pas de points d’entrée ou de sortie du réseau non contrôlés.

Exemple:
Eviter l’utilisation des modems sauvages.

Firewall

Interdiction par défaut

Interdire par défaut tout transit à travers le pare feu et ne laissé passé que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement accepté .

Pourquoi?

- Nous ne pouvons jamais savoir à l'avance toutes les menaces auxquelles nous serons exposer
- Si nous faisons une erreur, il est préférable d'interdire quelque chose d'utile que de permettre une attaque.

Firewall

Simplicité

Les règles de filtrage du pare feu doivent être les plus simples et donc les plus compréhensibles possible afin d'éviter toute erreur de la part de l'administrateur et de ses successeurs

Dans un système avec des règles de filtrage simples:

- Le risque d'erreur est plus petit
- Il est plus facile de vérifier son bon fonctionnement

Firewall

Type 1

Firewall Logiciel

- Un poste de travail standard avec un logiciel pare-feu
- **Exemple:** (IP Cop, IPTables,…etc)

Firewall matériel

- Une boîte noire spéciale (qui contient aussi un logiciel)
- **Exemple:** (CISCO PIX, CISCO IOS, Junipr,…etc)

Firewall

Logiciel VS matériel

Un pare-feu logiciel hérite toutes les vulnérabilités du système d'exploitation sur lequel ils s'éxécute

L' architectures du pare-feu logiciel est connu, donc c'est plus facile à exploiter ses vulnérabilités (exemple : buffer overflow)

Firewall

Type 2

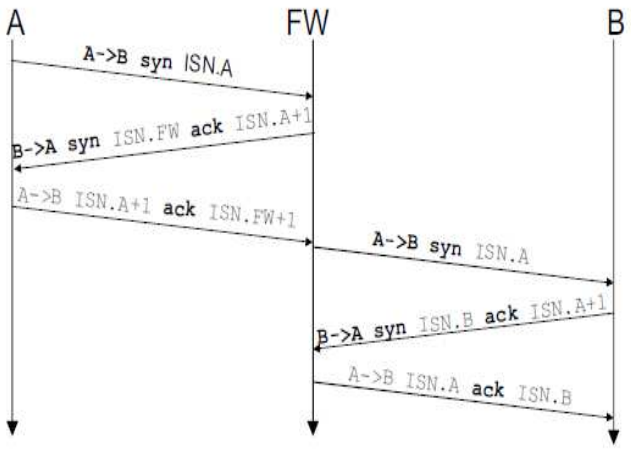
Firewall sans mémoire

- Ne se souvient pas des paquets qu'il a déjà vu

Firewall avec mémoire

- Garde une trace des paquets qui passent par lui.
- Reconstruit l’état de chaque connexion

Firewall avec mémoire
VS SYN Flooding



Firewall

Filtrage

Le filtrage permet de limiter le trafic au services utiles.

Plusieurs types de filtrage:

- Filtrage par : IP source ou destination
- Filtrage par : Protocoles (TCP, UDP, ICMP,…etc)
- Filtrage par : Flags et options (ACK, SYN,…etc)
- Filtres Applicatifs (proxy HTTP, FTP, SMTP,…etc)

Firewall

Translation d’adresses NAT

- Les adresses IP publiques sont rares

- Au lieu de réserver les 256 adresses pour 100 stations de travail, on peut cacher ces 100 stations de travail derrière une seule adresse.

- Pour ce la, l'IEFT a réservé trois plages d'adresses non routable sur internet:

10.0.0.0	-10.255.255.255
172.16.0.0	-172.31.255.255
192.168.0.0	-192.168.255.255

Translation d’adresses NAT
(Avantages et inconvénients du NAT)

Avatages:

- Cache la structure interne du réseau
- Offre une Protection automatique
- Moins d'adresses publiques, donc des coûts limités (NAT Dynamique)
- Facile de réorganiser le réseau interne

Inconvénients

- Certains protocoles ne Permettent pas des modifications de paquet

Firewall
Authentification

- Le FW peut demander l'authentification avant d'établir une connexion

- **De l'intérieur vers internet**: limiter l'accès a Internet seulement aux utilisateurs privilégiés

