SÉCURITÉ DES RÉSEAUX

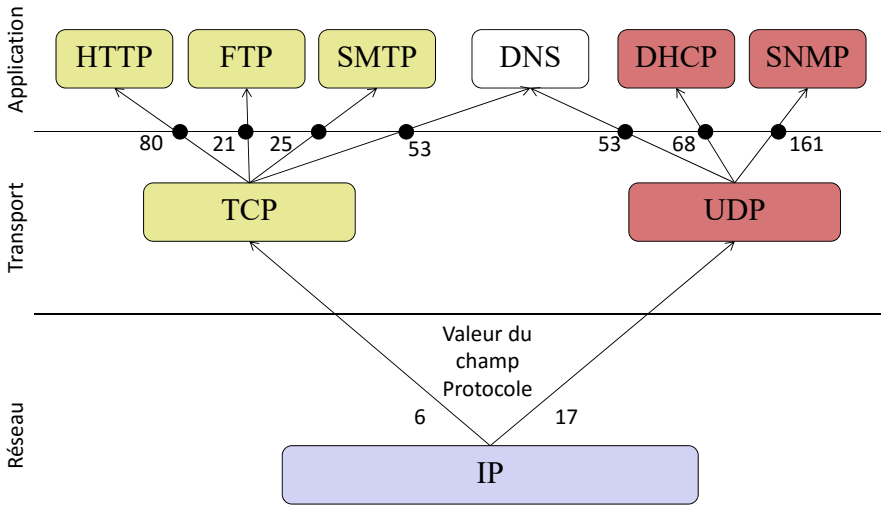
Les services réseaux

- Les services réseaux sont des applications nécessitant un ou plusieurs ports de communication
  - Une application pourra utiliser plusieurs service réseau
- Les services réseaux peuvent fonctionner en parallèle sur une même machine hôte
  - Le système d'exploitation utilise plusieurs service réseaux
    - Mises à jours
    - Récupération de l'adresse IP
    - Récupération de l'heure
    - …

Les services réseaux

- Pour gérer le fait que plusieurs services peuvent fonctionner en parallèle, les protocoles de transport utilisent la notion de port de communication
  - Les ports sont des numéros codés sur 16bits
  - UDP et TCP fournissent chacun un ensemble de ports indépendant l'un de l'autre
    - Ex: sur le port 22 on peut avoir un service TCP et un service UDP (ce n'est pas le même port)
  - Certains numéros de ports sont réservés et correspondent à des services spécifiques
    - Ex le port 22 en TCP correspond à SSH
- Pour contacter un service réseau on va avoir besoin de trois informations
  - L'adresse IP de la station hôte
  - Le protocole de transport à utiliser
  - Le numéro du port sur lequel le service peut être contacté par le protocole de transport

Les services réseaux



Les services réseaux

- La connaissance des services réseaux fonctionnant sur un serveur est un élément important en terme de sécurité
  - L'étude des services peut révéler certaines vulnérabilités du système
    - Connaissance des versions des logiciels
- Certains outils sont spécialisés dans la découverte de ces services: les scanners réseaux ou scanner de ports
  - Ce ne sont pas des outils d'intrusion mais plutôt des outils d'analyse
  - Certains sont capables de fournir la liste des applications connectés sur les ports de communication
  - Ex: Nmap et ISS Scanner

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-03-28 15:55 CET
Nmap scan report for svn.castres.univ-jfc.fr (172.18.128.51)
Host is up (0.0021s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```


Les attaques sur services réseaux

- On va recenser trois grands types d'attaques visant explicitement les services réseaux
  - L'intrusion
    - L'intrusion est souvent une première étape dans une attaque visant à l'infection d'autres machines, au vol de données, à la mise en place de portes dérobées ou à l'injection de logiciels malveillants
    - Elle est suivie d'une phase d'effacement des traces
  - L'interception
    - De données
    - De sessions
      - ★ *Reprend le principe des attaques « man-in-the-middle » appliqué aux sessions Web*
      - ★ *Exploite le fait que dans des sessions SSL seul la phase d'authentification est chiffrée, le reste des échanges s'effectuant à l'aide de cookies de session*
  - Le déni de service
    - Va viser la disponibilité du service réseau

