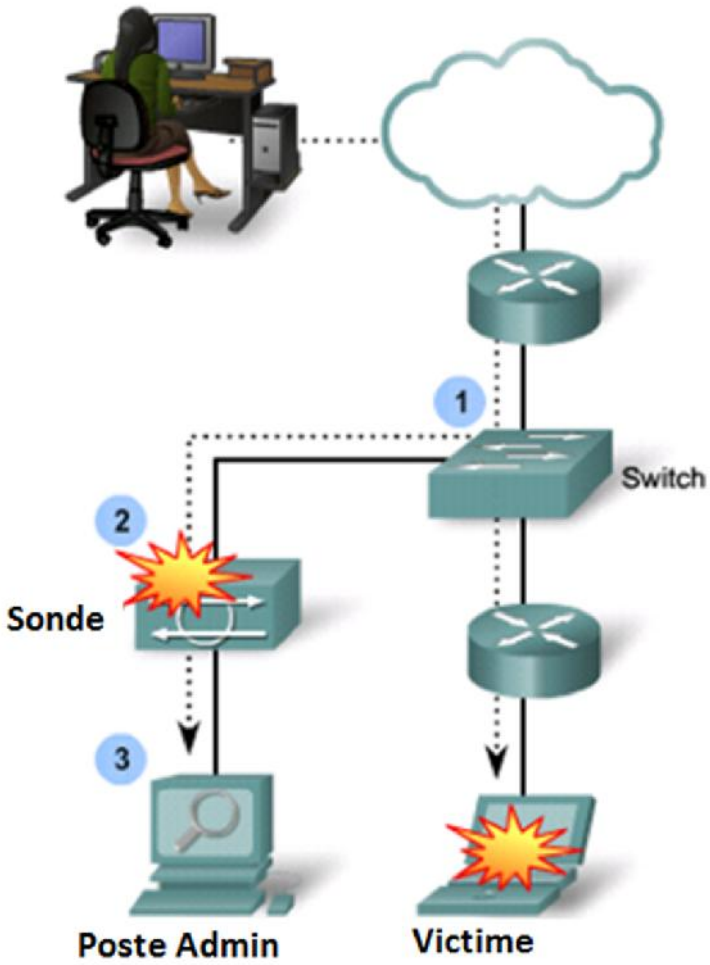
Chapitre 6

DÉTECTION ET PRÉVENTION D'INTRUSION

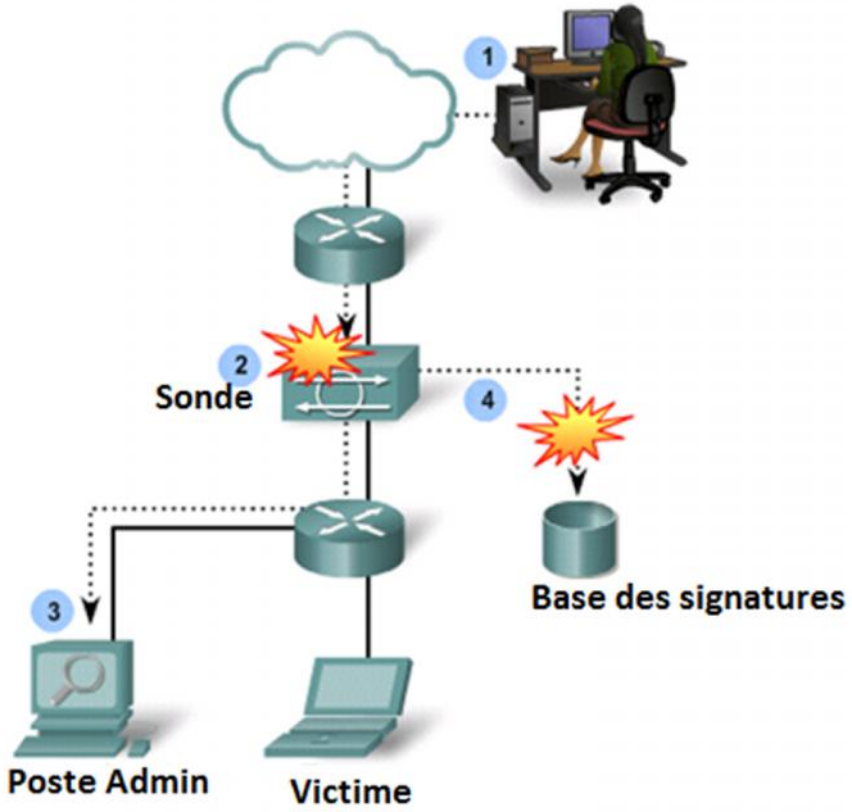
IDS & IPS

- IDS
  - Intrusion Detection System
    - Système de monitoring et de supervision du trafic d'un réseau
    - C'est un dispositif **passif**
    - Il écoute le trafic, crée sa propre copie et ensuite il l'analyse
    - Il compare le trafic enregistré par rapport à des signatures d'attaques
    - Il n'arrête pas les attaques → **il n'est pas réactif**



IDS & IPS

- IPS
  - Intrusion Prevention System
    - Même rôle qu'un IDS
    - **Mais,** il est capable **d'arrêter et bloquer** les attaques
    - Dispositif **Actif**
      - → tout le trafic doit le traverser



IDS & IPS

- IDS ou un IPS peut être
  - Un routeur avec un module spécial (IDS/IPS)
  - Un équipement physique « appliance »
  - Module spécial installé d'un autre équipement (switch ou firewall)
- Un IDS/IPS
  - Utilise la signature pour détecter l'existence d'un trafic « mal-saint »
    - Les modèles de trafic
