

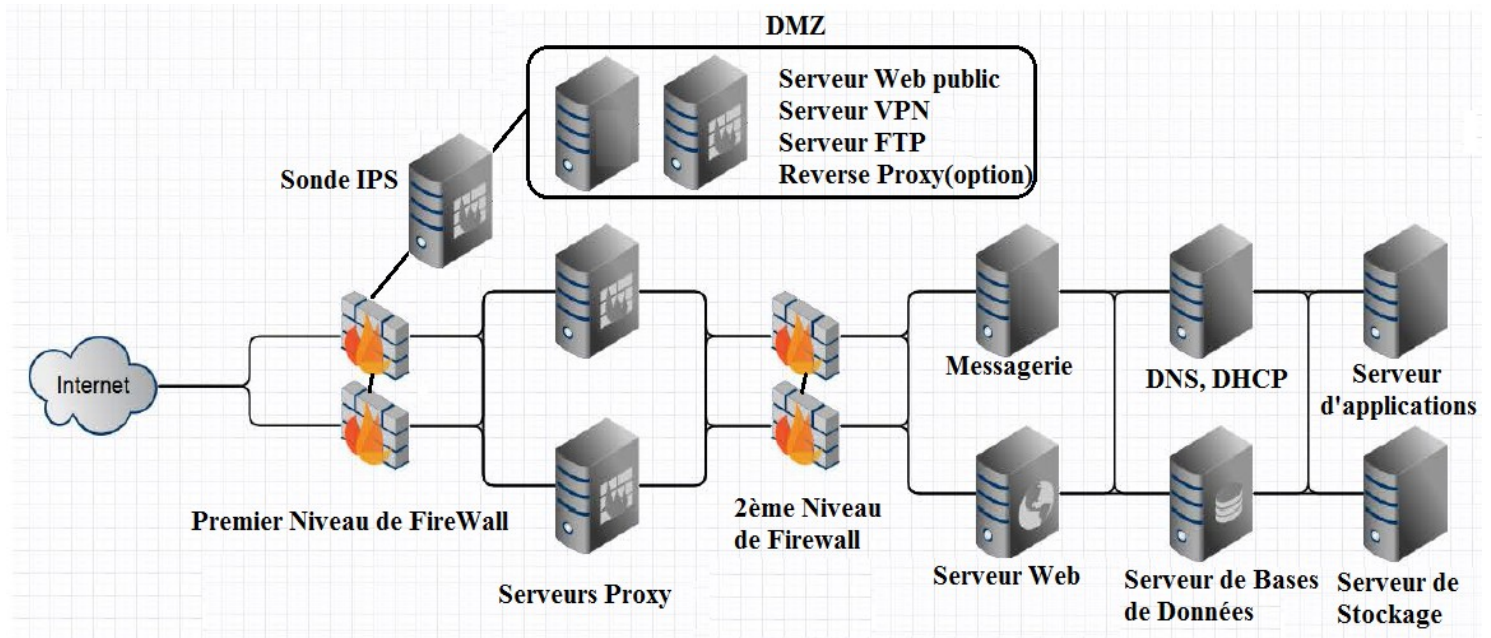
Mathieu BOISNARD  
Valentin FRIES  
Vincent MILANO

# ENOVATIVE keys

# Table des matières

1 . Définition des besoins client.....	2
2 . Architecture réseau.....	3
3 . Technologies & Interfaçage.....	4
3.1 Routeur/Firewall – pfSense.....	4
3.2 Le LAN – Zentyal.....	7
3.3 La DMZ – Debian.....	13

