Ledoux
Antoine
SIO26

PPE 2

L'entreprise ANTOX

Sécurisation des données de services et utilisateur à l'aide de certificats d'une PKI

Présentation de la situation

L'entreprise ANTOX , située à Paris, possède un petit réseau informatique composé d'un contrôleur de domaine, d'un serveur web hébergeant un intranet et d'une quinzaine de postes utilisateurs reliés à Active Directory. Les employés utilisent quotidiennement cet intranet pour consulter des documents et se connecter avec leurs identifiants professionnels.

Actuellement, le site fonctionne en HTTP, ce qui signifie que les données échangées (identifiants, mots de passe) ne sont pas sécurisées et peuvent être interceptées sur le réseau local. L'objectif est donc de sécuriser ces échanges en mettant en place une solution simple basée sur une PKI, sans utiliser de VPN.

Mise en place de la solution

Pour répondre au besoin, l'administrateur installe une autorité de certification (PKI) sur un serveur Windows de l'entreprise via les Services de certificats Active Directory. Cette autorité permet de créer et de signer des certificats numériques utilisés pour sécuriser les communications. Elle devient une source de confiance pour tous les ordinateurs du domaine.

Un certificat est ensuite généré pour le serveur web hébergeant l'intranet. Ce certificat est installé dans IIS afin d'activer le protocole HTTPS. Une fois configuré, le site intranet n'est plus accessible en HTTP mais en HTTPS, ce qui permet de chiffrer les données échangées entre les utilisateurs et le serveur.

Afin d'éviter les alertes de sécurité dans les navigateurs, le certificat racine de la PKI est déployé automatiquement sur tous les postes du domaine grâce à une stratégie de groupe (GPO). Les ordinateurs reconnaissent alors l'autorité de certification comme fiable, ce qui permet un accès sécurisé sans message d'erreur.

Dans une optique de renforcement de la sécurité, il est également possible de mettre en place des certificats utilisateurs. Chaque employé possède alors un certificat personnel installé sur son poste, permettant d'ajouter une authentification forte en complément du mot de passe.

Résultats et conclusion

Grâce à la mise en place de cette solution, l'entreprise a pu sécuriser son intranet de manière simple et efficace. Les communications sont désormais chiffrées via HTTPS, ce qui garantit la confidentialité des données échangées.

L'utilisation d'une PKI interne permet également de garantir l'identité du serveur et de simplifier la gestion des certificats au sein du réseau. Enfin, l'ajout de certificats utilisateurs permet de renforcer l'authentification et de limiter les risques d'usurpation d'identité.

Domaine : Promeo.local

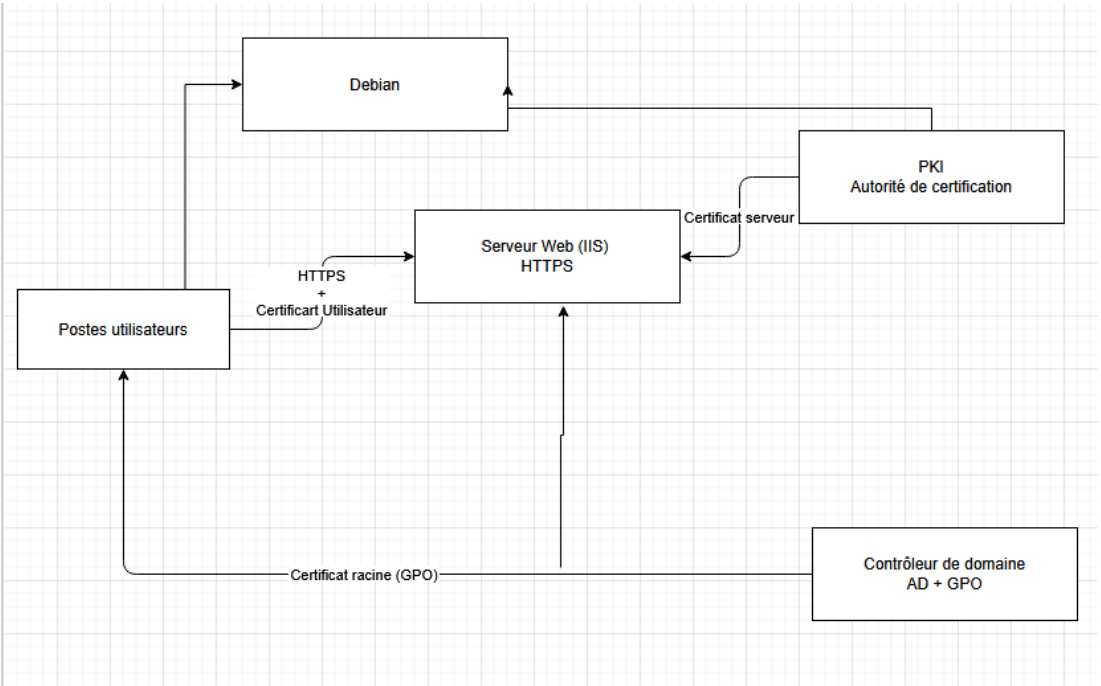
Tableau Adresse IP :

Matériel	Nom	IP
Serveur Windows	PPE 2 WDS	192.168.1.10
Windows	PPE 2 W	192.168.1.12
Serveur Web	PPE 2 WWEB	192.168.1.11
Debian	PPE 2 Debian	192.168.1.100

Tableau Mot de passe :

Localisation	Nom	Mot De Passe
PPE WDS	admin	Promeo60!
PPE W	admin	Promeo60!
PPE WWE	admin	Promeo60!
PPE Debian	admin	Promeo60!
PPE WDS	User	Promeo60!
PPE W	User	Promeo60!
PPE WWE	User	Promeo60!
PPE Debian	User	Promeo60!

Schémas :


Debian
PKI
Autorité de certification
Certificat serveur
Serveur Web (IIS)
HTTPS
HTTPS
+
Certificart Utilisateur
Postes utilisateurs
Certificat racine (GPO)
Contrôleur de domaine
AD + GPO