



INF4420: Éléments de Sécurité Informatique

Exercices Sécurité Web + Corrigé



Exercices de sécurité Web

- Exercice 1 : Comprendre l'authentification dans les serveurs Web
- Objectif :
 - Connaître la structure des certificats
 - Comprendre à quoi servent les certificats
 - Comprendre à quoi servent les infrastructures à clé publique (PKI – Public Key Infrastructure)

Exercices de sécurité Web

- Exercice 1 : Comprendre l'authentification dans les serveurs Web
- Vous souhaitez accéder au site web de votre banque
- Vous saisissez l'URL de votre banque dans votre navigateur
- Votre navigateur fait la demande de connexion avec le serveur de la banque via le protocole HTTPS



Exercices de sécurité Web

- Question 1 : Que se passe-t-il toujours immédiatement après la demande de connexion du client ?
 1. Le serveur envoie sa clé de chiffrement symétrique au client
 2. **Le serveur envoie son certificat au client**
 3. Le serveur demande au client de s'authentifier
 4. Le serveur demande au client de lui envoyer son certificat



Exercices de sécurité Web

- Réponse question 1 : Le serveur envoie son certificat X.509 au client
- Le serveur peut demander son certificat au client
 - C'est optionnel

quand le serveur renvoie son certificat, il contient sa clé publique

ce type de certificat ne fonctionne que si la cryptographie est asymétrique
si on utilise de la cryptographie post quantique il faut trouver un nouveau moyen
pour la vérification des certificats



Exercices de sécurité Web

- Question 2 : Qu'est-ce qu'un certificat X.509 ne contient jamais ?
 - La clé publique du serveur
 - La date de validité du certificat
 - La clé symétrique qui va permettre d'établir une connexion sécurisée entre le client et le serveur
 - La signature électronique des informations contenues dans le certificat

client va forger une clé symétrique et chiffrer cette clé avec la clé publique du serveur et l'envoyer au serveur par la suite le serveur va déchiffrer la clé symétrique avec sa clé privée la communication va être chiffré avec la clé symétrique.

chiffrement symétrique pour communication car meilleur en performance



Exercices de sécurité Web

- Réponse question 2 : Un certificat ne contient jamais la clé symétrique de session
- La clé symétrique pour établir la session sécurisée entre le client et le serveur sera générée ensuite par le client
- Le client utilisera la clé publique transmise par le serveur dans son certificat pour transmettre la clé de session au serveur
- Voir plus tard la présentation du protocole SSL-TSL dans le cours de sécurité réseau 2



Exercices de sécurité Web

- Question 3 : Que fait le client lorsqu'il reçoit le certificat du serveur ?
 1. Le navigateur du client consulte sa base de certificats pour vérifier s'il en possède un qui est le même que celui envoyé par le serveur
 2. Le navigateur du client consulte sa base de certificats pour vérifier s'il existe une autorité de certification qui confirme la signature du client
 3. Le navigateur n'a pas de base de certificats. Il doit envoyer le certificat à une autorité de certification pour vérification

navigateur a une liste de CA root qui émet les certificats
il vérifie si dans le certificat du serveur son root CA est dans
sa liste pour confirmer



Exercices de sécurité Web

- Réponse question 3 : Réponse 2
 - Le navigateur du client consulte sa base de certificats (la plupart est intégrée par défaut à l'installation du navigateur)
 - Le certificat envoyé par le serveur annonce une autorité de certification
 - Si le navigateur a le certificat de cette autorité dans sa base, il utilise la clé publique de cette autorité pour vérifier la signature du certificat envoyée par le serveur
- Comment consulter cette base de certificats ?
 - Sous Firefox : Menu → Options
 - Vie privée et sécurité → Certificats → Afficher les certificats

Exercices de sécurité Web

- Structure d'un certificat X.509
 - DN (*Distinguished Name*) de l'entité détentrice du certificat (le serveur)
 - DN du délivreur (autorité de certification)
 - Validité (dates limites)
 - Pas avant
 - Pas après
 - Informations sur la clé publique
 - Algorithme de la clé publique
 - Clé publique proprement dite
 - Divers
 - Numéro de série
 - Algorithme de signature du certificat
 - Version
 - Extensions (optionnel, à partir de X.509v3)
 - Liste des extensions
 - Identifiant unique du signataire (optionnel, X.509v2)
 - Identifiant unique du détenteur du certificat (optionnel, X.509v2)
 - Signature des informations ci-dessus par l'autorité de certification

le propriétaire du site génère une paire de clé public et privée et l'envoie a un CA qui va vérifier l'identité du propriétaire.
CA va générer un certificat avec la clé publique et d'autres info

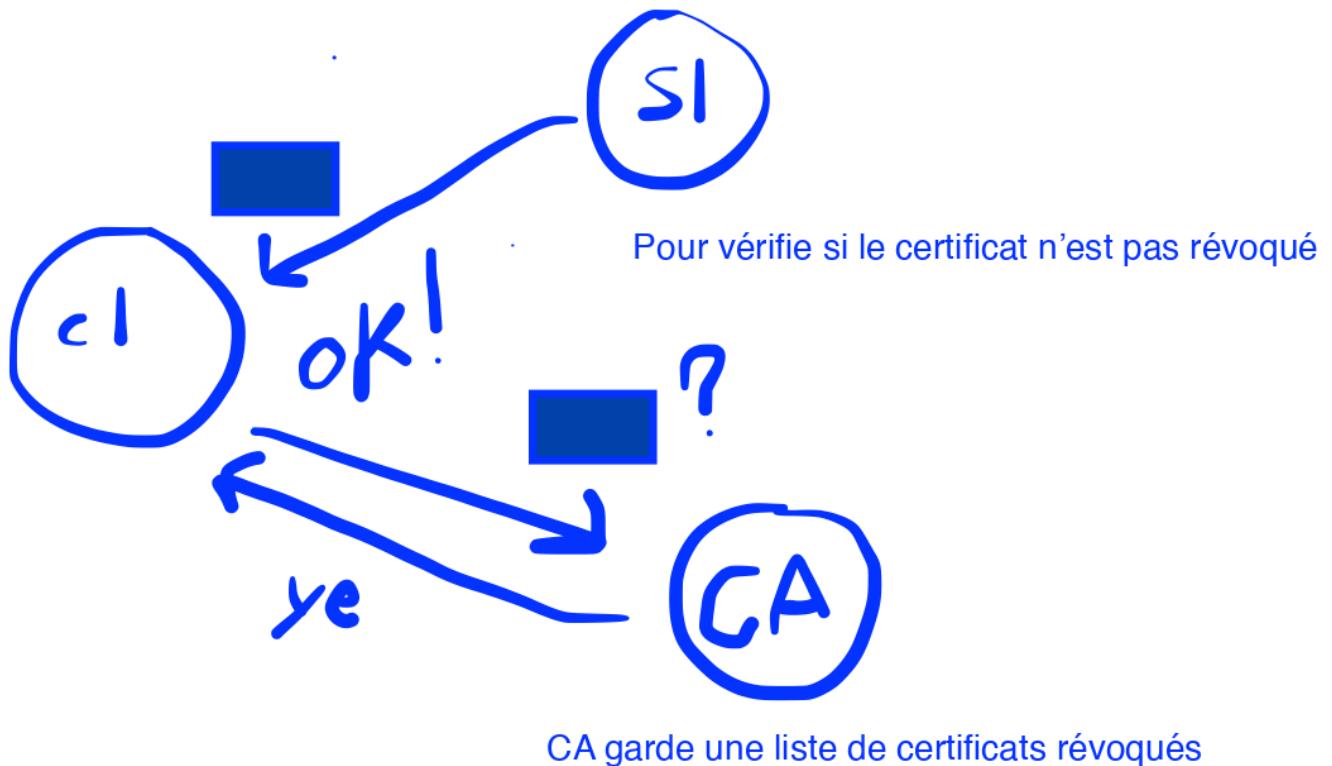
client utilise le certificat du server pour générer un hash avec algo SHA-256 et chiffre le hash avec la clé public du CA trouvé avec un algo comme RSA et compare le résultat avec la signature du certificat



Exercices de sécurité Web

- Question 4 : Une fois que le navigateur du client a vérifié que le certificat du serveur est signé par une autorité valide, le client va consulter cette autorité de certification ?

1. Vrai
2. Faux





Exercices de sécurité Web

- Réponse question 4 : C'est vrai
- Le client demande à l'autorité de certification de confirmer que le certificat n'a pas été révoqué par l'autorité



Exercices de sécurité Web

- Remarque : il peut arriver que certains sites utilisent leur clé privée pour signer leur certificat
 - On parle alors de certificat auto-signé
 - En général, c'est une anomalie que votre navigateur va vous signaler
 - A vous de décider ! (soyez prudent)

 **Cette connexion n'est pas certifiée**

Vous avez demandé à Firefox de se connecter de manière sécurisée à **192.168.116.6**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

[Sortir d'ici !](#)

► **Détails techniques**

▼ **Je comprends les risques**

Si vous comprenez ce qui se passe, vous pouvez indiquer à Firefox de commencer à faire confiance à l'identification de ce site. **Même si vous avez confiance en ce site, cette erreur pourrait signifier que quelqu'un est en train de pirater votre connexion.**

N'ajoutez pas d'exception à moins que vous ne connaissiez une bonne raison pour laquelle ce site n'utilise pas d'identification certifiée.

[Ajouter une exception...](#)



Exercices de sécurité Web

- Hiérarchie d'autorités de certification et autorités racines
 - Certaines autorités de certification jouent le rôle d'autorités racines
 - Ce sont les seuls certificats qui devraient pouvoir être auto-signés
- Exemple de certificats racines installés par défaut :
 - VeriSign
 - Entrust.net certificat chainé si entreprises avec ses filiales ou objets connectés
 - Equifax Secure CA émet un certificat pour un CA intermédiaire qui à son tour va signer un certificat à un site
 - GlobalSign
 - GTE CyberTrust Root et Global Root
 - Secure Server (RSA) Client vérifie le CA root et descend jusqu'à la fin si un dans chaîne foire tout foire
 - Thawte Premium Server



Exercices de sécurité Web

- Conséquence 1

- Le serveur n'a peut-être pas un certificat signé par une autorité racine
- Dans ce cas, c'est une chaine de certificats remontant jusqu'à une autorité racine que le serveur doit envoyer au client
- Le client doit vérifier tout la chaîne pour valider le certificat du serveur
- On parle alors de certificats chainés



Exercices de sécurité Web

- Conséquence 2 et question 5 : Que se passe-t-il si une autorité de certification se fait voler sa clé privée ?
 1. Game over !
 2. Il faut réinstaller le navigateur
 3. L'autorité doit immédiatement révoquer tous ses certificats
 4. L'autorité et toutes les autorités ayant des certificats chainés avec cette autorité doivent révoquer leurs certificats

relation hiérarchique CA peut prévenir
Bob (serveur)



Exercices de sécurité Web

- Réponse question 5 : Réponse 4
 - Si une autorité se fait voler son certificat, c'est toute la chaîne de certificats issues de cette autorité qui est potentiellement corrompue !
 - C'est pourquoi il est très important que le client vérifie auprès de l'autorité de certification que le certificat n'a pas été révoqué



Exercices de sécurité Web

- Infrastructures de Gestion de Clés (IGC)
 - En Anglais : Public Key Infrastructure (PKI)
- Une autorité de certification est un cas particulier d'IGC
 - Modèle de PKI reposant sur les certificats X.509
 - Il existe d'autres modèles de PKI notamment PKI distribuée
 - Toile de confiance avec OpenPGP
 - Blockchain-based PKI



plusieurs noeuds chaque recommande la confiance pour un autre



INF4420: Éléments de Sécurité Informatique

Exercice Sécurité des logiciels et des OS



Exercices de sécurité logiciel et des OS

- Exercice 1 : Analyse d'un shell code
- Objectif :
 - Mieux comprendre l'écriture d'un shell code

```
#include <stdio.h>
#include <string.h>

void func(char * name) {
    char buf[100];
    strcpy(buf,name);
    printf("Welcome %s\n",buf);
}

int main(int argc, char *argv[]) {
    func(argv[1]);
    return 0;
}
```



Exercices de sécurité logiciel et des OS

- Retour sur le shell code vu en cours

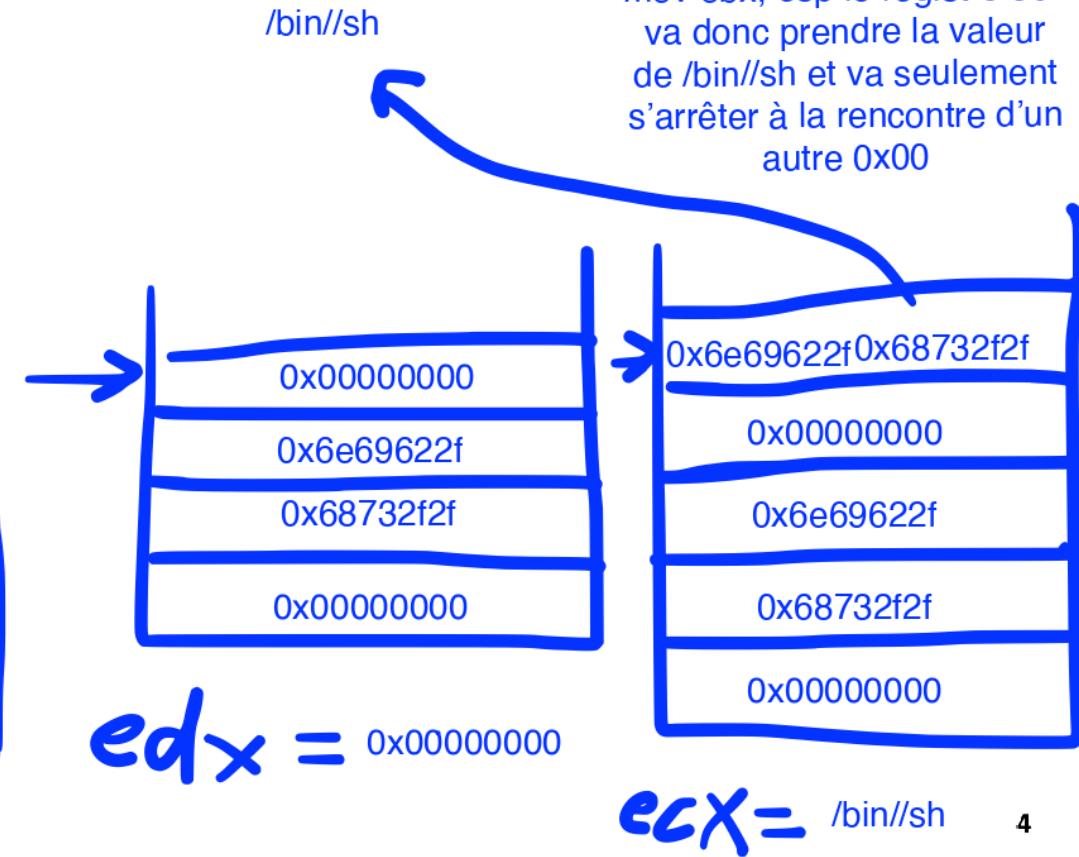
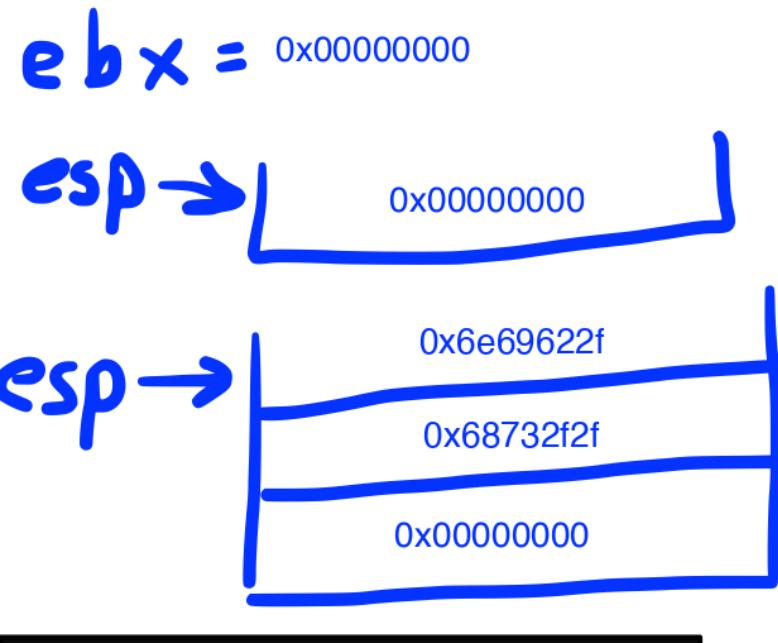
```
xor eax, eax          ; Clearing eax register
push eax              ; Pushing NULL bytes
push 0x68732f2f       ; Pushing //sh
push 0x6e69622f       ; Pushing /bin
mov ebx, esp           ; ebx now has address of /bin//sh
push eax              ; Pushing NULL byte
mov edx, esp           ; edx now has address of NULL byte
push ebx              ; Pushing address of /bin//sh
mov ecx, esp           ; ecx now has address of address
                       ; of /bin//sh byte
mov al, 11             ; syscall number of execve is 11
int 0x80              ; Make the system call
```



