Architecture de Sécurité des Réseaux Informatiques

Module: Sécurité Informatique

2023/2024

Objectifs

Après avoir suivi ce chapitre, vous serez capables de :

- ✔ **Comprendre le contrôle d'accès; principe, terminologies et différents modèles**
- ✔ **Comprendre les apports de la sécurité pour les réseaux**
- ✔ **Présenter les solutions essentielles de sécurité réseau**
- ✔ **Identifier les types de firewalls et leurs usages**
- ✔ **Concevoir des règles firewalls en fonction des besoins**
- ✔ **Décrire le fonctionnement des systèmes de détection d'intrusions, leurs différents types, et comment évaluer leur performance.**
- ✔ **Introduire la notion de réseaux privés virtuels (VPN)**
- ✔ **Positionner les protocoles de sécurité phares qui assurent la sécurité des VPNs**

Plan

- Introduction au contrôle d’accès
- Les firewalls
- Les Systèmes de Détection et de Prévention d’intrusions (IDS/IPS)
- Introduction aux Réseaux Privés Virtuels (VPN)

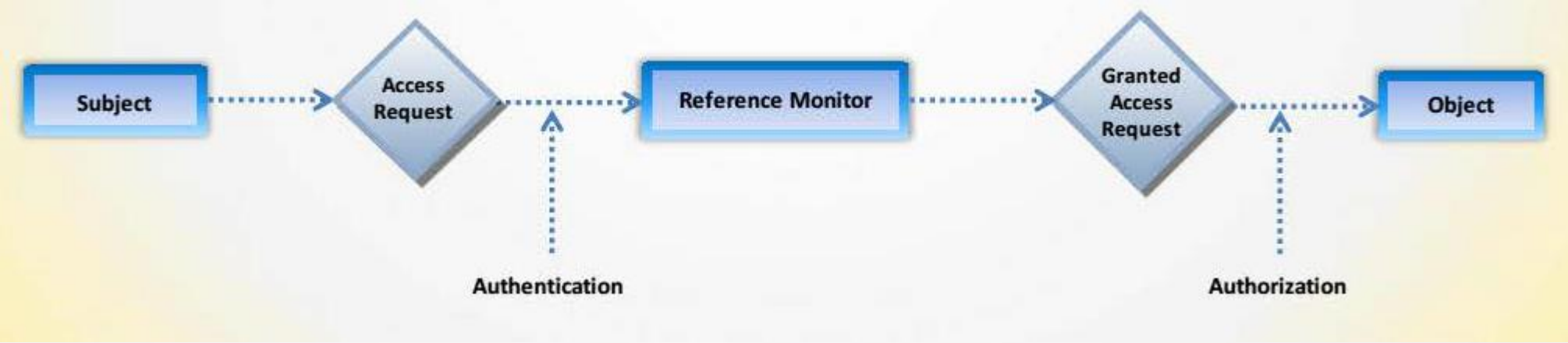
Introduction

Le contrôle d’Accès

Contrôle d'Accès

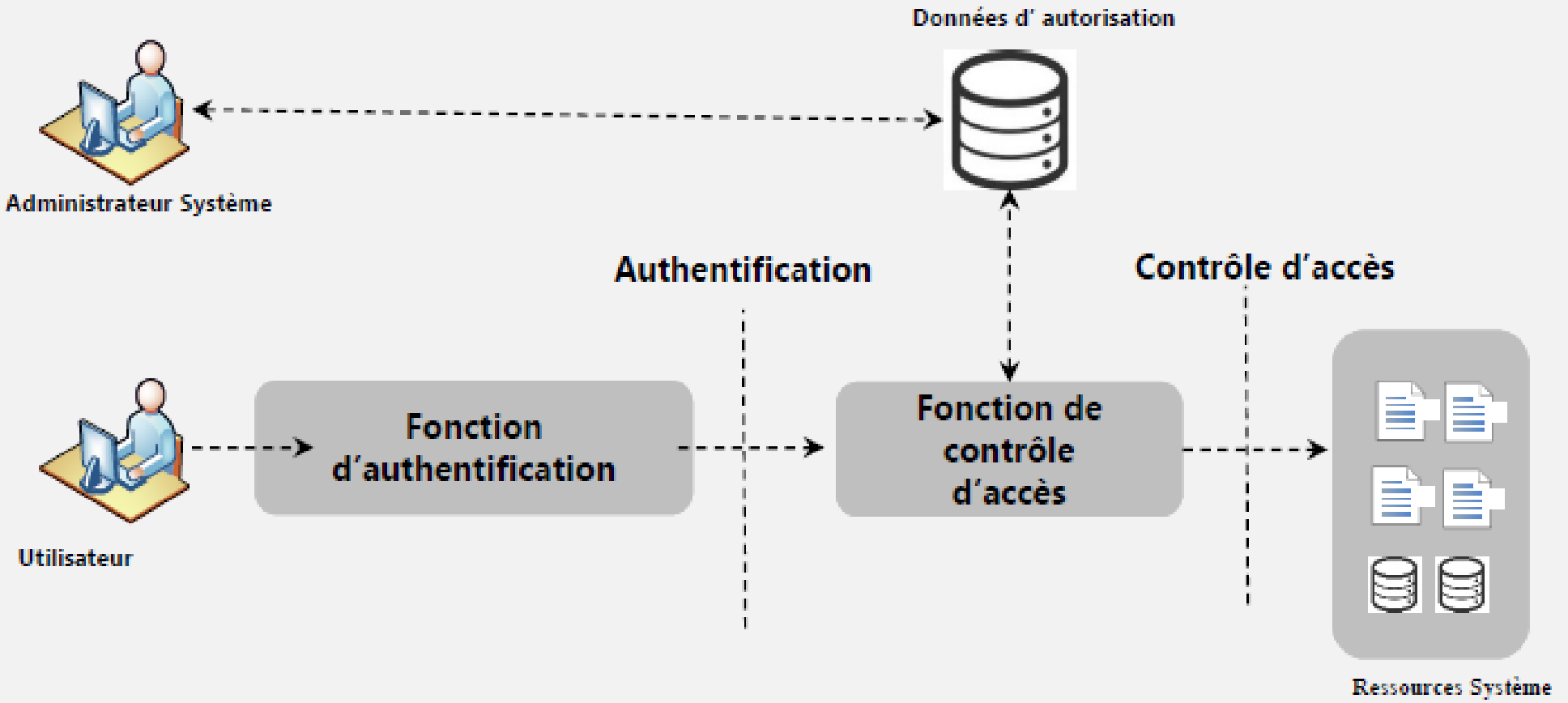
Terminologie

- **Sujet :** cela fait référence à un utilisateur ou à un processus particulier qui souhaite accéder à une ressource
- **Objet :** Il s'agit d'une ressource spécifique à laquelle l'utilisateur souhaite accéder, comme un fichier ou un périphérique matériel Référence
- **Superviseur :** Il vérifie la règle de contrôle d'accès pour des restrictions spécifiques
- **Opération :** Elle représente une action effectuée par un sujet sur un objet



Contrôle d'Accès

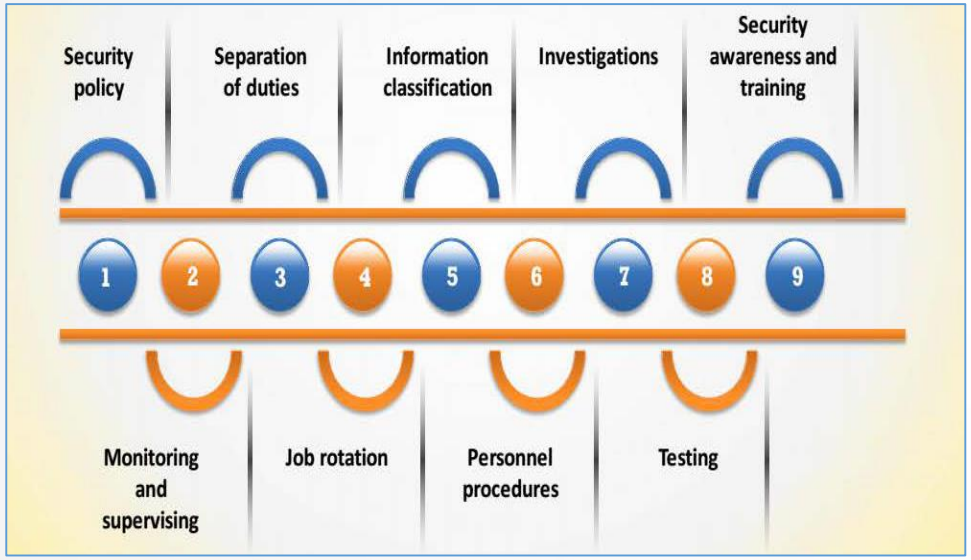
Principe



Exemples de Contrôle d’accès:

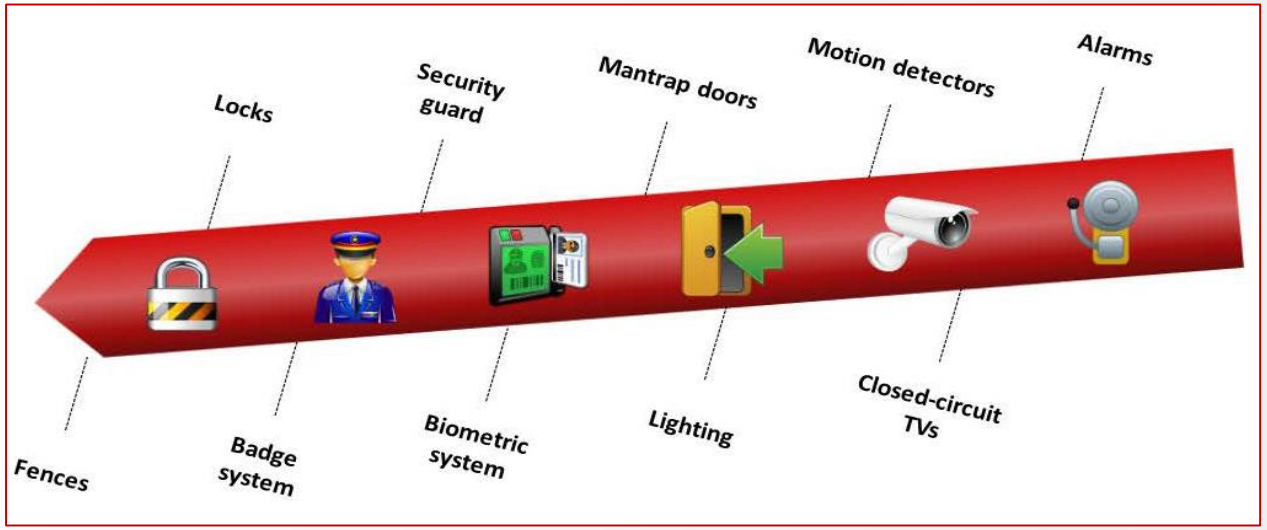
- **Administratif:**

La direction met en place des contrôles d'accès administratifs pour assurer la sécurité de l'organisation



- **Physique:**

Il s'agit d'un ensemble de mesures de sécurité prises pour empêcher l'accès non autorisé aux ressources physiques



- **Technique:**

C'est un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité des ressources

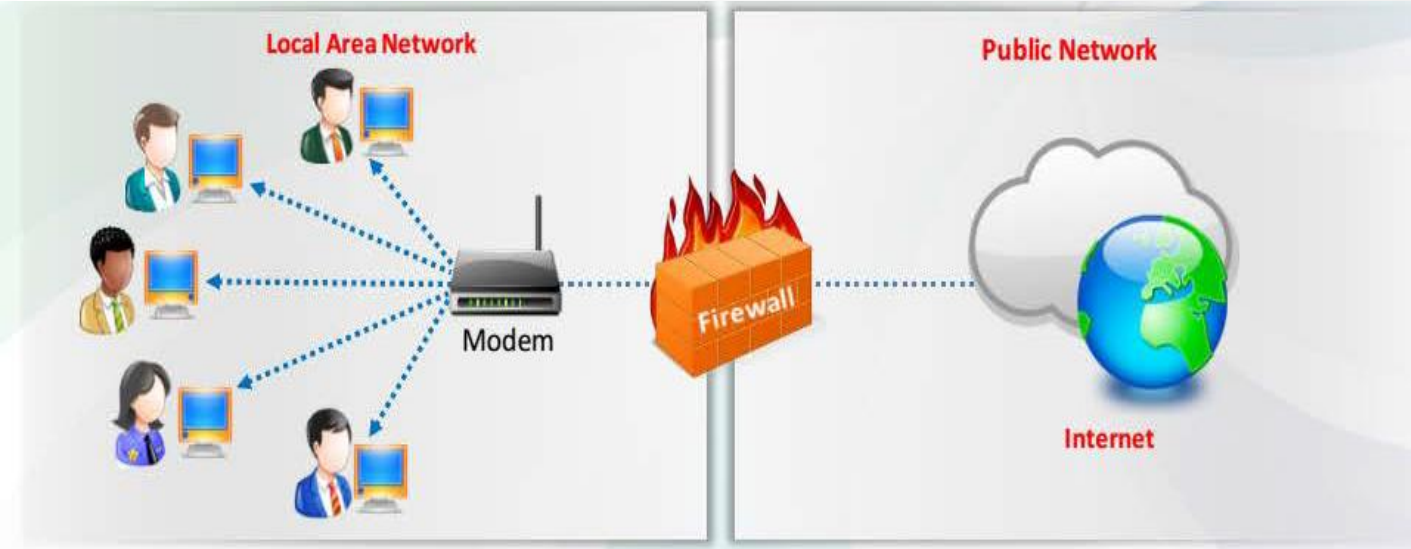
Plan

- Introduction au contrôle d’accès
- Les firewalls
- Les Systèmes de Détection et de Prévention d’intrusions (IDS/IPS)
- Introduction aux Réseaux Privés Virtuels (VPN)

Les Firewalls

Définition

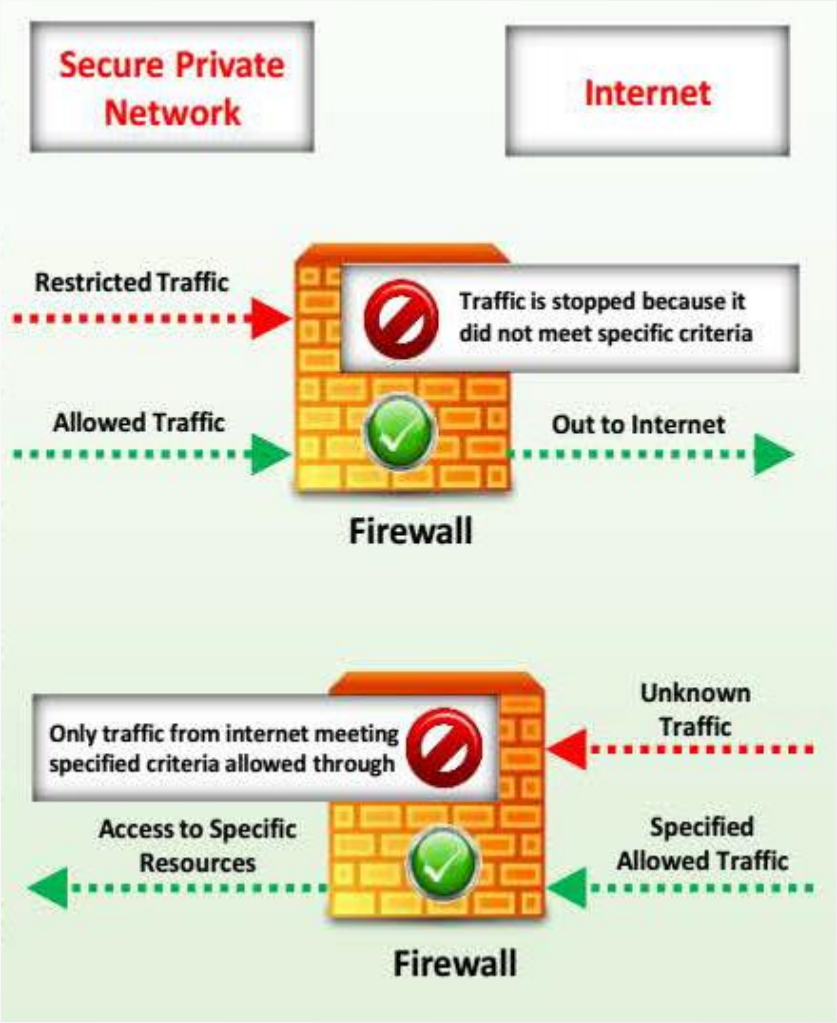
- Un **pare-feu** (*firewall* en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet).
- Un firewall peut être matériel ou logiciel
- Le pare-feu est permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum deux interfaces réseau:
  - ✔ une interface pour le réseau à protéger (réseau interne) ;
  - ✔ une interface pour le réseau externe.