## 1. Définition des besoins client



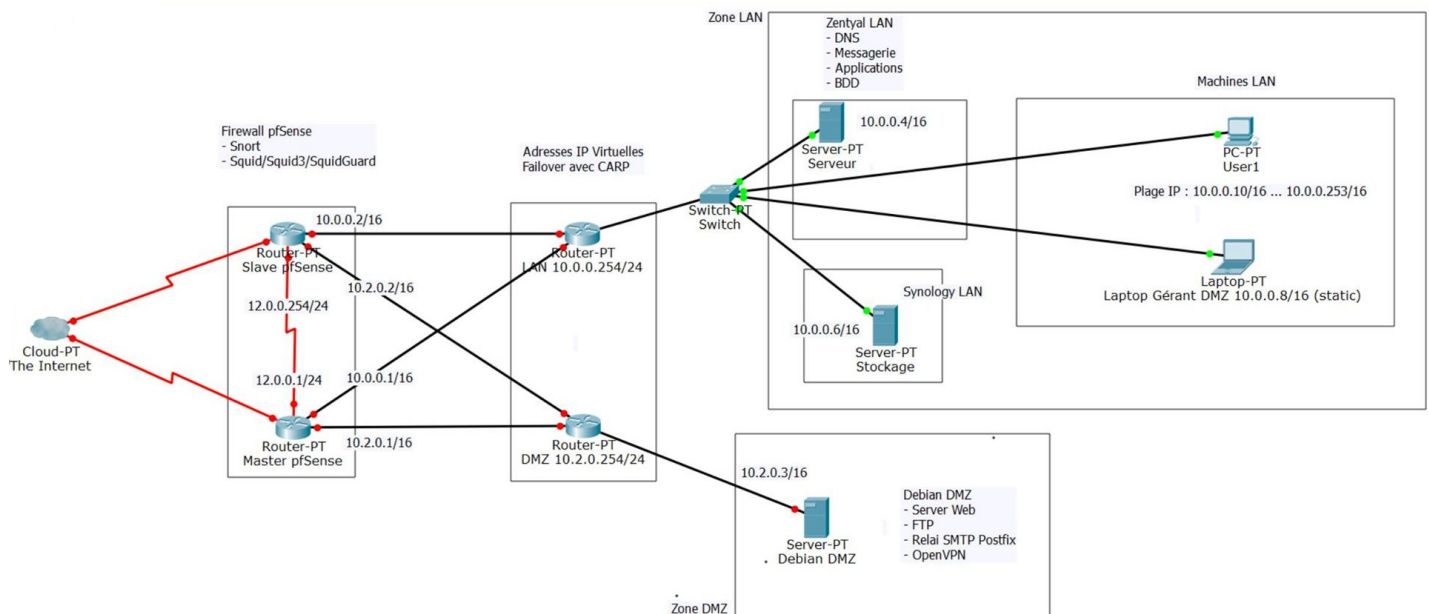
L'architecture réseau sera constituée de plusieurs parties :

Une zone DMZ, faisant office d'interface entre WEBEX et ses clients. Cette zone sera sécurisée par un firewall. Une sonde IPS sera placée en amont afin de perfectionner cette sécurisation.

Deux niveaux de firewalls protégeront l'accès au réseau local (LAN) de l'entreprise. Un serveur Proxy sera chargé de filtrer les requêtes sortantes du réseau LAN de WEBEX vers le WAN.

Enfin, un LAN sera installé, disposant d'une solution SAN pour le stockage et de serveurs faisant fonctionner différents services : Web, Messagerie, Applications, Bases de Données...

## 2. Présentation de l'architecture générale de la solution



Afin de répondre aux différentes spécifications nécessaires à l'architecture réseau de WEBEX, E-Novative Keys propose :

Une machine Zentyal, afin de représenter le LAN. Celle-ci contiendra les différentes nécessités de la zone LAN, à savoir serveur Web, Base de Données, Stockage, Applications, Messagerie. Une redondance est applicable sur cette interface. Comme nous le voyons sur le schéma, la zone LAN contiendra également un routeur. L'adressage général est statique, sauf à l'intérieur de la LAN. Le routeur sera adressé en 10.0.0.3 (em1). Il communiquera avec l'interface 10.0.0.1 du firewall pfSense.

Une machine Debian, afin de représenter la DMZ. Celle-ci contiendra le serveur Web, le FTP et le VPN nécessaires à la DMZ. Alors que le FTP devra assurer l'échange de fichiers sur le réseau, le VPN devra s'occuper de créer un lien direct avec l'interface du LAN afin de permettre le stockage et l'interfaçage applicatif du Web Service – situé dans le LAN - avec le Cloud situé dans la DMZ. Avec un adressage statique en 10.2.0.3, cette Linux communiquera avec l'interface 10.2.0.1 (em2) du firewall pfSense.

Enfin, un système de firewalls pfSense en double clusters sera mis en place, la redondance sera assurée entre les deux machines (failover avec CARP), qui auront chacune 3 interfaces (sans tenir compte de leur interconnexion) : em0 (192.168.X.X) représentant le WAN, em1 (10.0.0.1) représentant le réseau local (LAN), et em2 (10.2.0.1) représentant la DMZ. Différents packages seront installés sur les machines pfSense, dont le détail est précisé ci-dessous.

