SAÉ 201 Rapport

Dans ce rapport vous trouverez une proposition d'infrastructure que nous allons déployer pour une entreprise dans son nouveau siège. L'infrastructure sera composée d'une Zone démilitarisée (DMZ) qui héberge les serveurs publics de l'entreprise; il y aura un accès à internet et nous mettrons en place des règles de sécurité.

L'entreprise est organisée en trois services :

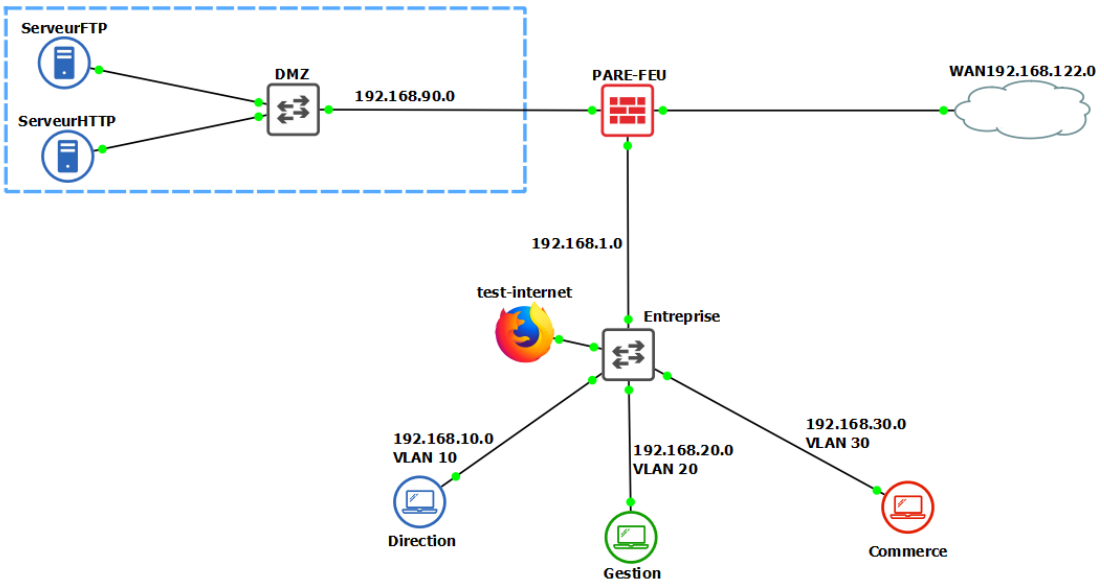
- Direction
- Gestion administrative et financière
- Commercial (agent) et technique (suivi travaux)

Cette société désire créer un réseau informatique pour travailler sur une application WEB et partager des données internes (contrats, commandes, factures, procès-verbal d'assemblée générale, etc).

SOMMAIRE :

I. Configuration des serveurs
   a. Serveur FTP
   b. Serveur HTTP
II. Configuration pare-feu
   a. Configuration des interfaces
   b. Création VLANs
III. Configuration des règles de sécurité

Toutes les configurations sont disponibles en vidéo ici.



I. Configuration des serveurs

A. Serveur FTP

SERVEUR FTP

login : ftp; mdp : user

Nous créons le serveur FTP, sans interface graphique, sur une machine virtuelle Debian (sous VirtualBox).

Il faut installer le serveur, ici nous installons proftpd ;

```
ftp@srvftp:~$ sudo apt-get install proftpd
```

Nous vérifions que le serveur écoute bien sur le port 21 (port FTP par défaut) avec la commande netstat :

```
ftp@srvftp:~$ netstat -paunt
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir toutes.)
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 2c0f:f918:302:f40:37832 2a04:4e42:29::644:80    TIME_WAIT   -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
```

Puis nous créons le groupe qui permettra les échanges de dossiers et fichiers entre chaque secteur de l'entreprise. Le nom du groupe est *ftp-users* et nous ajoutons les membres dans le groupe :

```
ftp@srvftp:~$ sudo groupadd ftp-users
```

```
ftp@srvftp:~$ sudo usermod direction -g ftp-users && sudo usermod gestion -g ftp-users && sudo userm
od commerce -g ftp-users
```

Ensuite nous créons un dossier partagé (*ftp*) dont nous donnons l'accès au groupe ftp-users :

```
ftp@srvftp:/home$ sudo mkdir ftp
ftp@srvftp:/home$ sudo chown direction:ftp-users /home/ftp/
ftp@srvftp:/home$ sudo chown gestion:ftp-users /home/ftp/
ftp@srvftp:/home$ sudo chown commerce:ftp-users /home/ftp/
ftp@srvftp:/home$ sudo chmod -R 777 /home/ftp/
```

Pour finir, dans le fichier conf de ftp, nous définissons le répertoire courant des utilisateurs :

```
DefaultChdir /home/ftp
```

B. Serveur HTTP

SERVEUR HTTP

login : http; mdp : user

Nous créons le serveur HTTPs, sans interface graphique, sur une machine virtuelle Debian (sous VirtualBox).

