PPE 2 : Mise en place d'une infrastructure sécurisée avec PKI

SOMMAIRE

1 OBJET DU DOCUMENT 3
1.1 Introduction 3
1.2 Problématique 3
1.3 Matériel / environnement utilisé 3
1.4 Résumé de la solution 3
1.5 Schéma simplifié de l'infrastructure 4
2 POSTES / SERVICES 4
2.1 Client Windows 4
3 SERVEUR WINDOWS: SRV-AD-CRT 4
3.1 Active Directory 4
3.1.1 Compte Utilisateurs 5
3.2 Service DNS 5
3.3 PKI (AD CS) 5
3.4 Serveur Web IIS 5
3.4.1 Objectif : 5
3.4.2 Accès : 5
3.5 Serveur de fichiers 5
3.5.1 Accès : 5
4 SERVEUR WEB LINUX : WEB-LINUX 6
4.1 Présentation 6
4.2 Services installés 6
4.3 Fonctionnement 6
4.4 Intégration 6
5 TESTS ET VALIDATION 7
5.1 Tests réalisés 7
6 CONCLUSION 7

1 OBJET DU DOCUMENT

1.1 Introduction

Dans le cadre de son développement, l'entreprise souhaite sécuriser ses services, ses données et ses utilisateurs à l'aide d'une infrastructure basée sur une PKI interne.
L'objectif est de garantir :

- La confidentialité des échanges
- L'authentification des services
- L'intégrité des données

1.2 Problématique

Sans système de certificats, les services web ne sont pas sécurisés et les données peuvent être exposées.
Cela entraîne :

- Des risques de sécurité (attaques, interception)
- Une absence de confiance dans les services
- Une mauvaise protection des données

La problématique est donc :

➔ Comment sécuriser les services, les données et les utilisateurs à l'aide d'une PKI interne et de certificats numériques ?

1.3 Matériel / environnement utilisé

Pour réaliser ce projet :

- VMware (virtualisation)

Machines utilisées :

- 1 Serveur Windows: SRV-AD-CRT (192.168.200.10)
- 1 serveur Linux : WEB-LINUX (192.168.200.40)
- 1 poste client : CLIENT-W11 (192.168.200.100)

1.4 Résumé de la solution

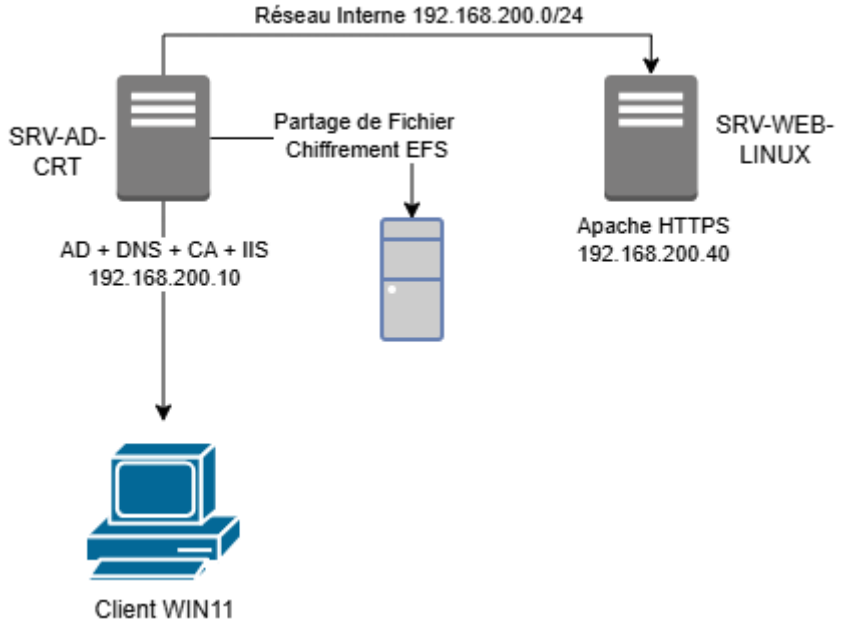
Le serveur Windows assure plusieurs rôles :

- Active Directory : gestion des utilisateurs
- DNS : résolution de noms
- PKI (AD CS) : génération de certificats
- IIS : site web sécurisé en HTTPS
- Serveur de fichiers : stockage sécurisé

Un serveur Linux est utilisé pour héberger un site web sécurisé en HTTPS.
Les certificats sont utilisés pour :

- Sécuriser les services web (HTTPS)
- Chiffrer les données (EFS)
- Assurer la confiance entre les machines

1.5 Schéma simplifié de l'infrastructure



2 POSTES / SERVICES

2.1 Client Windows

Le poste CLIENT-W11 permet :

- De tester l'accès aux services web sécurisés
- De vérifier les certificats
- D'accéder aux partages réseau

Il est intégré au domaine ppe.local.

3 SERVEUR WINDOWS: SRV-AD-CRT

3.1 Active Directory

Le serveur est configuré comme contrôleur de domaine.
Domaine :

ppe.local

- **Objectifs :**
- Centraliser la gestion des utilisateurs
- Gérer les ordinateurs du réseau
- Faciliter l'administration

3.1.1 Compte Utilisateurs

Nom	Identifiant
Marie FRANCE	m.france
Bob Martin	b.martin
Admin	administrateur

3.2 Service DNS

Le serveur DNS permet de résoudre :

- Intranet.ppe.local
- www.ppe.local

3.3 PKI (AD CS)

Une autorité de certification interne est mise en place.
Elle permet :

- La création de certificats serveur
- La création de certificats utilisateur

3.4 Serveur Web IIS

Le serveur IIS est configuré en HTTPS.

3.4.1 Objectif :

- Sécuriser l'accès à l'intranet
- Utiliser un certificat signé par la CA

3.4.2 Accès :

https://intranet.ppe.local

3.5 Serveur de fichiers

Un partage est configuré :
C:\Partages\Commun

3.5.1 Accès :

- Lecture / écriture pour les utilisateurs

Les fichiers sont sécurisés avec EFS :

- Chiffrement basé sur certificat utilisateur
- Accès limité aux utilisateurs autorisés

4 SERVEUR WEB LINUX : WEB-LINUX

4.1 Présentation

Serveur Linux dédié à l'hébergement web.

4.2 Services installés

- Apache2
- OpenSSL

4.3 Fonctionnement

Le serveur propose un site web sécurisé :

https://www.ppe.local

Le certificat utilisé est signé par la CA Windows.

4.4 Intégration

Le serveur Linux est intégré dans l'infrastructure :

- Communication sécurisée HTTPS
- Confiance via certificats

5 TESTS ET VALIDATION

5.1 Tests réalisés

✓ Test 1 : Domaine
Connexion avec un compte AD → OK
✓ Test 2 : DNS
Ping des serveurs → OK
✓ Test 3 : HTTPS IIS
Accès sécurisé avec cadenas → OK
✓ Test 4 : HTTPS Linux
Accès sécurisé → OK
✓ Test 5 : Certificats
Certificats reconnus par le client → OK
✓ Test 6 : Partage fichiers
Accès au dossier partagé → OK

6 CONCLUSION

Ce PPE a permis de mettre en place une infrastructure sécurisée basée sur une PKI interne.
Les services sont protégés grâce au protocole HTTPS, les données sont sécurisées par chiffrement et les utilisateurs sont gérés de manière centralisée.
Cette solution permet d'assurer la confidentialité, l'intégrité et l'authentification au sein du réseau.