



POLYTECHNIQUE
MONTRÉAL

UNIVERSITÉ
D'INGÉNIERIE

INF4420: Éléments de Sécurité Informatique

Sécurité des réseaux : Partie 2



Contenu du cours

- Détection d'intrusion
 - Partie 1 : Différents types d'IDS
 - Partie 2 : Synthèse et exemples
- Protection contre les attaques par inondation
 - Partie 1 : Exemples d'attaques par inondation
 - Partie 2 : Comment se protéger
- VPN
 - Partie 1 : Concept de VPN
 - Partie 2 : VPN IPSec



1. Définitions et identification d'objectifs
 - Quelle est la cible ?
2. Reconnaissance
 - Où se trouve la cible ?
3. Caractérisation (« Fingerprinting »)
 - Identification de vulnérabilité
4. Pénétration
 - Exploitation de vulnérabilité
5. Exploitation
 - Garder l'accès
 - Ne pas se faire prendre
 - Accomplir les objectifs



- But d'un IDS Réseau :
 - Déetecter la présence de vecteurs d'attaque en examinant le trafic réseau
- Méthode de base
 - Le trafic est capturé à un ou plusieurs endroits sur le réseau
 - Examen de chacun des paquets capturés
 - En-tête IP (ICMP, TCP ou UDP)
 - En-tête spécifiques aux applications (e.g. HTTP, FTP)
 - Message ("payload")
 - Un mécanisme de détection est appliqué
 - Des alertes sont générées et enregistrées dans un journal



Systèmes de détection d'intrus (IDS)

- Définitions importantes
- Faux positif
 - Fausse alerte
 - Une alerte est générée par l'IDS alors qu'il n'y a pas d'attaque
- Faux négatif
 - Absence de détection
 - Pas d'alerte alors qu'il y a une attaque
- On peut tester expérimentalement les IDS pour mesurer le taux de faux positifs et de faux négatifs qu'ils génèrent



- Le positionnement des IDS/IPS réseau doit se baser sur la capacité des IDS
 - Bande passante
 - Nombre d'alarmes générées
 - Trafic qu'il est possible d'inspecter
 - Règle vs anomalie
- On ne peut pas inspecter ce qu'on ne peut pas « sniffer »
 - Trafic chiffré
 - Trafic passant sur d'autres segments réseau
- On doit placer les IDS en fonction des risques qu'on cherche à détecter
 - Attaque de Hacker
 - Ver informatique
 - Attaque interne



- Il existe deux types principaux d'IDS
 - Détection par règle
 - Utilise des signatures pour déterminer si une attaque est en cours. Si le trafic intercepté contient une signature, une alarme est levée.
 - Déetecte uniquement des attaques pour lesquelles des signatures existent
 - Détection par anomalie
 - Utilise la déviation statistique à partir de l'utilisation normale (baseline) pour déterminer si une attaque est en cours. Si le trafic intercepté dévie de façon trop grande de la normale, une alarme est levée.
 - Doit avoir une situation normale avec un profil statistique très délimité
- Les deux types fonctionnent à partir d'alertes
 - Un humain doit traiter les alertes
 - Les alertes peuvent être regroupées et combinés



- Détection « par règle »
 - Ou par « signature »
 - Examen de chacun des paquets capturés
 - En-tête IP (ICMP, TCP ou UDP)
 - Payload (DPI – Deep Packet Inspection)
 - Application de règles pour détection d'attaques
 - Signatures d'attaques réseaux (e.g. "Land attack")
 - Signatures de code malveillant (e.g. traîneau de NOP, /bin/sh)
 - Signature spécifique à un outil (e.g. message spécifique envoyé par un Botnet pour activer les machines esclaves)



- Paradigme général des IDS par « signature »
 - « X évènements de type Y dans un temps Z »
- Exemples de règles possibles
 - 1 paquet dont la « payload » contient une suite de plus de 25 « A » ou « C » (bourrage typique pour les buffer overflow)
 - 1 paquet dont la configuration des drapeaux ne suit pas la spécification du protocole (x-mas scan)
 - 10 paquets provenant de la même source sur des ports différents (port scan)
 - 20 paquets de type SYN vers la même destination sans paquet ACK correspondant (SYN flood)



- Limites de l'approche par « signature »
- Limite 1
 - Seules les attaques connues (pour lesquelles une signature existe) seront détectées
 - Ne permet pas de détecter les nouvelles attaques (« zero-day » en anglais)
 - Conséquence : Il est nécessaire de mettre à jour régulièrement la base de signatures (comme un anti-virus)
- Limite 2
 - Les signatures correspondent à des motifs en général fixes.
 - Or, une attaque n'est pas toujours identique à 100%.
 - Le moindre octet différent par rapport à la signature provoquera la non détection de l'attaque
- Limite 3
 - Il est nécessaire d'adapter la base de signatures en fonction du système à protéger
 - Inutile d'appliquer une signature d'attaque pour Windows si on est sous Linux



- Détection « par anomalie »
 - On parle aussi d'approche comportementale
 - Examen de chacun des paquets capturé
 - Application de calculs statistiques pour déterminer si une attaque est en cours
 - Variation dans le volume de trafic
 - Communication à des heures anormales
 - Trafic sur des ports « anormaux »
 - Etc.



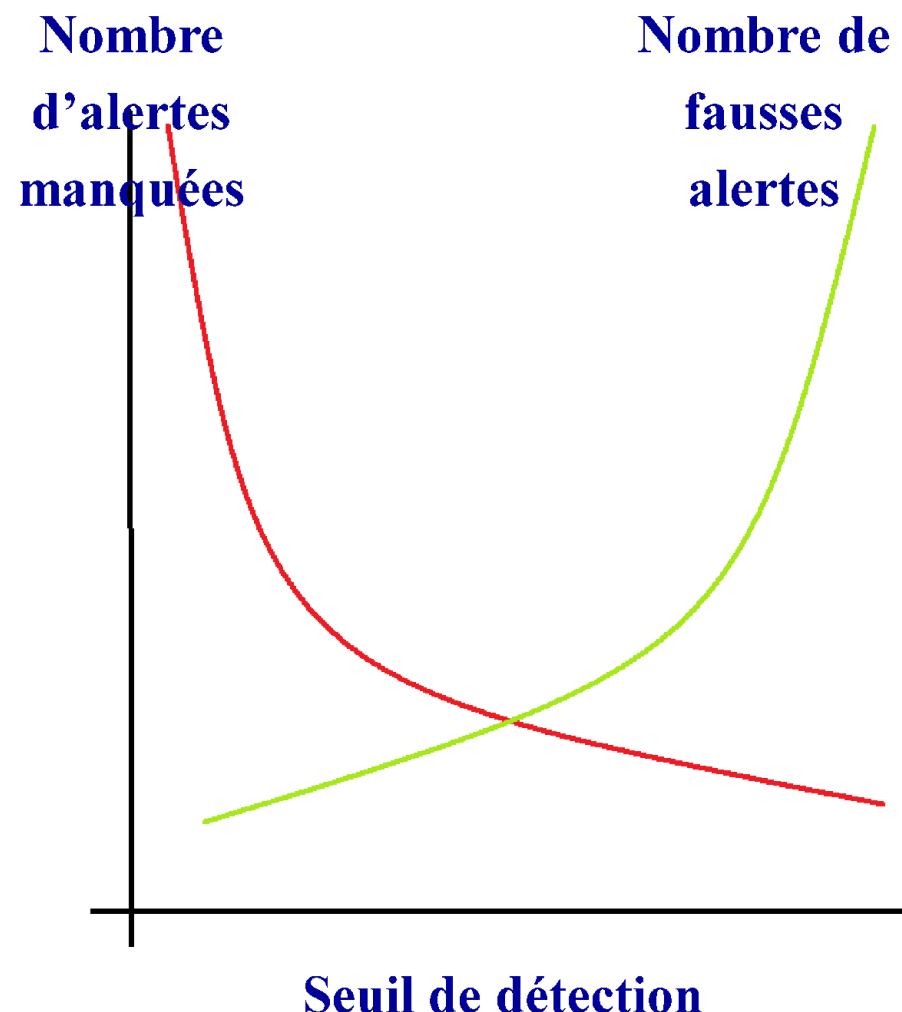
- Paradigme général
 - « X évènements déviant du baseline dans un temps Z »
- Construction d'un profil « normal »
 - Besoin des choisir des attributs représentatifs
 - On parle de métriques ou d'indicateurs (« features » en Anglais)
- Utilisation de techniques d'apprentissage reposant sur l'Intelligence Artificielle
 - Machine Learning
 - Deep Learning