  - Il est capable de détecter
    - En se basant sur un seul paquet
    - Un flux de paquet

IDS: exemples

- Un IDS
  - Est un équipement dédié pour l'écoute de trafic réseau
  - Il peut contrôler plusieurs machines
- Composition: contient au moins
  - Une carte réseau
    - Généralement spéciale
    - Toujours en mode écoute
  - Un CPU puissant
    - Analyse et comparaison de modèle de trafic
  - Mémoire RAM
    - Importante pour le volume de données et le traitement

La signature

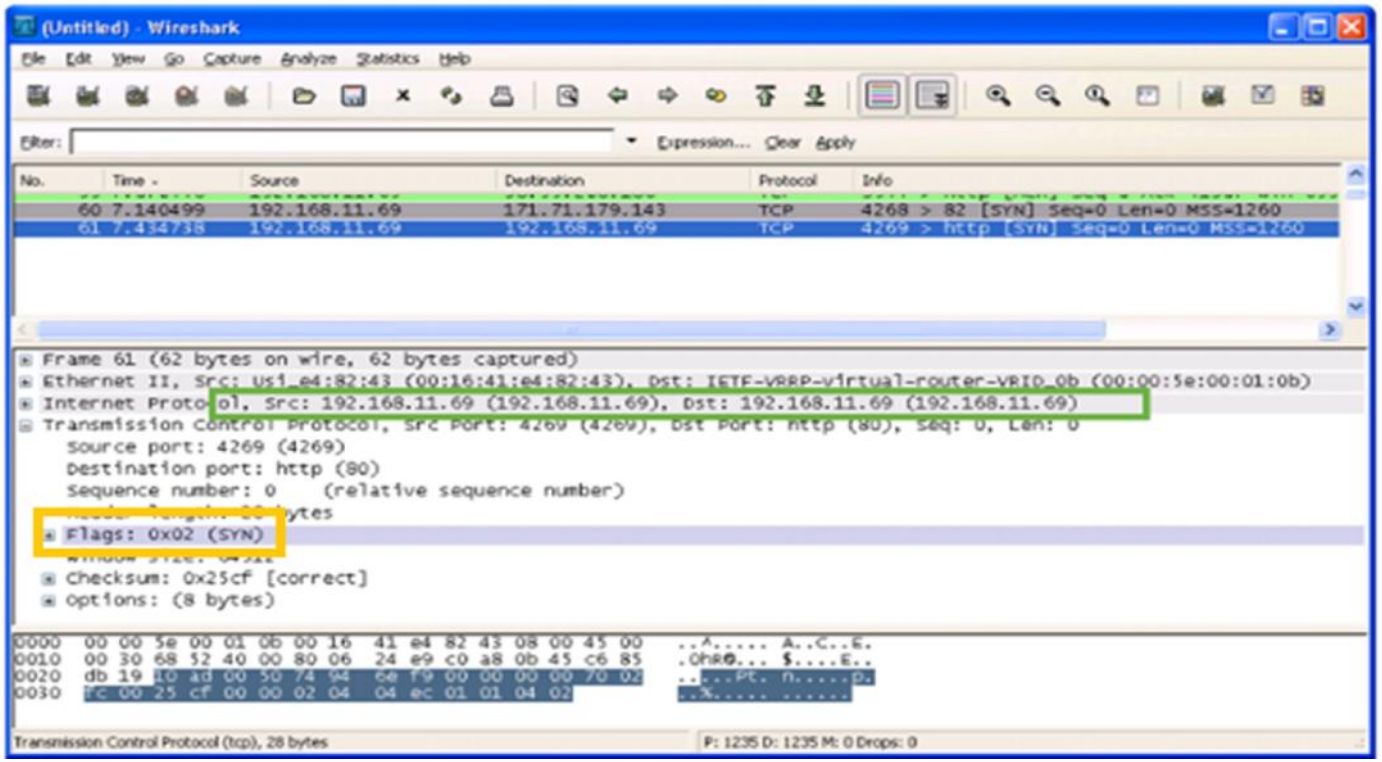
- Modèle de trafic
  - Chaque attaque, virus, vers, etc ,,, possède des caractéristiques uniques et différentes des autres
  - Un IDS/IPS cherche ces caractéristiques dans le trafic supervisé
- Signature
  - La description des caractéristiques d'une attaque donnée
  - C'est un ensemble de règles logiques qui décrit
    - Un évènement
    - Un paquet
- Deux types de signatures
  - Signature atomique→ cherche un seul paquet, évènement
  - Signature composite→ suit un flux de paquets, évènements