L'interception

- L'interception va pouvoir se jouer à plusieurs niveaux
  - ARP Poisoning
    - Attaque visant à infecter la table ARP d'un hôte avec de fausses traductions d'adresses
    - Permet de mettre en œuvre une attaque de type « Man In The Middle » mais peut également être un préalable à une attaque par déni de service
  - DNS Poisoning
    - Similaire à l'attaque précédente, elle vise les serveurs DNS dans le but de compromettre les traductions d'adresses
    - Naturellement les serveurs DNS sont très sensibles aux attaques MITM dans la mesure où les requêtes de mises à jours peuvent être émise par n'importe qui
    - Pour palier à ce problème deux solutions existent
      - ★ *TSIG [RFC 2845]*
      - ★ *DNSSEC [RFC 2535]*

L'interception

- TSIG (Transaction SIGnature*)* permet de sécuriser les échanges entre serveurs DNS avec
  - ★ *De l'horodatage (reposant sur NTP)*
    - Pour éviter les attaques par rejeu
  - ★ *Partage de clé secrète*
  - ★ *des signatures électroniques des requêtes*
    - Repose sur HMAC-MD5
- DNSSEC
  - ★ *Utilise la cryptographie à clé publique pour assurer l'authentification et la confidentialité des échanges*
  - ★ *Ajout d'une signature électronique pour identifier une zone*
- Les deux mécanismes sont utilisés par les serveurs racines

L'interception

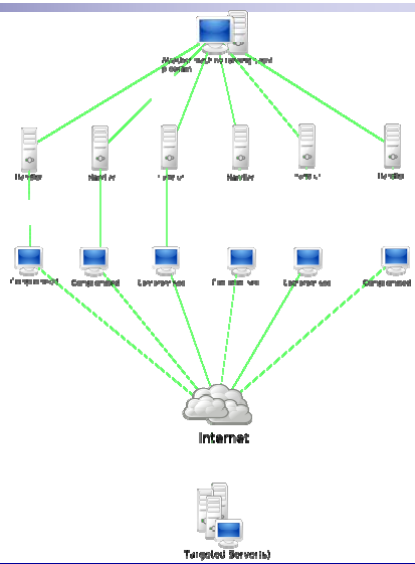
- Route poisoning
  - Même principe cette fois-ci appliqué aux tables de routage
  - RIPv1 n'intègre pas de mécanisme de sécurité pour se protéger de paquets forgés par exemple
  - Les dernières versions des protocoles de routage intègrent des mécanismes de chiffrement et d'authentification pour assurer la fiabilité des informations échangées
- ICMP redirect
  - Cette attaque vise l'intégrité des tables de routages en générant de faux messages ICMP
  - Lorsqu'un routeur reçoit un message ICMP il peut renvoyer un message ICMP redirect pour indiquer à un hôte de contacter un autre routeur pour sa requête
  - Normalement seul un routeur doit pouvoir envoyer ce type de paquet
    - ★ *Un hôte devrait rejeter les autres mais ce n'est pas obligatoirement le cas*

Le déni de service

- L'objectif d'une attaque par Déni de Service (DS) est de rendre les services réseaux indisponibles
- Sur un LAN le DS peut être réalisé de façon involontaire en usurpant une adresse IP
  - Privilégier la distribution d'adresses par DHCP
  - L'usurpation peut être détecté par TCP/IP qui désactive dans ce cas les services réseaux
- ICMP: Attaque par rebond (Smurf Attack)
  - L'attaquant usurpe l'adresse IP de sa cible et broadcast des requêtes ICMP
  - Les machines connectées au réseau local répondent toutes vers l'adresse de la cible causant une surcharge
  - Pour se prémunir, il faut interdire les réponses à ce type de requêtes sur les hôtes
  - Depuis 1999, les routeurs sont, par défaut, configurés pour ne pas router ce type de paquets

Le déni de service

- Sur Internet, les attaques par Déni de Service ne sont plus réalisées par un seul attaquant mais par un ensemble de machines
  - On parle alors de Déni de Service Distribué (ou DDS en anglais)