- Exemples d'indicateurs
 - Charge CPU
 - Volume de données échangées
 - Temps de connexion sur des ressources
 - Répartition statistique des protocoles et applications utilisés
 - Heures de connexion, ...
- Plus la normale est facilement identifiable, plus les attaques seront facilement identifiées comme des « outliers » statistique
 - Éviter des indicateurs qui changent de façon aléatoire
 - Difficulté pour analyser du trafic Web



- L'approche comportementale doit être calibrée pour notre réseau
- Si on augmente le seuil de détection, on réduit le nombre d'alertes manquées, mais on augmente le nombre de fausses alertes
- Il faut faire un compromis en fonction du coût opérationnel d'investiguer les alertes





- Avantage de l'approche comportementale
 - En théorie, possibilité de détecter de nouvelles attaques (zero-day)
 - Dès lors que la nouvelle attaque conduit à une déviation des indicateurs choisis
 - Dans la pratique, peu de résultats probants
 - Notamment, difficulté de séparer la nouvelle attaque des faux positifs



- Limites des approches comportementales
- Limite 1
 - Risque de faux positifs : tout changement dans les habitudes de l'utilisateur provoque une alerte
- Limite 2
 - Nécessite une période de fonctionnement sans intrusion pour mettre en œuvre les mécanismes d'apprentissage
 - Si un pirate attaque pendant cette période, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement mis en place
- Limite 3
 - Attaque adverse contre l'apprentissage
 - Le pirate peut discrètement intervenir pour modifier le profil de l'utilisateur afin d'obtenir après plusieurs jours ou semaines, un profil qui lui permettra de mettre en place son attaque sans qu'elle ne soit détectée



Types d'implantation

- Network-based IDS (NIDS)
 - Vu dans la partie 1
- Host-based IDS (HIDS)
 - Logiciel ajouté sur un serveur ou un client
 - Objectifs
 - Analyser les logs systèmes et applicatifs
 - Intercepter et analyser les commandes systèmes
 - Déetecter les modifications illégales de logiciel (attaque par Rootkit)
 - Avantages
 - Configuration des règles plus précises, étant donné que le contexte est connu
 - Débit plus bas, donc moins demandant en terme de puissance de calcul
 - Peut être intégré dans un anti-virus

- Combiner approche par signature et approche comportementale
- Utilisation des techniques de « Machine Learning » pour l'approche comportementale
 - Les réseaux de neurones et le « Deep Learning » sont à la mode
 - Mais on utilise aussi d'autres méthodes
 - Arbres de décision, Random Forest, SVM (Support Vector Machine), Algorithme génétique, etc.
- Intégrer les connaissances métiers dans l'IDS
 - Organisation du travail (workflow)
 - Processus industriel
 - Etc.



IDS/IPS : Tendances actuelles

- « Intrusion Prevention Systems » (IPS)
 - Associe des actions de protection aux alertes
 - Actions typiques
 - Bloquer un port
 - Bloquer une machine ou un sous réseau
 - Rejeter des paquets
 - Peut être dangereux sur des faux positifs
- « Network Appliances »
 - Peuvent intégrer
 - Pare-feu
 - IDS et IPS
 - DéTECTeur de virus
 - Utilise du matériel spécialisé (e.g. FPGA) pour pouvoir analyser des hauts débits (Gbit/s)

Exemple d'IDS : Snort

- Snort est un NIDS reposant sur l'approche par signature
 - Snort est aujourd'hui la propriété de SourceFire
- Snort est un logiciel « ouvert »
 - Possibilité de définir sa propre base de signatures d'attaques
 - De nombreuses bases de signatures ont déjà été développées pour Snort
 - Possibilité de réutiliser ou de compléter les bases existantes

Exemple d'IDS : Snort

- Exemple de signature Snort

```
alert tcp any any -> 192.168.1.0/24 143  
(content: "|9068 C0FF FFFF|/bin/sh";  
msg: "IMAP buffer overflow"; )
```

- Le langage de signature de Snort propose de très nombreuses options
 - Mais analyse limitée au niveau du paquet IP
 - Pas de reconstruction de sessions TCP
 - Détection « stateless »
- Voir aussi les NIDS Suricata et Zeek (anciennement Bro)

IDS et IPS : La couche supervision

- Les SIEM : Security Information and Event Management
- SIEM (définition) : logiciel permettant de gérer et corrélérer des événements de sécurité.
- Fonctions du SIEM :
 - Collecte : alertes remontées par les IDS / IPS, journaux des équipements système et réseau (pare-feux, routeurs, serveurs, bases de données, ...)
 - Normalisation : format lisible permettant des recherches multi-critères et enrichissement
 - Agrégation : regrouper et réduire le nombre d'événements
 - Corrélation : application de règles logiques ou statistiques
 - Reporting : création et gestion des tableaux de bord
 - Archivage : besoin de garantir l'intégrité des traces pour avoir une valeur probante juridique et réglementaire
 - Rejet des événements : permet de mener des investigations post-incidents

IDS et IPS : La couche supervision

- Exemple de SIEM : *Prelude*
 - Deux versions
 - Prelude SIEM : SIEM commercialisée aujourd'hui par C-S (Communication et Systèmes)
 - Prelude OSS : version Open Source sous licence GPL2
1. Implémentation des différentes fonctionnalités d'un SIEM + chiffrement des communications
 2. Normalisation des événements au format IDMEF (standard IETF)
 - Intrusion Detection Message Exchange Format
 3. Corrélation des événements remontés par les sources suivantes :
 - SNORT
 - Anti-Virus
 - Prelude LML (Log Management Laky)
 - NESSUS (Scanner de vulnérabilités)
 - OSSEC (Activité système LINUX)

Attaques de déni de services (DoS)

- Objectifs d'un Denial of Service (DoS)
 - Éliminer ou réduire la qualité de service d'un fournisseur de services
- Types
 - Par vulnérabilité (« crippling DoS »)
 - Par saturation (« Flood DoS »)
 - Par absorption (« Black hole DoS »)
- Particularités
 - Pas de pénétration
 - Camouflage optionnel
 - Pas de contre-mesures absolues !!