Exercices de sécurité logiciel et des OS

- Question 1 : L'instruction « xor eax, eax » est logiquement équivalente « mov eax, 00 »

- Vrai
- Faux





Exercices de sécurité logiciel et des OS

- Réponse question 1 : La réponse est vrai
- L'effet de l'instruction « xor eax, eax » est de remettre le registre eax (l'accumulateur) à 0

moves value 11 in register al
11 is the number for execve in linux call table
executes a new process by replacing
the current one

int 0x80
interrompre le processus courant
et executer le processus en mode
root



Exercices de sécurité logiciel et des OS

- Question 2 : Pourquoi l'attaquant utilise-t-il l'instruction « xor eax, eax » plutôt que « mov eax, 00 » ?
 1. Pour que le shell code soit plus difficile à détecter
 2. Pour éviter que le shell code contienne des 00
 3. Pour que l'exécution du shell code soit plus rapide
 4. Pour que le shell code soit plus compact

pour éviter qu'il y a des 00 dans le shellcode
car signifie fin de chaîne de caractères et
processeur va arrêter d'executer après la première instruction

les 4 octets avec mov eax,00 seulement les 2 derniers
octets sont mis à 0 les 2 premiers ne changent pas
en utilisant le registre à la suite peut introduire
des octets nuls et couper des chaînes de caractères



Exercices de sécurité logiciel et des OS

- Réponse question 2 : réponse 2
- Le shell code ne doit pas contenir de 00 (NULL)
 - 00 est le caractère indiquant la fin de chaîne de caractères
 - Si un shell code contient un NULL, la fin du programme après le NULL sera ignorée



Exercices de sécurité logiciel et des OS

- Question 3 : Que fait le couple d'instruction « push 0x68732f2f push 0x6e69622f » ?

1. Il fait un appel système pour exécuter un shell
2. Il pousse /bin//sh sur la pile
3. Il pousse hs//nib/ sur la pile

lecture à l'envers

processeur moderne avec pile qui descend et tas qui monte car mémoire limité donc pour optimisé la gestion de mémoire

Unix a introduit ça mais Multix pas vulnérable à buffer overflow



Exercices de sécurité logiciel et des OS

- Réponse question 3 : La bonne réponse est 3
- Le codage en hexa correspondant à « hs//nib/ » est poussé sur la pile
 - Le shell code est écrit du bas vers le haut
 - Mais la mémoire va être lue du haut vers le bas



Exercices de sécurité logiciel et des OS

- Pour récapituler (et pour faire simple), le shell code va :
 - Provoquer un **appel système** (instruction « `int 0x80` » sous Linux)
 - Demander l'**exécution** de la **commande execve** (exécute le programme passé en paramètre)
 - **Ecrire dans la mémoire** le programme que **doit exécuter** la commande **execve** (correspondant ici à « `/bin//sh` »)
 - Tout ça étant écrit de manière à éviter la présence de Null dans le shell code !



Exercices de sécurité logiciel et des OS

- Exercice 2 : Imprimer illégalement des fichiers
- Objectif :
 - Savoir identifier une vulnérabilité dans un programme C



Exercices de sécurité logiciel et des OS

- Exercice 2 : Imprimer illégalement des fichiers
- Un collègue qui n'a pas suivi le cours INF4420A a écrit le programme suivant sous DOS pour imprimer un fichier :

```
void main(int argc, char *argv[])
{
    FILE *imprim;
    imprim=fopen("PRN","wt");
    fprintf(imprim, "%s\n" ,argv[1]);
    fclose(imprim); }
```

ne s'assure pas s'il y a d'autres processus en train d'accéder le fichier PRN et n'a pas de sémaphores ou vérifications pour être sûr que l'écriture est le bon fichier et pas un lien symbolique

lien symbolique: type de fichier spécial qui agit comme un pointeur ou référence à un autre fichier ou dossier.



Exercices de sécurité logiciel et des OS

- **Explication**
 - Sous DOS, l'imprimante est considérée comme un fichier
 - Le nom de ce fichier (en écriture seule) est « PRN »
 - Pour imprimer, il suffit d'ouvrir ce fichier, d'y écrire et le résultat sera sur l'imprimante



Exercices de sécurité logiciel et des OS

- Question 1 : Quelle vulnérabilité « potentielle » identifiez-vous dans ce programme ?
 1. Stack overflow
 2. Heap overflow
 3. Race condition
 4. Format string vulnerability
 5. Fuite de mémoire



Exercices de sécurité logiciel et des OS

- Réponse question 1 : Le programme est potentiellement vulnérable à une attaque par race condition

Les 2 en course si le processus trouve le bon fichier avant
ou trouve le lien symbolique avant
la création du lien symbolique est une opération instantané



Exercices de sécurité logiciel et des OS

- Question 2 : Quel scénario envisagez-vous pour exploiter cette vulnérabilité ?

comme on voit dans le programme, lorsqu'il ouvre le fichier PRN il ne n'assure pas que c'est le bon fichier. l'attaque peut créer un fichier de lien symbolique dans un des dossiers spécifié dans PATH. la fonction fopen() si on donne juste le nom du fichier en paramètre le système va essayer de retrouver le fichier dans un des dossier spécifié dans PATH

le fichier lien symbolique va donc rediriger le système vers le fichier avec le même nom créé par l'attaquant et l'opération d'écriture va écrire de l'information sensible dans le fichier de l'attaquant.



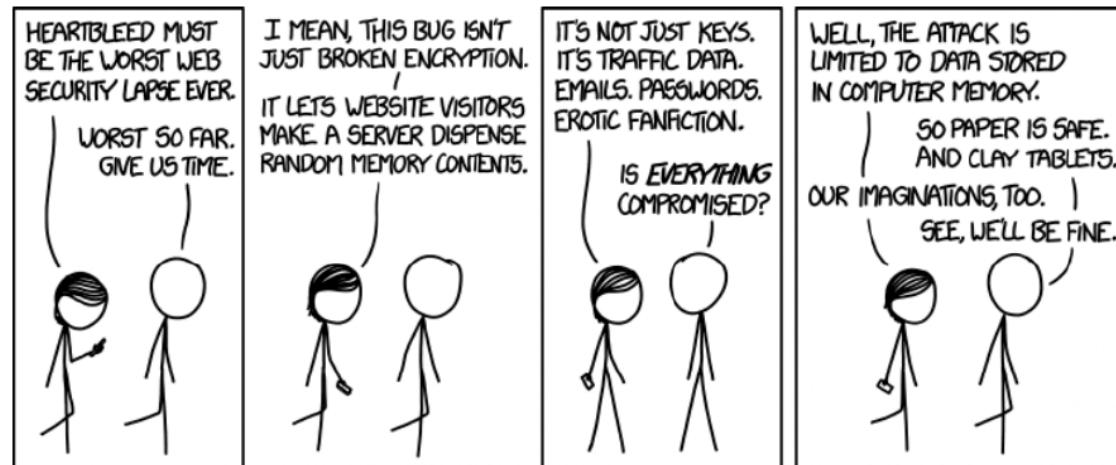
Exercices de sécurité logiciel et des OS

- Réponse question 2 :
 - Scénario possible : empêche la sortie du résultat sur papier physique
 - Vous retirez le tiroir de l'imprimante
 - Vous lancez une impression avec le programme de votre collègue redirige la sortie vers le fichier passwd
 - Vous exécutez la commande symlink("/etc/passwd", "PRN")
 - Vous remettez le tiroir de l'imprimante et vous attendez de voir ce qui est imprimé Le contenu dans le fichier passwd va être imprimé
- Si le programme a des priviléges spéciales, il peut écrire dans le fichier passwd
- Remarque
 - De nos jours, le fichier "/etc/passwd" ne sera pas imprimé
 - Mais les vieilles versions de la fonction "print" étaient vulnérables à ce type d'attaque par race condition



Exercices de sécurité logiciel et des OS

- Exercice 3 : Heartbleed
- Objectif :
 - Savoir identifier et comprendre une vulnérabilité





Exercices de sécurité logiciel et des OS

- **Exercice 3 : Heartbleed**

TLS: protocol qui chiffre les données en utilisant la clé public du server pour le chiffrement de la clé symétrique et le serveur déchiffre la clé symétrique en utilisant sa clé privée

les données de communication sont chiffrés en utilisant la clé symétrique

- Février 2012 : Introduction de la fonction Heartbeat dans le protocole TLS (Transport Layer Security)

- Heartbeat permet de tester et de maintenir en vie un lien SSL-TLS sans avoir à renégocier la connexion

Client sends random payload of data to server
server respond by sending back the same payload of data
to confirm that connection is still alive

- Mars 2012

- Détection d'un bug dans l'implémentation de la fonction Heartbeat de OpenSSL



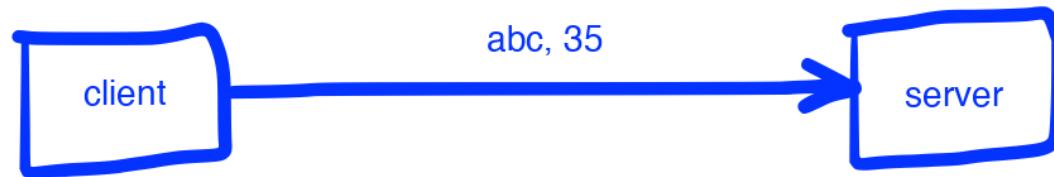
Exercices de sécurité logiciel et des OS

- Principe du heartbeat
 - Envoi d'un message <Mot, Nombre de lettres> dans le VPN SSL
 - Exemple : <bird, 4 letters>
 - Si l'autre extrémité du VPN est « vivante », elle répond « bird »
- Question 1 : Sans avoir plus détail sur l'implémentation de la fonction Heartbeat, quelle vulnérabilité « potentielle » identifiez-vous dans ce programme ?
 1. Stack overflow
 2. Heap overflow
 3. Race condition
 4. Format string vulnerability
 5. Fuite de mémoire



Exercices de sécurité logiciel et des OS

- Réponse question 1 : En l'occurrence, la bonne réponse est **fuite de mémoire**
- Remarque : une attaque par buffer flow serait également envisageable



vulnérabilité de serveur
OpenSSL





Exercices de sécurité logiciel et des OS

- Question 2 : Quel scénario (simple) envisagez-vous pour réaliser une attaque en fuite de mémoire ?

nom utilisateur, mot de passe, clé privée



Exercices de sécurité logiciel et des OS

HOW THE HEARTBLEED BUG WORKS:

- Réponse question 2 :

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



User Meg wants these 6 letters: POTATO. User Linda wants pages about "irl games". Unlocking secure records with master key 5130985733435. Note: (random) Linda has this password: 1234567890



POTATO

User Meg wants these 6 letters: POTATO. User Linda wants pages about "irl games". Unlocking secure records with master key 5130985733435. Note: (random) Linda has this password: 1234567890



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.883.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 345 connections open. User Brendan uploaded the file testcar (contents: 34ba962ac0baff9131ff8)



HMM...



BIRD

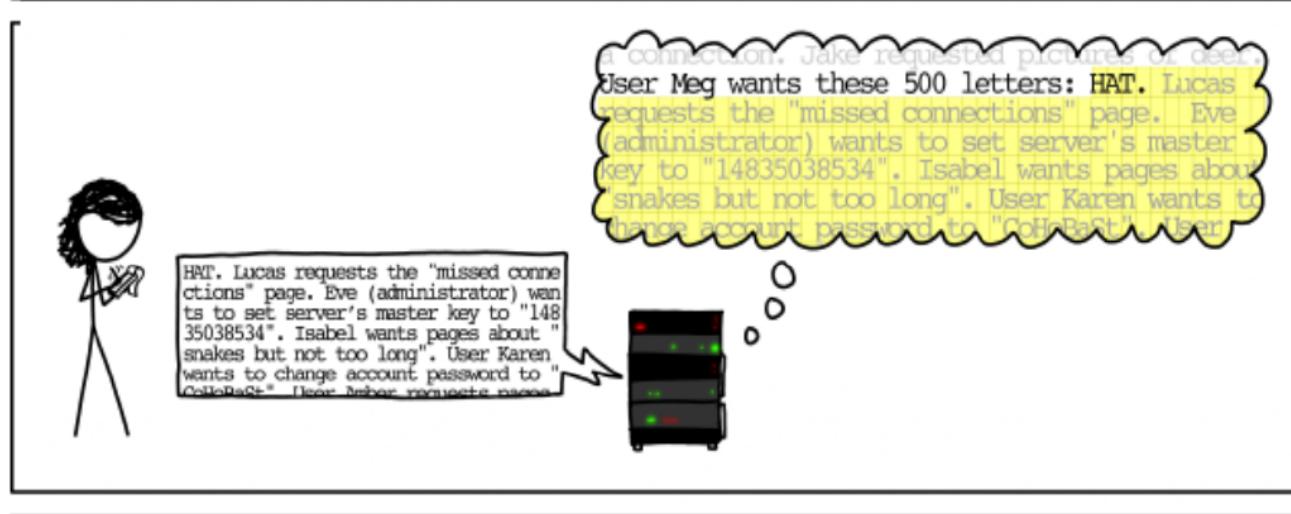
User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.883.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 345 connections open. User Brendan uploaded the file testcar (contents: 34ba962ac0baff9131ff8)





Exercices de sécurité logiciel et des OS

- Réponse question 2 :





Exercices de sécurité logiciel et des OS

- Réponse question 2 :
 - Attaque extrêmement simple !
 - Possibilité de récupérer jusqu'à 64kB de données sur le serveur en envoyant un heartbeat mal formé
 - Et possibilité de répéter l'opération à plusieurs reprises
 - Environ 500 000 serveurs vulnérables quand le bug fut découvert
- Risque
 - Vol de la clé privée du serveur (clé primaire)
 - Vol des clés secondaires du serveur
 - Vol d'autres données se trouvant à « proximité »
 - Mot de passe, numéro de carte, cookies
 - Etc.



