3TI
Sécurité des réseaux informatiques
2015-2016

La détection d'intrusion

V.Van den Schrieck

Quelques tendances

- Verizon : d'après leurs investigations sur des intrusions,
  - 92% venaient de l'extérieur
  - 14% venaient de l'intérieur
- Verizon et Symantec :
  - Croissance de l'activité malicieuse
  - Augmentation du nombre d'attaques spécifiques

Les intrus

- Les cyber-criminels : crime organisé, objectif de gain financier
- Les activistes : Motivés par des causes sociales ou politiques. Armes : Defacement, DoS, vols et publications de données
- Les organisations sponsorisées par des états (APT)
- Les autres : « hobby hackers », challenge

Niveau de compétence

- Apprentits/Script kiddies : Les plus nombreux. Compétences techniques limitées, utilisent des toolkits existants.
- Compagnons : Capable de modifier les toolkits pour exploiter de nouvelles vulnérabilités.
- Maîtres : Haut niveau de compétence, capables de découvrir de nouveaux types de failles ou d'écrire de nouveaux toolkits

Exemples d'intrusions

- Défacement d'un site web
- Craquage de mots de passe
- Copie d'une BDD contenant des données de carte de crédit
- Utiliser un sniffer pour capturer du trafic réseau
- Utiliser une session ouverte sur un PC
- …

Etapes d'une intrusion

1. Acquisition d'une cible et collecte d'infos
2. Accès initial
3. Gain de privilège
4. Collecte d'information ou exploit sur le système
5. Consolidation de l'accès
6. Dissimulation des traces

Détection d'intrusion

RFC2828 :

La détection d'intrusion est un service qui surveille et analyse les événements système dans le but de trouver et avertir en temps réel ou presque les tentatives d'accès non autorisé aux ressources systèmes

IDS : Composants logiques

- Senseurs : Responsables de la collecte de données (logs, traces réseau, traces d'appel systèmes)
- Analyseurs : Déterminent sur base des données si une intrusion a/a eu lieu
- Interface utilisateur : Pour voir l'output de l'IDS ou contrôler son comportement