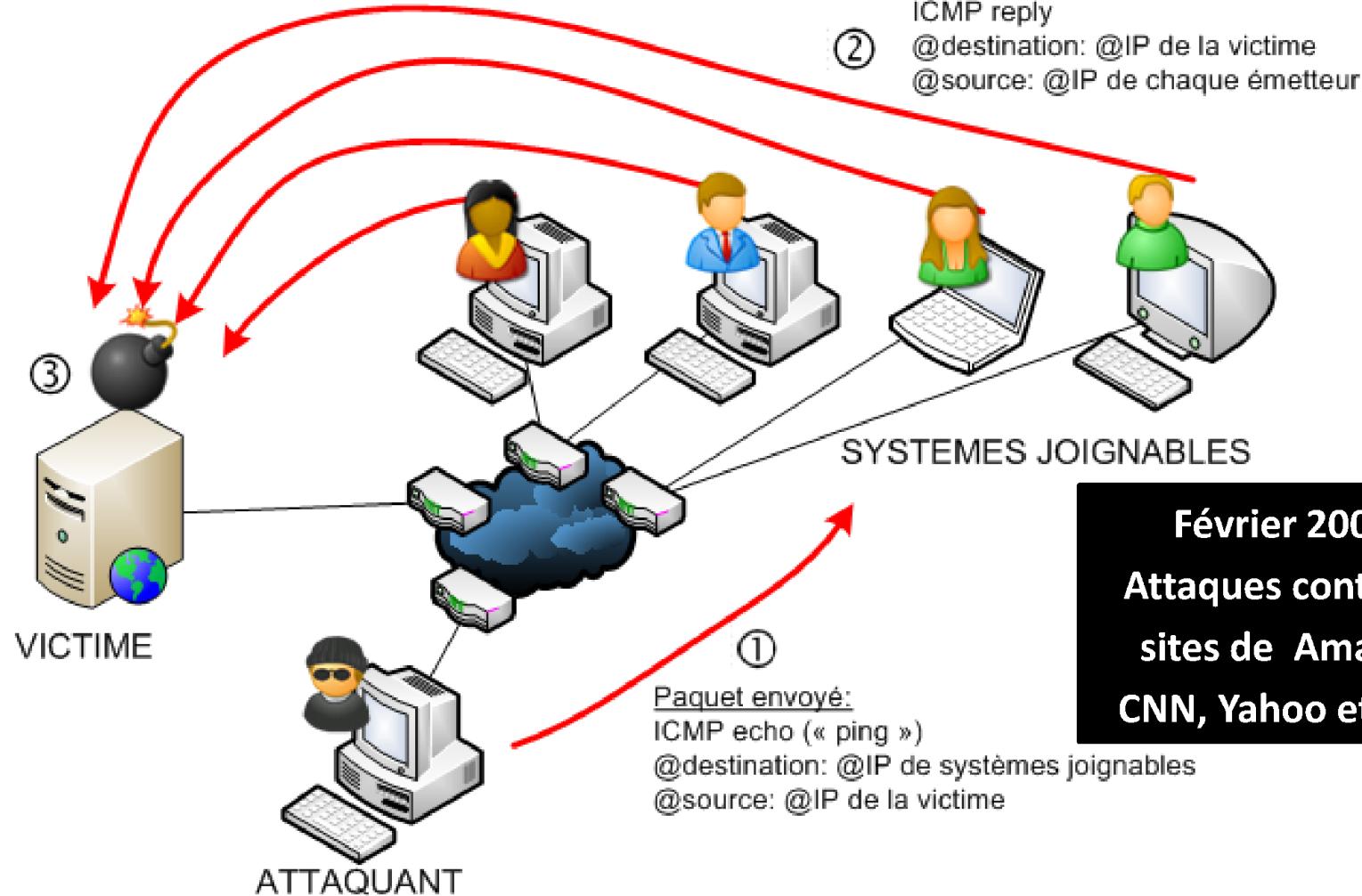
Attaques de déni de services (DoS)

- Différents types de flooding
 - Flooding TCP (e.g. Syn Flooding, déjà présenté)
 - Flooding UDP (très facile)
 - Flooding ICMP
 - Flooding HTTP
 - SlowLoris
 - Ouverture de sessions HTTP puis renvoi de requêtes bidon pour maintenir les sessions ouvertes
 - Etc.



Exemple de flooding ICMP

- Smurf attack (attaque par réflexion)



