Nadir DJEDIDEN
Nassim BENBOUHAMOU
Ismael BAHRI

FONCTIONNALITES D'UN NAS

DJEDIDEN Nadir
[NOM DE LA SOCIETE]

PLAN :

Document 2 :

II. Etude sur les principales fonctionnalités d'un serveur Nas

a. Qu'est-ce qu'un serveur Nas :

Le NAS, ou Network Attached Storage, est un appareil de stockage autonome qui peut se connecter à votre réseau privé ou professionnel via Internet. Il permet de sauvegarder, partager, sécuriser mais aussi de faciliter l'accès à vos fichiers depuis plusieurs appareils en même temps. Il constitue ainsi un atout pratique pour rendre le travail en équipe plus efficace ou partager plus facilement des photos et des vidéos entre les membres de la famille.

Le NAS peut être utilisée dans la vie privée pour sauvegarder ses photos, jeux vidéo ou encore films.

Pour résumer cela, le Nas c'est, de la sauvegarde de données et leurs sécurisations principalement, il permet également le partage de données et bien sur les données du Nas sont très facile d'accès puisqu'il est connecter à internet.

b. De quoi est composé un NAS :

Fonctionnant comme un disque dur externe, mais offrant davantage de sécurité, le serveur NAS se compose d'un boîtier comprenant différents emplacements appelés des baies, ainsi qu'un ou plusieurs disques durs installés à l'intérieur. Le nombre de baies dépend de vos besoins d'espace de stockage, mais aussi de la configuration souhaitée en termes de sécurisation des données : différents niveaux de sécurité, déterminés par une technologie qu'on appelle RAID, sont disponibles. Un câble d'alimentation, un ventilateur, un processeur, de la RAM et une carte mère viennent compléter le tout.

Ce composant est la carte RAID, elle permet de choisir une solution de stockage, la carte contient un système intelligent appelé raid qui permet de choisir plusieurs configurations pour sauvegarder ses données. Le choix devra être fais selon le besoin de l'entreprise ou du client et le niveau de sécurisation des données.

c. Les fonctionnalités offertes par un serveur NAS

Le boîtier NAS offre diverses fonctionnalités clés :

Sauvegarde de données :

- Stockage illimité grâce aux disques durs et au nombre de baies du boîtier.
- Protection contre la perte de données, incluant photos, documents, vidéos, et plus encore.

Usage multimédia :

- Serveur multimédia permettant l'accès aux contenus (films, vidéos, musiques) via le réseau.
- Possibilité de transcodage en temps réel pour une lecture fluide.

Stockage dans le Cloud et partage :

- Synchronisation des données entre tous les appareils via le système Cloud Station.
- Partage simplifié des fichiers, avec mise à jour automatique sur toutes les copies.

Contrôle de la vidéosurveillance :

- Gestion de la vidéosurveillance avec la possibilité d'ajouter plusieurs caméras IP.
- Fonctionnalité adaptée tant aux particuliers qu'aux professionnels.

Mise en place d'un serveur mail :

- Gestion centralisée des mails avec Synology Mail Server.
- Interface web conviviale pour faciliter la visualisation, la gestion, et l'envoi de messages.

Hébergement d'un site web :

- Hébergement de sites web personnels ou professionnels.
- Prise en charge de PHP et MariaDB pour l'utilisation d'applications comme phpMyAdmin ou WordPress via WebStation.

Chiffrage des données :

Les NAS offrent plusieurs méthodes de chiffrement pour assurer la sécurité des données, parmi eux le plus courantes sont :

1. Le Chiffrement des Données en Repos (Data-at-Rest Encryption) :

   Les données stockées sur le NAS sont sécurisées grâce à l'utilisation de l'algorithme AES (Advanced Encryption Standard), un choix courant pour sa sécurité élevée et sa large adoption.

2. Chiffrement des Données en Transit (Data-in-Transit Encryption) :

Le NAS assure la sécurité des échanges de données entre lui-même et les appareils clients en utilisant les protocoles SSL/TLS (Secure Sockets Layer/Transport Layer Security). Ces protocoles garantissent une transmission sur des données sur le réseau.

3. Chiffrement de Système de Fichiers :

Certains NAS intègrent BitLocker, un outil de chiffrement de disque complet fréquemment utilisé sur les systèmes Windows. Par ailleurs, le standard LUKS (Linux Unified Key Setup) est déployé sur les systèmes Linux pour garantir la sécurité des systèmes de fichiers.

4. Chiffrement au Niveau du Dossier ou du Fichier :

Pour une sécurité accrue, certains NAS offrent la possibilité de chiffrer des dossiers spécifiques ou des fichiers individuels. Cette fonctionnalité permet une protection ciblée des données sensibles.

5. Chiffrement Matériel vs Logiciel :

Certains NAS optimisent la vitesse de chiffrement en prenant en charge le chiffrement matériel, tandis que d'autres offrent une flexibilité accrue avec le chiffrement logiciel. Ces choix permettent d'adapter la sécurité du NAS aux besoins spécifiques de l'utilisateur.

