Mise en place d'un tunnel OpenVPN avec certificats AD CS

Sommaire

Cahier des charges – Expression des besoins

Descriptif de l'existant

L'infrastructure est inexistante, j'ai seulement accès à une sortie Internet via le LAN du GRETA.

Besoin(s)

Dans le cadre d'un TP pédagogique, je dois mettre en place un serveur OpenVPN dans un sous-réseau et un serveur Active Directory avec AD CS *(Active Directory Certificate Services)* dans un autre sous-réseau. Le serveur VPN devra utiliser des certificats émis par l'autorité de certification AD CS pour authentifier les clients. Je dois également configurer un routeur sous pfSense pour simuler un routeur d'entreprise avec des règles NAT et fournir un accès sécurisé à Internet ainsi qu'aux ressources internes via le VPN.

Contrainte(s)

J'ai 8 heures pour mettre en place cette solution et tester le bon fonctionnement de l'authentification par certificats, l'accès VPN sécurisé et la connectivité aux ressources internes.

Ressources

Ressources mises à disposition

J'ai à ma disposition une machine hôte qui possède Hyper-V comme logiciel de virtualisation. De plus, j'ai accès au réseau LAN du GRETA, ce qui me permet d'avoir un accès à Internet.

Ressources nécessaires à la mise en place

J'ai besoin d'une machine hôte qui possède un logiciel de virtualisation, d'un accès à Internet, ainsi que des ISO de Debian 13, Windows Server 2025 et Windows 11.

Gestion des ressources

J'ai déjà à ma disposition les ISO de Windows 11, Windows Server 2025 ainsi que celui de Debian 13.

Analyse

Descriptifs des solutions

OpenVPN est une solution VPN open-source reconnue pour sa robustesse et sa flexibilité. Elle permet de créer des tunnels chiffrés sécurisés entre des clients distants et un réseau d'entreprise. OpenVPN supporte différents modes d'authentification, notamment l'authentification par certificats X.509 via une PKI *(Public Key Infrastructure)*. Cette solution s'intègre parfaitement avec Active Directory Certificate Services *(AD CS)*, permettant une gestion centralisée des certificats utilisateurs et serveurs. OpenVPN utilise le chiffrement SSL/TLS, offre une compatibilité multiplateforme *(Windows, Linux, macOS, Android, iOS)*. Son architecture modulaire et sa configuration flexible en font un choix privilégié pour les environnements professionnels nécessitant une sécurité renforcée.

WireGuard est une solution VPN moderne et minimaliste qui se distingue par sa simplicité et ses performances exceptionnelles. Développé avec une approche de sécurité par conception, WireGuard utilise des algorithmes cryptographiques modernes (Curve25519, ChaCha20, Poly1305) et propose un code source extrêmement compact (environ 4 000 lignes contre plus de 100 000 pour OpenVPN), facilitant ainsi les audits de sécurité. Il offre des temps de connexion quasi instantanés et une consommation CPU réduite. WireGuard est désormais intégré nativement dans le noyau Linux et dispose de clients officiels pour toutes les plateformes majeures. Cependant, sa gestion des certificats et son intégration avec une PKI existante comme AD CS sont moins matures que celles d'OpenVPN, et son modèle de configuration basé sur des clés statiques peut nécessiter des outils additionnels pour une gestion centralisée en entreprise.

Comparaison des solutions (tableau)

Fonctionnalités	**OpenVPN**	**WireGuard**
Coûts	Gratuit, open-source.	Gratuit, open-source.
Intégration PKI / AD CS	Excellente, support natif des certificats X.509.	Limitée, nécessite des outils tiers pour gérer les certificats avec AD CS.
Facilité d'installation et de configuration	Moyenne, nécessite une configuration détaillée mais très documentée.	Simple, configuration minimaliste avec peu de paramètres.
Performances	Bonnes, mais consommation CPU plus élevée.	Excellentes, très rapide avec faible latence et consommation CPU réduite.
Protocoles et chiffrement	SSL/TLS, AES-256, SHA256, configurables.	ChaCha20, Poly1305, Curve25519, non configurables (sécurité par défaut).
Compatibilité multiplateforme	Excellente : Windows, Linux, macOS, Android, iOS, routeurs.	Excellente : Windows, Linux, macOS, Android, iOS, intégré au noyau Linux.
Gestion centralisée des utilisateurs	Native via AD CS et GPO, distribution automatique des certificats.	Nécessite des outils externes, gestion manuelle des clés par défaut.
Audit et logs	Logs détaillés, traçabilité complète des connexions et événements.	Logs basiques, moins de détails sur les événements.
Révocation de certificats	Support natif via CRL et OCSP avec AD CS.	Pas de support natif, nécessite des scripts personnalisés.
Complexité du code	Code volumineux (~100 000 lignes), plus de surface d'attaque potentielle.	Code compact (~4 000 lignes), facilite les audits de sécurité.