- **De internet vers l'intérieur** : pour autoriser l'accès aux ressources internes pour les employés qui voyagent

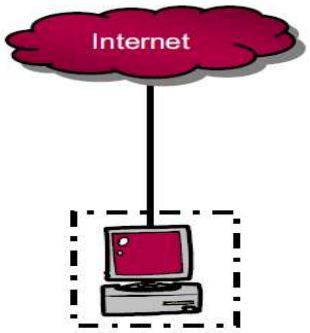
- L'authentification peut être basée sur une base de données locale ou une base de données centrale

Firewall
Autres fonctions

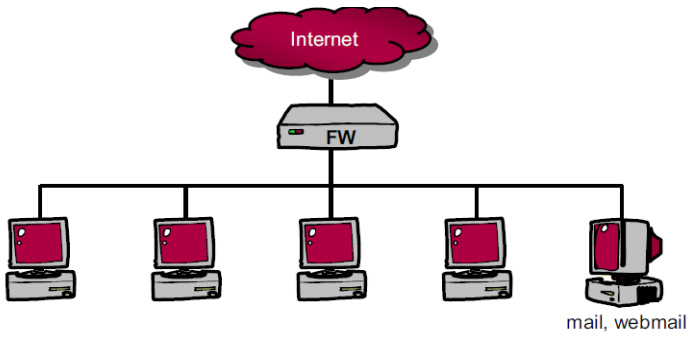
- Accès de réseau à distance (VPN)
- Chiffrement
- Analyse de paquet
- Journalisation

Exemple d’architectures des Firewalls

Firewall Personnel

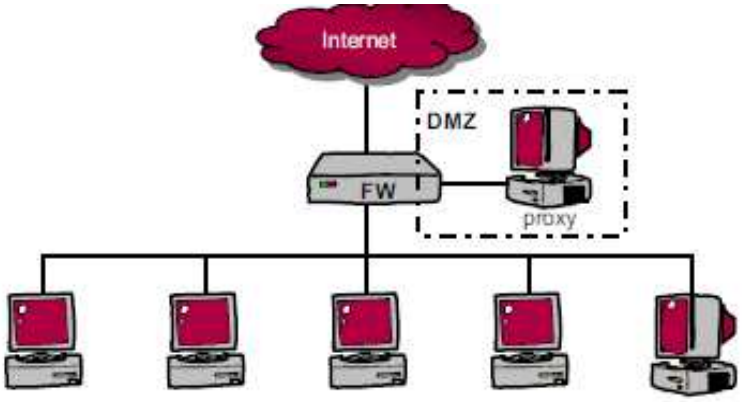


Firewall
NAT+ Filtrage

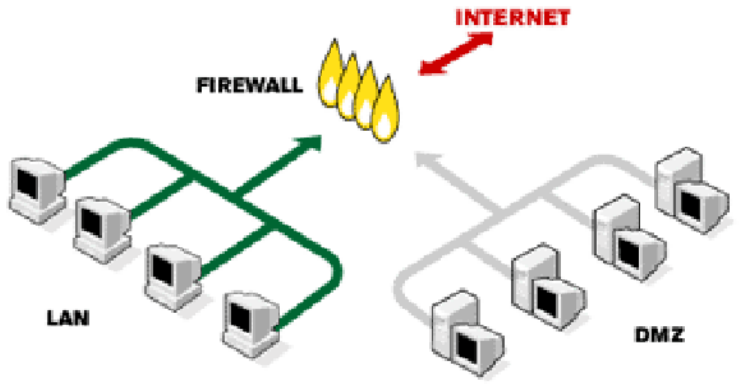


Firewall

Zone demilitarize (DMZ)



