Firewall – IDS – Architecture sécurisée d'un réseau

- Assurer le contrôle des connexions au réseau

Sommaire général

Mise en oeuvre d'une politique de sécurité à travers :

- **Pare-feu (Firewall)**
- **Système de Détection d'intrusion (IDS)**
- **Architecture sécurisée d'un réseau**

Pare-feu – Sommaire

Définition

Définition

Un **pare-feu (ou firewall)** : ensemble matériel et/ou logiciel qui

- **met en oeuvre la politique de sécurité** du réseau : quels sont les types de communication autorisés ou interdits ?
- **concentre l'administration de la sécurité en des points d'accès limités**
- **crée un périmètre de sécurité** entre le réseau intranet de l'entreprise et le réseau internet

L'analyse du trafic est opéré à l'aide de **règles** aussi appelées *ACL* (*Access Control List* poru les pare-feu Cisco), politique ou *policy* (pare-feu Juniper/Netscreen), filtres...

Fonctions principales d'un pare-feu

- **Filtrage de paquets** hors contexte et avec le contexte de sessions,
- **Translation** statique/dynamique d'adresses IP (NAT), translation de ports (PAT)
- **Journalisation** des évènements

NAT et PAT

Translation statique/dynamique d'adresses IP (NAT) et translation de ports (PAT)

- ☺ Gestion d'un petit parc d'adresses IP sur internet
- ☺ Masquage (*masquerading*) du plan d'adressage interne

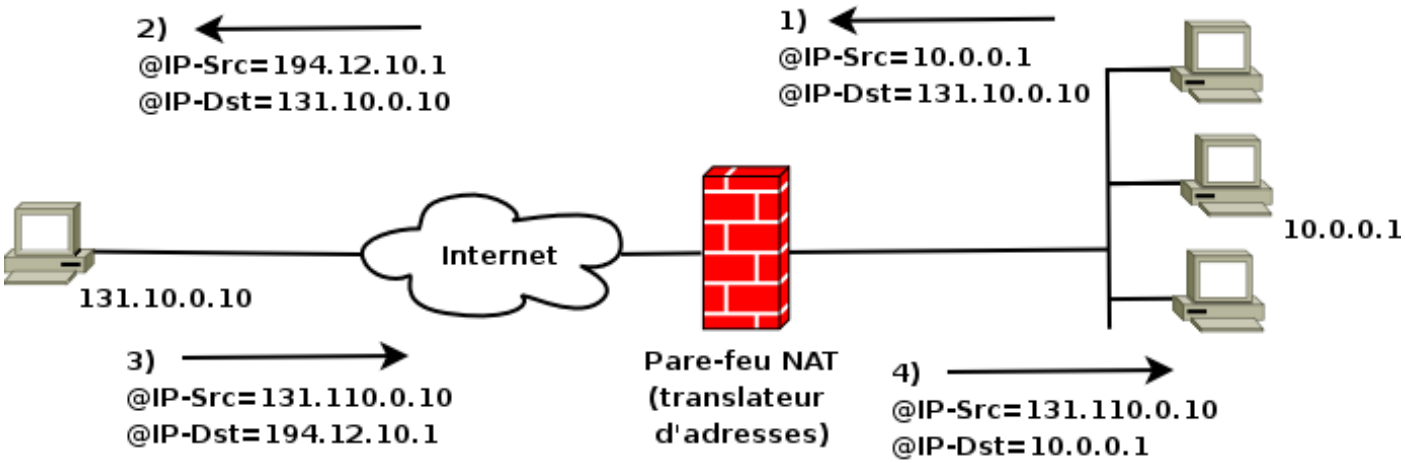
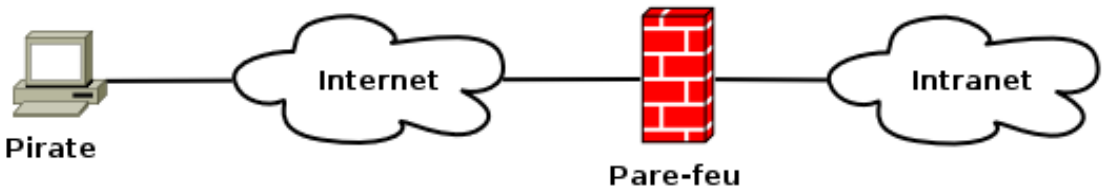


