Université de Technologie d'Abidjan

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Enseignante: Dr KIE VICTOIRE

Enseignant-chercheur à ESATIC

CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau
2. Les pares-feux
3. Systèmes de détection d'intrusion (IDS) et de prévention d'intrusions (IPS)
4. Réseaux privés virtuels (VPN)

CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

Les protocoles de sécurité réseau sont ***un ensemble de règles et de normes*** qui régissent la manière dont les données sont transmises en toute sécurité sur un réseau. Ils visent à ***protéger*** la **confidentialité**, **l'intégrité** et la **disponibilité** des données en empêchant les accès non autorisés, les interceptions et les modifications.

❑ Types courants de protocoles de sécurité réseau

- **SSL/TLS (Secure Sockets Layer/Transport Layer Security)** : SSL/TLS est un protocole qui consiste à chiffrer de bout en bout des données applicatives échangées entre deux machines sur un réseau. Il est principalement utilisé par des fournisseurs de service tels que les sites de vente en ligne, en offrant une session sécurisée entre le client (le navigateur Web) et le serveur (le site Web). Ce protocole est généralement intégré par défaut dans tous les navigateurs Web en maintenant à jour ses différentes versions sans l'intervention de l'utilisateur. La majorité des protocoles applicatifs offrent une version sécurisée basée sur SSL/TLS, par exemple HTTP et HTTPS.

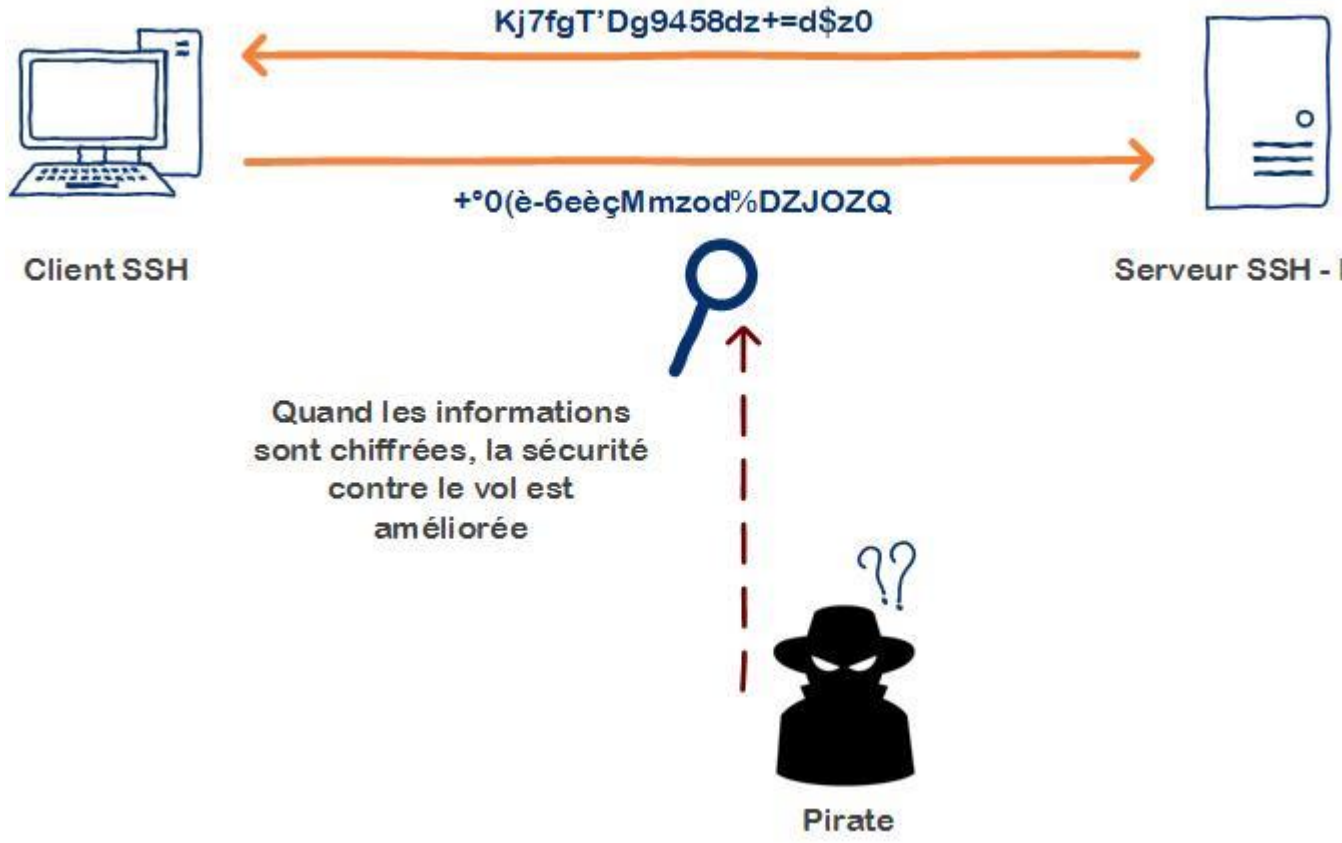
CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

- **protocole Secure Shell (SSH)**: est un protocole réseau cryptographique utilisé pour opérer des services réseau de manière sécurisée sur un réseau non sécurisé. Les cas d'utilisation typiques incluent l'accès distant à des systèmes, la gestion de réseaux de manière sécurisée.

(des serveurs distants, le transfert sécurisé de fichiers, et l'exécution de commandes à distance.)



CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

➢ **IPSec (Internet Protocol Security):** regroupe un ensemble de protocoles, qui utilisent des algorithmes destinés à transporter des données sur un réseau IP de façon sécurisée.

L'IPSec est intimement lié aux protocoles IPv4 et IPv6. Il permet ***d'authentifier*** et de ***chiffrer*** des données, de sorte à assurer une certaine ***confidentialité*** et une certaine ***intégrité*** des flux des données.

Protocoles clés utilisés par IPSec:

- **Protocole AH (Authentication Header):** fournit l'authentification et l'intégrité des paquets IP, garantit que les paquets n'ont pas été modifiés en transit.

