INF4420: Éléments de Sécurité Informatique

Exercices : Sécurité des réseaux - Partie 3

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité réseau

- Exercice 1 : Positionner un système de détection d'intrusion dans une architecture réseau

- Objectif :
  - Comprendre les flux dans une architecture réseau
  - Savoir positionner un système de détection d'intrusion en fonction du scénario considéré

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

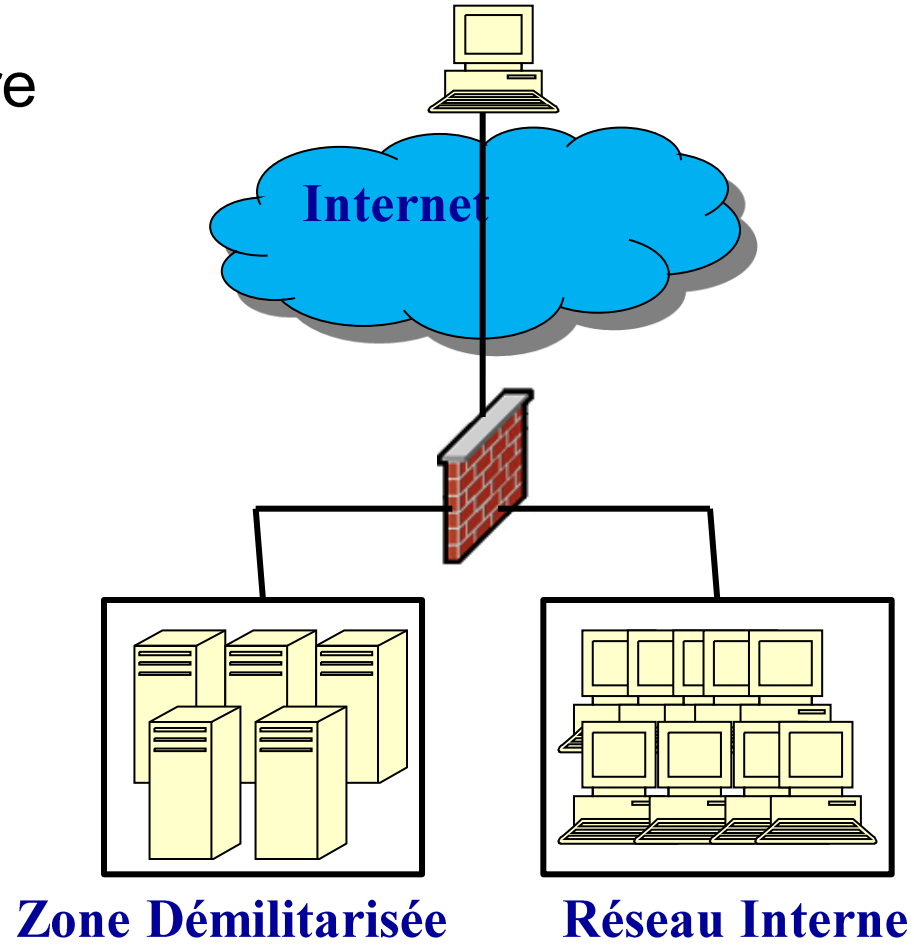
Exercices de sécurité réseau

- Exercice 1 : Positionner un système de détection d'intrusion dans une architecture réseau

- Vous avez présenté votre projet d'architecture réseau
- Le projet a été accepté par votre direction
- Vous décidez maintenant de renforcer la sécurité de votre système en intégrant un système de détection d'intrusion
- Vous considérez plusieurs scénarios

Exercices de sécurité réseau

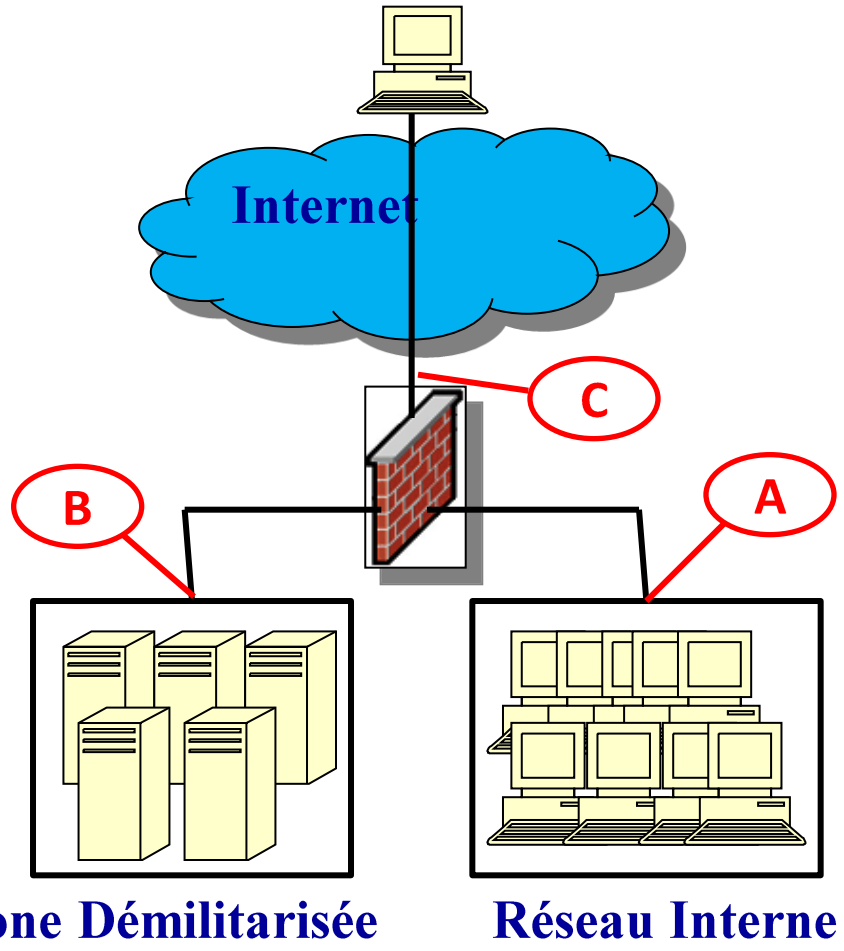
- Version simplifiée de votre architecture de sécurité