Les Firewalls

Fonctionnement d’un firewall

- Un pare-feu fonctionne sur le principe suivant :
  - ✔ Un pare-feu laisse passer le trafic si le trafic répond à certains critères
  - ✔ Un pare-feu refuse le trafic s'il ne correspond pas à certains critères
- Ces critères sont les règles et restrictions configurées sur le pare-feu et cela peut varier d'un type de pare-feu à l'autre
- Généralement, un pare-feu filtre le trafic en fonction du type de trafic, des adresses source ou de destination, des protocoles et des ports



Les technologies de firewalls

Filtrage par paquet	Filtrage via circuit	Proxy
Filtrage dynamique	Firewall applicatif	Filtrage multicouches

Pour plus de détails:
voir Annexe 1

Les différentes technologies dépendent des couches (3, 4, 5, 6 ou bien 7) du modèle OSI

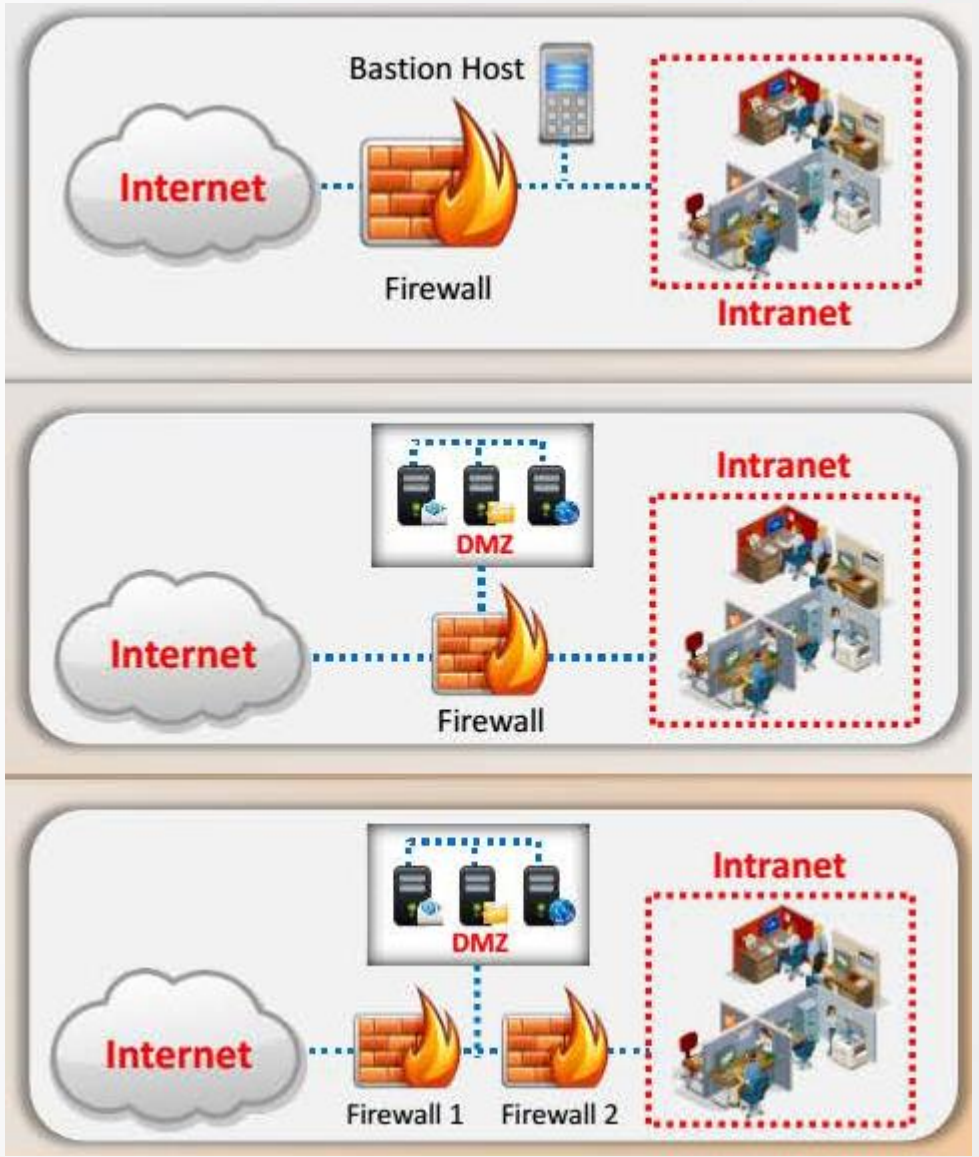
Les Firewalls

Les topologies de firewalls

- **Bastion host :** c’est un système informatique conçu et configuré pour protéger les ressources réseau contre une attaque. Il est placé entre deux réseaux et agit comme une passerelle au niveau de l'application Le trafic entrant ou sortant du réseau passe par un pare-feu, qui a deux interfaces :

- L'interface publique est directement connectée à Internet
- L'interface privée est connectée à l'Intranet

- **Screened subnet ou DMZ :** contient des hôtes qui offrent des services publics La zone publique est connectée directement à Internet et n'a pas d'hôtes contrôlés par l'organisation La zone privée est constituée de systèmes auxquels les internautes n'ont aucun accès professionnel.
- **Multi-homed firewall:** Ce type de pare-feu se compose de trois interfaces qui permettent de subdiviser davantage les systèmes en fonction d'objectifs de sécurité spécifiques dans l'organisation.

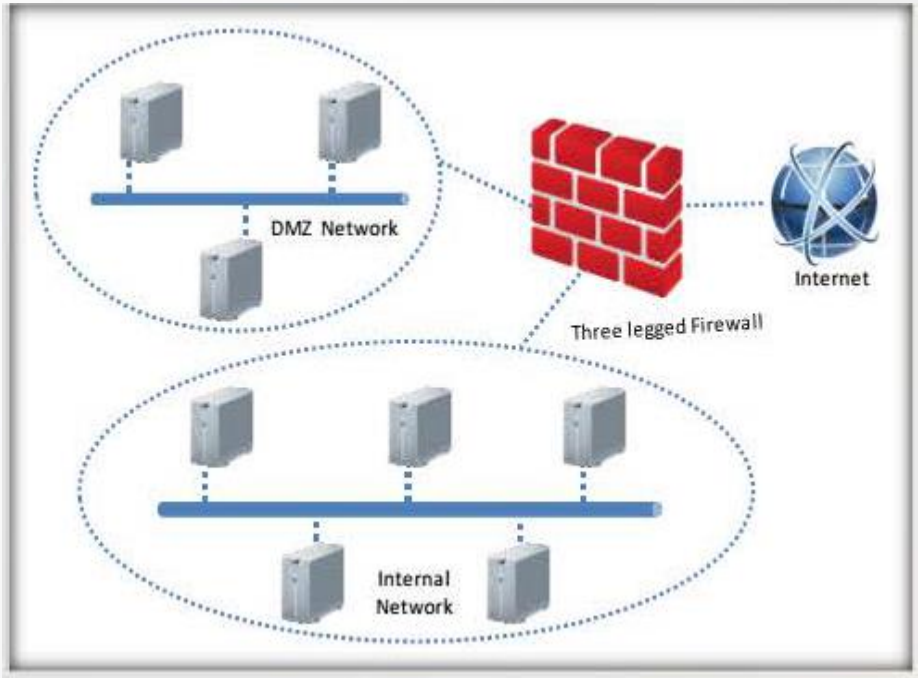


Les Firewalls

DMZ

Une zone **DMZ** (**DeMilitarized Zone**) est une zone de réseau privée ne faisant partie ni du LAN privé ni de l'Internet. Concrètement, c'est une machine ou un réseau placé comme un réseau neutre entre le réseau privé (Intranet) et le réseau public (Internet) pour empêcher tout accès du réseau public vers les ressources et données du réseau privé. Elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes que le LAN.

- Contient les serveurs qui doivent être accessible depuis un réseau extérieur:
  - ✔ Serveurs Web
  - ✔ Serveurs de messagerie
  - ✔ Serveurs DNS
- **Configurations DMZ:**
  - ✔ Les réseaux internes et externes peuvent se connecter à la DMZ
  - ✔ Les hôtes de la DMZ peuvent se connecter aux réseaux externes
  - ✔ Mais les hôtes de la DMZ ne peuvent pas se connecter réseaux internes



Récapitulatif: Ce que fait et ce que ne fait pas un firewall

- ✔ Prévenir des scans réseau
- ✔ Contrôle du trafic
- ✔ Authentification des utilisateurs
- ✔ Filtrage des paquets, services et protocoles
- ✔ Journalisation
- ✔ Translation d'adresse réseau

- x Ne prévient pas des backdoors
- x Ne protège pas des menaces internes
- x N'est pas une alternative aux antivirus et antimalwares
- x Ne prévient pas contre les attaques de social engineering
- x Ne prévient pas contre la mauvaise utilisations des mots de passe

Critères de choix d'un firewall

- **Type de filtre et la nature de filtrage:**
  - ✔ **La nature et le nombre d'application appréhendées (FTP, messagerie, HTTP, SNMP, RealAudio, etc.)**
- **Facilité à enregistrer les actions (login, paramètres de connexion, ...) à des fins d'audit**
- **Facilité d'administration**
  - ✔ **Interface graphique ou ligne de commandes, administration distante après authentification du gestionnaire**
- **Simplicité du système pare-feu (facile à comprendre par le(s) administrateur(s))**
- **Capacité à supporter un tunnel chiffré**
- **La possibilité d'effectuer de l'équilibrage de charge / Haute disponibilité.**
- **Le dimensionnement du firewall:**
  - ✔ **Nombre de pattes nécessaires (inside, outside, DMZ)**

Hardware Firewalls

Software Firewalls

Mise en Pratique: Solution Logicielle

- Pour mettre en place un firewall logiciel:
  1. Rédiger/décrire la politique de sécurité (description textuelle)
  2. Installer une application firewall
  3. Configurer l'application firewall
  4. Traduire la politique de sécurité en un ensemble de règles de contrôle d'accès: ACL (access control list)
  5. Mettre à jour et relancer l'application firewall afin de déployer la nouvelle ACL

Mise en Pratique: Solution Logicielle

Règles de Sécurité:

- Un système pare-feu contient un ensemble de règles prédéfinies permettant:
  - D'autoriser la connexion (**allow**) ;
  - De bloquer la connexion (**deny**) ;
  - De rejeter la demande de connexion sans avertir l'émetteur (**drop**).
- L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité.

- On distingue habituellement deux types de politiques de sécurité permettant :

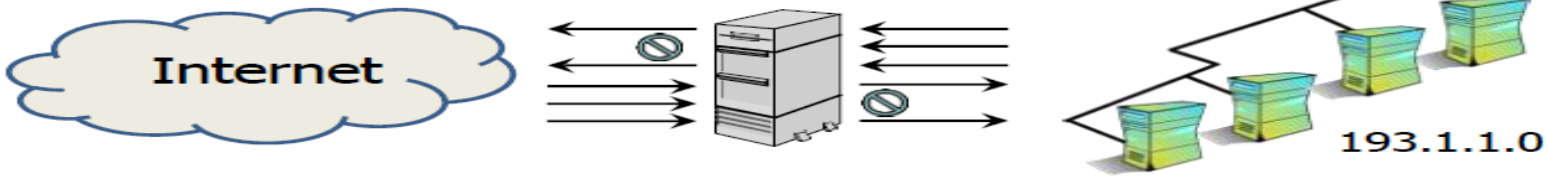
soit **d'autoriser** uniquement les communications ayant été explicitement autorisées

soit **d'empêcher** les échanges qui ont été explicitement interdits.

- La première méthode est la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Mise en Pratique: Solution Logicielle

Règles de Sécurité: Exemple



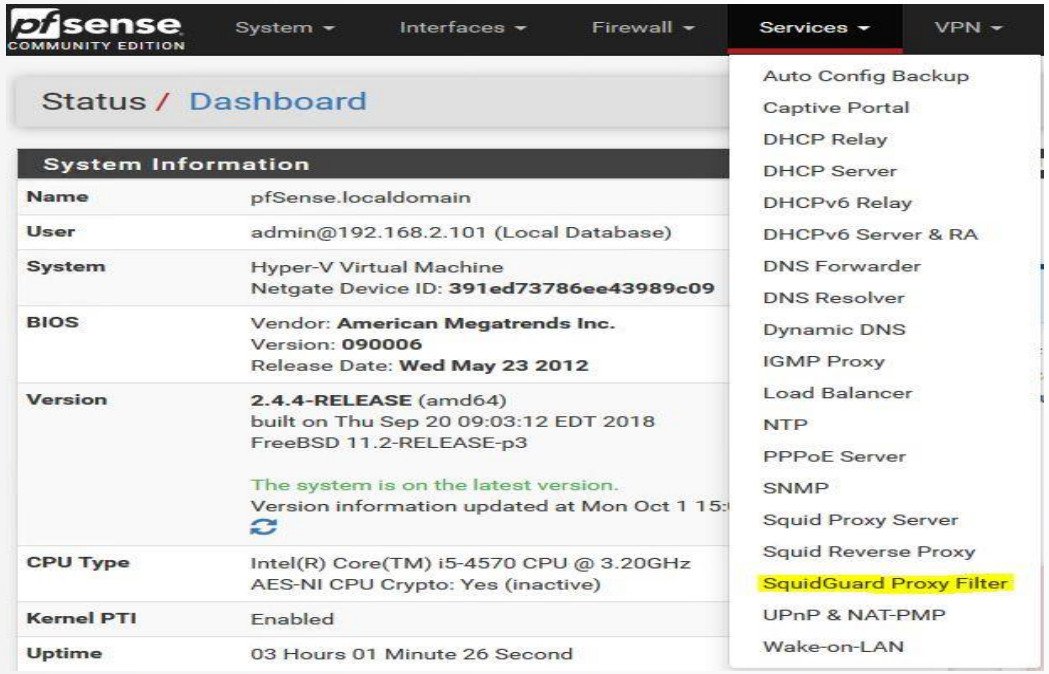
Action	Protocole	source	port	destination	Port	flag
Deny	IP	193.1.1.0	*	10.1.1.1	*	
Allow	TCP	193.1.1.0	*	*	80	
Allow	TCP	*	80	193.1.1.0	*	ACK
Drop	IP	*	*	*	*	

- **Règle1**: Toute connexion depuis le réseau interne (193.1.1.0) vers le serveur distant 10.1.1.1 est bloquée.
- **Règle2**: Seulement les connexions HTTP (TCP, port 80) depuis le réseaux interne (193.1.1.0), sont permises.
- **Règle3**: Seulement le trafic web en réponse à une connexion déjà initiée du réseau interne sera accepté de l'extérieur.
- **Règle4**: Interdiction par défaut.

