INSTALLATION DE SERVEURS WEB APACHE ET NGINX, SÉCURISATION SSL ET INSTALLATION D'UN REVERSE PROXY

Winness R.

SOMMAIRE

1. Introduction et présentation de la problématique
2. Plan de refonte du système informatique & présentation de l'infrastructure
    1. Le firewall pfsense
    2. Le reverse proxy
    3. Le serveur DNS
    4. Les sites ventes et sav (serveurs apache)
    5. Les sites web ERP et CRM (serveur nginx)
    6. Iptables
    7. Fail2ban
    8. Conclusion

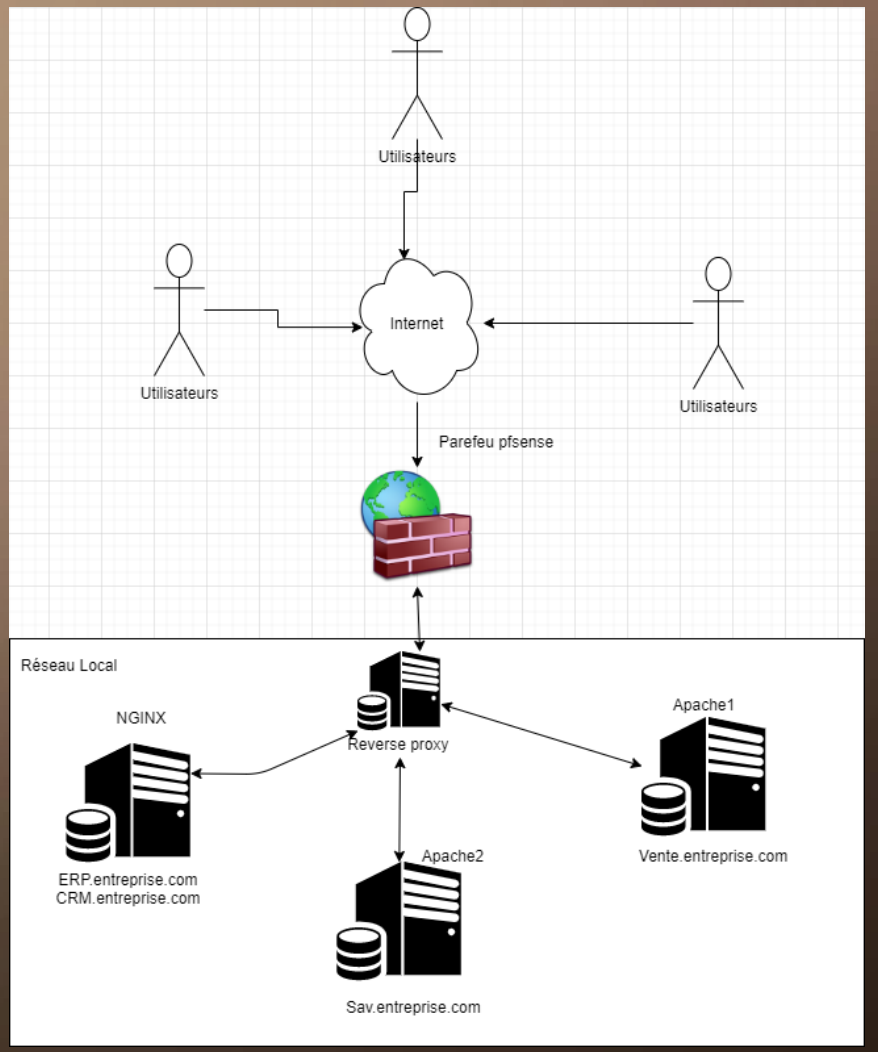
PRÉSENTATION DE LA PROBLÉMATIQUE

- La société BeTheFirst dispose d'un site de vente en ligne ainsi que d'un site pour la gestion du SAV, aucun des serveurs n'a de certificat SSL, la gestion du SI ne respecte pas les bonnes pratiques et les moteurs de recherche ne référencent plus les sites du client.
- Pour régler cette problématique, nous proposons de remettre à plat l'infrastructure afin de retrouver une architecture homogène et sécurisée, qui permettra l'intégration d'un nouvel ERP/CRM

A. PLAN DE REFONTE DE L'INFRASTRUCTURE

- Le nouvelle SI se composera de :

1. 1 serveur reverse proxy SSL (nginx)
2. 2 serveurs web apache (sav/ventes.entreprise.com)
3. 1 serveur web nginx (erp.entreprise.com et crm.entreprise.com)