Table de translation statique

@IP locales internes	@IP globales internes
10.0.0.1	194.12.10.1
10.0.0.2	194.12.10.2

Catégories de filtres de pare-feu



On distingue différentes catégories de pare-feu selon :

- son niveau dans le *modèle OSI* (Réseau, Transport, Applicatif),
- sa sensibilité au contexte d'un échange (session),
- ses possibilités *d'identification* de l'utilisateur,
- le *périmètre* qu'il couvre (un réseau ou une machine hôte),
- ...

D'abord les catégories principales, puis les catégorie secondaires (plus un désir de structurer la présentation qu'une réalité)

Filtrage de paquets sans états (stateless firewall)

Définition

Filtrage statique de paquets (Couche 3 ISO) selon les critères suivants :

- adresse IP source/destination, protocole encapsulé (ICMP, IP, TCP, OSPF...), numéro de ports source/destination

- ☺ Mise en oeuvre aisée à l'aide de règles simples
- ☺ Performant si règles limitées et leur enchaînement optimisé
- ☹ Statique : ne prend pas en compte les états des sessions
- ☹ Ni le filtrage des applications
- ☹ Ni l'authentification des utilisateurs

Pare-feu à états (stateful firewall)

Définition

Filtrage dynamique de paquets (Couches 3 et 4 ISO) selon :

- états des sessions TCP (*NEW, ESTABLISHED, RELATED, INVALID*), ports sources TCP/UDP, séquencement des paquets, IP, interfaces associées aux sessions en cours...

- ☺ Dynamique : prend en compte les états des sessions
- ☺ Performance bonne
- ☺ Gestion de la translation d'adresses (*NAT, Network Address Translation*) et de ports (*PAT, Port Address Translation*)
- ☹ Complexe à configurer (nombre important d'options)
- ☹ Authentification limitée à l'adresse IP
- ☹ Non prise en compte des protocoles supérieures à la couche transport (telnet, FTP, ...)

Pare-feu applicatif (proxy ou service mandataire ou relais)

Définition

Filtre applicatif (Couche 7 ISO) : chaque connexion correspond à 2 connexions : 1) utilisateur et pare-feu, 2) pare-feu et système visé
un agent agit comme relais pour chaque application (SMTP, HTTP, ...)

- ☺ Filtre les protocoles applicatifs en profondeur

  Exemple : Seules les requêtes `http get` authorisées et des sites interdits
- ☺ Service d'authentification plus puissant que l'adresse IP
- ☺ Cache le plan d'adressage interne
- ☺ Journalisation des évènements très détaillée
- ☹ Forte puissance de traitement pour ne pas impacter trafic
- ☹ Non prise en compte ni des trafic UDP, ni des protocoles applicatifs RPC (*Remote Procedure Call*)

Pare-feu identifiant

Définition

Pare-feu identifiant : identification des connexions passant à travers le filtre IP.
L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par IP, et suivre l'activité réseau par utilisateur.

Pare-feu personnel ou embarqué

Définition

Pare-feu personnel (embarqué) : notion de périmètre de sécurité réduite au système local et à ses applications (s'oppose à **pare-feu zonal**)

- ☺ catégories possibles : *stateless*, *stateful* ou *proxy*
- ☺ liberté de choisir le produit le mieux adapté à une situation
- ☺ contrôle le trafic réseau entre 2 systèmes d'un même LAN ; ce que ne permet pas un pare-feu zonal
- ☹ difficulté de désolidariser la gestion de la sécurité de celle de ses applications (le pare-feu est en soi une application)
- ☹ gestion fastidieuse même pour parc de taille moyenne