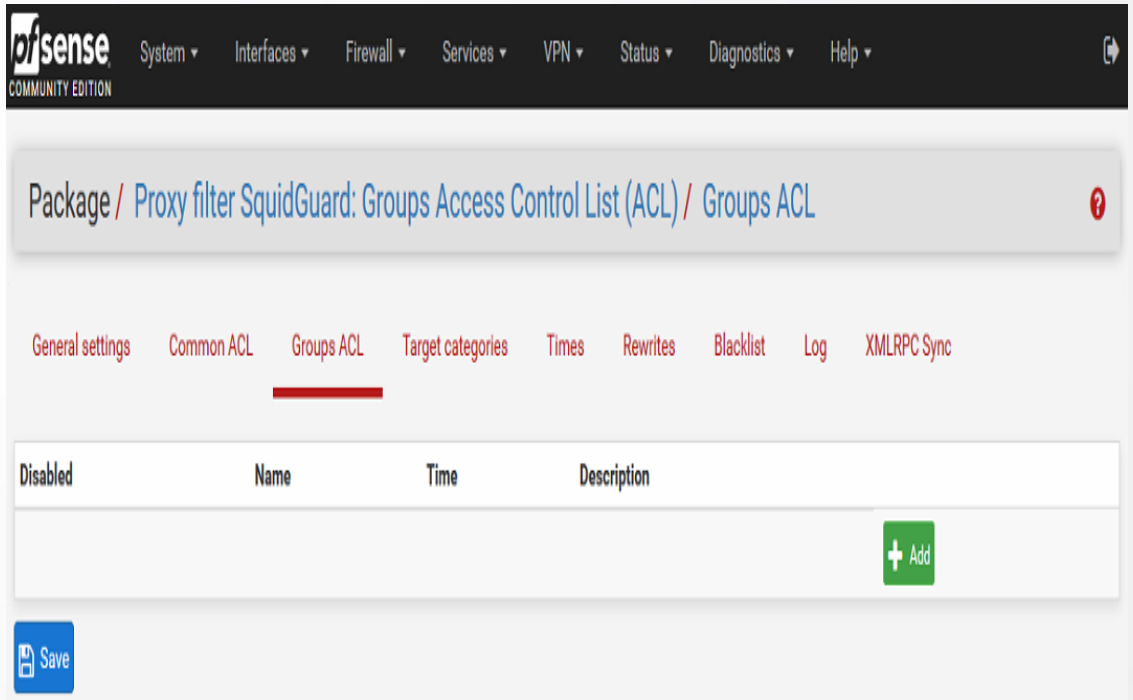
Mise en Pratique: Solution Logicielle

Règles de Sécurité: Exemple avec pfsense

1: Configuration des IP de Confiance dans SquidGuard
Sélectionner “Services” et “SquidGuard Proxy Filter”



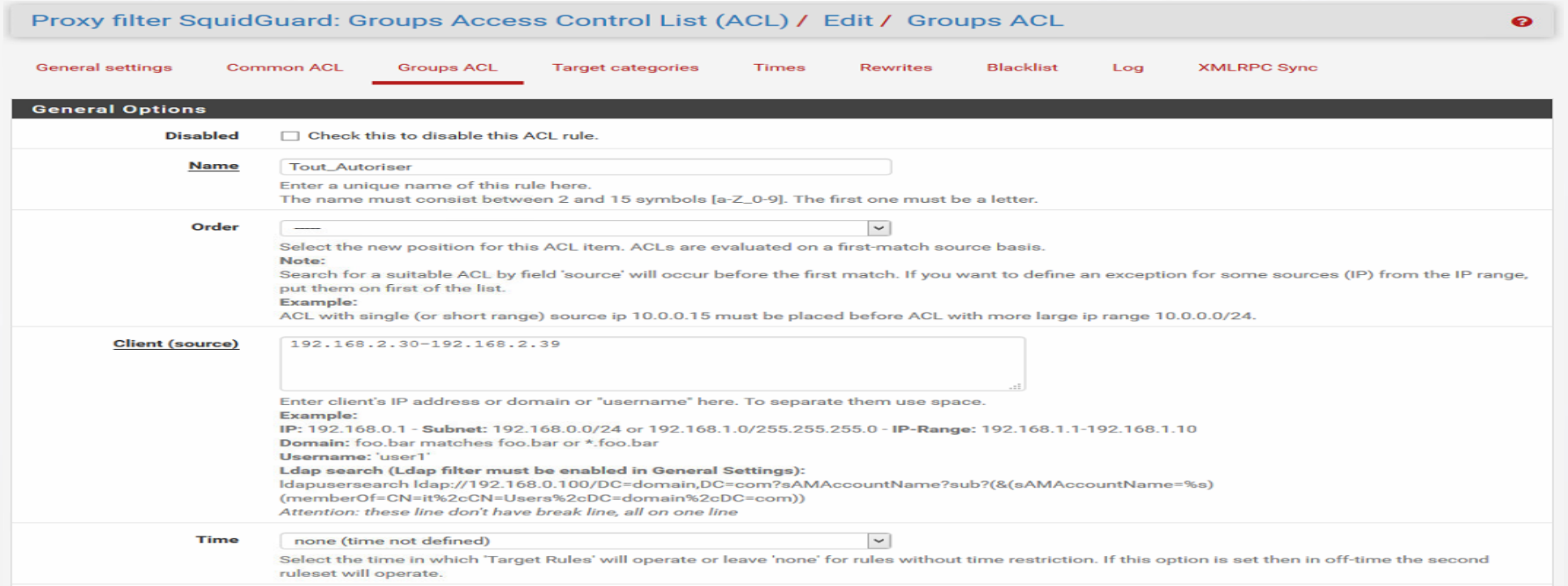
2: Sélectionner « **Groups ACL** » et cliquer sur “**Add**”



Mise en Pratique: Solution Logicielle

Règles de Sécurité: Exemple avec pfsense

3: Donner un « **Nom** » à cette règle de contrôle d'accès. Exemple : « **Tout_Autoriser** »
Client (source) : Indiquer la ou les **IP** des **ordinateurs** qui ne seront pas soumis au filtrage URL :
•Soit les IP, une à une, séparées par un espace. (Sur une seule ligne et sans retour à la ligne)
•Soit une **plage d'adresse IP**, comme dans la capture d'écran ci-dessous. (Sans espace, séparée par un tiret, sur une seule ligne et sans retour à la ligne)
•Ou bien les 2 – Exemple : 192.168.2.30-192.168.2.39 192.168.2.95 192.168.2.100



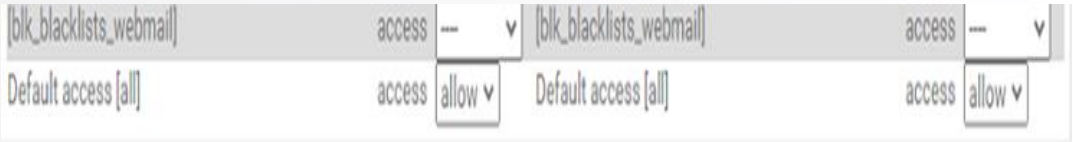
Mise en Pratique: Solution Logicielle

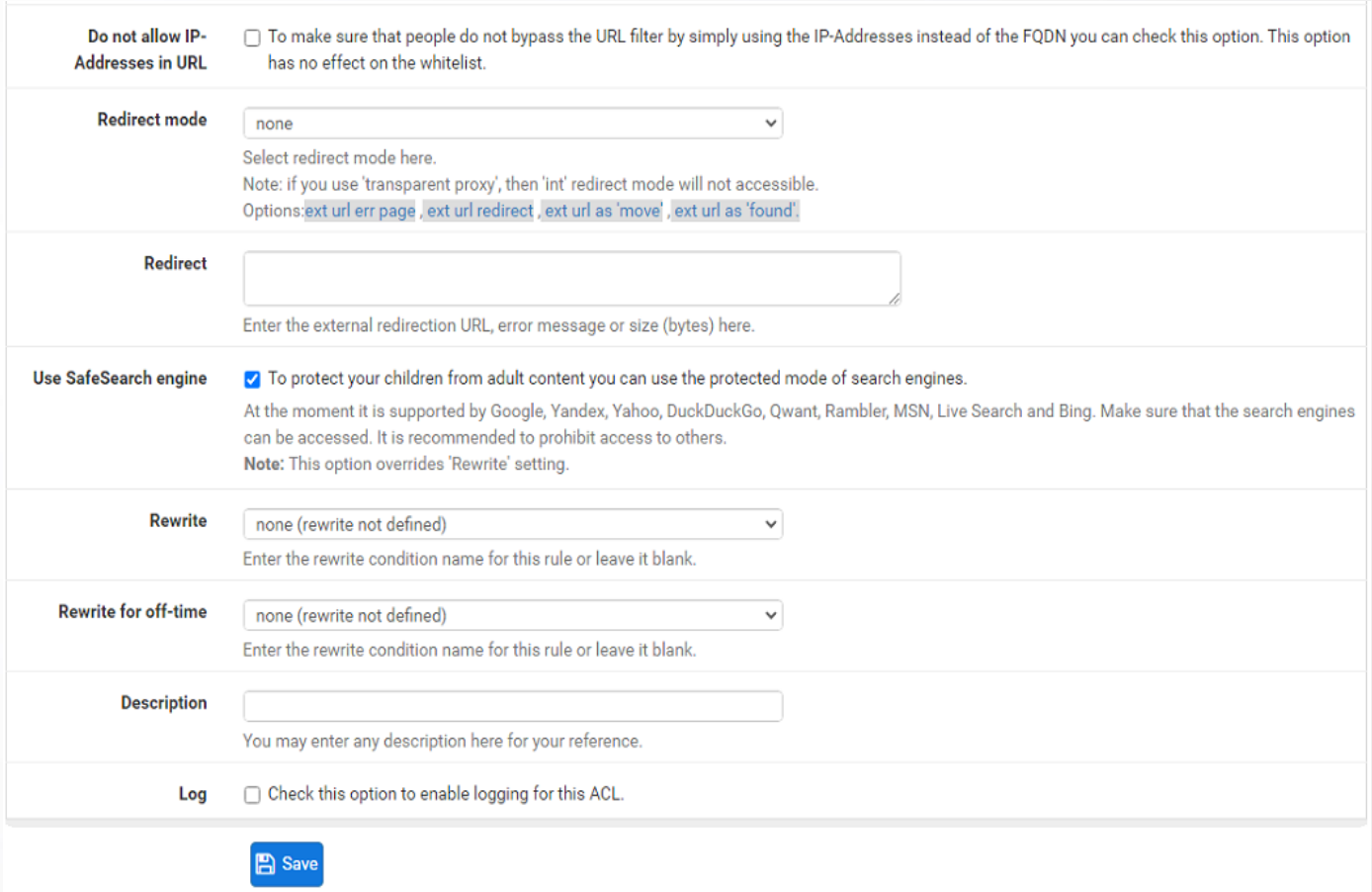
Règles de Sécurité: Exemple avec pfsense

4: Cliquez, dans "**Target Rules List**" sur le " **+** "

5: Sélectionner "**Allow**" pour "**Default access [all]**"

6: Cocher "**Use SafeSearch engine**" – (*Ne pas cocher "Do not allow IP addresses in URL »)*



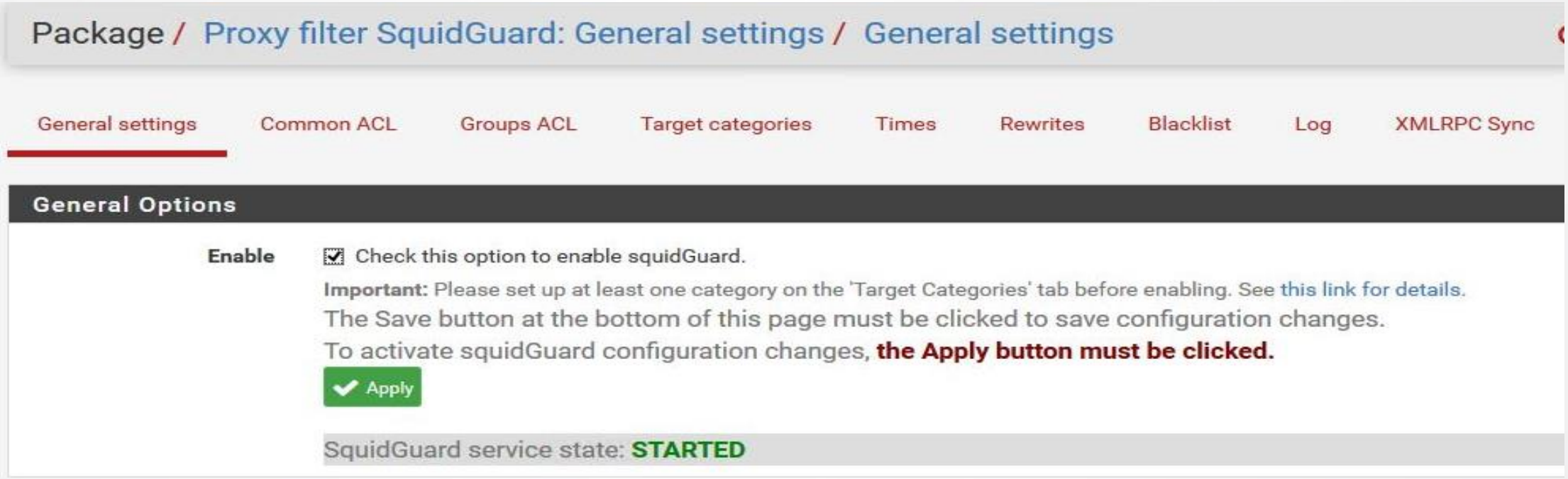


Mise en Pratique: Solution Logicielle

Règles de Sécurité: Exemple avec pfsense

7: Après avoir sauvegardé, le « **Groups ACL** » est enregistré.

8: TRES IMPORTANT : Pour valider les paramétrages, retournez sur l'onglet "**General settings**" et cliquez sur "**Apply**"



Plan

- Introduction au contrôle d’accès
- Les firewalls
- Les Systèmes de Détection et de Prévention d’intrusions (IDS/IPS)
- Introduction aux Réseaux Privés Virtuels (VPN)

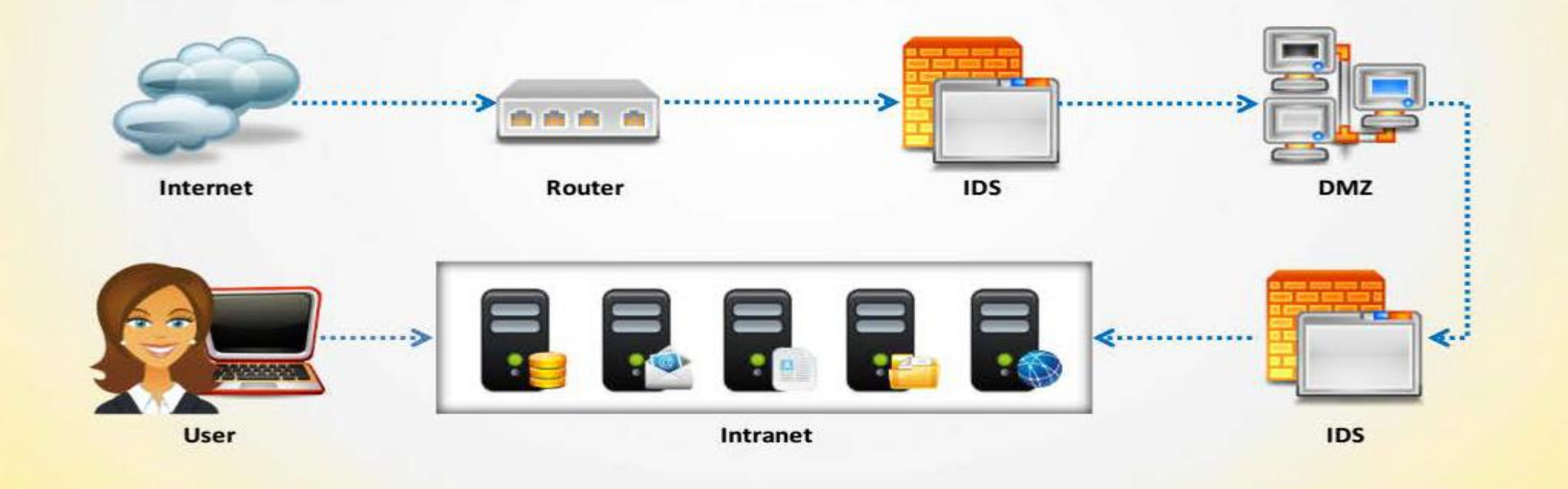
Une intrusion: c'est quoi?