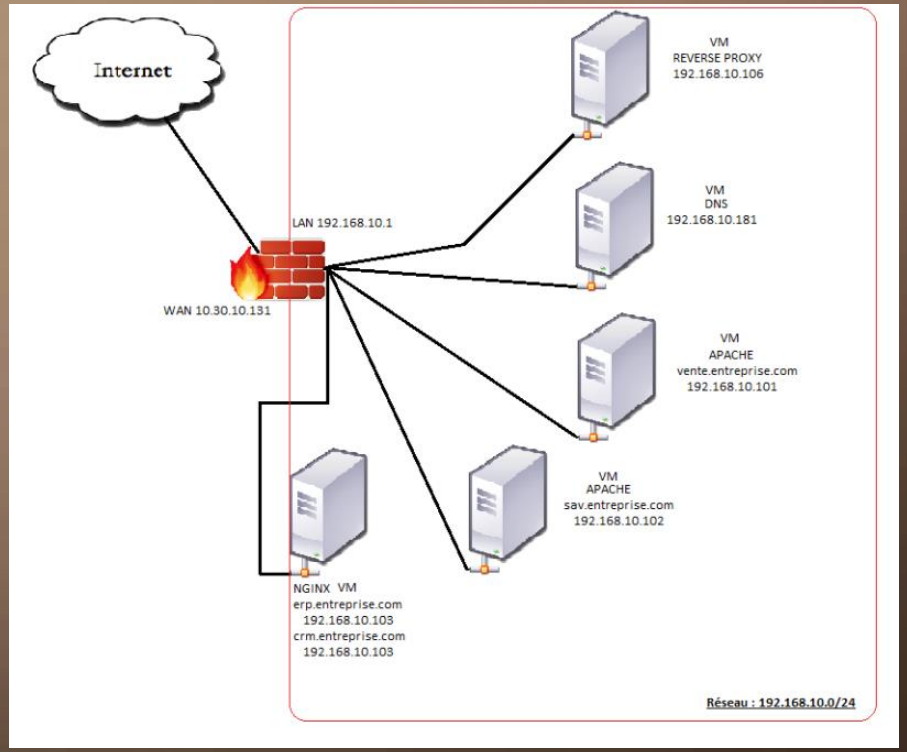


B. INFRASTRUCTURE

Nous avons d'abord mis un firewall pfsense afin d'apporter une sécurité supplémentaire en amont de vos serveurs web.

Puis nous avons organisé votre nouvelle structure tout en gardant vos deux sites existants (sav/ventes.entreprise.com) ainsi qu'un serveur menant à votre nouvel ERP et CRM

Nous avons également ajouter un reverse-proxy permettant le filtrage du trafic provenant d'internet vers le réseau, en aiguillant les requêtes vers les serveurs à atteindre