INF4420a: Sécurité Informatique

Exercices Réseau Partie 1



Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise
- Objectif :
 - Savoir définir une architecture de sécurité réseau pour une petite entreprise
 - Savoir configurer un pare-feu à état conformément à une politique de filtrage réseau

Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise
- La petite entreprise YLOP.com a déployé, sur son réseau privé 192.168.0.0/16, plusieurs serveurs
 - 3 serveurs FTP (port TCP 22) (192.168.1.1, 192.168.2.1, 192.168.3.1)
 - 3 serveurs WEB (port TCP 80) (192.168.1.2, 192.168.2.2, 192.168.3.2)
 - 3 serveurs DNS (port UDP 53) (192.168.1.3, 192.168.2.3, 192.168.3.3)
- Il y a environ 100 employés dans l'entreprise YLOP.com qui ont leurs adresses de 192.168.4.1 à 192.168.4.254

Exercice de réseau

- Exercice 1 : Configuration du pare-feu d'une petite entreprise
 $11111111.11111111.11111111.11111000$ -2 : adr réseau et broadcast
32 bits in total 29 bits set to 1
 $2^{(32-29)}-2=6$ IP pour utilisateur
- L'entreprise YLOP.com a acheté une plage d'adresses publiques sur Internet
– 195.55.55.0/29 195.55.55.0 IP du réseau
- Vous venez d'être embauché en tant qu'administrateur de sécurité dans l'entreprise YLOP.com
- Vous avez en charge de proposer et configurer une architecture de sécurité pour l'entreprise YLOP.com

6 IP machines et 1 IP réseau et 1 IP broadcast= 8 IP

0-7



Exercice de réseau

- On vous demande d'écrire la table de port forwarding qui fera la liaison entre le réseau privé et Internet
 - Question 1 : Est-ce que ce déploiement est possible ?
 - Oui **OUI**
 - Non

Es ce que avec mes 6 adr IP public
peut déployer mes 9 serveurs ?

minimum 3 adr IP public pour les 3 types de serveurs
doivent être visible de l'extérieur

employés n'ont pas besoin d'être visible de l'extérieur du réseau donc peut réutiliser IP public des 3



Exercice de réseau

- Question 2 : Si réponse est oui à la question 1, proposez votre solution de NAT dynamique et de port forwarding ?

IP publique	port public	IP privée	port privée	
195.55.55.1	21	192.168.1.1	21	serveur FTP 1,
195.55.55.1	80	192.168.1.2	80	serveur WEB 1,
195.55.55.1	53	192.168.1.3	53	serveur DNS 1
195.55.55.2	21	192.168.2.1	21	serveur FTP 1,
195.55.55.2	80	192.168.2.2	80	serveur WEB 1,
195.55.55.2	53	192.168.2.3	53	serveur DNS 1
195.55.55.3	21	192.168.3.1	21	serveur FTP 1,
195.55.55.3	80	192.168.3.2	80	serveur WEB 1,
195.55.55.3	53	192.168.3.3	53	serveur DNS 1
195.55.55.1	>1024 (PAT)	192.168.4.0/24	>1024	

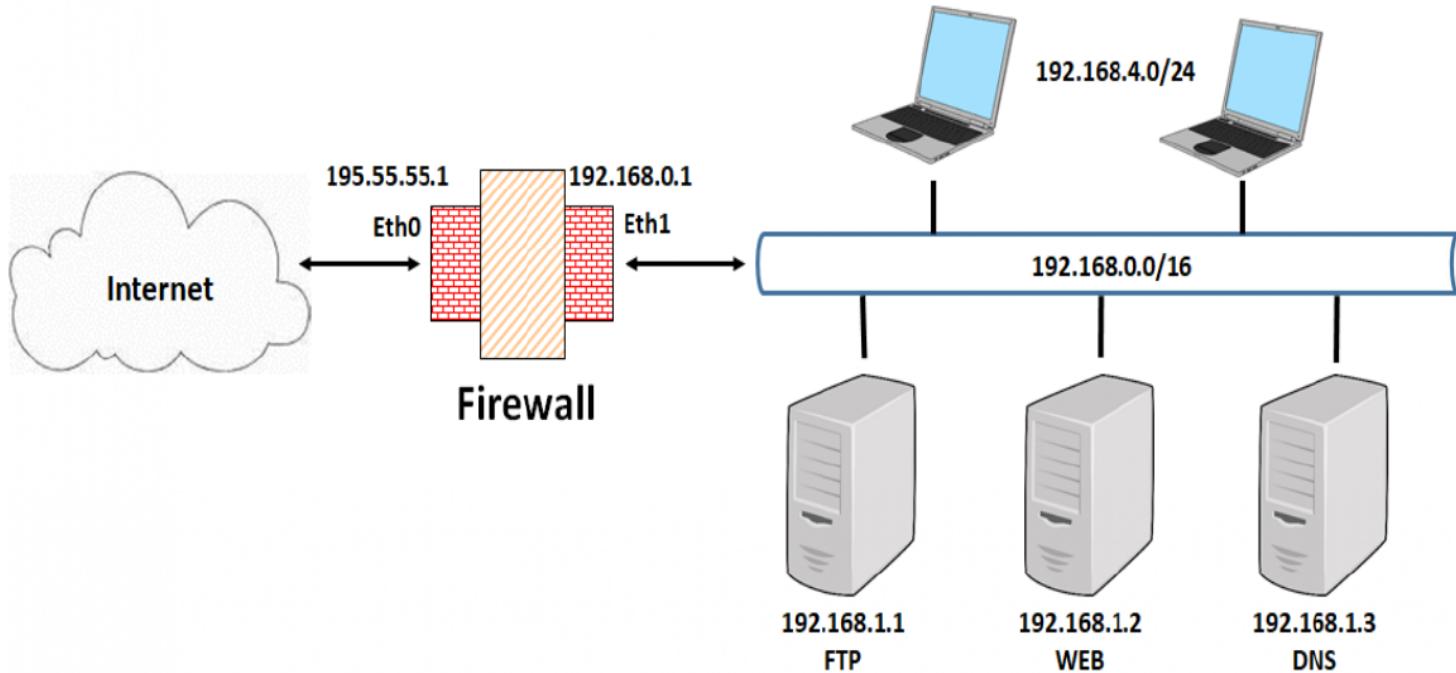
Exercice de réseau

- Sur son site de Montréal (adresse publique 195.55.55.1), l'entreprise YLOP.com a déployé
 - Les 3 serveurs d'adresses 192.168.1.1 (FTP), 192.168.1.2 (WEB) et 192.168.1.3 (DNS)
 - Les 100 employés (EMP)
- Pour assurer la sécurité du site de Montréal, YLOP.com a déployé un pare-feu Netfilter



Exercice de réseau

- Voici l'architecture de sécurité qui a été déployée chez YLOP.com



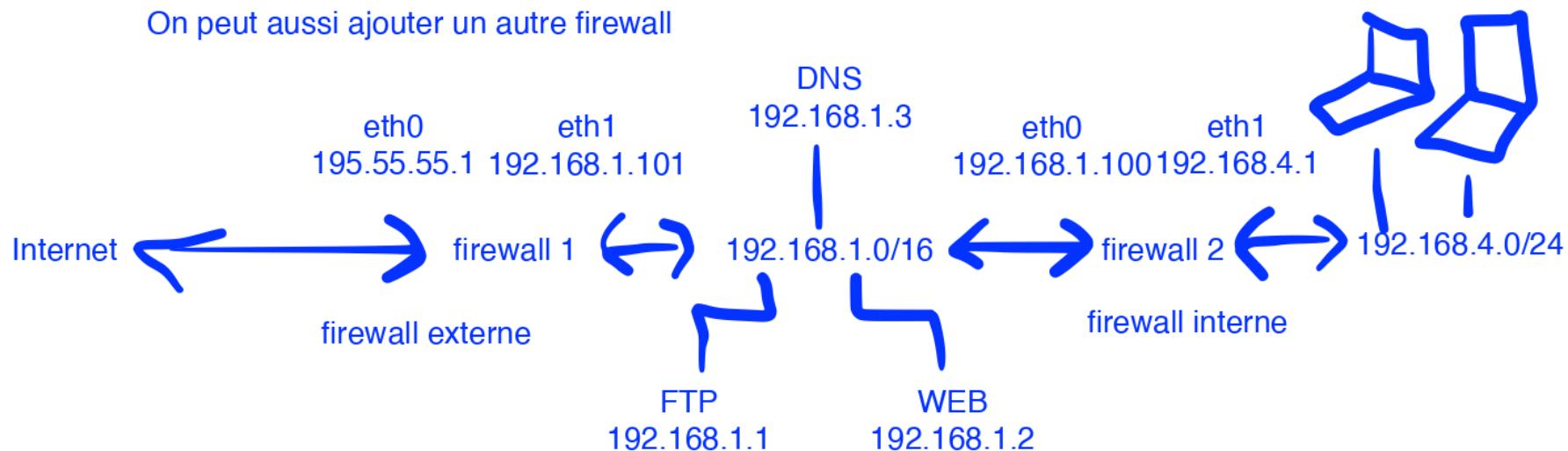


Exercice de réseau

- Question 3 : Quelles recommandations faites-vous à YLOP.com pour améliorer cette architecture de sécurité ?

comme les serveurs doivent être visibles de l'extérieur
mais pas nécessairement les machines des employés
on peut créer un DMZ pour mettre les serveurs dans
cette zone et les employés dans une zone privée

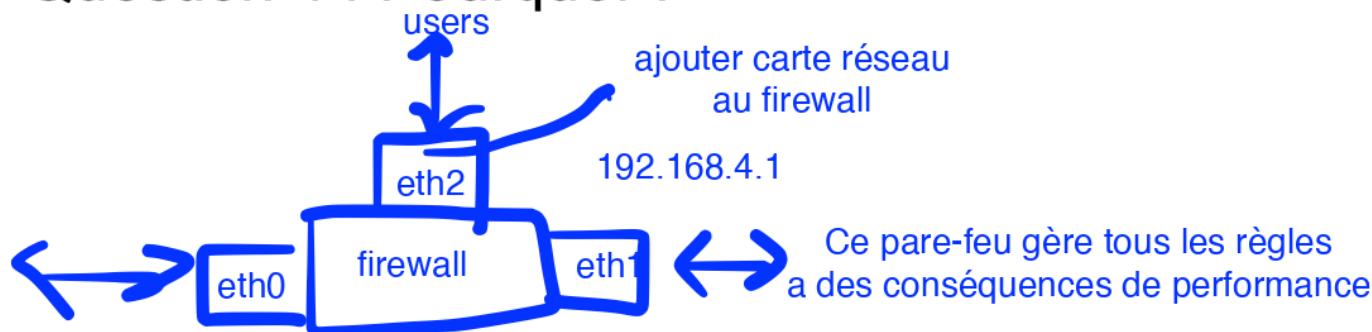
On peut aussi ajouter un autre firewall





Exercice de réseau

- Vous recommandez à votre direction la solution 1 avec deux pare-feux
- Question 4 : Pourquoi ?



La solution avec DMZ permet une double protection donc l'attaquant qui a accès au premier pare-feu doit attaquer le deuxième pare-feu pour pouvoir accéder aux données plus sensible



Exercice de réseau

- En raison de restrictions budgétaires, c'est finalement la solution 2 avec un seul pare-feu et trois interfaces réseau qui est retenue



Exercice de réseau

- Vous avez maintenant la charge de corriger / mettre à jour la configuration de ce pare-feu conformément à la politique de filtrage suivante :
 - Les serveurs FTP, WEB et DNS doivent être accessibles depuis Internet
 - Les employés EMP doivent pouvoir accéder à Internet
 - Les employés EMP doivent pouvoir accéder aux serveurs de la DMZ
 - Les serveurs de la DMZ ne peuvent pas initier de sessions avec les employés EMP mais seulement répondre à leur requête.

[par default politique fermé](#)



Exercice de réseau

- Ancienne config (page 1)

```
# set default closed policy
```

```
iptables -P INPUT DROP
```

Par défaut on jette les paquets
des sources inconnues

```
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
```

```
# network interfaces
```

```
EXTIF=eth0      déclare interface  
INTIF=eth1    doit en rajouter une      DMZIF=eth1  
INTIF=eth1      INTIF=eth2
```

```
# addresses
```

```
EXTIP=195.55.55.1 IP interface eth0
```

/24 8+8+8
pour 3 interfaces

```
FTP_SERVER=192.168.1.1
```

IP des serveurs

```
WEB_SERVER=192.168.1.2
```

```
DNS_SERVER=192.168.1.3
```

```
EMP_HOST=192.168.4.0/16
```

réseau privée des employés

```
# accept packets on the local interface
```

```
iptables -A INPUT -i lo -j ACCEPT
```

accept traffic arrivant sur interface

INPUT du firewall

```
iptables -A OUTPUT -o lo -j ACCEPT
```

accept traffic qui sort
du firewall

firewall personnelle
doit avoir FORWARD



Exercice de réseau

- Ancienne config (page 2)

reverse proxy internet -> firewall

manque translation d'adresse

the FTP server must be accessible from Internet

iptables -A FORWARD -i \$EXTIF -o \$INTIF -p tcp --dport 21 -j ACCEPT
DNAT port translation internet to FTP

iptables -t nat -A PREROUTING -i \$EXTIF -p tcp -d \$FTP_SERVER:21 -j DNAT - -to-destination

the web server must be accessible from Internet

iptables -A FORWARD -i \$EXTIF -o \$INTIF -p tcp --dport 80 -j ACCEPT

iptables -t nat -A PREROUTING -i \$EXTIF -p tcp -d \$WEB_SERVER:80 -j DNAT - -to-destination

the dns server must be accessible from Internet

iptables -A FORWARD -i \$EXTIF -o \$INTIF -p udp --dport 53 -j ACCEPT

iptables -t nat -A PREROUTING -i \$EXTIF -p udp -d \$DNS_SERVER:53 -j DNAT - -to-destination
\$DNS_SERVER:53

accessibilité des serveurs

iptables -t nat -A FORWARD -i \$EXTIF -o \$DMZIF -p tcp - -dport 21 -m state
- -state NEW, ESTABLISHED -j ACCEPT

iptables -t nat -A FORWARD -i \$EXTIF -o \$DMZIF -p tcp - -dport 80 -m state
- -state NEW, ESTABLISHED -j ACCEPT

iptables -t nat -A FORWARD -i \$EXTIF -o \$DMZIF -p udp - -dport 53 -m state
- -state NEW, RELATED -j ACCEPT



