Mise en place d'un accès distant sécurisé via OpenVPN sur NAS Synology

L'Excellence de l'Aide à Domicile

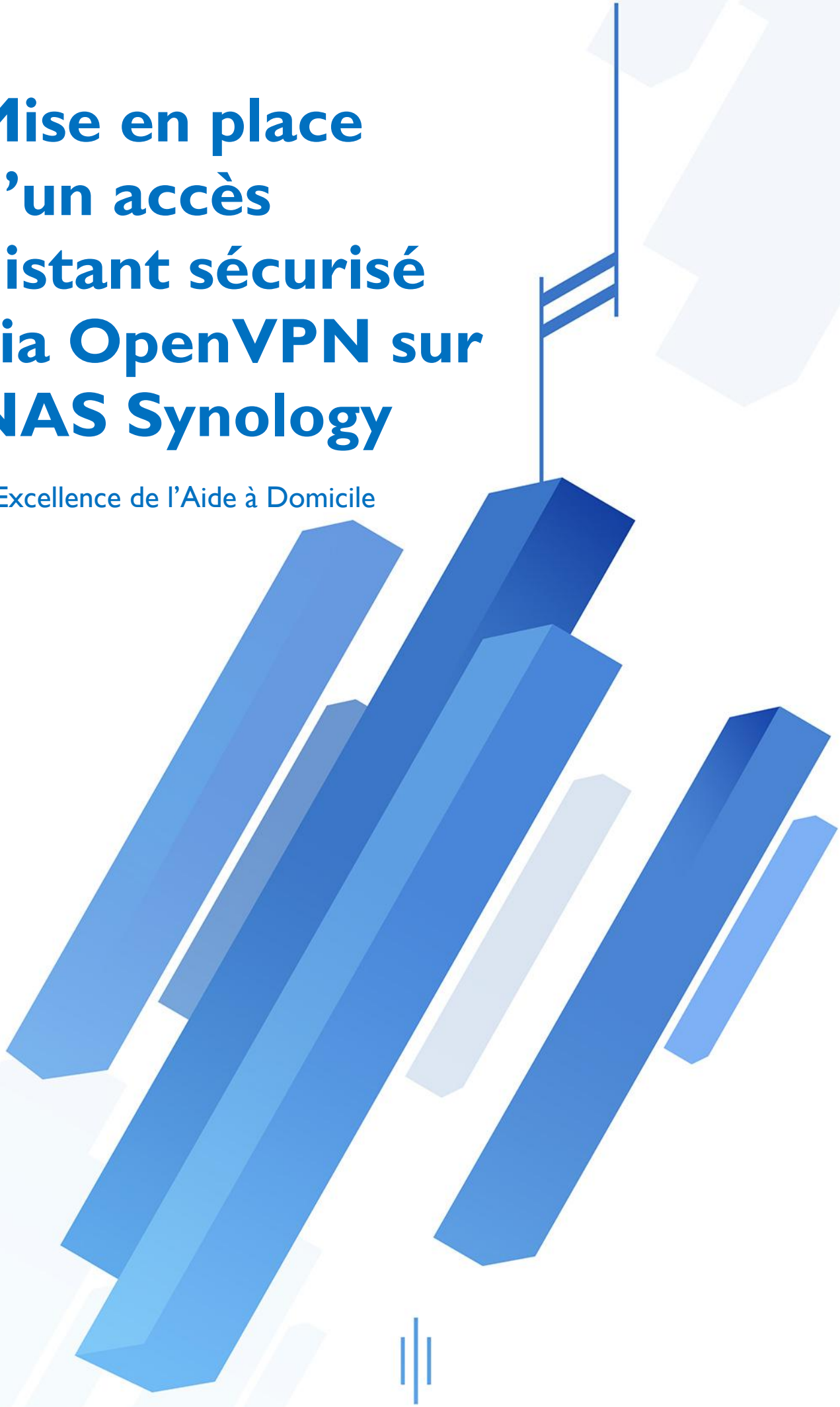

Table des matières

Situation professionnelle

Mise en place d'un accès distant sécurisé via OpenVPN sur NAS Synology

Présentation de la situation professionnelle

À la suite de la mise en place du serveur NAS Synology au sein de l'entreprise L'Excellence de l'Aide à Domicile, un nouveau besoin est apparu : permettre un accès distant sécurisé aux ressources internes pour la direction, notamment en situation de mobilité ou de télétravail.

L'objectif n'était pas seulement de permettre un accès aux fichiers, mais de le faire dans un cadre sécurisé, maîtrisé et conforme aux bonnes pratiques de sécurité. J'ai donc été chargé de concevoir et de mettre en œuvre une solution d'accès distant basée sur le protocole OpenVPN, en utilisant le NAS Synology comme point de terminaison VPN.

Cette mission s'inscrivait dans une logique de sécurisation globale du système d'information, amorcée lors du déploiement du NAS.

Contexte et situation existante

Après la centralisation des données sur le NAS, l'accès aux fichiers était parfaitement opérationnel en local via le réseau interne. En revanche, dès lors qu'un membre de la direction souhaitait travailler depuis l'extérieur, l'accès devenait plus complexe.

