**Rapport de Projet**

Contents

[I. OBJECTIF DU PROJET 4](#_Toc200830464)

[II. ARCHITECTURE TECHNIQUE 4](#_Toc200830465)

[1. Segmentation Réseau 4](#_Toc200830466)

[2. Contrôles d'Accès 4](#_Toc200830467)

[III. ÉTAPES D'INSTALLATION 4](#_Toc200830468)

[1. Phase 1 : Infrastructure de Base 4](#_Toc200830469)

[2. Phase 2 : Segmentation Réseau 4](#_Toc200830470)

[3. Phase 3 : Services d'Authentification 4](#_Toc200830471)

[4. Phase 4 : Sécurisation 5](#_Toc200830472)

[IV. SÉCURITÉ IMPLÉMENTÉE 5](#_Toc200830473)

[1. ### Isolation Réseau 5](#_Toc200830474)

[2. ### Contrôles d'Accès 5](#_Toc200830475)

[V. MONITORING ET MAINTENANCE 5](#_Toc200830476)

[1. Surveillance Continue 5](#_Toc200830477)

[2. Maintenance Programmée 6](#_Toc200830478)

[VI. DOCUMENTATION FOURNIE 6](#_Toc200830479)

[1. Guides Utilisateurs 6](#_Toc200830480)

[2. ### Documentation Technique 6](#_Toc200830481)

[VII. RÉSULTATS ATTENDUS 6](#_Toc200830482)

[1. ### Sécurité 6](#_Toc200830483)

[2. ### Performance 6](#_Toc200830484)

[3. ### Gestion 7](#_Toc200830485)

[VIII. MISE EN PRODUCTION 7](#_Toc200830486)

[IX. 💡 ÉVOLUTIONS FUTURES 7](#_Toc200830487)

[1. \*\*Module d'authentification RADIUS :\*\* 7](#_Toc200830488)

[2. \*\*Module portail captif :\*\* 8](#_Toc200830489)

[3. \*\*Module de segmentation réseau :\*\* 8](#_Toc200830490)

[4. Spécifications techniques 8](#_Toc200830491)

[a. Architecture système 8](#_Toc200830492)

[b. Couche réseau physique : 8](#_Toc200830493)

[c. Couche réseau logique :\*\* 8](#_Toc200830494)

[d. Couche services :\*\* 8](#_Toc200830495)

[e. Couche sécurité :\*\* 9](#_Toc200830496)

[f. Spécifications matérielles 9](#_Toc200830497)

[1) Serveur pfSense : 9](#_Toc200830498)

[2) Système d'exploitation : 9](#_Toc200830499)

[3) Services réseau :\*\* 9](#_Toc200830500)

[5. Plan d'adressage IP 10](#_Toc200830501)

[6. Flux de données et protocoles 10](#_Toc200830502)

[7. Modélisation de sécurité 10](#_Toc200830503)

[8. Modèle de sécurité multicouche 11](#_Toc200830504)

[9. IMPLÉMENTATION 11](#_Toc200830505)

# OBJECTIF DU PROJET

Sécuriser l'accès Internet WiFi de l'entreprise en séparant les flux visiteurs et collaborateurs via un portail captif pfSense.

# ARCHITECTURE TECHNIQUE

## Segmentation Réseau

- VLAN 10 : Collaborateurs (192.168.10.0/24) - Authentification RADIUS/Active Directory

- VLAN 20 : Visiteurs (192.168.20.0/24) - Authentification par jetons (vouchers)

- VLAN 30 : Management (192.168.30.0/24) - Administration système

## Contrôles d'Accès

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Profil** | **Authentification** | **Durée** | **Bande Passante** | **Quota** | **Accès Interne** |
| **Collaborateurs** | RADIUS/AD | Illimitée | Illimitée | Aucun | Autorisé |
| **Visiteurs** | Vouchers | 1 heure | 10/5 Mbps | 20 Mo | Bloqué |

# ÉTAPES D'INSTALLATION

## Phase 1 : Infrastructure de Base

* **Installation pfSense sur serveur dédié**
* **Configuration réseau initiale (WAN/LAN)**
* **Sécurisation accès administrateur**

## Phase 2 : Segmentation Réseau

* **Création VLANs (10, 20, 30) avec tags 802.1Q**
* **Configuration IP et passerelles par VLAN**
* **Serveurs DHCP dédiés par segment**

## Phase 3 : Services d'Authentification

* **Installation FreeRADIUS et connexion Active Directory**
* **Configuration portail captif sur VLAN visiteurs**
* **Système de vouchers avec limitations temporelles**

## Phase 4 : Sécurisation

**10. \*\*Règles pare-feu\*\* granulaires par VLAN**

**11. \*\*Limitation bande passante\*\* pour visiteurs**

**12. \*\*Isolation réseau\*\* complète entre segments**

# SÉCURITÉ IMPLÉMENTÉE

## Isolation Réseau

- Visiteurs : Accès Internet uniquement, isolation complète des ressources internes