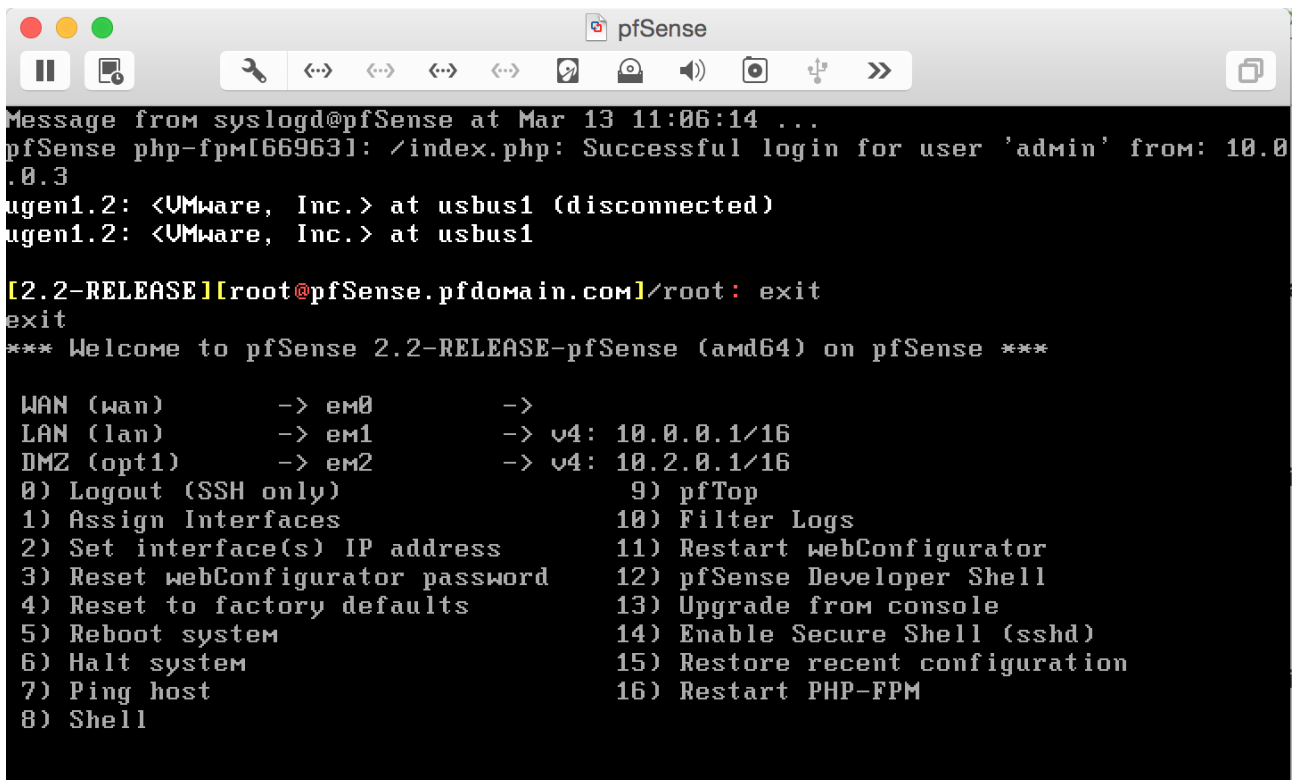
## 3 - Technologies & Interfaçage

### 3.1 Routeur/Firewall - pfSense



L'interfaçage de l'architecture demandée par WEBEX demande un filtrage des accès choisi avec précision et efficacité. L'ensemble des employés internes à l'entreprise, situés dans le LAN, auront un accès aux applications internes à l'entreprise, logées sur le applicatif, mais également à toute la zone DMZ. L'accès au panel de gestion des firewalls doit également pouvoir être effectué directement depuis le LAN, afin qu'une maintenance plus simple soit effectuée en termes de sécurité. L'ensemble de l'entreprise aura également accès au réseau WAN, seulement ces connexions seront filtrés via un proxy Squid 3 pour des raisons de sécurité et de propreté du réseau interne et général. La pfSense doit également assurer un accès à la DMZ depuis le WAN, afin que les clients puissent se connecter à leur interface sur le Cloud. Cet accès sera directement filtré à l'entrée du WAN via Snort\_inline, configuré en mode sonde IPS. Enfin, la DMZ n'aura aucun accès direct au LAN, pour des raisons évidentes de sécurité.