Exercice de réseau

- m state --state // defines the state to match
NEW // accepter la création en recevant le SYN
- ESTABLISHED // accepter la ACK
protocol udp considère que c'est RELATED
- Ancienne config (page 3)
- translation d'adresse équivalent à SNAT

```
# enable SNAT (MASQUERADE) functionality on External interface
```

```
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
```

POSTROUTING par default IP public
du reseau

```
# EMP must be able to access Internet
```

```
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 80 -j ACCEPT
```

```
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 443 -j ACCEPT
```

les utilisateurs peuvent accéder internet

```
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 80  
-m state --state NEW, ESTABLISHED -j ACCEPT
```

HTTP

ne spécifie pas IP dest car
n'importe où

```
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 443  
-m state --state NEW, ESTABLISHED -j ACCEPT
```

HTTPS

IP dynamique => MASQUERADE

SNAT et DNAT marche juste si
l'adresse IP est statique
ex serveur toujours même IP



Exercice de réseau

- Question 5 : Corriger et mettre à jour la configuration du pare-feu conformément à l'architecture retenue et à la politique de filtrage

PAT : translation d'adresse IP avec port

```
# employé peuvent accéder serveurs DMZ
iptables -A FORWARD -i $INTIF -o $DMZIF - -s $EMP_HOST - -dport 80 -m state
          - -state NEW, ESTABLISHED -j ACCEPT

iptables -A FORWARD -i $INTIF -o $DMZIF - -s $EMP_HOST - -dport 21 -m state
          - -state NEW, ESTABLISHED -j ACCEPT

iptables -A FORWARD -i $INTIF -o $DMZIF - -s $EMP_HOST - -dport 53 -m state
          - -state NEW, RELATED -j ACCEPT
```



Exercice de réseau

- Question 6 : Que devient la règle de la politique :
 - Les serveurs de la DMZ ne peuvent pas initier de sessions avec les employés EMP mais seulement répondre à leur requête

```
iptables -A FORWARD -i $DMZIF -o $INTIF -m state  
        - -state NEW -j DROP
```

si politique ouvert par défaut

INF4420a: Sécurité Informatique

Sécurité Réseau 2



Exercices de sécurité réseau

- Exercice 1 : Conception d'une architecture de sécurité
- Objectif :
 - Comprendre les risques pour la sécurité réseau
 - Savoir concevoir une architecture de sécurité permettant d'y faire face



Exercices de sécurité réseau

- Exercice 1 : Conception d'une architecture de sécurité
 - Une entreprise vient de créer sa filiale à Montréal
 - Vous venez d'être embauché comme administrateur de sécurité de cette filiale
 - Vous devez proposer une architecture de sécurité pour le réseau informatique de cette entreprise



Exercices de sécurité réseau

- Cahier des charges (partie 1)
 - L'entreprise fournit un site WEB de e-commerce
 - Afin de fonctionner, l'entreprise possède également des serveurs internes (comptabilité, wiki, etc.)

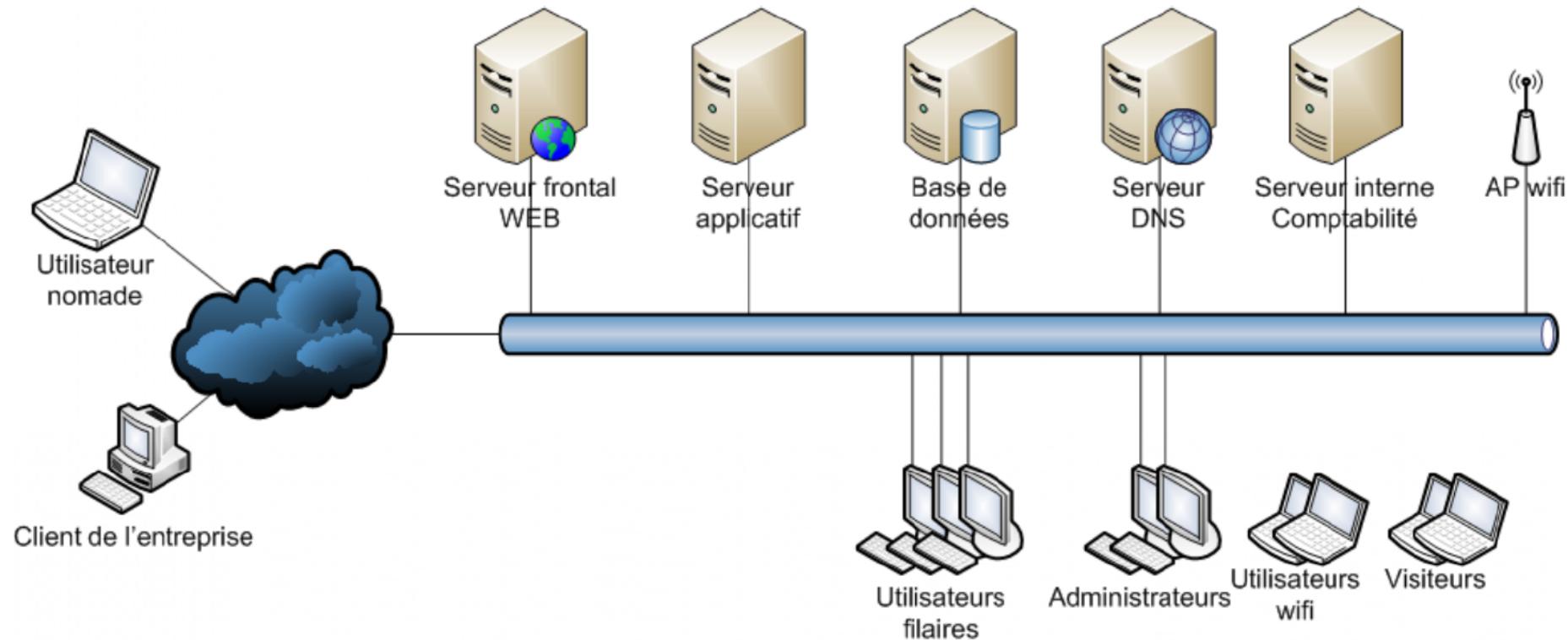
Exercices de sécurité réseau

- Cahier des charges (partie 2)
 - Certains employés se connectent sur le **réseau local filaire**, d'autres se connectent en **wifi**
 - Certains employés sont **nomades** et doivent pouvoir se **connecter à distance**
 - Il existe deux catégories principales d'utilisateurs : les **utilisateurs « standard »** et les **administrateurs du S.I.**
 - L'entreprise souhaite permettre à ses **visiteurs** de se connecter en **wifi** afin de naviguer sur internet



Exercices de sécurité réseau

- Réseau « à plat » de l'entreprise avant sécurisation





Exercices de sécurité réseau

- Vous devez donc proposer une architecture de sécurité pour ce réseau
- Vous allez procéder par étape
- Note :
 - Il existe plusieurs façons d'améliorer la sécurité de ce réseau
 - Nous présentons ici les grandes lignes
 - Cet exercice n'est pas exhaustif
 - Ce n'est pas non plus la seule solution possible



Exercices de sécurité réseau

- Faiblesse 1
 - Le réseau est directement connecté à Internet
- Conséquence 1
 - Tous les systèmes et utilisateurs et systèmes peuvent communiquer avec l'extérieur
 - Attention aux fuites de données
- Conséquence 2
 - Tout Internet peut se connecter sur notre réseau interne
 - Attention aux attaques



Exercices de sécurité réseau

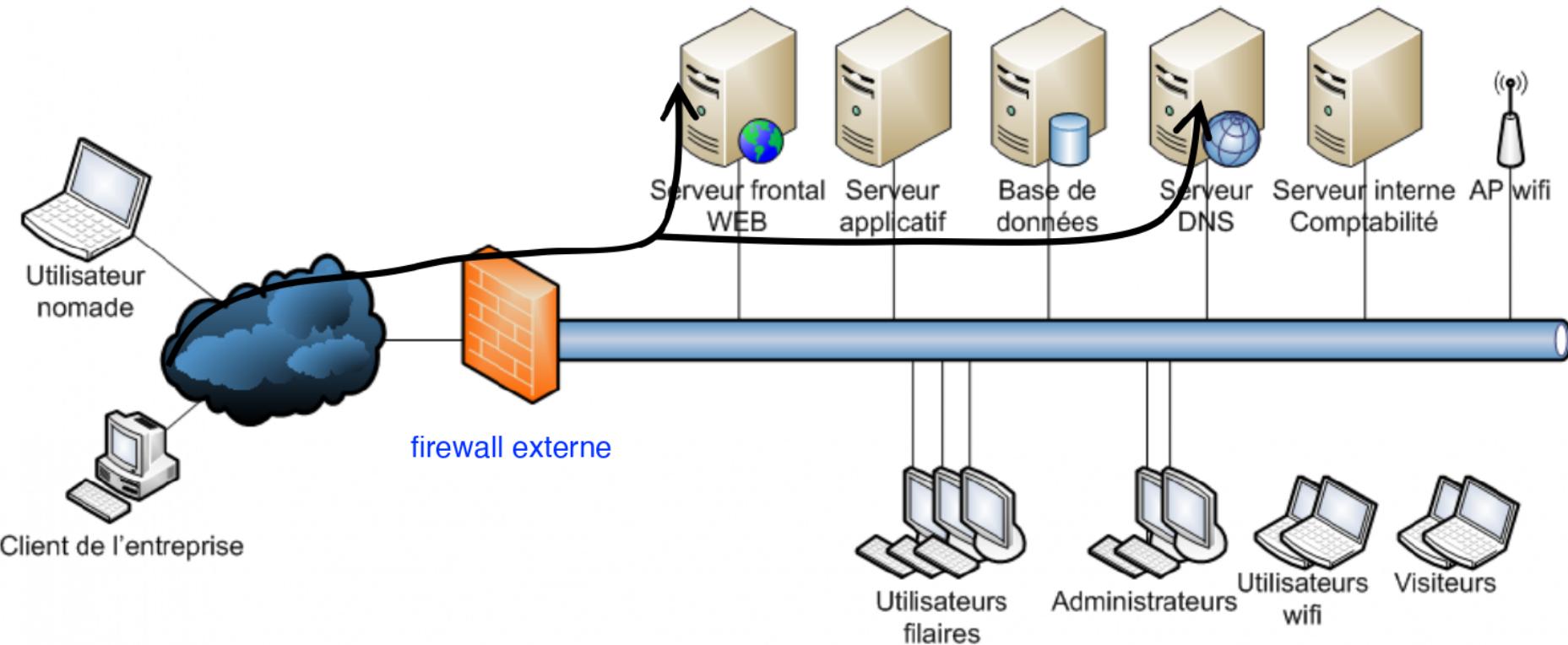
- Question 1 : Comment procédez-vous pour corriger la faiblesse 1 ?

Rajouter un firewall externe



Exercices de sécurité réseau

- Réseau « à plat » de l'entreprise avec un pare-feu en frontal





Exercices de sécurité réseau

- Le pare-feu en frontal empêche la connexion directe entre internet et le réseau interne, mais :
- Faiblesse 2
 - Au cas où le serveur WEB présente une vulnérabilité, un hacker présent sur Internet peut potentiellement prendre la main sur ce serveur
 - Il pourra ensuite rebondir sur le réseau interne



Exercices de sécurité réseau

- Question 2 : Comment procédez-vous pour corriger la faiblesse 2 ?

Utiliser une DMZ pour isoler les serveurs accessibles
de l'extérieur du réseau

Zone 1: DMZ

Zone 2: serveurs métiers (applicatif et bd)
serveur internes de l'entreprise

Zone 3: poste de travail filaires des utilisateurs

Zone 4: poste de travail wifi des utilisateurs

Zone 5: poste de travail wifi des visiteurs

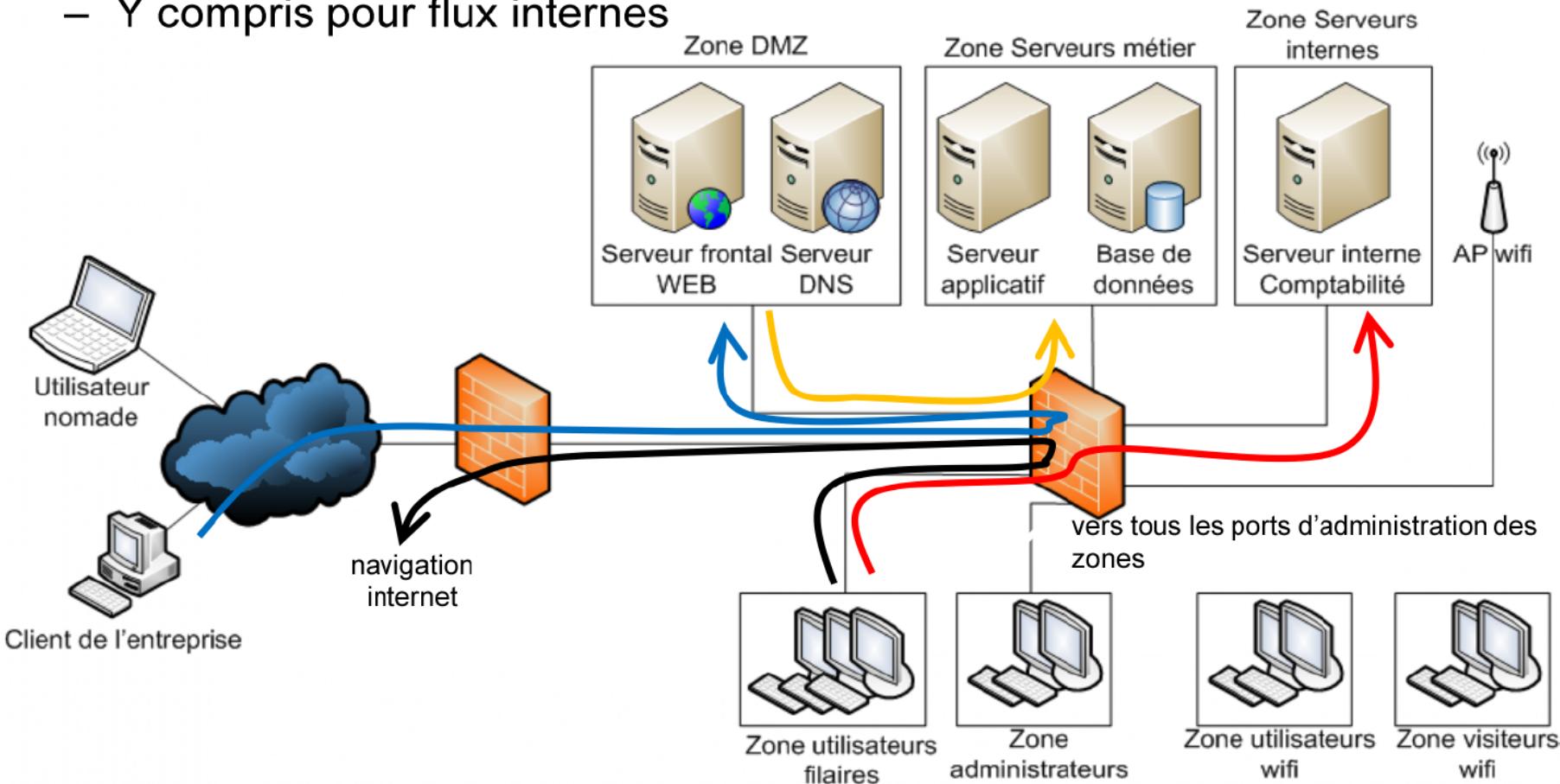
Zone 6: poste de travail des administrateurs

pare-feu externe 1 interface
pare-feu interne 6 interface



Exercices de sécurité réseau

- Réseau avec zones segmentées,
 - Filtrage systématique via le pare-feu
 - Y compris pour flux internes





Exercices de sécurité réseau

- Question 3 : Comment proposez-vous de gérer les points d'accès Wifi ?