Le déni de service

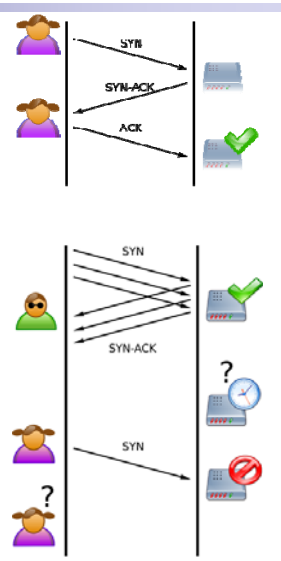
- A l'échelle d'Internet, ces attaques par DDS vont cibler soit un serveur spécifique pour interrompre son service, soit le réseau tout entier
  - Utilisation d'ordinateurs zombis pour maximiser le nombres d'attaquants
  - Les ordinateurs zombis sont en général contaminés par un vers en prévision de l'attaque
    - L'attaque peut être scriptée dès le départ (ex: CodeRED en 2001)
    - Elle peut être déclenchée par une commande à distance
      - ★ *Directe: possibilité de la bloquer avec un pare-feu*
      - ★ *Par un relais IRC à travers une connexion SSL/TLS*
- Les serveurs DNS: Le talon d'Achille?
  - La plupart des attaques à grandes échelles visent les 13 serveurs DNS racines
  - Les serveurs DNS mal configurés sont également utilisés pour réaliser des attaques
    - 03/2013: Attaque DrDDS ciblant SpamHaus

Le déni de service

- Fonctionnement d'une attaque par déni de service
  - Le nombre de machine est important mais pas uniquement
  - En général une attaque par DS va utiliser des failles des protocoles réseaux
    - ICMP Flood
      - *Envoie de paquets ICMP de plus de 65535 octets*
      - *Les anciennes versions de la pile IP ne savent pas gérer ces paquets de grande taille*
      - *Le problème est résolu dans les versions actuelles mais le temps de traitement est toujours plus long que pour des paquets normaux*
      - *L'attaque consiste donc à surcharger le processeur de la machine cible avec des paquets plus long*
      - *Très simple à mettre en œuvre avec des outils logiciels comme hping*
      - *Pour prévenir, le mieux est de bloquer les paquets à l'entrée du réseau*
    - TCP SYN Flood
      - *Utilisation de la phase d'ouverture de connexion TCP pour surcharger une cible*

Le déni de service

- *Le principe de l'attaque consiste en fait à surcharger un serveur en requêtes SYN*
- *Le serveur va répondre par des paquets SYN-ACK et attendre l'arrivée d'un paquet d'acquittement pour finaliser l'ouverture de connexion*
  - Si l'ACK n'arrive jamais on se retrouve avec des connexions à demi établies
- *Chaque demande de connexion est stockée dans une file d'attente*
  - Si l'attaquant envoie suffisamment de requêtes le serveur ne pourra plus traiter les demandes légitimes
- *Le RFC4987 recense les moyens de défense*
  - SYN Cookie, SYN Cache, réduction des timers…
- *Détectable avec netstat*
  - netstat –n –p TCP



Le déni de service

- D'autre au contraire vont tirer s'appuyer sur les protocoles proprement dits
  - Slow-Read
    - *Le principe est d'envoyer des requêtes au serveur et de lui répondre très lentement*
    - *Le protocole est bien suivit mais la lenteur des réponses va ralentir le serveur et dégradé son service*
    - *Fait partie d'une large famille d'attaque dites par « starvation »*
  - DHCP Starvation
    - *Attaque de niveau 2-3 OSI visant à surcharger un serveur DHCP de requêtes jusqu'à ce que son pool d'adresses IP soit vide*
    - *En cas de requête d'un hôte légitime le serveur ne pourra plus lui offrir d'adresses*

Le déni de service

- Le déni de service au niveau réseau n'est pas la seule menace d'un SI
  - Les dénis de services peuvent cibler spécifiquement une application et deviennent beaucoup plus difficile à détecter au niveau réseau
  - En particulier si l'attaque se passe dans une connexion sécurisée SSL/TLS
- Ces attaques utilisent des failles logicielles d'où la nécessité de maintenir ses version à jours
  - Ex: HTTP permet de connaitre très simplement la version d'un serveur Web avec une simple requête GET envoyée en TELNET sur le port 80
  - Une ancienne version du serveur Web pourra permettre à l'attaquant de mettre en œuvre des techniques d'intrusion connues sur cette ancienne version

