Mise en place d’un site web vitrine sécurisé avec HTTPS

🎯 Pourquoi avoir mis en place un site web

L’entreprise **Uranus Logistique**, spécialisée dans le transport et la gestion de marchandises, a souhaité disposer d’un **site web vitrine** afin de :

✅ Présenter ses activités

Le site web permet de mettre en avant les points suivants :

- la nature de l’activité logistique de l’entreprise,
- les services proposés,

- des informations de contact basiques accessibles aux visiteurs autorisés.

✅ Proposer une interface claire et professionnelle

Le site est conçu comme une **landing page moderne**, avec un menu simple, un slogan principal, un bouton d'action ("Demander un devis"), et un design épuré. Il permet à l'entreprise de renforcer sa **présentation visuelle** et sa cohérence numérique.

✅ Héberger le site de manière sécurisée

Le site est hébergé sur un **serveur web dédié situé dans la zone DMZ** de l'infrastructure. Il est accessible via le protocole **HTTPS**, garantissant :

- une communication chiffrée entre le client et le serveur,
- l'absence d'alertes de sécurité dans les navigateurs,
- une meilleure compatibilité avec les standards actuels.

⚠️ Prérequis avant le déploiement du site web

- Une **machine Debian** fonctionnelle et à jour
- Un **serveur web** installé (Apache ou Nginx)
- Les **droits administrateur (root)** pour configurer le système
- Les **fichiers du site vitrine** prêts à être déployés (HTML/CSS)

🛠️ Installation et configuration du serveur web

Le site vitrine est hébergé sur une machine Debian, à l'aide du serveur web **Apache2**. Voici les étapes suivies pour mettre en place le service.

🧱 Installation d'Apache

```
apt update && apt install apache2 -y
```

Une fois installé, le serveur web est automatiquement lancé. Il est accessible en local via l'adresse :

`http://localhost` ou `http://<IP_DU_SERVEUR>`

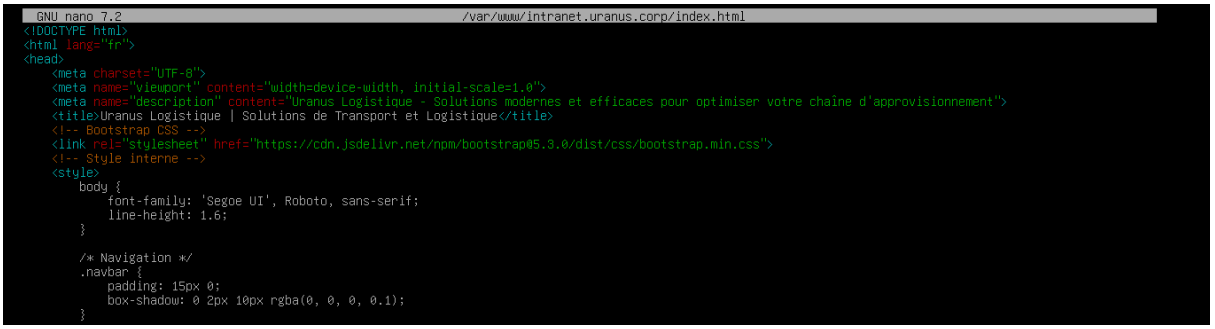
📁 Déploiement du site vitrine

Les fichiers du site vitrine (HTML, CSS, images...) sont stockés dans le dossier suivant :

```
/var/www/extranet.uranus.corp/
```

> Exemple pour modifier la page d'accueil :

```
nano /var/www/extranet.uranus.corp/index.html
```



⚙️ Configuration du VirtualHost Apache

Un VirtualHost spécifique a été créé pour le domaine `intranet.uranus.corp` :

```
nano /etc/apache2/sites-available/extranet.uranus.corp.conf
```

Contenu du fichier :

```
<VirtualHost *:80>
    ServerName extranet.uranus.corp
    DocumentRoot /var/www/intranet.uranus.corp

    <Directory /var/www/intranet.uranus.corp>
```

```
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/intranet_error.log
    CustomLog ${APACHE_LOG_DIR}/intranet_access.log combined
</VirtualHost>
```

✅ Activation du site et redémarrage d'Apache

```
a2ensite intranet.uranus.corp.conf
systemctl reload apache2
```

Le site est maintenant accessible via :

`http://extranet.uranus.corp` (en attendant l'activation du HTTPS)

🔒 Activation du HTTPS avec un certificat signé par l'Active Directory

Pour sécuriser le site vitrine `extranet.uranus.corp`, un certificat SSL a été généré et signé **par l'autorité de certification interne** hébergée sur le contrôleur de domaine `AD1`.