Afin d'assurer un niveau constant de services, une redondance sera mise en place sur le firewall pfSense, Il y aura donc deux machines, l'une en service, l'autre à l'écoute de la première afin de reprendre son activité avec les mêmes paramètres dans l'éventualité où la première machine tombe suite à un problème réseau quelconque. Le failover sera assuré avec CARP, qui permet une installation intuitive et surtout stable.



```
Message from syslogd@pfSense at Mar 13 11:06:14 ...
pfSense php-fpm[66963]: /index.php: Successful login for user 'admin' from: 10.0.0.3
ugen1.2: <UMware, Inc.> at usb1 (disconnected)
ugen1.2: <UMware, Inc.> at usb1

[2.2-RELEASE][root@pfSense.pfdomain.com]/root: exit
exit
*** Welcome to pfSense 2.2-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 10.0.0.1/16
DMZ (opt1)     -> em2      -> v4: 10.2.0.1/16
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Trois interfaces sont configurées de base : **em0**, **em1** et **em2**.

**em0** représente le WAN. Cette interface représente l'accès extérieur des clients. Il sera directement redirigé sur l'interface em2, la DMZ. L'adressage de l'interface sur la pfSense est en 192.168.X.X, la sonde IPS y est directement installée.

**em1** représente le LAN. Cette interface représente l'intérieur du réseau de WEBEX. Cette interface doit avoir un accès filtré à la DMZ, ainsi qu'un accès au réseau extérieur, dont l'accès sera filtré via un proxy squid3. L'adressage de l'interface sur la pfSense est en 10.0.0.1 (failover en 10.0.0.2).

**em2** représente la DMZ. Cette interface héberge le Cloud de WEBEX. Les clients, venant du WAN, doivent y avoir un accès filtré (IPS, voir em0). Cependant toute personne dans la DMZ venant du WAN ne peut pas avoir accès au réseau LAN de l'entreprise. L'adressage de l'interface sur la pfSense est en 10.2.0.1 (failover en 10.2.0.2).

pfSense.pfdomain.com - System: Package Manager - Icwesael

File Edit View History Bookmarks Tools Help

pfSense.pfdomain.com - System...

https://10.0.0.1/pkg\_mgr\_installed.php

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

Sense

- System
- Interfaces
- Firewall
- Services
- VPN
- Status
- Diagnostics
- Gold

Name	Category	Version	Description
snort	Security	2.9.7.0 pkg v3.2.3	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.  Package info
spamd	Services	4.9.1_2 v1.1.1	Tarpits like spamd are fake SMTP servers, which accept connections but don't deliver mail. Instead, they keep the connections open and reply very slowly. If the peer is patient enough to actually complete the SMTP dialogue (which will take ten minutes or more), the tarpit returns a 'temporary error' code (4xx), which indicates that the mail could not be delivered successfully and that the sender should keep the mail in their queue and retry again later.  No package info, check the forum
squid3	Network	3.4.10_2 pkg 0.2.6	High performance web proxy cache. It combines squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, ssl filtering and antivirus integration via i-cap  Package info

https://10.0.0.1/index.php

pfSense.pfdomain.com... root@kali: ~

*Packages installés sur le routeur/firewall pfSense*

### 3.2 Le LAN - Zentyal



#### Routeur LAN

```
enkeys@lan-router:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d6:7f:f7
          inet addr:10.0.0.3  Bcast:10.0.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:d6:7f:01
          inet addr:10.1.0.1  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:303 errors:0 dropped:0 overruns:0 frame:0
          TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28382 (28.3 KB)  TX bytes:25671 (25.6 KB)
```

**eth0** représente le sous-réseau du routeur/firewall pfSense. Cette interface représente le lien entre le premier et le second niveau de firewall situés entre le WAN et le LAN. Adresse statique définie sur 10.0.0.3.

**eth1** représente le LAN. Cette interface est la passerelle de tous les postes du LAN, leur permettant ainsi de sortir vers la DMZ et le WAN. Adresse statique définie sur 10.1.0.1.



Le routeur LAN fait de plus office de serveur DHCP & DNS pour les postes de travail du réseau local de l'entreprise.

La plage DHCP configurée sur le sous-réseau 10.1.0.0/16 du LAN attribue les adresses de 10.1.0.10 à 10.1.255.254.

## Plage DHCP

**Adresse IP de l'interface**

10.1.0.1

**Sous-réseau**

10.1.0.0/16

**Plage disponible**

10.1.0.1 - 10.1.255.254

## Plages

[+ AJOUTER UN NOUVEAU](#)

Nom	De	To	Action
ENK-LAN	10.1.0.10	10.1.255.254	 

10 ▼

K &lt;

Page 1

&gt; X

Il est possible de visualiser les beaux DHCP attribués par le serveur depuis le Panneau de Contrôle du routeur.

### Baux DHCP



Adresse IP	Adresse MAC	Nom d'hôte
10.1.0.10	00:0c:29:45:e0:d2	WIN-6K5RB6S3TRI

Faisant de plus office de serveur DNS pour le LAN, ce serveur dispose d'un cache DNS, configure un forwarder en cas de problème quelconque (8.8.8.8 : Google Public DNS), et redirige le FQDN **enkeys.com** vers le serveur LAN situé à l'adresse **10.1.0.3**.

## Settings

☒ **Activer le cache DNS transparent**

**CHANGE**

## Forwarders

**+ AJOUTER UN NOUVEAU**

Forwarder	Action
8.8.8.8	<input type="button" value="X"/> <input type="button" value="P"/>

10   Page 1

## Domaines

**+ AJOUTER UN NOUVEAU**

Domaine	Adresses IP du domaine	Noms d'hôtes	Gestionnaires de Courrier	Serveurs de noms	Enregistrement TXT	Services	Domaine dynamique	Action
enkeys.com	<input type="button" value="⚙"/>	<input type="button" value="⚙"/>	<input type="button" value="⚙"/>	<input type="button" value="⚙"/>	<input type="button" value="⚙"/>	<input type="button" value="⚙"/>	<input checked="" type="checkbox"/>	<input type="button" value="X"/> <input type="button" value="P"/>

10   Page 1

Enfin, le routeur intègre aussi un module Firewall, permettant d'ajouter une couche de sécurité à l'entrée et à la sortie du réseau LAN de l'entreprise.

## Serveur LAN

