Mise en place de l'infrastructure réseau de l'unité de maternité

Contexte

L'hôpital d'Argenteuil s'agrandit et installe une nouvelle unité de maternité dans un bâtiment flambant neuf. Pour garantir un fonctionnement optimal et sécurisé des équipements informatiques, l'hôpital a fait appel à vos services en tant que techniciens réseau pour concevoir et déployer l'infrastructure réseau nécessaire.

Votre mission consiste à :

1. **Créer des VLANs dédiés** pour chaque catégorie de personnel :
   - **Service infirmier**
   - **Service médecin**
   - **Poste de sécurité**

2. **Configurer un routeur** afin de répondre aux besoins suivants :
   - Fournir un **réseau Wi-Fi 2,4 GHz accessible aux invités**, protégé par un mot de passe respectant les règles minimales de sécurité (longueur minimale, mélange de caractères, etc.).
   - Fournir un **réseau Wi-Fi 5 GHz caché**, exclusivement réservé au personnel (médecins et infirmiers), avec un mot de passe renforcé conforme aux bonnes pratiques de cybersécurité (longueur, complexité, absence de mots communs, renouvellement).

3. **Mettre à jour les paramètres essentiels du routeur** pour assurer son bon fonctionnement et sa sécurité :
   - Activation du pare-feu intégré.
   - Modification des identifiants par défaut pour l'administration du routeur.
   - Application des dernières mises à jour du firmware.

Votre travail devra garantir :

- Une séparation claire des réseaux pour la sécurité et la confidentialité des données.
- Une connectivité stable et efficace pour tous les utilisateurs.
- Un réseau invité sécurisé tout en étant facile d'accès.

À vous de jouer pour fournir une solution performante et adaptée aux besoins de ce nouveau bâtiment de l'hôpital !

Problématique

Comment concevoir et mettre en œuvre une infrastructure réseau fiable et sécurisée, adaptée aux besoins spécifiques d'un hôpital, tout en respectant les normes de cybersécurité et en assurant une connectivité fluide pour différents utilisateurs (médecins, infirmiers, poste de sécurité et invités) ?

Objectif pédagogique

- Comprendre et appliquer les principes de segmentation réseau à l'aide de VLANs pour garantir la sécurité et la gestion du trafic dans une infrastructure réseau professionnelle.
- Configurer un routeur afin de mettre en place des réseaux Wi-Fi adaptés aux besoins spécifiques des utilisateurs (invités, médecins, infirmiers).
- Renforcer la cybersécurité des équipements réseaux en configurant des mots de passe sécurisés et en appliquant les bonnes pratiques de gestion des routeurs.
- Tester et valider le bon fonctionnement de l'infrastructure réseau configurée.

Préparation du TP

Architecture réseau à réaliser

VLAN	ID	Description	Equipements
Medecin	10	Réseau des médecins	5 PC + 1 imprimante + 2 machines médicalisées
Infirmier	20	Réseau des infirmiers	3 PC + 2 imprimantes
Agent_securite	30	Réseau des agents de sécurité	2 PC + Caméra IP + Enregistreur (NVR)
Invites	40	Réseau des invités extérieurs	Jusqu'à 148 Machines (PCs, Smartphone…)

Déroulement du TP

Partie 1 : Configuration des VLAN sur le Switch

Etapes :

- Connexion au Switch
- Création des VLAN
- Affectation des ports aux VLAN
- Vérification par ligne de commande et test

Questions :

1. Quel est l'intérêt d'utiliser des VLANs dans une infrastructure réseau ?
    - Expliquez en quoi les VLANs améliorent la segmentation et la sécurité d'un réseau.

2. Deux VLANs distincts peuvent-ils communiquer ensemble ?
    - Si oui, quelles sont les solutions ou configurations nécessaires pour permettre cette communication ?

3. Est-il possible de renommer un VLAN après sa création ?
    - Si oui, quelle commande devez-vous utiliser pour modifier le nom d'un VLAN existant ?

Partie 2 : Configuration du mode trunk

Étapes :

- Connexion au switch
- Accédez au mode configuration
- Configure terminal
- Sélectionnez l'interface ou le groupe d'interfaces à configurer en mode trunk
- Configurez le port en mode trunk
- Spécifiez les VLAN autorisés
- Ajoutez une balise VLAN native (facultatif) :
    - Par défaut, le VLAN 1 est le VLAN natif. Si nécessaire, vous pouvez changer le VLAN natif pour éviter les problèmes de sécurité
- Sauvegardez la configuration
- Vérification de la configuration
    - Affichez la configuration de l'interface :
    - Vérifiez les ports trunk actifs

Questions :

1. Qu'est-ce que le mode trunk sur un switch et pourquoi est-il utilisé dans une infrastructure réseau avec plusieurs VLAN ?