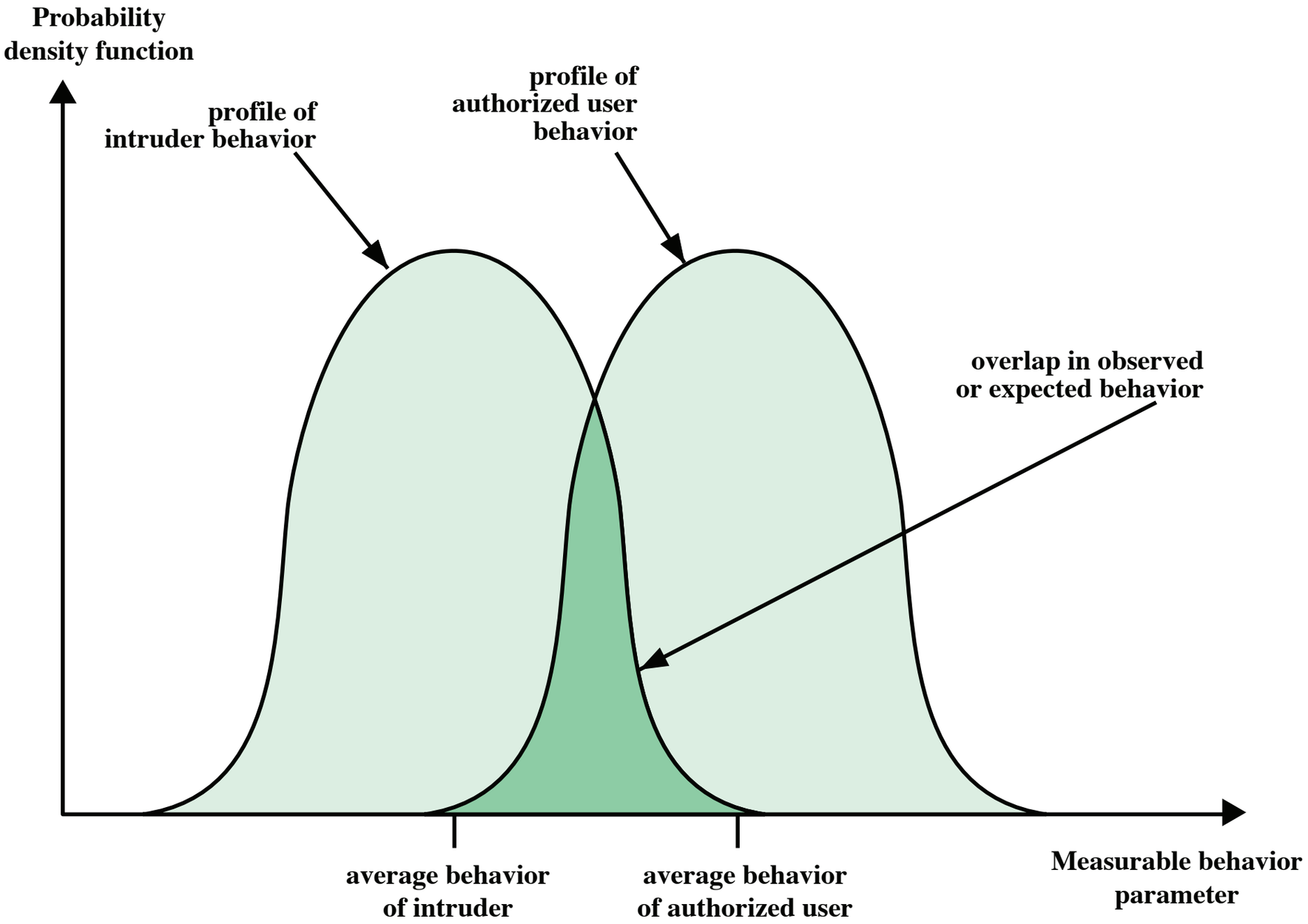
Types d'IDS

- **Host-based IDS (HIDS)** : Surveille un hôte unique, en analysant les appels système ou ou les processus
- **Network-based IDS (NIDS)** : Surveille le trafic réseau et les protocoles associés pour identifier de l'activité suspecte
- **Distributed IDS** : Combine de l'info de plusieurs senseurs (NIDS et HIDS) en un analyseur central pour mieux identifier les intrusions

Motivations pour les IDS

- Détection d'intrusion efficace : Possibilité d'identifier et d'éjecter l'attaquant du système avant qu'il ait pu nuire, ou au moins de mitiger les dégats
- Un IDS peut décourager les attaquants
- Un IDS permet de récupérer des infos sur les techniques d'intrusion et améliorer les techniques de défense