```
enkeys@lan:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ca:4c:fe
          inet addr:10.1.0.3  Bcast:10.1.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:416 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:69883 (69.8 KB)  TX bytes:37346 (37.3 KB)
```

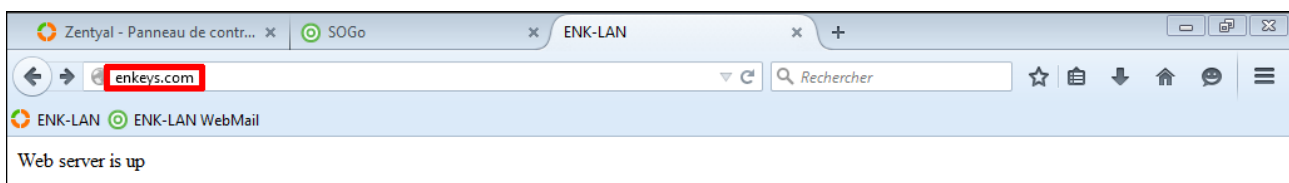
**eth0** est connecté sur le réseau LAN. Adressage statique en 10.1.0.3. Redondance possible en 10.1.0.2.

Devant faire office de serveur de base de données, le serveur LAN dispose d'un serveur MySQL 5.5 totalement fonctionnel.