2. Quel est l’intérêt de restreindre les VLAN autorisés sur un port configuré en mode trunk ?

3. Qu'est-ce que le VLAN natif dans un trunk, et pourquoi est-il recommandé de le changer par défaut ?

Partie 3 : Configuration du routeur

Étape : Configuration des interfaces VLAN sur le routeur

- **Connectez-vous à l'interface de configuration du routeur.**
- **Configurer les VLAN conformément à ceux créés sur le switch :**
  - Assurez-vous que le port reliant le switch au routeur est configuré en mode **trunk** sur le switch (vérification Partie 2).
  - Configurez les sous-interfaces VLAN sur le routeur :
    - Accédez à la section "VLAN Settings" ou "LAN" de l'interface du routeur.
    - Créez 4 VLANs avec leurs ID respectifs et associez-les à des sous-réseaux IP :
      VLAN 10 (Médecins) : 192.168.10.0/24
      VLAN 20 (Infirmiers) : 192.168.20.0/24
      VLAN 30 (Agents de sécurité) : 192.168.30.0/24
      VLAN 40 (Invités) : 192.168.40.0/24
    - Assignez une adresse IP pour chaque VLAN sur le routeur (Passerelle) :
      VLAN 10 : 192.168.10.1
      VLAN 20 : 192.168.20.1
      VLAN 30 : 192.168.30.1
      VLAN 40 : 192.168.40.1

- **Activer le routage inter-VLAN :**
  - Activez le **routage inter-VLAN** pour permettre la communication entre les VLAN si nécessaire (exemple : entre médecins et infirmiers).
    - Sur un routeur, cela se fait souvent dans les paramètres de routage ou NAT.
    - Assurez-vous que les règles NAT ou ACL (Access Control List) n'interdisent pas les flux nécessaires.
- **Configuration des réseaux Wi-Fi :**
  - Créer un réseau Wi-Fi 2,4 GHz pour les invités :
    - Dans les paramètres Wi-Fi du routeur, activez un SSID 2,4 GHz public.
    - Configurez les paramètres suivants :
      Nom du réseau (SSID) : "Maternite_Guest"
      Mot de passe : Respectez les règles de sécurité et justifier votre choix
      Sécurité : Activez la sécurité WPA3 (ou WPA2 si non disponible).

- **Créer un réseau Wi-Fi masqué 5 GHz pour les médecins :**
  - Activez un second SSID sur la bande 5 GHz.
  - Configurez les paramètres suivants :

    Nom du réseau (SSID) : "Medecins_5G"
    Mode : Masquez le SSID pour qu'il ne soit pas visible.
    Mot de passe : Respecter les règles de cybersécurité
    Sécurité : Activez la sécurité WPA3 (ou WPA2 si non disponible).

- **Configuration des fonctionnalités supplémentaires :**
  - Configurer le DHCP :

    Activez le serveur DHCP sur chaque VLAN pour attribuer des adresses IP dynamiques dans les sous-réseaux respectifs :

    VLAN 10 : 192.168.10.10 à 192.168.10.100
    VLAN 20 : 192.168.20.50 à 192.168.20.130
    VLAN 30 : 192.168.30.2 à 192.168.30.150

  - Configurer des règles de sécurité (ACL) :

    Bloquez l'accès au réseau des invités vers les autres VLAN (Médecins, Infirmiers, Sécurité).
    Méthode :
    - Accédez à la section ACL ou Firewall.
    - Ajoutez une règle pour chaque VLAN :

      Interdire les flux des invités 192.168.40.0/24 vers les VLAN internes

  - Test de connectivité :

    Testez les réseaux pour vérifier :

    Les PC d'un même VLAN communiquent entre eux.
    Les invités n'ont pas accès aux autres VLAN.
    Le Wi-Fi invité fonctionne avec mot de passe.
    Le Wi-Fi 5 GHz masqué est accessible

- **Sauvegarde de la configuration :**

  Une fois les paramètres vérifiés, sauvegardez la configuration du routeur pour éviter de perdre les modifications en cas de redémarrage.

Questions :

1. Pourquoi est-il important de créer des VLANs distincts pour chaque service (Médecins, Infirmiers, Agents de Sécurité) sur le routeur ?

2. Quelles sont les différences entre le réseau Wi-Fi 2,4 GHz pour les invités et le réseau Wi-Fi 5 GHz masqué pour les médecins et infirmiers en termes de configuration et de sécurité ?

3. Comment pouvez-vous vérifier que le réseau Wi-Fi 5 GHz masqué est correctement configuré et fonctionne uniquement pour les utilisateurs autorisés ?

4. Expliquez le rôle des ACL dans la configuration du routeur. Pourquoi est-il essentiel de restreindre l'accès des invités aux VLAN internes ?

5. Quels paramètres de sécurité supplémentaires pourriez-vous appliquer au mot de passe du réseau Wi-Fi masqué pour qu'il respecte les règles de cybersécurité ?