Le déni de service

- Les moyens de défense pour le DDS réseau existent mais ne permettent pas de tout prévenir
  - Les attaques ICMP flooding et TCP flooding sont connues et peuvent être bloquées à l'entrée du réseau
  - Les attaques par starvation sont plus difficiles à bloquer, elles doivent être anticipées au niveau des protocoles et de leurs implémentations
  - Les attaques visant à saturer la bande passante ne peuvent être empêchées mais elles peuvent être contenues
- On va donc mettre en place des architectures réseaux dotées de moyens de prévention, de détection et de protections spécifiques
  - Firewall
  - Proxies
  - IDS, IPS…

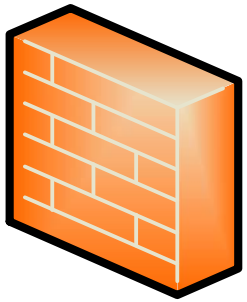
LES ARCHITECTURES DE SÉCURITÉ

Généralités

- L'objectif premier d'une architecture de sécurité réseau est de restreindre la manière dont les machines d'un réseau peuvent accéder à Internet
- On cloisonne donc le réseau en deux grande parties:
  - Le réseau interne à protéger
  - Le réseau Internet
- Le niveau de confiance dans ces réseaux ne sera pas le même
  - Le réseau interne sera également cloisonné en fonction des besoins
    - Le réseau WiFi aura un niveau de confiance au réseau des serveurs
- Le cloisonnement permet également de définir des règles d'accès plus poussées que les simples masques de réseaux IP
- Les règles sont centralisées dans un pare-feu ou firewall
  - Il assure le contrôle des communications entre différents réseaux ayant des niveaux de confiance différents

Le pare-feu

- Le pare-feu pourra être
  - Un matériel dédié
  - Un logiciel



- Les deux présentent les même fonctionnalités mais pas les mêmes performances
  - Filtrage statique des paquets
  - Filtrage dynamique des paquets
  - Proxys applicatifs
  - …

Le filtrage statique et les ACL

- Le filtrage statique est le plus ancien et consiste à bloquer un paquet sans se préoccuper de son état (stateless)
  - Est-ce un paquet d'une session TCP ou un paquet UDP seul ?
- Ce mode de filtrage est proposé par tous les pare-feu et va permettre d'établir des règles prenant en compte
  - L 'adresse de l'émetteur
  - L'adresse du destinataire
  - Le port de l'émetteur
  - Le port du destinataire
- Les ACL (Access Control List) contiennent l'ensemble de ces règles
  - Les règles s'enchaînent de la plus spécifique à la plus générale
  - Elles disposent en générale d'une règle par défaut permettant d'interdire tous le trafic ou au contraire de tout autoriser

Le filtrage statique vs le filtrage dynamique

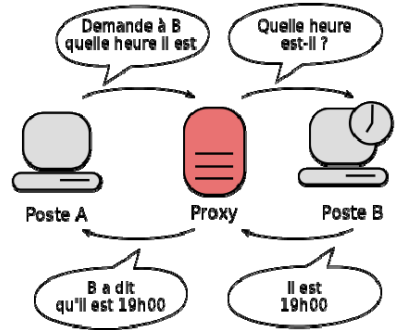
- Le filtrage statique permet une gestion en tout ou rien du réseau mais ne se préoccupe pas du trafic transporté
  - Il ne permet pas de stopper des attaques de type TCP SYN flooding par exemple
  - On va par exemple accepter toutes les communications en provenance du port 80 même celles qui n'ont pas été sollicitées
  - Mauvaise gestion de la fragmentation
    - Le numéro de port n'est présent que dans le premier fragment
- Le filtrage dynamique au contraire va maintenir une table d'états concernant l'ensemble des communications
  - On conserve un historique des communications
  - On peut faire un suivit des établissement de connexion pour TCP
    - Par exemple, on n'acceptera un SYN-ACK que si un SYN a été envoyé avant
  - Permet de gérer des communications liées (Ex RTP/RTCP)