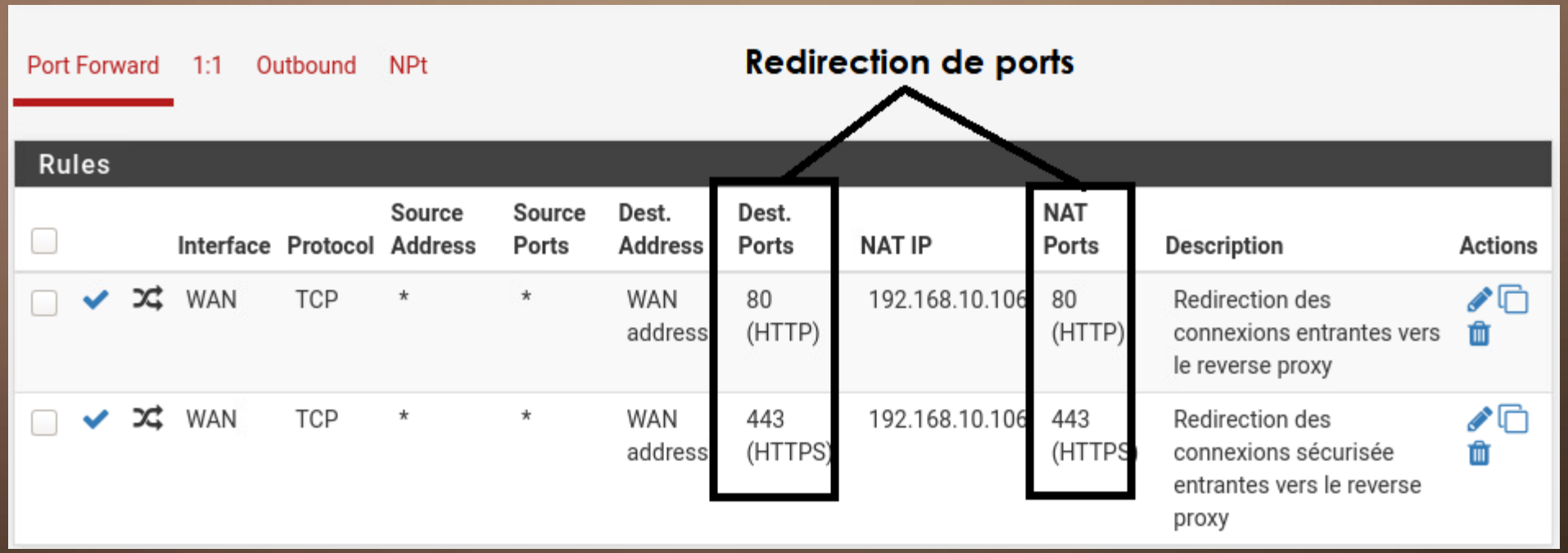
1.PFSENSE

Le pfsense est un pare-feu open-source (libre de droit) permettant de sécuriser votre SI des tentatives d'intrusion externe.

Il est le premier outil mis en place afin de protéger les serveurs du trafic externe.

Il va également nous être utile à assurer la sécurisation de vos sites web en appliquant une règle permettant l'accès sécurisé de votre SI.

