

M1

Sécurité des systèmes d'informations

2023-2024

SESSION

Partie
1



Aujourd’hui : Session 4 : Les aspects réseaux et applicatifs

- Correction TP3
- La sécurité du protocole IP
- Sécurisation d'un réseau
- Les bases de la cryptographie
- Serveurs applicatifs



- La sécurité du protocole IP
- Sécurisation d'un réseau
- Les bases de la cryptographie
- Serveurs applicatifs

Correction TP 3

- Sujet :
 - Décrivez les types d'attaques 'ciblée' et 'non ciblée' ?
- Réponse attendue :
 - Ciblée
 - Ingénierie sociale, Malware, Réseau...
 - Non ciblée
 - Phishing, Malware, virus, Scan, bots...

Virus informatique (1/2)



- Programme se dupliquant
 - sur d'autres ordinateurs
 - s'accrochant à des logiciels existants
- Perturbe le fonctionnement de l'ordinateur infecté
- Se répand par tous les moyens :
 - Clé USB, CD, disquettes, Bluetooth, réseau, etc.
- Plus de 100 000 virus connus aujourd'hui
- Grande majorité sur Windows
- Plusieurs types :
 - « Classique », boot, macrovirus, virus-vers, etc.

Virus informatique (2/2)



- Exemple les plus connus :
 - MyDoom.A
 - scan de l'ordinateur et envoie d'emails
 - Psyb0t
 - chercher des failles sur MySQL, PHPMyAdmin et DDoS
 - Tchernobyl
 - destructeur pour la machine physique. Réécriture du BIOS
 - Rançongiciel ou Ransomware
 - bloque l'ordinateur et se déverrouille contre rançon
 - BRAIN, le plus vieux (1986)
 - Bloque le boot des disquettes de démarrage

Spyware



- Logiciel espion en Français
- Collecte d'informations sur la machine de l'utilisateur
- Présents dans des gratuiciels
 - Mais aussi dans des cracks / keygen
 - Faux codecs
 - Sur des sites de streaming

Malware



- Publiciel en Français
- Logiciel qui affiche des publicités lors de son utilisation
- Couplé à des Spyware, pour afficher des publicités ciblées
- Exemple
 - Edition du fichier hosts des devices



- Type de malware
- Logiciel malveillant
 - Propagation d'un ordinateur à un autre
- Capacité de se dupliquer
- Ne s'accroche pas à des logiciels
 - comme les virus
- Diffusion
 - par réseau, courriel, messagerie instantanée

Vers (2/2) Exemple



- ver Sasser
 - Lié à une faille de sécurité publiée par Microsoft, et qui n'a pas été corrigée sur toutes les machines via les mises à jour de l'OS
- ver Blaster
 - Ordinateur qui s'éteind toutes les 60 secondes
Attaque de type DDoS

Phishing (1/2)



CORRECTION

- L'hameçonnage consiste à envoyer des e-mails
 - Qui semblent provenir de sources fiables
- But
 - Obtenir des informations personnelles
 - Inciter les utilisateurs à faire quelque chose.
- Technique combine ingénierie sociale et stratagème technique.
- Impliquer une pièce jointe à un e-mail
 - Charge
 - Logiciel malveillant sur votre ordinateur.
 - Utiliser un lien pointant vers un site Web illégitime



- Réduire le risque d'être victime d'un hameçonnage
 - Esprit critique
 - Ne prenez pas un e-mail pour argent comptant
 - Faites une petite pause et analysez cet e-mail.
 - Passer le curseur sur les liens
 - Déplacez votre curseur de souris sur les liens, mais sans cliquer !
 - Analyse des en-têtes des e-mails
 - Les en-têtes des e-mails indiquent comment un e-mail est arrivé à votre adresse
 - Sandboxing
 - Vous pouvez tester le contenu d'un e-mail dans un environnement sandbox

Chevaux de Troie (Trojan)



- Comme la légende Grecque
 - Programme “inoffensif” à la différence des Virus / Vers
 - Permet d'installer un logiciel divers
 - Mais qui contient souvent un programme malveillant

Ransomware (rançongiciels)



CORRECTION

- Logiciel malveillant
- Bloque l'accès aux données de la victime
 - Menace de les publier ou de les supprimer à moins qu'une rançon ne soit versée.
- Attaque
 - Simple
 - Verrouiller le système d'une manière qui n'est pas difficile à réparer pour une personne bien informée
 - Avancé
 - Utilisera une technique appelée extorsion cryptovirale
 - Chiffre les fichiers de la victime de manière à les rendre presque impossible à récupérer sans la clé de déchiffrement.

Spoofing



CORRECTION

- Ensemble des cyberattaques

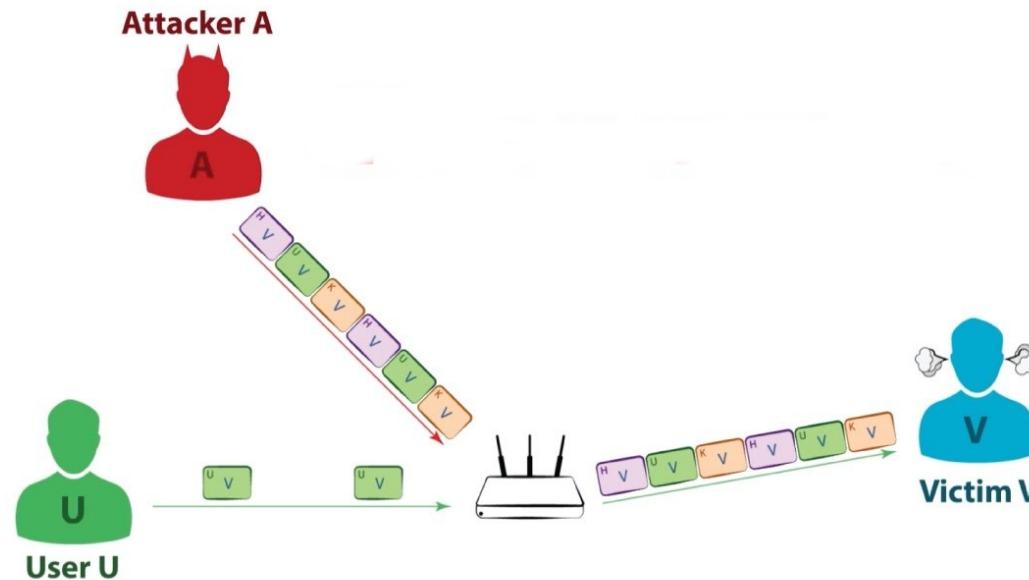
- Consiste

- Vol de l'identité électronique telle que

- Adresse mail, le nom de domaine ou l'adresse IP

- But

- Obtenir des informations bancaires et confidentielles.

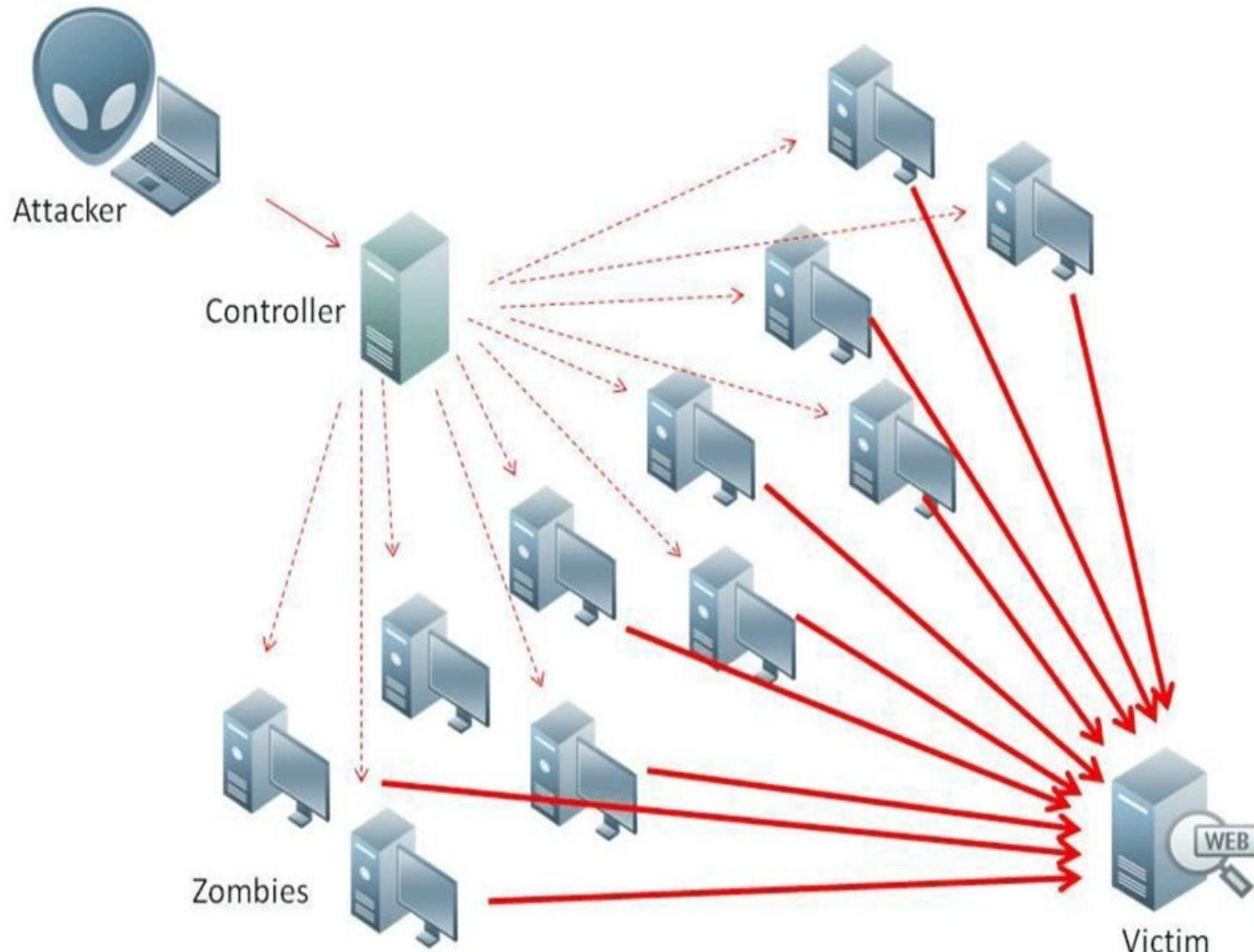




- Denial of Service attack (DoS) / Distributed Denial of Service attack (DDoS)
 - Inondation d'un réseau
 - Perturbation des machines d'un réseau
- Peut être faite depuis 1 seule machine avec une forte bande passante
- Peut être décentralisée avec des groupuscules de cyber terroristes
 - Orchestration d'attaque
- Cas de la Chine : sur Baidu vs les USA
 - <http://www.digitalattackmap.com>

DDoS / Déni de service (2/

CORRECTION

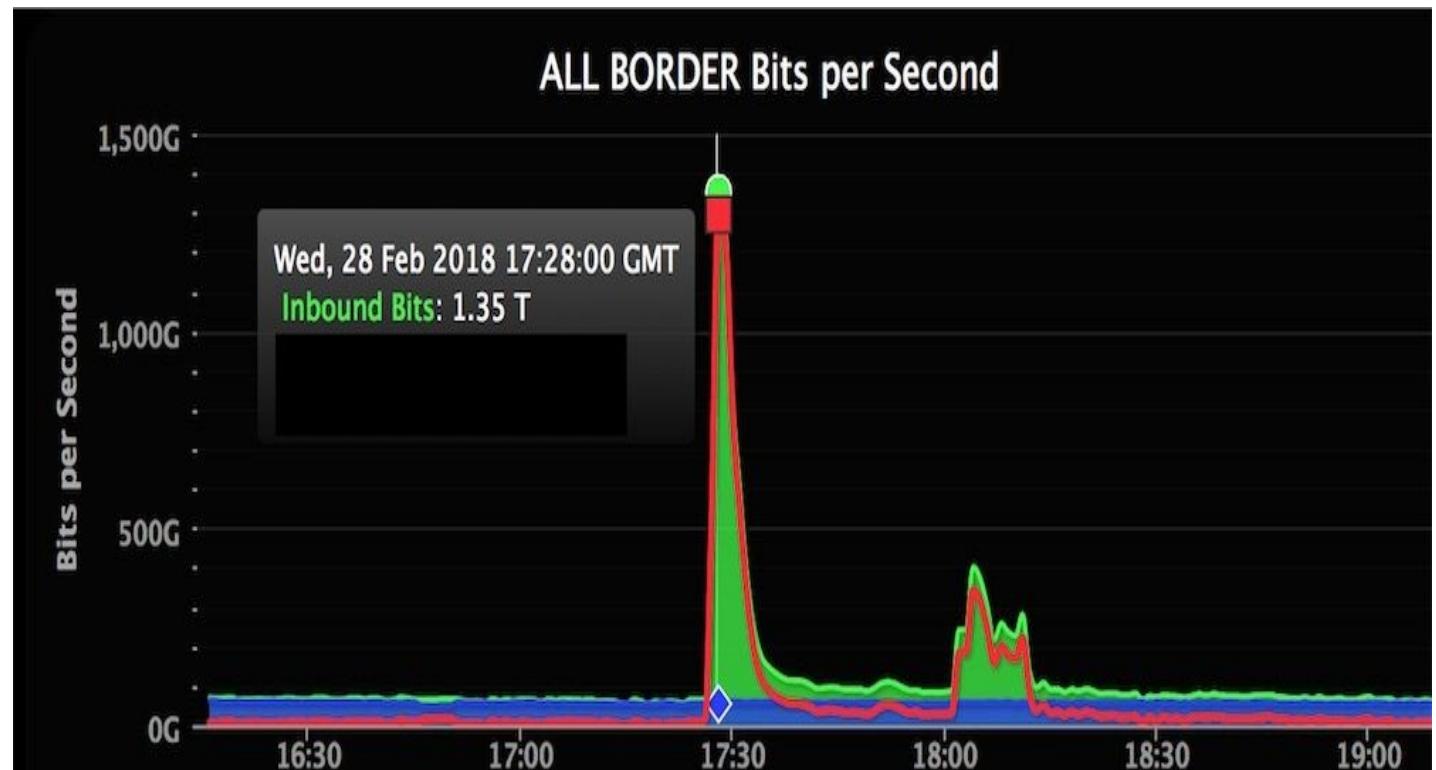


DDoS / Déni de service (3/

CORRECTION



- Plus grosse attaque DDoS
 - Github le 28 février 2018
- 1,35 Tbps en pic
- Faille Memcached



Logiciel connu pour du DDoS

CORRECTION



- Pour windows : Loïc



Logiciel connu pour du DDoS

CORRECTION



- Pour UNIX : siege

```
[11:02:04] in ~ | siege -c50 -d10 -t3M https://www.iim.fr
** SIEGE 4.0.4
** Preparing 50 concurrent users for battle.
The server is now under siege...
HTTP/1.1 200      0.10 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.11 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.11 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.13 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.13 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.15 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.18 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.18 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.18 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.19 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.19 secs: 25190 bytes ==> GET /
HTTP/1.1 200      0.19 secs: 25190 bytes ==> GET /
```

Botnet (1/24)

CORRECTION



- Un botnet est
 - Groupe d'ordinateurs
 - Ou dispositifs sous le contrôle d'un attaquant
- utilisé pour mener des activités malveillantes
 - contre une victime ciblée.
- Botnet = “robot” et “réseau” (network en anglais)
- But
 - Pannes Internet les plus répandues
 - Mettre hors service de grandes organisations et des infrastructures de réseau
 - A partir d'une attaque par déni de service distribué (DDoS).

Botnet (2/4)

CORRECTION



J'ai l'honneur de porter à votre connaissance les faits suivants :

Nous avons reçu des plaintes concernant l'utilisation du serveur que vous avez crée auprès de nos services: 173.246.100.105

Plus particulièrement, il nous est rapporté que ce serveur est utilisé pour participer à une attaque par déni de service.

----- Informations sur l'incident -----

I am a network security manager of NongHyup-CERT(NongHyup Computer Emergency Response Team).

NongHyup-CERT's mission is to work for nonghyup Bank. Our services include threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures.

We have received a report of unauthorised access trial from your site as shown below.

===== Timezone of the Log is (GMT+9)

=====

- Firewall Activity Log

TIMESTAMP	SRC_IP	DEST_IP	DEST_PORT	PROTOCOL
-----------	--------	---------	-----------	----------

2012-07-09 11:47	173.246.100.105	121.157.xxx.1	80	TCP
------------------	-----------------	---------------	----	-----

2012-07-09 11:47	173.246.100.105	121.157.xxx.2	80	TCP
------------------	-----------------	---------------	----	-----

2012-07-09 11:47	173.246.100.105	121.157.xxx.3	80	TCP
------------------	-----------------	---------------	----	-----

.....

