Mission 10 :

Sécurité des échanges

Introduction :

Les serveur RDS utilise des certificat afin de pouvoir se connecter à l'interface web de façons sécurisé par le protocole HTTPS. Pour ce projet nous configureront le protocole HTTPS afin d'accéder à notre site web par un certificat. Il nous demande également de créer un accès FTP. Cette connexion nécessite l'utilisation de SSL.

Objectifs :

Mise en place d'un certificat web afin de sécuriser la connexion de notre site web s'appuyant sur le protocole HTTPS

Mise en place d'un serveur FTP afin de sécuriser la connexion en s'appuyant sur le protocole SLL

Contrainte :

-Un serveur ISS fonctionnelle

-Un AD avec une autorité de certification

-Un serveur FTP

-Certificat validé par une autorité de certification

Démarche :

I-Configuration d'un certificat pour le site web.

- Duplication du certificat "Serveur Web"
- Configuration du nouveaux modèle de certificats : nom ; publication du certificat dans l'AD ; autorisation de l'exportation de clé privé.
- Création d'un nouveau modèle de certificat à délivrer à partir des modèle crée
- Depuis le gestionnaire de certificats : Personnel -> Certificats, faire une demande d'un nouveau certificat
- Sélection du certificat précédemment crée, pour l'inscrire
- Ajout du "Nom commun" à partir des propriétés du certificat
- Exportation du nouveau certificat inscris
- Exportation de la clé privée
- Protection de la clé privé avec un mot de passe
- Sauvegarde du fichier de certificat (*.pfx) dans le dossier de partage

II-Ajout du certificats dans le Gestionnaire du serveur web

III- Lier le certificat au site Web et à port

Cliquer sur liaison

Cliquer sur ADD setting for web-site

Type = HTTPS Port 443 (pour les connexion en HTTPS)

Sélectionner lui le certificat créer précédemment

Test

A partir d'un navigateur saisir le fqdn de notre site web. SI tous cela vas bien nous devrions nous connecter sur notre site web. Celui-ci seras protéger par un certificat qui a été délivré pars notre autorité de certification

V-Installation du rôle FTP

VI- Configuration d’un certificat web pour les connexion en FTP :

- Duplication du certificat “Serveur Web”
- Configuration du nouveaux modèle de certificats : nom ; publication du certificat dans l’AD ; autorisation de l’exportation de clé privé.
- Création d’un nouveau modèle de certificat à délivrer à partir des modèle crée
- Depuis le gestionnaire de certificats : Personnel -> Certificats, faire une demande d’un nouveau certificat
- Sélection du certificat précédemment crée, pour l’inscrire
- Ajout du “Nom commun” à partir des propriétés du certificat
- Exportation du nouveau certificat inscris
- Exportation de la clé privée
- Protection de la clé privé avec un mot de passe
- Sauvegarde du fichier de certificat (*.pfx) dans le dossier de partage

VII-Ajout du certificats dans le Gestionnaire du serveur web

VIII-Paramétrer la publication d’un site internet

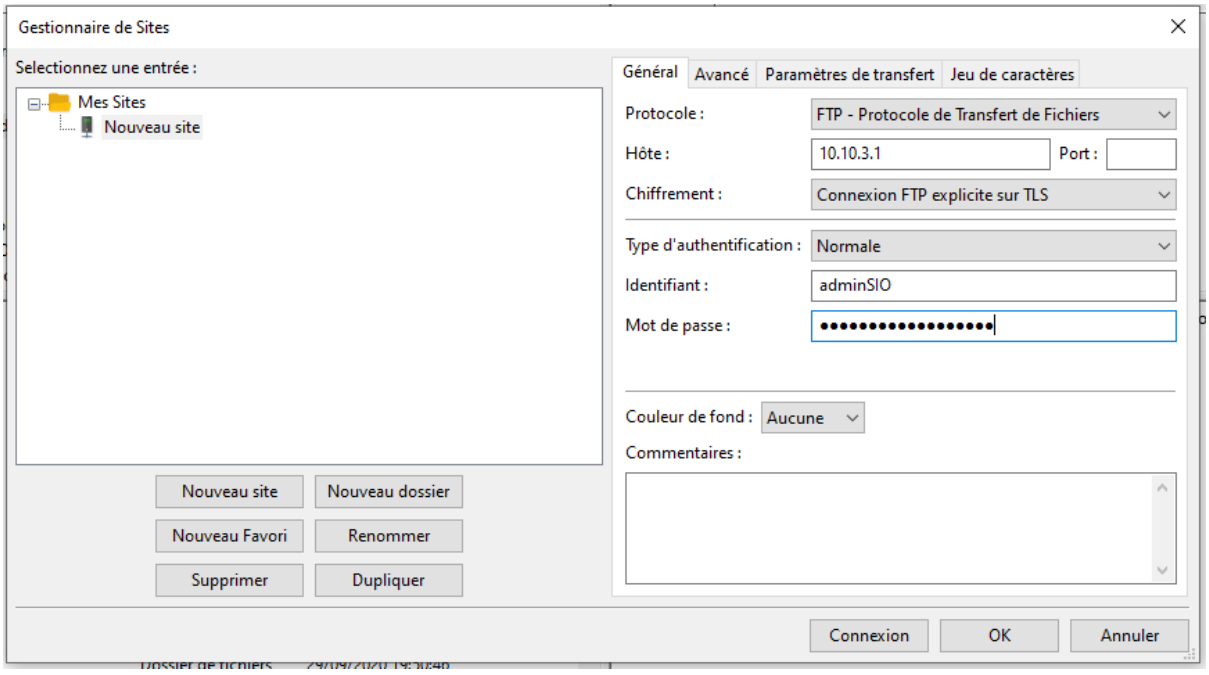
- Configurer la liaison
- Renseigner le port
- Dans la partie SSL cocher exiger les certificat SSL
- Sélectionner le certificat créer précédemment pour les connexions en SSL

- Cocher Authenfication de Base pour permettre la connexion qu'au utilisateur de l'AD
- Autoriser l'accès au utilisateur de l'active directory en lecture,ecriture.

Test

Connection a partir depuis un navigateur sur notre serveur en utilisant le fqdn via le protocole HTTPS :

Connection depuis Filezilla depuis notre FTP via une connexion FTP explicite sur TLS. En saisissant un utilisateur de L'AD



Filezilla va ouvrir une connexion sécurisée à notre FTP en utilisant une connexion FTO explicite sur TLS et en s'appuyant sur le certificat. Afin de savoir que l'on s'authentifie bien au bon serveur.