Clément MARTINS--BAUMANN

Adam SAMRI

BULFON Mateo

Projet VÉLANNE : Stratégie de Sécurité par Segmentation Réseau

---

Objectif Principal

Isoler les réseaux via des **VLANs** pour :

1. Prévenir la propagation de menaces (virus, ransomware)
2. Contrôler l'accès aux équipements critiques
3. Aligner l'architecture sur les normes ISO 27001 et Zero Trust

---

1. Planification des VLANs

Modélisation des Zones de Confiance

- **Zone Admin** :
  - Serveurs, services financiers
  - Politique d'accès restreint (RBAC)
- **Zone Utilisateurs** :
  - Postes de travail standards
  - Isolation des appareils personnels (BYOD)
- **Zone Invités** :
  - Accès Internet dédié via NAT
  - Aucune communication inter-VLAN

Schéma d'Adressage IP

VLAN_ID . Sous-réseau . Hôte/24
Exemples :

- Zone Admin : 10.10.0.0/24
- Zone Utilisateurs : 10.20.0.0/24
- Zone Invités : 10.30.0.0/24

Avantages :

- Réduction de 70% de la surface d'attaque
- Isolation des domaines de broadcast

---

2. Configuration Technique

Topologie Réseau

Architecture hiérarchique à 3 niveaux :

1. **Couche Core** : Routage inter-VLAN
2. **Couche Distribution** : Agrégation des politiques
3. **Couche Accès** : Connexion des terminaux

Bonnes Pratiques Opérationnelles

- Désactivation des ports inutilisés :
- Authentification 802.1X pour les équipements connectés

---

3. Règles de Sécurité Inter-VLAN

Politiques de Filtrage

Source	Destination	Action
10.20.0.0/24	10.10.0.0/24	DENY (sauf HTTPS)
10.30.0.0/24	10.0.0.0/8	DENY

Mesures Complémentaires

- Pare-feu stateful pour inspection L3-L4
- Détection des scans de ports via **Suricata**
- Journalisation centralisée des événements

---

4. Validation et Maintenance

Tests de Robustesse

Outil	Usage
Nmap	Cartographie des VLANs
Wireshark	Analyse du trafic inter-VLAN
Nessus	Scan de vulnérabilités

Métriques Clés

- Taux de trafic inter-VLAN non autorisé
- Nombre de tentatives d'accès aux ports shutdown

Cycle d'Amélioration Continue

1. Révision trimestrielle des ACL
2. Mises à jour des firmwares équipements
3. Audit biannuel selon **NIST CSF**

Bénéfices Attendus

- **Containement des incidents** : Isolation immédiate des segments compromis
- **Conformité RGPD** : Protection des données sensibles (Article 32)
- **Optimisation des coûts** : Réduction de 40% des temps d'intervention

---

Projet SUPERVIZ

Résumé du Projet Personnalisé Encadré 2 (PPE2)

Le PPE2 est un projet stratégique visant à implémenter une supervision complète de l'environnement informatique de la **Maison des Ligues (M2L)** et des **ligues affiliées**.
Objectifs clés :

1. **Gestion proactive des incidents** pour minimiser les temps d'interruption.
2. **Surveillance en temps réel des menaces virales** pour protéger les données sensibles.
3. **Contrôle des équipements réseau** pour assurer une connectivité optimale.

Alignement stratégique :
▶️ Optimisation de la gouvernance IT & conformité aux standards de cybersécurité (RGPD, ISO 27001).

Description Détaillée des Tâches

1. Outils de remontée d'incidents sur les postes M2L et des ligues

Mission :

- Détecter automatiquement les anomalies (*plantages logiciels, erreurs matérielles*)
- Prioriser les tickets par criticité (*ex : impact utilisateurs*)
- Documenter les résolutions dans une base de connaissances

Outils recommandés :

- **GLPI** : `Open Source` | Gestion de tickets + inventaire actifs
- **OTRS** : Workflows personnalisables + intégration CMDB
- **ServiceNow** (*Option cloud*) : IA pour analyse prédictive

Objectifs complémentaires :

- Réduction du **MTTR** (*Mean Time To Repair*) de 30%
- Alertes automatisées via SMS/email

---

2. Outils de supervision d'activité virale

Mission :

- Analyser les comportements suspects (*scripts non autorisés, accès anormaux*)
- Isoler automatiquement les postes infectés
- Générer des rapports pour audits RGPD/ISO 27001

Outils recommandés :

- **Kaspersky Endpoint Security** : Sandboxing pour analyse de fichiers
- **Snort/Suricata** : IDS/IPS contre ransomware
- **Cortex XDR** : Détection étendue (*endpoints, cloud, réseau*)

Objectifs complémentaires :

- Simulations de phishing pour tester les utilisateurs
- Mise en quarantaine intelligente (*basée sur le risque*)

---

3. Outils de supervision des éléments actifs

Mission :

- Cartographier le réseau en temps réel (*topologie, appareils connectés*)
- Analyser les performances (*latence, bande passante, CPU*)
- Détecter les pannes matérielles (*surchauffe, défaillances de ports*)

Outils recommandés :

- **Zabbix** : Surveillance SNMP/ICMP + alertes personnalisables
- **PRTG Network Monitor** : Dashboards visuels pour points d'accès Wi-Fi
- **SolarWinds NPM** : Analyse avancée du trafic

Objectifs complémentaires :

- Seuils d'alerte personnalisés (*ex : CPU > 80%*)
- Intégration avec SIEM (*ex : Splunk*)

Bénéfices Globaux du PPE2

Pour les utilisateurs	Pour l’organisation	Pour les équipes techniques	
Réduction des interruptions	Conformité réglementaire	Centralisation des opérations	
Meilleure expérience utilisateur	Optimisation des coûts de maintenance	Gain de temps via automatisation	

Conclusion

Feuille de route critique :

- Tests de charge pré-déploiement
- Documentation détaillée des configurations
- Formation des équipes aux nouveaux outils