Liste des tâches

A ajouter : Sécurité de couche 2 (port sec, DHCP snooping, DAI, ...)

Serveur Web dans la DMZ

ACL

1. **Documenter**

1. DRP (Plan de Reprise d'Activité), Plan de sauvegarde

- Développer un plan détaillé pour restaurer les opérations après une panne majeure.

- Créer un plan de sauvegarde pour assurer la disponibilité et l'intégrité des données critiques.

2. Créer un plan d’adressage

- Concevoir une structure logique pour l'attribution des adresses IP afin d'optimiser l'efficacité du réseau.

3. Créer un schéma topologique

- Dessiner une représentation graphique de l'infrastructure réseau pour une meilleure compréhension et gestion.

4. Documenter et faire un journal de bord

- Tenir un journal décrivant les modifications apportées au réseau pour une traçabilité et une gestion efficace.

5. S'informer sur les dernières vulnérabilités des OS

- Effectuer une veille régulière sur les vulnérabilités et les correctifs des systèmes d'exploitation pour assurer la sécurité du réseau.

6. Créer un schéma de redondance

- Concevoir un plan de redondance pour assurer la disponibilité continue des services en cas de défaillance matériel ou logiciel.

1. **Configurer sur périphérique**

1. Automatisation du plan de sauvegarde

- Mettre en place des scripts ou des outils pour automatiser le processus de sauvegarde des configurations périphériques.

2. Configurer le DRP

- Configurer les périphériques conformément au plan de reprise d'activité pour une restauration rapide en cas de sinistre.

3. Configurer l'accès aux périphériques

* Créer des comptes user/admin
* Adressage IP des interfaces
* Accès ssh/https

4. Configuration IP.

- Configurer les adresses IP soit :

* En utilisant DHCP pour une allocation dynamique
* En les fixant manuellement pour une attribution statique.
* Configurer les passerelles (gateways)

- Définir les passerelles par défaut pour permettre aux périphériques de communiquer avec des réseaux externes.

5. Configurer le routage

- Mettre en place des routes pour permettre la communication entre différents réseaux.

* Routage statique
  + Route par défaut
* Routage dynamique
  + EIGRP
  + OSPF
  + ~~BGP~~

6. Configurer les VLANs (Virtual Local Area Networks)

- Diviser le réseau en segments logiques pour améliorer la performance et la sécurité.

7. Configurer les VPNs (Virtual Private Networks)

- Pour relier les différents WAN entre eux

- Mettre en place des tunnels sécurisés pour permettre l'accès distant aux ressources réseau.

-> Protocole : IPsec

8. Configurer les permissions et les privilèges

- Définir les autorisations d'accès aux ressources réseau pour garantir la confidentialité et l'intégrité des données.

9. Sécuriser les périphériques et les accès externes :

* Appliquer des mesures de sécurité telles que la désactivation des services non essentiels
* Désactivation des services inutiles
* Mise en place d’authentification forte (MFA)
* Chiffrement des communication (TLS)
* Contrôle d’accès
* Revues de sécurité régulière

10. Configurer les pares-feux :

- Définir des règles de filtrage pour contrôler le trafic entrant et sortant et protéger le réseau contre les menaces externes.

- Définition des règles de filtrage --> trop vague : règle de pare-feu + filtrage Web + Contrôle d’application

- Règles de pare-feu :

- Règles entrantes (http, HTTPS)

- règles sortantes

- Négation par défaut

- Filtrage web

- Catégories de sites à bloquer ou autoriser

- Liste noires et blanches

- Analyse du contenu pour détecter et bloquer les menaces potentielles

- Contrôle d’application

- Identification des applications

- Politiques par application

- Gestion de la bande passante

- Segmentation du réseau

- Mettre en place une DMZ

- NAT

11. Mettre à jour les périphériques si nécessaire

- Appliquer les correctifs de sécurité et les mises à jour logicielles pour combler les vulnérabilités et améliorer les performances.

13. Tolérance aux pannes

- Mettre en place des mécanismes de redondance pour assurer la continuité du service en cas de défaillance matérielle tels que :

* Identifier les composants critiques en premier
* HSRP (Hot Standby Router Protocol) pour assurer la continuité du service en cas de défaillance matérielle
* Mettre en place de la redondance physique (serveurs miroirs, routeurs doublés, liaisons montantes multiples)
* Agrégation de liens : Etherchannel pour combiner plusieurs liens physiques en un seul lien logique
* Plan de basculement : Etablir des plans de basculement automatiques ou manuels pour les services critiques pour assurer une transition transparente vers des systèmes de secours en cas de panne
* Tests de redondance : effectuer régulièrement des tests de redondance pour vérifier l’efficacité des mécanismes de redondance
* Documenter tout
* Mettre en place système de surveillance et alertes

14. Optimiser le réseau

* + EIGRP
  + OSPF
  + ~~BGP~~
* Configuration du bail
* Placer les logs sur un serveur pour alléger les routeurs
* Spécifier la bande passante pour tel ou tel périphériques
* Service de compression du cache et envoyer vers serveur

15. Mise en place du monitoring

- Installer des outils de surveillance pour surveiller les performances du réseau et détecter les problèmes potentiels

16. Rendre le réseau modulable

- Concevoir une architecture réseau flexible pour s'adapter aux besoins futurs de l'entreprise.

17. Test de pénétration et évaluation de la sécurité

- Effectuer des tests de sécurité réguliers pour identifier et corriger les vulnérabilités potentielles dans le réseau.

18. Sécurité de couche 2

- Port security : limite le nb d’adresses MAC autorisées sur un port donné

- DHCP snooping : différencie les ports fiables et non fiables connectés au DHCP

- Dynamic ARP Inspection (DAI) : inspecte les paquets ARP traversant les ports non fiables, vérifie que chaque adresse MAC correspond à l’adresse IP enregistrée dans une table de liaison DHCP snooping sécurisée.