```
enkeys@lan:~$ mysql --version
mysql Ver 14.14 Distrib 5.5.41, for debian-linux-gnu (x86_64) using readline 6.3
```

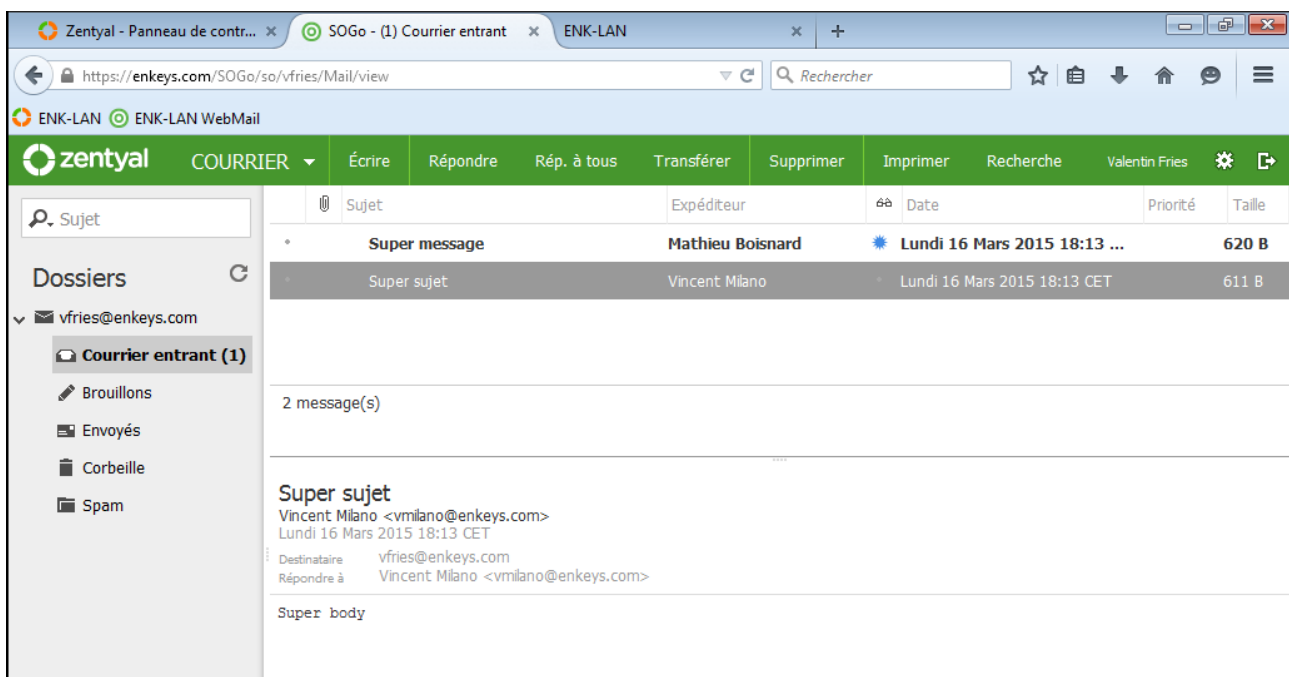
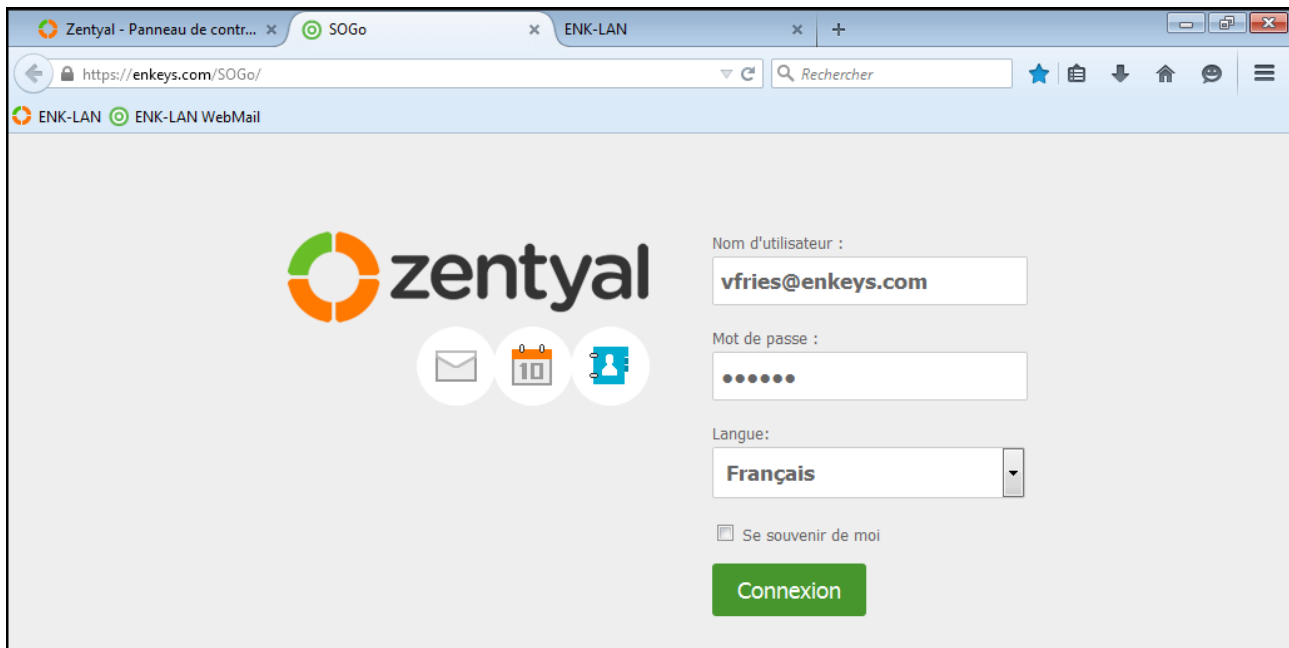
Le serveur Web apache2 est lui aussi installé et fonctionnel.