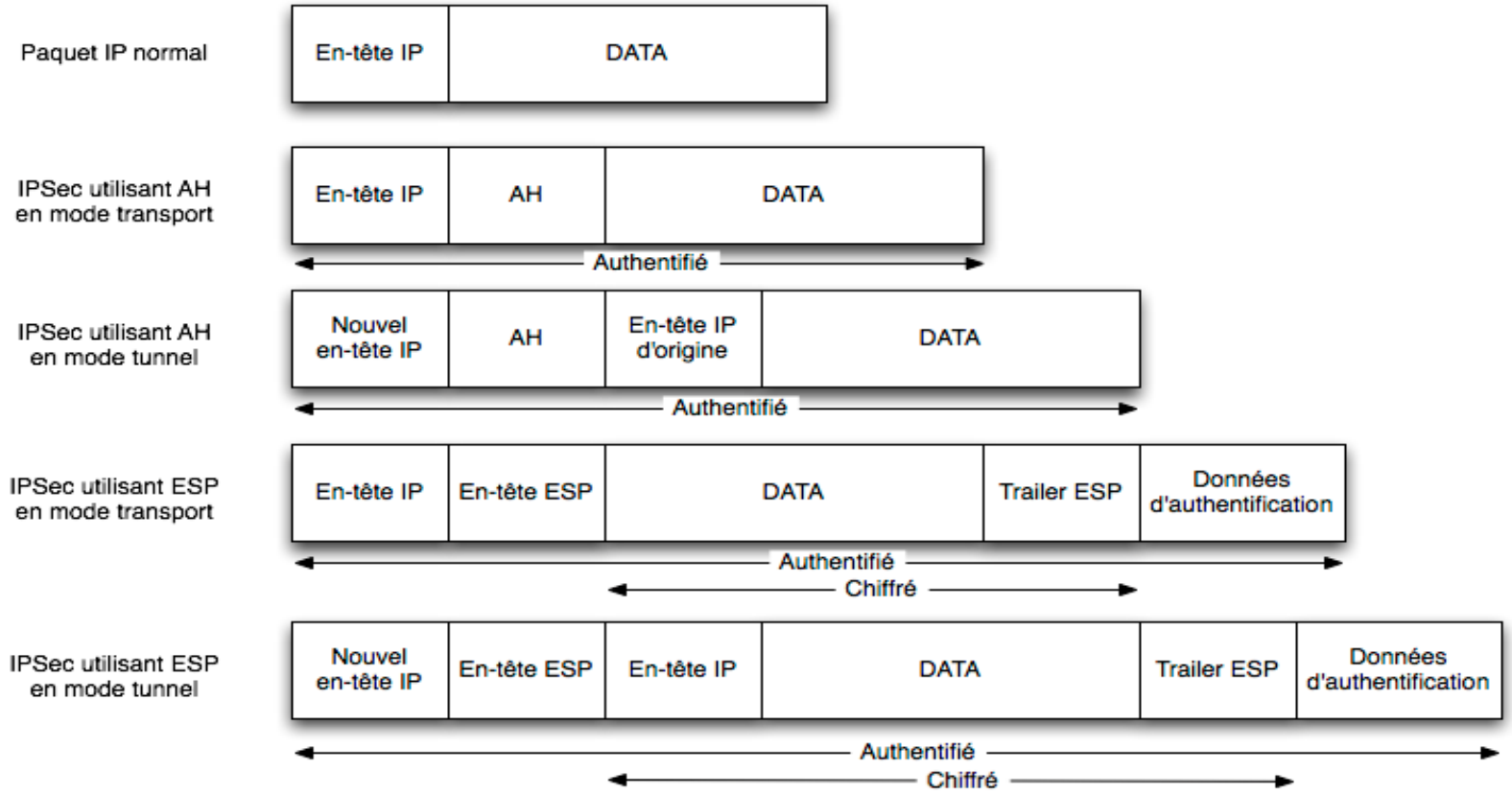
- **Protocole ESP (Encapsulating Security Payload):** fournit la confidentialité, l'authentification et l'intégrité des données. Il encapsule les données à protéger et les protège en chiffrant le contenu, en ajoutant un en-tête pour l'authentification et l'intégrité, et en option, en ajoutant un en-tête de protection contre la relecture

CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

➢ IPSec (Internet Protocol Security)-Protocoles clés utilisés par IPSec:



CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

➢ **IPSec (Internet Protocol Security)-Protocoles clés utilisés par IPSec:**

- **SA (Security Association):** un ensemble de paramètres de sécurité qui définissent la manière dont deux parties communiqueront en toute sécurité en utilisant le protocole IPSec

- **Protocole IKE (Internet Key Exchange):** un protocole utilisé pour configurer de manière sécurisée les associations de sécurité (SA) dans le cadre d'IPSec. IKE est essentiel pour négocier les clés de cryptage et les paramètres de sécurité entre deux entités communicantes, garantissant ainsi une communication sécurisée sur les réseaux IP.

CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

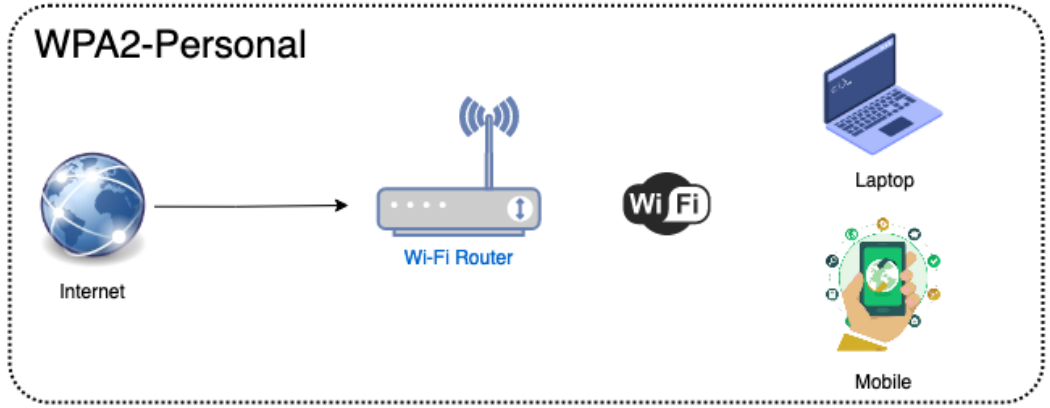
➢ **WPA/WPA2 (Wi-Fi Protected Access):** est un protocole de sécurité chiffré qui protège le trafic Internet sur les réseaux sans fil. Deuxième génération de la norme de sécurité Wi-Fi Protected Access, WPA2 corrige les failles plus anciennes et offre un chiffrement plus robuste. Ils cryptent les données transmises entre un appareil sans fil et un point d'accès sans fil, empêchant ainsi les pirates informatiques d'intercepter et de lire les données. De plus, ils permettent d'authentifier l'appareil sans fil et le point d'accès sans fil.