- Collaborateurs : Accès complet après authentification AD

- Règles pare-feu : Blocage inter-VLAN non autorisé

## Contrôles d'Accès

**- \*\*Authentification forte\*\* : RADIUS avec Active Directory pour staff**

**- \*\*Jetons temporaires\*\* : Usage unique, expiration automatique**

**- \*\*Limitations techniques\*\* : Quotas et bande passante pour visiteurs**

# MONITORING ET MAINTENANCE

## Surveillance Continue

**-** Logs centralisés : Authentifications, connexions, sécurité

- Alertes automatiques : CPU, RAM, services critiques

- Statistiques d'usage : Bande passante, utilisateurs actifs

## Maintenance Programmée

**-** Quotidienne : Sauvegarde config, nettoyage logs, purge vouchers

- Hebdomadaire : Vérification services, tests authentification

- Mensuelle : Audit sécurité, analyse statistiques, mises à jour

# DOCUMENTATION FOURNIE

## Guides Utilisateurs

- Visiteurs : Procédure connexion, FAQ, dépannage

- Collaborateurs : Configuration WiFi Enterprise, support

- Administrateurs : Gestion vouchers, monitoring RADIUS

## Documentation Technique

**-** Architecture complète avec schémas réseau

- Procédures d'installation étape par étape

- Configuration détaillée de tous les composants

- Scripts de maintenance et monitoring automatisé

# RÉSULTATS ATTENDUS

## Sécurité

* **Isolation complète visiteurs/collaborateurs**
* **Traçabilité totale des connexions**
* **Contrôle granulaire des accès**

## Performance

* **Limitation bande passante visiteurs (10/5 Mbps)**
* **Quotas respectés (20 Mo par session)**
* **Accès illimité pour collaborateurs**

## Gestion

* Interface d'administration centralisée
* Génération automatique de vouchers
* Monitoring temps réel des connexions

# MISE EN PRODUCTION

Durée d'implémentation : 2-3 jours

Interruption de service : Minimale (fenêtre de maintenance)

Formation requise : 4 heures (équipes IT + accueil)

Support : Documentation complète + procédures dépannage

# ÉVOLUTIONS FUTURES

- Configuration haute disponibilité (HA)

- Authentification multi-facteurs

- Monitoring avancé (Grafana/InfluxDB)

- Intégration IDS/IPS

## **Spécifications détaillées par module**

## Module d'authentification RADIUS

- Entrée : Identifiants utilisateur, adresse MAC, informations NAS

- Traitement : Validation LDAP, application des politiques

- Sorties : Autorisation/refus, attributs de session

- Performances : 100 authentifications/seconde, timeout 5 secondes

## Module portail captif :

**-** Entrées : Code d'accès, adresse MAC, adresse IP

- Traitement : Validation code, application quotas/limitations

- Sorties : Autorisation réseau, redirection utilisateur

- Performances : Interface responsive, chargement < 2 secondes

## Module de segmentation réseau

**-** Entrées: Trafic réseau, règles de routage

- Traitement : Classification VLAN, application règles pare-feu

- Sorties: Routage sélectif, blocage/autorisation

- Performances: Débit 1 Gbps, latence < 1ms

## Spécifications techniques

### Architecture système

L'architecture proposée s'appuie sur une approche multicouche intégrant les composants suivants :

### Couche réseau physique :

**-**Switch manageable : Support 802.1Q VLAN, 24 ports minimum

- Points d'accès WiFi : Support WPA3-Enterprise et VLAN

- Serveur pfSense: Matériel x86 ou virtualisation

### Couche réseau logique

- \*\*VLAN 10\*\* : Collaborateurs (192.168.10.0/24)

- \*\*VLAN 20\*\* : Visiteurs (192.168.20.0/24)

- \*\*VLAN 30\*\* : Management (192.168.30.0/24)

### Couche services :

**-** \*\*DHCP\*\* : Attribution automatique d'adresses IP par VLAN

- \*\*DNS\*\* : Résolution de noms avec filtrage par segment

- \*\*NTP\*\* : Synchronisation temporelle pour les logs

### Couche sécurité :

**- \*\***Pare-feu\*\* : Règles granulaires par VLAN et utilisateur

- \*\*IDS/IPS\*\* : Détection et prévention d'intrusions

- \*\*Logging\*\* : Centralisation et archivage des événements

### Spécifications matérielles

### Serveur pfSense :

**Infrastructure réseau :**

**Spécifications logicielles**

### Système d'exploitation :

**-** \*\*pfSense CE\*\* : Version 2.7.0 ou supérieure

- \*\*FreeBSD\*\* : Base système Unix sécurisée

- \*\*Packages\*\* : FreeRADIUS3, Squid (optionnel), ntopng

### Services réseau :

#### Architecture proposée

#### Vue d'ensemble architecturale

L'architecture proposée implémente une approche de sécurité multicouche (defense-in-depth) avec les principes suivants :