QUELQUES MANIPULATIONS

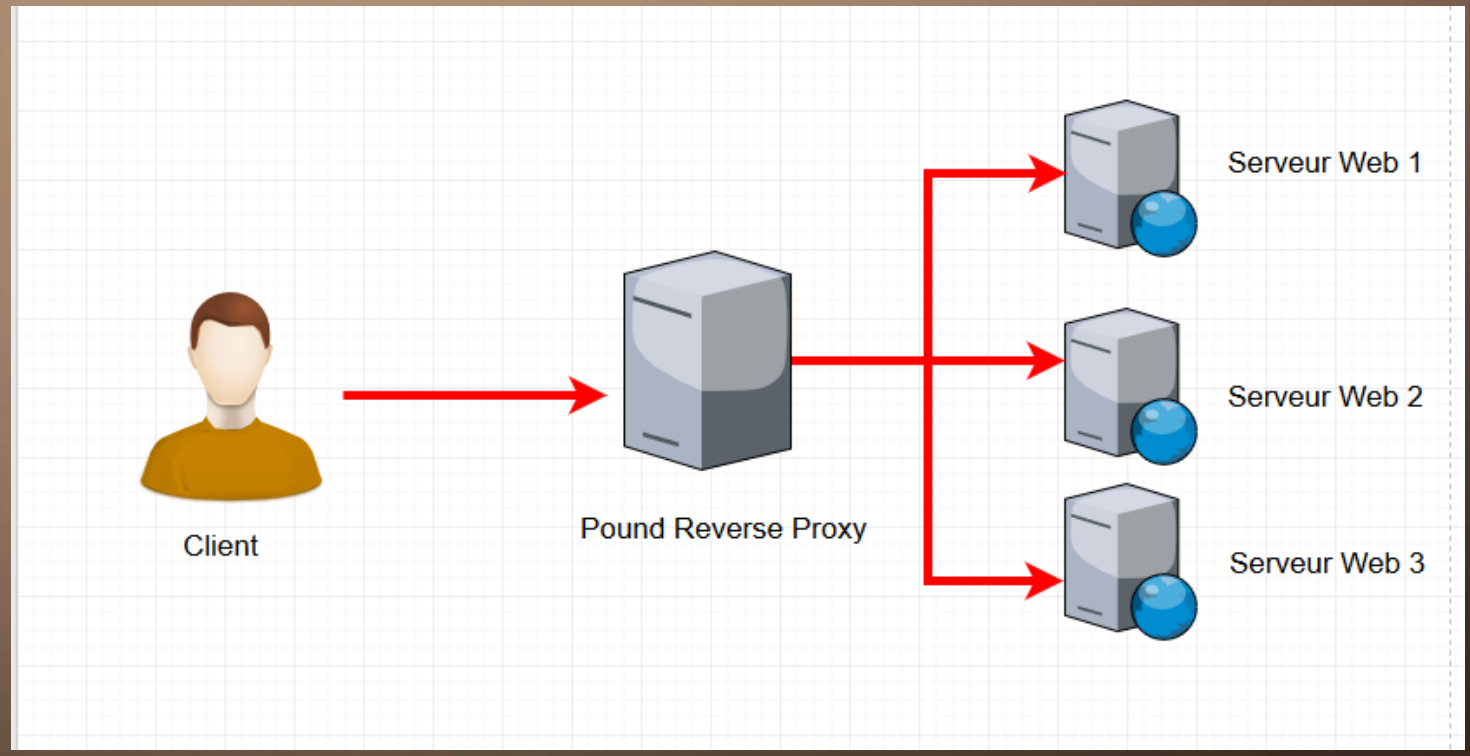


2. REVERSE PROXY

Il remplit le rôle de passerelle entre internet et le réseau local, il donne l'accès via internet aux serveurs dans votre réseau de façon à ce que lorsque l'on cherchera à joindre vos sites, les utilisateurs n'interrogeront que le reverse proxy.

Le reverse proxy se chargera d'aiguiller les requêtes vers les serveurs demandés.

Pour finir, on lui attribuera certificats de nos serveurs web.



QUELQUES MANIPULATIONS

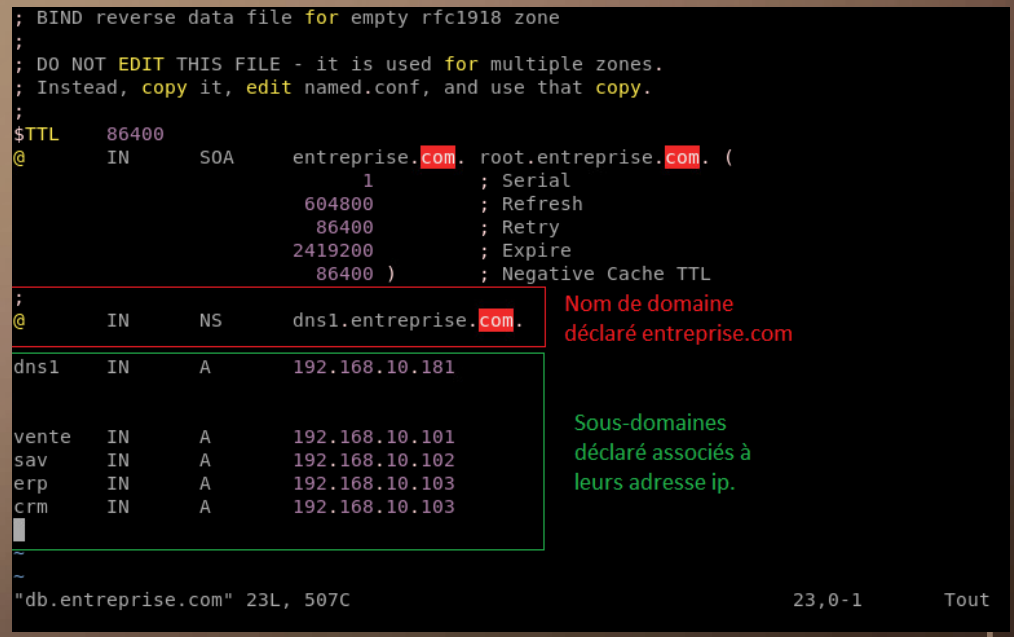
```
server {
        listen 443;
        server_name vente.entreprise.com;

ssl on;
ssl_certificate /etc/ssl/ventes.crt;
ssl_certificate_key /etc/ssl/ventes.key;

access_log /var/log/nginx/access.log;
error_log /var/log/nginx/error.log;


        location / {
                proxy_pass https://192.168.10.101;
                proxy_set_header Host $host;
                        proxy_set_header                X-Forwarded-For
        $proxy_add_x_forwarded_for;
        proxy_connect_timeout 30;               proxy_send_timeout 30;
        }
}
```

```
#Quand un client effectuera une requête sur internet en cherchant vente.entreprise.com
#Le reverse proxy aiguillera le trafic vers le serveur d'apache ventes
#Toutes les requêtes destinées à une adresse publique sont transférer par le reverse-proxy
#A l'adresse interne spécifiée dans le ProxyPass.

#header X-Forwarded-For : il va nous permettre de changer l'ip source arrivant du client
#en transformant cette ip par celle du reverse proxy qui lui seul pourra atteindre le serveur web
# cela sécurise encore plus notre accès aux serveurs web.
```