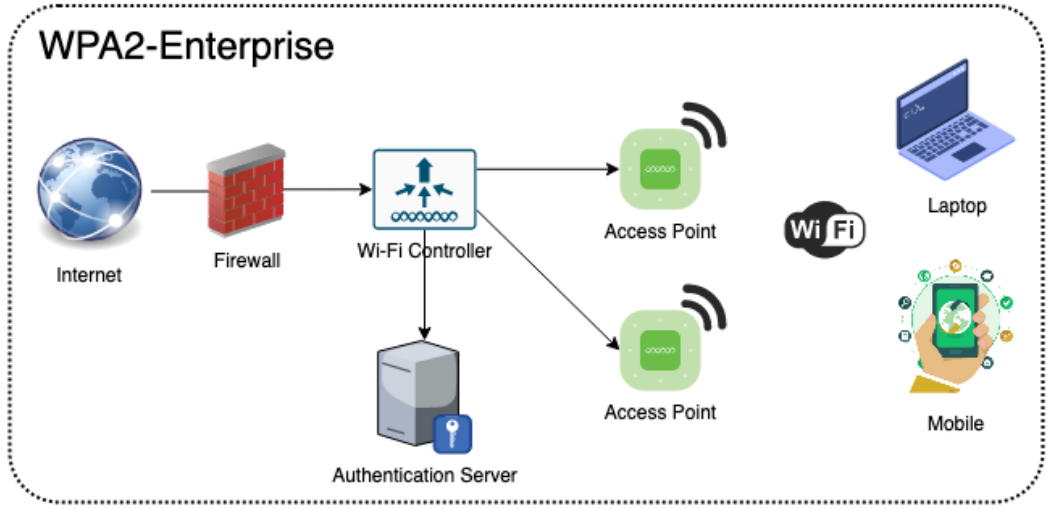
CHAPITRE II: Sécurité des réseaux

1. Protocoles de sécurité réseau

❑ Types courants de protocoles de sécurité réseau

➢ **WPA/WPA2 (Wi-Fi Protected Access)**



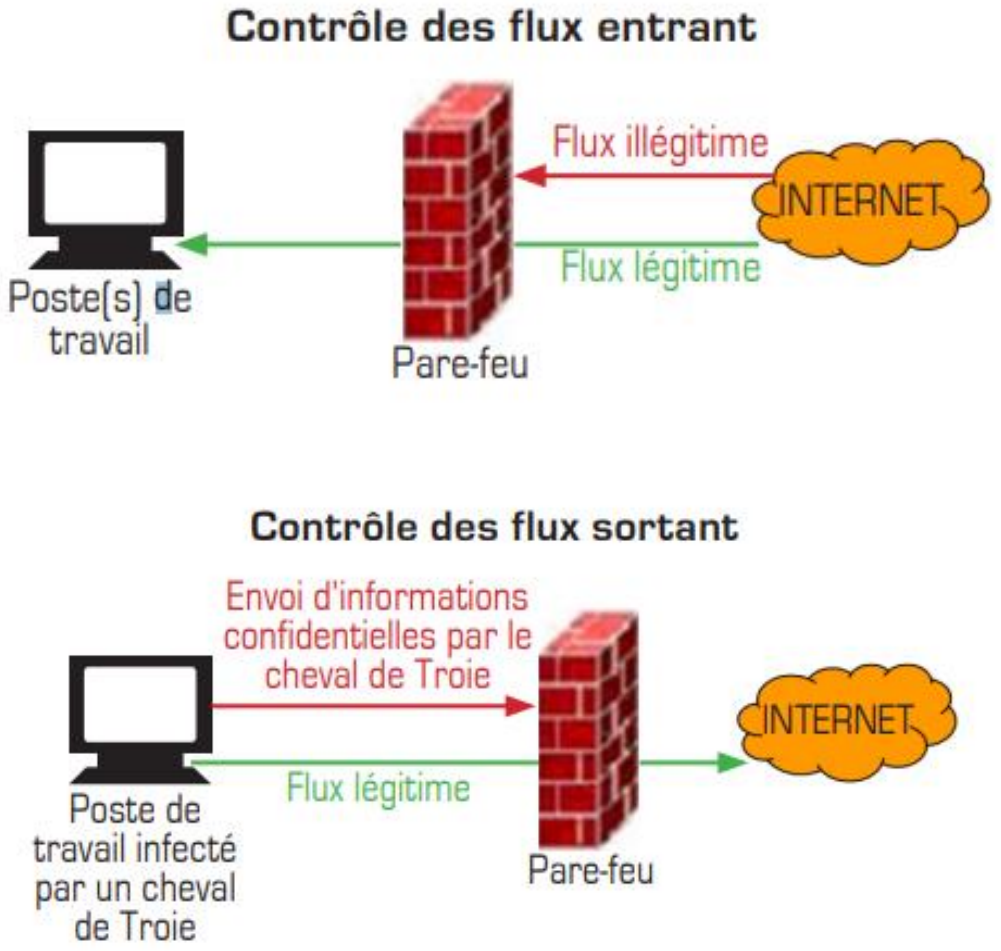


CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

Un pare-feu est un dispositif ou un logiciel qui permet de contrôler ce qui pénètre et ce qui sort d'un réseau. Toutes les entreprises utilisent un pare-feu pour protéger leur réseau interne du monde extérieur.