2012-07-09 11:47	173.246.100.105	121.157.xxx.253	80	TCP
------------------	-----------------	-----------------	----	-----

2012-07-09 11:47	173.246.100.105	121.157.xxx.254	80	TCP
------------------	-----------------	-----------------	----	-----

2012-07-09 11:47	173.246.100.105	121.157.xxx.255	80	TCP
------------------	-----------------	-----------------	----	-----

=====

Selon le code pénal, article 323-2 du Code pénal :

"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 € d'amende."

En outre, nous vous rappelons qu'en vertu de notre contrat et notamment des articles 3, 14 et 15 de nos conditions générales du service d'hébergement

<http://www.gandi.net/contracts/fr/hosting/pdf/>

vous vous êtes engagé à choisir et utiliser votre serveur et nos services dans le respect des droits des tiers, de la législation et de la réglementation en vigueur, et que vous avez accepté qu'en cas de manquement grave ou de perturbation de nos services nous puissions suspendre ou résilier nos services sans préavis.

Conformément à ce contrat, l'utilisation que vous faites de nos services, pour vous livrer aux activités susvisées constitue un manquement grave à vos obligations contractuelles.

En conséquence de quoi nous vous demandons de prendre toutes mesures nécessaires pour stopper cette activité et nous tenir informé de votre action en la matière.

Cordialement.

le département Abuse

<http://www.gandi.net/abuse/>

Botnet (3/4)

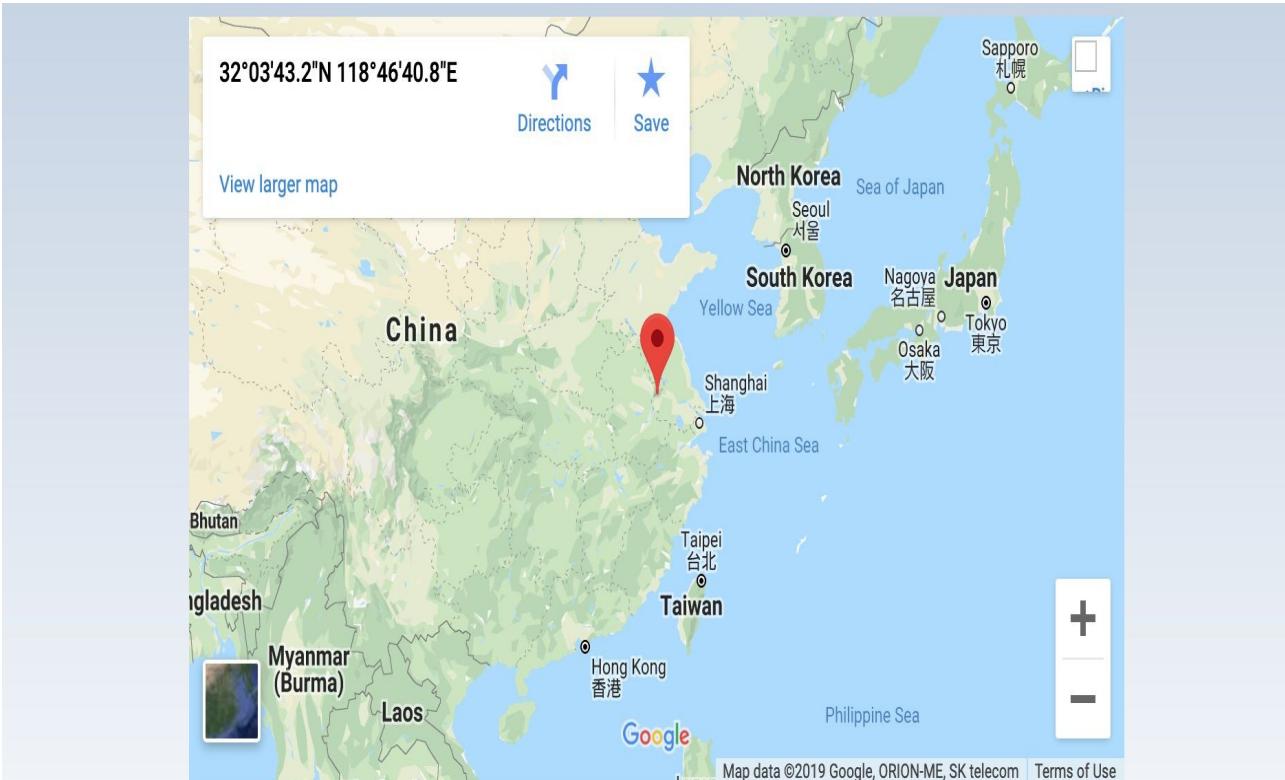
CORRECTION



```
Jul 16 02:21:04 serveur1 sshd[3702]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:06 serveur1 sshd[3702]: Failed password for root from 58.221.206.250 port 21978 ssh2
Jul 16 02:21:10 serveur1 sshd[3731]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:12 serveur1 sshd[3731]: Failed password for root from 58.221.206.250 port 1957 ssh2
Jul 16 02:21:16 serveur1 sshd[3737]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:18 serveur1 sshd[3737]: Failed password for root from 58.221.206.250 port 64317 ssh2
Jul 16 02:21:21 serveur1 sshd[3743]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:23 serveur1 sshd[3743]: Failed password for root from 58.221.206.250 port 9278 ssh2
Jul 16 02:21:26 serveur1 sshd[3749]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:29 serveur1 sshd[3749]: Failed password for root from 58.221.206.250 port 6025 ssh2
Jul 16 02:21:32 serveur1 sshd[3755]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:34 serveur1 sshd[3755]: Failed password for root from 58.221.206.250 port 41167 ssh2
Jul 16 02:21:38 serveur1 sshd[3761]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.221.206.250 user=root
Jul 16 02:21:40 serveur1 sshd[3761]: Failed password for root from 58.221.206.250 port 12893 ssh2
```

Botnet (4/4)

CORRECTION



Hostname	Unknown	ISP	No.31,Jin-rong Street
Continent	Asia	Flag	
Country	China	Country Code	CN
Region	Jiangsu	Local time	09 Apr 2019 05:18 CST
City	Unknown	Postal Code	Unknown
IP Address	58.221.206.250	Latitude	32.062
		Longitude	118.778

Keylogger

CORRECTION



- Espionner ce que l'utilisateur tape sur son clavier
- Accès sur un site internet
- Espionnage par logiciel
- Espionnage aussi par hardware
 - Petit dongle sur le port PS/2 ou USB



Attaque par mot de passe

CORRECTION



- 2 types
 - Attaque par dictionnaire
 - Récupération d'un fichier contenant les mots de passe les plus utilisés
 - darkc0de.txt
 - Attaque par bruteforce
 - Essaie de tous les mots de passe possible
 - a, b, c... aa, ab... aaa, aab... aaaa, aaab.... aaaaa, aaaa

Man in the middle (1/)

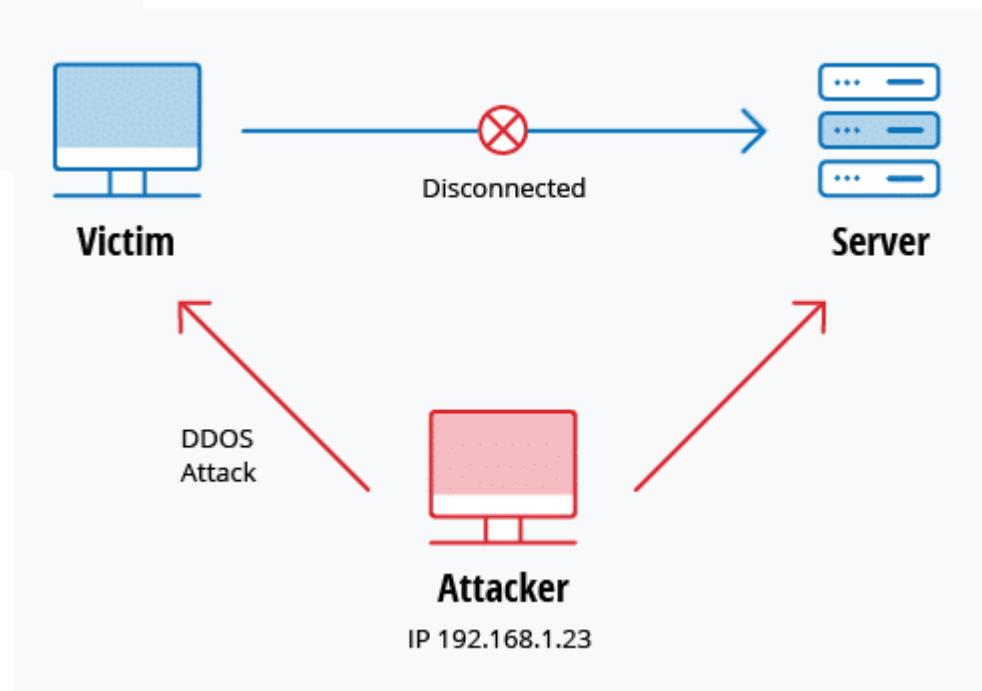
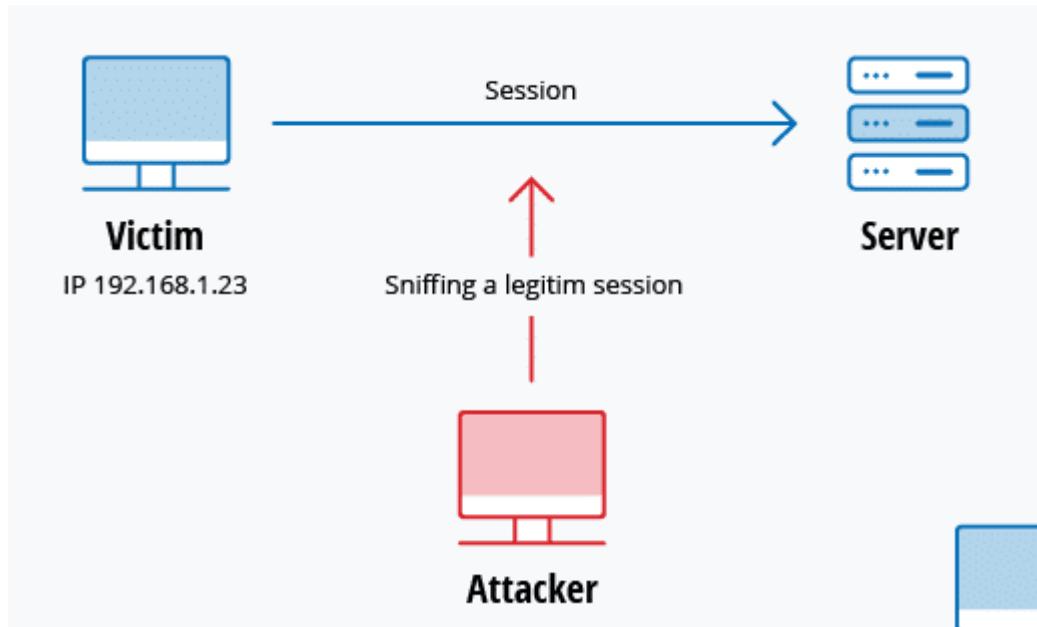
CORRECTION



- Attaque de l'homme du milieu
- Attaque de l'intercepteur
- Utilisateur posté sur le réseau
 - qui peut lire et analyser les données qui transitent

Man in the middle : Exemple

CORRECTION



Man in the middle (3/3)

CORRECTION



- Exemple avec Wireshark

Wireshark - Packet 1300 · wireshark_en0_20190409003830_uYgDWY

▶ Frame 1300: 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on interface 0
▶ Ethernet II, Src: Apple_80:f6:b9 (ac:bc:32:80:f6:b9), Dst: Sagemcom_a2:48:80 (90:4d:4a:a2:48:80)
▶ Internet Protocol Version 4, Src: 192.168.1.15, Dst: 163.172.6.57
▶ Transmission Control Protocol, Src Port: 54058, Dst Port: 80, Seq: 1, Ack: 1, Len: 1276
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "log" = "azdza"
▶ Form item: "pwd" = "azd"
▶ Form item: "wp-submit" = "Se connecter"
▶ Form item: "redirect_to" = "http://meolia.fr/wp-admin/"
▶ Form item: "testcookie" = "1"

0000	90 4d 4a a2 48 80 ac bc 32 80 f6 b9 08 00 45 02	.MJ.H... 2.....E.
0010	05 30 00 00 40 00 40 06 ca 29 c0 a8 01 0f a3 ac	.0..@. @. .).....
0020	06 39 d3 2a 00 50 6a 53 94 62 5f 44 3c f3 80 18	.9.*.PjS .b D<...
0030	ff ff 6e 36 00 00 01 01 08 0a 09 7a da 80 48 92	..m6.....z..H.
0040	90 9d 50 4f 53 54 20 2f 77 70 2d 6c 6f 67 69 6e	..POST / wp-login
0050	2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48	.php HTT P/1.1..H
0060	6f 73 74 3a 20 6d 65 6f 6c 69 61 2e 66 72 0d 0a	ost: meo lia.fr..
0070	43 6f 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70	Connecti on: keep
0080	2d 61 6c 69 76 65 0d 0a 43 6f 74 65 6e 74 2d	-alive.. Content-
0090	4c 65 6e 67 74 68 3a 20 31 30 32 0d 0a 43 61 63	Length: 102..Cac
00a0	68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d	he-Contr ol: max-
00b0	61 67 65 3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68	age=0..0 rigin: h
00c0	74 74 70 3a 2f 2f 6d 65 6f 6c 69 61 2e 66 72 0d	ttp://meolia.fr.
00d0	0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72	.Upgrade -Insecu
00e0	65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 43	e-Reques ts: 1..0
00f0	6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70	ontent-T ype: app
0100	6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 72 66	lication /x-www-f
0110	6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a	orm-urle ncoded..

No.: 1300 · Time: 11.792573 · Source: 192.168.1.15 · Destination: 163.172.6.57 · Protocol: HTTP · Length: 1342 · Info: POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)

Help Close



- L'injection SQL → problème courant
 - Affecte les sites Web exploitant des bases de données
- Exécute une requête SQL sur la base de données
 - via les données entrantes du client au serveur
- Des commandes SQL sont insérées dans la saisie du plan de données
 - Afin d'exécuter des commandes SQL prédéfinies.
- Un exploit d'injection SQL réussi
 - Lire les données sensibles de la base de données
 - Modifier (insérer, mettre à jour ou supprimer)
 - Récupérer le contenu d'un fichier spécifique
 - ...



- Technique de manipulation
 - Inciter les gens à partager à des informations confidentielles.
- Mise sur l'instinct fondamental de l'être humain
 - Faire confiance pour voler
 - des informations personnelles et corporatives
 - Pour être utilisées pour commettre d'autres cybercrimes.

Exemple :

Un cybercriminel peut utiliser le harponnage

- pour convaincre un employé de divulguer des mots de passe de l'entreprise
- Ceux-ci sont ensuite utilisés
 - pour accéder aux réseaux de l'entreprise
 - voler des données et installer un logiciel malicieux.



