Besoin client : Entreprise PiedPiper

Contexte

PiedPiper est une entreprise spécialisée dans les solutions de compression de données. Elle cherche à moderniser son infrastructure réseau pour améliorer la performance, la sécurité et la gestion de ses ressources. Avec la croissance de ses effectifs et l'augmentation de la quantité de données à gérer, l'entreprise a besoin d'une infrastructure réseau fiable, segmentée et supervisée, tout en permettant une centralisation des données via un NAS. L'objectif est de concevoir et mettre en œuvre une solution réseau complète intégrant un pare-feu, un routeur, des VLAN, un serveur Windows, un serveur de stockage ainsi qu'un système de supervision.

Objectifs

1. **Mettre en place une infrastructure réseau** incluant un pare-feu **PFSENSE** et un routeur **CISCO**, permettant la création et la gestion de VLAN pour une meilleure isolation des services et des départements.
2. **Déployer un serveur Windows** centralisant la gestion des utilisateurs, des postes de travail et des configurations réseau via les services DHCP, Active Directory et GPO.
3. **Mettre en œuvre un système de supervision** pour surveiller les équipements critiques et garantir une disponibilité optimale.
4. **Installer et configurer un NAS** pour le stockage centralisé et sécurisé des données d'entreprise.

Cahier des charges

1. Infrastructure réseau

- **Pare-feu PFSENSE :**
  - Mise en place d'un pare-feu PFSENSE pour gérer le trafic réseau et les règles de sécurité.
  - Création de règles spécifiques pour protéger les flux entre les VLAN et les services critiques (ex. : NAS, Active Directory).
- **Routeur CISCO :**
  - Configuration des VLAN sur le routeur pour segmenter les différents départements :
    - VLAN 10 : Administration
    - VLAN 20 : Développement
    - VLAN 30 : Ressources Humaines
    - VLAN 40 : Stockage (NAS)
  - Implémentation de la communication inter-VLAN pour les flux nécessaires avec contrôle strict via des ACL (Access Control Lists).
- **Switch :**
  - Configuration des ports pour l'assignation des VLAN aux équipements réseau.
  - Mise en place de trunks pour assurer la connectivité entre le routeur et le switch.

2. Serveur Windows

- **DHCP (Dynamic Host Configuration Protocol)** :
  - Configuration pour attribuer dynamiquement des adresses IP aux équipements connectés, en fonction des VLAN.

- **Active Directory (AD)** :
    - Mise en place d'un domaine pour centraliser la gestion des comptes utilisateurs et des groupes.
    - Création de groupes spécifiques par département, avec des permissions adaptées aux ressources (Administration, Développement, RH).
- **GPO (Group Policy Objects)** :
    - Déploiement de stratégies de groupe pour sécuriser les postes de travail (ex. : restrictions logicielles, politiques de mots de passe).
    - Automatisation de la configuration réseau pour les utilisateurs (ex. : mappage des lecteurs réseau vers le NAS).

3. Supervision réseau

- **Outil de supervision :**
    - Installation d'un système de monitoring réseau tel que **Zabbix**, **Nagios**, **PRTG** ou **Observium** pour surveiller :
        - L'état des équipements critiques (PFSENSE, routeur CISCO, switch, serveur Windows, NAS).
        - Les performances réseau (bande passante, utilisation CPU/mémoire des équipements).
        - Etat stockage NAS).
    - Configuration d'alertes pour notifier les administrateurs en cas de panne ou d'anomalie par mail ou autre.

4. NAS (Network Attached Storage)

- **Configuration et intégration :**
    - Installation et configuration d'un NAS pour :
        - Le stockage centralisé des fichiers.
        - L'intégration avec l'Active Directory pour gérer les droits d'accès par utilisateur et groupe.
    - Mise en place d'une structure de dossiers par département pour organiser les fichiers de manière logique et sécurisée.

Contraintes techniques

1. **Sécurité :**
    - Mise en place de règles de pare-feu strictes via PFSENSE pour protéger les services critiques.
    - Sécurisation des VLAN pour limiter les accès non autorisés.
2. **Évolutivité :**
    - Préparer l'infrastructure à accueillir des utilisateurs supplémentaires ou de nouveaux VLAN à l'avenir.
3. **Documentation :**
    - Fournir une documentation détaillée incluant :
        - Le schéma réseau.
        - Les configurations des équipements (PFSENSE, CISCO, Switch).
        - Les procédures de maintenance et d'ajout de nouveaux services.

Livrables attendus

1. **Pare-feu PFSENSE** configuré pour gérer les règles de sécurité et les connexions VPN.

2. **Routeur CISCO** opérationnel avec des VLAN configurés selon les besoins de l'entreprise.
3. **Switch** configuré pour assurer la connectivité des VLAN et le routage vers les équipements critiques.
4. **Serveur Windows** fonctionnel, avec DHCP, Active Directory et GPO configurés.
5. **Système de supervision** actif, incluant des alertes et un tableau de bord pour le suivi des performances.
6. **NAS** installé, configuré, et accessible via des permissions définies par l'Active Directory.
7. Une **documentation complète** décrivant l'installation, les configurations, et les recommandations de maintenance.