Cette méthode repose sur :

- La génération d'une **clé privée et d'une CSR** (demande de signature) sur le **serveur web**
- La **signature** de cette CSR depuis l'interface **Web CA Active Directory**
- La **configuration d'Apache2** avec le certificat et la clé privée
- Et la résolution DNS du nom `extranet.uranus.corp` par l'AD

📥 Étape 1 – Génération de la clé privée et de la CSR

Sur le **serveur web**, exécuter les commandes suivantes :

```
# Créer le dossier de stockage si nécessaire
mkdir -p /etc/ssl/uranus.corp

# Générer la clé privée
openssl genrsa -out /etc/ssl/uranus.corp/uranus.corp.key 2048

# Générer le fichier CSR
openssl req -new -key /etc/ssl/uranus.corp/uranus.corp.key -out /etc/ssl/uranus.corp/uranus.corp.csr
```

📌 Pendant la génération, bien remplir le champ **Common Name (CN)** avec : `extranet.uranus.corp`

📤 Étape 2 – Signature du certificat via le serveur Active Directory

Depuis le serveur AD, ouvrir un navigateur et accéder à :

```
http://ad1.uranus.corp/certsrv
```

1. Cliquer sur **“Demander un certificat”**
2. Choisir **“Soumettre une demande de certificat avancée”**
3. **Copier le contenu du CSR** généré précédemment sur le serveur web :

   ```
   cat /etc/ssl/uranus.corp/uranus.corp.cs
   ```

   Le contenu ressemble à ceci :

   ```
   -----BEGIN CERTIFICATE REQUEST-----
   MIICzDCCAbQCAQAwgYsxCzAJBgNVBAYTAkZSMRIwEAYDVQQIDAlJbGUtZGUtRnJh
   ...
   -----END CERTIFICATE REQUEST-----
   ```

4. Coller ce bloc dans le champ prévu sur le site
5. Ne rien remplir dans "Attributs supplémentaires"

6. Valider la demande
7. Télécharger le fichier `.cer` généré
8. Le copier sur le serveur web sous :

```
/etc/ssl/uranus.corp/web.uranus.corp.cer
```

⚙️ Étape 3 – Création du VirtualHost HTTPS Apache

Sur le serveur web, créer le fichier suivant :

```
nano /etc/apache2/sites-available/uranus-logistique.conf
```

Contenu :

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/extranet.uranus.corp

    ErrorLog ${APACHE_LOG_DIR}/uranus-logistique_error.log
    CustomLog ${APACHE_LOG_DIR}/uranus-logistique_access.log combine
d

    SSLEngine on
    SSLCertificateFile /etc/ssl/uranus.corp/web.uranus.corp.cer
    SSLCertificateKeyFile /etc/ssl/uranus.corp/uranus.corp.key
</VirtualHost>
```

✅ Étape 4 – Activation du site et du SSL

Activer le module SSL et le site Apache :

```
a2enmod ssl
a2ensite uranus-logistique.conf
systemctl reload apache2
```

🧭 Étape 5 – Configuration DNS (Active Directory)

Dans le **DNS Windows**, créer un enregistrement de type **A** :

Nom	Type	Adresse IP
intranet	A	172.17.3.10

> Cela permet aux clients internes de résoudre intranet.uranus.corp vers ton serveur web.

🔎 Étape 6 – Vérification dans un navigateur

Depuis un poste client :

- Accéder à : `https://extranet.uranus.corp`
- Le site doit s'afficher en HTTPS 🔒

✅ Conclusion

Ce projet avait pour objectif de déployer un **site vitrine simple, fonctionnel et sécurisé** pour l'entreprise fictive **Uranus**, dans un environnement réseau structuré.