Il faut installer le serveur, ici nous installons apache2 :

```
http@srvhttp:~$ sudo apt-get install apache2
```

Dans le dossier /etc/apache2, nous générons un certificat auto-signé.

Explications :

- X509 est un format de certificat numérique, standardisé par l'IETF (RFC 2527)
- On génère ici un couple de clés RSA, avec une longueur de clé de 2048 bits (valeur recommandée actuellement pour RSA)
- Le certificat (qui contient la clé publique), est stocké dans le fichier server.pem : il sera transmis au client HTTPS
- La clé privée est stockée dans le fichier server.key : elle ne sera jamais transmise sur le réseau

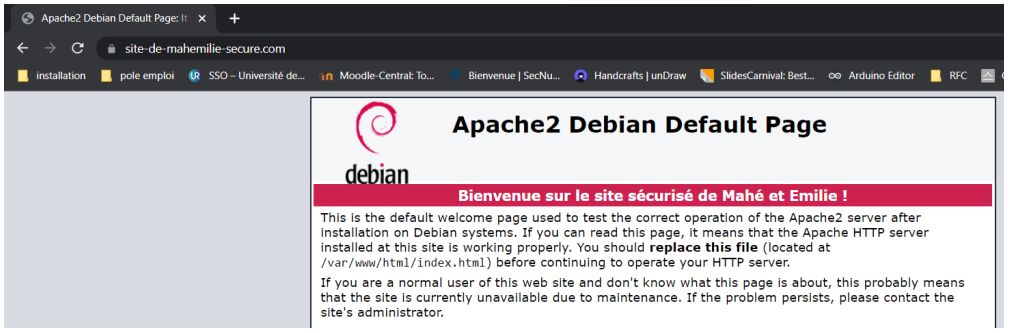
```
http@srvhttp:~$ cd /etc/apache2/
http@srvhttp:/etc/apache2$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out /etc/apache
2/server.pem -keyout /etc/apache2/server.key
```

Pour finir nous personnalisons la page d'accueil de l'interface web dans le dossier /var/www/html_ssl. Sans oublier de définir le répertoire par défaut de l'index et des clés dans le fichier conf de notre site /etc/apache2/sites-available/default-ssl.conf :

```
  GNU nano 5.4                /etc/apache2/sites-available/default-ssl.conf *
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html_ssl
                ServerName www.site-de-mahemilie-secure.com
```

```
                SSLCertificateFile      /etc/apache2/server.pem
                SSLCertificateKeyFile /etc/apache2/server.key
```



II. Configuration du Pare-feu

A. Configuration des interfaces

Nous procédons à l'installation classique de Pfsense. Après installation du pare-feu nous n'avons que deux interfaces, le WAN et le LAN.

Nous allons configurer les interfaces de notre routeur Pfsense afin qu'il donne l'accès Internet à notre DMZ et aux futures machines présentes dans l'entreprise.

Nous créons donc l'interface em2 qui sera l'interface dédiée à la DMZ et nous lui assignons l'adresse 192.168.90.1/24.

B. Créations VLANs

Nous allons créer nos VLANs directement sur Pfsense en les reliant à l'interface LAN :

```
WAN (wan)       -> em0       -> v4/DHCP4: 192.168.122.14/24
LAN (lan)       -> em1       -> v4: 192.168.1.1/24
DMZ (opt1)      -> em2       -> v4: 192.168.90.1/24
VLAN10 (opt2)   -> em1.10    -> v4: 192.168.10.1/24
VLAN20 (opt3)   -> em1.20    -> v4: 192.168.20.1/24
VLAN30 (opt4)   -> em1.30    -> v4: 192.168.30.1/24
```

Nous avons configuré nos VLANs de tel sorte qu'ils agissent en tant que serveur DHCP, afin de faire l'adressage IP de chaque machine. L'adressage des adresses IP des PCs se fait donc par DHCP. Nous devons alors configurer le switch, nommé Entreprise, en créant les VLANs et en attribuant les interfaces de la bonne machine au bon VLAN :

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gi0/0
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Création des VLANs sur le switch :

```
Switch(config)#vlan 10
Switch(config-vlan)#name direction
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name gestion
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name commerce
Switch(config-vlan)#exit
```