Exercices de sécurité réseau

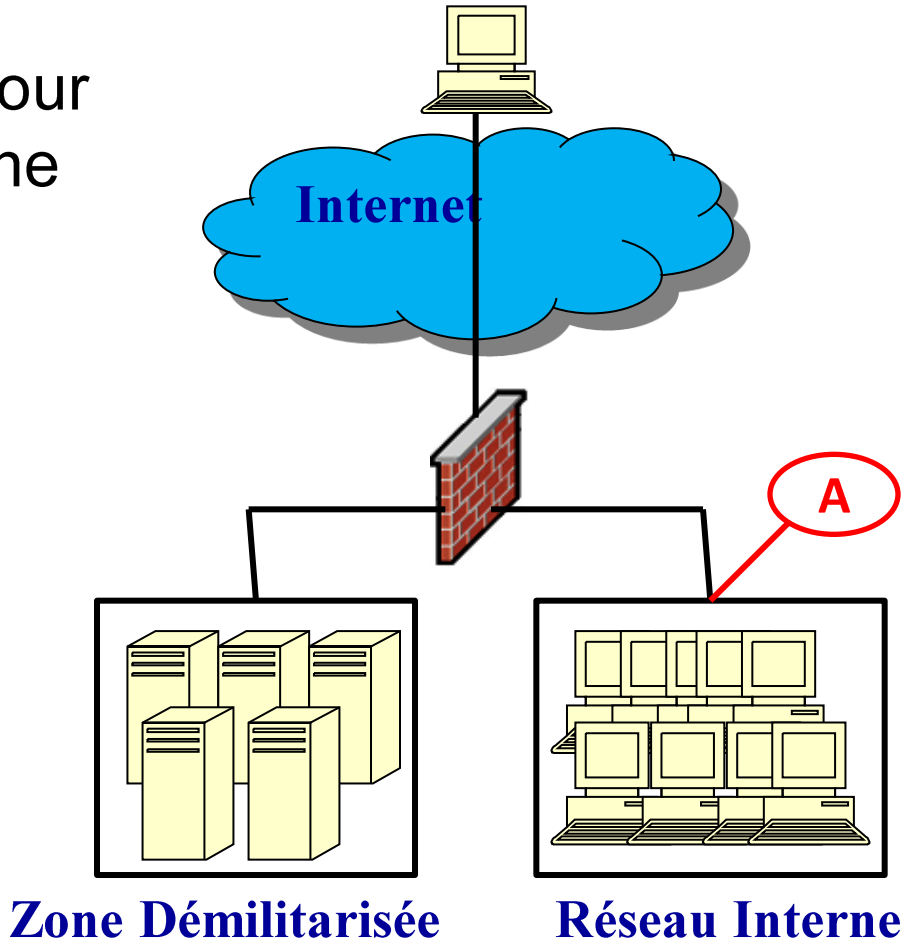
- Scénario 1 : Vous voulez détecter les attaques d'employés mécontents

- Question 1 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

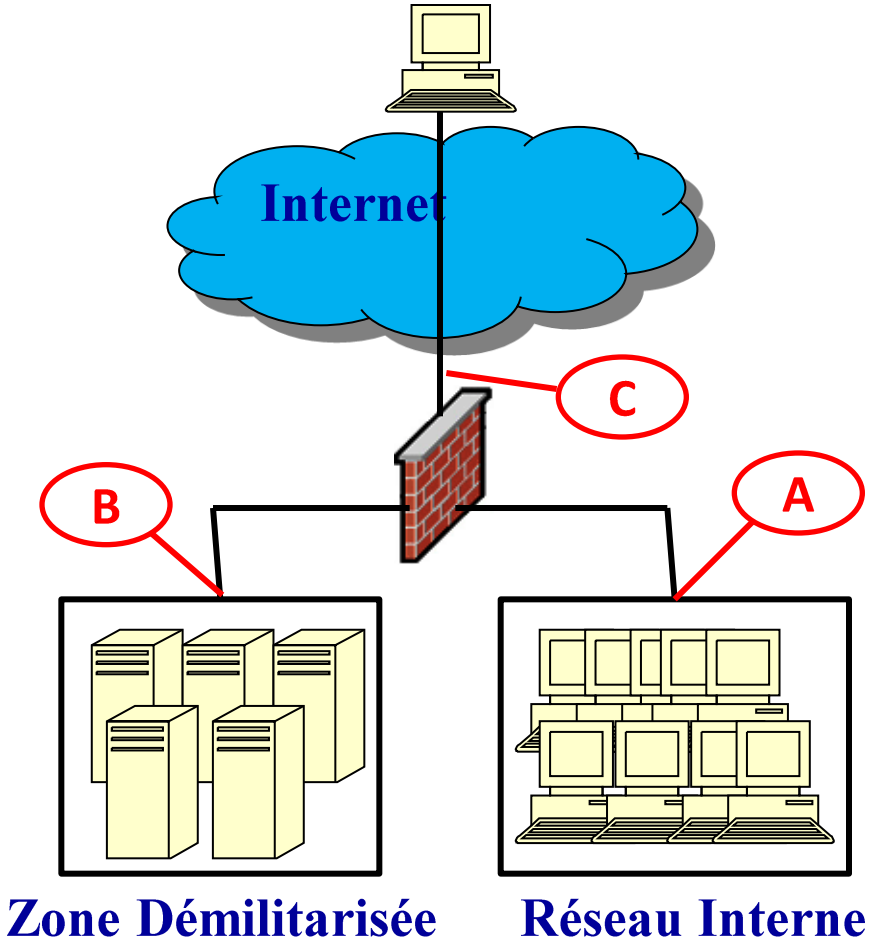
- Réponse question 1 : A, pour intercepter le réseau interne