Le choix entre pare-feu zonal et pare-feu embarqué est un compromis entre ces facteurs

Recommandations

- **Tout accès externe au réseau interne est filtré** :" *tout ce qui n'est pas autorisé est interdit*"
- **La profondeur du filtrage –couches OSI réseau (3), transport (4) et application (7)– est fonction des besoins de sécurité** ; le contrôle le plus fin est au niveau applicatif
- **Tout trafic non autorisé est détruit sans donner de réponses (DROP)**
- **Tout trafic détruit est journalisé (LOG) à des fins d'investigation**

Produits du marché

- Versions libres
  - **Linux Netfilter/Iptables**, pare-feu à état, libre des noyaux Linux 2.4 et 2.6.
  - **NuFW**, Pare-feu identifiant, licence GPL pour serveur et clients Linux, FreeBSD et Mac OS. NuFW est basé sur Netfilter et en augmente les fonctionnalités.
- Versions propriétaires
  - **Cisco – PIX**, boîtier pare-feu à état
  - **Check Point – FireWall-1**, boîtier pare-feu à état
  - **Gauntlet** , proxy applicatif

Critères de choix d'un pare-feu

- **Moyens d'administration** (interface, accès distants, ...)
- **Niveau de détails des règles de filtrage**
- **Audit des règles de filtrage et des journaux** (consistance des règles, vérification des sauvegardes et de leur intégrité, ...)
- **Options pour gérer et archiver les journaux**
- **Réactions en cas de problèmes** (perte d'un lien de connexion, intégrité de la base des règles de filtrage...)
- **Interfaçage possible avec d'autres équipements de sécurité** (IDS, anti-virus, authentification d'utilisateur, ...)
- **Vulnérabilités et mise à jour des correctifs**
- **Certifications de sécurité**

Quizz de synthèse

- Quelles sont les fonctions principales d'un pare-feu ?
- Quelles différences et similitudes y a t'il entre un pare-feu zonal et un pare-feu embarqué ?

IDS – Sommaire

Définition

Définition

Un **Système de Détection d'Intrusion (IDS)** : ensemble des pratiques et des mécanismes utilisés pour détecter une erreur (incident, anomalie) pouvant conduire à la violation de la politique de sécurité
Repose sur des techniques de **Sniffing des réseaux** et de **journalisation des évènements sur les systèmes**

Pour certains l'avenir est aux Systèmes de *Prévention* d'Intrusion (IPS)

Fonctions et mode opératoire

1. **Collecte des informations**,
2. **Analyse et détection des informations récupérées**,
3. **Réponse à donner à la suite d'une intrusion décelée**

Collecte des informations

Au niveau des :

- **Machines hôtes par le biais du système d'exploitation** : identification d'objet responsable d'un évènement, du processus qui a lancé évènement, de utilisateur associé à évènement, de sa date, ...
  - ☺ efficace même si les applications sont chiffrées
  - ☹ non multiplate-forme : difficulté de déploiement de cette solution car dépendante de l'OS du système
  - ☹ programmes d'audit affectent les performances (anti-virus)
- **Réseau** (source d'informations pour la majorité des IDS)
  - n'est généralement pas un routeur, et sa localisation dépend de l'architecture du réseau
  - ☺ pas de problème de performance
  - ☺ transparent pour utilisateur interne, invisible pour extérieur
  - ☺ maintenance et coût relativement bas
  - ☹ données chiffrées
  - ☹ trafics élevés

Méthodes d'analyse et de détection des intrusions

Transformation des données en suite d'actions et *détection* fondées sur :

- **Signatures : comparaison à scénarios d'attaques déjà connus**
  - ☺ rapide, facile à implémenter, largement utilisé
  - ☺ faible nombre de fausses alarmes
  - ☹ nécessité de mise à jour régulière
  - ☹ inefficace pour contrer des attaques inconnues
- **Profils : comparaison à profils de comportements normaux** associés à un utilisateur ou une application
  - ☺ pas besoin de maintenance et aucune connaissance antérieure des attaques requises
  - ☹ nombre important de *faux positifs* (alarme sans préjudice)
  - ☹ phase d'apprentissage indispensable dans un environnement stable et non hostile : difficulté de mise en place dans un environnement dynamique (utilisateurs nomades, changements fréquents des applications)