Février 2000 :
Attaques contre les
sites de Amazon,
CNN, Yahoo et eBay

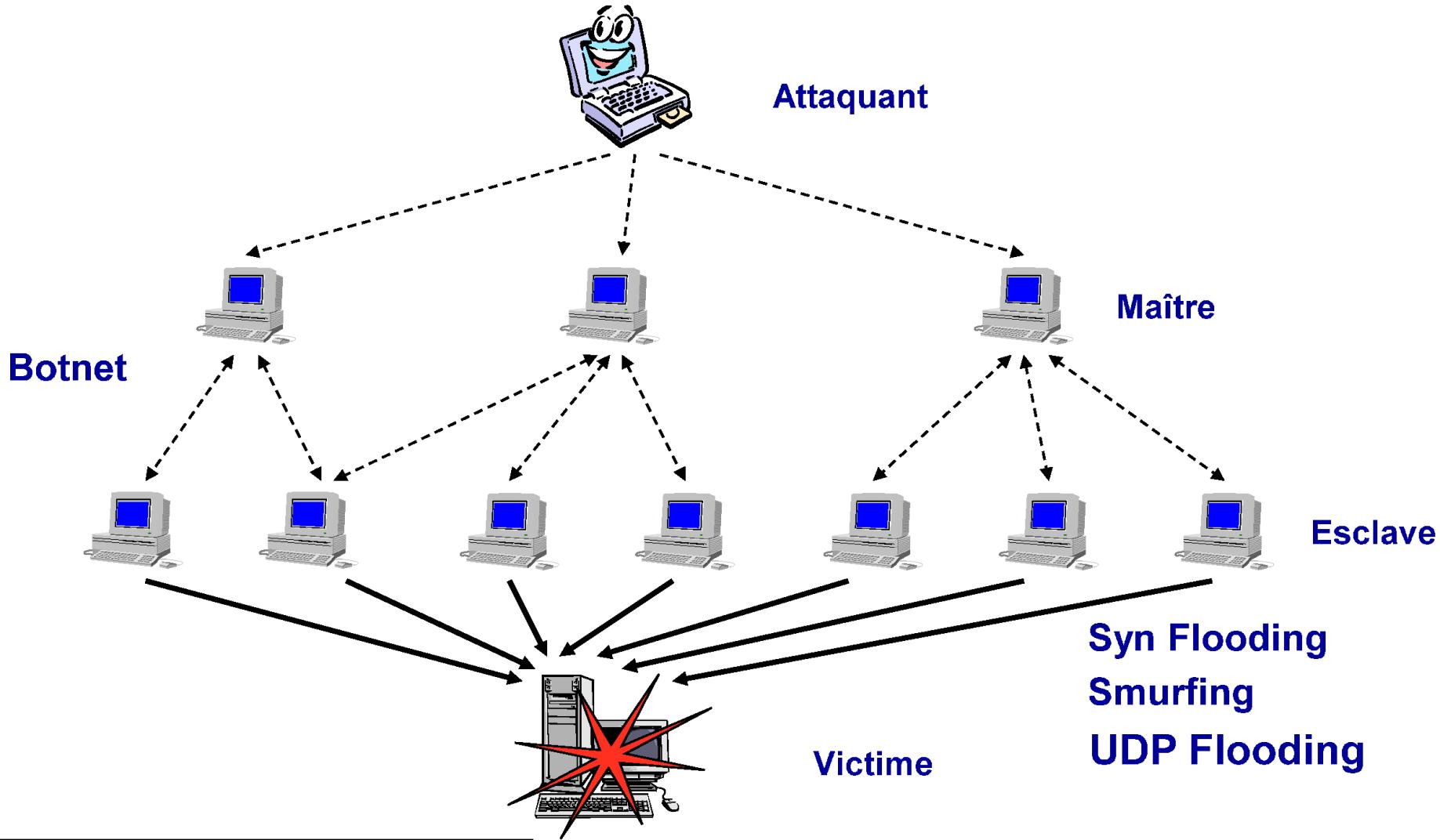
Exemple de flooding ICMP

- Smurf attack (attaque par réflexion)
- Quelles sont les caractéristiques de l'attaque ?
 - usurpation d'adresse IP (spoofing)
 - réflexion de trafic en ayant recours à des systèmes tiers « innocents »
- Séquences de l'attaque
 1. Un attaquant envoie des paquets PING à des systèmes tiers joignables en indiquant l'@IP de la future victime comme @IP source
 2. Chaque système pense ainsi recevoir un PING de la part d'un système distant, et chacun va répondre à ce PING
 3. Avec suffisamment de ressources, l'attaquant sera en mesure de faire générer suffisamment de trafic pour affecter les performances de la victime.



DDoS

- Réalisation d'un DoS distribué (DDoS) par un botnet





- Exemple de Botnet

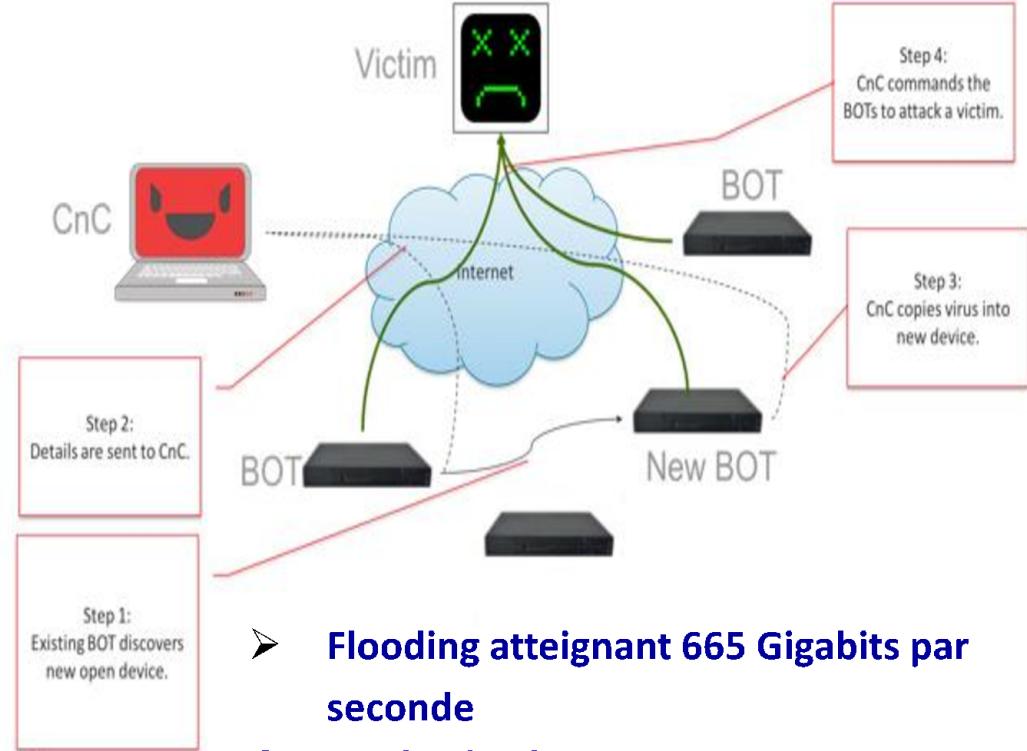
- MIRAI botnet

Attaque en DDoS contre le site de KrebsOnSecurity le 20/09/2016

- MIRAI : botnet constitué d'objets connectés

Routers, caméras IP ou systèmes d'enregistrement vidéos

- MIRAI utilise des mots de passe faibles ou mots de passe codés en dur
 - MIRAI exploite des malwares comme Lizkebab,” “BASHLITE, “gafgyt”



➤ Flooding atteignant 665 Gigabits par seconde

Attaque la plus importante connue jusqu'alors atteignait 363 Gbps

➤ Puis 1Tbit/s

Attaque contre les serveurs d'OVH

➤ Et 1.2Tbit/s

Attaque contre la société DYN

- Plusieurs types de flooding (TCP, UDP, ICMP, HTTP)
 - Attaques simples et très efficaces
- Pas de solution de protection « parfaite » aujourd’hui
- Plusieurs approches complémentaires
 - Configuration du pare-feu
 - Protection au niveau du protocole TCP
 - Utilisation de répartiteur de charge
- La plupart de ces fonctionnalités sont intégrées dans les ADC
 - Application Delivery Controller

(1) Configuration du pare-feu

- Règle 1 : Vérifier que le trafic entrant sur Eth0 correspond à des adresses externes
 - Efficace pour bloquer les attaques par réflexion (smurfing)
- Règle 2 : Vérifier que le trafic sortant sur Eth1 correspond à des adresses internes
 - Efficace pour détecter si une machine hôte est utilisée comme esclave par un botnet
- Remarque : les hôtes esclaves dans les botnets utilisent de moins en moins de trafic spoofé

Voir les règles de bonne pratique des RFC 2979 (Firewall requirements) et RFC 2267 (Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing)