```
enkeys@lan:/var/www/html$ sudo service apache2 status
* apache2 is running
```

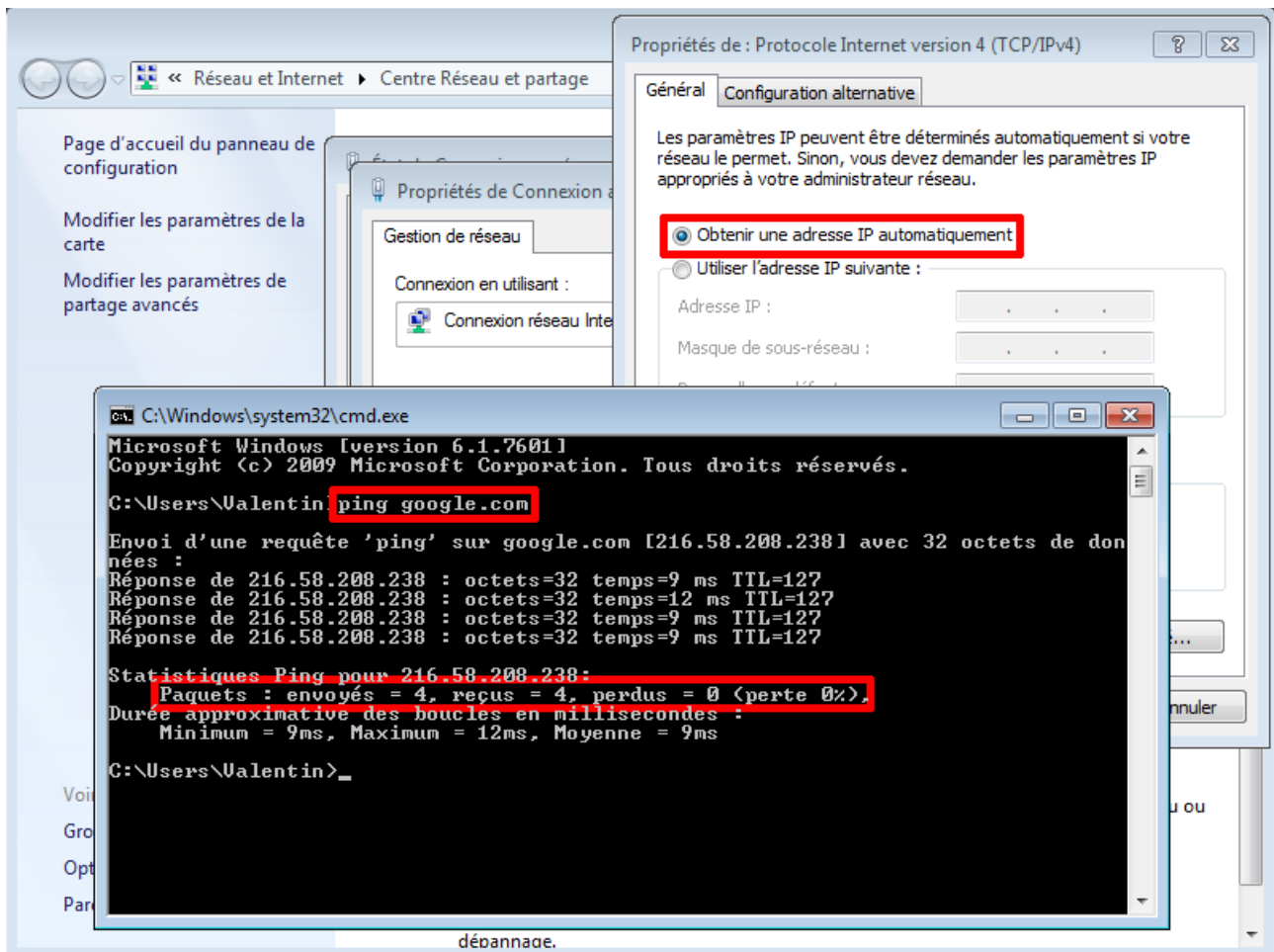


*Atteinte du serveur web LAN depuis un poste de travail connecté au réseau LAN.*

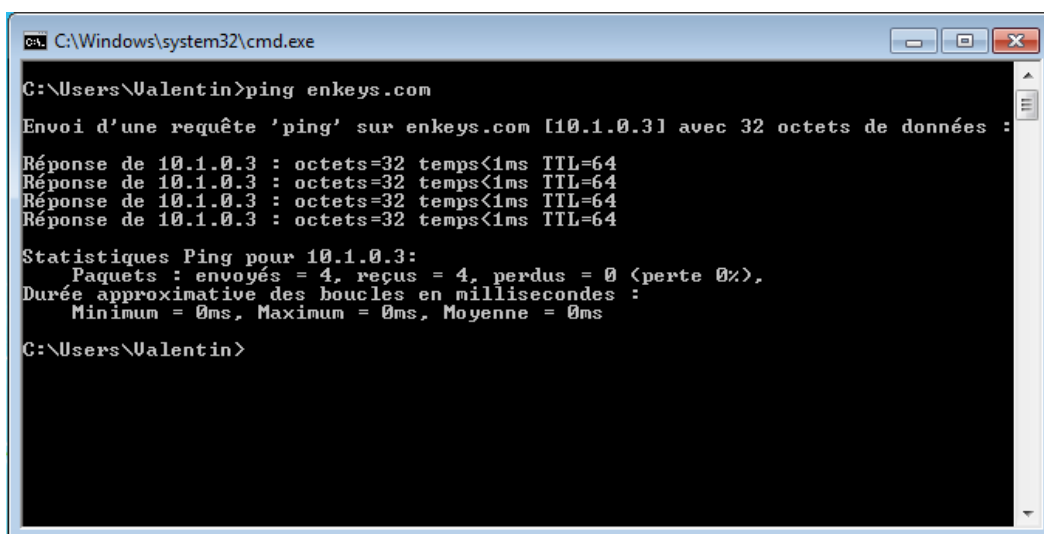
Il est de plus possible pour chaque employé de l'entreprise d'accéder à ses emails, son calendrier et ses carnets d'adresses depuis le Webmail du serveur LAN :



## Postes de travail « clients » LAN



Les postes de travail connectés au LAN de l'entreprise obtiennent un bail DHCP de manière automatique de la part du routeur et peuvent dès lors accéder au LAN et sortir vers le WAN



### 3.3 La DMZ - Debian

N'ayant pas besoin de services aussi développés que pour le LAN, la DMZ est composée d'une simple mouture Debian sur laquelle les différents paquets concernant les services Web, FTP, VPN et relais mail seront installés.