Le filtrage dynamique et le filtrage applicatif

- Le filtrage dynamique permet également de gérer les communications UDP
  - Pour la fragmentation, le premier paquet est conservé en mémoire
    - on utilise les informations qu'il contient pour accepter ou refuser les fragments suivants
  - Pour les communications UDP standards, seules les réponses UDP sont tolérées
- Dans les versions modernes des firewalls, il est également possible de spécifier des règles propres aux applications
  - Bloquer toutes les applets JAVA ou le flash, interdire le P2P…
  - Ils permettent également de repérer les spywares ou trojan à l'intérieure d'une communication apparemment légitime
  - Les firewall dédiés aux applications Web sont appelés WAF (Web Application Firewall)

Les serveurs mandataires

- Un autre mécanisme de sécurité important est le serveur mandataire ou proxy
- L'objectif principal d'un proxy est de servir d'intermédiaire dans une communication
  - Il va servir de relais pour masquer et protéger l'origine des requêtes
  - Dans une architecture client serveur
    - le client va envoyer sa requête au proxy qui la fera suivre au serveur légitime
    - Le serveur répond au proxy qui fait suivre la réponse au client
  - Il va mettre en œuvre deux connexions au lieu d'une

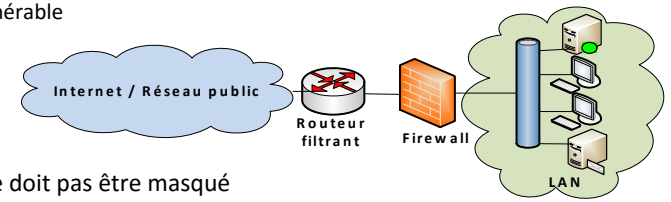


Les serveurs mandataires

- Le serveur mandataire peut également avoir des fonctionnalités
  - De cache pour accélérer la navigation Web
  - De filtrage de contenu (publicité, sites interdits)
    - On parle alors de proxy filtrant
  - De journalisation des échanges
  - D'anonymisation des requêtes (NAT)
- Le proxy peut donc être utilisé dans le cadre de la sécurité mais également pour contourner des règles de sécurités
  - Ex: Utilisation d'un proxy américain pour accéder aux services de rattrapage des télévisions américaines
- Un serveur mandataire est utilisé en sortie d'un réseau mais certains proxy peuvent être utilisés pour accéder à des ressources internes (Serveur Web)
  - On parle alors de serveur mandataire inverse (reverse proxy)

DMZ

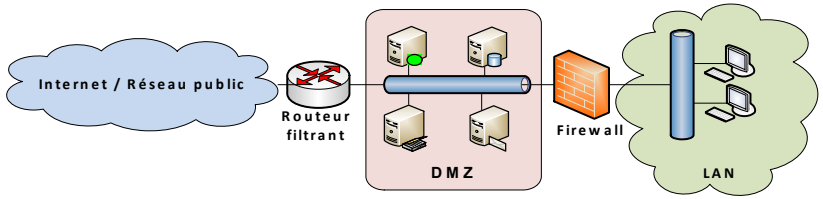
- Autour du proxy et du firewall différente architecture de sécurité se sont construites
- La première consiste à mettre un simple firewall en frontal de son réseau local
  - Très simple à mettre en œuvre
  - Peu de garantie de sécurité car si le firewall est compromis le réseau est vulnérable



- Tout ne doit pas être masqué
  - Les serveurs Web, Mail etc. doivent pouvoir être accessibles de l'extérieur
  - Avec cette solution le trafic externe circule sur le LAN pour contacter les serveurs

DMZ

- La DMZ (Zone Démilitarisée) est utilisée pour permettre d'assurer ces fonctionnalités
  - Elle s'appuie sur des routeurs pour le filtrage statique et sur des firewall pour le filtrage dynamique
  - Des serveurs proxys peuvent également être utilisés dans le cas d'architecture complexes
- La topologie standard

