



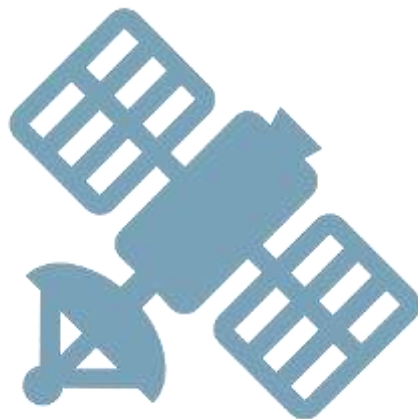
SAE2.0 I

CONSTRUIRE UN RÉSEAU INFORMATIQUE POUR UNE PETITE STRUCTURE

CALPETARD MAHÉ & CHÉLONÉ ÉMILIE



Contexte



Configurations



Tests

SOMMAIRE

CONTEXTE



La société cliente est une petite structure dans le secteur de l'immobilier. Elle est organisée en trois services :

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

Cette société immobilière 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.).

Les données de la direction, de l'administration et du service commercial technique doivent être sur des serveurs différents. Le personnel faisant partie de la direction doit pouvoir accéder aux autres serveurs de données, mais la réciproque n'est pas vraie.

Les applications WEB et FTP devront être accessibles depuis l'extérieur, mais devront être sécurisées pour le réseau interne au sein d'une DMZ

CONFIGURATIONS

Topologie -> GNS3

- Serveur

VMs pour les serveurs -> VirtualBox

- Pare-feu

PFSENSE -> GNS3

- Règles de sécurité

Interface Web de PFSENSE

SERVEUR FTP

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

```
ftp@srvftp:~$ sudo groupadd 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/
```

```
DefaultChdir /home/ftp
```

SERVEUR HTTP

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

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

```
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
```



PFSENSE & VLANS

```
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
```

```
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
```

```
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
```

SERVICE	RANGE D'ADRESSE	VLAN
Direction 192.168.10.1	192.168.10.5 192.168.10.50	10
Gestion 192.168.20.1	192.168.20.5 192.168.20.50	20
Commerce 192.168.30.1	192.168.30.5 192.168.30.50	30

RÈGLES DE PARE-FEU

Autorisé

LAN vers WAN
LAN vers DMZ
WAN vers DMZ

Interdit

DMZ vers LAN
DMZ vers WAN
WAN vers LAN

Rules (Drag to Change Order)

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

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	DMZ net	*	*	*	*	none	

Rules (Drag to Change Order)

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

TESTS

VLAN30 vers VLAN20

```
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
```

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
```

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
```

DMZ vers LAN

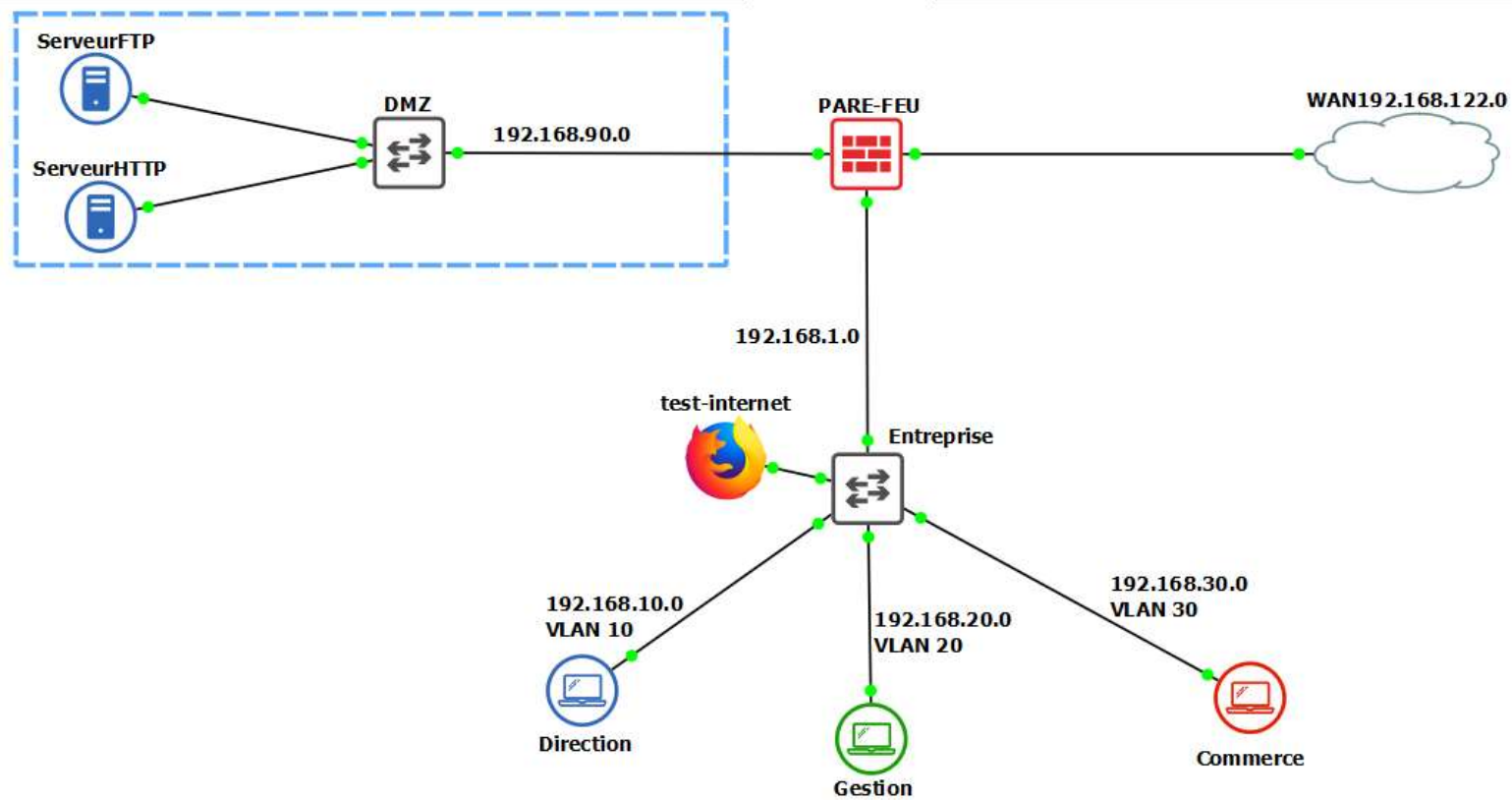
```
DMZ-test> ping 192.168.1.1
192.168.1.1 icmp_seq=1 timeout
192.168.1.1 icmp_seq=2 timeout
192.168.1.1 icmp_seq=3 timeout
192.168.1.1 icmp_seq=4 timeout
192.168.1.1 icmp_seq=5 timeout
```

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
```

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
```



TOPOLOGIE FINALE