Exercices de sécurité réseau

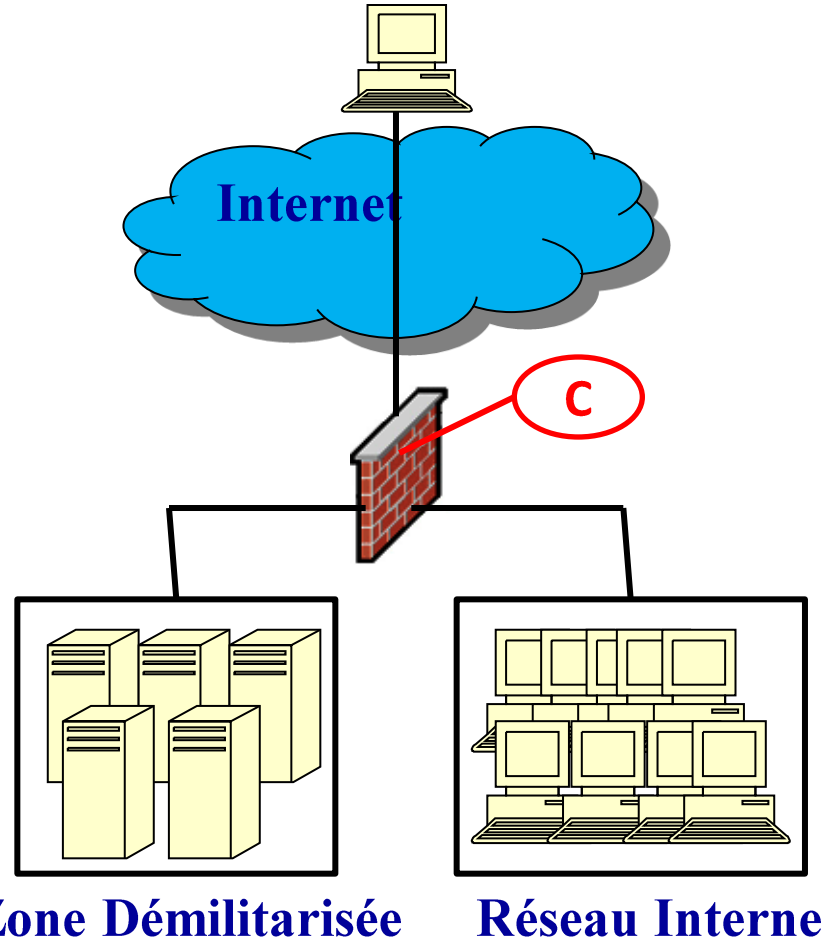
- Scénario 2 : Vous voulez obtenir de l'information sur le type d'attaque qui vous cible

- Question 2 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

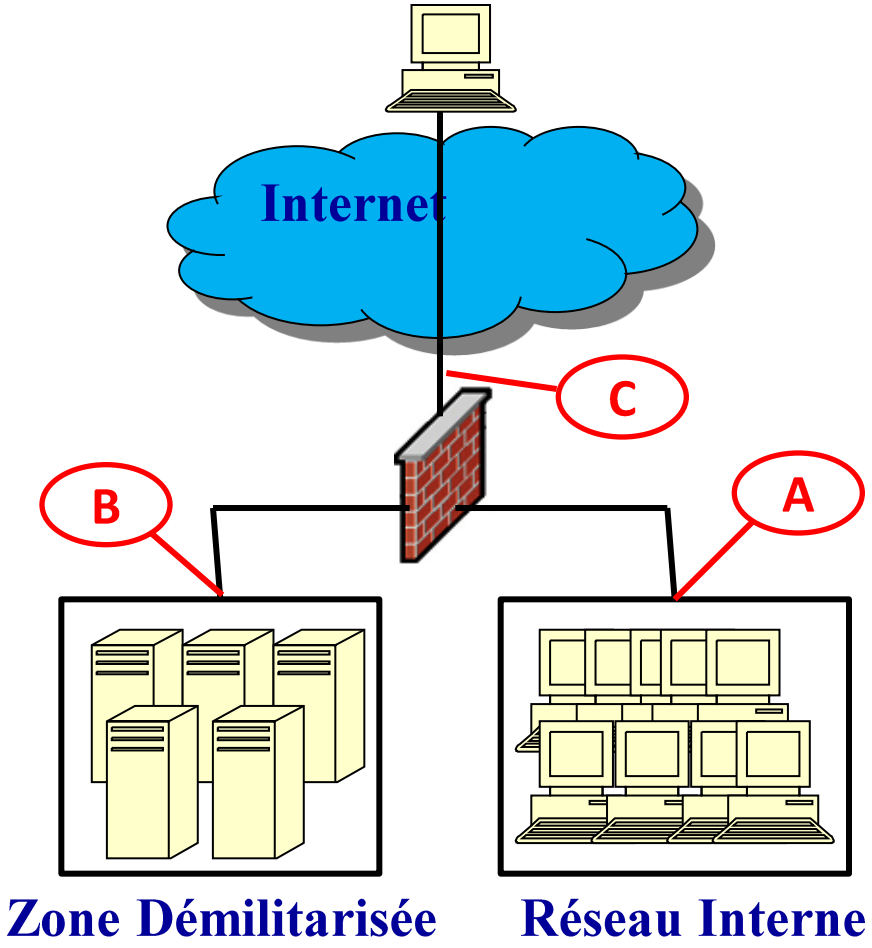
- Réponse question 2 : C, pour intercepter toutes les attaques venant d'Internet