Accès des interfaces vers le VLAN qui le concerne (exemple sur le VLAN 10) :

```
Switch(config)#int gi0/1
Switch(config-if)#swit
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no sh
```

Résultat final :

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/2, Gi0/3, Gi1/0, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/2, Gi2/3
                                                Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   direction                        active    Gi0/1
20   gestion                          active    Gi1/1
30   commerce                         active    Gi2/1
```

L’adressage est le suivant :

SERVICE	MACHINE	IP	VLAN
direction PASSERELLE : 192.168.10.1	PC1	192.168.10.5 à 192.168.10.50	10
gestion PASSERELLE : 192.168.20.1	PC2	192.168.20.5 à 192.168.20.50	20
commerce PASSERELLE : 192.168.30.1	PC3	192.168.30.5 à 192.168.30.50	30

Ainsi quand nous allumons une machine, la requête DHCP s'active et la machine obtient une adresse qui correspond à son réseau de VLAN :

```
DORA IP 192.168.10.6/24 GW 192.168.10.1

Direction> sh

NAME    IP/MASK              GATEWAY          MAC                LPORT  RHOST:PORT
Directi192.168.10.6/24       192.168.10.1     00:50:79:66:68:00  20060  127.0.0.1:20061
        fe80::250:79ff:fe66:6800/64
```

III. Configuration des règles de sécurité

PFSENSE

id : admin; mdp : admin

Les règles de sécurité a appliqués sont les suivantes :

Autorisé	Interdit
LAN vers WAN LAN vers DMZ WAN vers DMZ	DMZ vers LAN DMZ vers WAN WAN vers LAN

Annonce des règles

WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✗	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks
✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks
✓	0 /0 B	IPv4 TCP	WAN net	*	DMZ net	*	*	none		

LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	0 /3.47 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
✓	2 /70 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

DMZ	Rules (Drag to Change Order) States Protocol Source Port Destination Port Gateway Queue Schedule Description 0 /0 B IPv4 TCP DMZ net * * * * none

Applications des règles	
PC VLAN 30 vers PC VLAN 20	DORA IP 192.168.30.6/24 GW 192.168.30.1 Commerce> ping 192.168.20.6 84 bytes from 192.168.20.6 icmp_seq=1 ttl=63 time=8.026 ms 84 bytes from 192.168.20.6 icmp_seq=2 ttl=63 time=4.351 ms 84 bytes from 192.168.20.6 icmp_seq=3 ttl=63 time=4.126 ms 84 bytes from 192.168.20.6 icmp_seq=4 ttl=63 time=4.552 ms 84 bytes from 192.168.20.6 icmp_seq=5 ttl=63 time=5.786 ms
PC vers Internet	Commerce> ping 8.8.8.8 84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=84.409 ms 84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=72.691 ms 84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=163.110 ms 84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=81.990 ms 84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=90.095 ms
LAN vers DMZ	Commerce> ping 192.168.90.12 84 bytes from 192.168.90.12 icmp_seq=1 ttl=63 time=4.765 ms 84 bytes from 192.168.90.12 icmp_seq=2 ttl=63 time=3.591 ms 84 bytes from 192.168.90.12 icmp_seq=3 ttl=63 time=3.365 ms 84 bytes from 192.168.90.12 icmp_seq=4 ttl=63 time=3.031 ms 84 bytes from 192.168.90.12 icmp_seq=5 ttl=63 time=3.994 ms
LAN vers WAN	Commerce> ping 192.168.122.14 84 bytes from 192.168.122.14 icmp_seq=1 ttl=64 time=3.371 ms 84 bytes from 192.168.122.14 icmp_seq=2 ttl=64 time=3.227 ms 84 bytes from 192.168.122.14 icmp_seq=3 ttl=64 time=2.169 ms 84 bytes from 192.168.122.14 icmp_seq=4 ttl=64 time=2.116 ms 84 bytes from 192.168.122.14 icmp_seq=5 ttl=64 time=2.863 ms
DMZ vers LAN	DMZ-test> ping 192.168.1.1 192.168.1.1 icmp_seq=1 timeout 192.168.1.1 icmp_seq=2 timeout 192.168.1.1 icmp_seq=3 timeout 192.168.1.1 icmp_seq=4 timeout 192.168.1.1 icmp_seq=5 timeout
DMZ vers WAN	DMZ-test> ping 192.168.122.14 192.168.122.14 icmp_seq=1 timeout 192.168.122.14 icmp_seq=2 timeout 192.168.122.14 icmp_seq=3 timeout 192.168.122.14 icmp_seq=4 timeout 192.168.122.14 icmp_seq=5 timeout