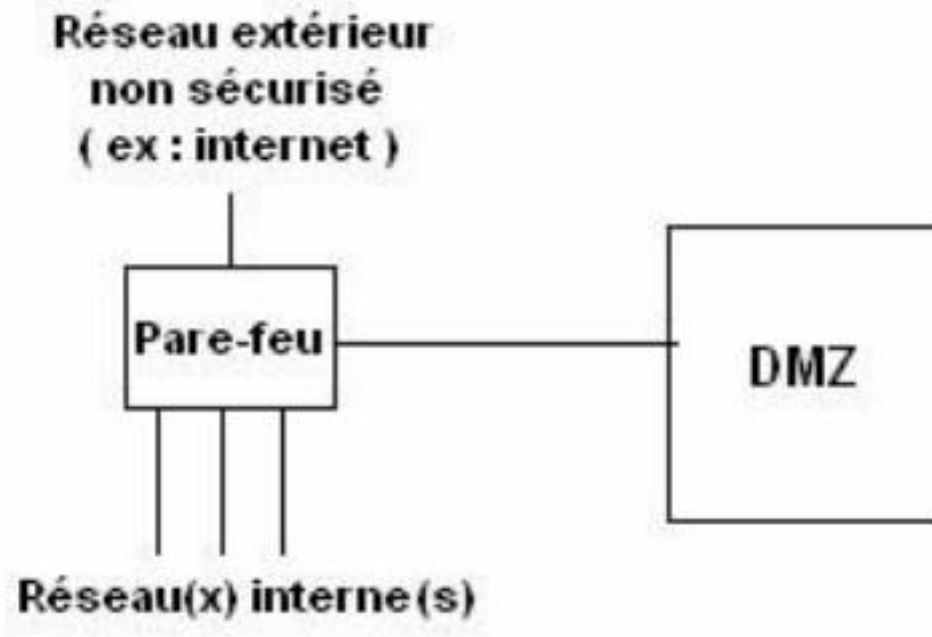
Le firewall Cisco fait partie de la gamme des pare-feu hardware, il est donc plus efficace sur des réseaux à gros débit, c'est pour cela qu'il est très répandu dans les réseaux des moyennes et grandes entreprises



CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

- Il permet de segmenter le réseau en trois parties
  - Le réseau extérieur
  - Le réseau interne
  - La DMZ (De-Militarized Zone) : zone démilitarisée, dans laquelle se trouvent les serveurs publics de l'entreprise, auxquels les réseau internes et externes auront accès.



- Il permet aussi le filtrage de paquets au niveau 3 et 4 de TCP/IP (couche réseau (IP) et couche transport (TCP-UDP-ICMP)), entre les différents réseaux.

CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

❑ Types de pare-feu

Il existe deux types principaux de pare-feu :

- Les pare-feux statiques utilisent des règles de filtrage prédéfinies pour autoriser ou bloquer le trafic. Ces règles sont généralement basées sur des paramètres tels que l'adresse IP source et de destination, le port et le protocole.

- Les pare-feux dynamiques utilisent des techniques plus sophistiquées pour analyser le trafic et identifier les menaces potentielles. Ces techniques peuvent inclure le filtrage basé sur le contenu, l'analyse des signatures de virus et l'analyse comportementale.

CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

❑ Principes de fonctionnement

Les pare-feux fonctionnent en filtrant le trafic entrant et sortant d'un réseau. Ils analysent chaque paquet de données et décident s'il doit être autorisé ou bloqué.

- **Filtrage de paquets** : Examens et autorisations/refus de paquets individuels en fonction de règles prédéfinies.
- **Filtrage de l'état** : Contrôle des connexions en fonction de leur état (état de la session).
- **Proxy** : Agit comme intermédiaire entre les utilisateurs et les serveurs pour filtrer le trafic.

CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

- **Règles de pare-feu** :

- **Autorisations** : Permettent le passage du trafic en fonction de critères tels que l'adresse IP, le port, le protocole, etc.

- **Refus** : Bloquent le trafic en fonction des mêmes critères.

CHAPITRE II: Sécurité des réseaux

2. Les pares-feux

- **Règles de pare-feu :**

- **Autorisations** : Permettent le passage du trafic en fonction de critères tels que l'adresse IP, le port, le protocole, etc.

- **Refus** : Bloquent le trafic en fonction des mêmes critères.

CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

❑ Systèmes de détection d'intrusion (IDS)

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network Based Intrusion Detection System) : ils assurent la sécurité au niveau du réseau.

- Les H-IDS (Host Based Intrusion Detection System) : ils assurent la sécurité au niveau des hôtes.

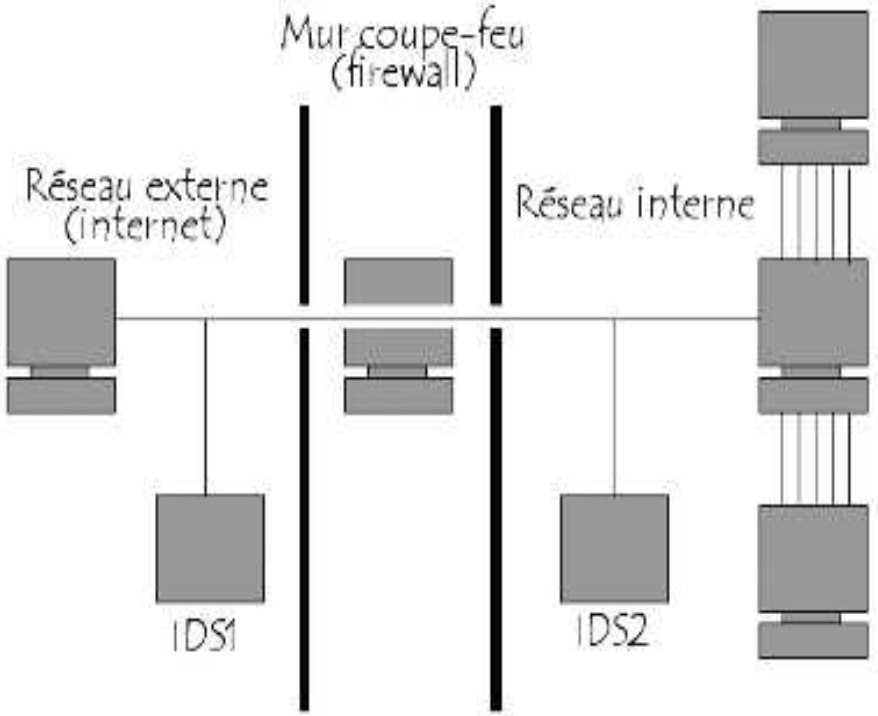
CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

❑ Systèmes de détection d'intrusion (IDS)

Un N-IDS nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs liens réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.