Défacement (1/2)

CORRECTION



- Conséquence d'une faille de sécurité sur un site web.
 - Le hacker modifie généralement seulement la page d'accueil.
- Exploite
 - Faille d'un système d'exploitation d'un serveur web
 - Pirate les accès administrateurs
 - Par injection SQL, de manière à modifier la présentation d'un site internet.
- Résultat :
 - La page d'accueil, est un fond uni, souvent blanc ou noir
 - Message :
 - « owned » ou « hacked » est inscrit sur la page
 - Pseudo du hacker



Défacement (2/2)

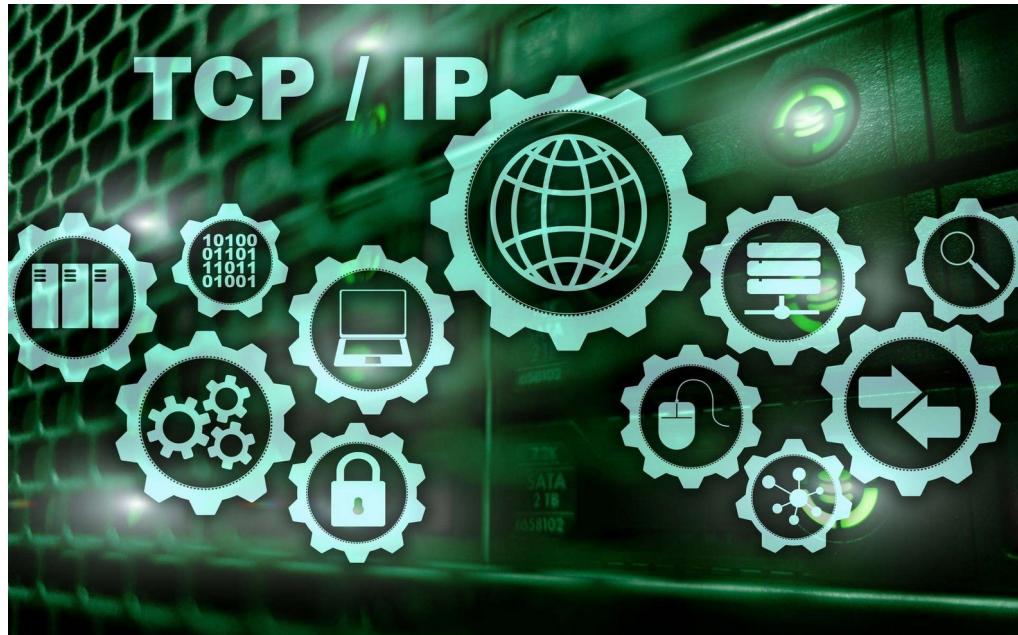
CORRECTION



- But
 - Pour exprimer une revendication
- Cibles
 - Organisations gouvernementales
 - Sites religieux.
- Objectif des hackers
 - Hacktivisme
 - Revendiquer une opinion, souvent à caractère politique
 - donne à son message une plus grande portée
 - Un concours entre pirates
 - Concours de groupe de hacker qui défacera le plus de sites internet en un temps imparti
 - Utilisée de manière à cacher un délit plus important

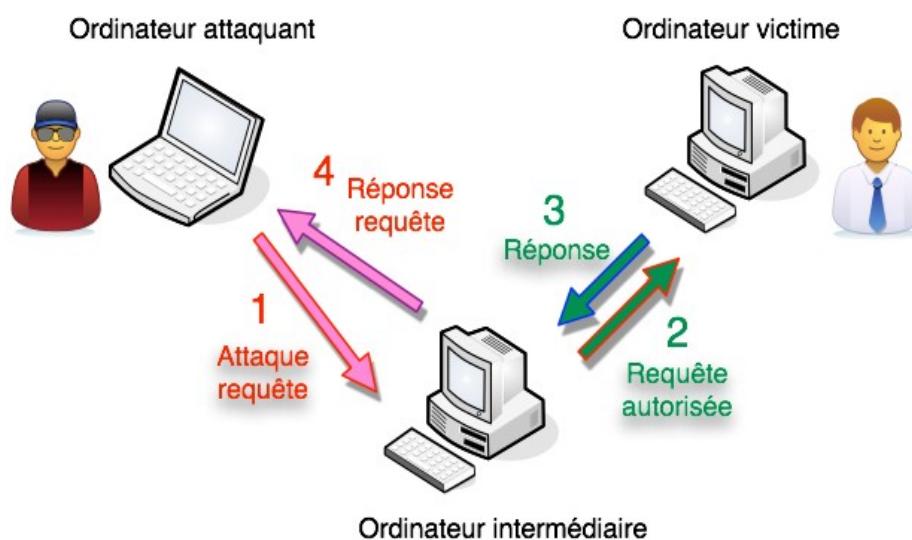
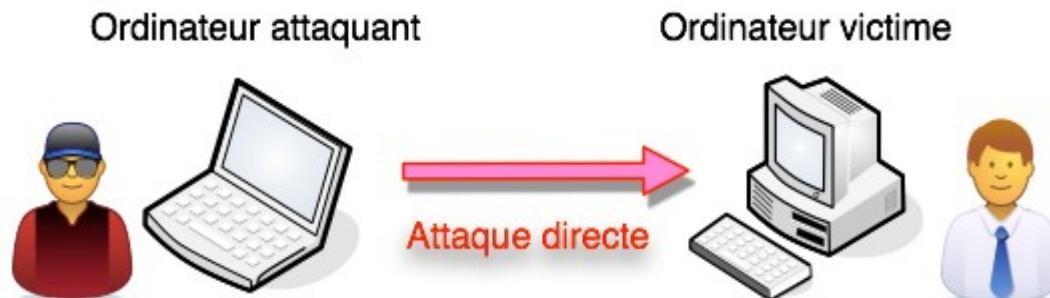
Correction TP 4 : Complément ?





- La sécurité du protocole IP
- Sécurisation d'un réseau
- Les bases de la cryptographie
- Serveurs applicatifs

Attaque : apprenti sorcier



Solution

- Etre rapide !
 - Une attaque n'est souvent qu'une affaire de secondes, voire de minutes
- Ne pas contre-attaquer le hacker
 - Disparition
 - Il est énervé
- TODO
 - Notez l'adresse IP de l'ordinateur victime de l'attaque
 - Notez l'heure de l'attaque.
 - Notez le temps de l'attaque.
 - Log(s)



Introduction (1/2)

- IP = protocole Internet
- Famille de protocoles de communication de réseaux informatiques
 - Protocoles associés :
 - TCP, UDP, ICMP, Routage...
 - Pas pris en compte la sécurité

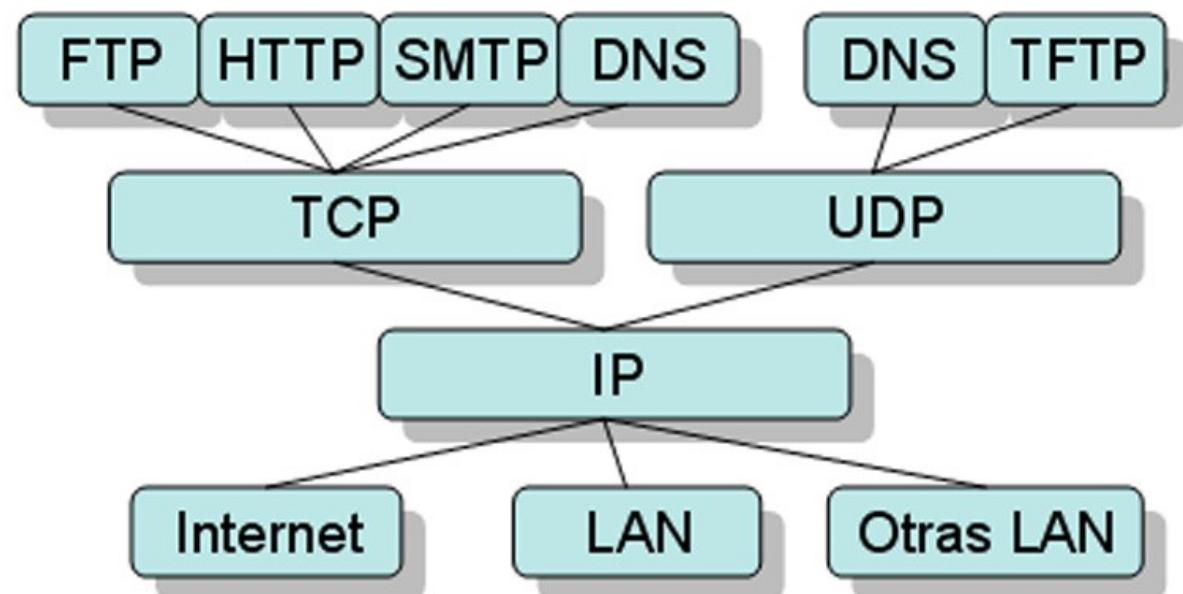


- « Concept sécurité »
 - Inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;

Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles

Introduction (2/2)

- L'exploitation de ces faiblesses nécessite des prérequis techniques
- Pas systématiquement applicables à tous les réseaux.



Exemple : Faiblesses des protocoles

- Authentification
- Chiffrement
- Routage

- Absence d'authentification
 - des émetteurs
 - des récepteurs
- d'un datagramme :
 - usurpation d'adresse IP possible

Exemple : Faiblesses des protocoles

➤ Authentification

➤ Chiffrement

➤ Routage

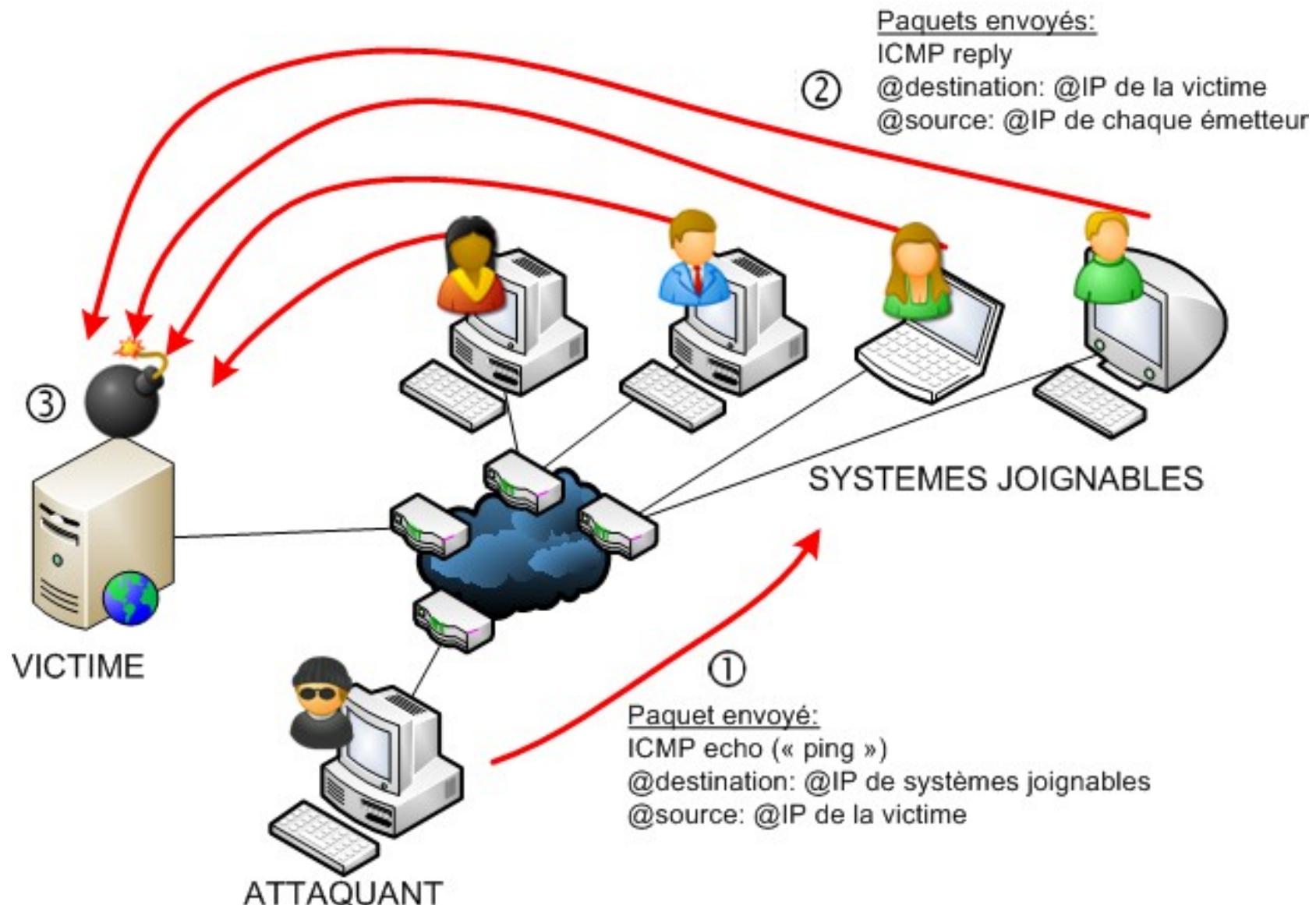
- Absence de chiffrement des données
- Données transmises en clair.
- Un hacker positionné sur un réseau peut
 - Ecouter les connexions
 - Accéder aux données

Exemple : Faiblesses des protocoles

- Authentification
- Utilisations de ressources
- Routage

- Le routage des datagrammes peut être modifié
 - de façon à rediriger les datagrammes
 - vers un autre destinataire

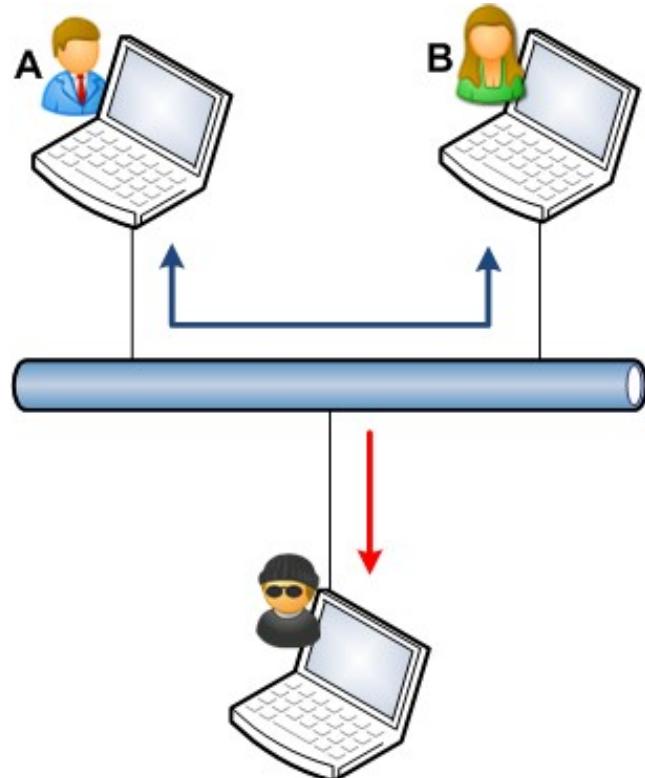
Exemple d'attaque par réflexion (1/2)



Exemple d'attaque par réflexion (2/2)

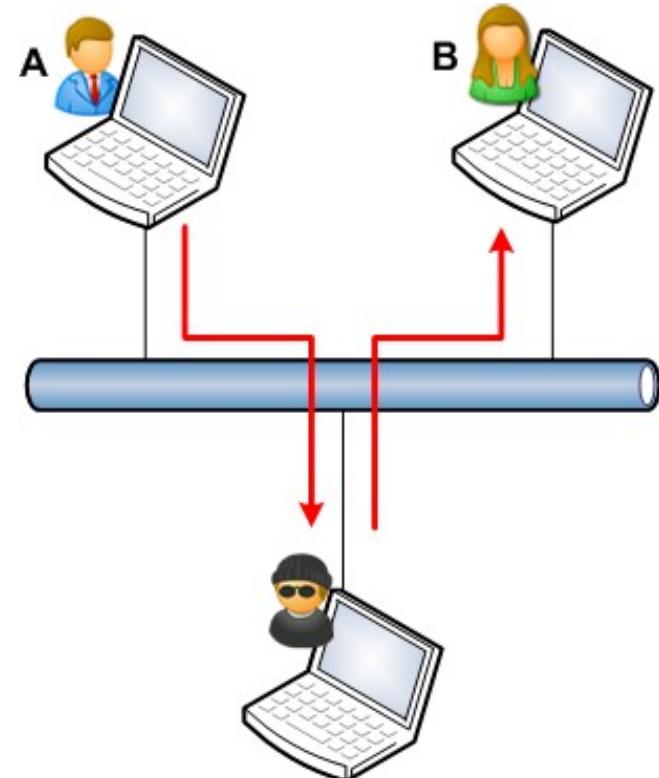
- But de l'attaque
 - porter atteinte aux performances d'un système cible (déni de service).
- Quelles sont les caractéristiques de l'attaque ?
 - usurpation d'adresse IP ;
 - réflexion de trafic en ayant recours à des systèmes tiers « innocents ».
- Séquences de l'attaque
 - Un attaquant envoie des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

Exemples d'écoute de trafic



Ecoute passive

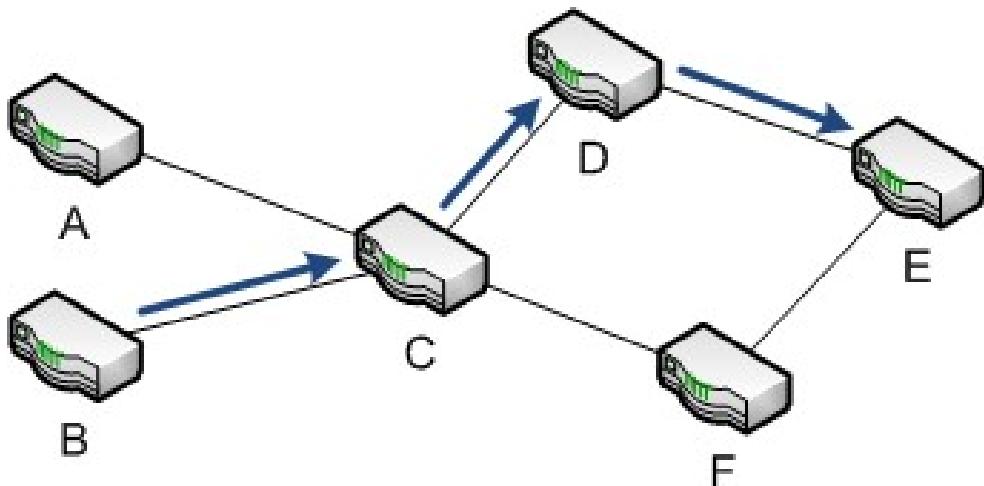
L'attaquant est en mesure d'écouter les conversations entre A et B (atteinte à la **confidentialité** des échanges).