Exercices de sécurité réseau

- Scénario 3 : Vous voulez détecter les attaques de type cheval de Troie

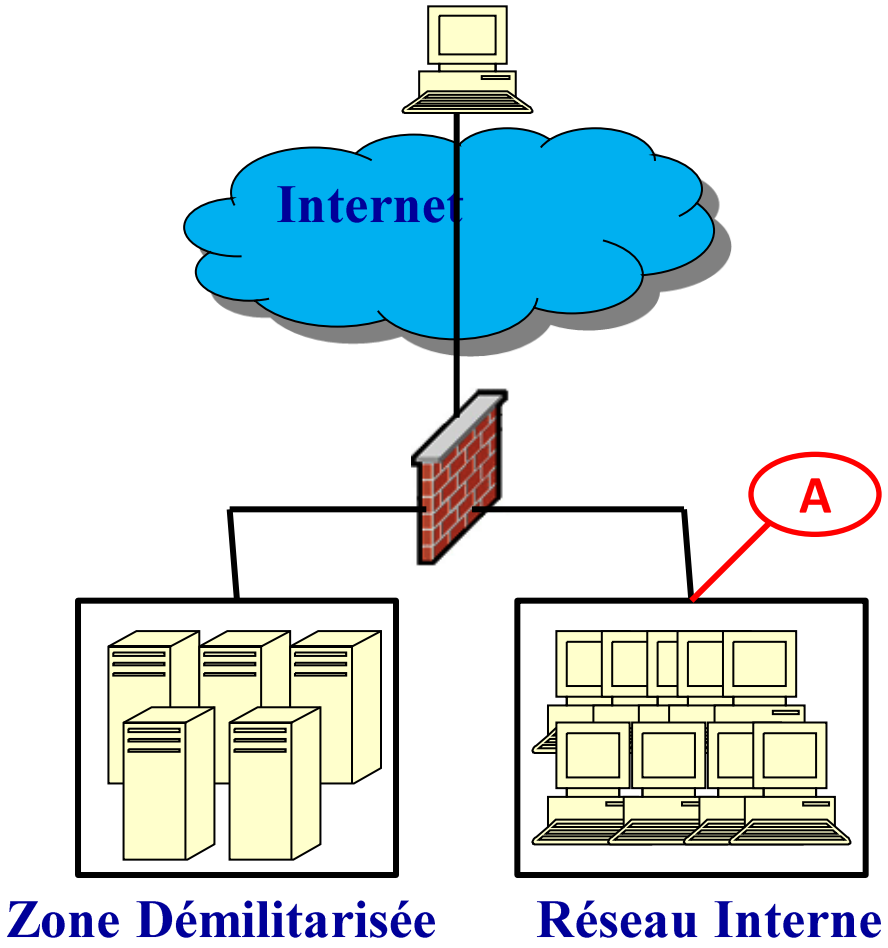
- Question 3 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

- Réponse question 3 : A, pour intercepter le réseau interne

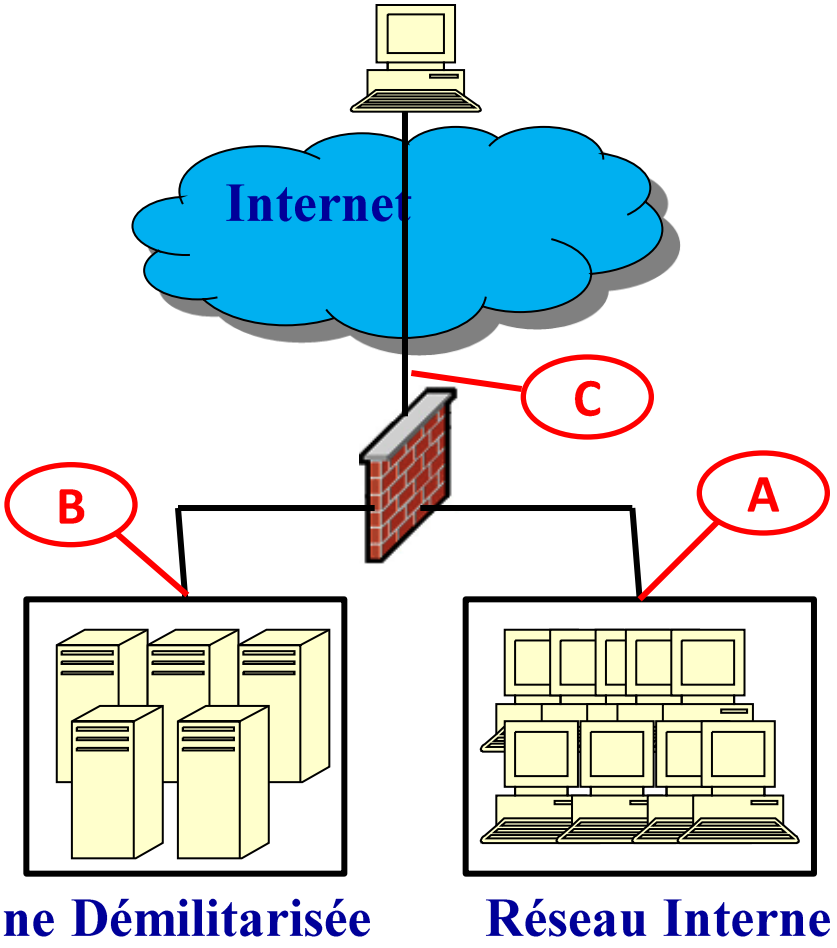
- Convient pour détecter si une machine du réseau interne a été corrompue