Il est fréquent de trouver plusieurs IDS à l'extérieur du réseau afin d'étudier les tentatives d'attaques ainsi en interne pour analyser les requêtes ayant traversé le pare-feu ou bien menées depuis l'intérieur.



CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

❑ Systèmes de détection d'intrusion (IDS)

Le H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Solaris, Linux, HP-UX, Aix, etc.

Le H-IDS se comporte comme un service standard sur un système hôte. Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (déni de services, backdoors, chevaux de Troie, tentatives d'accès non autorisés, exécution de codes malicieux, attaques par

débordement de tampon, etc.)..

CHAPITRE II: Sécurité des réseaux

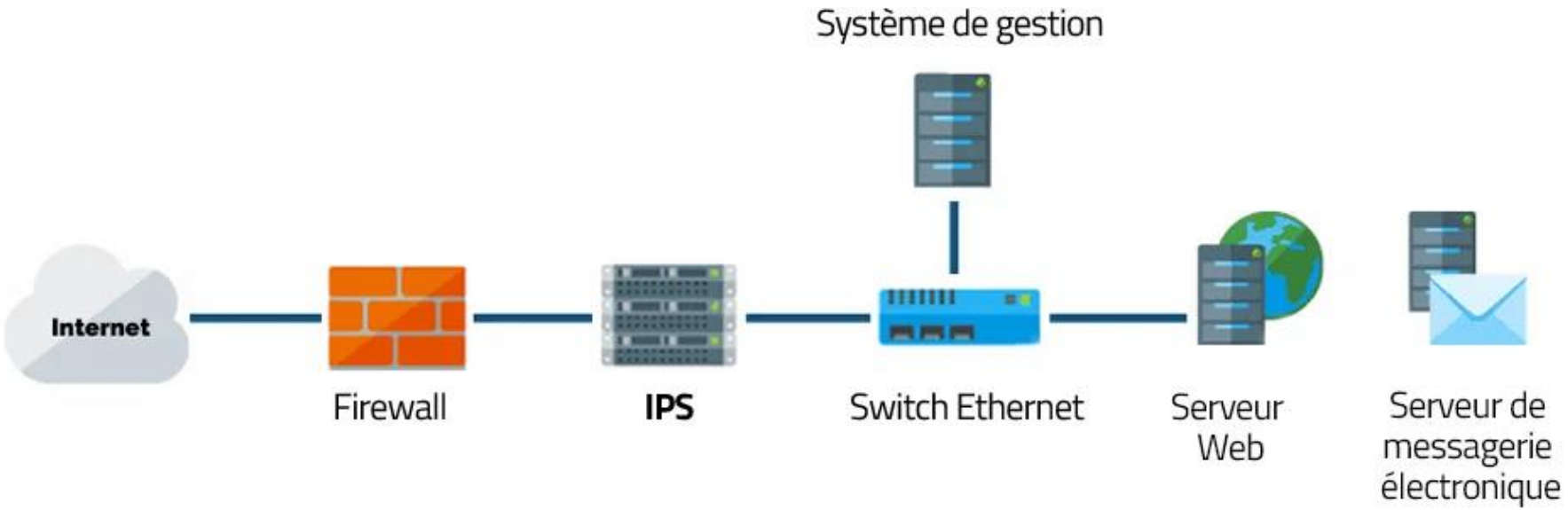
3. IDS/ IPS

- **Système de prévention des intrusions(IPS)**

Un système de prévention des intrusions (IPS) est un dispositif de sécurité réseau conçu pour repérer et stopper les menaces détectées. Il surveille de manière continue le réseau à la recherche d'activités malveillantes potentielles, collectant des données à leur sujet. L'IPS alerte les administrateurs en cas d'incidents et prend des mesures préventives telles que la fermeture des points d'accès et la reconfiguration des pares-feux pour éviter de futures attaques. En outre, les IPS peuvent être utilisés pour identifier les violations des politiques de sécurité de l'entreprise, décourageant ainsi les employés et les visiteurs du réseau de violer ces règles.

CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS



CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

- **Système de prévention des intrusions(IPS)**

➢ **fonctionnent les systèmes de prévention des intrusions**

Les systèmes de prévention des intrusions fonctionnent en analysant tout le trafic du réseau. Il existe un certain nombre de menaces différentes que les IPS peuvent empêcher, notamment :

- ✓ Attaque par déni de service (DDoS)
- ✓ Attaque par déni de service distribué
- ✓ Divers types de failles de sécurité
- ✓ Ver
- ✓ Virus

CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

❑ **Système de prévention des intrusions(IPS)**

➢ **fonctionnent les systèmes de prévention des intrusions**

L'IPS réalise une surveillance en temps réel des paquets en scrutant attentivement chaque transmission sur le réseau. En cas de détection de paquets suspects ou malveillants, l'IPS prendra l'une des mesures suivantes :

- ✓ ***Mettra fin à la session TCP*** qui a été exploitée et bloquera l'adresse IP source ou le compte utilisateur fautif pour empêcher l'accès non éthique à toute application, hôte cible ou ressource réseau.
- ✓ ***Reprogrammera ou reconfigurera le firewall*** pour éviter qu'une attaque similaire ne se reproduise à l'avenir.
- ✓ ***Supprimera ou remplacera tout contenu malveillant*** resté sur le réseau suite à une attaque. Cela est effectué en reconditionnant les charges, en supprimant les informations d'en-tête et en retirant toute pièce jointe infectée des serveurs de fichiers ou de courrier électronique.

