# Projet Cyber B3 – Virtualisation du CHU de Ynov

## Rapport Technique de Mise en Œuvre – Partie Réseau & Sécurité

### Objectif du projet

L'objectif est de concevoir, configurer et virtualiser une architecture réseau sécurisée pour un hôpital fictif (CHU de Ynov), en mettant en œuvre des principes de segmentation, de protection des données et de détection des menaces, en réponse aux exigences définies dans le projet "Cyber B3 2024".

## Architecture réseau proposée

### Segmentation par VLAN

| **VLAN** | **Nom** | **Usage principal** |
| --- | --- | --- |
| 10 | Médical | Appareils médicaux, serveur Web/BDD |
| 20 | Administratif | RH, gestion, serveur DHCP/AD/DNS |
| 30 | Invités | Visiteurs, accès internet uniquement |
| 99 | Management | Administration, IDS/IPS, monitoring |

### Équipements utilisés

* 1 Routeur Cisco (2911) avec sous-interfaces (router-on-a-stick)
* 1 Switch 2960 (avec configuration VLAN)
* 1 Serveur DHCP/AD/DNS (VLAN 20)
* 1 Serveur Web/BDD (VLAN 10)
* 4 PC (un par VLAN)
* 1 PC “IDS/Snort” (VLAN 99)

### Création des VLANs sur le switch

* Vlan 10 Médical
* Vlan 20 Admin
* Vlan 30 Invite
* Vlan 99 Management

### Affectation des ports :

* Interface fa0/1 switchport access vlan 10
* Interface fa0/2 switchport access vlan 20
* Interface fa0/3 switchport access vlan 30
* Interface fa0/4 switchport access vlan 99
* Interface fa0/24 switchport mode trunk

### Configuration du routeur (router-on-a-stick)

* Interface g0/0 no shutdown
* interface g0/0.10
* encapsulation dot1Q 10
* ip address 192.168.10.1 255.255.255.0
* interface g0/0.20
* encapsulation dot1Q 20
* ip address 192.168.20.1 255.255.255.0
* interface g0/0.30
* encapsulation dot1Q 30
* ip address 192.168.30.1 255.255.255.0
* interface g0/0.99
* encapsulation dot1Q 99
* ip address 192.168.99.1 255.255.255.0

### Serveur DHCP centralisé (VLAN 20)

IP statique : 192.168.20.2

Pools DHCP :

* VLAN 10 → 192.168.10.100-150 / GW: 192.168.10.1
* VLAN 20 → 192.168.20.100-150 / GW: 192.168.20.1
* VLAN 30 → 192.168.30.100-150 / GW: 192.168.30.1
* VLAN 99 → 192.168.99.100-150 / GW: 192.168.99.1

### Ajout de ip helper-address sur les interfaces du routeur (sauf VLAN 20) :

interface g0/0.10

ip helper-address 192.168.20.2

### Serveur Web (VLAN 10)

* IP statique : 192.168.10.2
* Service HTTP activé
* Page simulée : “Bienvenue sur le portail médical du CHU de Ynov”
* Test d’accès depuis PC1 via navigateur : http://192.168.10.2

Mise en place des règles de sécurité (ACLs)

Objectifs :

* Bloquer VLAN 30 (invités) vers tous les autres
* Bloquer le trafic de VLAN 10 vers VLAN 30
* Autoriser la communication VLAN 10 ↔ VLAN 20
* Autoriser VLAN 99 partout

### ACLs configurées :

### Bloquer les invités

ip access-list standard BLOCK\_INVITE

deny 192.168.30.0 0.0.0.255

permit any

interface g0/0.30

ip access-group BLOCK\_INVITE in

### Bloquer le médical vers VLAN invité

ip access-list extended MEDICAL\_OUT

deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255

permit ip any any

interface g0/0.10

ip access-group MEDICAL\_OUT in

### Sécurisation du VLAN 30 (Wi-Fi invités)

Le VLAN invité est souvent une **porte d’entrée critique** si mal configuré. On applique ici une sécurité stricte :

**Objectifs :**

* Accès Internet uniquement
* Isolation client à client (éviter l’espionnage entre utilisateurs)
* Authentification possible via portail captif

**Configuration :**

**ACL sur l’interface VLAN 30 :**

**ip access-list extended VLAN30\_OUT**

**deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255**

**deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255**

**deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255**

**permit ip 192.168.30.0 0.0.0.255 any**

### Sécurisation du VLAN 99 (Management) – Whitelist / Blacklist

Ce VLAN contient des équipements critiques (pfSense, Snort, routeur), donc on applique une **politique d’accès stricte**.

**Objectifs :**

* Autoriser uniquement les postes d’administration (IP précises)
* Interdire tous les autres accès par défaut

**Whitelist par IP (ACL sur VLAN 99) :**

ip access-list extended VLAN99\_ADMIN

permit ip host 192.168.99.10 any

permit ip host 192.168.99.11 any

deny ip any any

Ici seuls les postes 192.168.99.10 et .11 peuvent communiquer avec VLAN 99

**Blacklist dynamique :**

Si une machine du VLAN 20 tente un accès réseau non autorisé (scan ou brute-force détecté), son IP peut être bloquée :

ip access-list extended BLOCKED

deny ip host 192.168.20.55 any

permit ip any any

Ce blocage peut être **déclenché automatiquement** par :

* Le **SIEM** (alertes)

### Intégration IDS/IPS

* Un PC dans VLAN 99 représente un poste de monitoring IDS
* Fichier snort\_logs.txt simulant les détections :
* Scan Nmap depuis invité
* Requête HTTP vers /admin
* Tentative de DoS (ICMP flood)
* Positionné en VLAN 99 pour surveiller les flux inter-VLAN et centraliser la détection.

### Simulations de test d'intrusion

PC pentester dans VLAN 99

Simulation de scan avec nmap vers 192.168.10.2 :

nmap -sS -p 21,22,23,80,443 192.168.10.2

Simulation d’un exploit MS17-010 via Metasploit (script ou texte fictif)

Détection par IDS (via logs)

### Gestion des rôles (routeur/switch)

Création d’utilisateurs avec droits limités :

username admin privilege 15 secret SuperAdmin123

username user privilege 1 secret Lecteur

Principe du moindre privilège appliqué aux équipements réseau

## Conclusion

Grâce à cette virtualisation complète :

* L’infrastructure du CHU est segmentée et sécurisée
* Les accès sont filtrés et surveillés
* La distribution d’adresses IP est centralisée et dynamique
* Une solution IDS est simulée pour détecter les comportements anormaux
* Des tests d'intrusion sont réalisés pour valider la solidité de l’architecture

Une image contenant ligne, diagramme, capture d’écran, Parallèle

Le contenu généré par l’IA peut être incorrect.