- **L'intrusion** c'est quoi.
- Qui peut être des intrus
- **La détection d'intrusion** c'est quoi.
- Quand s'applique la détection d'intrusion

Les systèmes de détection d'inrusions

IDS

Un **IDS** (**Système de détection d'intrusion**) est un ensemble de composants logiciels ou matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction volontaire ou non dans un SI ainsi que toute altération éventuelle de ces données.



IPS

Un **IPS** (**Système de prévention d'intrusion**) est un ensemble de composants logiciels ou matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.

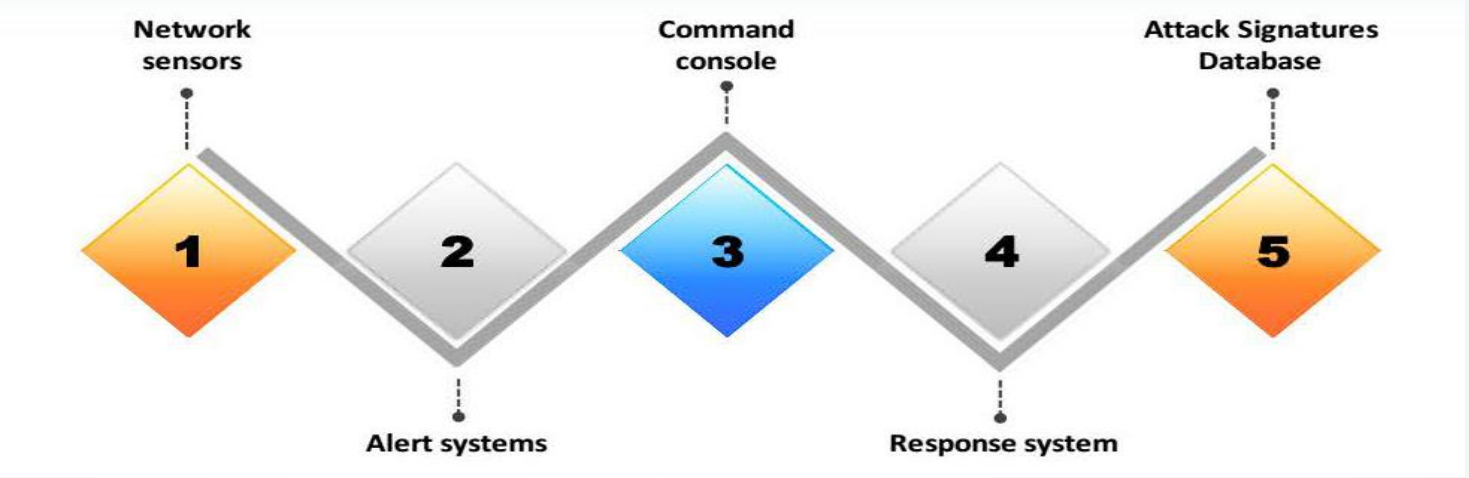
Les systèmes de détection d'inrusions

Terminologie IDS/IPS

- **Faux positif (FP):** (fausse alerte) Activité non malicieuse signalée comme étant une intrusion par l'IDS
- **Faux négatif :** Activité ou évènement d'une attaque non détectés ni signalé par l'IDS
- **Vrai positif :** détection d'attaque qui a réellement eu lieu.
- **Vrai négatif :** est une non détection d'attaque lorsqu'en effet il n'y a pas eu d'attaque.
- **Evasion:** Attaque informatique ou technique qui détourne les équipements de détection d'intrusion (non détectée par les IDS)
- **Sensibilité = VP/(VP+FN).**
- **Spécificité = VN/(VN+FP).**
- Si un test a une sensibilité de 100%, alors toutes les attaques sont correctement détectées.
- Si un test a une spécificité de 100%, alors tous les cas normaux sont correctement identifiés.

Les systèmes de détection d'inrusions

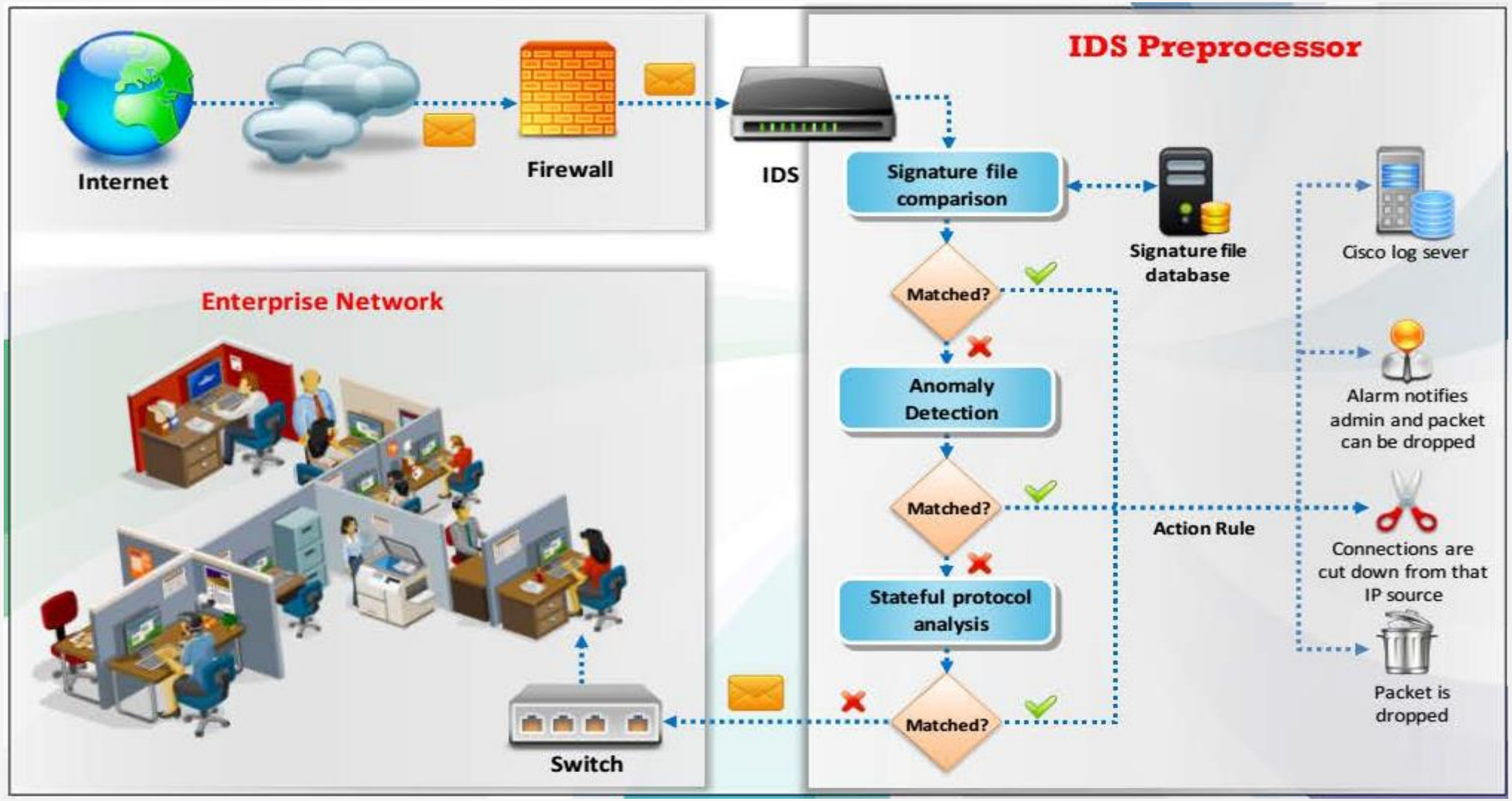
Composantes d'un IDS



- **sondes réseau :** ces agents analysent et signalent toute activité suspecte.
- **Analyseur :** analyse les données collectées par les sondes.
- **Systèmes d'alerte :** ces systèmes déclenchent des alertes lorsqu'ils détectent une activité malveillante.
- **Console de commande :** Elle agit comme une interface entre l'utilisateur et la détection d'intrusion système.
- **Système de réponse :** un IDS utilise ce système pour initier des contre-mesures aux activités détectées
- **Base de données des signatures ou des comportements d'attaque :** une liste des signatures précédemment détectées stockées dans une base de données qui assiste l'IDS dans la détection d'intrusion.

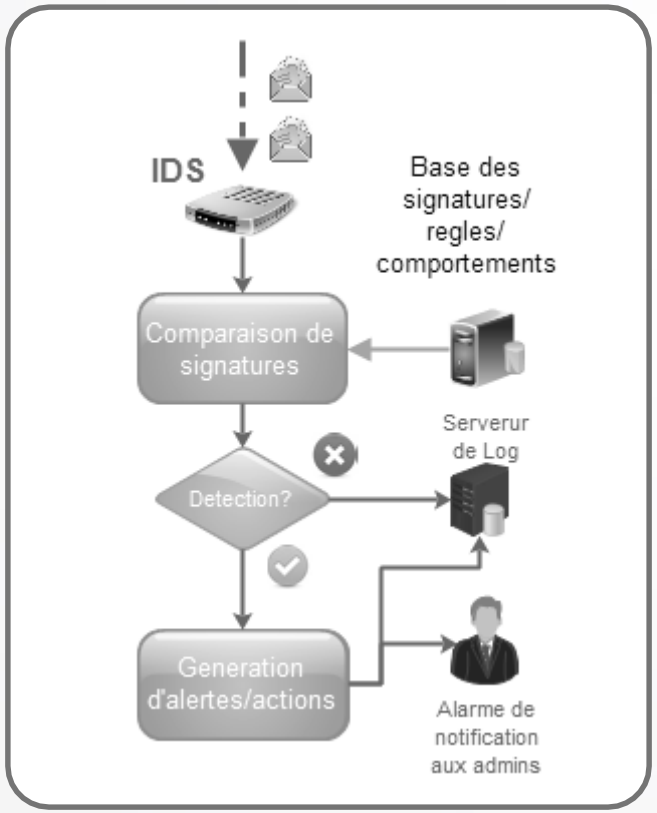
Les systèmes de détection d'inrusions

Fonctionnement d'un IDS



Les méthodes de détection

Comment détecter si le flux est normal ou susceptible d'être une intrusion ?



Signature-based

- Pattern matching
- Stateful matching

Anomaly-based (heuristic-based)

- Statistical anomaly based
- Protocol anomaly based
- Traffic anomaly based

Rule based

Les systèmes de détection d'inrusions

Signature based IDS

- La **détection par signature,** appelée aussi **détection par scénarios** consiste à comparer l'activité du réseau aux représentations d'intrusion ou signatures préétablies comme la présence de certains motifs dans une requête au niveau applicatif ou même dans un paquet IP.
- Ce type de détection permet de détecter toutes les attaques ou intrusions dont les motifs sont connus et référencés.
- Par ailleurs, la détection est très rapide.
- **INCONVENIENT:** une attaque ou nouvelle intrusion non référencée ne sera pas détectée.
- Ce type de détection, nécessite donc de mettre à jour la base de signatures régulièrement.
- Deux types:
  - ✔ **Pattern matching**: Comparer les paquets aux signatures
  - ✔ **Stateful matching**: Comparer les signatures à plusieurs évènements en même temps.

Les systèmes de détection d'inrusions

Anomaly based IDS

- **La détection comportementale**, appelée aussi **détection par apprentissage**, consiste à comparer l'activité d'un utilisateur à un référentiel prédéfini ce qui permet de détecter des attaques non connues comme l'accès à une ressource à des heures non habituelles ou l'envoi d'une requête inhabituelle à un serveur web sur un port fermé par exemple.
- L'IDS établit un modèle de trafic normal en se basant sur certains paramètres comme la moyenne de connexions et le type de trafic à des heures précises et ensuite compare le trafic actuel au modèle ou référence. Si les deux trafics sont trop différents, alors il se pourrait qu'une attaque soit en cours.
- Ce type de détection permet de détecter des nouvelles intrusions si les profils ont été bien définis ce qui n'est pas facile parce que les méthodes de détection comportementale se basent sur des outils de complexité diverses comme les seuils, l'intelligence artificielle, les méthodes probabilistes ou même la Big Data ce qui rend forcément le système très gourmand en temps de calcul, sans garantir pour autant qu'il ne génère pas de fausses alertes.
- En outre, s'il y a un grand besoin de sécurité cela signifie que l'IDS devra analyser plus de flux d'une manière plus détaillée nécessitant de bien meilleures performances matérielles et logicielles pour l'IDS.

Les systèmes de détection d'inrusions

Rule based IDS

- C'est une technique de détection basée sur la comparaison des évènements avec un ensemble de règles.

Drop icmp any any $HOME_NET any (msg: "tentative ping" ; …)

- Utilisation de règles à base de condition **if/else** dans un système expert.
- L'utilisation d'un système expert permet d'intégrer des caractéristiques de l'intelligence artificielle
- Les règles utilisées peuvent être complexes ce qui demande généralement plus de ressources matérielles et temps de traitement des activités
- La signalisation par alerte suite à une attaque ou intrusion n'est pas en temps réel.
- Cette technique ne permet pas de détecter de nouvelles attaques

Les systèmes de détection d'inrusions

Types d'IDS

Network based IDS (NIDS)

Surveiller l'état de la sécurité au niveau du réseau:

- contenu des paquets (entête et données)
- paramètres du trafic (Volume, cibles, etc.)

L'utilisation d'une sonde permet la surveillance d'une ou plusieurs zones du réseaux.

Host based IDS (HIDS)

Surveiller l'état de la sécurité au niveau des hôtes:

- les évènements sur les journaux de logs
- l'intégrité des fichiers
- les accès au processus

L'utilisation d'une sonde pour chaque machine.

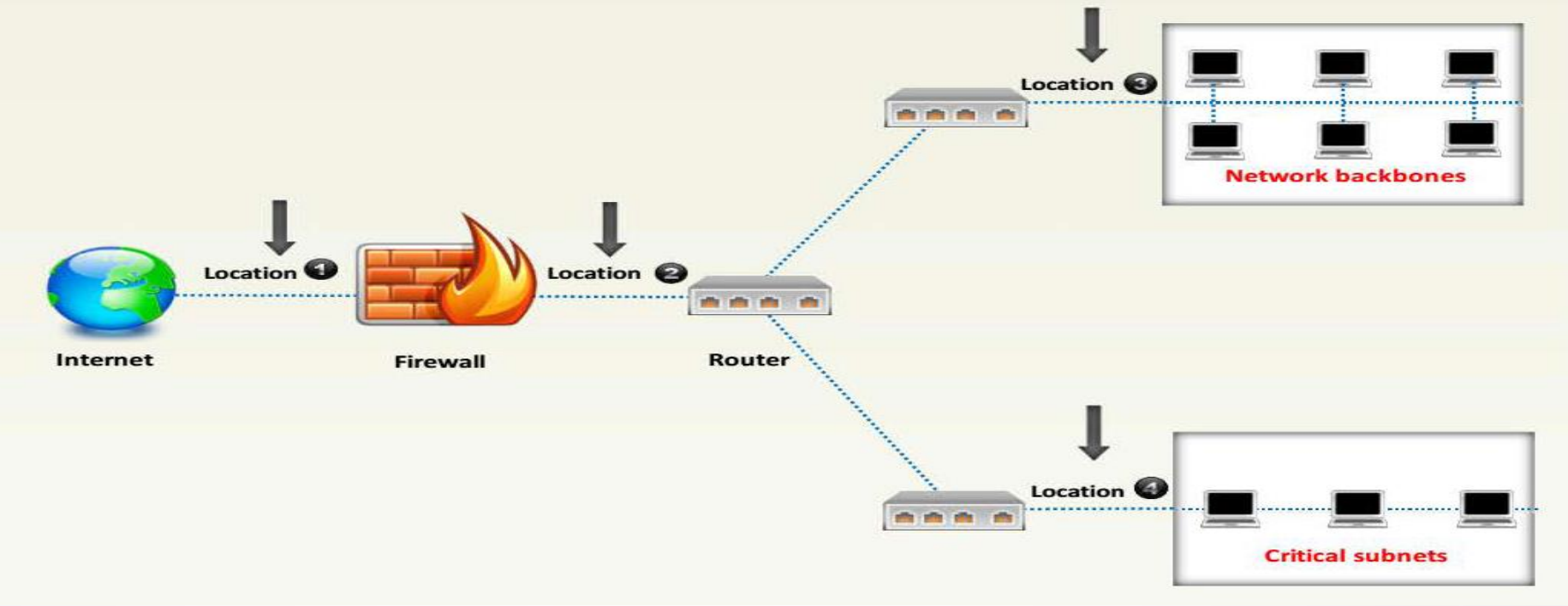
IDS Hybride

Rassemble les fonctionnalités d'un NIDS et HIDS, surveillance du réseau et de terminaux. L'IDS hybride est utilisé dans un environnement décentralisé avec une supervisons centralise.