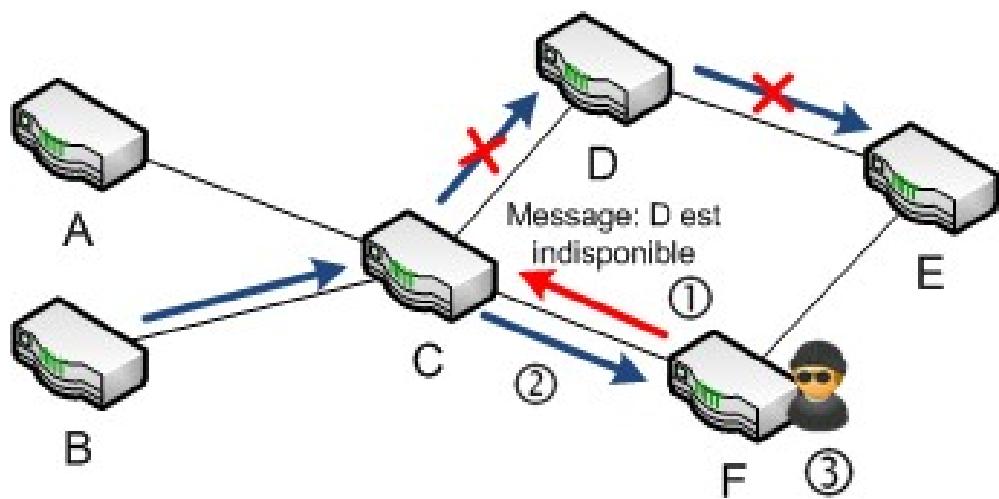
Ecoute active

L'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent (atteinte à la **confidentialité** et à l'**intégrité** des échanges).

Exemple de modification du routage des datagrammes IP



Chaque routeur possède une table de routage qui indique vers quel routeur voisin transmettre les datagrammes. Cette table peut être mise à jour dynamiquement en fonction des évènements réseaux (protocoles BGP, RIP, OSPF, etc.).



But de l'attaque : **dérouter les paquets** à destination du réseau E, vers le réseau F maitrisé par l'attaquant.

Méthode :

- L'attaquant utilise une faiblesse du protocole de routage pour indiquer au routeur C que le routeur D est indisponible, et que le routeur F peut router les paquets vers E ;
- Le routeur C transfère donc à F les paquets pour E, afin qu'ils puissent être routés à destination ;
- Selon le but visé par l'attaquant, celui-ci peut décider de router ou non les paquets vers E.

Sécurisation du protocole IP

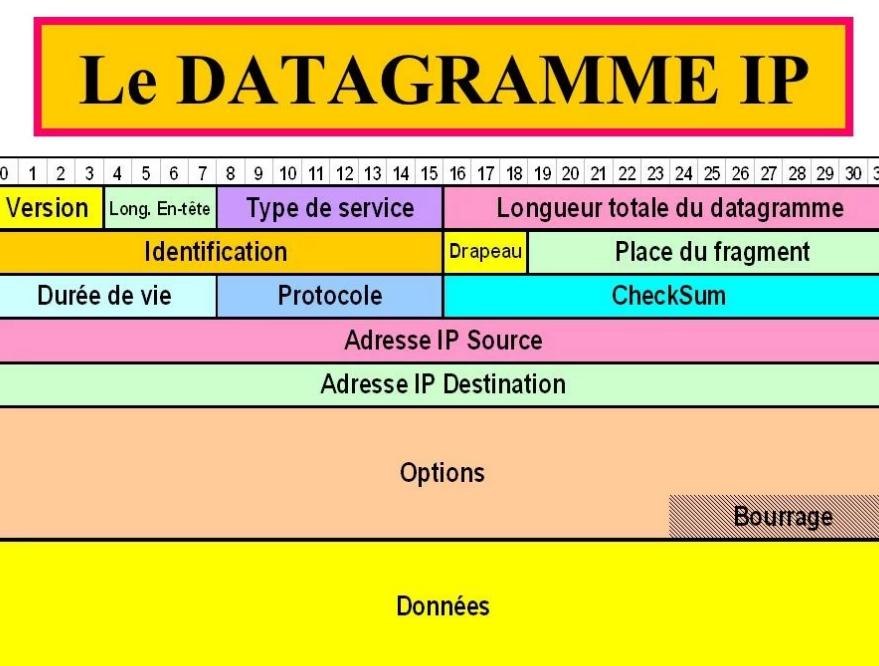
- But :
 - Mettre en œuvre des mécanismes de sécurité complémentaires
- Objectif :
 - Réduire et maîtriser les risques émanant des protocoles historiques régissant les réseaux.
- Exemple de mécanismes :
 - Chiffrement des communications ;
 - Authentification des entités
 - Cloisonnement réseau ;
 - Filtrage ;
 - Dimensionnement adapté des infrastructures ;
 - Règles de renforcement des configurations des équipements ;
 - Supervision des équipements ;
 - etc.



A retenir

Le protocole IP fait partie de la couche Internet
de la suite de protocoles TCP/IP

- C'est un des protocoles les plus importants d'Internet
 - Il permet :
 - L'élaboration
 - Le transport des datagrammes IP (les paquets de données),
 - sans toutefois en assurer la « livraison »





EXERCICE

<https://school.hello-design.fr>

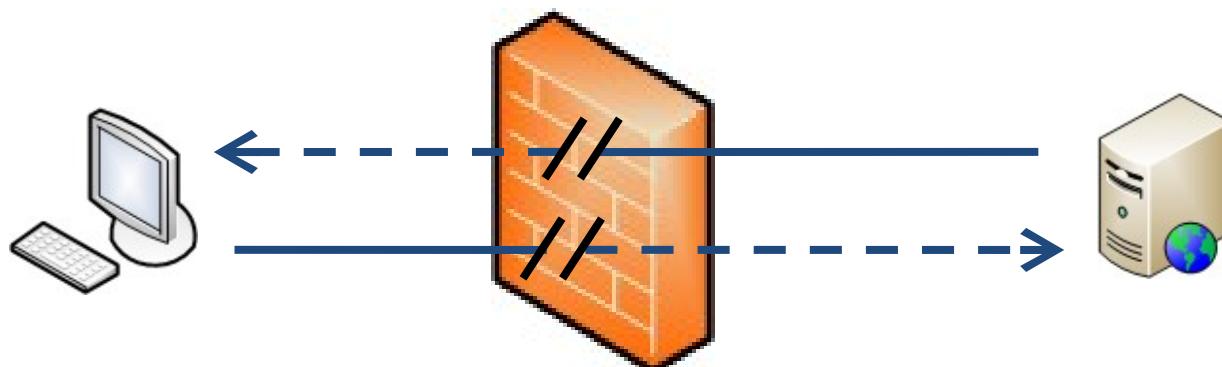
4A



- La sécurité du protocole IP
- Sécurisation d'un réseau
- Les bases de la cryptographie
- Serveurs applicatifs

Pare-feu

- Équipement en coupure entre 2 ou plusieurs réseaux ;
- Inspecte les paquets réseaux entrants et sortants d'un réseau à l'autre ;
- Implémente un **mécanisme de filtrage basé sur des règles** :
 - Ne transmet que les paquets réseaux
 - Respect des règles de filtrage implémentées dans la configuration du pare-feu.



Pour chaque flux entrant ou sortant, le pare-feu interroge ses règles de filtrage pour déterminer s'il doit laisser le paquet réseau ou non.

Pare-feu : Règles de filtrage

- Historiquement, elles étaient basées sur les couches basses de la pile protocolaire (réseau, transport), et portaient uniquement sur les paramètres comme les adresses IP et les ports TCP/UDP ;
- Les pare-feu sont également capables de filtrer selon les données de la couche applicative (protocole et contenu des données). Ex. : HTTP, SMTP, DNS, etc.
 - Les proxy et reverse-proxy peuvent être vus comme des pare-feu applicatifs dédiés. Ils permettent d'analyser finement les flux applicatifs (par exemple la navigation web des utilisateurs ou les flux web entrants sur un serveur de e-commerce).
- Un anti-virus ou un mécanisme de détection d'intrusion peuvent également être implémentés sur le pare-feu de façon à détecter un malware en transit ou certaines attaques.

Avantage sécurité :

- L'exploitant d'un réseau peut donc restreindre le trafic entrant et sortant aux seules connexions qu'il estime légitime. Toutes les autres connexions sont donc bloquées.

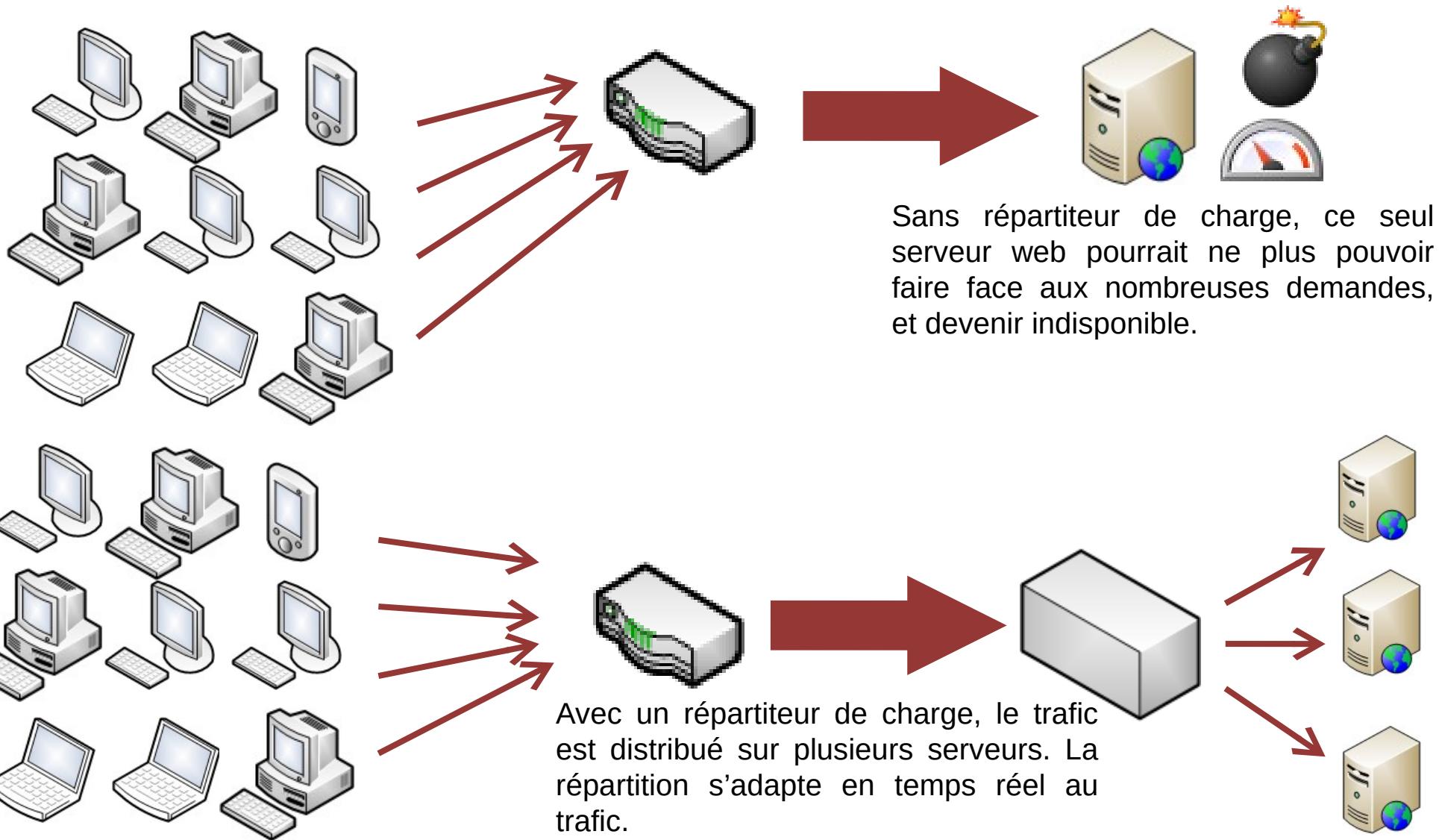
Répartiteur de charge (1/2)

- En Anglais : Load-balancer
- Utilisation pour les grosses infrastructures
 - Les serveurs doivent faire face
 - Fortes bandes passantes
 - Charges élevées de trafic
- Équipement chargé de **répartir/distribuer la charge réseau**
 - En fonction des caractéristiques de celui-ci
 - De la disponibilité des serveurs

Avantage sécurité :

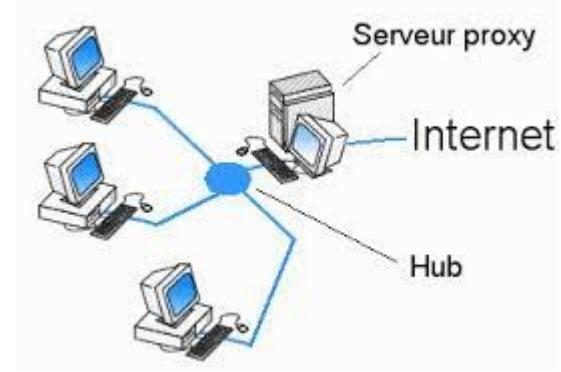
- Permet de mieux se protéger contre les **dénis de service distribués**.

Répartiteur de charge (2/2)



Serveurs proxy

- Un serveur proxy
 - ordinateur virtuel ou physique
 - sépare le trafic des utilisateurs finaux, d'Internet.
- Les proxys classiques
 - masquent vos adresses IP et vous évitent d'être pistés.
 - Placés entre vous et les serveurs web
 - renvoient les résultats de vos requêtes.
- Un serveur proxy remplit
 - plusieurs fonctions de sécurité et de confidentialité
 - Propose plusieurs types de fonctionnalités :
 - Filtrage de données et pare-feu / Partage de connexion / mise en cache des données / amélioration des performances / accès anonyme / sécurité



Serveurs proxy (2/2)

- Rôle
 - Bloqué les activités illégales qui affectent les entreprises.
 - E-mails d'hameçonnage
 - Fraude aux investissements
 - Attaques par rançongiciel
 - Usurpation d'identité

Anti-virus

- Logiciel chargé de détecter et stopper les malwares connus :
 - Virus
 - Vers
 - Enregistreur de frappe « Keylogger »
 - Chevaux de Troie
 - etc.



- Fonctionnement

- Possède une base de données
 - qui contient les signatures des malware connus.
- Ils analysent en permanence
 - Les fichiers
 - Les exécutables du système hébergeant l'anti-virus

Limites des anti-virus

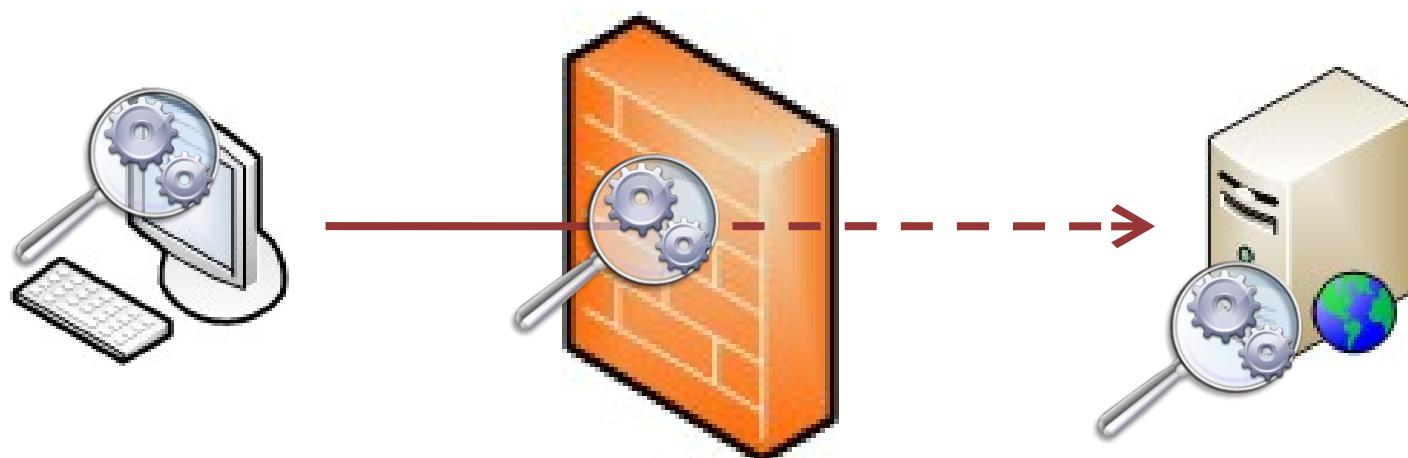
Détectent (en général) que les malware déjà répertoriés par les éditeurs.