Choix d'une solution - Argumentation

J'ai choisi OpenVPN car il s'agit d'une solution qui s'intègre parfaitement avec Active Directory Certificate Services *(AD CS)*. Cette intégration native permet une gestion centralisée et automatisée des certificats utilisateurs via les GPO *(Group Policy Objects)*, ce qui simplifie considérablement l'administration dans un environnement Windows. OpenVPN offre également une authentification forte basée sur les certificats X.509, éliminant les risques liés aux mots de passe faibles. Sa flexibilité de configuration permet de mettre en place des politiques de sécurité avancées. Bien que WireGuard soit plus performant en termes de vitesse et de légèreté, son intégration avec une PKI d'entreprise existante est moins aboutie et nécessiterait des développements supplémentaires pour atteindre le niveau d'automatisation offert par OpenVPN avec AD CS.

Plan d'adressage - Schéma - Tables de routage

- Tableau d'adressage :

Nom du réseau	@ réseau	Masque	1er @ IP	Dernière @ IP	@ broadcast	Passerelle	Nombre d'hôtes
WAN	192.168.1.0	255.255.255.0 (/24)	192.168.1.1	192.168.1.254	192.168.1.255	192.168.1.254	254
SR-01	192.168.0.0	255.255.255.0 (/24)	192.168.0.1	192.168.0.254	192.168.0.255	192.168.0.254	254
SR-02	192.168.2.0	255.255.255.0 (/24)	192.168.2.1	192.168.2.254	192.168.2.255	192.168.2.254	254
VPN	10.8.0.0	255.255.255.0 (/24)	10.8.0.1	10.8.0.254	10.8.0.255	10.8.0.1	254

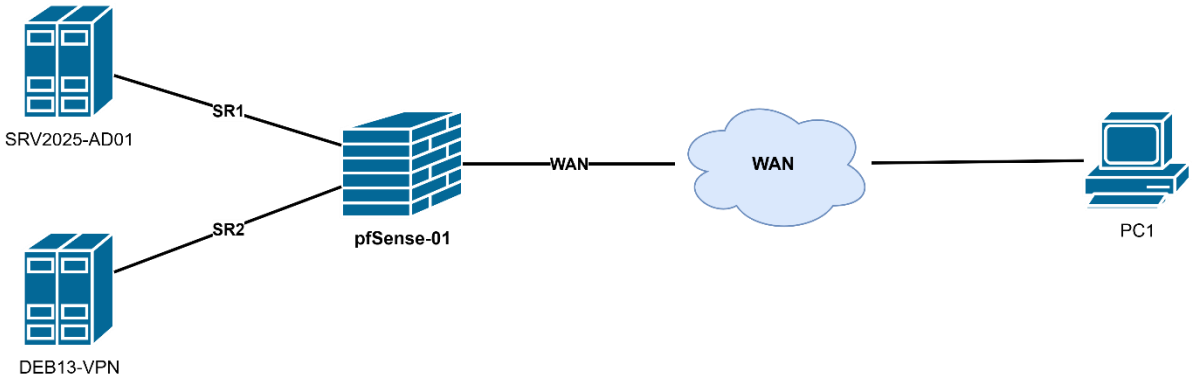
- Tableau des IP :

Réseau \ Équipement	pfSense-01	SRV2025-AD01	DEB13-VPN	W11-01
WAN	192.168.1.2			DHCP
SR-01	192.168.0.254	192.168.0.1		
SR-02	192.168.2.254		192.168.0.2	
VPN			10.8.0.1	DHCP

- Table de routage de pfSense-01 :

@ réseau	Masque réseau	@ passerelle	@ interface
0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.2
192.168.0.0	255.255.255.0	192.168.0.254	192.168.0.254
192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.2
192.168.2.0	255.255.255.0	192.168.2.254	192.168.2.254

- Schéma du réseau :



Étude de l'impact sur le SI existant

L'intégration d'un VPN OpenVPN avec authentification par certificats AD CS dans une infrastructure réseau représente une amélioration significative de la sécurité et de la flexibilité d'accès aux ressources de l'entreprise. Cette solution apporte un accès distant sécurisé, renforce l'authentification des utilisateurs et impacte les aspects techniques, organisationnels, stratégiques et humains du système d'information.

