FTP, FTPS et SFTP

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

FTP utilise un canal de commande et des connexions de données séparées. Le canal de commande utilise habituellement TCP 21. En mode actif, le serveur initie la connexion de données ; en mode passif, le client rejoint un port annoncé par le serveur.

FTPS ajoute TLS à FTP. SFTP fonctionne via SSH et constitue un protocole différent. Les ports et règles de filtrage de FTP ne peuvent donc pas être repris automatiquement pour SFTP.

2. Publication en DMZ

Dans cet exemple, l'objectif est de rendre un service FTP accessible depuis le WAN. Identifier d'abord le logiciel serveur et le mode de transfert retenu. Pour un fonctionnement passif, définir une plage de ports de données et l'adresse annoncée aux clients, puis rendre les règles NAT et de filtrage cohérentes.

L'ouverture du seul port 21 peut permettre l'authentification sans permettre la liste des répertoires ou les transferts.

3. Recette

1. Tester une connexion depuis un client externe autorisé.
2. Vérifier la liste des fichiers.
3. Télécharger un fichier de test et contrôler son intégrité.
4. Vérifier les droits d'écriture selon le rôle du compte.
5. Confirmer le refus des actions non autorisées.

4. Dépannage

Une connexion établie suivie d'un blocage lors du transfert oriente vers les canaux de données. Comparer les ports négociés aux règles actives et vérifier le chemin retour.

FTP sans protection expose les identifiants et les données. Le choix d'un protocole chiffré doit être documenté selon les contraintes du service, sans considérer un compte de test comme une protection suffisante.

5. Références

- IETF — protocole FTP
- OpenSSH — transferts via SSH

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=services:transfert_fichiers

Last update: **2026/10/18 01:23**