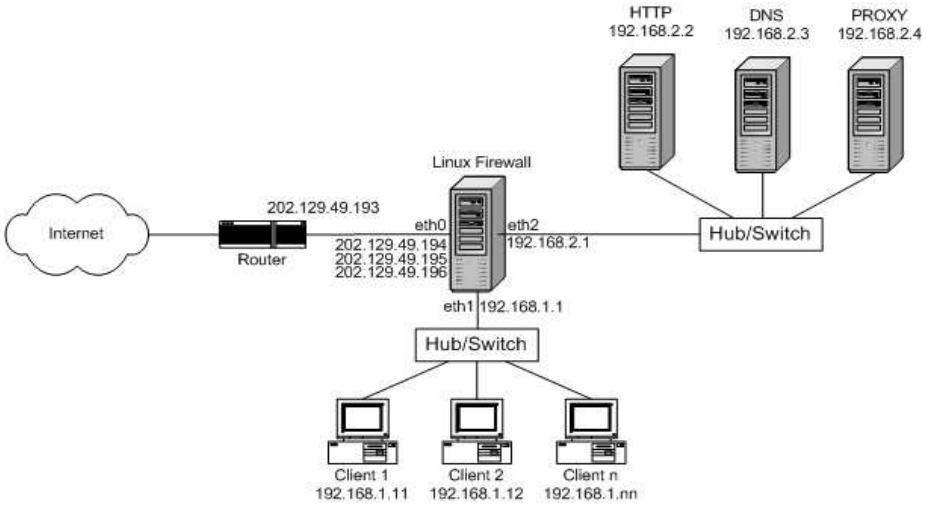
DMZ (Zone démilitarisé)



DMZ (Zone démilitarisé)

Dans certains sites on place les serveurs liés aux services Internet dans une « zone démilitarisée » (DMZ), les accès en provenance d'Internet ne peuvent voir que ces machines et les utilisateurs de l'entreprise doivent passer par les machines de la DMZ pour accéder à Internet.

DMZ (Zone démilitarisé exemple)



Firewall
Tableau: Règles de filtrage

	src	port	dst	port	protocol	action
1	any	any	128.12.1.2	25	TCP	permit
2	128.12.1.2	25	any	any	TCP	permit
3	128.12.1.2	any	any	25	TCP	permit
4	any	25	128.12.1.2	any	TCP	permit
5	any	any	any	any	TCP	deny

Les proxies

- Relai entre deux entités
- Analyse le contenu des données de l'application
- Dédié à une application
  - proxy http
  - proxy ftp
  - ...

- Il faut spécifier au niveau de l'application l'existence du proxy
- Complètement transparent à l'utilisateur

Les proxies

- Permet de faire du cache
- Permet d'effectuer certains filtres
  - Suivant les comptes utilisateurs pour FTP par exemple
  - Suivant les adresses sources...
  - Contenu des pages WEB ...
  - Détection de virus
- Permet de faire des statistiques
- Reverse-proxy

Les proxies

- Proxy HTTP
- Proxy FTP
- Proxy HTTP
- Proxy DNS
- Proxy SOCKS
- Proxy HTTPS

- Proxy Inverse

Systèmes de détection d'intrusion (IDS)

IDS

Un IDS est un ensemble de composants logiciels et matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction volontaire ou non dans un système d'information ainsi que toute altération de ces données

IPS: Système de Prévention d'intrusions

Un système de prévention d'intrusion est un ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein du système

Systèmes de détection d'intrusion (IDS)

- **Principe** : Détection d'une intrusion sur le réseau (NIDS) ou sur une machine (IDS).
- **Deux type de Système** : Comportementale et par scénarios.
- Utilisent des sniffers (outils pour 'écouter' le réseau)
- **Exemples d'IDS** : SNORT, PRELUDE-IDS

L’approche par scénario

- Cette approche consiste à détecter une intrusion en fonction du comportement actuel de l’utilisateur et non de ses actions passées.

- L’approche s’appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques

L’approche comportementale

- L’approche consiste à détecter une intrusion en fonction du comportement passé de l’utilisateur

- **Principe** : dresser un profil utilisateur établi selon ses habitudes et déclencher une alerte lorsqu’un événement hors profil se produit

Résumer des Fonctionnalités actuelles d' un firewall

- Filtrage sur adresses IP/Protocole,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif
  - HTTP (restriction des URL accessibles),
  - Anti Spam
  - Antivirus, Anti-Logiciel malveillant

Fonctionnalités actuelles d' un firewall

- Translation d'adresses (NAT),
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveur Web pour offrir une interface de configuration agréable.
- Relai applicatif (proxy),
- Détection d'intrusion (IDS)
- Prévention d'intrusion (IPS)