Les nouveaux virus ou les malwares ciblés ne sont souvent pas détectés.

Impératif que l'anti-virus soit mis à jour quotidiennement.

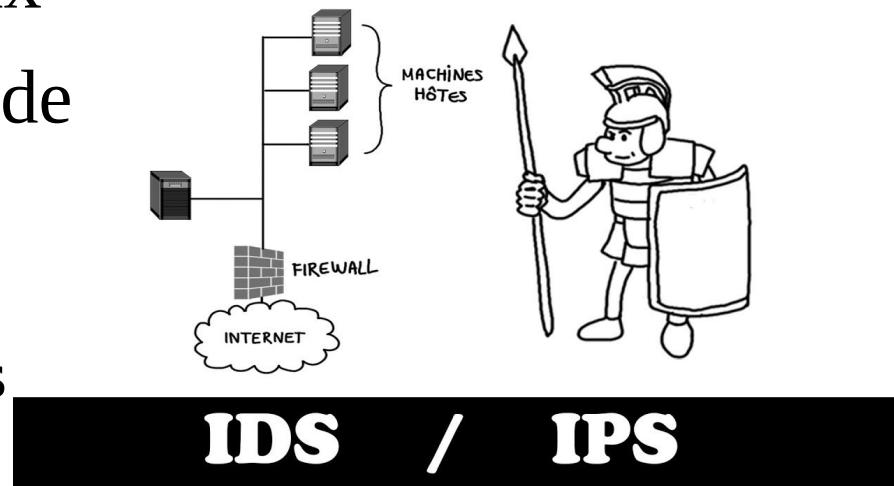
Où trouver les anti-virus ?

- Un anti-virus peut être déployé :
 - Local :
 - Sur un système (poste de travail ou serveur) afin de détecter les virus affectant cette machine
 - Coupure des flux réseaux :
 - Sur un pare-feu afin d'analyser les flux réseaux et détecter les malwares avant même qu'ils n'atteignent leur cible.
 - Ce fonctionnement peut être assimilé à un IDS (Intrusion Detection System)



IDS et IPS (1/3)

- IDS = Intrusion Detection System
- IPS = Intrusion Prevention System
- Chargés d'analyser le trafic réseau pour y détecter des tentatives d'intrusion :
 - soit en analysant le comportement des flux réseaux
 - soit en se basant sur une base de signatures identifiant des données malveillantes
 - principe similaire à celui des anti-virus

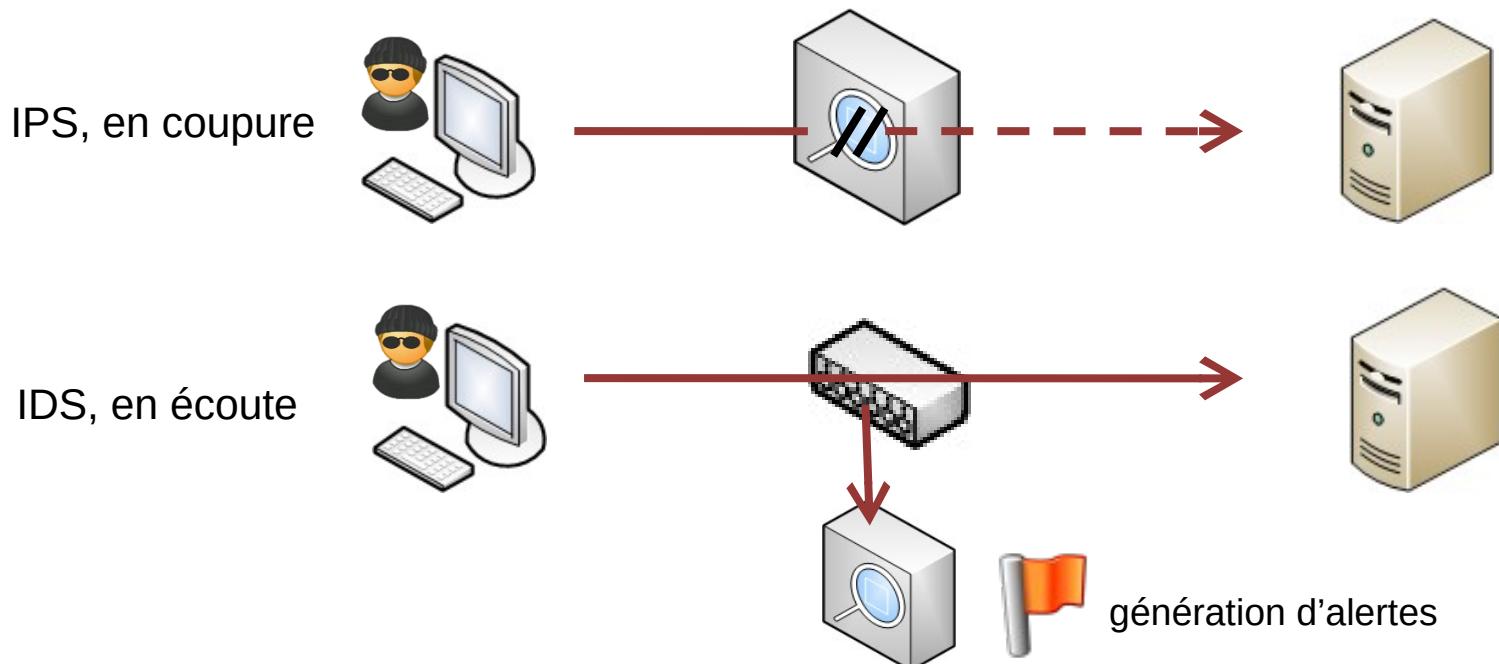


IDS et IPS (2/3)

- En cas de détection d'une intrusion
 - IDS alertent les administrateurs
 - Libre à eux d'intervenir ou non
 - IPS bloquent les flux réseau concernés.
- Nécessaire : Une configuration fine et maintenue :
 - Effet connus pour présenter de nombreux faux-positifs
 - Ex : ils détectent à tort une tentative d'intrusion
 - IDS/IPS basés sur des signatures ne peuvent détecter que les intrusions
 - Caractéristiques techniques sont déjà connues et référencées.

IDS et IPS (3/3)

- IDS peut être
 - soit en coupure du flux réseaux
 - soit positionné en écoute.
- IPS doit forcément être en coupure du flux de façon
 - à pourvoir bloquer le trafic lorsque cela est nécessaire.



VPN (1/2)

- VPN = Virtual Private Network
- Réseau virtuel → permet à deux réseaux distants de communiquer en toute sécurité
 - Y compris si la communication s'effectue via des réseaux inconnus et auxquels nous ne faisons pas confiance.

La technologie VPN repose sur une idée simple :

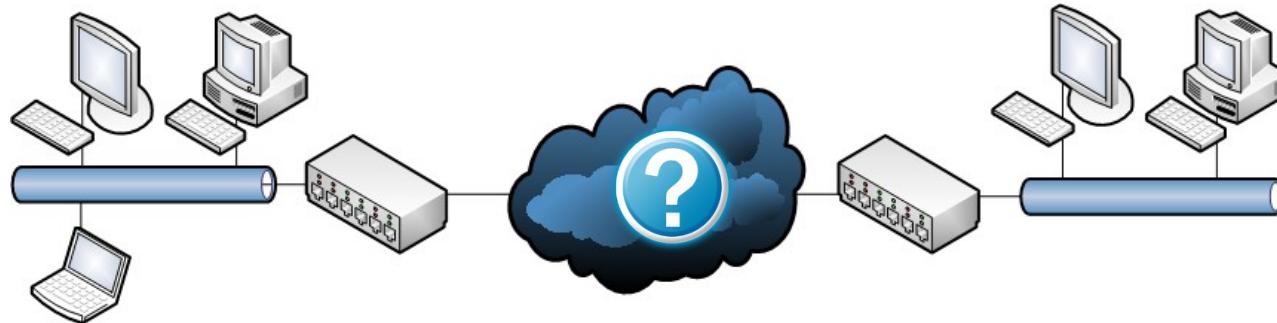
Connecter en toute sécurité une personne de confiance à une ressource dont elle a besoin via un réseau auquel vous n'avez pas confiance.



VPN : Exemple

Une entreprise qui possède deux sites distants
qui ont besoin de communiquer entre eux via internet :

Comment faire passer les flux en toute sécurité via Internet que l'on ne maîtrise pas ?



- Solution : Grâce à des mécanismes cryptographiques
 - Appliquer un chiffrement des données, ainsi qu'un motif d'intégrité, à tous les flux entre les 2 sites
 - On obtient ainsi un tunnel virtuel qui ne contient que des données chiffrées et protégées en intégrité :
 - Les données qui passent sur Internet sont donc chiffrées et non compréhensibles par un attaquant qui écouterait les flux
 - En cas de modification malveillante des flux,
 - Le mécanisme d'intégrité permettra au destinataire de déterminer que les données reçues ne sont pas intègres,
 - Et qu'il ne faut donc pas traiter ces données.

Différents types de VPN

- VPN basés sur les clients
 - VPN PPTP
 - L2TP VPN
 - VPN Site-to-Site
- VPN basés sur les réseaux
 - Les tunnels Ipsec
 - VPN multipoint dynamique
 - Hybrid VPN
- Autre
 - SSL et TLS



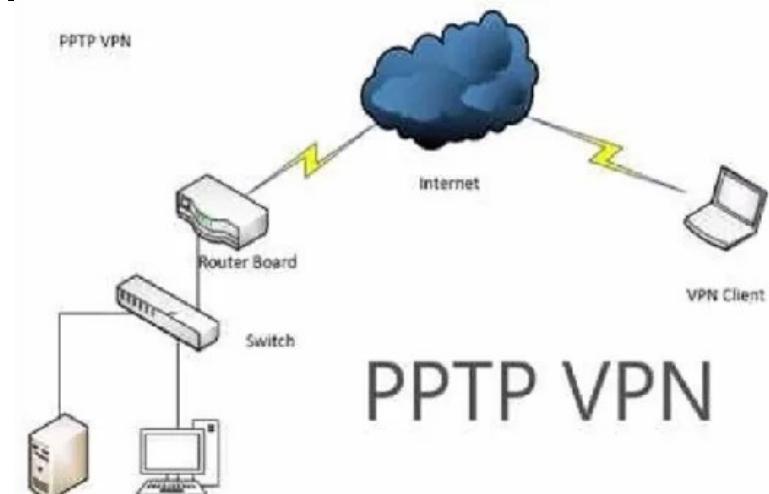
VPN PPTP (Alias VPN)

= Point-to-Point Tunneling Protocol (protocole de tunnel point-à-point).

- Utilisation
 - Par des utilisateurs éloignés pour se connecter à leur réseau
 - VPN en utilisant leur connexion internet existante
 - Principalement pour une utilisation privée
- Les utilisateurs s'y enregistrent en utilisant un mot de passe pré-approuvé.

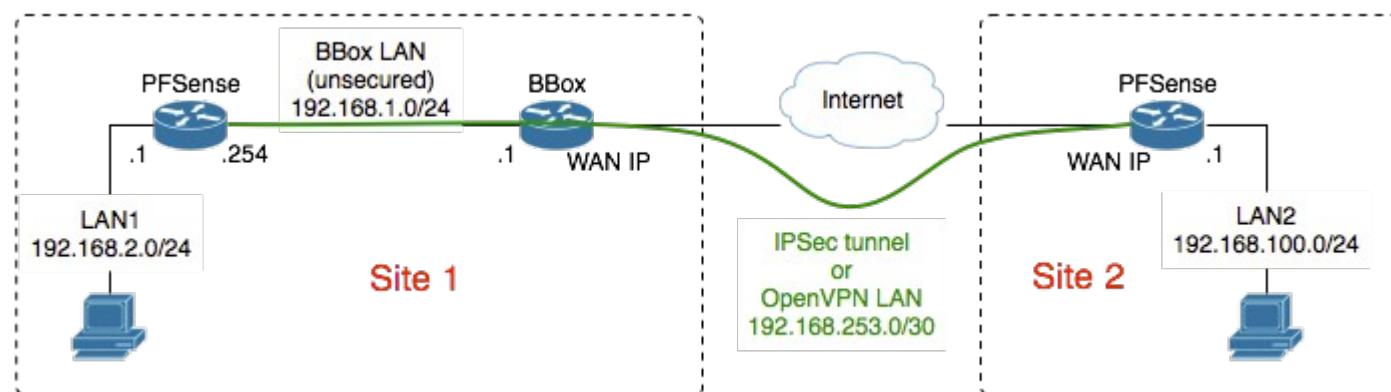
Inconvénient :

- Absence de chiffrement
- S'appuie sur le Point-à-point (PP), pour les mesures de sécurité.



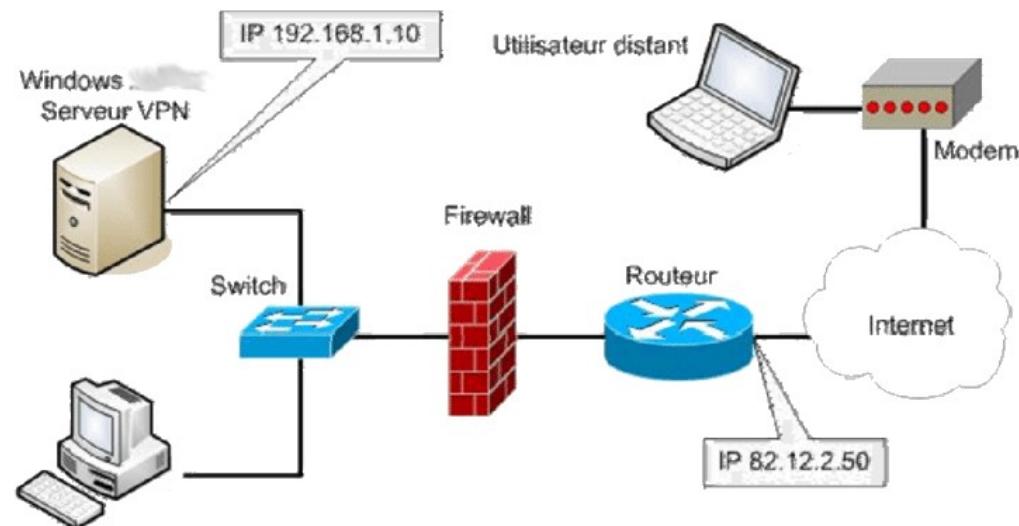
VPN Site-to-Site

- Appelé Router-to-Router (routeur-à-routeur),
- VPN basé sur Extranet
- Utilisation
 - Pour des opérations commerciales, entreprises (nationales, internationales)
 - Sert à relier le réseau des bureaux principaux au reste des bureaux.
- Intérêt
 - Construire un réseau virtuel avec des localisations variées pour les connecter à Internet
 - Maintenir des communications sécurisées et privées entre eux.



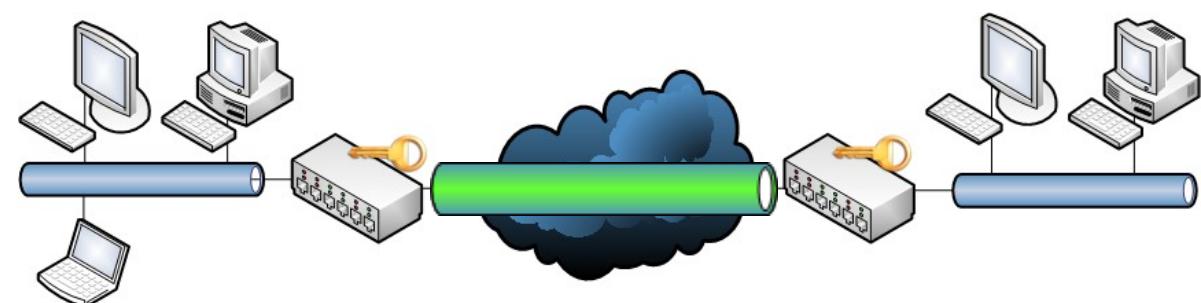
L2TP VPN

- Signifie Layer to Tunneling Protocol
 - protocole de tunnelling de niveau 2
 - développé par Microsoft et Cisco.
- Similaire au PPTP
- Utilisation
 - Forme un tunnel entre deux points de connexion L2TP
 - Un second VPN comme le protocole IPsec crypte les données
 - Se concentre sur la sécurisation des données entre les tunnels.