Protection contre les attaques par inondation

(2) Protection au niveau du protocole TCP

- Timer associé à la pile TCP
 - Les demandes SYN sont éliminées de la pile si un message ACK n'est pas reçu avant que le timer ne soit écoulé
 - Utile mais insuffisant pour résister

(2) Protection au niveau du protocole TCP

- Syn Cookie (1/3)
- Exemple d'établissement d'une session TCP:

Client

flags: SYN = 1, ACK = 0 SN : 56

flags: SYN = 1, ACK = 1 SN : 90, ACK : 57

flags: SYN = 0, ACK = 1 SN : 57, ACK : 91

Serveur

Pile TCP utilisée pour créer le contexte

Connexion établie

SYN Flooding va créer le déni de service en saturant la pile TCP

(2) Protection au niveau du protocole TCP

- Syn Cookie (2/3)
- Avec un Syncookie, le réseau devient une ressource mémoire qui remplace la pile TCP

Client

flags: SYN = 1, ACK = 0 SN : 56

Serveur

flags: SYN = 1, ACK = 1 SN : syncookie, ACK : 57

flags: SYN = 0, ACK = 1 SN : 55, ACK : syncookie + 1

(2) Protection au niveau du protocole TCP

- Syn Cookie (3/3)
- Le syncookie est généralement dans le champ acquittement sur 24 bits (sur 32 disponibles)
 - Codages des adresses source et destination, numéros de port et compteur de temps
 - En décodant le syncookie renvoyé par le client, le serveur retrouve les informations pour établir la connexion
- Remarques
 - Le syncookie est transparent coté client (pas besoin de mise à jour coté client)
 - Le syncookie est généralement couplé au fonctionnement normal de la pile TCP (le serveur bascule sur les syncookies lorsque la pile est pleine)



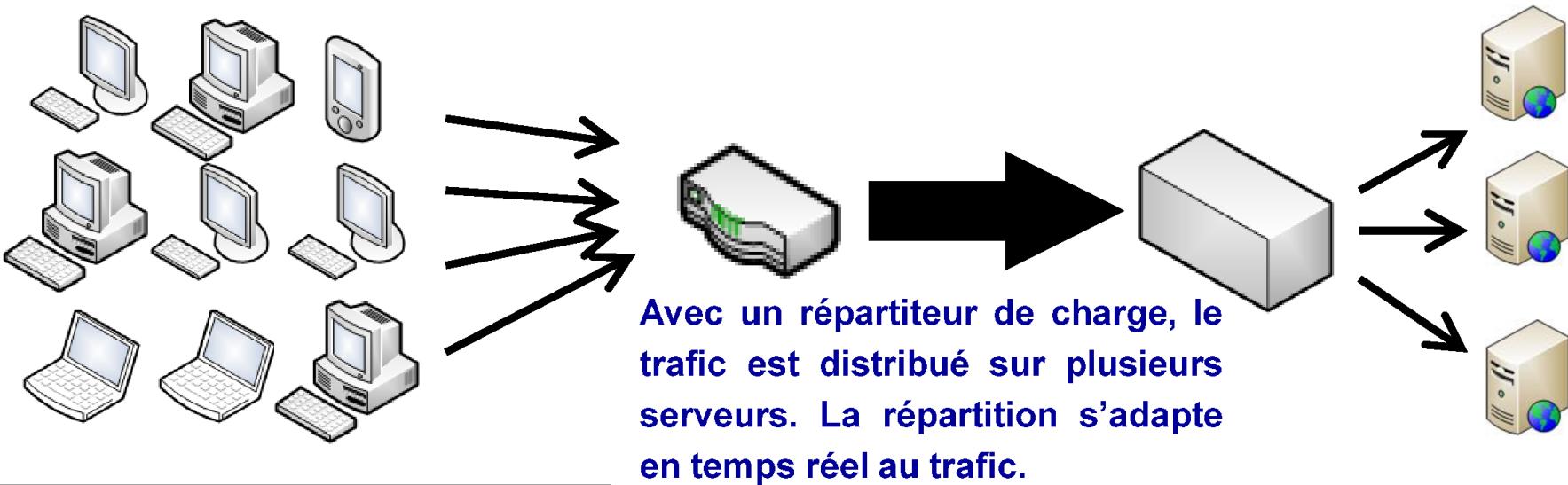
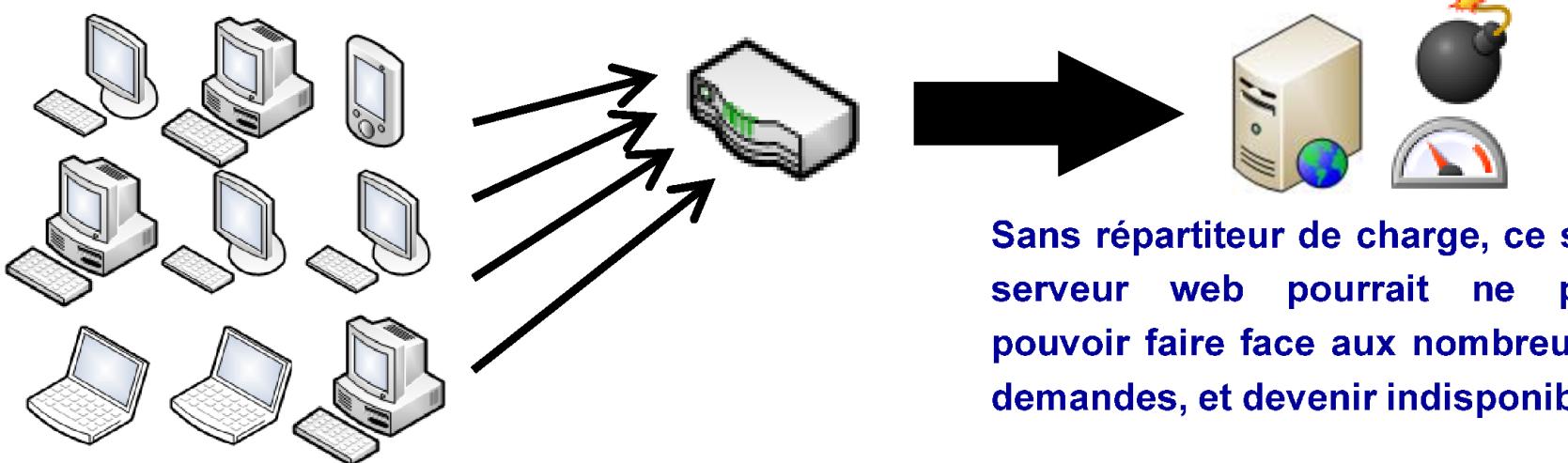
(3) Répartiteur de charge

- « Load-balancer » en anglais ;
 - Équipement rencontré sur les grosses infrastructures où les serveurs doivent faire face à de très fortes bandes passantes et charges élevées de trafic
 - Équipement chargé de répartir/distribuer la charge réseau en fonction des caractéristiques de celui-ci et de la disponibilité des serveurs
 - Avantage sécurité : permet de mieux se protéger contre les dénis de service distribués