La signature atomique

- La signature atomique
  - Est la plus simple
  - Elle caractérise un paquet, un évènement ou une activité
- Avantages
  - Simple
  - Rapide
  - Ne consomme pas beaucoup de ressource pour détecter l'attaque
- Exemple
  - Signature de l'attaque « LAND attack »
    - A **LAND** (Local Area Network Denial) **attack**
  - Type d'attaque de dénie de service
    - TCP SYN spoofing en mettant l'adresse IP source et destination identiques à celle de la victime
    - →Résultat: la victime répond infiniment à elle-même

La signature atomique

- Exemple: LAND attack
- La signature serait alors
  - **If (addr_source==addr_dest AND TCP_FLAG==SYN)**



La signature composite

- La signature composite
  - Notée aussi signature à état
  - Elle serait capable de superviser une suite d'évènements et d'actions et d'échanges sur plusieurs machines pour une période de temps « assez longue »
- Exemple
  - Attendre
    - Deux paquets (SYN) de PC1
    - Ensuite Un paquet ACK de PC2
    - → Signaler l'attaque
- Base de signatures
  - Pour des raisons d'efficacité et mise à jour les signatures sont stockées dans des fichiers

Construction d'une signature

- Construction d'une signature
  - Le plus important dans une signature c'est le mécanisme de déclenchement
  - **Sur quelle base, idée, principe on déduit que l'attaque a eu lieu!!**
  - **Appelée aussi le trigger de signature**
- Les méthodes de construction adoptées sont:
  - *Pattern based detection*
  - *Anaomaly based detection*
  - *Policy based detection*
  - *Hony-Pot based detection*

Construction de signature

- Pattern based detection
  - La plus simple
  - Un IDS possède une base de caractéristiques des attaques
  - Signale une attaque lorsqu'il détecte la présence d'une ressemblance entre la base et le trafic réel
- Avantages
  - Technique efficace à la détection et ne génère pas beaucoup de **fausses alarmes.**
  - Permet un diagnostic efficace et rapide des scénarios et des outils d'attaques.
  - Ceci permet aux administrateurs de définir les priorités pour les mesures correctives.

Construction de signature

- Pattern based detection: Avantages
  - Permet aux administrateurs de
    - Tracer les problèmes de sécurité sur leurs systèmes
    - Initier la procédure de gestion des incidents.
    - Possibilité de sélectionner les patterns en fonction du profil du système : possibilité de concentration sur une attaque ou un matériel
    - Consomme peu de ressources de calcul

Construction de signature

- Pattern based detection: Inconvénients
  - **Aussi puissants que le nombre d'attaques qu'elle connait**
  - Impuissance face aux nouvelles attaques
    - absence d'un mécanisme d'apprentissage.
  - Sensibles aux erreurs de traduction
    - Passage de la langue naturelle au langage machine

Construction de signature

- Anomaly based detection
  - Notée aussi « profile based »
  - Définit la notion de **profile de trafic**
    - Comment doit être un trafic **ordinaire** dans un réseau
  - Le comportement normal est définit par rapport aux
    - Utilisateur
    - Groupes
    - Fichiers
    - Ports
    - Horaire
    - Fréquence d'utilisation
    - Etc..