Sur les outils de chiffrements nous allons approfondir les chiffrements symétrique et asymétrique :

Chiffrement symétrique (materiel ou logiciel, exemple aes qui utilise le chiffrement symétrique) :

Le chiffrement symétrique est une méthode de chiffrement où la même clé est utilisée à la fois pour chiffrer et déchiffrer les données. Cela signifie que l'émetteur et le destinataire des données partagent la même clé secrète, et cette clé est utilisée à la fois pour protéger les données lors de leur transmission et pour les rendre à nouveau lisibles une fois qu'elles ont été reçues.

Les caractéristiques clés du chiffrement symétrique incluent :

- Une seule clé qui est utilisée à la fois pour le chiffrement et le déchiffrement.

- La rapidité du chiffrement symétrique est généralement plus rapide que le chiffrement asymétrique, car il n'implique qu'une seule clé.

Le chiffrement symétrique est souvent utilisé pour sécuriser la confidentialité des données en transit (comme dans les protocoles SSL/TLS) et des données stockées (comme dans le chiffrement des disques durs).

L’algorithme AES est largement utilisé dans le chiffrement Symétrique.

L’AES est utilisé pour sécuriser les données sensibles dans divers contextes, notamment les communications sécurisées ou AES est utilisée dans des protocoles sécurisées tel que SSL et TLS, lors de chiffrement de disques durs et autre support de stockage, pour le chiffrement de fichier.

En conclusion le chiffrement AES est un algorithme de chiffrement symétrique utilisé essentiellement pour assurer la sécurité des données et leurs confidentialités.

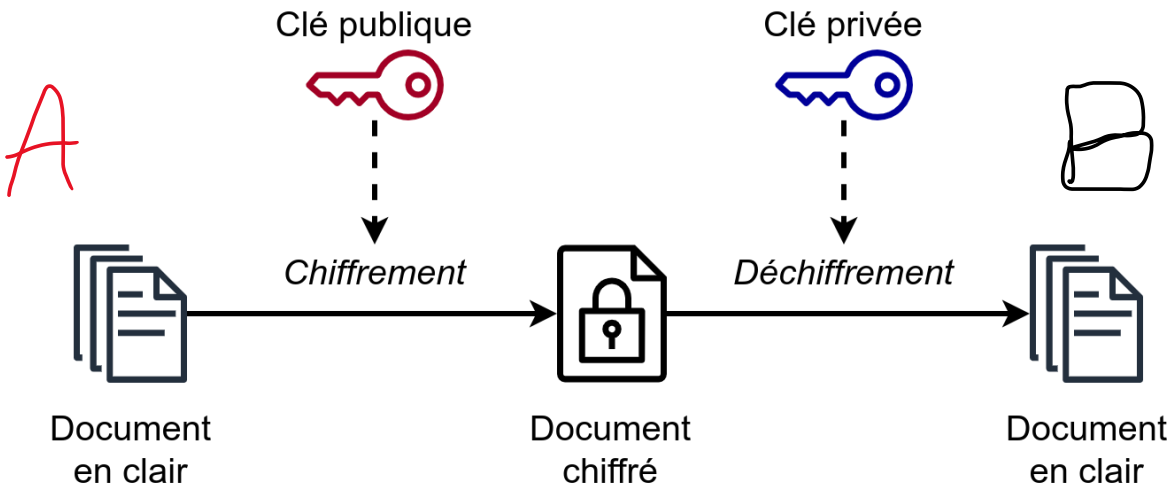
Chiffrement asymétrique (ssl / tls) :

Le chiffrement asymétrique est une méthode de chiffrement qui utilise une paire de clés distinctes, une clé publique et une clé privée, pour le processus de chiffrement et de déchiffrement. Contrairement au chiffrement symétrique, où une seule clé est utilisée pour les deux opérations, le chiffrement asymétrique offre un niveau supplémentaire de sécurité en utilisant des clés distinctes.

Le chiffrement asymétrique utilise quant à lui deux clés différentes, chaque utilisateur possède un pair de clés, une clé publique qu'il partage publiquement et une clé privée qu'il garde secrète. Les données chiffrer avec la clé publique peuvent uniquement être déchiffrées avec la clé privée correspondante et vice versa, cela offre une sécurité significative.

De plus, le chiffrement asymétrique est souvent utilisé dans les signatures numériques, on utilise une clé privée et une clé publique, pour garantir l'authenticité et l'intégrité d'un document ou d'un message.

Voici un exemple de chiffrement asymétrique :



Ici la personne A chiffre un document en clair avant de l'envoyer à la personne B a l'aide d'une clé publique, cela permet de s'assurer que seulement la personne B pourra le lire et le modifier, comme le message est chiffré, même s'il tombe aux mains d'un hackeur il pourra voir le message mais pas le décrypter, seule la personne B pourra lire le message grâce a la clé Privée. Ainsi la personne B pourra notamment s'assurer de l'authenticité du document.