IPsec

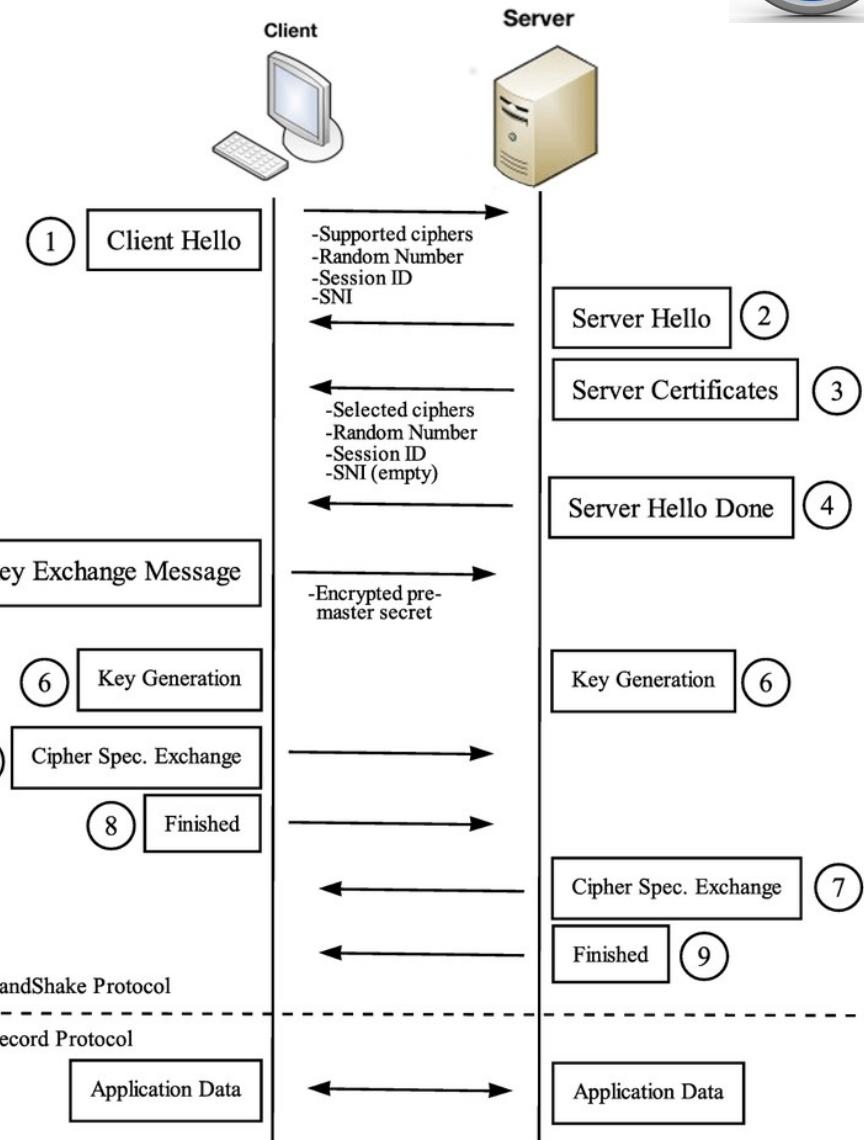
- Abréviation de Internet Protocol Security (protocole de sécurité internet).
- Utilisation
 - Sécuriser les communications par internet sur un réseau IP.
 - Protéger le transfert des données entre deux réseaux différents.
- Principe
 - Tunnel mis en place dans un endroit éloigné
 - Permet d'accéder à votre site central.
- Sécurise le protocole de communication internet
 - En vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toute la connexion.
- Deux modes d'opération dans un VPN IPsec.
 - Le mode transport
 - Le mode tunnel.



VPN de site à site, dont le tunnel est géré par les routeurs
IPsec – au niveau de la couche Internet

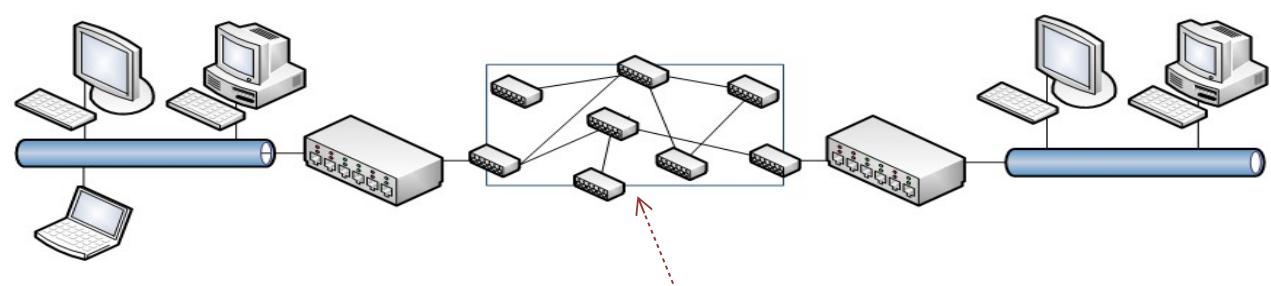
SSL et TLS

- SSL = Secure Sockets Layer
- TLS = Transport Layer Security.
- Fonctionnent ensemble comme un seul protocole.
- Utilisation
 - Pour construire une connexion VPN.
- Principe
 - Dans une connexion VPN :
 - Le navigateur internet sert de client et l'accès utilisateur est restreint à certaines applications seulement plutôt qu'un réseau entier.
 - Les protocoles SSL et TLS sont principalement utilisés par des sites de vente en ligne et des fournisseurs de service.
 - Les connexions SSL commencent par https au début de l'URL au lieu de http.



MPLS VPN

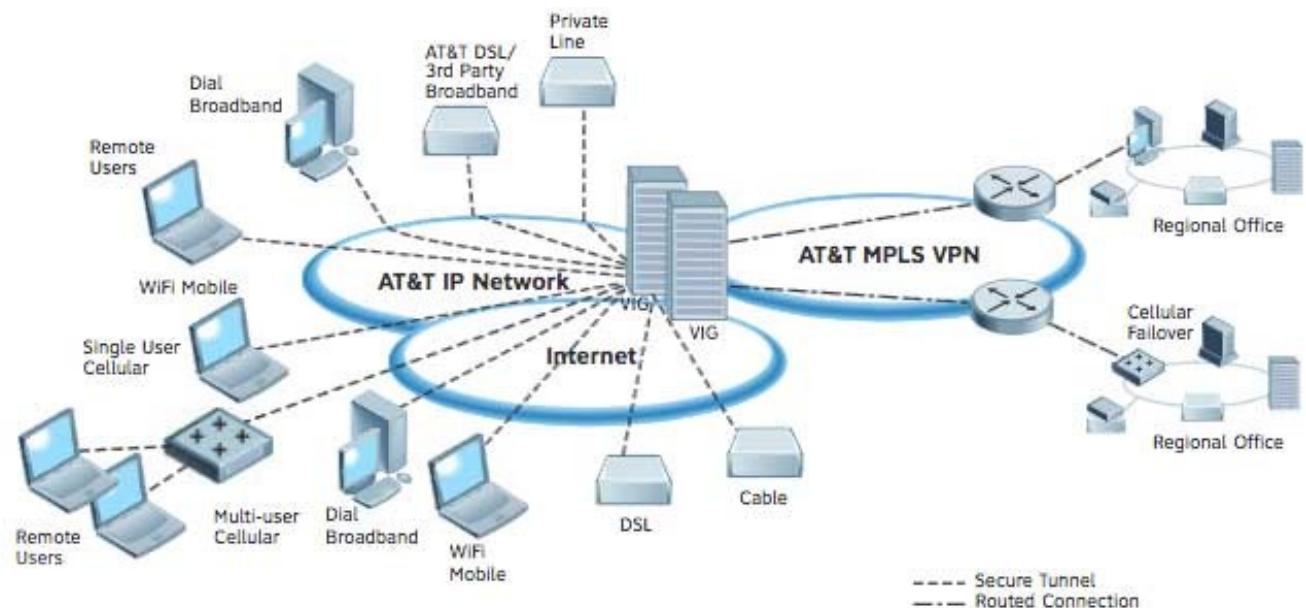
- Appelé Multi-Protocol Label Switching
 - Multi-protocole de commutation d'étiquettes
- Utilisation
 - Pour des connexions de type Site-à-Site.
- Principe
 - Flexibles et adaptables.
 - Accélérer le processus de distribution de paquets de réseau avec de multiples protocoles.
 - Systèmes basés sur fournisseurs d'accès.



Réseau opérateur **MPLS**, dont le cœur est inaccessible aux clients se connectant sur ce réseau

Hybrid VPN

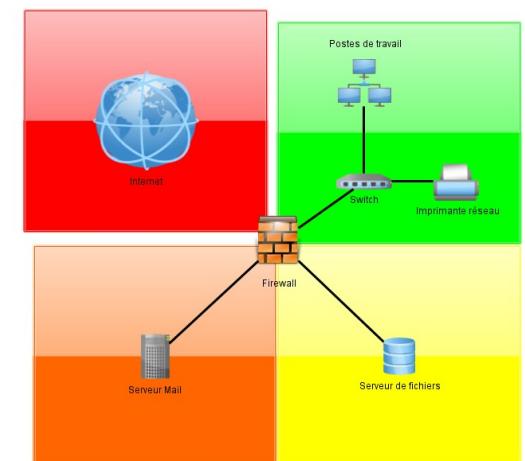
- Combine à la fois un MPLS et un IPsec.
- Utilisation
 - Le VPN IPsec comme soutien du VPN MPLS.
 - Les VPN IPsec nécessitent de l'équipement du côté du client
 - A destination des entreprises
- Principe
 - Posséder un routeur ou un appareil de sécurité multi-tâches.
 - Les données sont chiffrées et forment le tunnel VPN

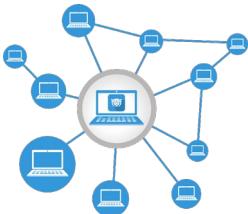




Segmentation

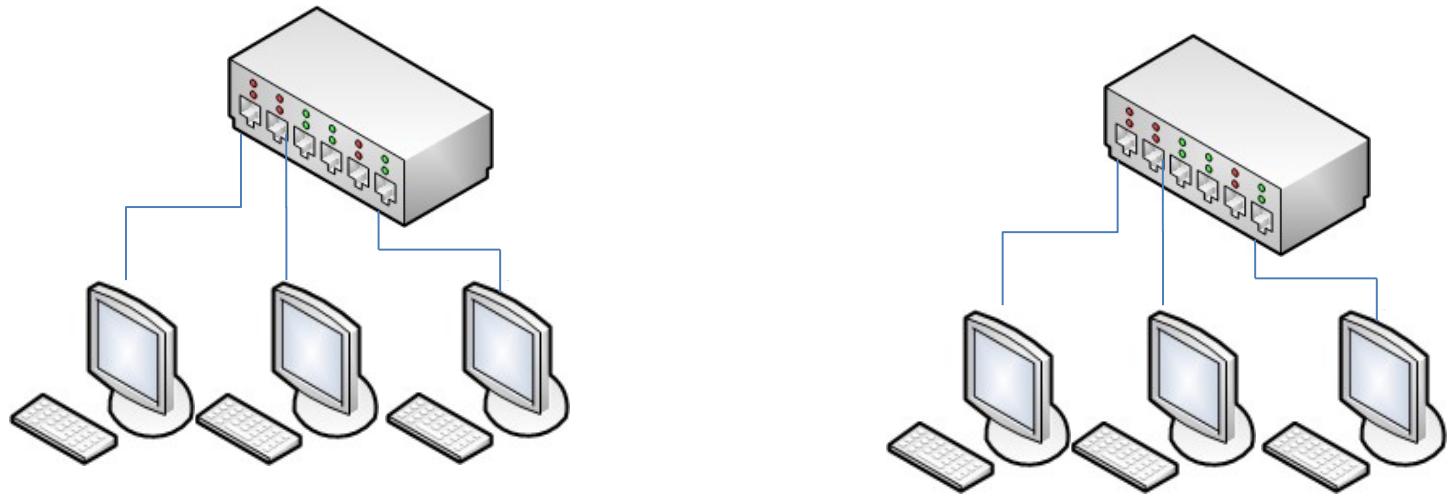
- Un principe majeur de la Sécurité est celui du moindre privilège :
 - On ne doit donner les droits d'accès à une ressource
 - Qu'aux seules personnes/entités ayant un besoin légitime d'y accéder.
- Appliqué au domaine réseau
 - Séparer le réseau en différentes zones.
- Droits d'accès
 - Ces zones doivent ensuite être filtrés
 - Afin de n'autoriser que les flux nécessaires entre chaque zone.





Segmentation : Simple

- Plusieurs techniques pour procéder à de la segmentation.
- La technique la plus évidente :
 - Implémenter deux réseaux distincts non connectés.



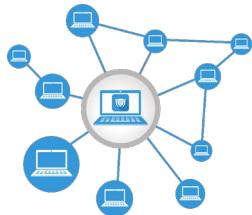
Implémentation de deux réseaux physiques différents, non connectés.

Avantage :

Etanchéité réseau parfaite (aucune communication possible entre ces deux zones).

Inconvénient :

Adapté à certains réseaux très sensibles seulement
peu adapté aux réseaux d'entreprise qui ont besoin de communiquer.



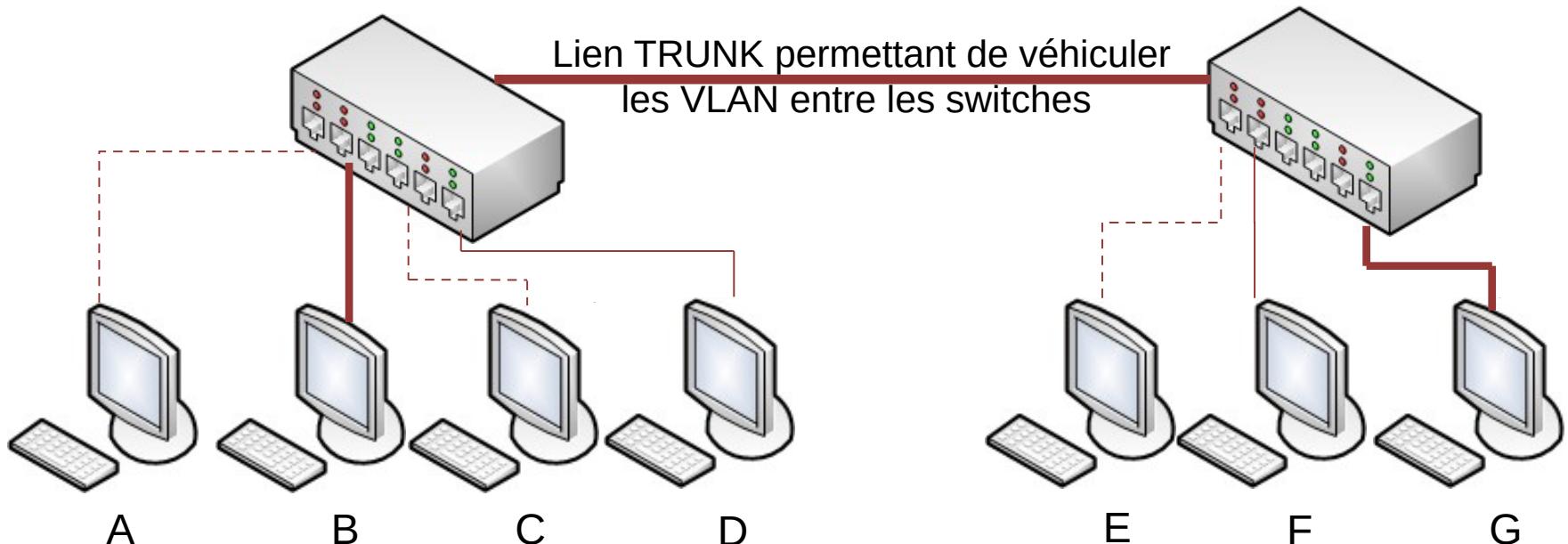
Segmentation : VLAN (Virtual LAN) (1/2)

- Réseaux virtuels implémentés par les switches.
- But
 - Restreindre la communication entre les systèmes
 - Suivant les règles configurées sur l'équipement réseau :
 - La segmentation peut se faire grâce aux ports Ethernet de chaque switch (on affecte un VLAN particulier à chaque port des switches, les deux switches étant reliés entre eux par un lien TRUNK afin de véhiculer les étiquettes des VLAN) ;
- Principe
 - La segmentation peut se faire grâce aux adresses MAC des systèmes.

Attention :

Les adresses MAC des cartes réseaux pouvant facilement être modifiées par les utilisateurs
→ Le filtrage sur les adresses MAC est à considérer avec précaution
Le niveau de sécurité effectif est limité.

Segmentation : VLAN (Virtual LAN) (2/2)



VLAN 1. Les machines B et G sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

VLAN 2. Les machines A, C et E sont segmentées des autres systèmes et peuvent communiquer entre-elles seulement.

VLAN 3. Les machines D et F sont segmentées des autres systèmes et peuvent communiquer entre-elles deux seulement.