- Placement stratégique des sondes sur le réseau.
- Centraliser les informations en provenance de plusieurs emplacements (sondes) sur le réseau.
- Avoir une vision globale sur les composants du système d'information

Les systèmes de détection d'inrusions

Où placer les sondes d'un IDS ?



Emplacement 1 : à l'extérieur du réseau local

Emplacement 2 : sécuriser le réseau de périmètre

Emplacement 3 : sécuriser le réseau interne

Emplacement 4 : protéger les hôtes sensibles

Les systèmes de détection d'inrusions

Les IPS (Systèmes de Prévention d'Intrusions)

- L'IDS traditionnel ne détecte que qu'une intrusion qui peut être en cours et envoie une alerte.
- Un IPS est système similaire aux IDS , permettant de prendre des mesures préventives afin de diminuer les impacts d'une attaque.
- Ainsi, un IPS est une technique de contremesure préventive et proactive, alors qu'un IDS est une technologie de contremesure détective (alerte en cours ou après impact de l'attaque)
- Il existe deux types d'IPS: IPS réseau (**NIPS**) et IPS hôte (**HIPS**)
- A l'inverse d'un NIDS qui fonctionne en mode promiscuité (positionné comme un sniffer sur le réseau) un NIPS va fonctionner en coupure sur le réseau.
- Les NIPS peuvent bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce, ce qui induit que le NIPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocges
- L'IPS ne remplace pas l'IDS ou le Firewall

Les systèmes de détection d'inrusions

Solutions IDS/IPS

Snort
https://www.snort.org

AIDE
http://aide.sourceforge.net

Suricata
http://suricata-ids.org

Next-Generation IPS
http://www.fortinet.com

OSSEC
http://www.ossec.net

Cyberoam Intrusion Prevention System
http://www.cyberoam.com

Strata Guard IDS/IPS
http://www.data-alliance.com.my

IBM® Security Network Intrusion Prevention System
http://www-03.ibm.com

McAfee Host Intrusion Prevention for Desktops
http://www.mcafee.com

AlienVault Unified Security Management
http://www.alienvault.com

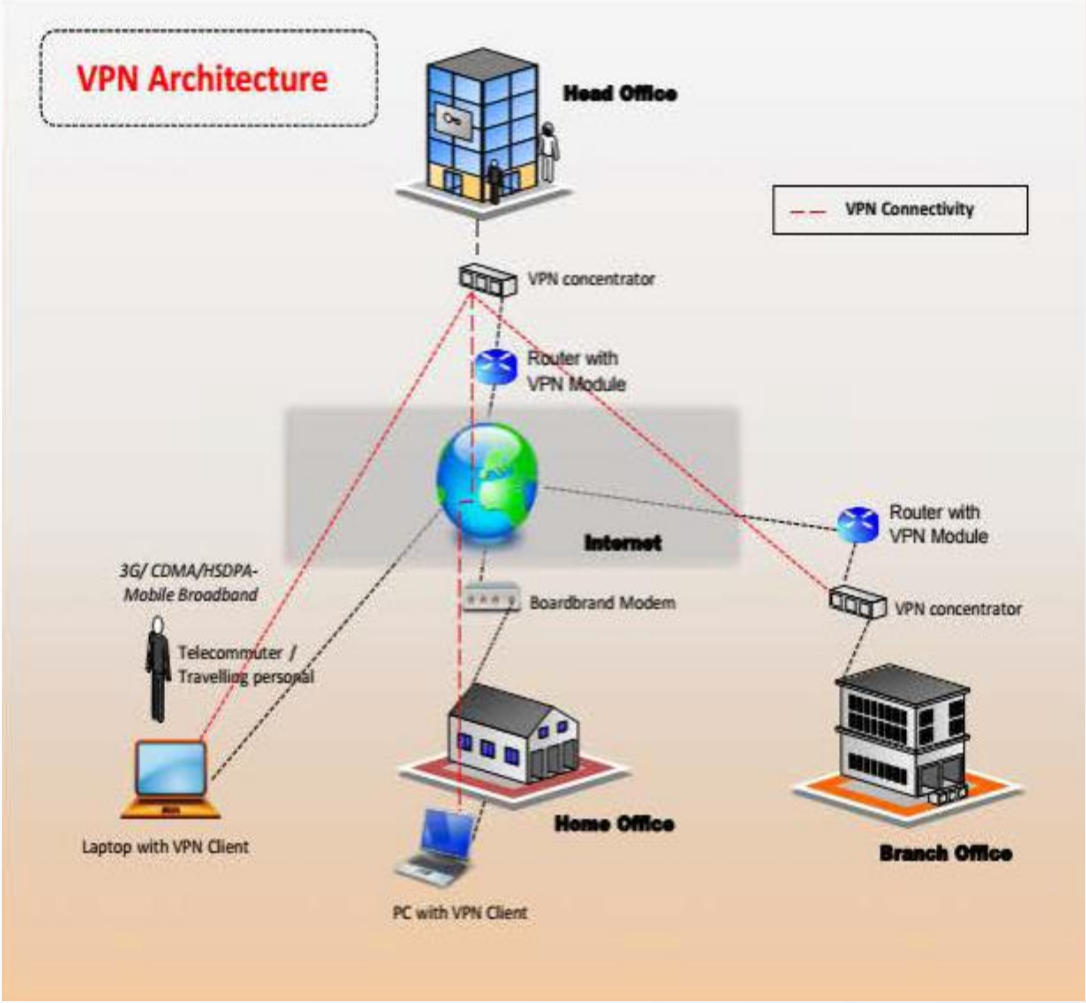
Plan

- Introduction au contrôle d’accès
- Les firewalls
- Les Systèmes de Détection et de Prévention d’intrusions (IDS/IPS)
- Introduction aux Réseaux Privés Virtuels (VPN)

Les Réseaux Privés Virtuels

Qu’est-ce qu’un VPN?

- Un **VPN** ou **réseau privé virtuel** a pour objectif de faciliter les communications entre entreprises partenaires ou les communications internes d'une entreprise dans le cas d'un réseau d'entreprise réparti géographiquement sur deux sites 1 et 2 distants, ou de télétravailleurs qui ont besoin de se connecter aux ressources de leur entreprise.
- Un **VPN** permet d'étendre virtuellement, grâce à la technologie de tunnel, un réseau privé ou le terminal du télétravailleur, un autre réseau privé, et ce au travers d'un réseau public.



Les Réseaux Privés Virtuels

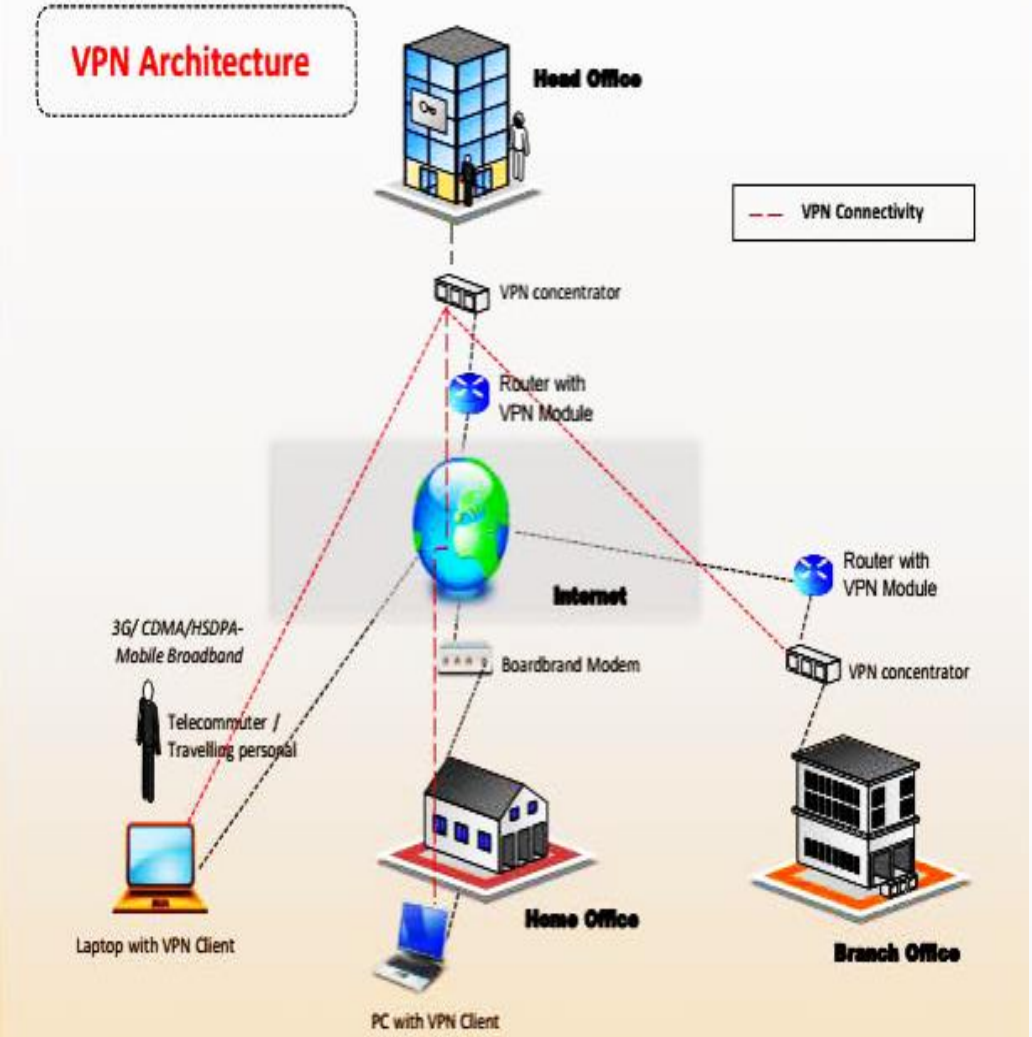
Besoins de Sécurité

Les données échangées dans le tunnel peuvent être sensibles et être la cible de cyber-attaques. Pour protéger les flux, il est utile de mettre en œuvre plusieurs services de sécurité, à savoir :

- **La confidentialité des données** pour empêcher un espion d'interpréter les contenus des échanges, ce qui nécessite de chiffrer les échanges dans le tunnel.
- **L'intégrité des données** pour détecter si les informations échangées ont été modifiées pendant leur transfert sur le réseau, le mécanisme adéquat sous-jacent reposant sur le principe de code d'intégrité cryptographique appelé HMAC.
- **L'authentification de l'origine des données** pour empêcher qu'un attaquant n'envoie des données en usurpant l'identité d'une des extrémités du tunnel. Ce service repose aussi sur HMAC.

Types de VPN

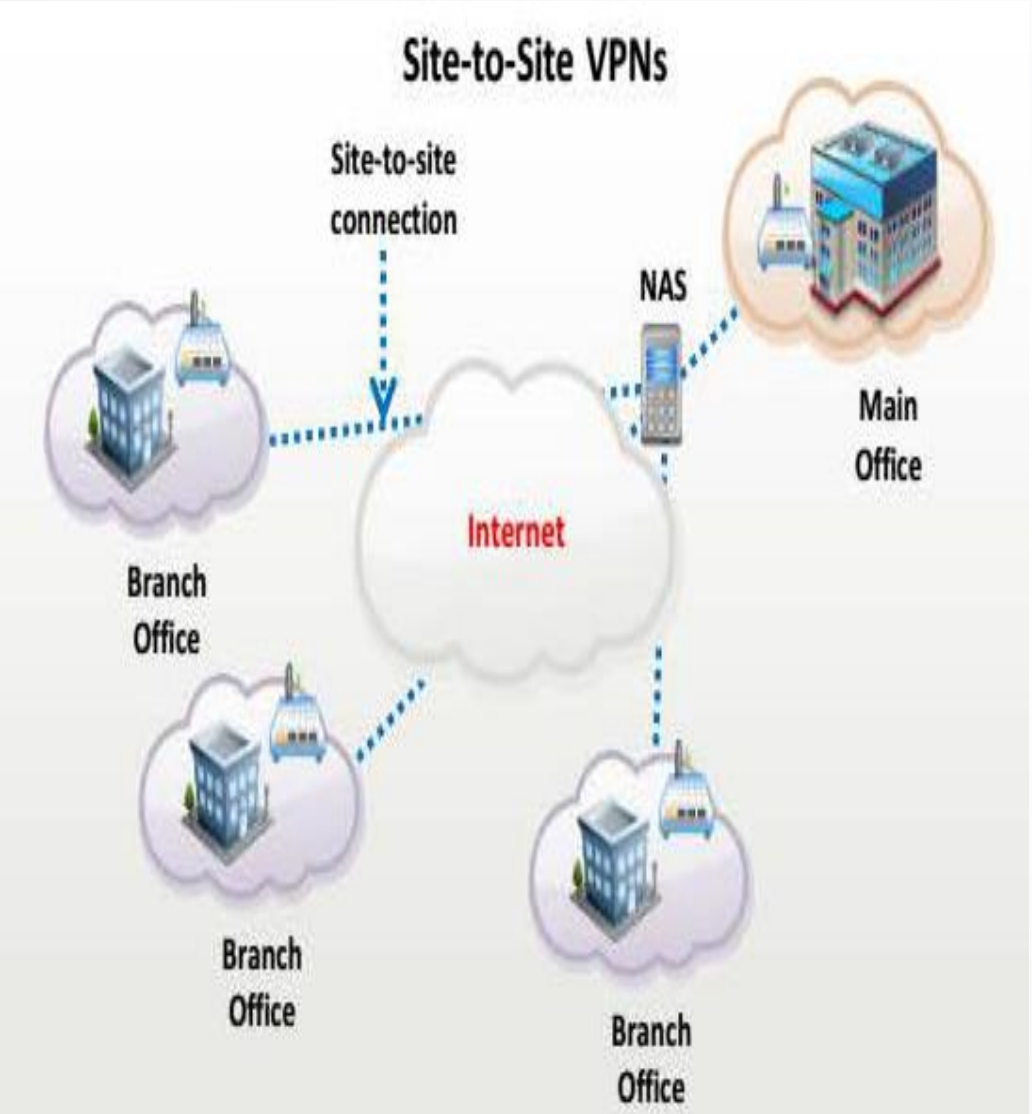
Client-to-Site VPNs



- Les VPN d'accès à distance permettent aux hôtes ou clients individuels, tels que les télétravailleurs et les utilisateurs mobiles pour établir des connexions sécurisées au réseau d'une entreprise via Internet
- Chaque hôte contient un logiciel client VPN ou utilise un client Web
- Le VPN crypte les paquets de données qui sont transmis via Internet à la passerelle VPN au périphérie du réseau cible, avec le logiciel installé sur la machine du client .
- Une passerelle VPN reçoit les paquets, puis ferme la connexion au VPN une fois le transfert terminé