Exercices de sécurité réseau

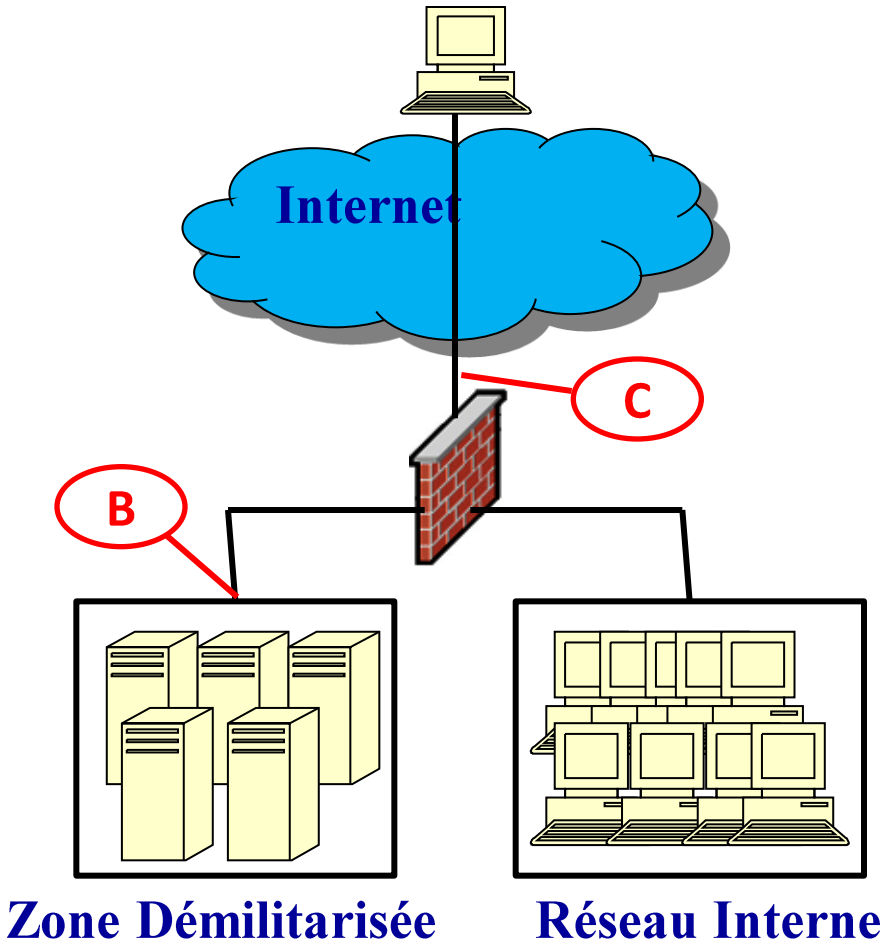
- Scénario 4 : Vous voulez obtenir de l'information sur le type d'attaque qui pénètre votre pare-feu