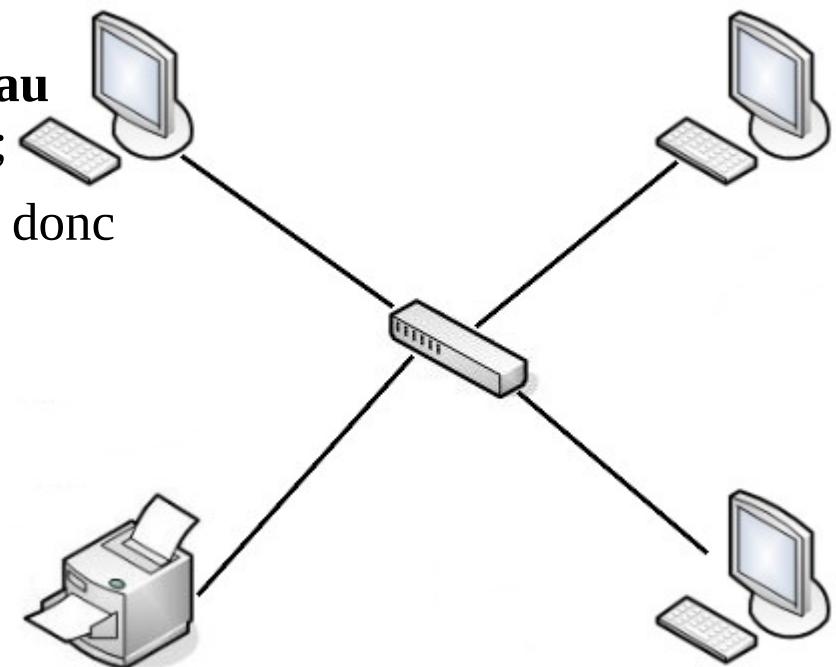
Exemple pratique de sécurisation avec un réseau simple



- Prenons l'exemple d'un réseau d'entreprise « à plat »

Caractéristiques de cette entreprise :

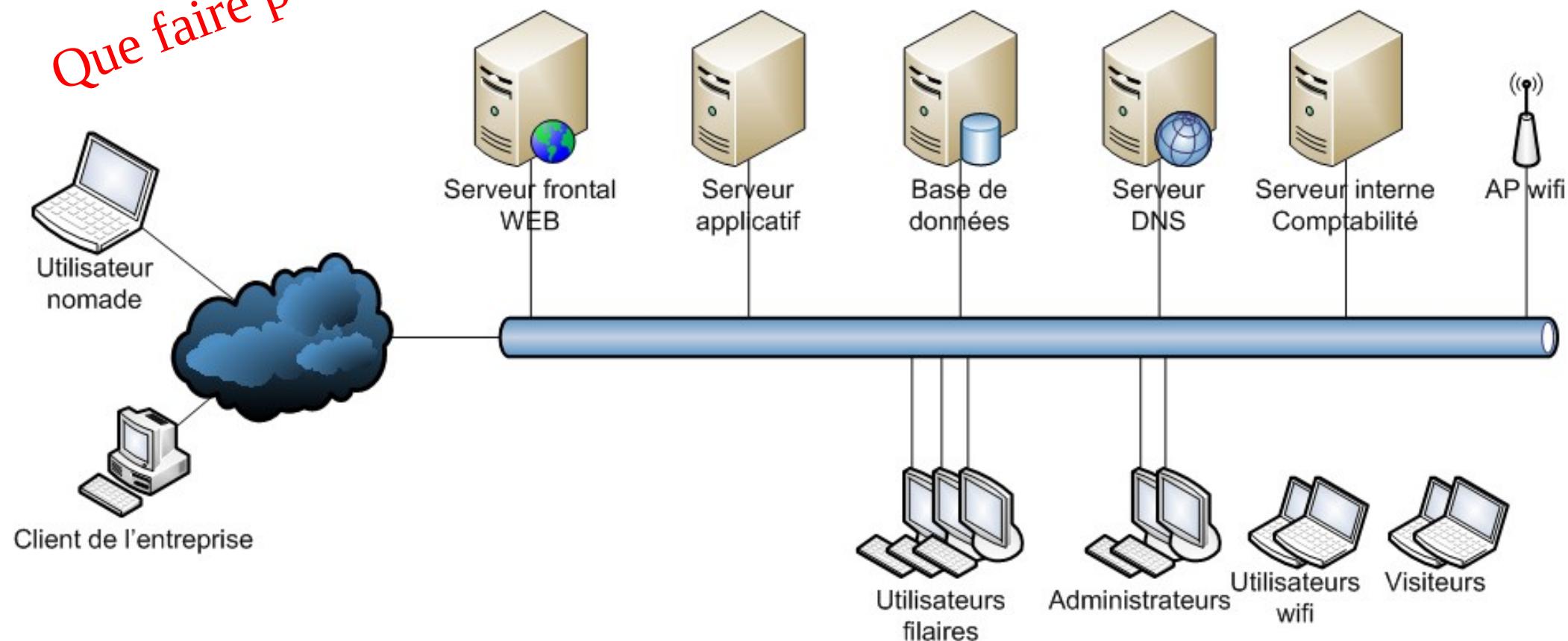
- Elle fournit un **site WEB de e-commerce** ;
- Certains employés se connectent sur le **réseau local filaire**, d'autres se connectent en **wifi** ;
- Certains employés sont **nomades** et doivent donc **se connecter à distance** ;
- Il existe deux catégories principales d'utilisateurs :
 - les **utilisateurs « standard »**
 - les **administrateurs** du S.I.
- Afin de fonctionner, l'entreprise possède également des **serveurs internes** (comptabilité, wiki, etc.) ;
- L'entreprise souhaite permettre à ses **visiteurs** de se connecter en **wifi** afin de naviguer sur internet.



Exemple pratique de sécurisation avec un réseau simple



Que faire pour sécuriser ?



Réseau « à plat », avant sécurisation



Exemple pratique de sécurisation avec un réseau simple

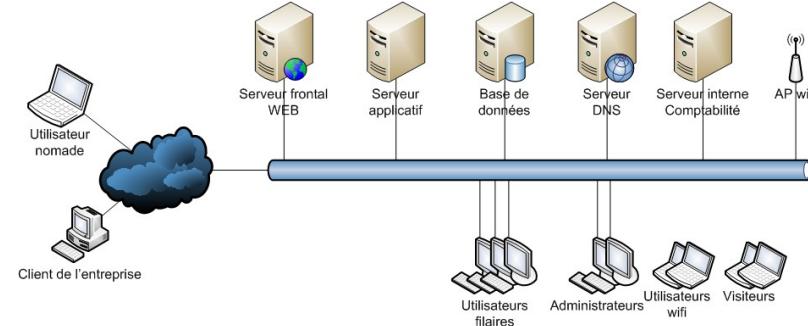
- Comment nous allons pouvoir sécuriser ce réseau :
 - Note : il existe plusieurs façons d'améliorer la sécurité de ce réseau
- Actuellement
 - Nombreuses faiblesses architecturales de ce réseau
 - Problème identifié :
 - Le réseau est directement connecté à Internet
 - Tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur
 - Risque de fuite de données
 - Tout Internet peut se connecter sur notre réseau interne.

Correction

- Implémenter un pare-feu en frontal
- Autoriser les flux entrants
 - Le serveur WEB (TCP/80 et TCP/443)
 - Le serveur DNS (UDP/53 et TCP/53)

Résultat :

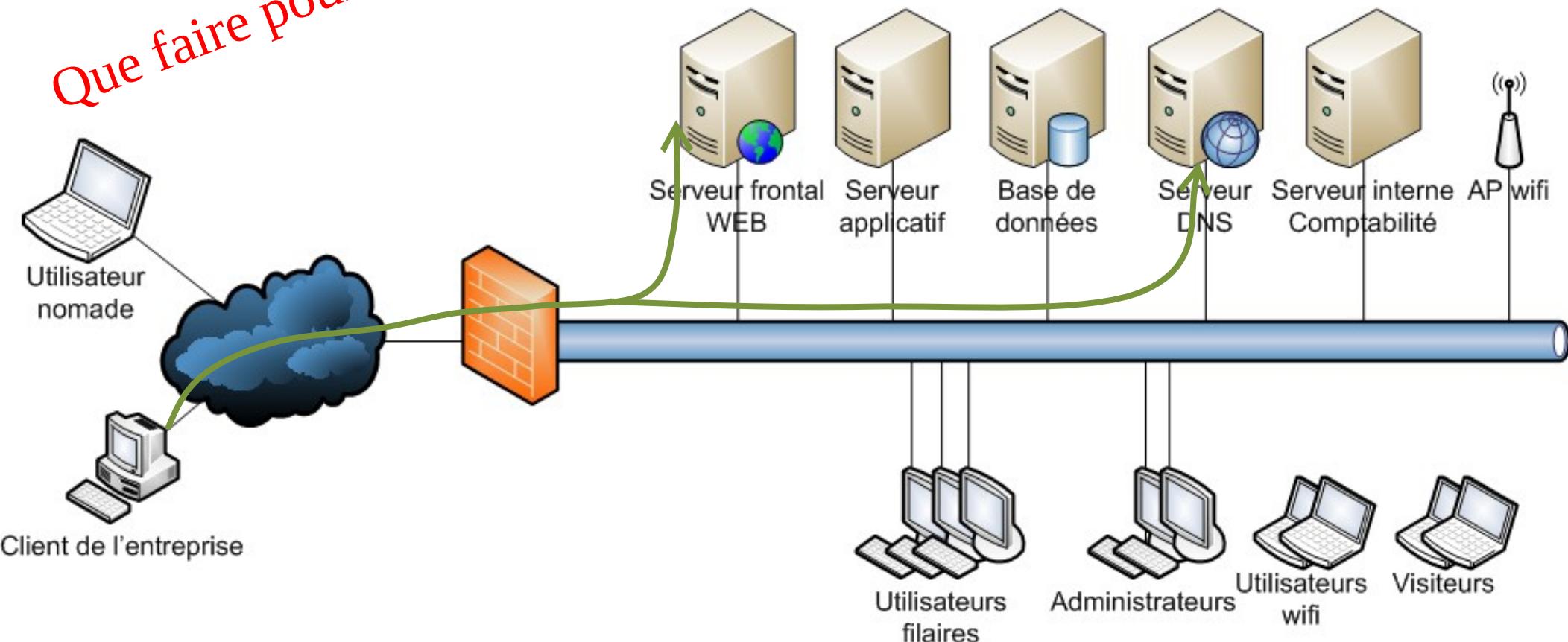
Internet ne pourra plus accéder au reste du réseau interne.



Exemple pratique de sécurisation avec un réseau simple



Que faire pour sécuriser ?



Réseau « à plat », avec un pare-feu en frontal



Exemple pratique de sécurisation avec un réseau simple

- Le pare-feu empêche la connexion directe entre internet et le réseau interne
 - Si le serveur WEB présente une vulnérabilité, Un hacker présent sur Internet peut potentiellement prendre la main sur ce serveur, puis rebondir ensuite sur le réseau interne

Solution :

Segmenter notre réseau en différentes zones de criticité, notamment :

- Une DMZ → Héberger tous les serveurs qui doivent être accessibles depuis internet (juste ceux-ci).

En cas de faille dans le serveur web, un attaquant aurait plus de difficultés pour rebondir sur le réseau interne

- Une zone destinée aux serveurs internes de l'entreprise ;

- Une zone pour les postes de travail filaires des utilisateurs ;

- Une zone pour les postes de travail wifi des utilisateurs ;

- Une zone pour les postes wifi des visiteurs ;

- Une zone pour les postes de travail des administrateurs, car ceux-ci ont besoin d'accéder à des interfaces d'administration (RDP, SSH...).

Optimisation segmentation :

- Ajout d'un 2^e pare-feu (interne) pour gérer tous les flux (y compris internes)

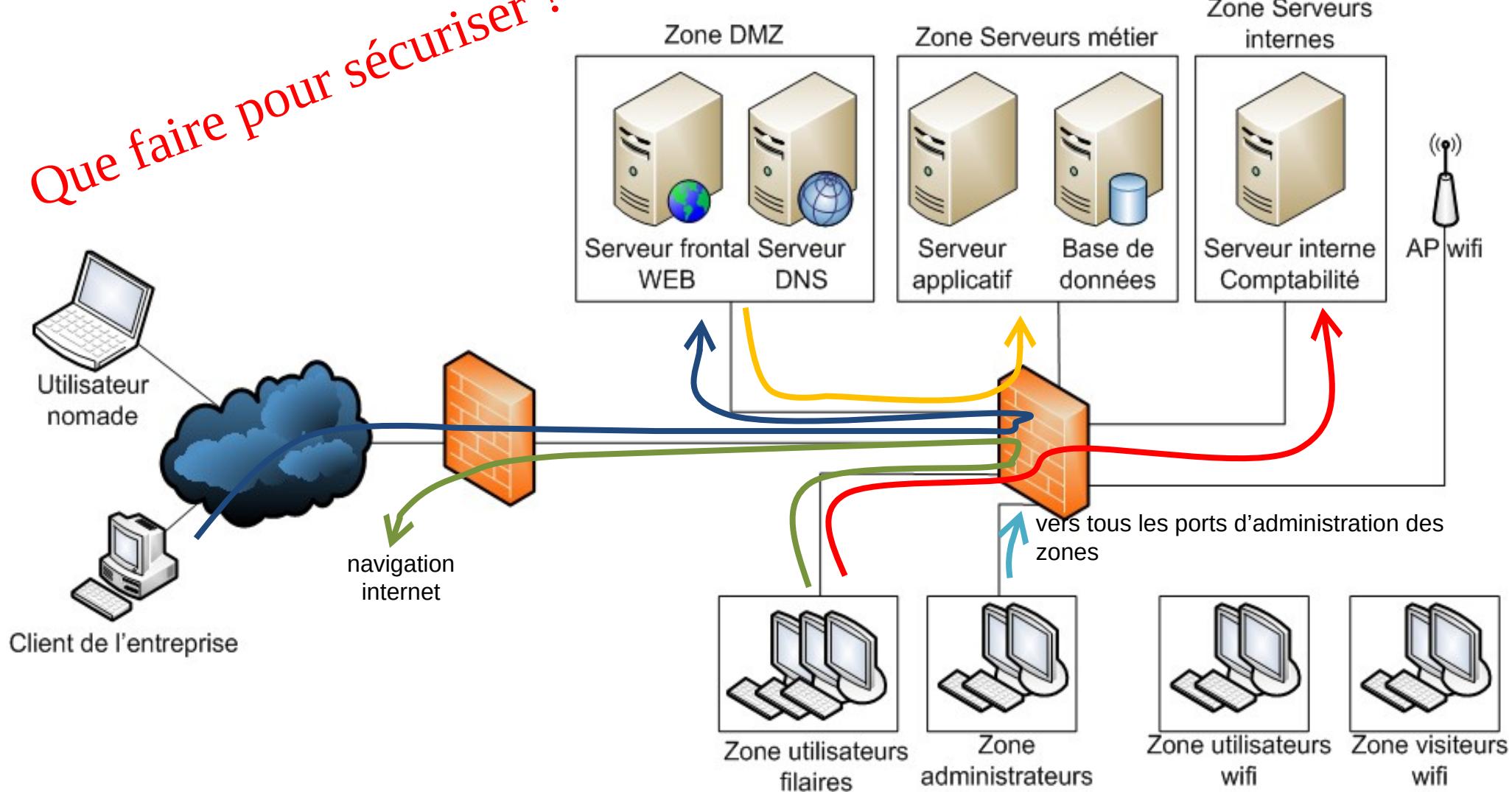
Note : Risque d'avoir les réseaux segmentés mais non filtrés.

Cela ne sert à rien en terme de sécurité, car toutes les zones peuvent communiquer entre-elles.

Exemple pratique de sécurisation avec un réseau simple



Que faire pour sécuriser ?