Types de VPN

Site-to-Site VPNs



- Le **VPN site-to-site**, aussi connu sous le nom de VPN LAN-to-LAN, étend le réseau de l'entreprise et permet l'accès aux ressources réseau d'une organisation à partir de différents emplacements
- Il connecte une succursale ou un réseau de bureaux distants au réseau du siège social de l'entreprise
- Les VPN site-to-site sont classés en deux types :

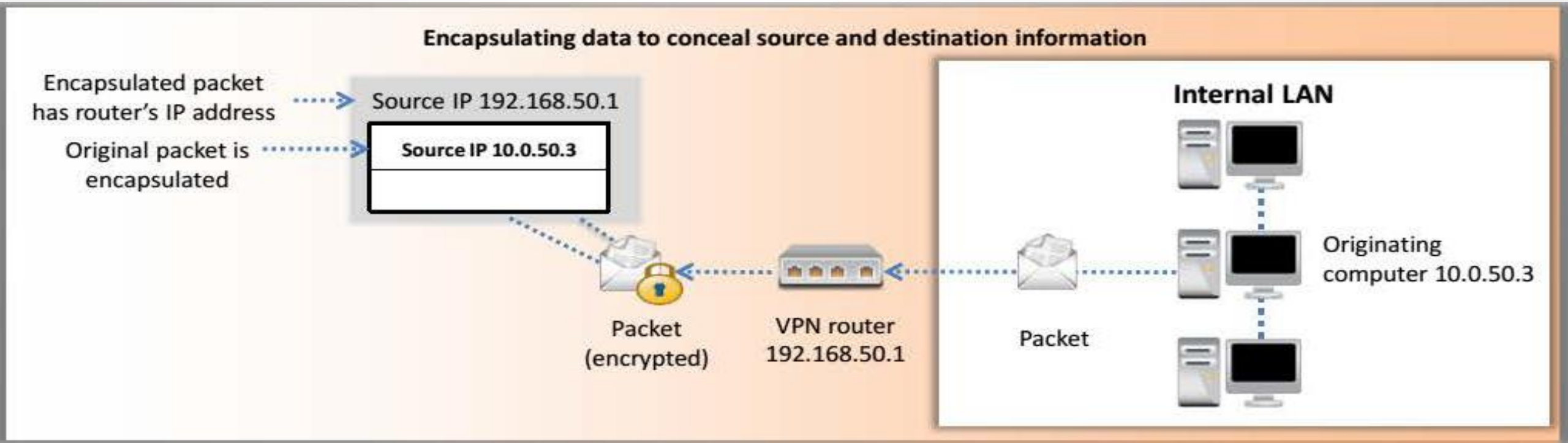
✔ Intranet-based : la connectivité VPN se fait entre les sites d'une même organisation

✔ Extranet-based : la connectivité VPN se fait entre différentes organisations telles que des partenaires commerciaux, l'entreprise et ses clients

Fonctionnalités principales des VPNs

Encapsulation

- Les paquets sur un VPN sont enfermés dans un autre paquet (encapsulation) qui a une IP source et une IP destination différentes
- La dissimulation de la source et de la destination des paquets protège l'intégrité des données envoyées



Fonctionnalités principales des VPNs

Les prinicipaux protocoles de tunnelisation

- **PPTP** (*Point-to-Point tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F** (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco Systems, Nortel et Shiva. Il est désormais quasi-obsolète.
- **L2TP** (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF (RFC 3931) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPsec** est une suite de protocoles qui fournit de la sécurité aux communications Internet de la couche IP du modèle TCP IP (IETF)
- **SSL/TLS** offre une très bonne solution de tunnelisation. L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN.
- **SSH** offre la possibilité de tunneliser des connexions de type TCP, permettant d'accéder ainsi de façon sûre à des services offerts sur un réseau protégé, sans créer un réseau privé virtuel au sens plein. Depuis sa version 4.3, le logiciel OpenSSH permet de créer des tunnels entre deux interfaces réseau virtuelles au niveau 3 (routage du seul trafic IP, interfaces TUN) ou au niveau 2 (tout le trafic Ethernet, interfaces TAP).

IPsec

IPsec c’est quoi?

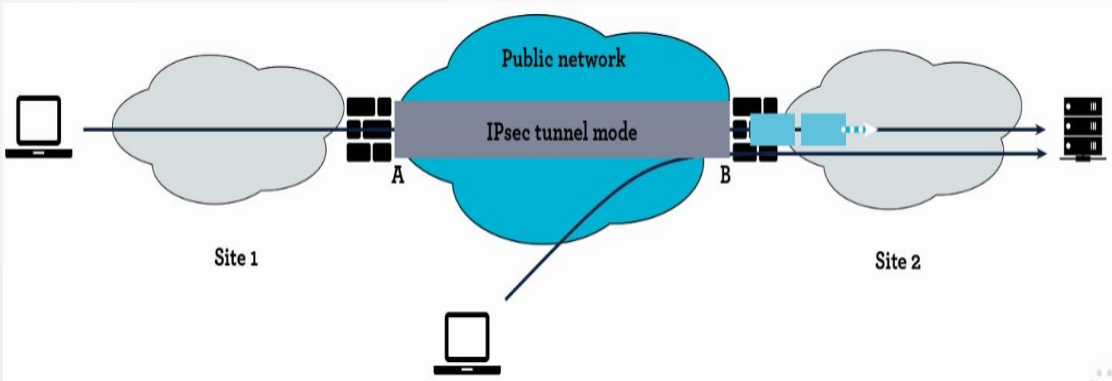
- ***IPsec (Internet Protocol Security)*** est une suite de protocoles qui fournit de la sécurité aux communications Internet de la couche IP du modèle TCP IP (IETF)

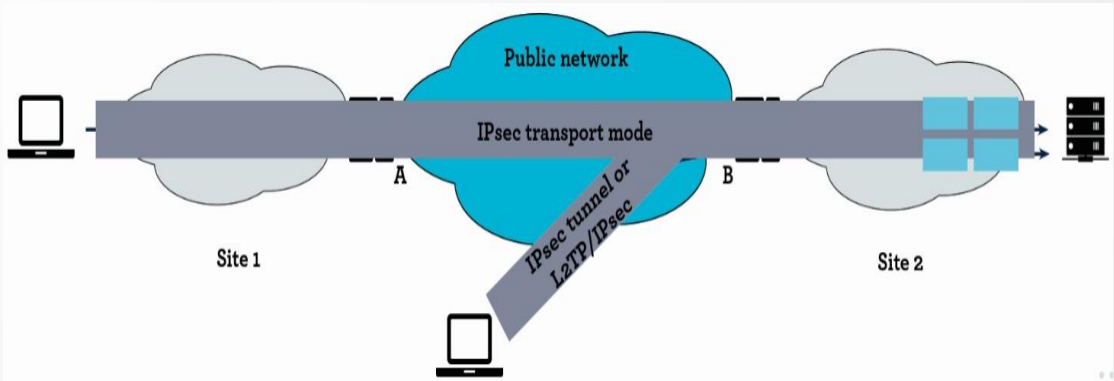
Deux modes sont supportés par chacun des protocoles :

le mode transport et le mode tunnel.

- IPsec peut être utilisé pour mettre en place un VPN soit :
  - ✔ entre deux sites : **mode tunnel**
  - ✔ entre un utilisateur nomade et un site **mode tunnel** ou **mode transport** (Ipsec/L2TP)
  - ✔ entre une machine hôte et une autre machine hôte :**mode transport**

Pour plus de détails: voir Annexe 2



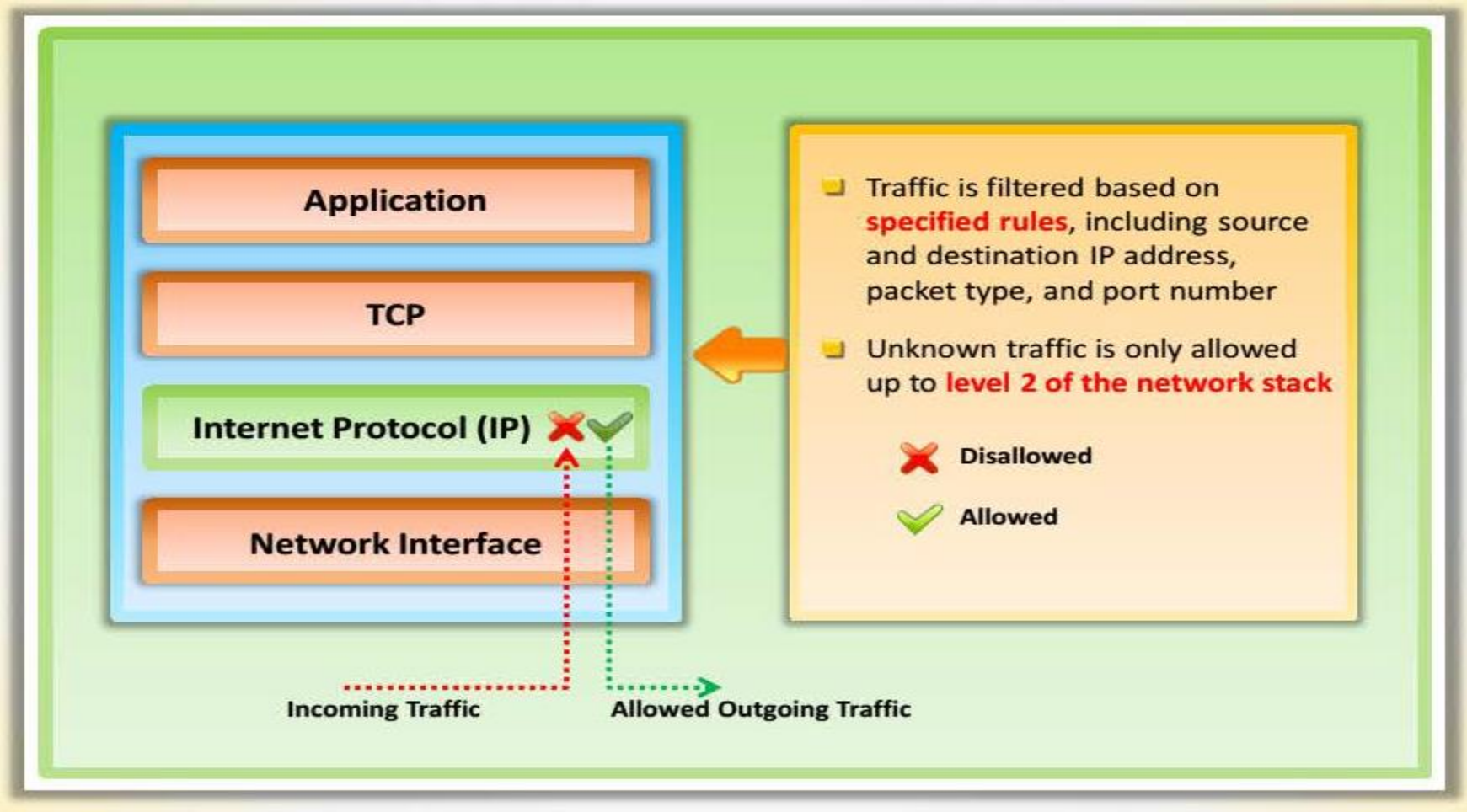


Fin chapitre

Annexes 1: Les Technologies de Firewall

Les Technologies de Firewall

Packet Filtering Firewall



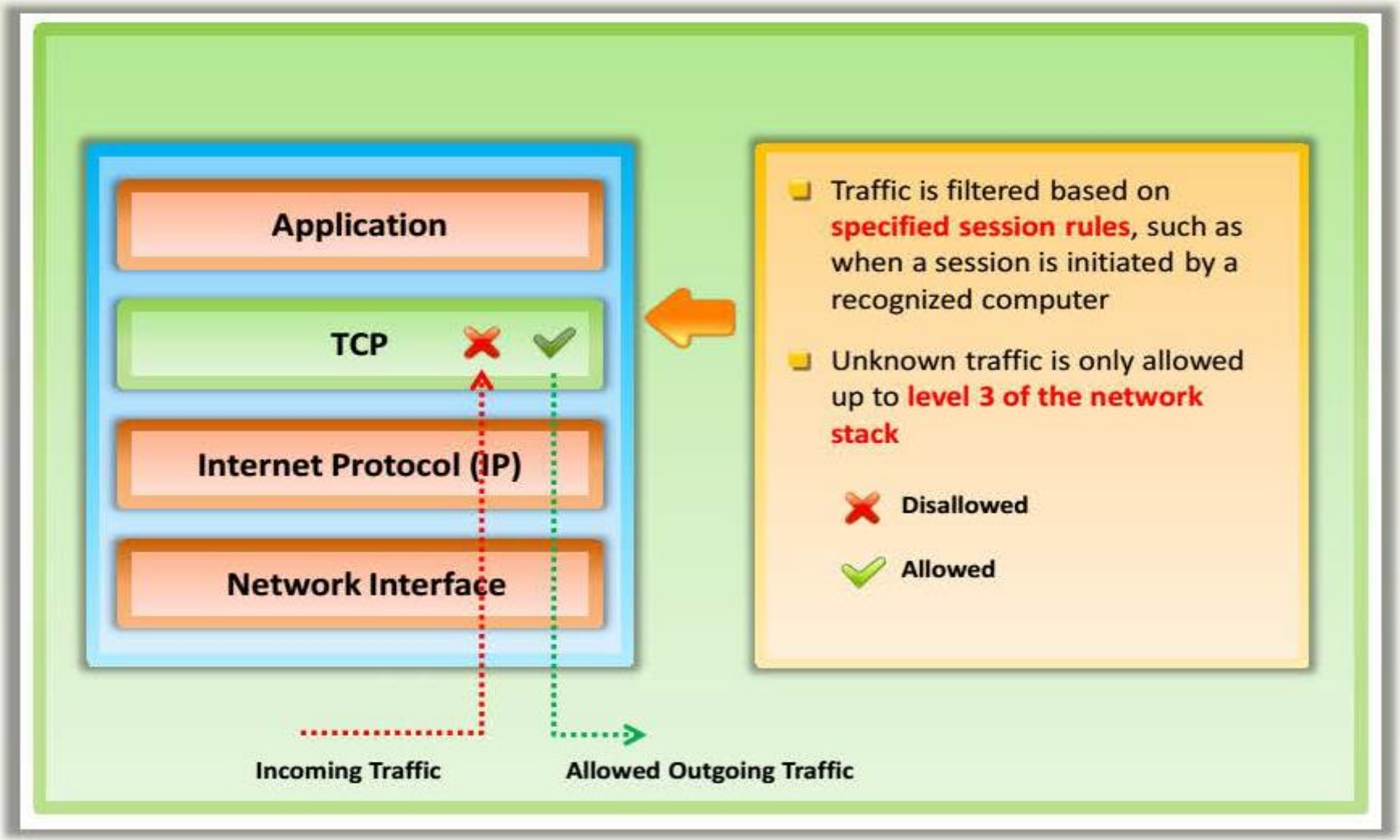
Les Technologies de Firewall

Packet Filtering Firewall

- Les pare-feu de filtrage de paquets fonctionnent au niveau réseau du modèle OSI (ou la couche IP de TCP/IP)
- Ils font généralement partie d'un routeur
- Dans un pare-feu de filtrage de paquets, chaque paquet est comparé à un ensemble de critères avant d'être transmis
- Selon le paquet et les critères, le pare-feu peut :
  - ✔ autoriser la connexion (**Allow**) ;
  - ✔ bloquer la connexion (**Deny**) ;
  - ✔ rejeter la demande de connexion sans avertir l'émetteur (**Drop**).
- Les règles incluent les adresses IP source et de destination, le numéro de port source et de destination et le protocole utilisé
- L'avantage des pare-feu de filtrage de paquets est leur faible coût et leur faible impact sur les performances du réseau
- La plupart des routeurs prennent en charge le filtrage de paquets