- Question 4 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

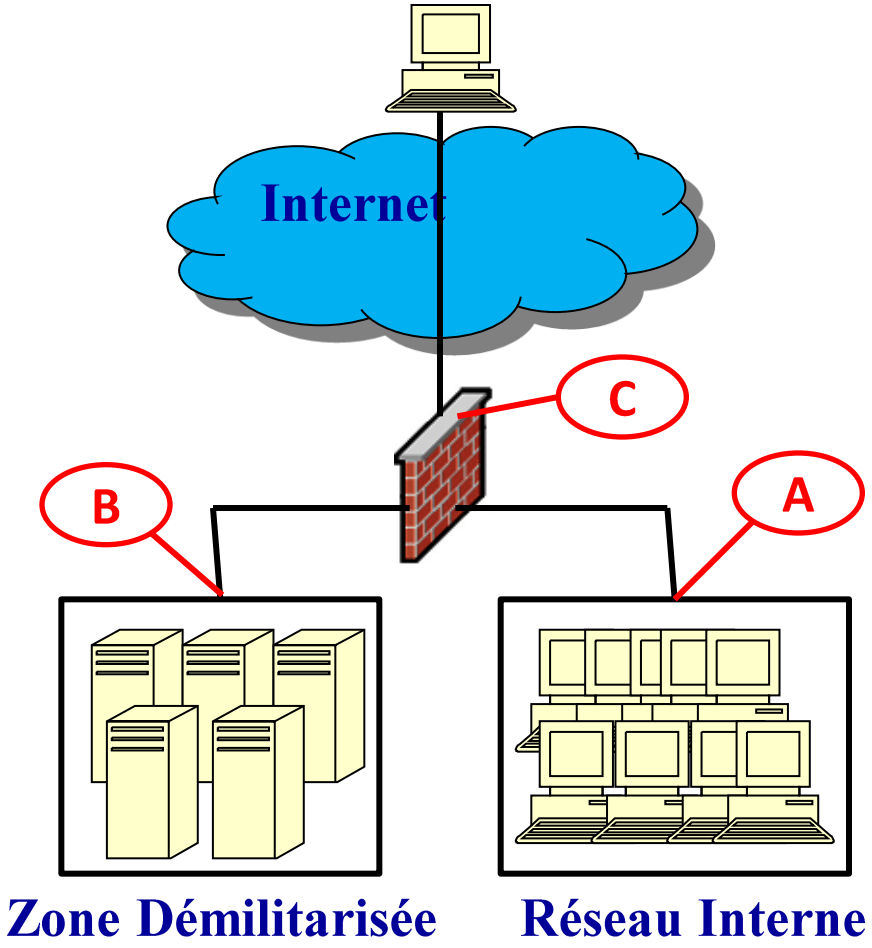
- Réponse question 4 : B (ou A) et C, pour voir la différence entre les alarmes externes et internes



Exercices de sécurité réseau

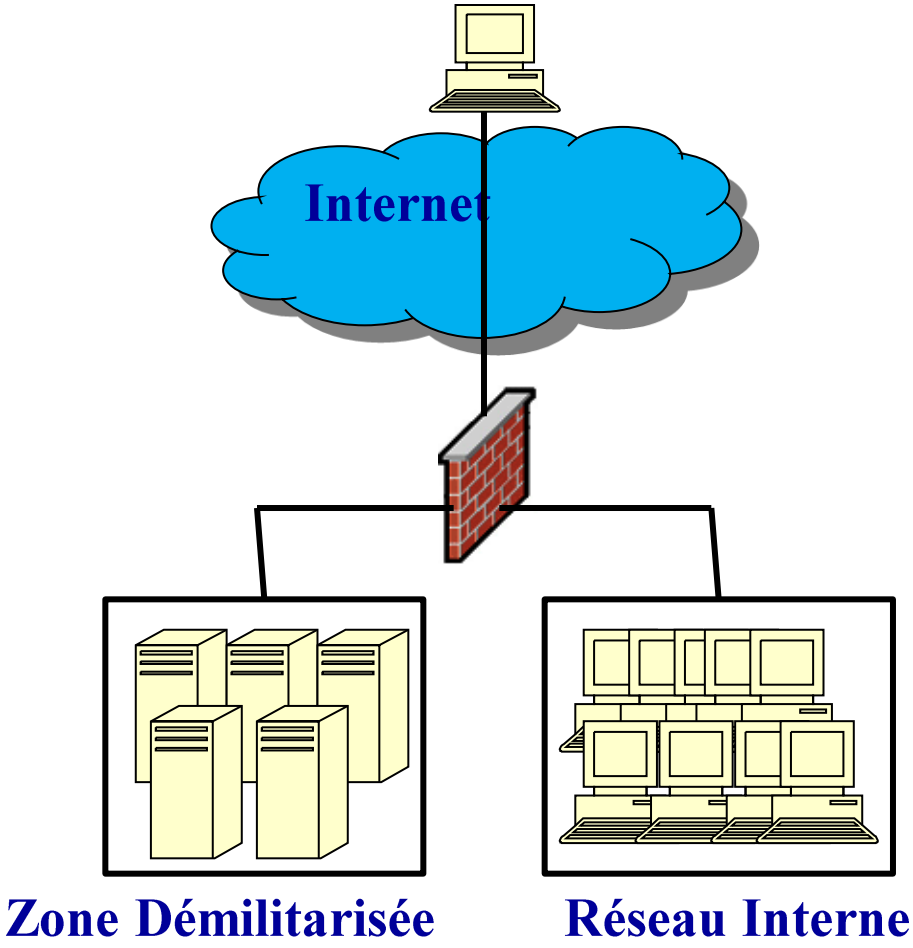
- Scénario 5 : Vous voulez détecter les attaques sur votre serveur Web (VPN SSL)