Protection contre les attaques par inondation

(3) Répartiteur de charge





(4) Autres mécanismes

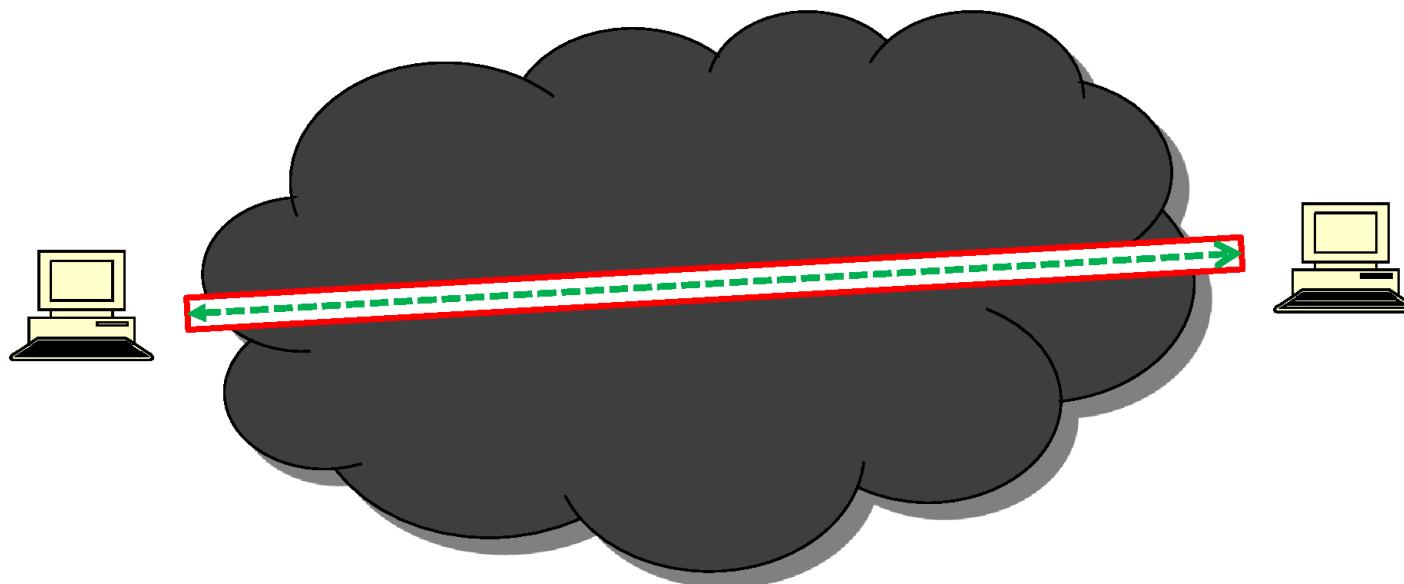
- Liste blanche
 - N'autoriser que le trafic nécessaire
- Prioriser le trafic
- uRPF (unicast Reverse Path Forwarding)
 - Technique pour détecter le spoofing
 - Consiste à comparer l'adresse IP source du paquet à la table de routage
 - Rejeter le paquet s'il ne provient pas de l'interface que le routeur aurait utilisé pour router la source du paquet
- Utilisation d'un NIDS comportemental
 - Pour détecter le trafic anormal



- Un réseau privé virtuel, ou VPN (virtual private network) est l'extension du réseau privé à travers un réseau public
- Permet à des usagers distants de se connecter à notre réseau comme s'ils étaient connectés sur le réseau local
 - Étend le NAT



- Utilise le concept de tunnel
 - Pour traverser une zone hostile (montagne, cours d'eau), on fait un tunnel, c'est-à-dire un trou enrobé d'une couche de protection, et on relie deux routes distantes





- **Remarque**

- Le concept de tunnel n'implique pas nécessairement que les données transitant dans le tunnel sont chiffrées
- Exemple : Tunnel MPLS
- Marquage des paquets pour la traçabilité et le routage des paquets
- Dans le cas d'un VPN, le tunnel est chiffré



- Le tunnel VPN offre plusieurs services :
 - Protège la confidentialité des données
 - Prévient l'interception de trafic
 - Prévient la modification de trafic en transit
 - Prévient la connexion par des utilisateurs non autorisés
- Plusieurs méthodes d'établir le tunnel :
 - IPSec
 - SSL
 - Pptp (VPN natif sous Windows)
 - Etc.
- Tout protocole point-à-point pouvant supporter du chiffrement et de l'authentification peut faire office de tunnel pour établir un VPN