Principe de base



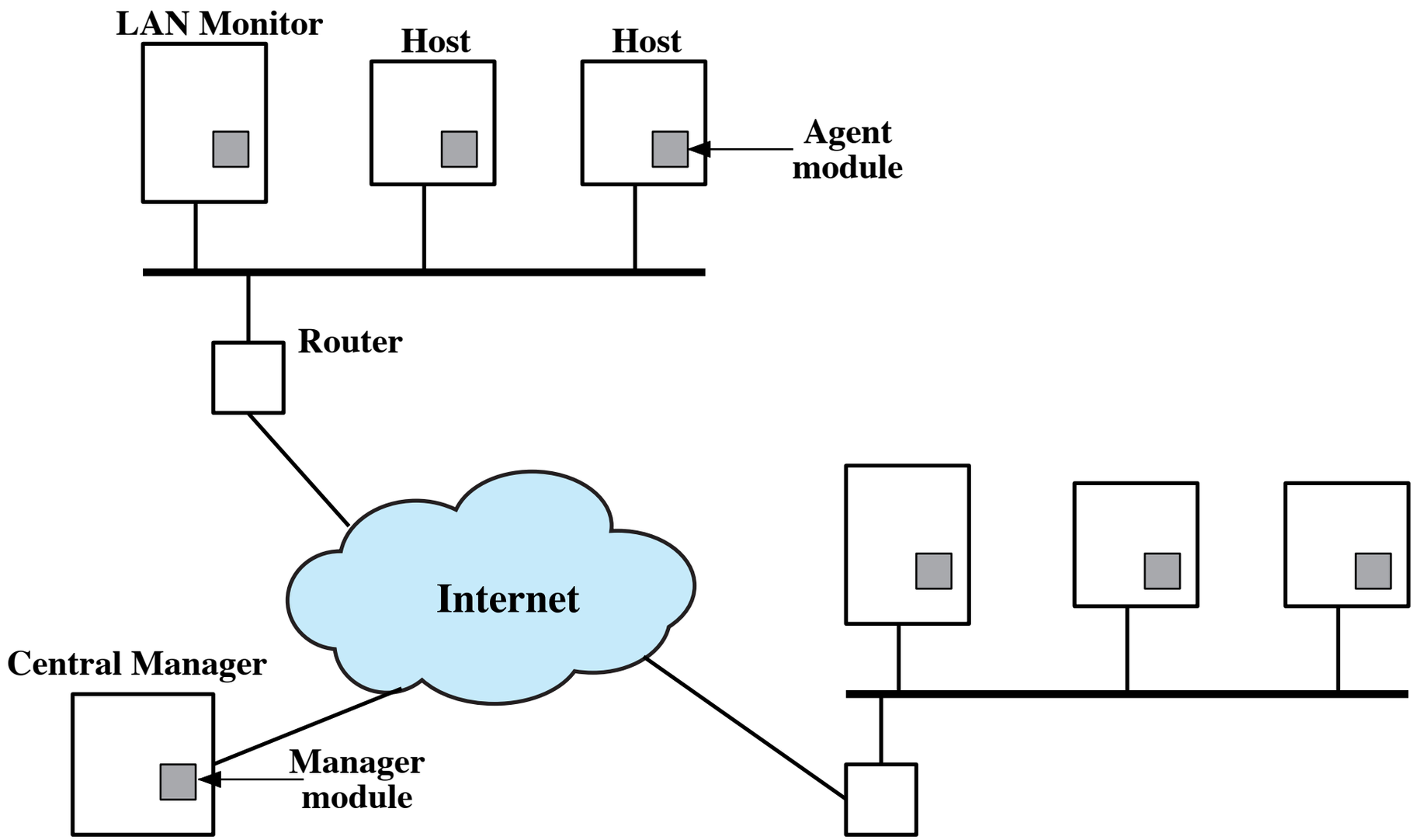
Approches analytiques

- **Détection d'anomalies** : Collecte de données sur le comportement légitime des utilisateurs, et comparaison du trafic observé par rapport à ce référent
- **Détection heuristique ou par signature** : Utilisation de signatures de données malicieuses ou de règles d'attaques pour identifier des attaques connues

HIDS

- Senseurs : Traces d'appel systèmes, logs, checksum pour l'intégrité des fichiers, registre d'accès
- Détection d'anomalie : sous Unix, surtout sur les traces d'appel système
- Signatures : Antivirus