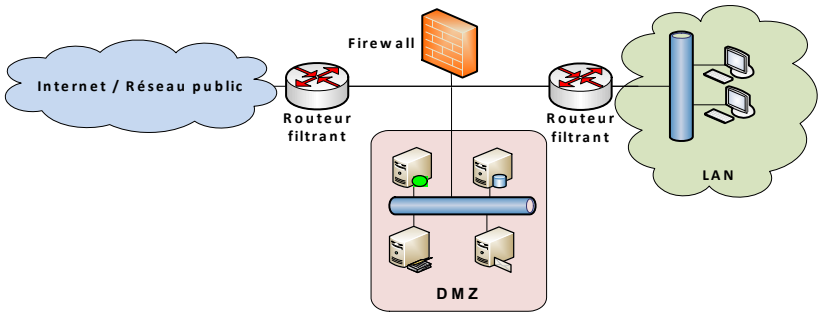


DMZ

- Avantages
  - Les réseaux privés et publiques sont bien séparés et n'impactent pas l'un sur l'autre
  - Le serveur DNS de la DMZ ne fournit que très peu d'informations sur le réseau interne
  - Le routeur filtrant en entrée restreint les accès extérieurs à la DMZ
- Inconvénients
  - Si le firewall est compromis, il va contenir toutes les informations pour pouvoir attaquer le LAN interne
  - Les serveurs externes sont très peu protégés

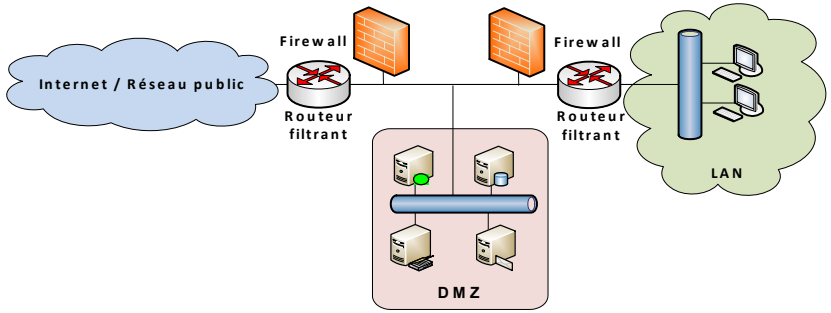
DMZ

- Une autre approche consiste à faire transiter tout le trafic entrant par le firewall qui va alors jouer le rôle de bastion
  - Un second routeur filtrant peut également être mis à l'entrée du LAN pour ajouter un niveau de protection (3 niveaux de défenses)



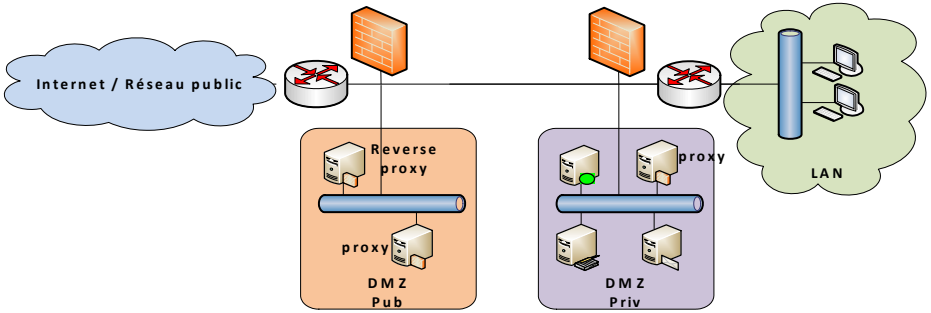
DMZ

- Dans cette solution, la protection est meilleure mais une fois encore si le firewall est compromis, le LAN n'est plus protégé que par le routeur filtrant
- Pour améliorer le niveau de sécurité, la solution la plus courante repose sur l'utilisation de deux firewalls



DMZ

- La DMZ peut également être fractionnée en plusieurs sous-réseaux chacun protégé par des règles différentes au niveau du firewall
  - Le firewall doit alors disposer d'autant d'interfaces que de sous-réseaux
- Il est également possible de définir une DMZ publique et une DMZ privée



DMZ

- De manière générale il n'existe pas d'architecture idéale et il est nécessaire de s'adapter
  - A la structure organisationnelle et géographique
  - A ce qui doit être accessible
  - Au ressources matérielles et humaines dont on dispose
- Les DMZs permettent de structurer son réseau et de disposer des moyens de défense
  - Les firewalls et les routeurs filtrants assurent une bonne protection mais ils peuvent néanmoins être compromis
  - De même ils ne voient pas forcément toutes les menaces
  - Pour les aider, on ajouter en général des outils de détection et de prévention d'intrusion (IDS et IPS)