Construction de signature

- Anomaly based detection
- Exemples
  - Trafic ping à 23h00→ comportement anormal
  - Trafic d'un port non connu→ comportement anormal
  - Un utilisateur tente de se connecter
    - plus de *N* fois et échoue → Donc anormal
  - Le nombre de connexions sur une page web
    - Il dépasse un seuil *X*→ anormal
  - Un utilisateur se connecte en dehors de son créneau horaire habituel
  - Etc..

Construction de signature

- Anomaly based detection: avantages
  - Possibilité d'apprentissage
  - Economie de mémoire
  - Les opérations sont faciles à traduire du langage naturel vers un langage machine
- Inconvénients
  - Difficulté de modéliser
    - Surtout un comportement humain
    - **Ce qui est normal pour quelqu'un pourrait être anormal pour un autre!!**
  - Problème de définition des seuils et des valeurs limites
    - Comment qualifier un comportement de « normal » sur la base de chiffres ?
      - **Demandes excessives → C'est 2 ou 3 ou plus que 10 ???**

Construction de signature

- Policy based detection
  - Notée aussi « behivor-based »
  - L'administrateur décrit le comportement anormal en se basant sur l'historique de son système
  - Même principe que « anomaly based »
  - La signature décrit alors « **l'anormal** » et non pas l'ordinaire.
- Hony-Pot based detection
  - Basée sur les serveurs Hony-Pot: Pot de miel
  - Serveur spécial dédié pour attirer les attaques
  - Rarement utilisé dans un environnement de production

Les erreurs d'un IDS

- Faux positifs
  - Détection d'une intrusion en absence d'attaque

  ➔ Alerte générée par un IDS pour un événement légal.
- Faux négatifs
  - Absence de détection d'une intrusion en présence d'attaque.

  ➔ Pas de génération d'alerte par un IDS pour un événement illégal.

IDS: les filtres

- Un IDS: les filtres
  - Il y a des IDS sous le format d'un filtre logiciel utilisé dans une machine cible
  - Capable de surveiller le trafic et détecter les attaques
- Exemples
  - TripWire
  - SNORT
  - TcpDump

IDS: les filtres

- Exemple: Tripwire
  - Surveille le Système de fichiers
  - Utilitaire disponible pour les systèmes UNIX
  - Création d'un état d'une arborescence de fichiers
  - Génération d'une alarme en cas d'occurrence d'un changement de l'arborescence
- Exemple : SNORT
  - Comprend un *sniffer* de paquets
  - Très grand nombres de filtres
  - Système d'alerte en temps réel
  - Ensemble de règles fonctionnant selon un modèle de correspondance

IDS: les filtres

- Exemple: TcpDump
  - Utilitaire UNIX qui permet de collecter les données circulant sur un réseau, de déchiffrer les bits et d'afficher la sortie dans un format brut
  - Dispose d'un filtre qui permet de spécifier les enregistrements à collecter
  - Exemple

    udp and dst port 31337

ARCHITECTURE D'UN IDS

Network-based IDSs

- Détectent les attaques en recueillant et en analysant les paquets sur un réseau
- Installés sur des machines dédiées
  - facilité de sécurisation
- Placés chacun au niveau d'un segment du réseau

Network-based IDSs : avantages

- Un petit nombre de détecteurs peut contrôler tout un réseau de plusieurs machines.
- Leur installation n'influe pas sur l'architecture du réseau.
- Les machines sur lesquelles sont installés
  - les détecteurs sont très sécurisées et invisibles.

Network-based IDSs : Inconvénients

- Difficulté d'analyser les paquets pendant les périodes de pointe du trafic
- Ne permettent pas de contrôler les liaisons cryptées
  - Exemple VPNs
- Les détecteurs sont vulnérables à certaines attaques réseau

Host-based IDSs

- Les informations
  - sont collectées depuis chaque machine.
- Visibilité des objets
  - (utilisateurs, processus) mis en jeu au cours d'une attaque.
- Les informations sont générées à partir du
  - noyau du système d'exploitation
    - *audit trail*
  - ou de fichiers d'historique
    - L*og files*
- Possibilité de gestion centralisée
  - En canalisant les informations recueillies vers un serveur central.