Réponses aux intrusions détectées

- **Réponses actives (automatiques) : impliquent une action à entreprendre suite à une détection**
  - **agresser l'intrus** (traquer, localiser, contre-attaquer et endommager) : illégale mais peut être un dernier recours
  - **restructurer le réseau** (isoler et modifier le système attaqué) : solution la plus répandue et la plus efficace pour stopper la propagation de l'attaque
  - **surveiller le système attaqué** (collecte de plus amples informations : faille exploitée, finalité, identité de l'intrus...) : facilite une poursuite en justice
- **Réponses passives : présentent toutes les informations récoltées à l'administrateur, qui entreprend ensuite des mesures qui lui semble pertinentes**

Attaques contre les IDS

- Essentiellement les **dénis de service** : pour pénétrer un système, effacer des traces en inondant les ressources de l'IDS

Quizz de synthèse

- Quelles sont les différentes phases de traitement d'un IDS ?
- A quel niveau la collecte d'informations peut être réalisée par un IDS ? Donner avantage et un inconvénient pour chacun.

Architecture sécurisé – Sommaire

Mise en place d'une architecture sécurisée

De nombreuses solutions en fonction de :

- **de la politique de sécurité à mettre en oeuvre**,
- **du systèmes d'information à représenter**,
- **des services à assurer**,
- **et des possibilités techniques et financières**

Questions techniques à se poser

- **Quels équipements (boîtiers ou machines serveurs) accompliront les fonctions de** routage ? de firewall ? de serveurs ?
  - un boîtier est plus fiable qu'une machine serveur
- **Quels systèmes d'exploitation et puissance** pour les machines ?
  - les OS windows sont plus vulnérables qu'un OS Linux
  - puissance peut être requise pour un serveur web mais peut être aussi un challenge pour un pirate
- **Quels regroupements de services ou de fonctions** sur un boîtier ou une machine serveur ?
  - une machine à la fois routeur et serveur représente une serieuse faille si compromise
- **Où positionner les différents équipements** entre eux et par rapport à l'internet ?