CHAPITRE II: Sécurité des réseaux

3. IDS/ IPS

❑ **Système de prévention des intrusions(IPS)**

➢ **Types de prévention**

Un système de prévention des intrusions est habituellement paramétré pour employer diverses méthodes afin de sécuriser le réseau contre les accès non autorisés. Parmi ces méthodes, on peut mentionner:

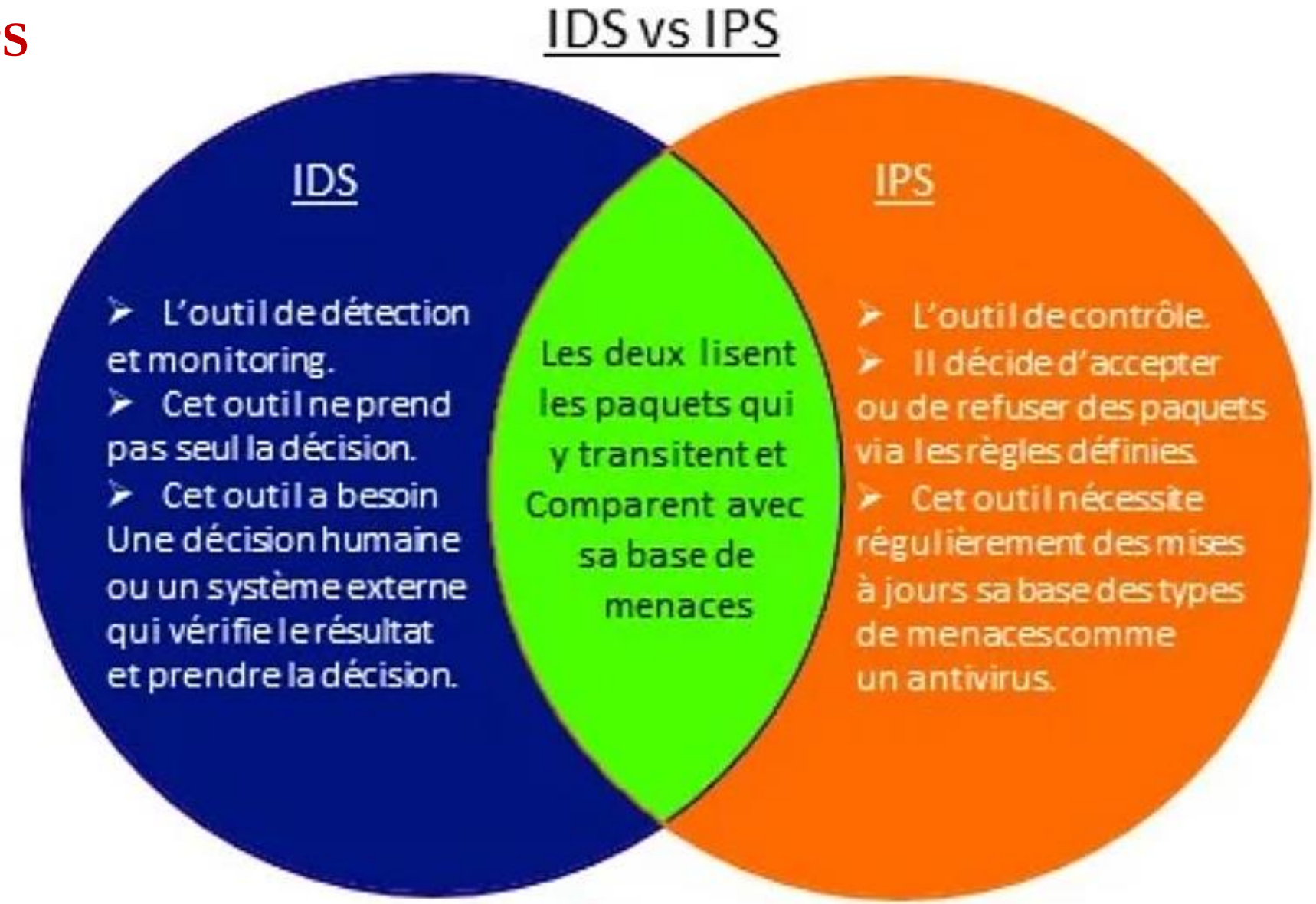
✓ ***Approche basée sur les signatures*** utilise des signatures prédéfinies de menaces réseau bien connues. Lorsqu'une attaque correspondant à l'une de ces signatures ou à l'un de ces modèles est lancée, le système prend les mesures nécessaires.

✓ ***Approche basée sur les anomalies*** Permet de surveiller tout comportement anormal ou inattendu sur le réseau. Si une anomalie est détectée, le système bloque immédiatement l'accès à l'hôte cible.

✓ ***Approche basée sur les politiques,*** lorsqu'une activité viole une politique de sécurité, une alerte est déclenchée et envoyée aux administrateurs système.