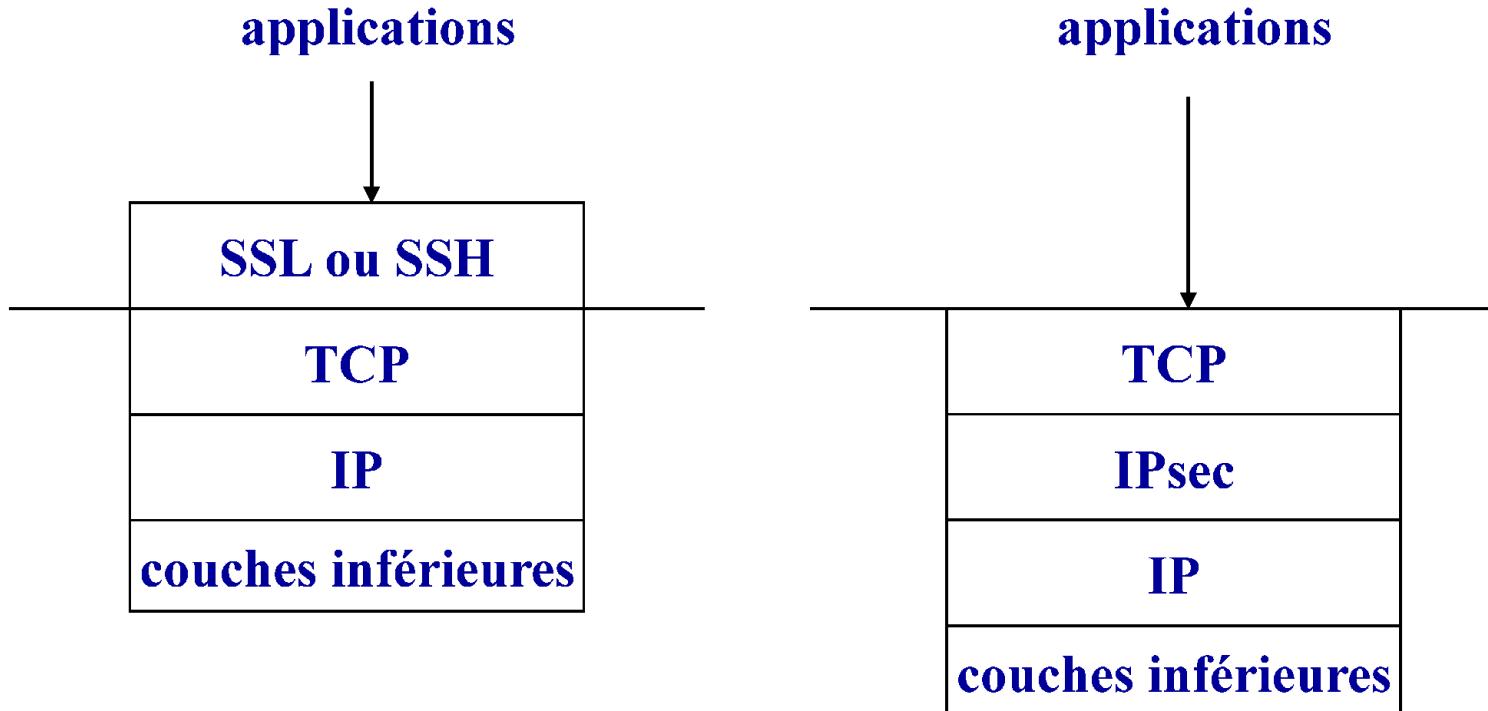


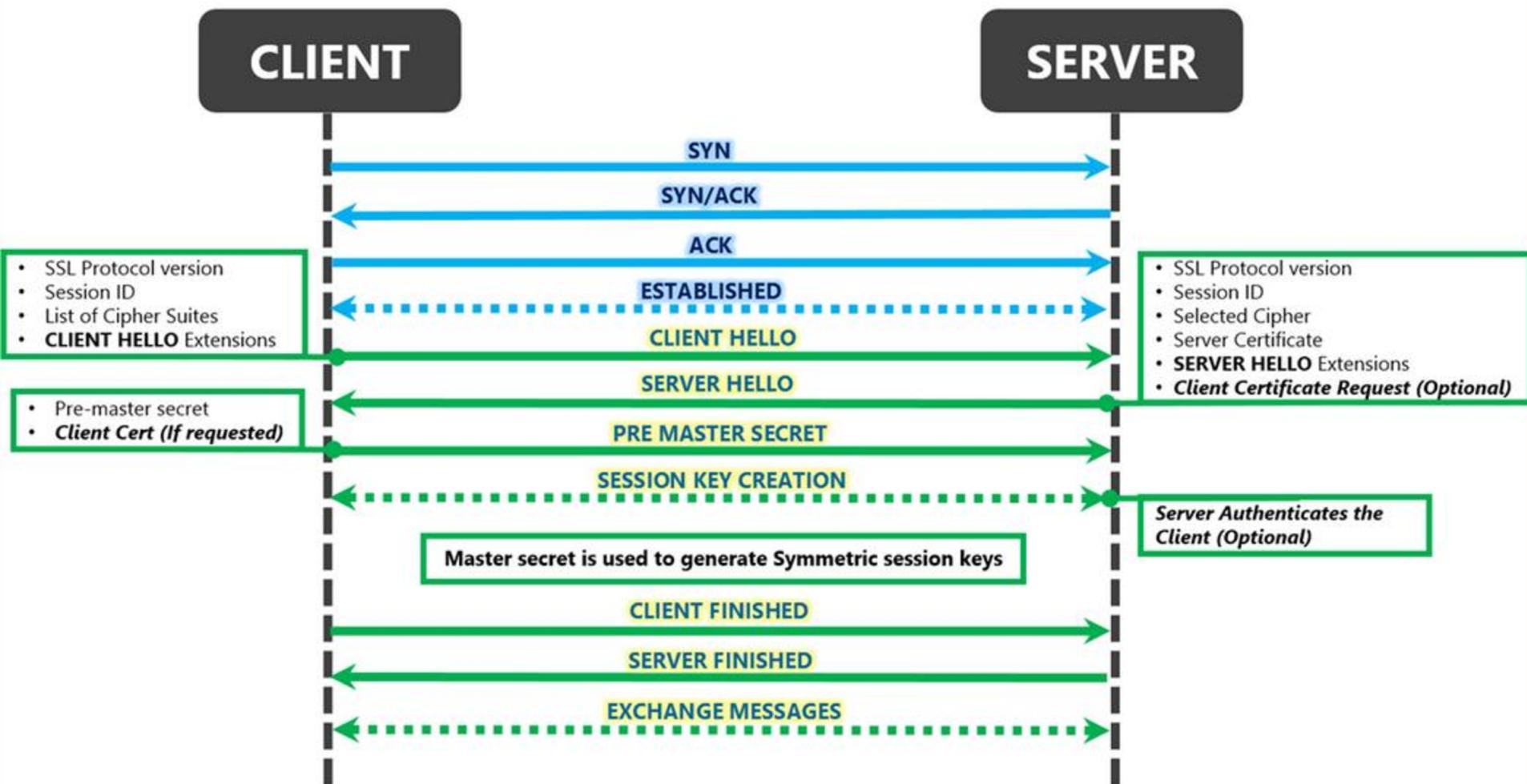
- Puisque le trafic transitant par le VPN est chiffré, il ne peut pas être inspecté
 - Impact pare-feu
 - Impact IDS
- Puisqu'il arrive sur une interface particulière, on doit établir des règles de pare-feu uniquement pour l'interface VPN
- Faire attention à la confiance qu'on donne aux clients arrivant par VPN
 - Sécurité des postes de travail distants
 - Sécurité des partenaires