Principe

Principe

Diviser et diversifier pour régner

Diviser

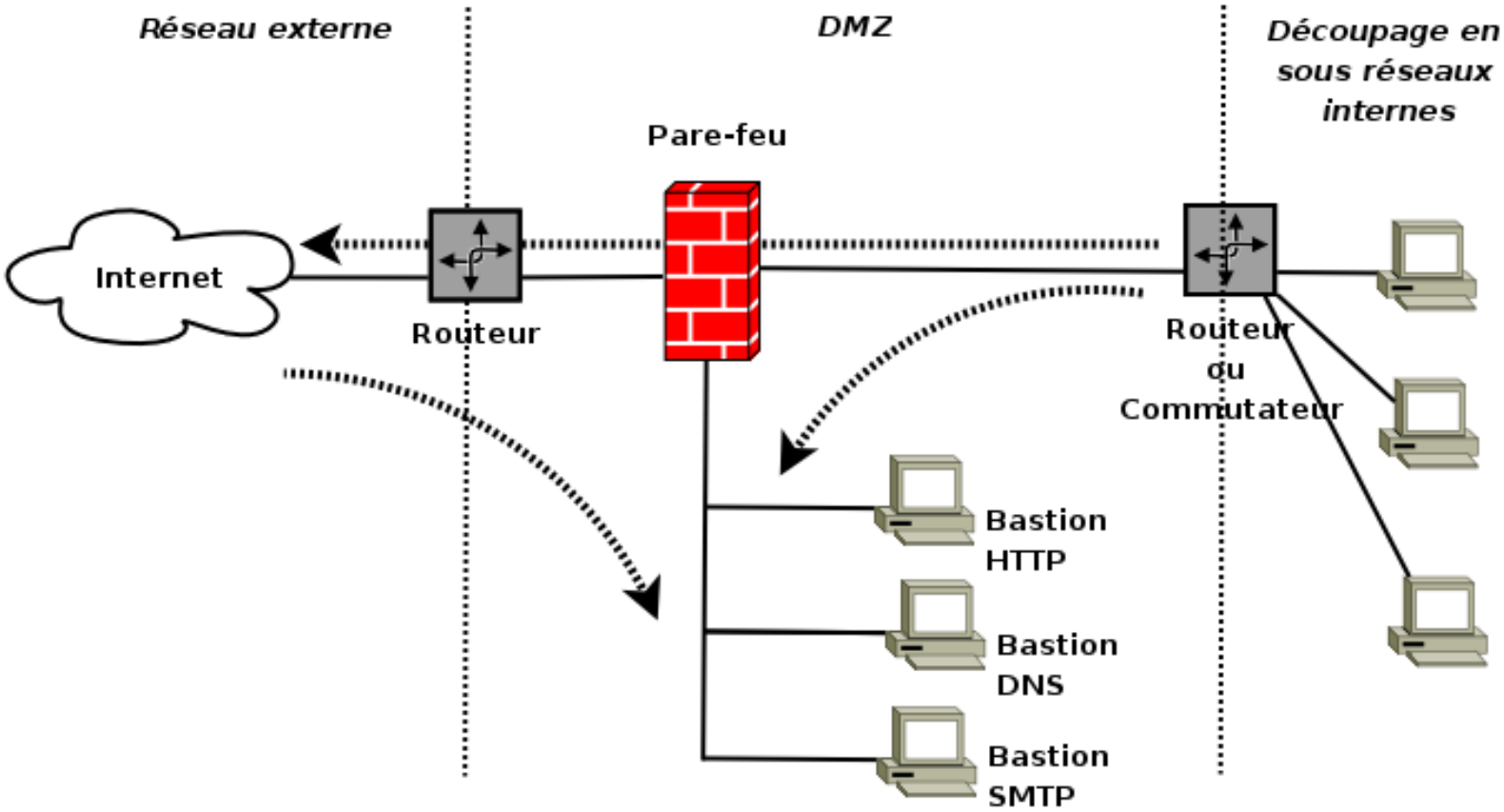
- Distribuer les services sur des machines distinctes
- Découper le réseau en sous-réseau (routeur ou commutateur-VLAN)
- Partager en plusieurs zones de sécurité

Diversifier

- Les systèmes d'exploitation, les équipements, les marques des logiciels et matériels

Même si une machine ou une partie du réseau venait à être compromise, l'accès aux parties restantes requerra d'autres connaissances pour les compromettre