2 populations visiteurs et employés internes

2 SSID (2 réseau distincts)

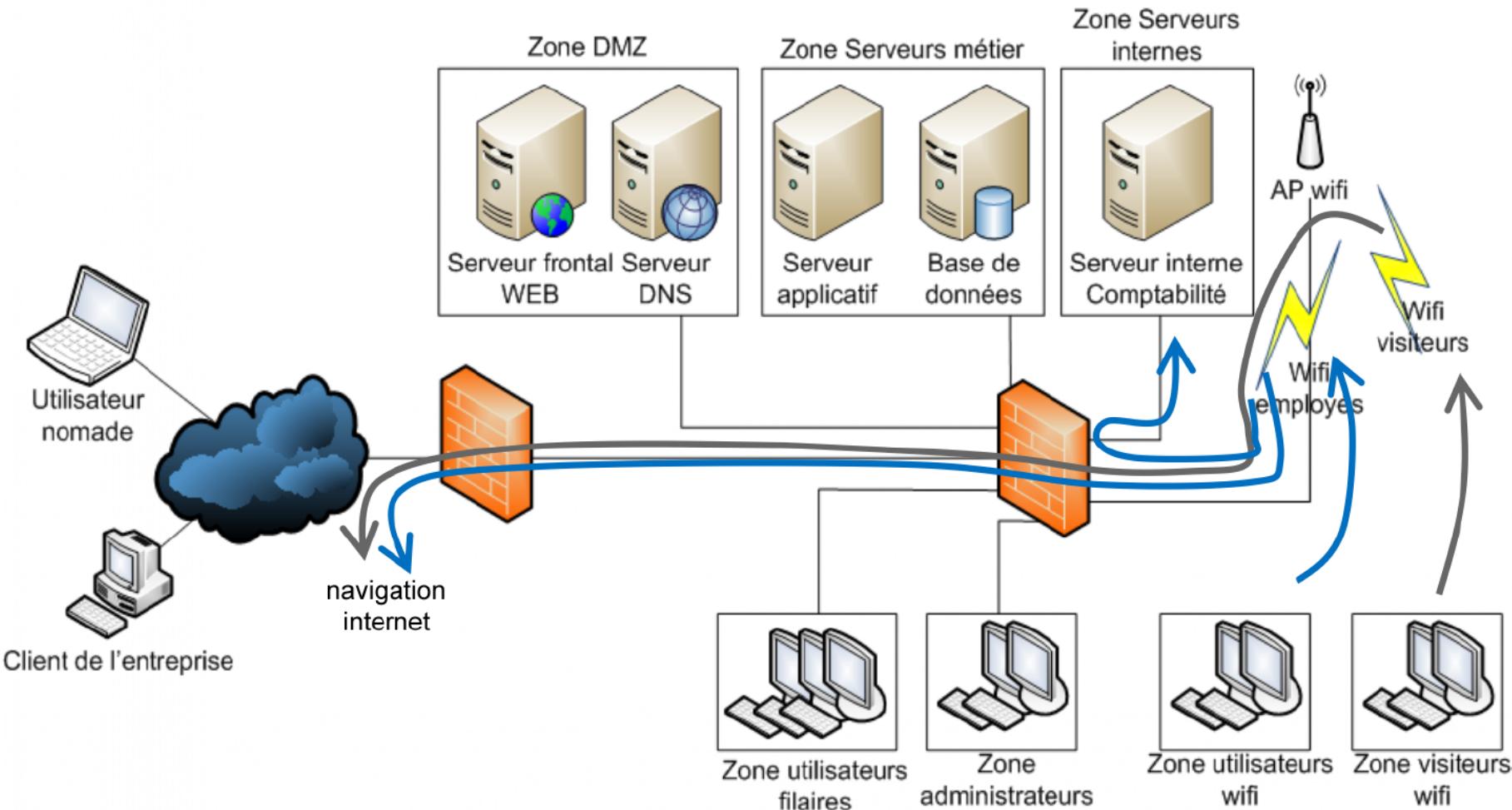
porté par le même point d'accès

pare-feu doit filtrer la charge



Exercices de sécurité réseau

- Deux réseaux wifi, dont les flux sont filtrés différemment





Exercices de sécurité réseau

- Vous devez également permettre aux utilisateurs nomades de se connecter au réseau interne depuis internet
- Question 4 : Quelle solution proposez vous pour gérer les accès des utilisateurs nomades ?

tunnel VPN permet utilisateurs nomades de se connecter

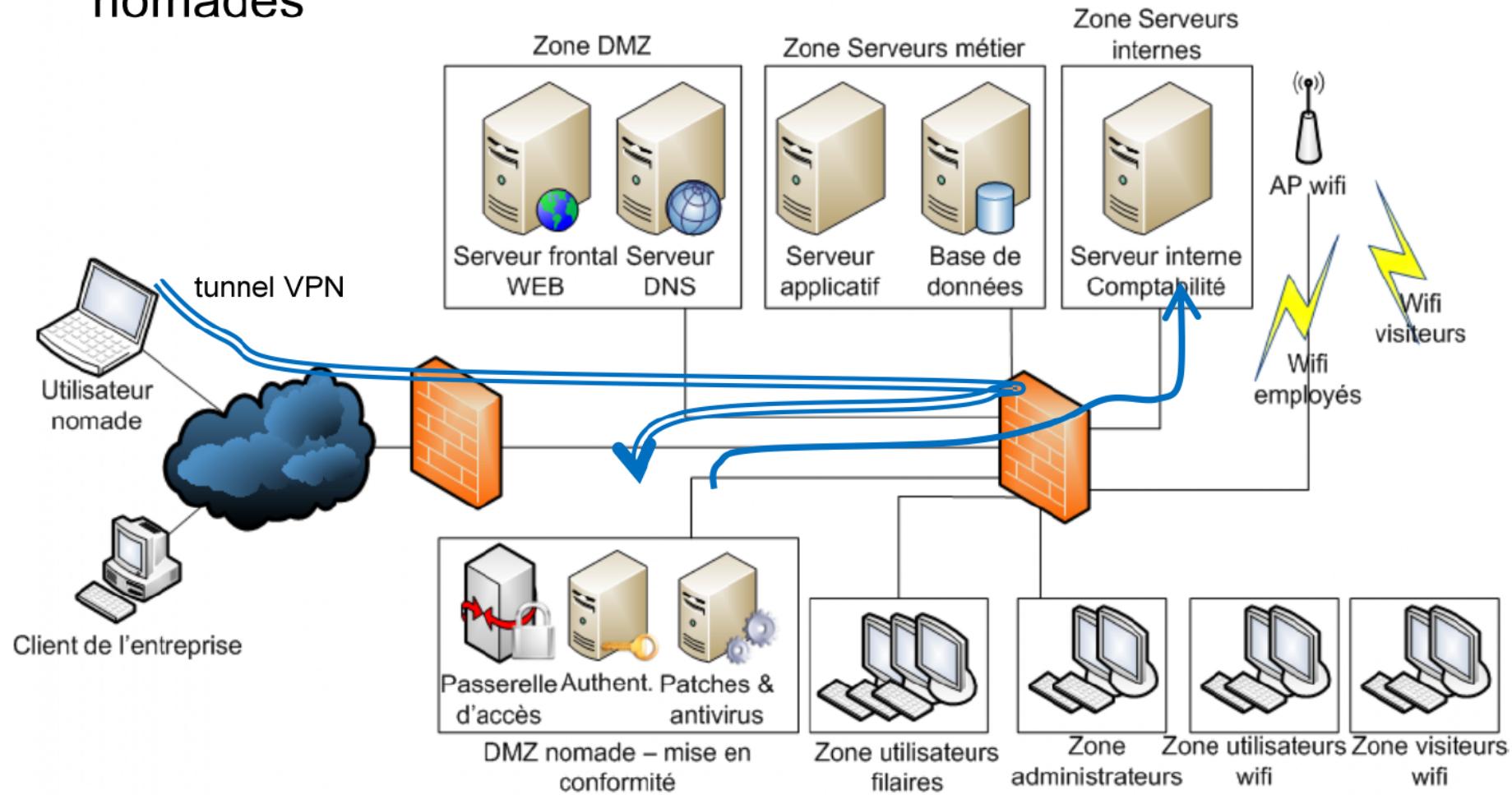
serveurs de mise en conformité vont venir voir pc employé si virus, à jour, actif.
tout est conforme selon la politique de sécurité de l'entreprise

creation DMZ spécifique
(zone de mise en conformité)
vérifier poste nomade et utilisateur sont habilités pour se connecter à distance
vérifier niveau de sécurité du poste avant d'autoriser la connection
si tout ok autoriser les flux vers zone internes toujours passant par pare-feu



Exercices de sécurité réseau

- Tunnel VPN avec DMZ de mise en conformité pour les postes nomades





Exercices de sécurité réseau

- Enfin, il reste à filtrer le trafic WEB entrant et sortant
- Question 5 : Quelle solution proposez-vous pour filtrer les connexions des usagers internes lorsqu'ils naviguent sur Internet ?

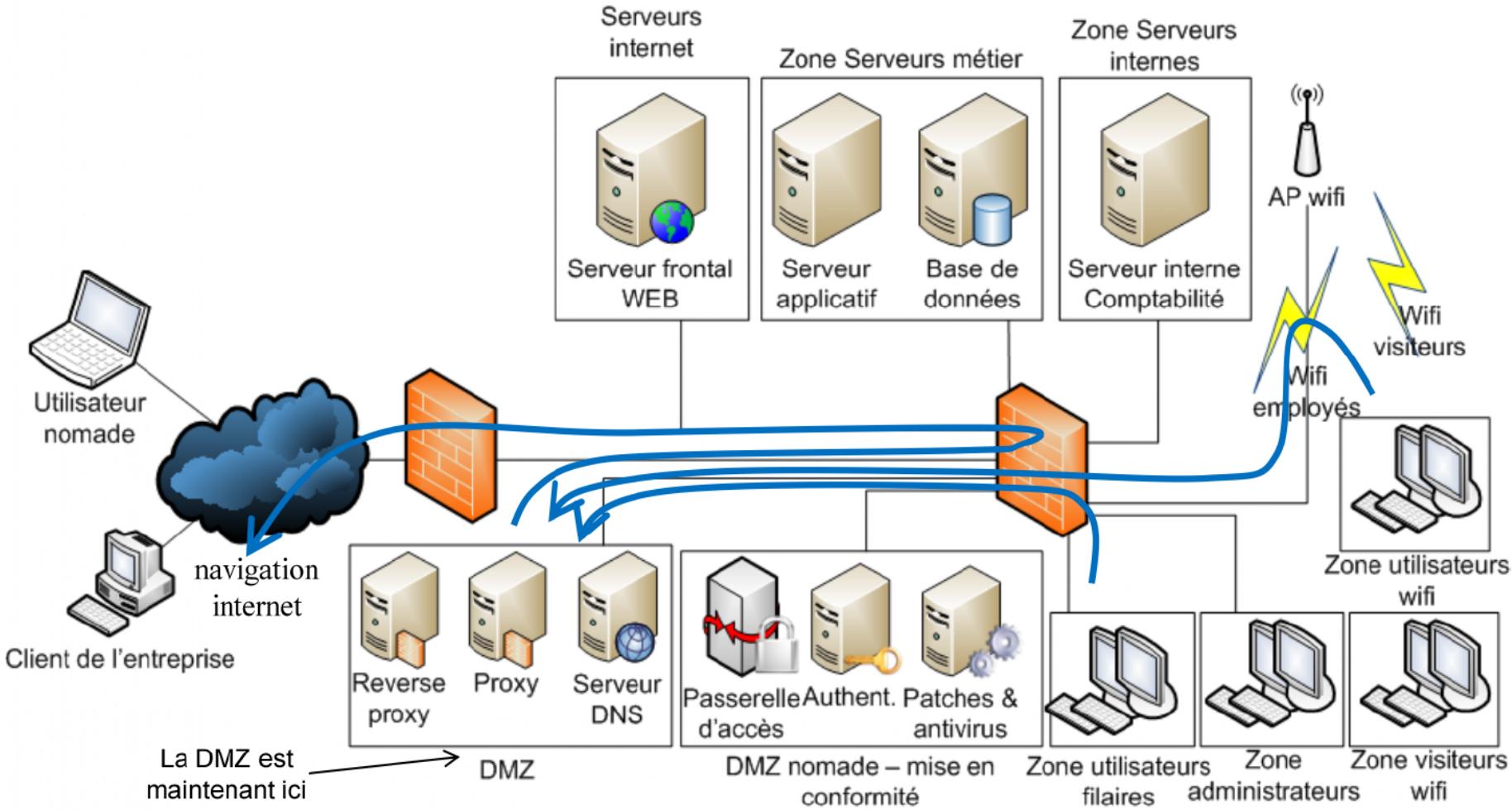
ajoute un proxy en frontal d'internet, placé dans DMZ, postes ne sont plus connectés directement à internet

définition de politique de filtrage des flux sortant catégories sites WEB employés ont droit de naviguer liste blanche ou noir des sites autorisé ou interdit



Exercices de sécurité réseau

- Réseau avec un proxy en coupure des flux vers Internet





Exercices de sécurité réseau

- Question 6 : Quelle solution proposez-vous pour filtrer les flux entrants ?