Host-based IDSs : avantages

- Possibilité de détecter des attaques invisibles par un *network-based IDSs*
- Possibilité de détecter les attaques sur des liaisons cryptées.
- Ne sont pas affectés par les contraintes de l'architecture du réseau.

Host-based IDSs : inconvénients

- Nécessité de configurer le détecteur sur chacune des machines à contrôler
- Le détecteur est plus facile à attaquer
- Ne sont pas efficaces contre les attaques distribuées
- Influence sur les performances des machines
  - consommation excessive des ressources

Application-based IDSs

- Dédiés à des applications spécifiques
- Utilisent les informations contenues dans les fichiers *log*
- Efficaces contre certaines attaques fondées sur le dépassement de privilège

Application-based IDSs : avantages

- Possibilité de détecter les activités douteuses des utilisateurs d'une application
- Sont efficaces sur les liaisons cryptées

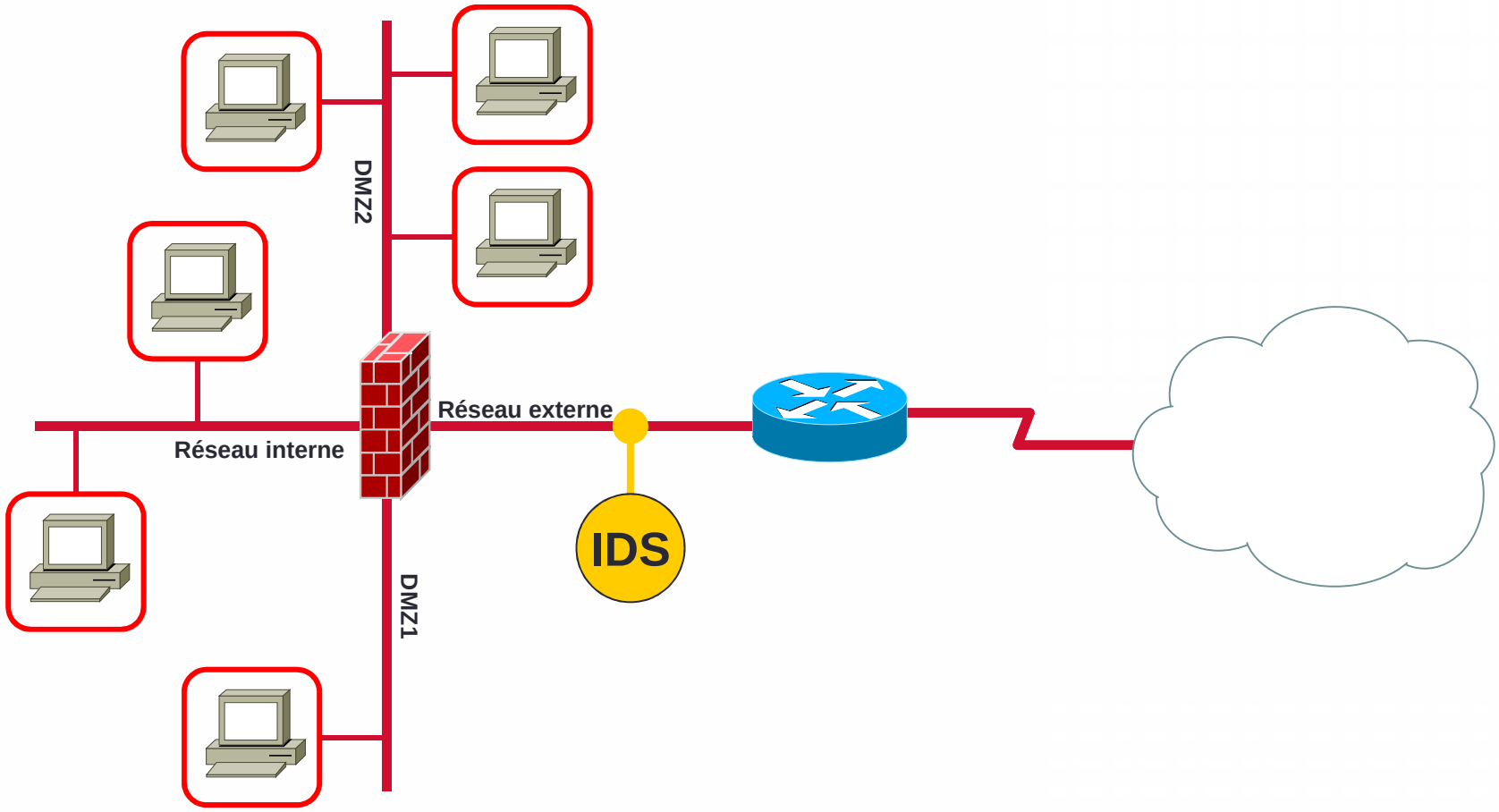
Application-based IDSs : inconvénients

- Les fichiers log utilisés par les applications courantes ne sont pas au même degré de protection que ceux du système d'exploitation.
- Ne dépassent pas le cadre de l'analyse du comportement des utilisateurs.

Placement d'un IDS réseau

- Placement des détecteurs
  - A l'extérieur du *firewall*
  - A l'intérieur du *firewall*
  - A l'extérieur et à l'intérieur du *firewall*
- Contrôle :
  - Centralisé
  - Partiellement distribué
  - Totalement distribué

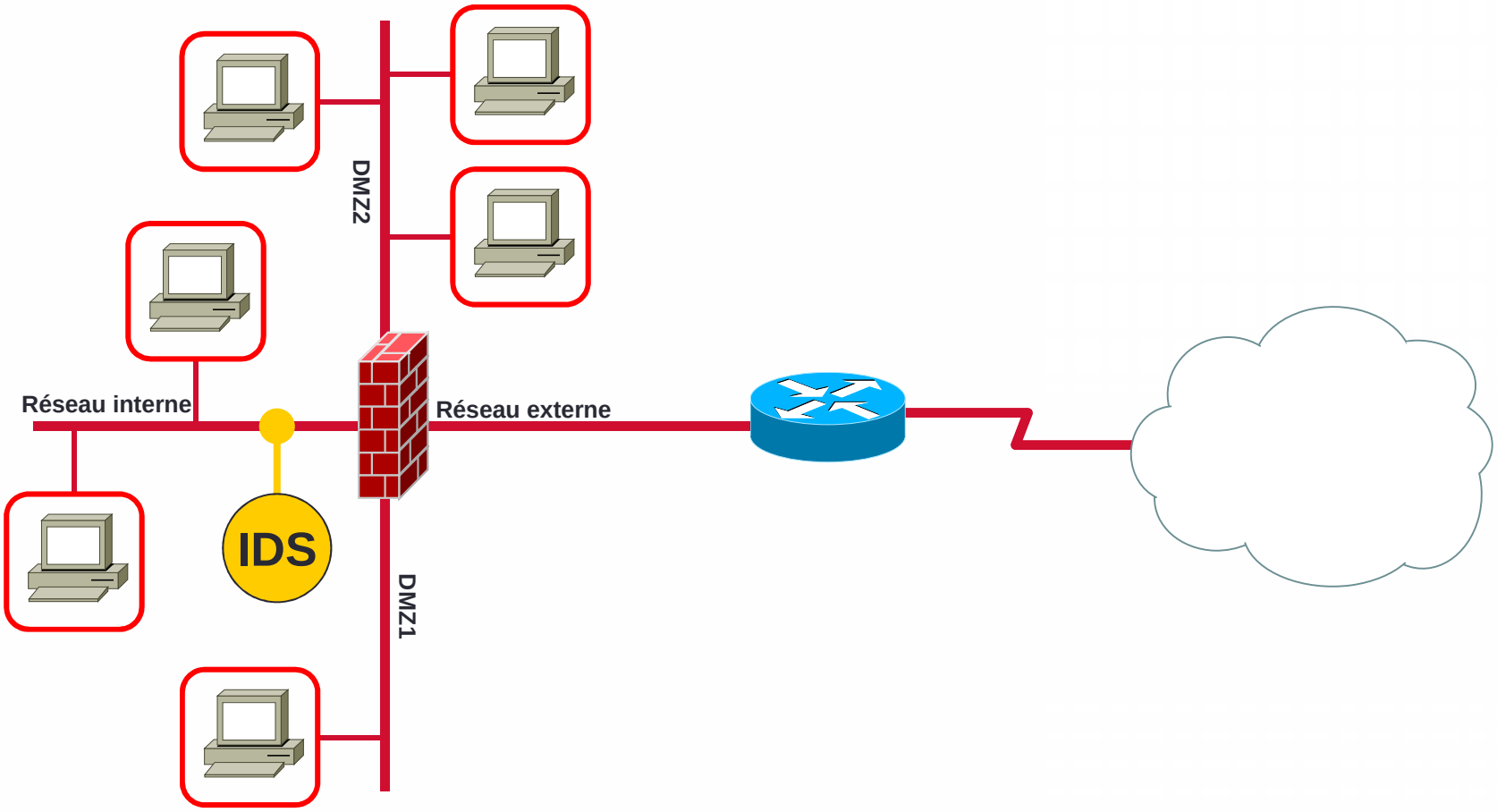
Détecteur à l'extérieur par rapport au *firewall*