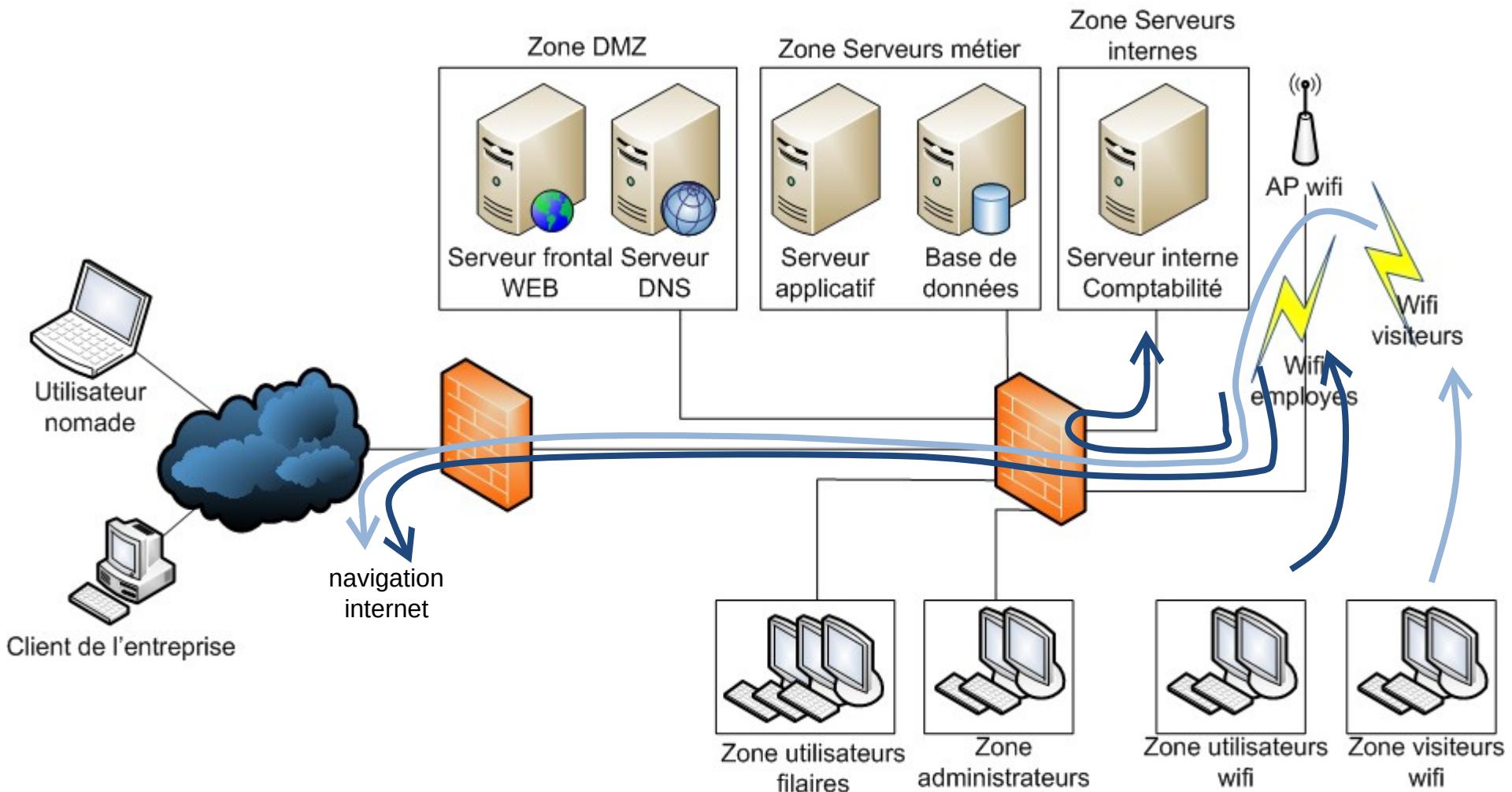


Réseau avec des zones segmentées, et un filtrage systématique via le pare-feu, y compris pour les flux internes.

Exemple pratique de sécurisation avec un réseau simple



- Le point d'accès wifi doit être accessible aux visiteurs et aux employés internes. Puisque le besoin d'accès aux ressources est différent pour ces 2 populations, nous allons donc implémenter deux SSID (deux réseaux wifi distincts, portés par le même point d'accès, et dont le pare-feu filtrera les flux).

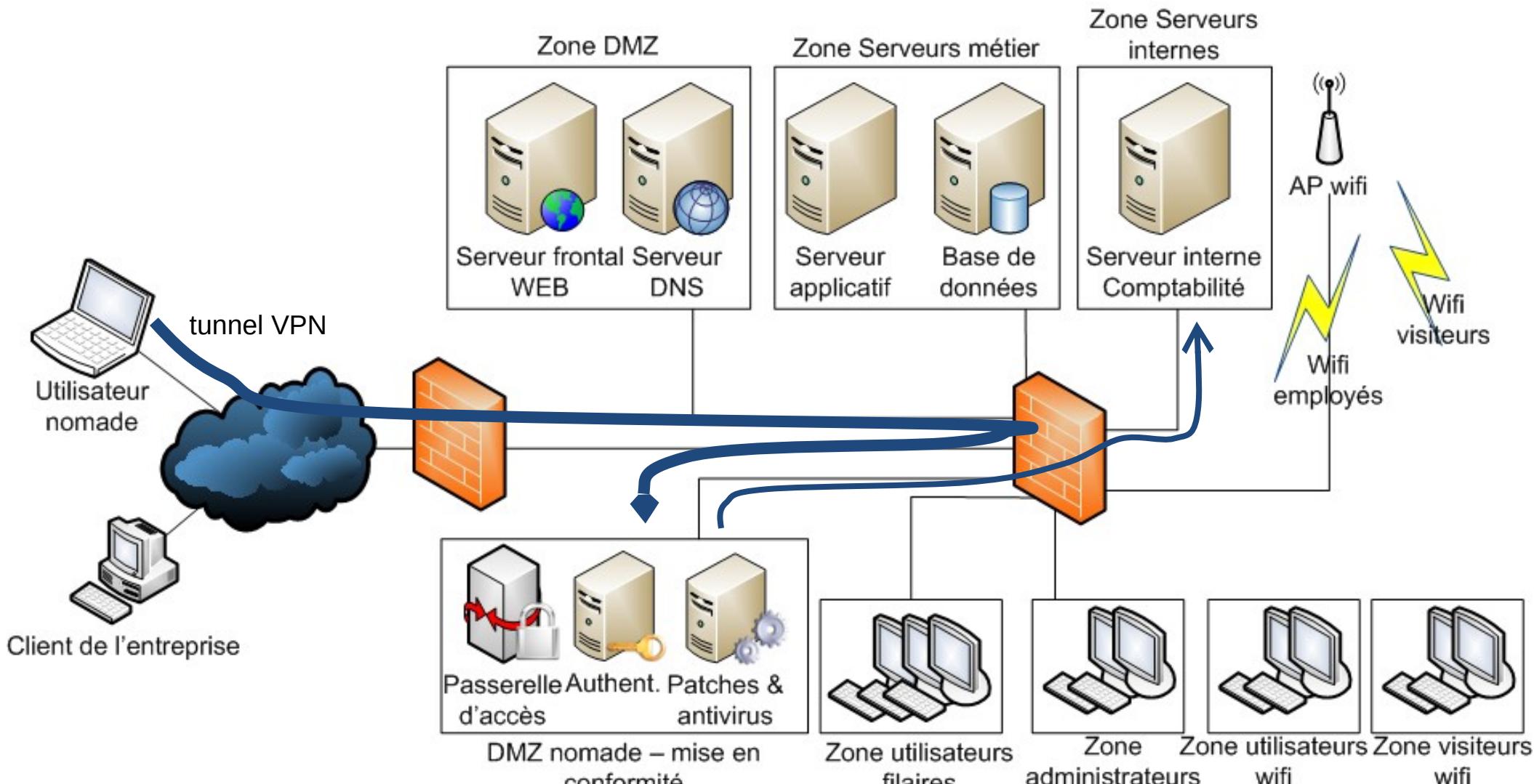




Exemple pratique de sécurisation avec un réseau simple

- Ne pas oublier les utilisateurs nomades
 - Pour se connecter au réseau interne depuis internet.
- Cela se fait via une DMZ spécifique
 - Appelée zone de mise en conformité
 - Le rôle est le suivant :
 - Fournir l'interface d'accès au réseau interne depuis internet,
 - via un tunnel VPN ;
 - Vérifier que le poste nomade et son utilisateur sont habilités
 - pour se connecter à distance
 - Vérifier le niveau de sécurité du poste avant d'autoriser la connexion
 - patches et anti-virus à jour notamment
 - Si tout est OK, alors autoriser les flux vers les zones internes
 - Seulement celles qui sont nécessaires pour le métier
 - Toujours en passant par le pare-feu.

Exemple pratique de sécurisation avec un réseau simple



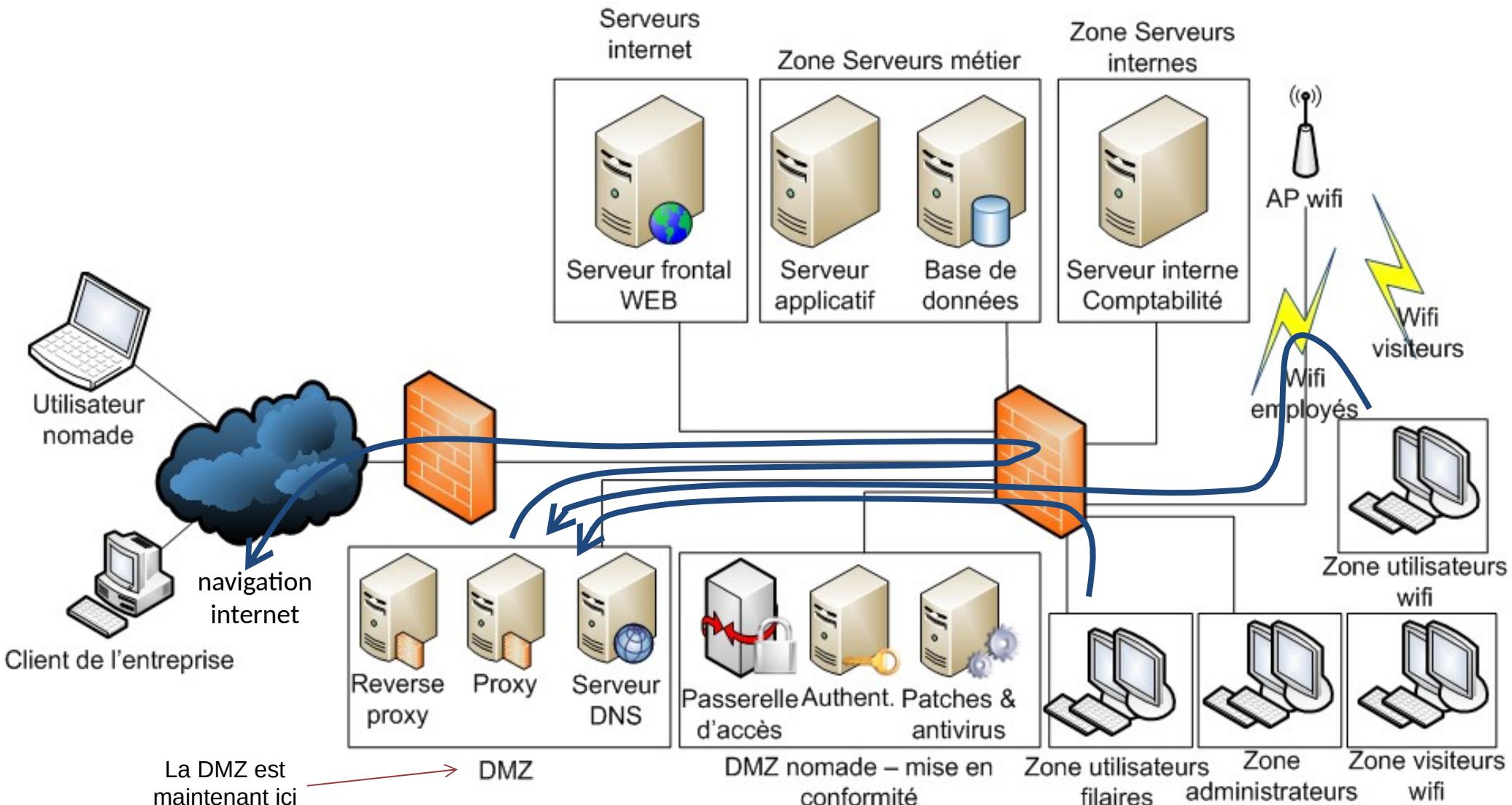
Réseau avec DMZ de mise en conformité pour les postes nomades.



Exemple pratique de sécurisation avec un réseau simple

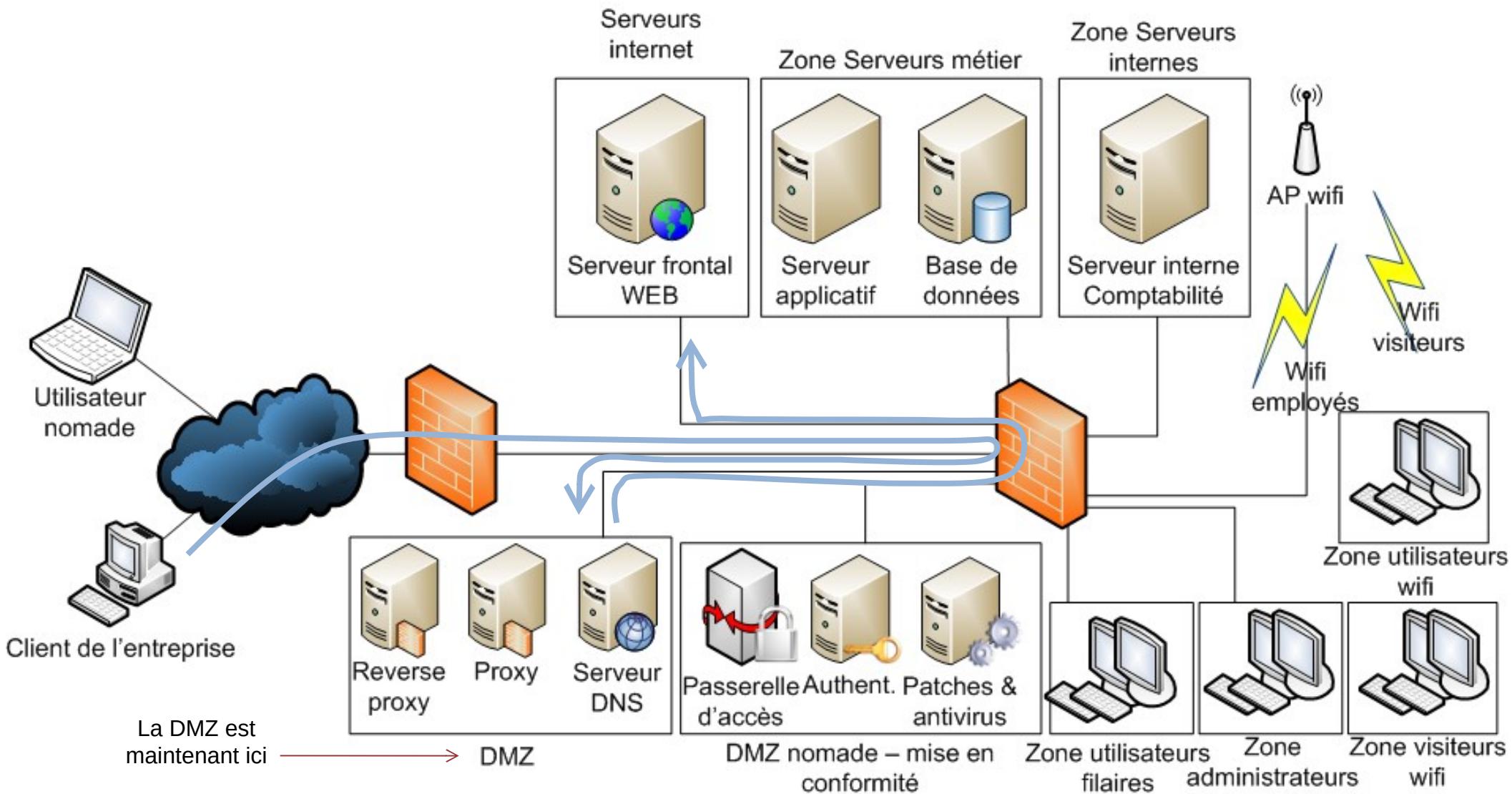
- Améliorer le filtrage du trafic WEB entrant et sortant :
 - Trafic sortant :
 - définir les catégories de sites WEB que les employés sont autorisés à naviguer,
 - implémenter une liste blanche ou noire de sites autorisés/interdits
 - Trafic entrant :
 - analyser les requêtes WEB d'internet vers le serveur de e-commerce afin d'intercepter les requêtes malveillantes (injection, malware, etc.)
- Solution
 - Prévoir :
 - Un proxy pour analyser les flux sortants,
 - Un reverse-proxy pour analyser les flux entrants.
 - Si coupure
 - bloquent les postes de travail des utilisateurs d'être connectés directement à Internet
 - Possibilité de toujours naviguer sur les sites autorisés.
 - Même remarque pour le serveur WEB :
 - Celui-ci n'est plus connecté directement sur Internet, c'est le reverse-proxy qui est maintenant en frontal.
- Puisque les proxies et reverse-proxies sont en frontal Internet, ce sont donc eux qu'il faut placer dans la DMZ maintenant.

Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet

Exemple pratique de sécurisation avec un réseau simple



Réseau avec un proxy et un reverse-proxy en coupure des flux de/vers Internet.

A retenir

- Le réseau sécurité a un rôle important
 - En entreprise
 - Ne pas l'oublier dans un projet
- L'exemple pratique
 - Présente juste les grandes lignes.
 - Cet exercice n'est ni exhaustif ni la seule solution possible.



EXERCICE

<https://school.hello-design.fr>

4B

La suite de la Session 4 ???

- La suite de cette partie
 - Rendez vous la semaine prochaine



Rendez-vous au prochain cours

- Merci de votre attention