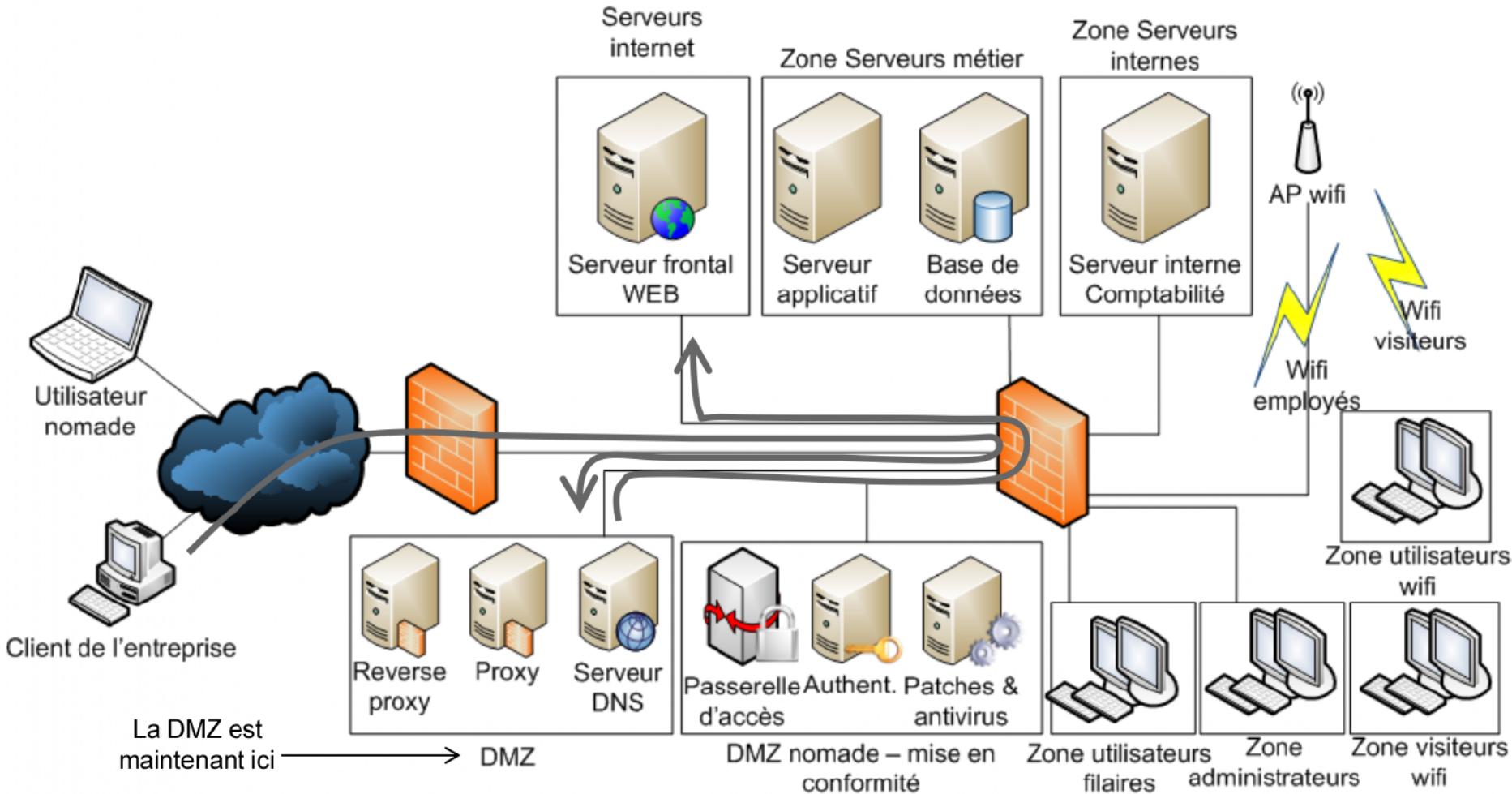
ajout d'un reverse proxy en frontal, serveur WEB
n'est plus connecté directement sur internet

politique de filtrage des flux entrants
analyse req WEB vers serveur e-commerce
blocage des requêtes non autorisées
deep packet inspection intercepter req malveillantes
SQL injection, malware, etc.



Exercices de sécurité réseau

- Réseau avec un reverse-proxy en coupure des flux entrants



A la semaine prochaine



INF4420: Éléments de Sécurité Informatique

Exercices : Sécurité des réseaux - Partie 3



Exercices de sécurité réseau

- Exercice 1 : Positionner un système de détection d'intrusion dans une architecture réseau
- Objectif :
 - Comprendre les flux dans une architecture réseau
 - Savoir positionner un système de détection d'intrusion en fonction du scénario considéré

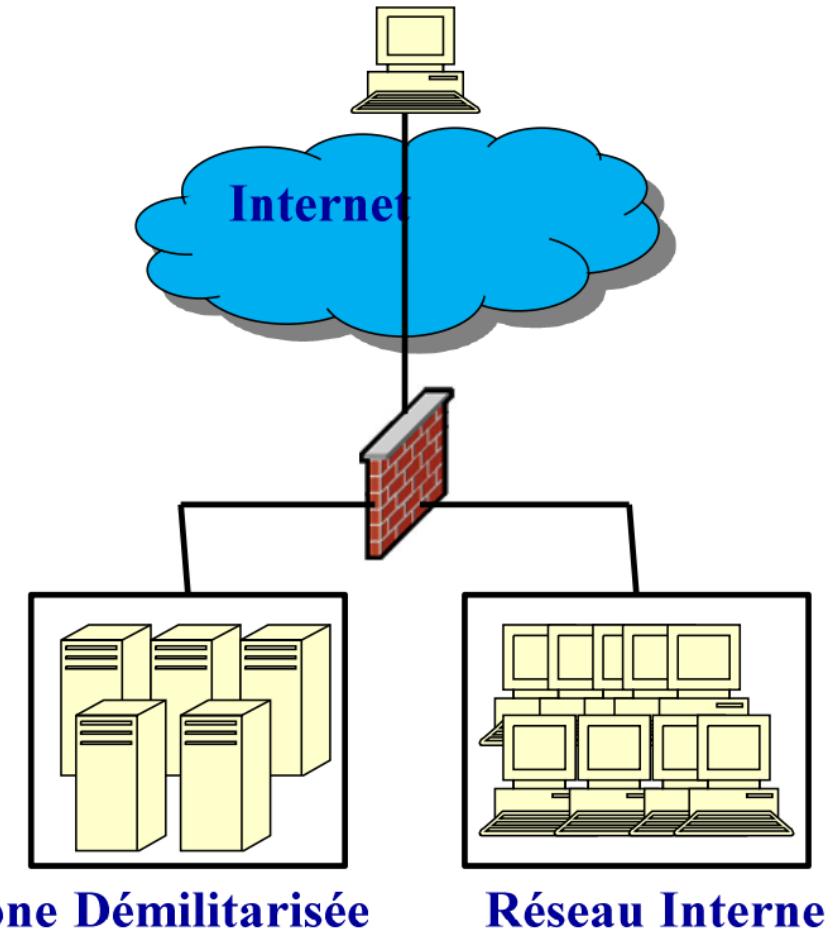
Exercices de sécurité réseau

- Exercice 1 : Positionner un système de détection d'intrusion dans une architecture réseau
- Vous avez présenté votre projet d'architecture réseau
- Le projet a été accepté par votre direction
- Vous décidez maintenant de renforcer la sécurité de votre système en intégrant un système de détection d'intrusion
- Vous considérez plusieurs scénarios



Exercices de sécurité réseau

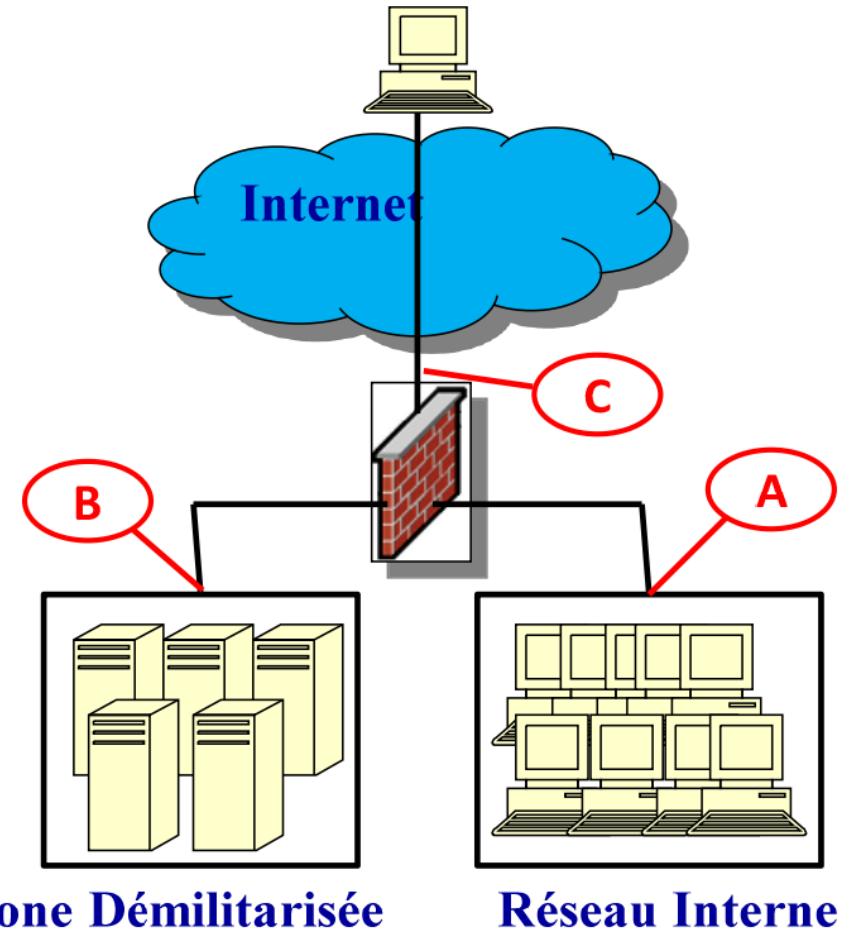
- Version simplifiée de votre architecture de sécurité





Exercices de sécurité réseau

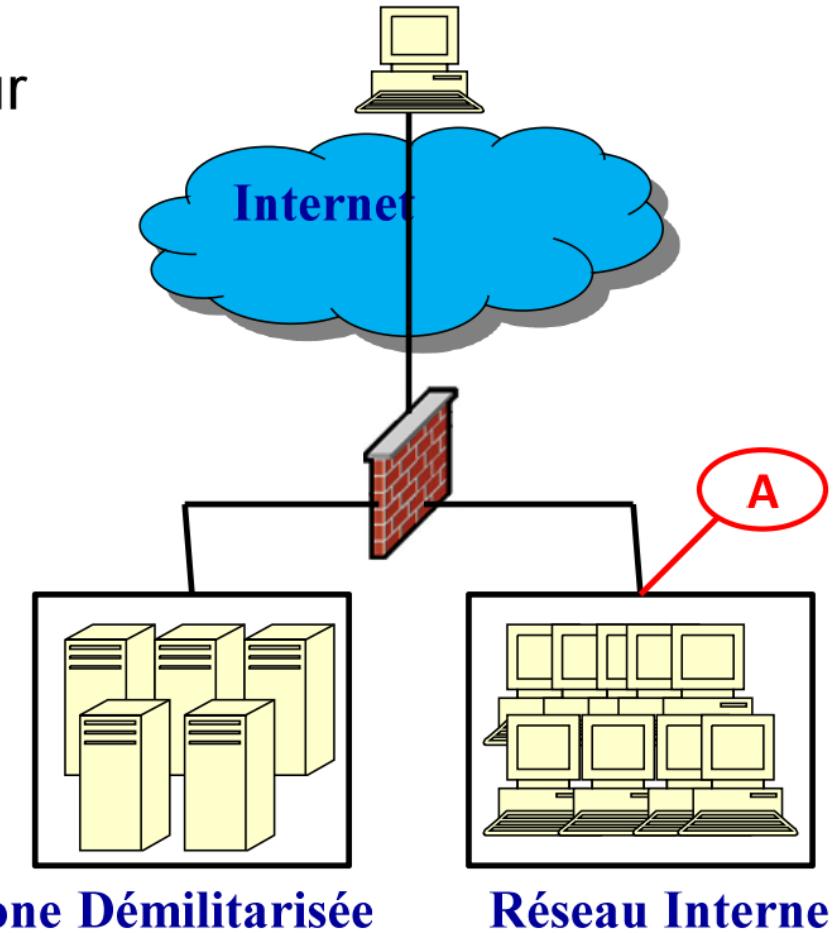
- Scénario 1 : Vous voulez détecter les attaques d'employés mécontents
- Question 1 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?





Exercices de sécurité réseau

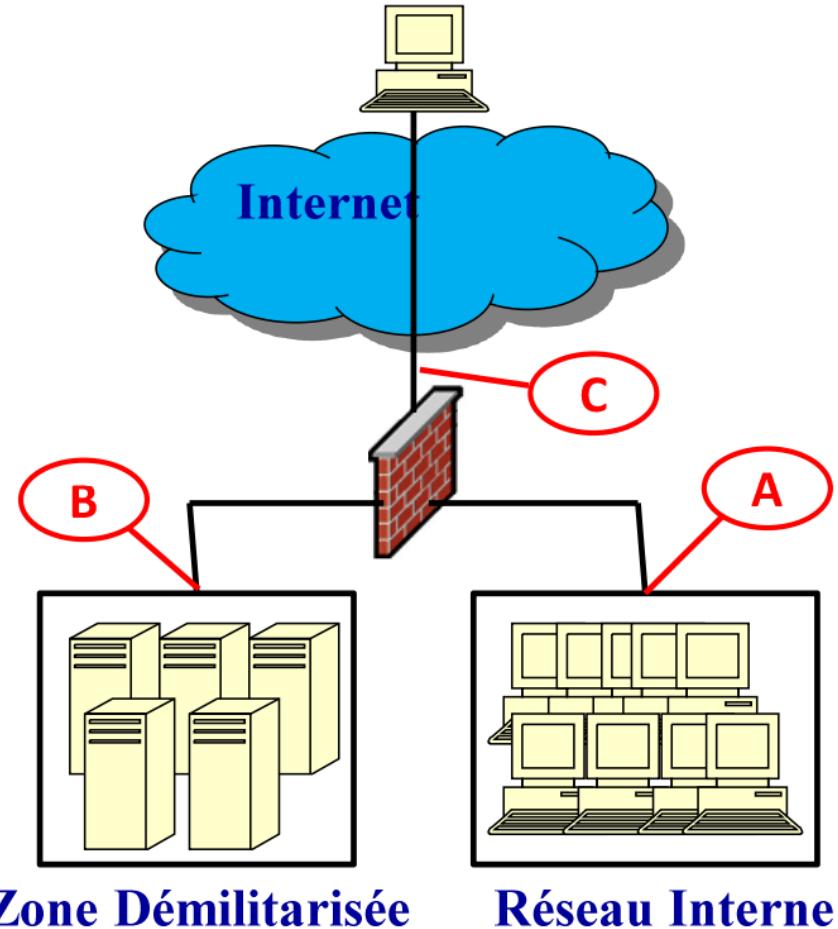
- Réponse question 1 : A, pour intercepter le réseau interne





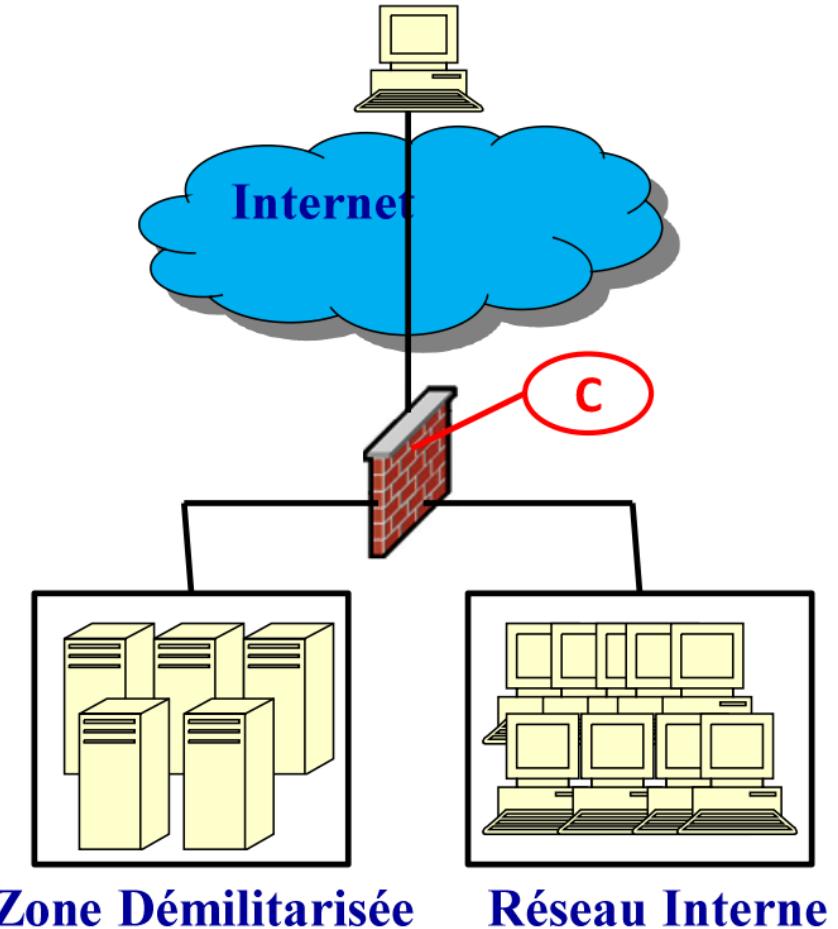
Exercices de sécurité réseau

- Scénario 2 : Vous voulez obtenir de l'information sur le type d'attaque qui vous cible
- Question 2 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?