Les Technologies de Firewall

Circuit Level Gateway

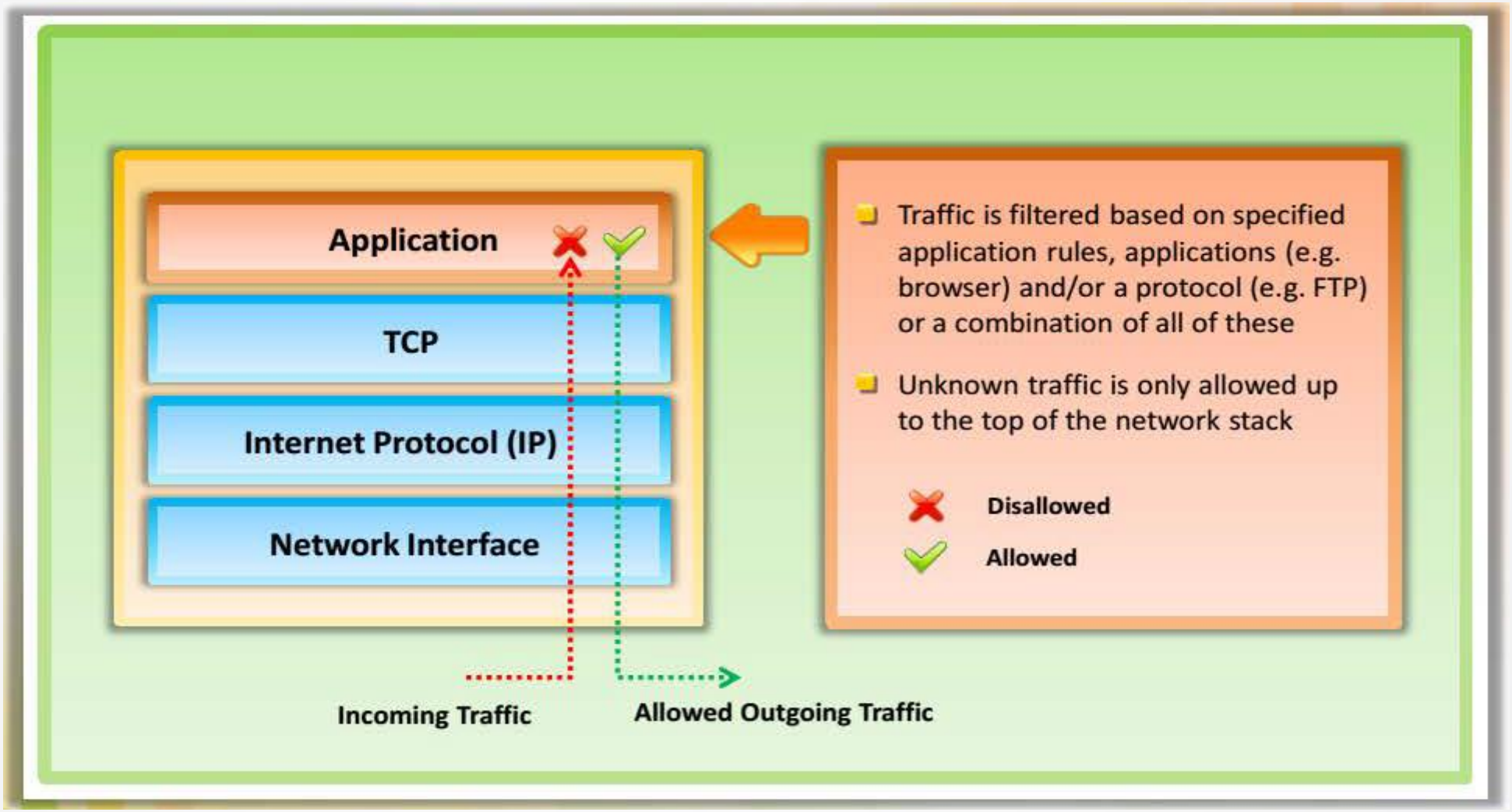


Les Technologies de Firewall

Circuit Level Gateway

- Les passerelles au niveau du circuit fonctionnent au niveau de la couche session du modèle OSI ou de la couche TCP de TCP/IP
- Elles surveillent le TCP-handshake entre les paquets pour déterminer si une session demandée est légitime ou non
- Les informations transmises à un ordinateur distant via une passerelle au niveau du circuit semblent provenir de la passerelle
- Les passerelles au niveau du circuit sont relativement peu coûteuses
- Elles ont l'avantage de cacher des informations sur le réseau privé qu'ils protègent
- Les passerelles au niveau du circuit ne filtrent pas les paquets individuels

Application Level Firewall

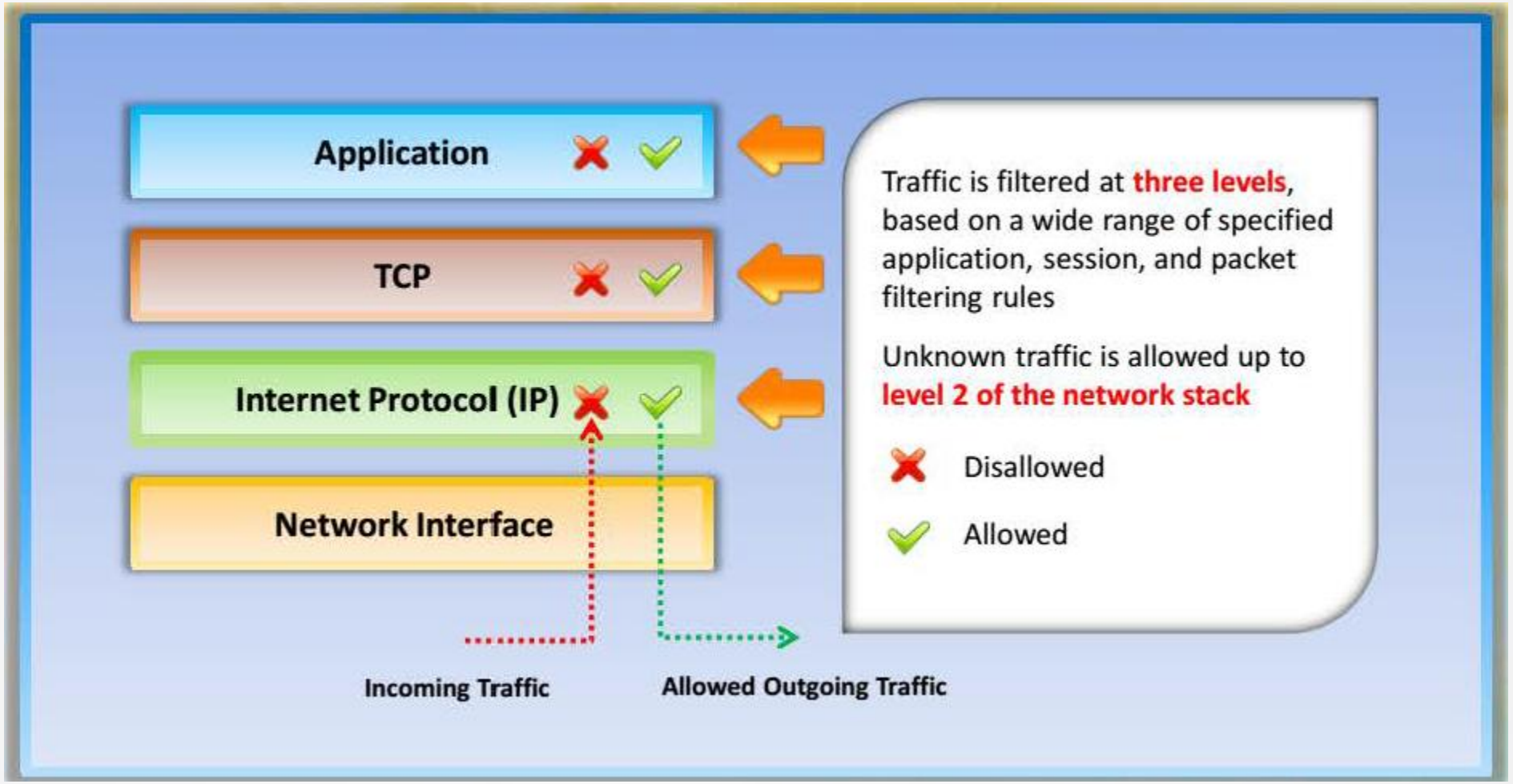


Les Technologies de Firewall

Application Level Firewall

- Les passerelles au niveau de l'application sont également appelées proxys
- Elles peuvent filtrer les paquets au niveau de la couche application du modèle OSI
- Les paquets entrants ou sortants ne peuvent pas accéder aux services pour lesquels il n'y a pas de proxy
- En clair, une passerelle de niveau application configurée pour être un proxy Web n'autorisera aucun trafic FTP, Gopher, Telnet ou autre
- Parce qu'ils examinent les paquets au niveau de la couche application, elles peuvent filtrer les commandes spécifiques à l'application telles que HTTP-POST et HTTP-GET

Stateful Multilayer Inspection Firewall



Les Technologies de Firewall

Stateful Multilayer Inspection Firewall

- Les pare-feux d'inspection multicouche avec état combinent l'aspect des trois autres types de pare-feu (c'est-à-dire le filtrage de paquets, les passerelles au niveau du circuit et le pare-feu au niveau de l'application) .
- Ils filtrent les paquets au niveau de la couche réseau du modèle OSI pour déterminer si les paquets de session sont légitimes, et ils évaluent le contenu des paquets au niveau de la couche application.
- Dans la plupart des cas, les pare-feux SMLI sont implémentés en tant que niveaux de sécurité supplémentaires.
- Ces types de pare-feu implémentent davantage de vérifications et sont considérés comme plus sûrs que les pare-feu sans état.
- C'est pourquoi l'inspection dynamique des paquets est implémentée avec de nombreux autres pare-feu pour suivre les statistiques de tout le trafic interne.

Proxy

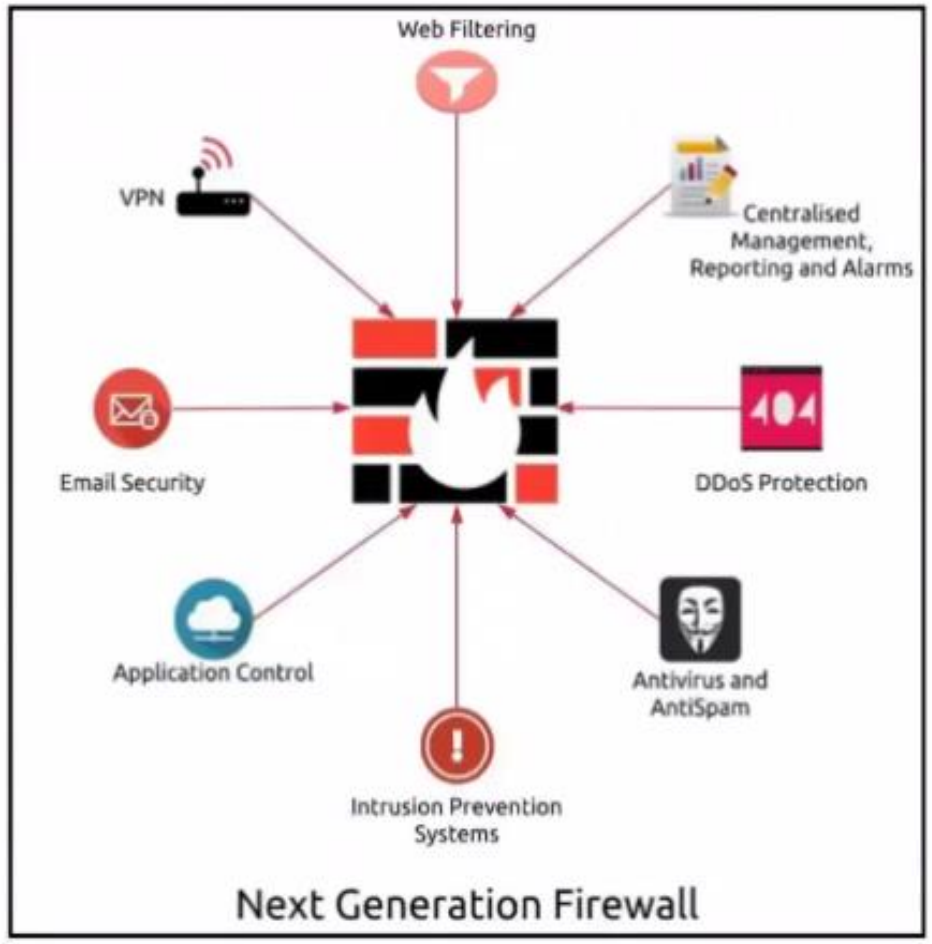
Un proxy est un matériel ou un logiciel servant d'intermédiaire entre deux réseaux. Une des utilisations les plus courantes de proxy concerne l'utilisation d'Internet (HTTP). Un utilisateur, pour se rendre sur Internet, va d'abord passer par le proxy et c'est le proxy qui va envoyer la requête HTTP vers Internet.

- Filtre la couche applicative et donc les protocoles HTTP et autre.
- Contrôle le réseau par utilisateur et donc permet de garder un historique.
- Permet de faire circuler le trafic HTTP et FTP via le proxy, en cas d'attaque, l'attaque se ferait sur le proxy et non sur le poste utilisateur.
- Permet de voir les attaques potentielles (IDS que nous verrons plus tard dans ce cours).
- Est très coûteux, plus vous avez d'utilisateurs et plus votre connexion Internet est puissante, plus vous devrez

Les Technologies de Firewall

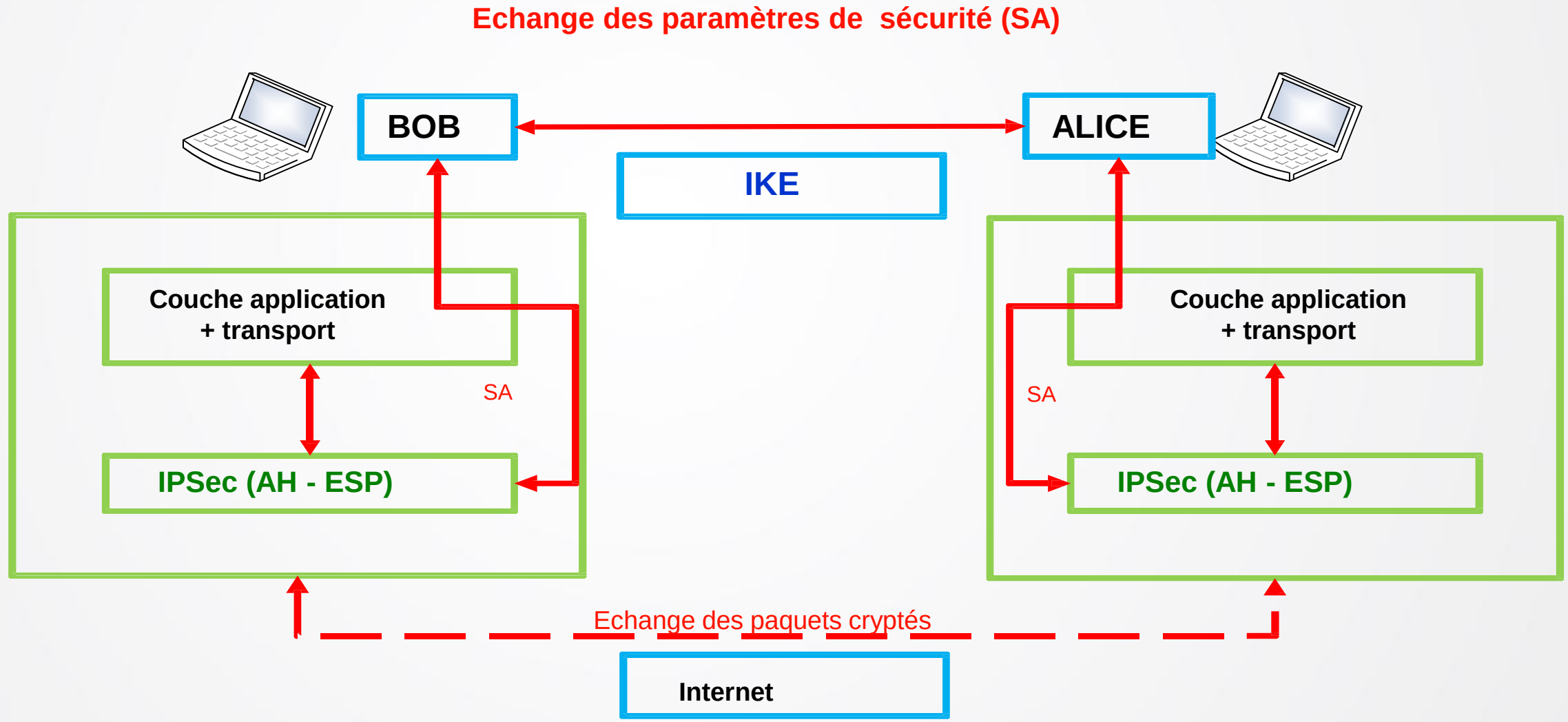
Next Generation Firewall (NGFW)

Un **pare-feu de nouvelle génération** (**NGFW**) fait partie de la troisième génération de technologie de pare-feu, combinant un pare-feu traditionnel avec d'autres fonctions de filtrage de périphériques réseau, comme un **pare-feu d'application** utilisant **l'inspection approfondie des paquets (DPI)** en ligne, **un système de prévention d'intrusions** (IPS). D'autres techniques peuvent également être utilisées, telles que **l'inspection du trafic crypté TLS/SSL** , le **filtrage des sites Web**, **la gestion de la qualité de service et de la bande passante** , l'inspection **anti-malware** et l' intégration de la **gestion des identités** par des tiers (c'est-à-dire LDAP , RADIUS ,Active Directory).