- **Impact technique :**

La mise en place d'OpenVPN avec AD CS nécessite l'installation et la configuration d'un serveur VPN sous Debian 13, d'une autorité de certification intégrée à Active Directory (AD CS) et d'un routeur pfSense pour gérer le NAT et le filtrage. L'infrastructure PKI (Public Key Infrastructure) doit être correctement paramétrer pour émettre, distribuer et révoquer les certificats clients et serveurs.

Cette architecture impose une gestion rigoureuse des certificats : création de modèles de certificats spécifiques (serveur et client), configuration de l'inscription automatique via GPO, export et conversion des certificats au format compatible OpenVPN. Le serveur VPN doit être configuré avec les bons paramètres cryptographiques (chiffrement AES-256, authentification SHA256, TLS 1.2 minimum).

Le bon fonctionnement du VPN dépend de la stabilité du serveur AD CS (point central de confiance), de la disponibilité du serveur OpenVPN, et de la configuration réseau (routage IP, NAT, règles de pare-feu sur pfSense). Une mauvaise configuration des certificats, une révocation non propagée ou une expiration non anticipée peuvent entraîner des interruptions de service pour les utilisateurs distants.

- **Impact organisationnel :**

L'arrivée d'une solution VPN basée sur certificats impose de revoir les procédures d'administration. Les équipes IT doivent désormais gérer un cycle de vie complet des certificats : émission, renouvellement, révocation en cas de départ d'un employé ou de

compromission. La distribution des certificats aux utilisateurs doit être automatisée via GPO pour éviter les manipulations manuelles et les erreurs.

Les procédures de support utilisateur doivent être adaptées pour gérer les problématiques liées aux certificats expirés, aux erreurs de connexion VPN, et aux configurations clients (installation d'OpenVPN GUI, import du fichier .ovpn). Une documentation claire et des guides utilisateurs sont indispensables pour faciliter l'adoption de la solution.

La gestion des groupes Active Directory devient stratégique : seuls les utilisateurs membres du groupe autorisé *(DL_Utilisateurs-VPN)* reçoivent automatiquement leur certificat client et peuvent se connecter au VPN. Toute modification des droits d'accès doit donc passer par une gestion rigoureuse des appartenances aux groupes AD.

- **Impact stratégique :**

OpenVPN avec AD CS renforce considérablement la sécurité d'accès distant. L'authentification forte par certificats élimine les risques liés aux mots de passe faibles ou réutilisés, et réduit la surface d'attaque en cas de tentative d'intrusion. Le chiffrement de bout en bout protège les données sensibles transitant entre les utilisateurs distants et le réseau d'entreprise.

Cette solution améliore la continuité d'activité en permettant aux collaborateurs de travailler à distance de manière sécurisée, que ce soit en télétravail, en déplacement ou depuis des sites distants. L'accès aux ressources internes (serveurs de fichiers, applications métier, bases de données) devient transparent pour les utilisateurs autorisés, quel que soit leur emplacement géographique.

L'intégration avec AD CS simplifie également la conformité réglementaire (RGPD, normes sectorielles) en offrant une traçabilité complète des accès via les logs OpenVPN et une gestion centralisée des identités numériques. La révocation instantanée d'un certificat permet de bloquer immédiatement l'accès d'un utilisateur sans avoir à changer de mot de passe partagé.

- **Impact humain :**

Les équipes techniques doivent monter en compétence sur plusieurs aspects : gestion d'une PKI d'entreprise, administration d'OpenVPN sous Linux, configuration de pfSense, et dépannage des problématiques liées aux certificats. Une formation sur les bonnes pratiques de sécurité des clés privées et sur la gestion des certificats est nécessaire.