Exercices de sécurité réseau

- Réponse question 2 : C,
pour intercepter toutes les
attaques venant d'Internet



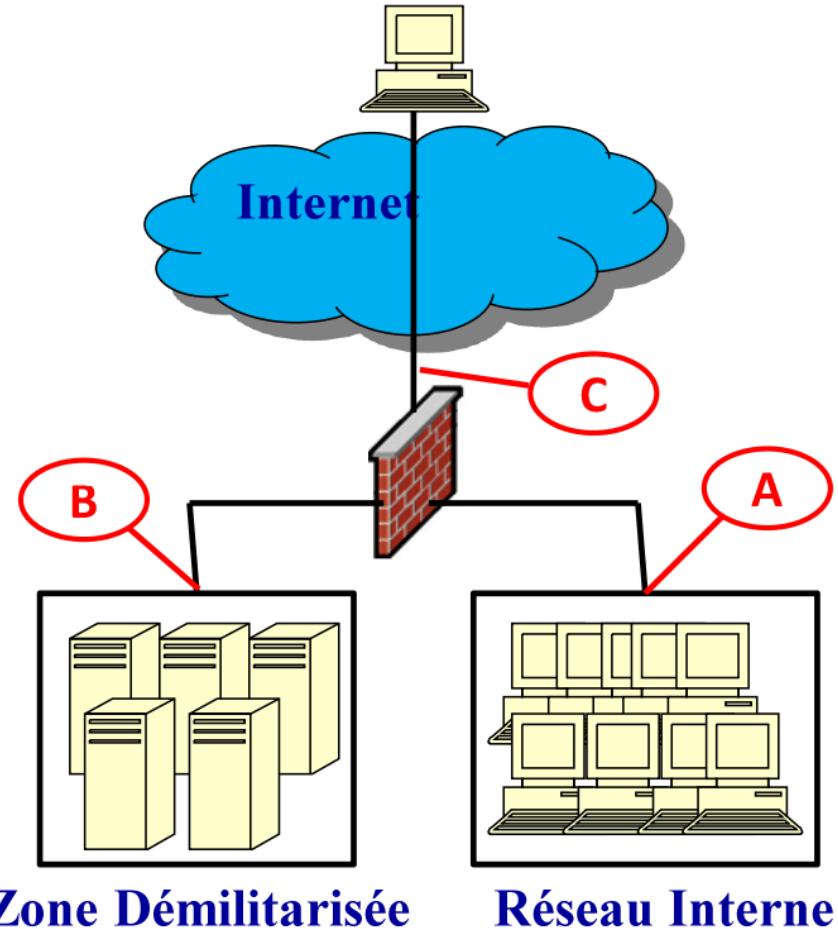
Zone Démilitarisée

Réseau Interne



Exercices de sécurité réseau

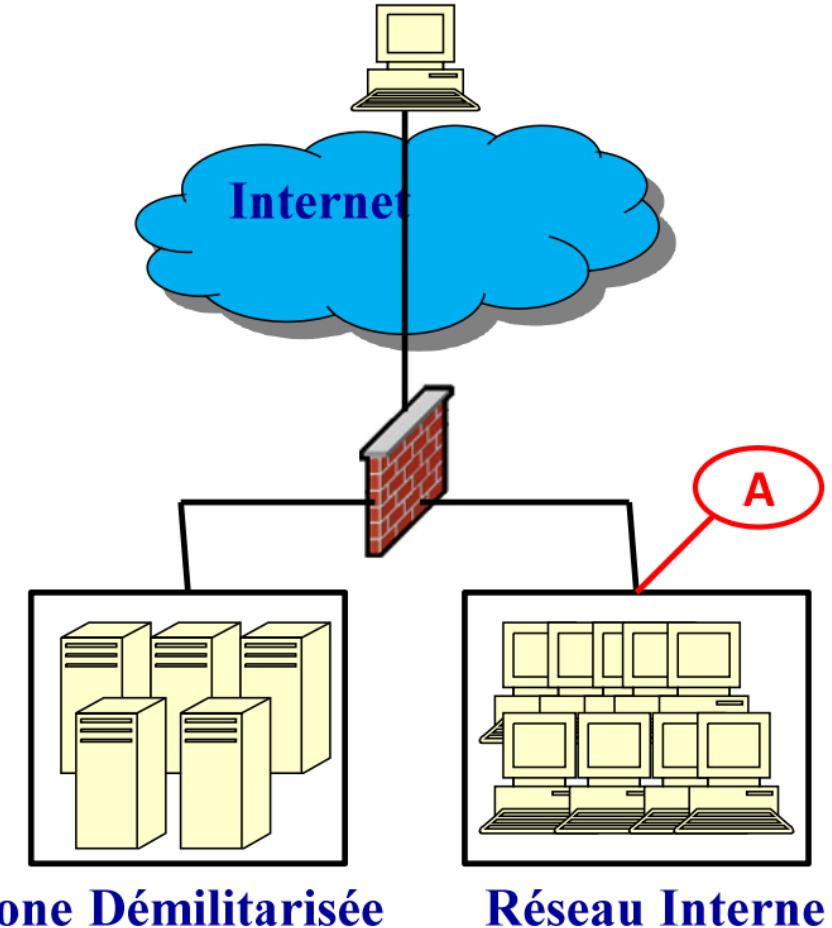
- Scénario 3 : Vous voulez détecter les attaques de type cheval de Troie
- Question 3 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?





Exercices de sécurité réseau

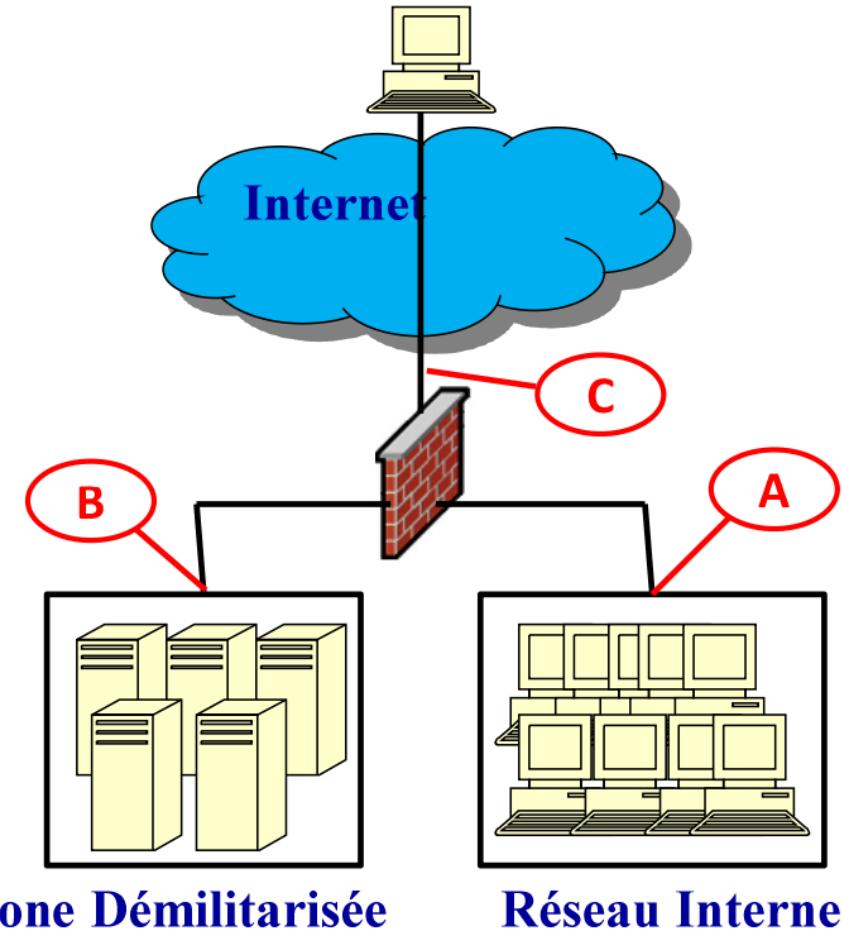
- Réponse question 3 : A,
pour intercepter le réseau
interne
- Convient pour détecter si
une machine du réseau
interne a été corrompue





Exercices de sécurité réseau

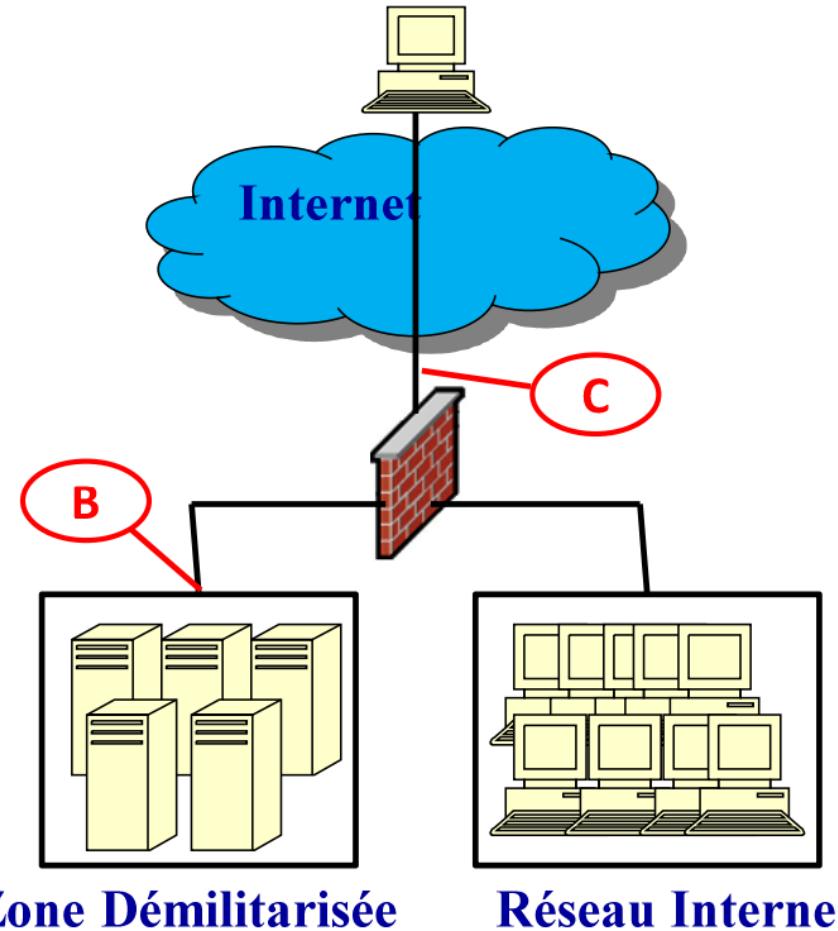
- Scénario 4 : Vous voulez obtenir de l'information sur le type d'attaque qui pénètre votre pare-feu
- Question 4 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?





Exercices de sécurité réseau

- Réponse question 4 : B (ou A) et C, pour voir la différence entre les alarmes externes et internes

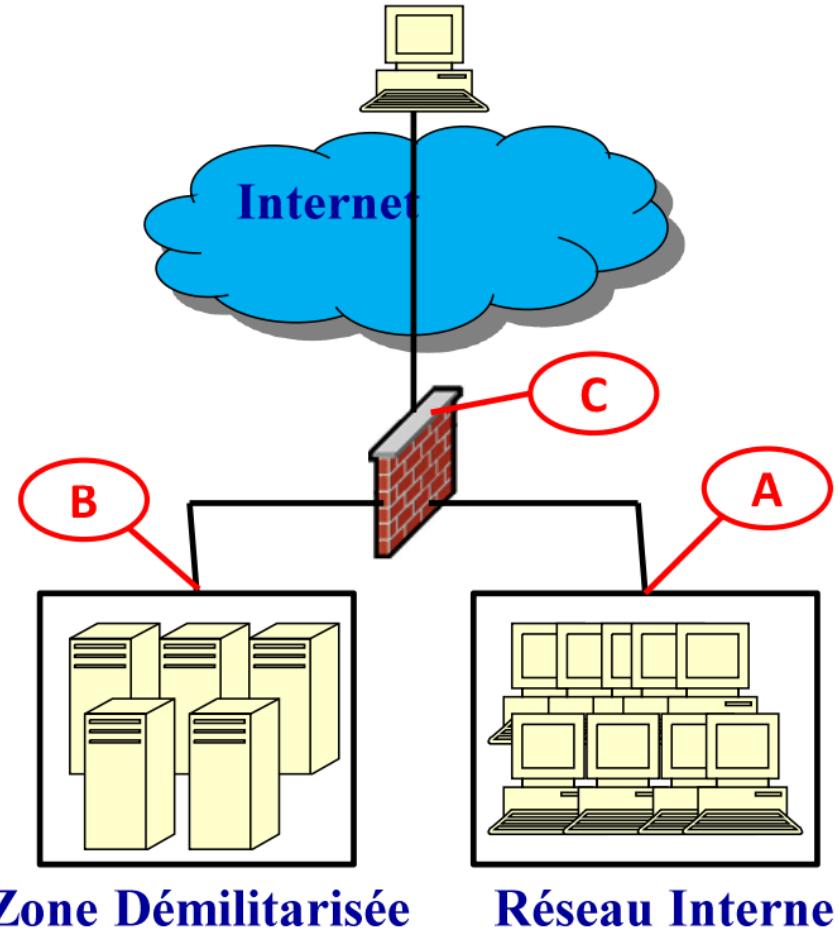


Zone Démilitarisée

Réseau Interne

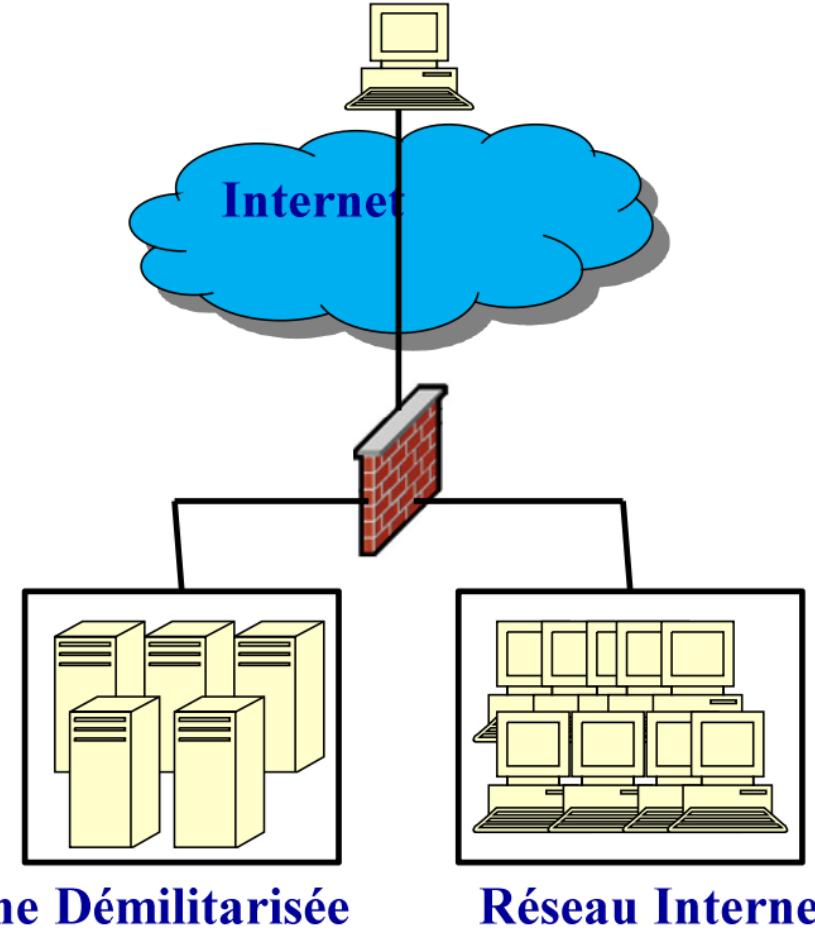
Exercices de sécurité réseau

- Scénario 5 : Vous voulez détecter les attaques sur votre serveur Web (VPN SSL)
- Question 5 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?