CHAPITRE II: Sécurité des réseaux

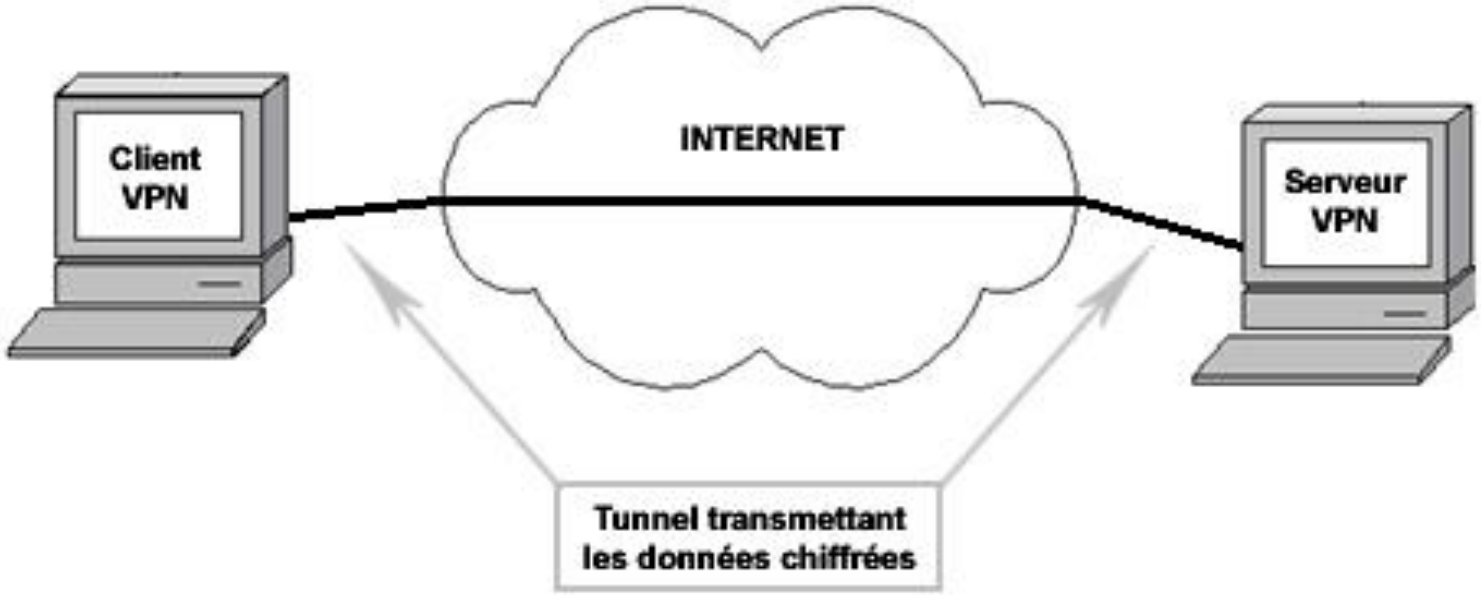
3. IDS/ IPS



CHAPITRE II: Sécurité des réseaux

4. Réseau privé virtuel (VPN)

Un réseau privé virtuel, étend un réseau privé à travers un réseau public tel qu'Internet. Il offre aux utilisateurs la possibilité de transférer des données sur des réseaux partagés ou publics comme s'ils étaient directement connectés au réseau privé. Les applications VPN sont compatibles avec une grande variété d'appareils, incluant les smartphones, les tablettes, les ordinateurs portables et les ordinateurs de bureau.



CHAPITRE II: Sécurité des réseaux

4. Réseau privé virtuel (VPN)

❑ Avantages de l'utilisation d'un VPN

- ✓ ***Sécurité*** : Les VPN cryptent le trafic Internet, ce qui le rend difficile à lire pour les pirates informatiques et autres regards indiscrets.

- ✓ ***Confidentialité*** : Les VPN masquent votre adresse IP, ce qui rend plus difficile le suivi de votre activité en ligne.

- ✓ ***Contournement des restrictions géographiques*** : Les VPN peuvent être utilisés pour accéder à des sites Web et à des services restreints dans votre région.

CHAPITRE II: Sécurité des réseaux

4. Réseau privé virtuel (VPN)

❑ Inconvénients de l'utilisation d'un VPN

- ✓ ***Coût :*** Les VPN peuvent être coûteux, en particulier si vous choisissez un service premium.
- ✓ ***Vitesse :*** Les VPN peuvent ralentir votre connexion Internet.
- ✓ ***Compatibilité :*** Les VPN ne sont pas compatibles avec tous les appareils et services

CHAPITRE II: Sécurité des réseaux

4. Réseau privé virtuel (VPN)

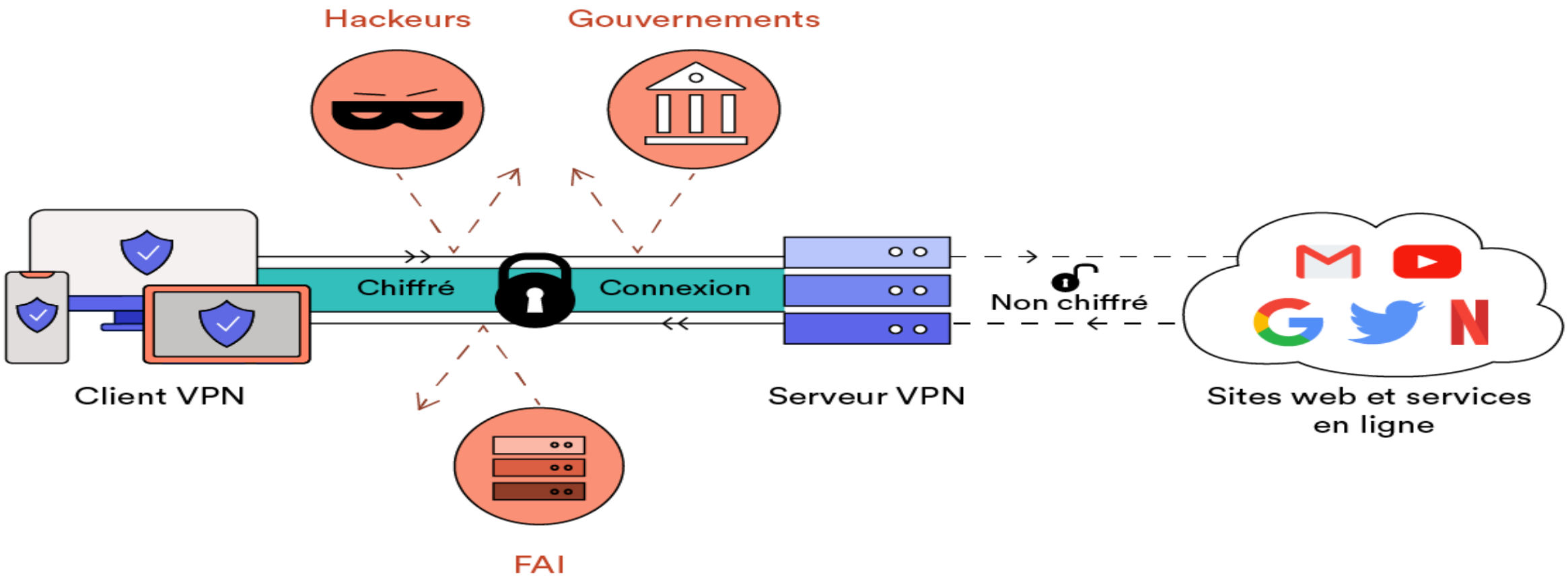
❑ Fonctionnement du VPN

Un réseau privé virtuel (VPN) achemine les données de votre appareil vers un serveur distant avant de les transmettre à des destinataires sur Internet. Voici les principes fondamentaux de cette technologie :