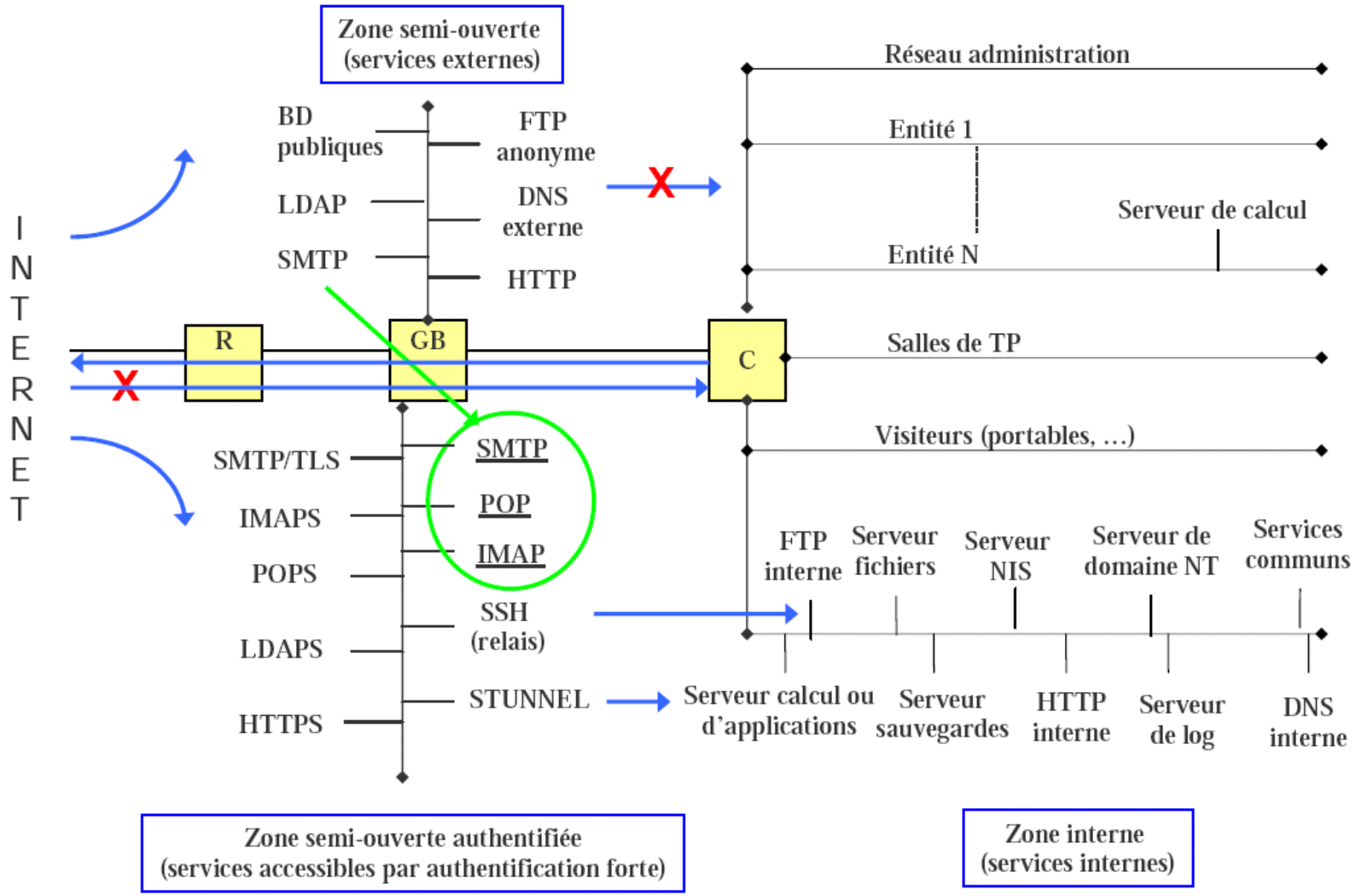
Configuration type



Les éléments d'un réseau

- **Pare-feu** (sans état, à état, proxy), par la suite GB pour Garde-Barrière
- **IDS**,
- **Bastion** : "avancée qui sert de premiers remparts", serveur (HTTP, DNS et/ou SMTP...) point d'entrée/sortie à internet
- **Routeur écran** (*screening router*) : filtrage sans état et à état et fonction de séparation de flux entre les réseaux
- **Commutateur** : séparation de flux entre les réseaux (Virtual Lan ou VLAN)
- **DMZ** (zone démilitarisée ou zone semi-ouverte) : sous-réseau isolé par deux pare-feux.
  Contient des machines bastions situées entre un réseau interne et un réseau externe (Internet)
  La DMZ permet à ces machines d'accéder à Internet et/ou de publier des services sur Internet sous le controle du pare-feu externe.
- **Pot de miel** (*Honeypot*) : système ou serveur volontairement vulnérable destiné à attirer et à piéger les pirates

Un exemple de déploiement



Quizz de synthèse

- Rappeler et expliquer le principe de base de la mise en place d'une architecture sécurisée ?
- Rappelez les fonctions du routeur écran ?