Le service QuickConnect de Synology permettait un accès distant simplifié, mais cette solution, bien que pratique, restait dépendante d'un service tiers et ne donnait pas un contrôle total sur l'exposition des services internes. Dans un contexte professionnel manipulant des données sensibles (informations salariés, données bénéficiaires), il était préférable d'opter pour une solution plus robuste.

L'enjeu était donc de permettre aux utilisateurs autorisés d'accéder au réseau interne comme s'ils étaient physiquement présents au bureau, tout en garantissant la confidentialité des échanges et en limitant l'exposition des services sur Internet.

Expression du besoin

Le besoin exprimé par la direction était clair : pouvoir consulter et modifier les documents hébergés sur le NAS depuis l'extérieur, sans complexité excessive, tout en assurant un haut niveau de sécurité.

La solution devait être stable, compatible avec des postes Windows et éventuellement des appareils mobiles, et ne pas nécessiter d'infrastructure supplémentaire coûteuse. Elle devait également s'intégrer proprement dans l'architecture existante.

Contraintes identifiées

Plusieurs contraintes ont orienté mes choix techniques. La connexion Internet de l'entreprise reposait sur une box opérateur standard, sans équipement de pare-feu dédié à ce stade. Il fallait donc configurer correctement la redirection de ports et limiter l'exposition aux seuls services nécessaires.

La solution devait rester compréhensible et administrable par mes soins, sans introduire une complexité excessive pour une petite structure. Enfin, la configuration devait être suffisamment sécurisée pour éviter les erreurs classiques, comme l'utilisation de ports par défaut facilement détectables.

Analyse et choix de la solution

Plusieurs solutions d'accès distant étaient envisageables : mise en place d'un VPN directement sur un pare-feu dédié, utilisation exclusive de QuickConnect, ou déploiement du service VPN intégré au NAS.

Compte tenu de l'infrastructure en place et du niveau de maturité du système d'information, j'ai retenu la solution OpenVPN intégrée au paquet "VPN Server" de Synology. Cette solution permet de créer un tunnel chiffré entre l'utilisateur distant et le réseau local, garantissant la confidentialité des données échangées.

OpenVPN présente plusieurs avantages : il est reconnu pour sa fiabilité, son niveau de sécurité, et sa compatibilité multiplateforme. De plus, il permet une gestion fine des autorisations et un contrôle total sur les accès.

Mise en œuvre technique

La première étape a consisté à installer le paquet "VPN Server" depuis le centre de paquets du NAS Synology. Une fois le service activé, j'ai configuré OpenVPN en veillant à désactiver la compression, afin d'éviter certaines vulnérabilités connues, et à autoriser l'accès au réseau local pour les clients connectés.

Ensuite, j'ai configuré la box opérateur afin de mettre en place une redirection de port vers le NAS. Par mesure de sécurité, j'ai évité d'utiliser strictement les ports par défaut lorsqu'il était possible de les modifier, afin de limiter les risques liés aux scans automatisés.

Une fois la configuration serveur finalisée, j'ai exporté le fichier de configuration OpenVPN généré par le NAS. Ce fichier a été modifié pour intégrer l'adresse publique ou le nom de domaine associé au service, puis importé dans le client OpenVPN installé sur le poste distant.

Après l'importation du profil et l'authentification avec les identifiants utilisateur définis sur le NAS, le tunnel VPN s'est établi correctement, permettant à l'utilisateur d'accéder aux ressources internes comme s'il était connecté en local.

Tests et validation

Plusieurs tests ont été réalisés afin de valider la solution. Une fois connecté via OpenVPN depuis un réseau externe, j'ai vérifié l'accès aux dossiers partagés du NAS, la consultation de fichiers, ainsi que la stabilité de la connexion sur une période prolongée.

J'ai également contrôlé que l'utilisateur distant obtenait bien une adresse IP issue du réseau VPN et que le routage vers le réseau interne fonctionnait correctement. Les journaux du NAS ont été consultés afin de vérifier l'absence d'erreurs ou de tentatives de connexion suspectes.

Les tests se sont révélés concluants : l'accès distant était fonctionnel, stable et sécurisé.

Impact sur le système d'information

La mise en place d'OpenVPN a renforcé la sécurité globale du système d'information. Les accès distants ne passent plus par une simple interface web exposée, mais par un tunnel chiffré nécessitant une authentification nominative.

Cela permet une meilleure maîtrise des accès, une traçabilité des connexions et une réduction significative de la surface d'exposition des services internes. L'entreprise bénéficie désormais d'un accès distant professionnel, comparable à celui utilisé dans des environnements plus structurés.

Bilan et retour d'expérience

Cette situation professionnelle m'a permis de travailler sur la mise en place d'un accès distant sécurisé dans un contexte réel, en prenant en compte à la fois les contraintes techniques et les enjeux de sécurité.

J'ai consolidé mes compétences en configuration de services VPN, en gestion de redirection de ports, en sécurisation d'infrastructures exposées à Internet et en analyse des risques liés à l'accès distant.

Au-delà de l'aspect technique, cette mission m'a également permis de mesurer l'importance de l'anticipation des failles potentielles et de l'application des bonnes pratiques de cybersécurité, même dans une structure de petite taille.

La solution déployée offre aujourd'hui à la direction une mobilité sécurisée et maîtrisée, tout en s'intégrant de manière cohérente dans l'architecture mise en place précédemment.