VPN : Protocoles sécuritaires

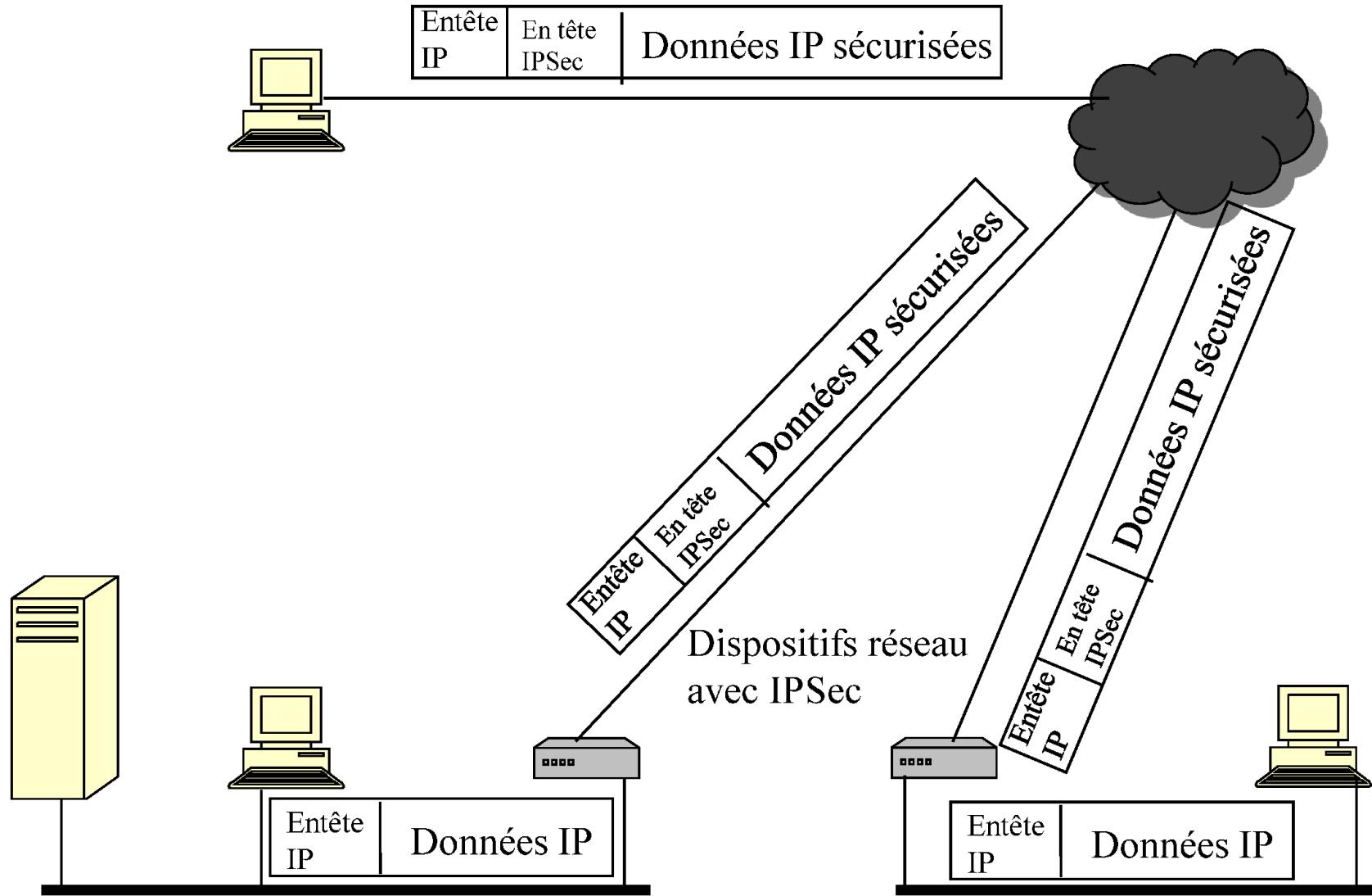
- SSH
- SSL/TLS (supporte https, SMTP, IMAP, etc.)
- IPSEC







- IPSEC
 - Solution VPN intégrée dans IPv6
 - Compatible avec la version courante: IPv4
- Applications
 - communication sécurisée de l'extérieur vers l'intérieur d'un intranet sécurisé
 - connectivité sécurisée entre deux intranets
 - sécurité supplémentaire aux applications ayant leur propre sécurité
- Offert par plusieurs fournisseurs de produits
 - En particulier utilisé pour la mise en place de VPN par Cisco





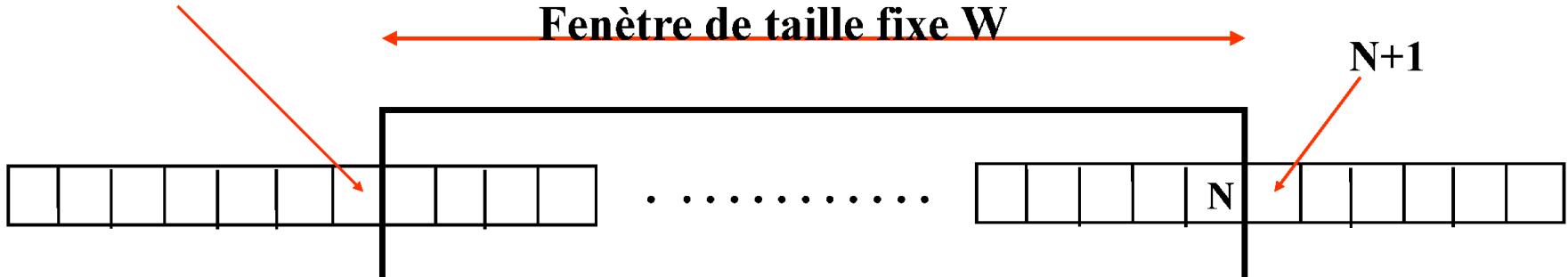
- Services:
 - contrôle d'accès
 - intégrité des paquets
 - authentification de l'origine (adresse IP)
 - rejet de paquets "rejoués"
 - confidentialité par chiffrement
- Protocoles:
 - authentification: entête de type AH (Authentication Header)
 - chiffrement seul: entête de type ESP (Encapsulating Security Payload)
 - ESP plus AH



Concept de fenêtre de séquencement

- Mécanisme anti-réutilisation
 - si un nouveau paquet tombe dans la fenêtre et qu'il est authentifié, il est marqué
 - si un nouveau paquet reçu est authentifié et se situe à droite de la fenêtre, la fenêtre est avancée
 - si le paquet reçu est à gauche de la fenêtre, ou qu'il n'est pas authentifié, il est rejeté

Numéro de séquence $N-W$





Modes

- Mode « tunnel »
 - protection d'un paquet au complet
 - après l'ajout de l'entête approprié, un nouvel entête IP est ajouté

Nouvel entête IP	AH	Entête IP original	TCP	Données à transmettre
------------------	----	--------------------	-----	-----------------------

- Mode « transport »
 - protection surtout pour les protocoles de plus haut niveau
 - simple ajout d'un entête approprié

Entête IP original	AH	TCP	Données à transmettre
--------------------	----	-----	-----------------------



- Concept de Security Association :
 - Relation unidirectionnelle entre un émetteur et un récepteur
 - Identifiée par:
 - SPI:"Security Parameter Index"
 - adresse de destination IP
 - identificateur de protocole de sécurité: AH ou ESP
 - Paramétré par:
 - compteur de messages: pour numérotter et éviter la réutilisation
 - indicateur d'action en cas de débordement de ce compteur
 - largeur de la fenêtre de séquencement
 - informations spécifiques au protocole choisi
 - durée de vie de cette association: en octets transmis ou en temps
 - mode IPSec: transport, tunnel, ou "wildcard"
 - taille maximale de paquet et autres variables



- Internet Security Association and Key Management Protocol (ISAKMP) & IKE
 - Utilise des algorithmes de clés publiques pour établir des clés de sessions
 - Ces clés de sessions protègent les paquets dans une SA
- Les outils d'attaque tentent de briser IKE en faisant une attaque de force brute sur la clé pré-échangée (PSK)
 - IKECrack
 - Cain & Abel



- Bénéfices :
 - Sécurité forte à tout trafic qui traverse le périmètre protégé
 - Ajoute à la sécurité d'un pare-feu
 - Sécurise les usagers individuels si requis
 - Ajoute à la sécurité des routeurs en assurant que...
 - l'annonce d'un nouveau routeur vient d'une source autorisée
 - même chose pour un routeur dans un autre domaine
 - un message redirigé vient bien du routeur auquel il a été originalement envoyé
 - une mise à jour d'un routeur n'a pas été falsifiée



POLYTECHNIQUE
MONTRÉAL

UNIVERSITÉ
D'INGÉNIERIE

A la semaine prochaine