- ✓ ***Protocole de tunneling:*** Un réseau privé virtuel établit essentiellement une connexion sécurisée à travers un tunnel de données entre votre appareil local et un serveur VPN distant, souvent situé à des distances considérables. En naviguant en ligne, toutes vos données passent par ce serveur VPN, rendant ainsi votre fournisseur d'accès Internet (FAI) et d'autres tiers incapables de visualiser le contenu de votre trafic Internet. de tunneling.

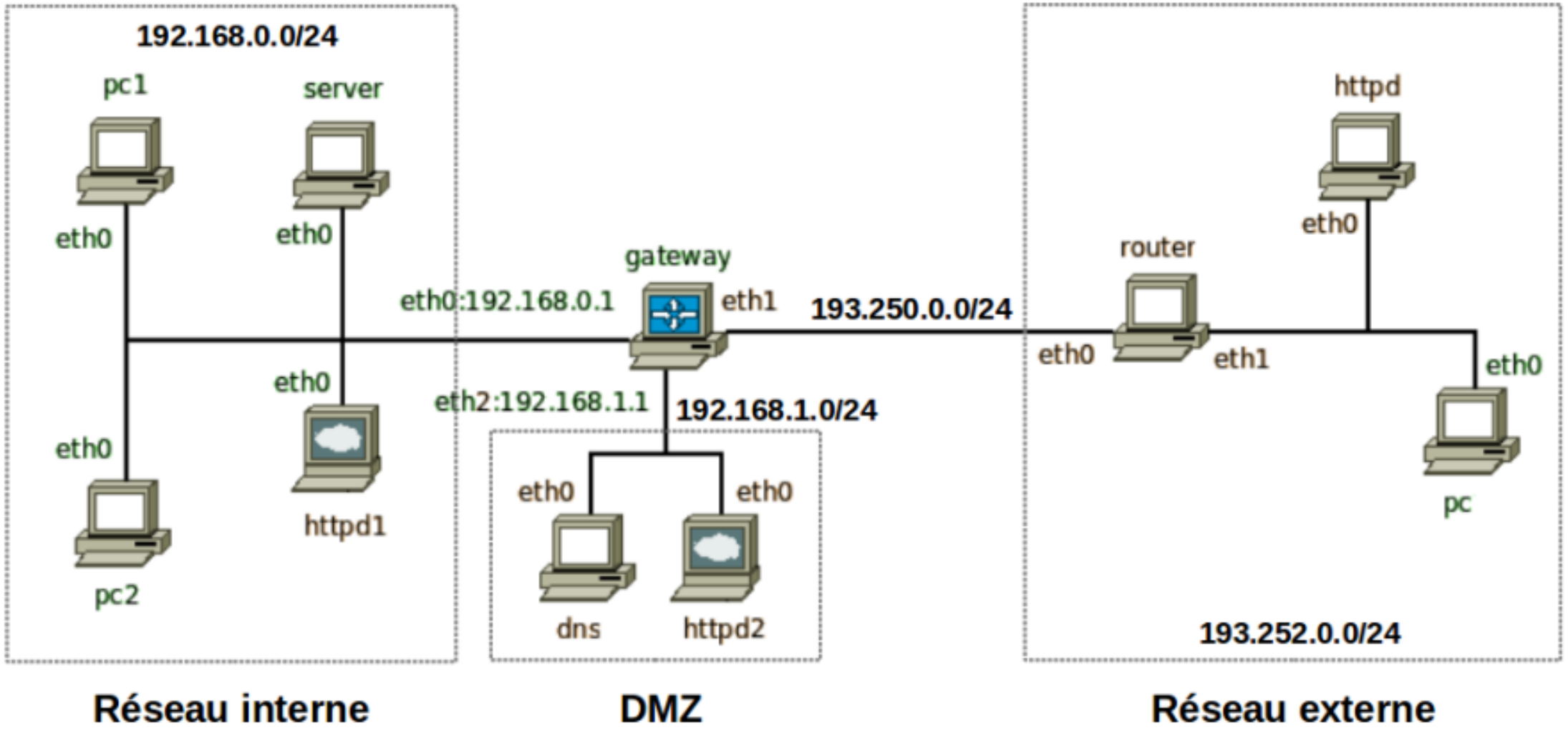
CHAPITRE II: Sécurité des réseaux

4. Réseau privé virtuel (VPN)



CHAPITRE II: Sécurité des réseaux

5. TP



CHAPITRE II: Sécurité des réseaux

5. TP

Exercice 1 : **Configurer un pare-feu statique**

1. Ouvrir Packet Tracer et créer un nouveau projet
2. Ajout d'un pare-feu, de deux ordinateurs sur le réseau interne et d'un ordinateur sur le réseau externe
3. Configuration de l'adressage IP des périphériques
4. Configuration du pare-feu
   a) Activation e pare-feu
   b) Ajout 'd'une règle filtrage pour autoriser le trafic TCP et UDP entre le réseau interne et le réseau externe sur tous les ports
5. Testez la configuration en envoyant un message du trafic entre les ordinateurs du réseau interne et du réseau externe

CHAPITRE II: Sécurité des réseaux

5. TP

Exercice 2 : Configurer un pare-feu dynamique

1. Configuration du pare-feu

2. Ajout d’une règle de filtrage pour autoriser le trafic TCP et UDP entre le réseau interne et le réseau externe sur les ports 80 et 443

3. Ajout d’une règle de filtrage pour bloquer tout le trafic provenant d'un autre ordinateur sur le réseau externe

4. Test de la configuration en envoyant un message du trafic entre les ordinateurs du réseau interne et du réseau externe.