3. LE SERVEUR DNS

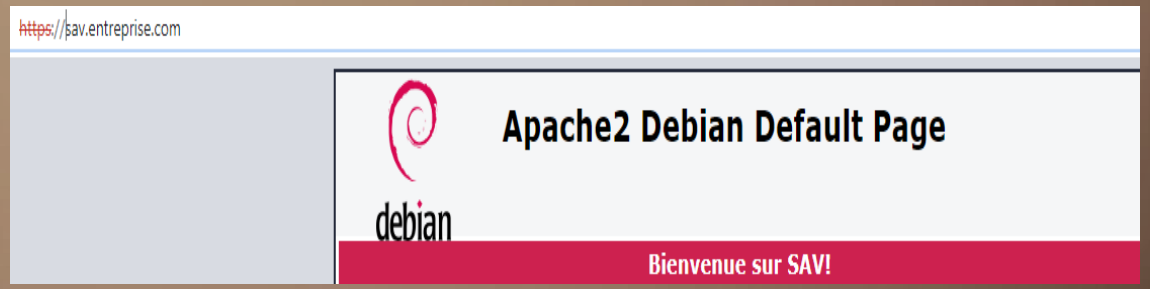
- Le DNS « Domain Name System » ou en Français le Système de noms de domaine est un service informatique permettant de traduire une adresse ip en nom de domaine.
- Imaginez un annuaire téléphonique où à côté de votre nom figure votre numéro de téléphone. Il est plus simple de retenir plusieurs noms que plusieurs numéro de téléphone.

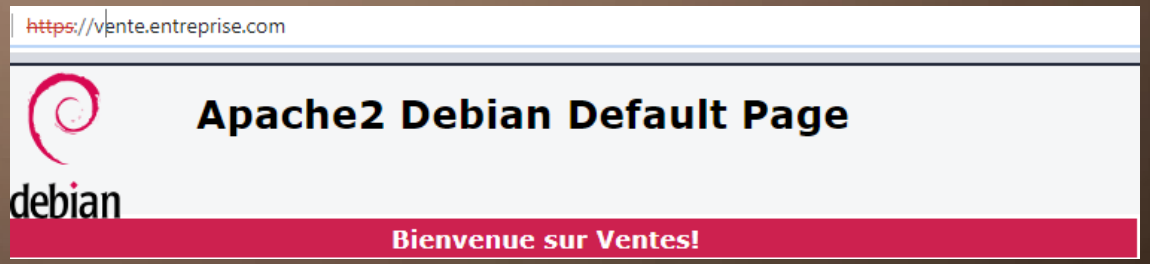
Le DNS permet donc de traduire une adresse ip en nom de nomaine et facilite la recherche d'un site sur internet.



4.A LES SERVEURS VENTES/SAV.ENTREPRISE.COM

- D'après votre infrastructure vos serveurs vente et sav étaient configurés sans connexions sécurisés.
- Nous avons donc apporté une sécurisation ssl à l'aide de certificats pour sécuriser vos serveurs web et ainsi les référencer sur google,