- Question 5 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

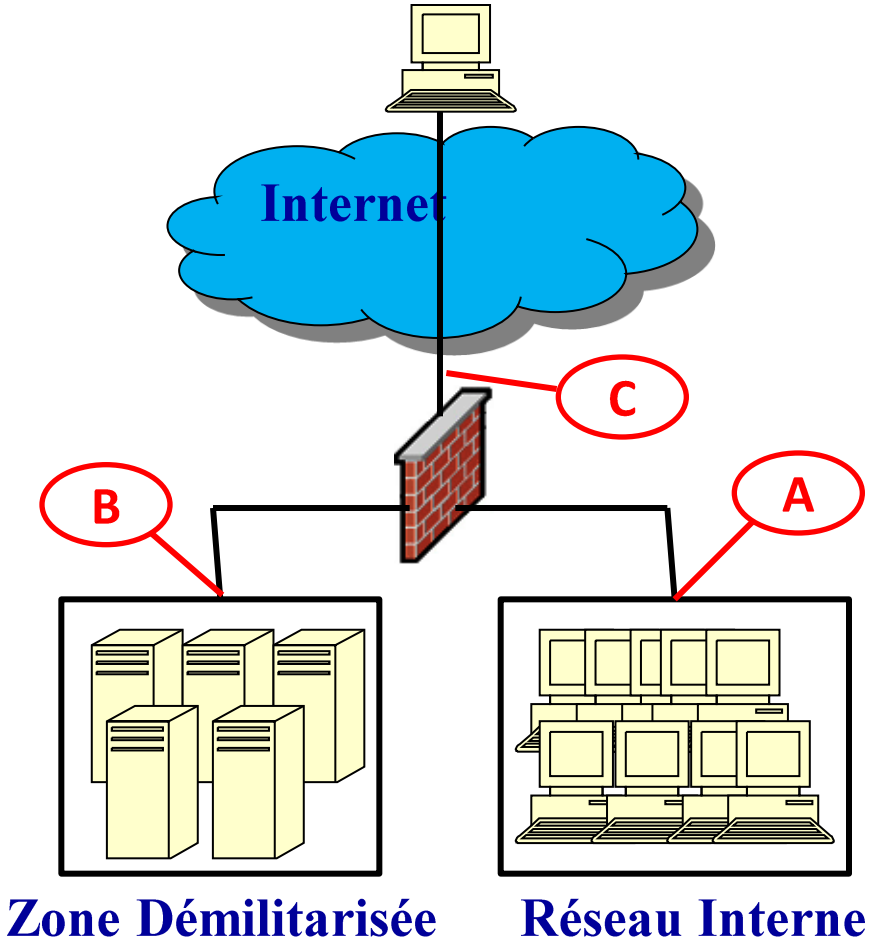
- Réponse question 5 : IDS hôte sur le serveur, le trafic SSL est chiffré jusqu'au serveur !



Exercices de sécurité réseau

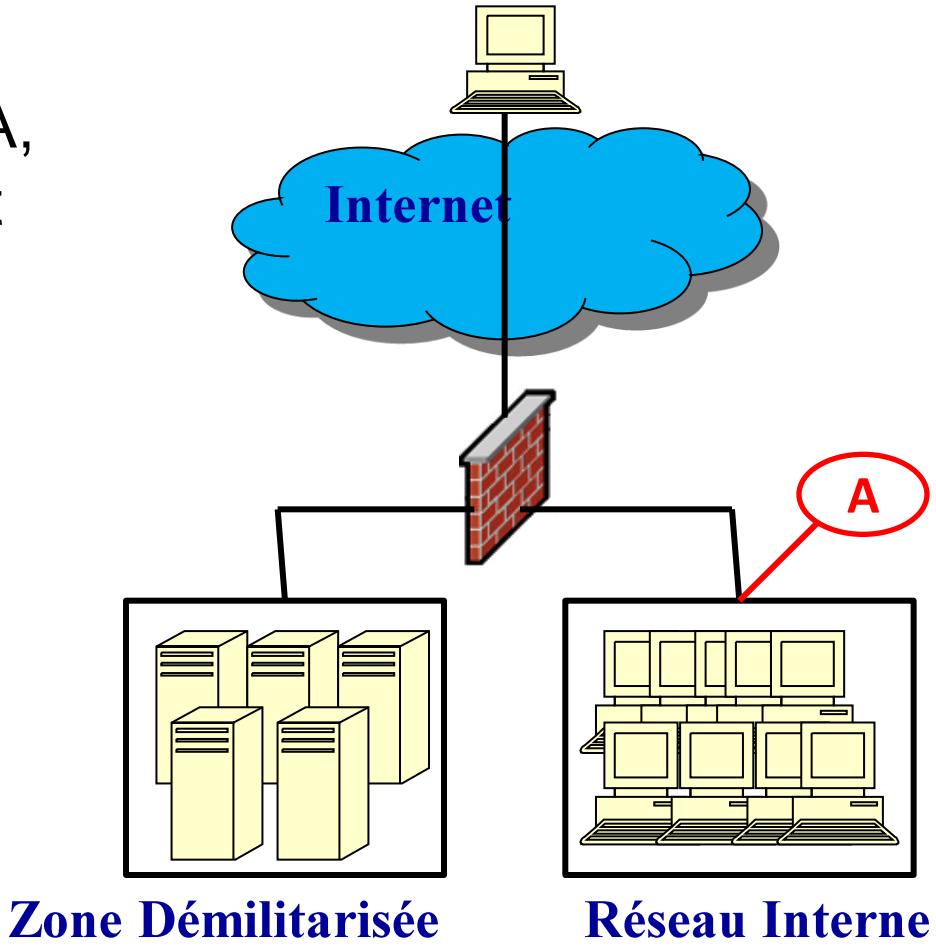
- Scénario 6 : Vous voulez détecter les attaques provenant du VPN IPSec (tunnel entre réseaux)

- Question 6 : Comment positionnez-vous votre IDS
  - A ?
  - B ?
  - C ?
  - Autre solution ?