Détecteur à l'extérieur par rapport au *firewall*

- Le détecteur est placé avant le firewall.
- Avantage
  - Voit venir toutes les attaques provenant du réseau public
- Inconvénients
  - Facilité d'attaquer le détecteur
  - Les attaques de l'intérieur du réseau ne sont pas détectées
  - Trop d'alertes parce qu'on analyse un trafic inutile
  - Beaucoup de *faux-negatifs*

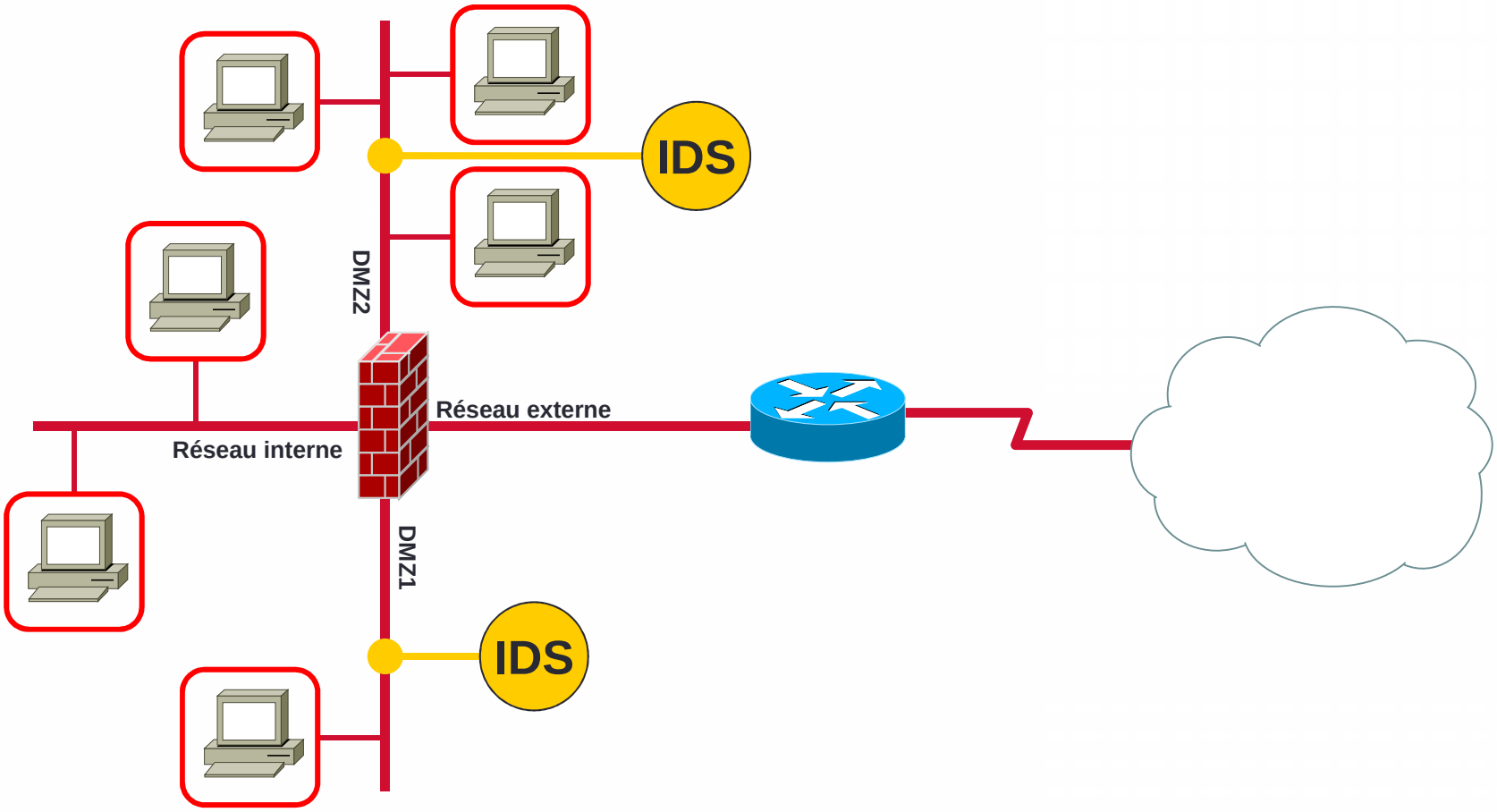
Détecteur à l'intérieur par rapport au *firewall*