Annexes 2: IPSec

VPN IPsec


Echange des paramètres de sécurité (SA)
BOB
ALICE
IKE
Couche application
+ transport
SA
IPSec (AH - ESP)
Couche application
+ transport
SA
IPSec (AH - ESP)
Echange des paquets cryptés
Internet

IPsec

Authentication Header (AH)

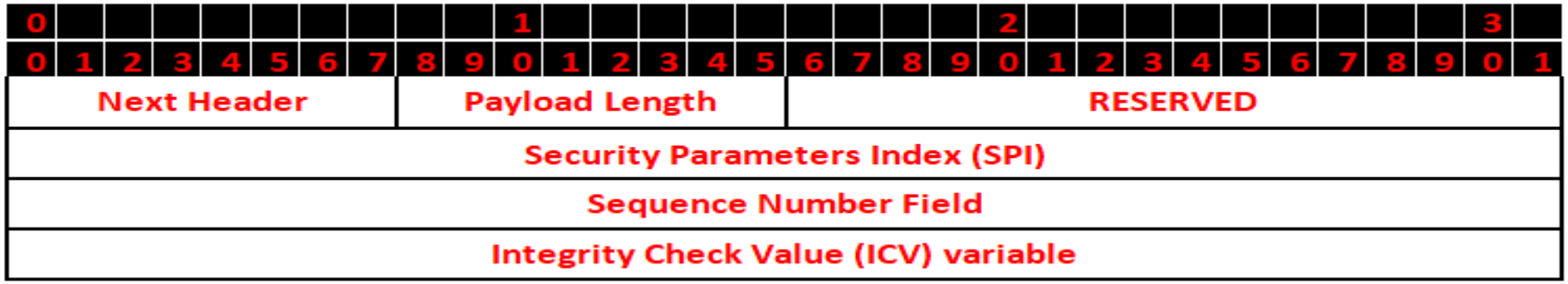
- **Vérification de l'intégrité et l'authenticité des paquets IP - Détection de rejeu**

Paquet d'origine

AH Mode Transport

AH Mode Tunnel

- **Format**

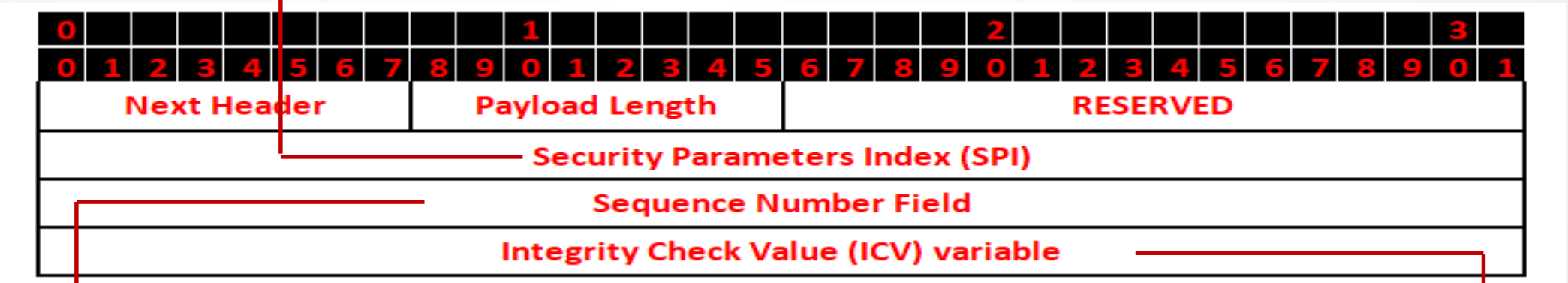


IPsec

Authentication Header (AH)

SPI: permet au récepteur d'identifier l'association de sécurité à utiliser pour vérifier le contenu de l'en-tête AH.

SA (Security Association): s'applique à une communication unidirectionnelle et se définit par un ensemble de paramètres de sécurité: algorithmes de chiffrement, fonction de hachage, clés cryptographiques, protocole IPsec, mode tunnel ou transport, durée de vie



Numéro de séquence:

- ✔ Utilisé pour détecter les rejeux de paquets
- ✔ Incrémenté par l'émetteur
- ✔ Le récepteur peut ne pas en tenir compte.

Valeur de Contrôle d'Intégrité:

- ✔ Multiple de 32 bits
- ✔ Code d'authentification de message (MAC) AES-CMAC96 / … HMAC-SHA1-96 / HMAC-SHA-256+ / …

IPsec

Encapsulating Security Payload (ESP)

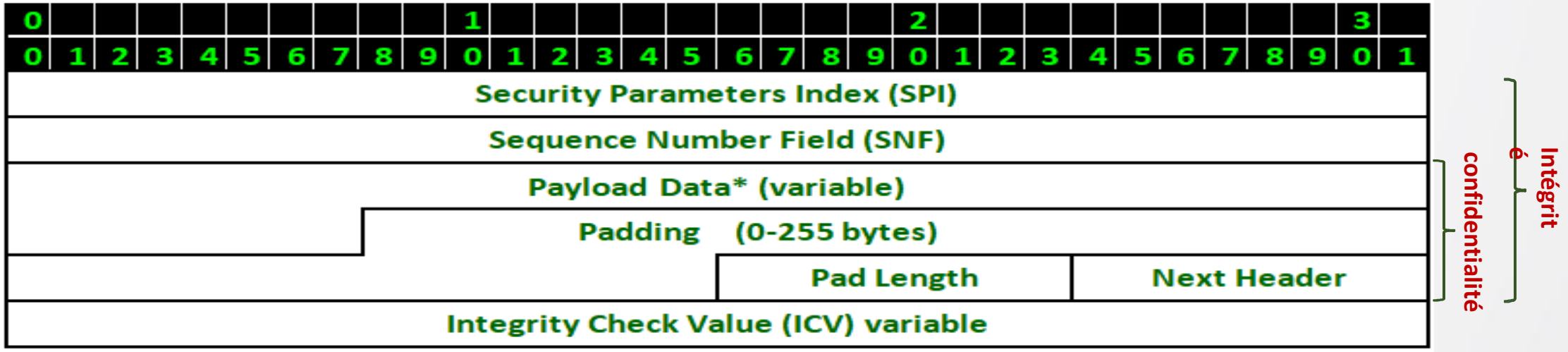
- Intégrité, authenticité, anti-rejeu + Confidentialité

Paquet d'origine

ESP Mode Transport

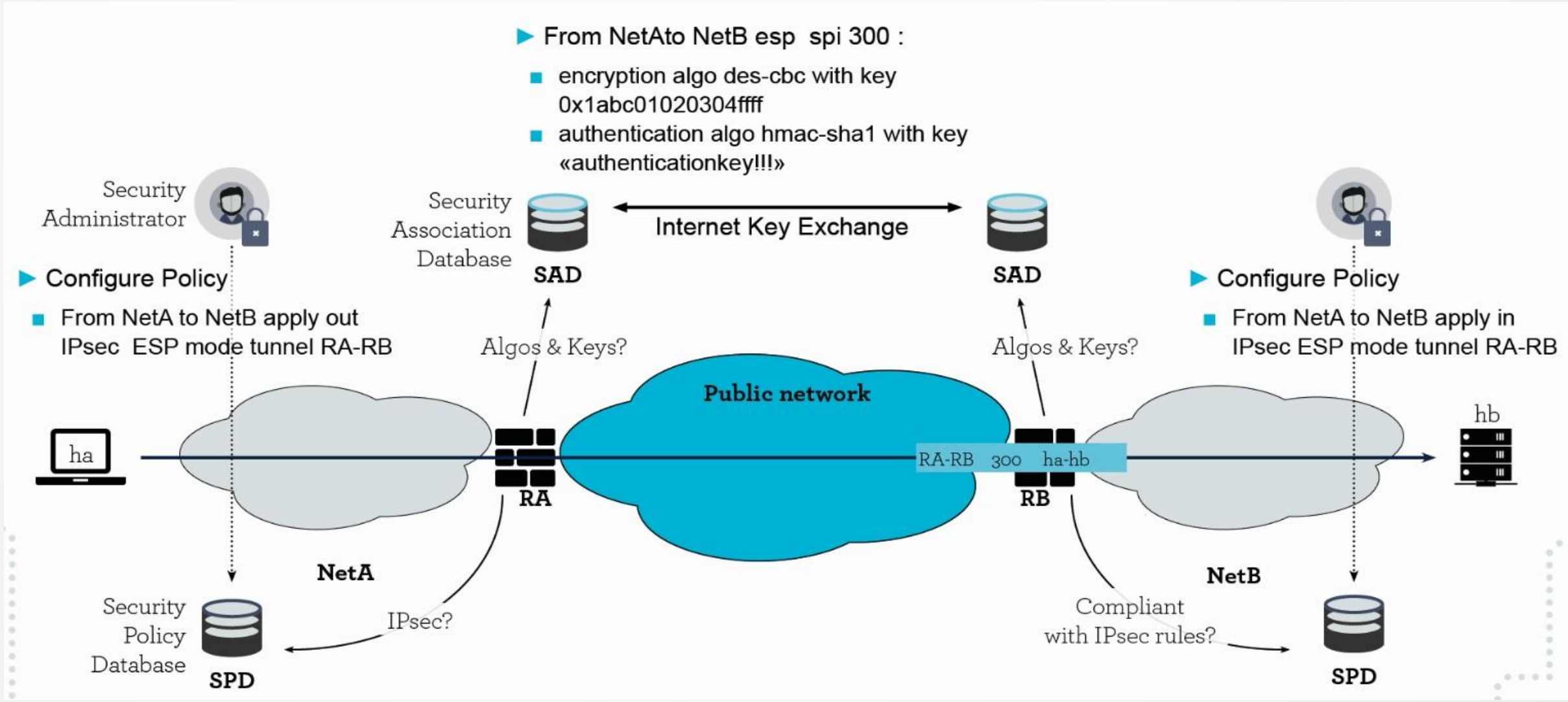
ESP Mode Tunnel

- Format



IPsec

Comment fonctionne IPsec?



Internet Key Exchange (IKE)

- IPsec le choix des clés et des algorithmes cryptographiques doit être effectué pour pouvoir sécuriser une connexion IP à l'aide de AH ou ESP.
- Pour pouvoir établir dynamiquement des associations de sécurité, un autre mécanisme doit être mis en place:
- **protocole IKE (Internet Key Exchange)**
- **IKE** intervient à la mise en place de la première association de sécurité et à chaque renouvellement d'associations de sécurité.
- **IKE** définit les échanges protocolaires pour négocier et mettre à jour le matériel cryptographique nécessaire à IPsec.
- **IKE** réalise l'authentification mutuelle des deux parties impliquées dans IPsec (hôtes ou passerelles).

Internet Key Exchange (IKE)

• **IKE** repose sur le format de messages **ISAKMP (Internet Security Associaciation and Key Management Protocol)** pour la syntaxe des messages décrivant les associations de sécurité.

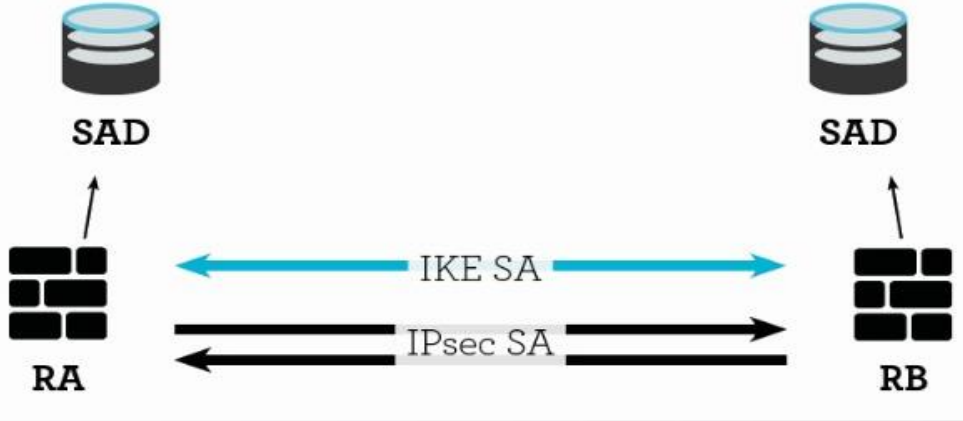
• Il existe deux versions d'**IKE** qui ne sont pas interopérables : **IKEv1** et **IKEv2.** L'objectif de la deuxième version est de simplifier le protocole et de rassembler toute sa description dans un seul document standard

IPsec

Internet Key Exchange (IKE)

IKE - version 1

- **IKE** établit 2 niveaux de SA.
- **IKEv1** Phase 1 - Phase 2
- Une SA doit être mise en place pour sécuriser les échanges IKE eux-mêmes
- Il s'agit de l'association de sécurité SA IKE appelée aussi **SA ISAKMP** dans IKEv1.
- Elle est bidirectionnelle.
- Une fois que cette SA IKE est établie, il est alors possible de négocier les SAs IPsec unidirectionnelles pour les protocoles ESP et/ou AH.



Internet Key Exchange (IKE)

IKE - version 2

IKEv2 commence avec deux échanges :

- **IKE_SA_INIT**: négocier les algorithmes cryptographiques, les nonces et les valeurs Diffie Hellman
- **IKE_AUTH**: authentifier les messages IKE_SA_INIT, échanger les identités et les certificats, établir la première association de sécurité IPsec, appelée aussi **SA CHILD.**
- **IKEv2** utilise un échange **CREATE_CHILD_SA** pour créer de nouvelles SA IPsec ou renégocier des clés, IKEv2