Les administrateurs doivent être capables de diagnostiquer rapidement les incidents : certificat expiré, clé privée corrompue, problème de synchronisation GPO, erreur de configuration OpenVPN, ou blocage pare-feu. La rigueur devient essentielle, car une mauvaise manipulation sur l'autorité de certification peut compromettre l'ensemble de l'infrastructure PKI.

Du côté des utilisateurs finaux, l'expérience doit rester simple malgré la complexité technique sous-jacente. L'inscription automatique des certificats via GPO et la configuration universelle du fichier .ovpn permettent de minimiser les interventions manuelles. Néanmoins, une sensibilisation à la sécurité est nécessaire pour que les utilisateurs comprennent l'importance de protéger leur certificat et ne pas le partager.

- **Impact juridique :**

L'utilisation de certificats numériques pour l'authentification VPN renforce la traçabilité et la responsabilisation des utilisateurs. Chaque certificat est nominatif et lié à un compte utilisateur Active Directory, permettant d'identifier précisément qui s'est connecté, quand et depuis où. Ces informations sont essentielles en cas d'audit de sécurité ou d'enquête interne.

La mise en place d'une PKI impose également des obligations de conservation et de protection des journaux d'événements : logs de l'autorité de certification (émission, révocation), logs du serveur OpenVPN (connexions, déconnexions, erreurs), et logs du pare-feu pfSense. Ces données doivent être conservées de manière sécurisée et conforme au RGPD, notamment en termes de durée de conservation et de droit d'accès.

En cas de compromission d'un certificat ou de départ d'un employé, la procédure de révocation doit être appliquée rapidement et documentée. La liste de révocation de certificats (CRL) ou le protocole OCSP doivent être correctement configurés pour que les certificats révoqués ne puissent plus être utilisés.

Phasage de l'intervention

Je commencerai par installer et configurer le routeur pfSense avec les règles NAT et de pare-feu nécessaires pour rediriger le trafic VPN vers le serveur OpenVPN. Ensuite, je déploierai le serveur Active Directory avec AD CS, je créerai les modèles de certificats (serveur et client), et je configurerai l'inscription automatique via GPO pour les utilisateurs autorisés. Puis, j'installerai le serveur OpenVPN sous Debian 13, je générerai et transférerai les certificats depuis AD CS, et je configurerai le service VPN avec les paramètres de sécurité appropriés. Pour finir, je créerai le fichier de configuration client .ovpn universel et je le distribuerai aux utilisateurs pour qu'ils puissent se connecter au VPN avec leur certificat.

Prévision des tests de validation

Les tests de validation sont détaillés dans la procédure disponible sur Notion via le lien fourni dans la section "Mise en place". Ils incluent la vérification du bon fonctionnement de l'autorité de certification AD CS, la distribution automatique des certificats via GPO, l'authentification réussie d'un utilisateur autorisé au VPN, le rejet d'un utilisateur non autorisé, et l'accès aux ressources internes depuis le tunnel VPN.

Mise en place

La mise en place a été rédigée sur Notion, elle est accessible via le lien suivant : https://mathys-demon.notion.site/Proc-dure-configuration-d-OpenVPN-avec-certificats-AD-CS-3028102ecdc980a4914ad57bc2d18d0e.

Bilan

Conclusion

L'installation du serveur OpenVPN avec authentification par certificats AD CS fonctionne en respectant le délai imparti de 8 heures. Les tests de connexion se sont déroulés correctement : les utilisateurs autorisés reçoivent automatiquement leur certificat via GPO et peuvent se connecter au VPN de manière transparente, tandis que les utilisateurs non autorisés sont correctement bloqués. L'accès aux ressources internes via le tunnel VPN est fonctionnel et sécurisé.

Auto-évaluation

J'ai réussi à correctement installer et configurer l'infrastructure VPN avec AD CS. La mise en place de la PKI et la création des modèles de certificats ont été bien maîtrisées. J'ai rencontré quelques difficultés lors de la conversion des certificats au format PEM pour OpenVPN, notamment avec la gestion des clés privées chiffrées, mais j'ai pu résoudre ces problèmes en utilisant les commandes OpenSSL appropriées. L'automatisation de la distribution des certificats via GPO a fonctionné du premier coup, ce qui a considérablement simplifié le déploiement côté client. À l'avenir, j'essaierai d'anticiper davantage les problématiques liées à la compatibilité des formats de certificats entre Windows et Linux pour gagner du temps lors de la configuration.