Détecteur à l'intérieur par rapport au *firewall*

- Le détecteur est placé en aval du *firewall*
- Avantages
  - Moins de vulnérabilité pour le détecteur
  - Réduction du volume de trafic à traiter
  - Détection des attaques internes

Détecteur sur les segments critiques



Détecteur sur les segments critiques : avantages

- Le détecteur est placé au niveau de la zone démilitarisée (DMZ).
- Identification des attaques qui ciblent les systèmes critiques.
- Identification des attaques qui ciblent les serveurs publics (Web, Ftp, …).

COMPOSITION D'UN IDS

Modélisation des IDS

- Module de source de données
- Module d’analyse de données
- Module de réponse

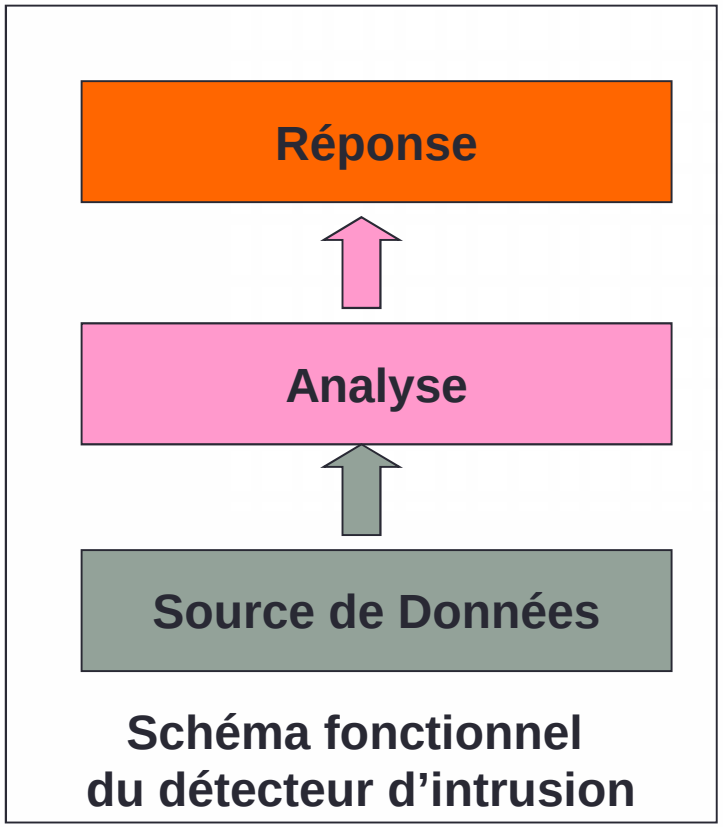


Schéma fonctionnel du détecteur d’intrusion

Module de source de données

- Collecte des évènements provenant de sources multiples qui serviront pour déterminer si une intrusion à eu lieu
- Les sources de données possibles sont :
  - Le réseau
  - Le système
  - Les applications
  - etc.

Module d’analyse de données

- C’est le module responsable de traiter les évènements, provenant de la source de données, afin de décider s’ils sont liés ou non à une intrusion ou une tentative d’intrusion

Module de réponse

- Ce module détermine la réaction de l'IDS suite à la détection d'une intrusion.
- Deux types de réponses
  - Réponses passives : l'intrusion est envoyée à un administrateur qui se charge de la suite
  - Réponses actives : l'IDS peut lui même agir sur la connexion liée à l'intrusion ou même reconfigurer les équipements de sécurité