```
root@enk-dmz:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b1:46:92
          inet adr:10.2.0.3  Bcast:10.2.255.255  Masque:255.255.0.0
          adr inet6: fe80::20c:29ff:feb1:4692/64  Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:0 (0.0 B)  TX bytes:2988 (2.9 KiB)
```

**eth0** est connecté sur le réseau représentant la DMZ (**em2**) créé par le routeur pfSense. IP Statique 10.2.0.3

#### Service Web/FTP

Installation des paquets `apache2` `php5` `apache2-mod-php5` pour les fonctionnalités du serveurs web. De plus, le paquet `php5-curl` est également installé pour une liaison future entre le webservice et le cloud.

```
root@enk-dmz:/etc# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the s
ver's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@enk-dmz:/etc# /etc/init.d/vsftpd start
Starting FTP server: vsftpd.
```

← → ↻ ⬆ 10.2.0.3



## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

← → ↻ ⬆ ftp://10.2.0.3

## Index de /

Nom	Taille	Date de modification
 <a href="#">fic1</a>	0 B	17/03/2015 22:41:00
 <a href="#">index.html</a>	177 B	16/03/2015 15:27:00

## Serveur VPN

Après l'installation du paquet OpenVPN, une étape de configuration et de génération de clés et de certificats est nécessaire avant de pouvoir exécuter le service de manière pérenne.

A partir d'easy-rsa, nous avons accès à un panel d'outils permettant la génération des différentes clés et certificats.

```
> cd /etc/openvpn/easy-rsa
> source vars
> ./clean-all
> ./build-dh
> ./pktool --initca
> ./pktool --server server
> openvpn --genkey --secret keys/ta.key
```

Les clés et certificats sont maintenant générés. Il ne reste plus qu'à créer un dernier fichier de configuration intégrant les différents fichiers précédemment créés et lancer le service openvpn.

```
# Server TCP/443

mode server
proto tcp
port 443
dev tun

# Keys & certificates

ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
tls-auth ta.key 1
key-direction 0
cipher AES-256-CBC
```

```
# Network

server 10.2.0.0 255.255.0.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120

# Security

user nobody
group nogroup
chroot /etc/openvpn/jail
persist-key
persist-tun
```

```
# Security

user nobody
group nogroup
chroot /etc/openvpn/jail
persist-key
persist-tun
comp-lzo

# Log

verb 3
mute 20
status open-status.log
log-append /var/log/openvpn.log
```

> openvpn server.conf

Le service openvpn est maintenant lancé et une nouvelle interface réseau est apparue.

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
      inet adr:10.2.0.1  P-t-P:10.2.0.2  Masque:255.255.255.255
      UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:100
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```