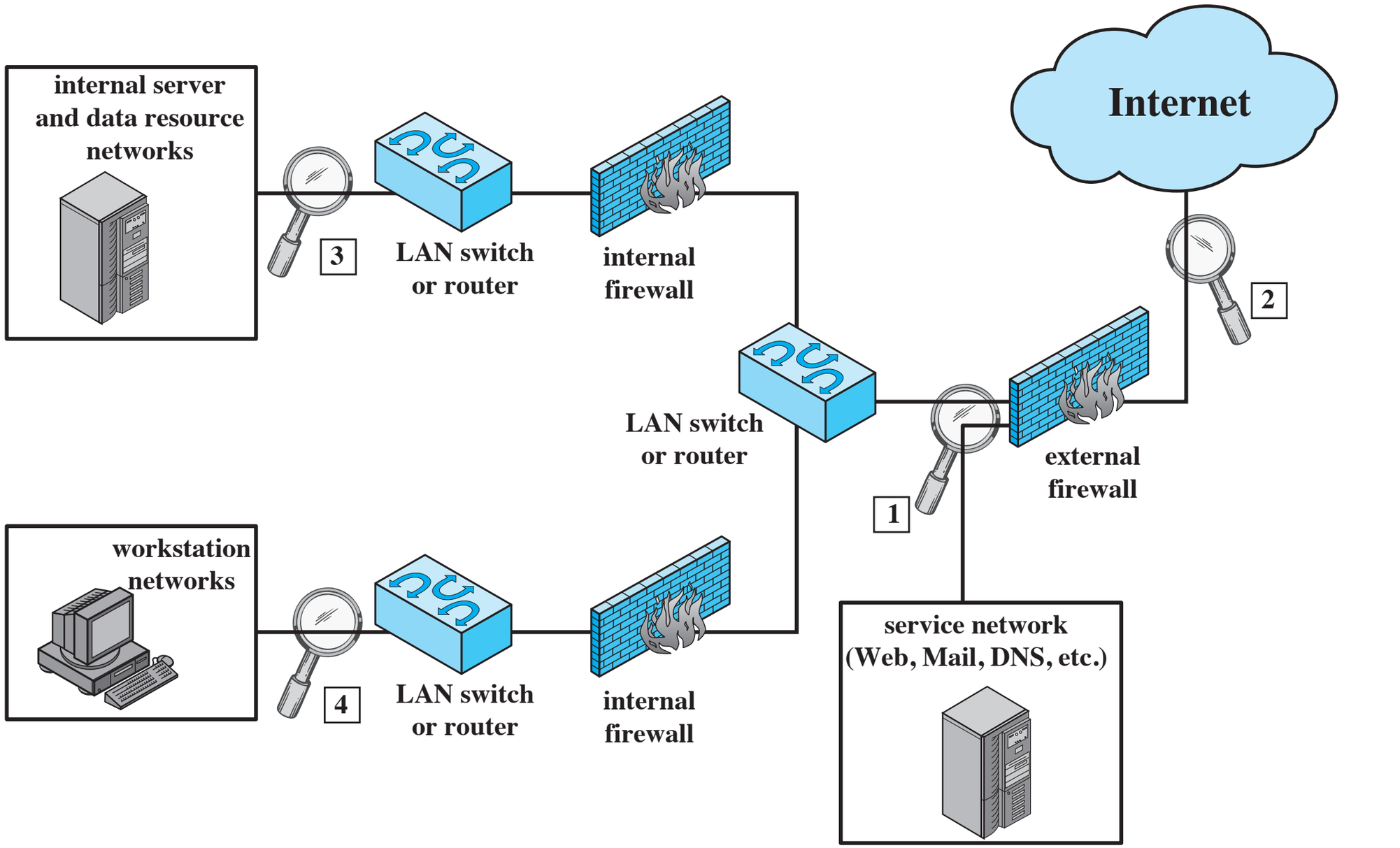
Distributed IDS



NIDS

- Types de senseurs :
  - Inline : Directement sur le lien. Intégré à un FW ou à un switch, ou stand-alone (peut bloquer les attaques - IPS)
  - Passif : effectue une copie de ce qui passe sur un lien réseau

Où placer le NIDS?



NIDS : Détection par signature

Pour chaque couche du modèle réseau, proposez des exemples de signatures typiques d'attaques sur cette couche