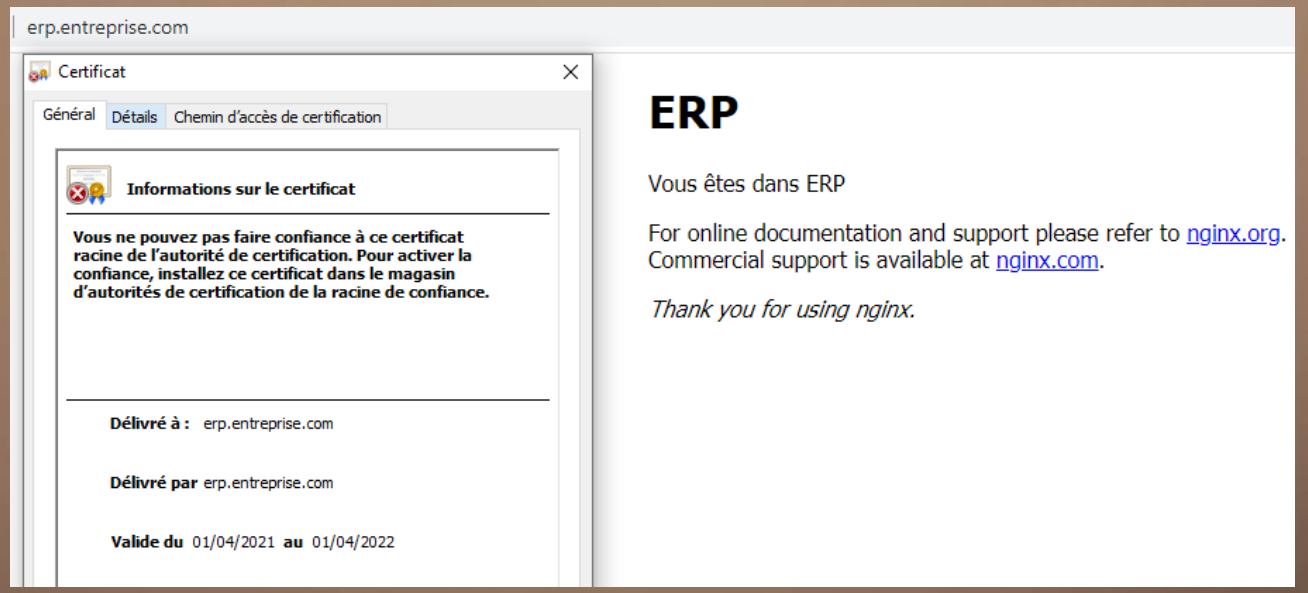




4.B EXEMPLE DE FICHIER DE CONFIGURATION APACHE

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                ServerName sav.entreprise.com
                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example the
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only the
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/ssl/SAV.crt
                SSLCertificateKeyFile /etc/ssl/SAV.key
```

5.A L'AJOUT DES SITES WEB ERP ET CRM



- Comme convenu, nous avons ajouté un serveur web nginx à votre infrastructure qui comporte deux sites web : erp.entreprise.com/crm.entreprise.com que nous avons sécurisé en SSL à l'aide de certificats.

5.B QU'EST-CE QU'UN ERP

- Un ERP (Entreprise Resource Planning) est un logiciel qui permet de gérer tous les processus de l'entreprise comme par exemple :

- Les ressources humaines

-La comptabilité

-La vente

-Les stocks

5.C QU'EST-CE QU'UN CRM

- Un CRM (Customer Relationship Management) est une stratégie de gestion des relations et interactions d'une entreprise avec ses clients ou futurs clients.
- Un système CRM aide les entreprises à interagir en permanence avec les clients, à rationaliser leurs processus et à améliorer leur production.

6.A IPTABLES

- Pour mieux sécuriser le déploiement et l'utilisation de vos serveurs, nous avons mis en place précédemment les certificats SSl, et actuellement nous allons mettre en fonction les iptables sur chaque serveur.

Iptables est une application de ligne de commande et un parefeu Linux que vous pouvez utiliser pour configurer, maintenir et inspecter les tableaux de filtres de paquets.

6.B QUELQUES MANIPULATIONS

```
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:4431

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:4431
```

Ce sont les politiques de régles de trafic par défaut.
Par défaut avec "DROP" nous interdisons simplement tout le trafic entrant ou sortant sur tous les ports.

Ce sont les règles que nous avons ajouté et qui sont des exceptions aux règles de trafic par défaut.

Dans notre cas, nous avons autorisé le port DNS et HTTPS à établir la connexion, ainsi que le port 4431 qui est le port d'écoute du site ERP sur le serveur nginx.

Seul les ports 53,443 et 4431 sont autorisé à établir des connexions.

7.A FAIL2BAN

- Fail2ban est un programme qui analyse les logs de connexions de divers services (SSH, Apache, FTP) en cherchant des correspondances entre des motifs définis dans ses filtres.

- Typiquement, fail2ban cherche des tentatives répétées de connexions infructueuses et procède à un bannissement en ajoutant une règlle au pare-feu Iptables.

7.B QUELQUES MANIPULATIONS

8. CONCLUSION

Pour conclure,

- Afin d'améliorer le référencement de vos sites et les sécurisés, nous avons refait une toute nouvelle infrastructure plus sécurisée que la précédente :
- -Nous avons organisé toute votre infrastructure en gardant votre base, en établissant la connexion de vos serveurs web avec des certificats SSL pour les référencer sur internet derrière un reverse proxy afin de les sécurisés davantage.
- -Nous avons également déplacer les certificats SSL dans le reverse proxy, pour faire la jonction entre les utilisateurs et les serveurs web et sécuriser l'ensemble des serveurs et le reverse proxy.
- -Nous avons fini par installer iptables et fail2ban pour ajouter des règles supplémentaires et bloquer des utilisateurs voulant entrer dans notre réseau sans avoir les mot de passe pour éviter toute intrusion intempestive.