Exercices de sécurité réseau

- Réponse question 5 : IDS hôte sur le serveur, le trafic SSL est chiffré jusqu'au serveur !



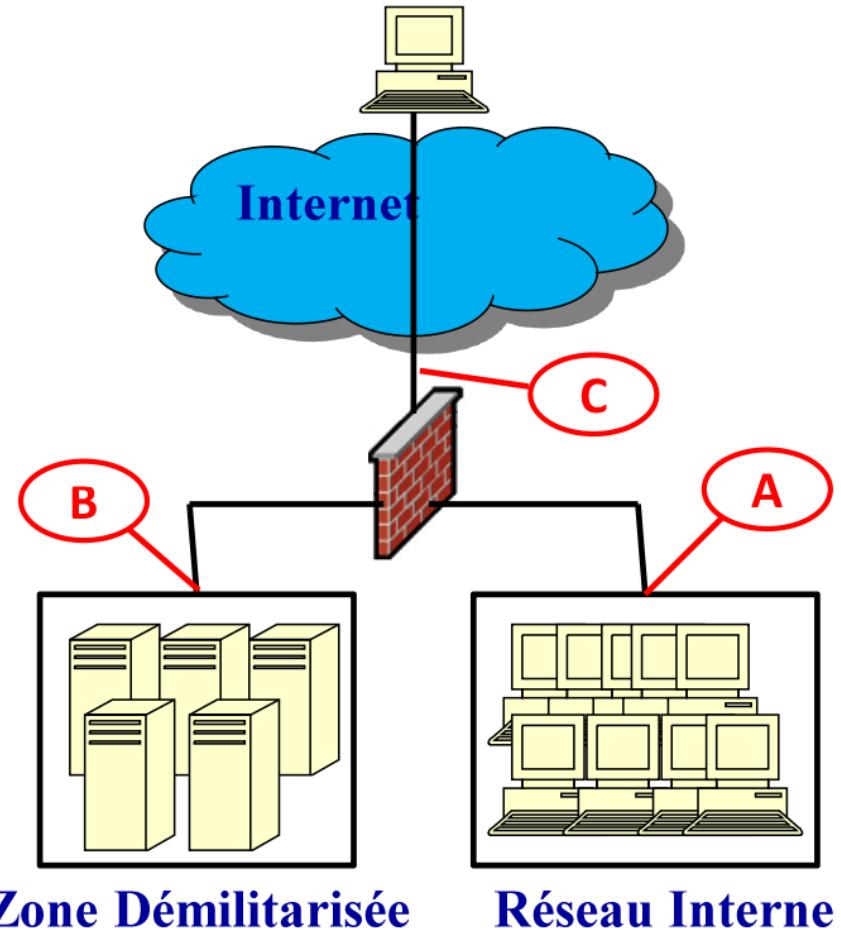
Zone Démilitarisée

Réseau Interne



Exercices de sécurité réseau

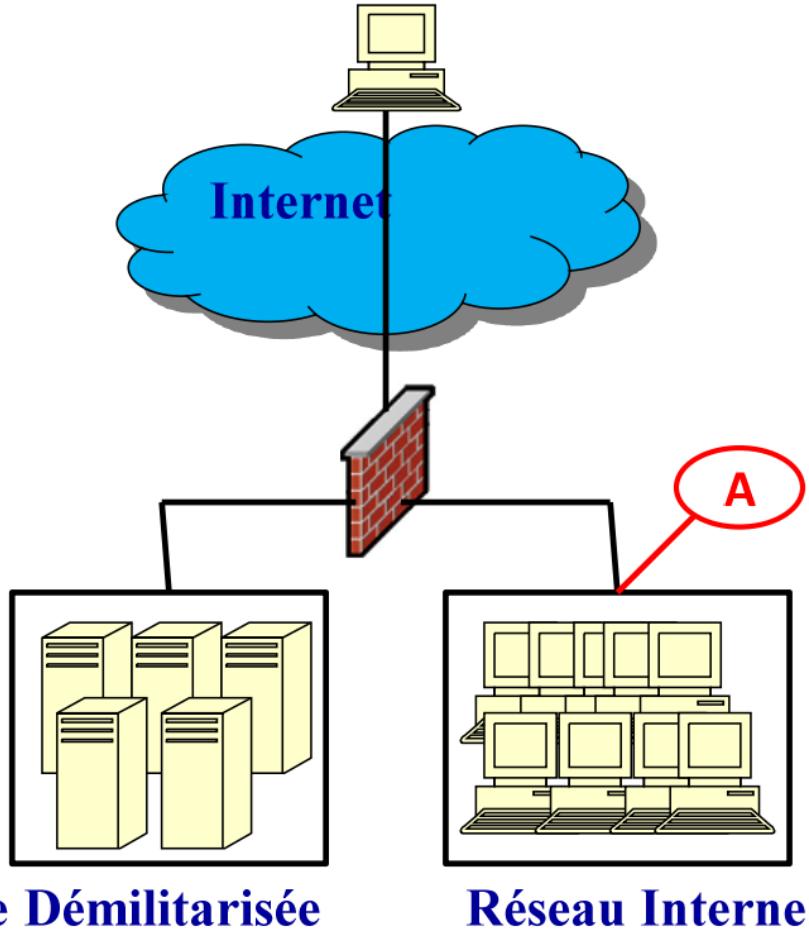
- Scénario 6 : Vous voulez détecter les attaques provenant du VPN IPSec (tunnel entre réseaux)
- Question 6 : Comment positionnez-vous votre IDS
 - A ?
 - B ?
 - C ?
 - Autre solution ?





Exercices de sécurité réseau

- Réponse question 6 : A,
le trafic VPN IPSec est
chiffré jusqu'à l'interne





Exercices de sécurité réseau

- Exercice 2 : VPN SSL et IPsec

- Objectif :
 - Comprendre les différences entre un VPN SSL et un VPN IPsec
 - Savoir utiliser les solutions de VPN SSL et de VPN IPsec à bon escient



Exercices de sécurité réseau

- Exercice 2 : VPN SSL et IPSec

- Question 1 : Au-dessus de quelle couche un VPN SSL est-il déployé ?
 - Couche 3
 - Couche 4
 - Couche 7

Exercices de sécurité réseau

- Réponse question 1 : Couche 4
- Un VPN SSL intègre le protocole TLS (Transport Layer Security) qui est déployé et construit au-dessus de la couche 4 (transport)
- Un VPN SSL permet d'assurer la sécurité de protocoles de la couche 7 (application) comme le protocole HTTP
- Un VPN IPSec est déployé au-dessus de la couche 3 (réseau)

When encryption is applied at a lower layer, all higher layer embedded data is encrypted as well. This means that not only is the data being transmitted over the network encrypted, but also any headers, trailers, or other information embedded in the data at higher layers. This provides a more comprehensive security approach compared to encryption at a higher layer, which may leave some lower layer information unencrypted and vulnerable to attacks.



Exercices de sécurité réseau

- Question 2 : La création d'un VPN IPSec nécessite une configuration préalable des deux extrémités du tunnel
 - Vrai
 - Faux

Exercices de sécurité réseau

- Réponse question 2 : La réponse est vrai
- Pour créer un VPN IPSec, il faut installer un client IPSec aux deux extrémités du tunnel
- Un VPN SSL est « transparent » pour le client
 - Le protocole SSL-TLS est intégré par défaut dans les navigateurs
 - Il n'est pas nécessaire de faire une installation côté client
 - Seul le serveur doit être préalablement configuré
- Remarque :
 - Le projet CISCO AnyConnect permet de déployer un client lourd compatible avec un VPN SSL et un VPN IPSec

Exercices de sécurité réseau

- La technologie de NAT Traversal a été développée pour permettre de traverser les passerelles qui applique la translation d'adresse (NAT)
 - NAT Traversal applique IPSec direct sur NAT à la place de appareil client
 - Ajoute un UDP header pour que l'encryption ne change pas le IP source et dest
- Question 3 : Pour quel type de VPN le NAT Traversal a été plus particulièrement conçu ?
 - IPSec en mode transport
 - IPSec en mode tunnel
 - SSL-TLS



Exercices de sécurité réseau

- Réponse question 3 : VPN IPSec en mode transport
- Il existe deux types de VPN IPSec
 1. IPSec en mode Tunnel
 2. IPSec en mode transport



Exercices de sécurité réseau

- Réponse question 3 (explication) :
- IPSec en mode tunnel
 - En mode tunnel, la totalité du paquet IP est chiffrée
 - Le paquet est encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP
 - Ce mode est compatible avec le NAT
 - Utilisation de IPSec en mode tunnel
 - VPN de réseau à réseau (c.a.d. entre deux sites distants)
 - VPN de hôte à réseau (accès à distance d'un utilisateur)
 - VPN de hôte à hôte (messagerie privée)

Tunnel mode is used to provide security to communication between two networks. In tunnel mode, both the IP header and the payload are encrypted. The original source and destination IP addresses are hidden, and new IP headers are added to the packet, with the new source and destination IP addresses representing the tunnel endpoints. This means that the entire packet is encapsulated within another packet, and the tunnel endpoints are the only visible IP addresses to the outside network.

Exercices de sécurité réseau

- Réponse question 3 (explication) :
- IPSec en mode transport
 - Dans ce mode, seule la payload du paquet IP est chiffrée
 - Le reste du paquet IP est inchangé
 - Le routage des paquets n'est donc pas modifié
 - Mais, IPSec intègre le protocole AH (Authentication Header) qui calcule un hash du paquet
 - On ne peut pas faire du NAT car le hash ne sera plus correct
 - Le NAT-Traversal permet de résoudre ce problème
 - Utilisation de IPSec en mode tunnel
 - VPN de hôte à hôte

Transport mode is used to provide security to end-to-end communication between two hosts. In transport mode, only the payload (the data being sent) is encrypted while the IP header remains untouched. The original source and destination IP addresses remain intact, which means that the hosts can directly communicate with each other.



Exercices de sécurité réseau

- Réponse question 3 :
- SSL-TLS
 - Un VPN SSL-TLS est construit au-dessus de la couche transport
 - Pas de problème de NAT, ni de PAT

Exercices de sécurité réseau

- Question 4 : On faire passer n'importe quel protocole de la couche 7 dans un VPN SSL
 - Vrai
 - Faux

Exercices de sécurité réseau

- Réponse question 4 : La réponse est faux
- Il est nécessaire de développer une version « over SSL-TSL » d'un protocole applicatif pour qu'il puisse être encapsulé dans un VPN SSL au dessus de couche 4
- En revanche, il est possible d'encapsuler n'importe quel protocole dans un VPN IPSec au dessus de couche 3

Exercices de sécurité réseau

- Réponse question 4 (suite) :
- Exemple de protocole « over SSL-TLS »
 - HTTP, FTP, Telnet, LDAP, NTTP
 - SMTP, IMAP, POP
 - DNS (ne pas confondre avec DNSSEC)
- Un protocole « over SSL-TLS » se voit attribuer un numéro de port spécifique
 - Par exemple, le port 443 pour HTTPS
 - Pour la couche réseau, c'est un protocole « normal »
 - Pas de problème de NAT ni de PAT

Exercices de sécurité réseau

- Question 5 : Dans un VPN SSL, le client et le serveur sont authentifiés
 - Vrai
 - Faux

AH provides integrity, authentication for entire IP packet, including the IP header, and is inserted between the IP header and the upper-level protocol (e.g. TCP, UDP) in the packet. It uses a keyed hash function to compute a message digest for the packet, which is then inserted into the AH header along with other security parameters.

When a packet is received, the AH header is checked to ensure that the packet has not been modified in transit, and the authentication data in the header is used to verify the packet's authenticity. If the packet is not authentic, it is discarded.

ESP provides confidentiality by encrypting the payload of IP packets, integrity by generating a message authentication code (MAC) for the encrypted payload and some header fields, and authenticity by using an integrity check value (ICV) to detect any changes to the packet during transmission.

Exercices de sécurité réseau

- Réponse question 5 : La réponse est faux
- Avec SSL, le client n'est en général pas authentifié
 - Le serveur peut demander au client de fournir son certificat mais c'est optionnel
 - Risque d'attaque man in the middle
- Avec SSL, le serveur est authentifié
 - Sauf si l'autorité de certification s'est fait voler son certificat
- Pour IPSEC, deux protocoles différents sont utilisés :
 - AH (Authentication Header) : authentification et intégrité
 - ESP (Encapsulating Security Payload) : confidentialité



Exercices de sécurité réseau

- Question 6 : Dans quel cas un VPN nécessite une autorité de certification pour être déployé
 - VPN SSL
 - VPN IPSec
 - Les deux mon capitaine

Exercices de sécurité réseau

- Réponse question 6 : Les deux mon capitaine
- Cas d'un VPN SSL
 - Une autorité de certification est nécessaire pour authentifier le certificat du serveur
- Cas d'un VPN IPSec
 - Les deux extrémités doivent présenter un certificat signé par une autorité de certification
 - Mais, le protocole IKE (Internet Key Exchange) propose aussi un mode où chaque extrémité pré-partage un secret