Partie 4 : Configuration de l'enregistreur et des caméras IP

Objectif :

Configurer un système de vidéosurveillance initialement composé de deux caméras :

- **Caméra 1 :** Salle d'attente
- **Caméra 2 :** Entrée principale

Le service de maternité est accessible au public tous les jours de 7h à 20h30. En dehors de ces horaires, la salle d'attente et l'entrée principale sont, en théorie, inoccupées.

Etapes :

- **Configuration de l'enregistreur (NVR) :**
  - **Adresse IP** : Assignez une adresse IP fixe au NVR dans le sous-réseau dédié aux agents de sécurité.
  - **Connexion des caméras** : Reliez les caméras au NVR et vérifiez que les flux vidéo sont accessibles
  - **Paramètres essentiels** : Configurez les options utiles au bon fonctionnement (date/heure, identifiant/mots de passe, résolution vidéo, paramètres réseau …)
- **Paramétrage des enregistrements vidéo :**
  - **En continu** : Enregistrez le flux vidéo 30 minutes avant l'ouverture et jusqu'à 30 minutes après la fermeture (6h30 - 21h).
  - **Sur détection de mouvement** : En dehors des horaires d'ouverture, activez l'enregistrement uniquement en cas de détection de mouvement.

- **Stockage sécurisé des données :**
  Pour sécuriser les enregistrements réalisés en dehors des horaires de visite :
  - **Captures et vidéos** : Configurez le NVR pour enregistrer les captures d'images et les vidéos détectées dans un dossier sécurisé via un serveur FTP.
  - **Mise en place du serveur FTP :**
    - Installez **FileZilla Server** sur un ordinateur distant.
    - Testez l'accès au serveur FTP depuis une autre machine en utilisant **FileZilla Client**.
  - **Configuration du NVR** : Paramétrez le NVR pour envoyer les fichiers directement vers le serveur FTP.
  - **Vérification** : Testez la fonctionnalité en déclenchant un mouvement et vérifiez que les fichiers s'enregistrent correctement sur le serveur.
- **Accès et visualisation à distance :**
  Visualisation en direct :
  - Accédez au flux vidéo en direct depuis une machine du sous-réseau des agents de sécurité.
  - Vérifiez également l'accès depuis les sous-réseaux des médecins, des infirmiers et des invités.

  Accès aux enregistrements à distance :
  - Configurez l'accès aux enregistrements et au serveur FTP depuis le réseau WAN.
  - Méthode : Effectuez une redirection de port sur le routeur via le NAT pour permettre l'accès externe.

Questions :

1. Quel niveau de sécurité est appliqué sur le serveur FTP (chiffrement, authentification) pour protéger les enregistrements sensibles ?

2. Y a-t-il une politique de rotation ou d'archivage des fichiers sur le serveur FTP pour éviter une surcharge ?

3. Quels ports spécifiques sont ouverts pour l'accès distant, et quelles sont les mesures qui peuvent être prises pour minimiser les risques d'intrusion ?

4. Est-il nécessaire de mettre en place un VPN pour un accès distant sécurisé, en complément de la redirection de port ?

5. Que se passe-t-il si le serveur FTP ou le NVR subit une panne ? Quelle solution mettre en place pour minimiser les risques ?

Partie 4 : Cybersécurité et bonnes pratiques

- **Désactivation des ports inutilisés :**
  Désactivez les ports inutilisés du switch pour empêcher tout accès non autorisé via des connexions physiques non surveillées. Assurez-vous que seuls les ports utilisés par le NVR, les caméras, et les appareils autorisés sont activés.

- **Filtrage des accès avec les ACL :**
  Configurez des listes de contrôle d'accès (ACL) sur le routeur pour limiter les communications :
  - Restreignez l'accès au réseau de vidéosurveillance (VLAN dédié) depuis les autres VLAN du réseau.
  - Autorisez uniquement les flux nécessaires, comme l'accès au NVR depuis le sous-réseau des agents de sécurité ou le serveur FTP.

- **Vérification :**
  Test des connexions entre VLAN :
  - Vérifiez qu'aucune connexion non autorisée n'est possible entre le VLAN vidéosurveillance et les autres VLAN.
  - Testez les restrictions d'accès en tentant de joindre les caméras et le NVR depuis des postes situés hors des VLAN autorisés.

  Test des équipements autorisés :
  - Assurez-vous que les équipements autorisés (ex. : NVR, caméras, PC des agents de sécurité) fonctionnent correctement et peuvent communiquer entre eux sans interruption.

  Audit final :
  - Réalisez un scan de ports pour vérifier que seuls les services essentiels sont actifs sur les équipements du réseau vidéosurveillance.
  - Simulez une tentative d'accès distant pour confirmer que les règles de filtrage et d'authentification fonctionnent comme prévu.