Exercices de sécurité réseau

- Réponse question 6 : A, le trafic VPN IPSec est chiffré jusqu'à l'interne



Exercices de sécurité réseau

- Exercice 2 : VPN SSL et IPSec

- Objectif :
  - Comprendre les différences entre un VPN SSL et un VPN IPSec
  - Savoir utiliser les solutions de VPN SSL et de VPN IPSec à bon escient

Exercices de sécurité réseau

- Exercice 2 : VPN SSL et IPSec

- Question 1 : Au-dessus de quelle couche un VPN SSL est-il déployé ?
  - Couche 3
  - Couche 4
  - Couche 7

Exercices de sécurité réseau

- Réponse question 1 : Couche 4

- Un VPN SSL intègre le protocole TLS (Transport Layer Security) qui est déployé et construit au-dessus de la couche 4 (transport)
- Un VPN SSL permet d'assurer la sécurité de protocoles de la couche 7 (application) comme le protocole HTTP

- Un VPN IPSec est déployé au-dessus de la couche 3 (réseau)

Exercices de sécurité réseau

- Question 2 : La création d'un VPN IPSec nécessite une configuration préalable des deux extrémités du tunnel
  - Vrai
  - Faux

Exercices de sécurité réseau

- Réponse question 2 : La réponse est vrai

- Pour créer un VPN IPSec, il faut installer un client IPSec aux deux extrémités du tunnel

- Un VPN SSL est « transparent » pour le client
  - Le protocole SSL-TLS est intégré par défaut dans les navigateurs
  - Il n'est pas nécessaire de faire une installation coté client
  - Seul le serveur doit être préalablement configuré
- Remarque :
  - Le projet CISCO AnyConnect permet de déployer un client lourd compatible avec un VPN SSL et un VPN IPSec

Exercices de sécurité réseau

- La technologie de NAT Traversal a été développée pour permettre de traverser les passerelles qui applique la translation d'adresse (NAT)

- Question 3 : Pour quel type de VPN le NAT Traversal a été plus particulièrement conçu ?
  - IPSec en mode transport
  - IPSec en mode tunnel
  - SSL-TLS

Exercices de sécurité réseau

- Réponse question 3 : VPN IPSec en mode transport

- Il existe deux types de VPN IPSec
  1. IPSec en mode Tunnel
  2. IPSec en mode transport

Exercices de sécurité réseau

- Réponse question 3 (explication) :

- IPSec en mode tunnel
  - En mode tunnel, la totalité du paquet IP est chiffrée
  - Le paquet est encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP
  - Ce mode est compatible avec le NAT
  - Utilisation de IPSec en mode tunnel
    - VPN de réseau à réseau (c.a.d. entre deux sites distants)
    - VPN de hôte à réseau (accès à distance d'un utilisateur)
    - VPN de hôte à hôte (messagerie privée)

Exercices de sécurité réseau

- Réponse question 3 (explication) :

- IPSec en mode transport
  - Dans ce mode, seule la payload du paquet IP est chiffrée
  - Le reste du paquet IP est inchangé
  - Le routage des paquets n'est donc pas modifié
  - Mais, IPSec intègre le protocole AH (Authentication Header) qui calcule un hash du paquet
  - On ne peut pas faire du NAT car le hash ne sera plus correct
  - Le NAT-Traversal permet de résoudre ce problème
  - Utilisation de IPSec en mode tunnel
    - VPN de hôte à hôte

Exercices de sécurité réseau

- Réponse question 3 :

- SSL-TLS
  - Un VPN SSL-TLS est construit au-dessus de la couche transport
  - Pas de problème de NAT, ni de PAT

Exercices de sécurité réseau

- Question 4 : On faire passer n'importe quel protocole de la couche 7 dans un VPN SSL
  - Vrai
  - Faux

Exercices de sécurité réseau

- Réponse question 4 : La réponse est faux

- Il est nécessaire de développer une version « over SSL-TSL » d'un protocole applicatif pour qu'il puisse être encapsulé dans un VPN SSL

- En revanche, il est possible d'encapsuler n'importe quel protocole dans un VPN IPSec

Exercices de sécurité réseau

- Réponse question 4 (suite) :

- Exemple de protocole « over SSL-TLS »
  - HTTP, FTP, Telnet, LDAP, NTTP
  - SMTP, IMAP, POP
  - DNS (ne pas confondre avec DNSSEC)
- Un protocole « over SSL-TLS » se voit attribuer un numéro de port spécifique
  - Par exemple, le port 443 pour HTTPS
  - Pour la couche réseau, c'est un protocole « normal »
  - Pas de problème de NAT ni de PAT

Exercices de sécurité réseau

- Question 5 : Dans un VPN SSL, le client et le serveur sont authentifiés
  - Vrai
  - Faux

Exercices de sécurité réseau

- Réponse question 5 : La réponse est faux

- Avec SSL, le client n'est en général pas authentifié
  - Le serveur peut demander au client de fournir son certificat mais c'est optionnel
  - Risque d'attaque man in the middle
- Avec SSL, le serveur est authentifié
  - Sauf si l'autorité de certification s'est fait voler son certificat

- Pour IPSEC, deux protocoles différents sont utilisés :
  - AH (Authentication Header) : authentification et intégrité
  - ESP (Encapsulating Security Payload) : confidentialité

Exercices de sécurité réseau

- Question 6 : Dans quel cas un VPN nécessite une autorité de certification pour être déployé
  - VPN SSL
  - VPN IPSec
  - Les deux mon capitaine

Exercices de sécurité réseau

- Réponse question 6 : Les deux mon capitaine

- Cas d'un VPN SSL
  - Une autorité de certification est nécessaire pour authentifier le certificat du serveur

- Cas d'un VPN IPSec
  - Les deux extrémités doivent présenter un certificat signé par une autorité de certification
  - Mais, le protocole IKE (Internet Key Exchange) propose aussi un mode où chaque extrémité pré-partage un secret