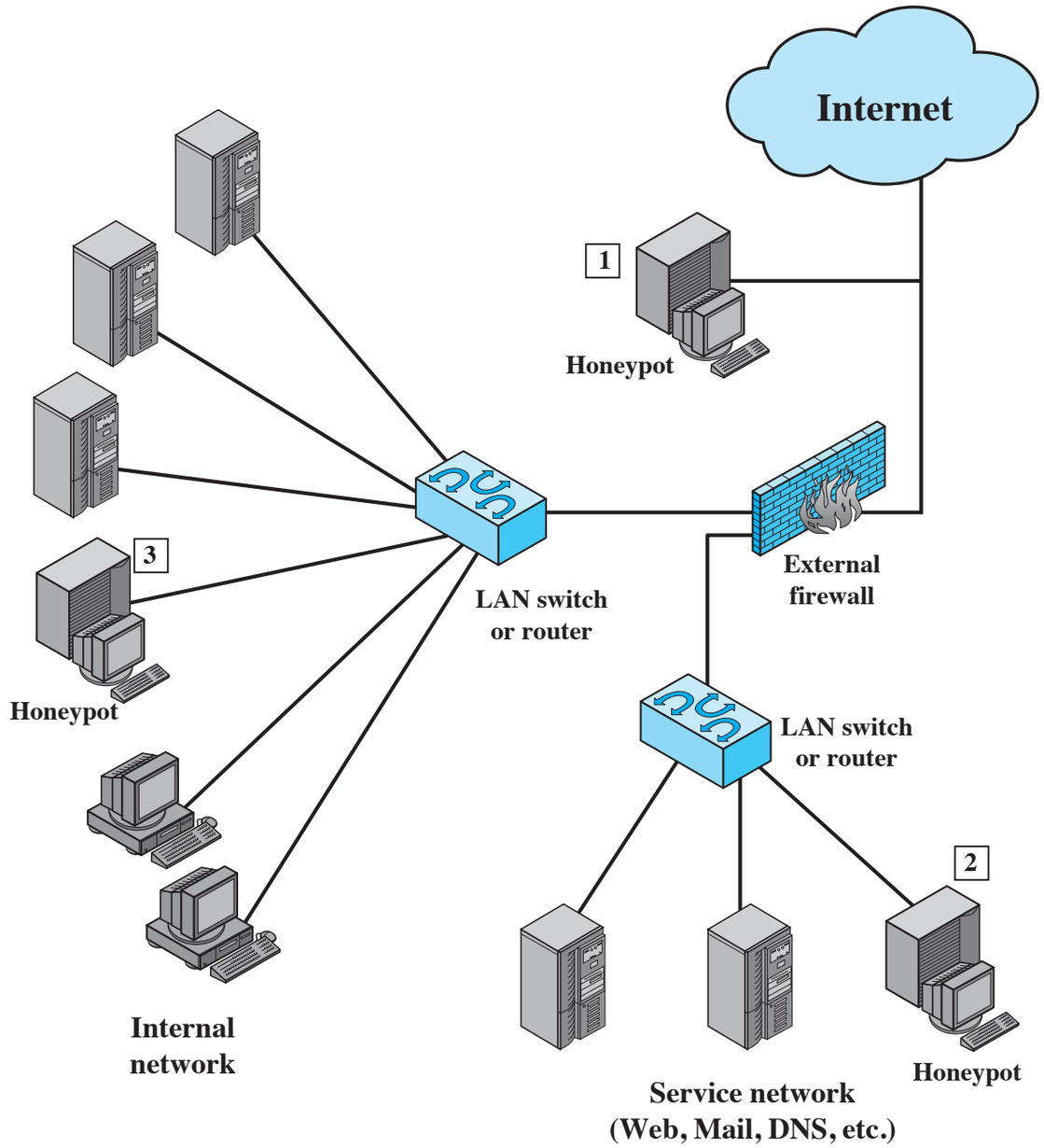
NIDS : Détection par signature

- **Couche applicative** : Analyse DHCP, Finger, FTP, HTTP, IMAP, IRC, NFS, POP, RPC, SIP, SMB, SMTP, SNMP, Telnet, TFTP, …
- **Couche transport** : Fragmentation TCP inhabituelle, scan de ports vulnérables, SYN floods, …
- **Couche réseau** : IPv4, IPv6, ICMP, IGMP. Ex : Adresses IP spoofées, en-têtes IP illégaux
- **Services applicatifs non prévus** : Le trafic vu correspond-il à un service légitime?
- **Violations de politique** : Protocole ou sites web interdits

NIDS : Détection d'anomalie

- **Attaques DoS** : Accroissement inattendu dans le volume de trafic
- **Scanning** : Flux de trafic atypique au nivaux applicatif (bannière), transport (scan UDP/TCP) ou réseau (scan ICMP)
- **Vers** : Propagation rapide, BW large, pattern atypique de communication entre hôtes infectés, scanning

Honeypot


Internet
1
Honeypot
External firewall
LAN switch or router
3
Honeypot
LAN switch or router
Internal network
2
Honeypot
Service network
(Web, Mail, DNS, etc.)