**Séparation des préoccupations :**

- \*\*Plan de données\*\* : Routage et commutation des paquets

- \*\*Plan de contrôle\*\* : Authentification et autorisation

- \*\*Plan de gestion\*\* : Administration et supervision

**Principe du moindre privilège :**

**-** \*\*Accès par défaut\*\* : Deny-all avec autorisation explicite

- \*\*Segmentation\*\* : Isolation maximale entre segments

- \*\*Escalade contrôlée\*\* : Accès administrateur séparé

#### Topologie réseau détaillée

### Plan d'adressage IP

**Tableu**

**Adresses statiques réservées :**

- 192.168.10.10 : Contrôleur de domaine Active Directory

- 192.168.30.10 : Serveur de monitoring/logs

- 192.168.30.100 : Poste d'administration principal

### Flux de données et protocoles

##### Authentification collaborateurs (802.1X) :

**```plaintext**

##### Authentification visiteurs (Portail captif) :

**```plaintext**

## Modélisation de sécurité

#### Analyse des menaces (STRIDE)

L'analyse des menaces suit la méthodologie STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) :

#### Spoofing (Usurpation d'identité) :

**- \*\***Menace\*\* : Usurpation d'identifiants collaborateurs

- \*\*Impact\*\* : Accès non autorisé aux ressources internes

- \*\*Mitigation\*\* : Authentification forte 802.1X, certificats clients

#### Tampering (Altération) :\*\*

- \*\*Menace\*\* : Modification des codes d'accès visiteurs

- \*\*Impact\*\* : Accès non autorisé ou déni de service

- \*\*Mitigation\*\* : Chiffrement des vouchers, validation cryptographique

#### Repudiation (Répudiation) :\*\*

**-** \*\*Menace\*\* : Déni d'actions par les utilisateurs

- \*\*Impact\*\* : Impossibilité d'audit et de conformité

- \*\*Mitigation\*\* : Logs détaillés, horodatage NTP, archivage sécurisé

#### Information Disclosure (Divulgation d'information) :\*\*

- \*\*Menace\*\* : Interception du trafic réseau

- \*\*Impact\*\* : Compromission de données sensibles

- \*\*Mitigation\*\* : Chiffrement WPA3, HTTPS obligatoire, isolation VLAN

#### Denial of Service (Déni de service) :\*\*

- \*\*Menace\*\* : Saturation des ressources réseau

- \*\*Impact\*\* : Indisponibilité du service

- \*\*Mitigation\*\* : Limitation de bande passante, quotas, monitoring

\*\*Elevation of Privilege (Élévation de privilèges) :\*\*

- \*\*Menace\*\* : Accès visiteur aux ressources internes

- \*\*Impact\*\* : Compromission du réseau d'entreprise

- \*\*Mitigation\*\* : Segmentation VLAN, règles pare-feu strictes

### Modèle de sécurité multicouche

#### Matrice de contrôles de sécurité

#### Politique de sécurité

**Principes directeurs :**

1. \*\*Défense en profondeur\*\* : Multiples couches de sécurité

2. \*\*Moindre privilège\*\* : Accès minimal nécessaire

3. \*\*Séparation des responsabilités\*\* : Rôles distincts et contrôlés

4. \*\*Audit continu\*\* : Surveillance et logging exhaustifs

**Règles d'accès :**

**Politique de mots de passe :**

- \*\*Collaborateurs\*\* : Politique Active Directory (complexité, expiration)

- \*\*Codes visiteurs\*\* : Génération aléatoire, usage unique

- \*\*Comptes administrateur\*\* : MFA obligatoire, rotation régulière

Cette conception détaillée constitue la base de l'implémentation pratique présentée dans le chapitre suivant.

### IMPLÉMENTATION

#### Environnement de développement

#### Infrastructure de laboratoire

L'implémentation a été réalisée dans un environnement de laboratoire reproduisant fidèlement un contexte d'entreprise. Cette approche permet de valider la solution avant déploiement en production tout en documentant précisément les procédures.

#### IMPLÉMENTATION

Environnement de développement

Infrastructure de laboratoire

L'implémentation a été réalisée dans un environnement de laboratoire reproduisant fidèlement un contexte d'entreprise. Cette approche permet de valider la solution avant déploiement en production tout en documentant précisément les procédures.

#### Outils et méthodologie

**Outils de développement :**

- \*\*Éditeur de configuration\*\* : nano/vim pour les fichiers de configuration

- \*\*Navigateur web\*\* : Firefox/Chrome pour l'interface pfSense

- \*\*Client SSH\*\* : PuTTY/OpenSSH pour l'accès console

- \*\*Analyseur réseau\*\* : Wireshark pour le debug protocoles

- \*\*Générateur de charge\*\* : Apache Bench pour les tests de performance

**Méthodologie de développement :**

1. \*\*Installation progressive\*\* : Déploiement par composant avec validation

2. \*\*Configuration itérative\*\* : Tests après chaque modification

3. \*\*Documentation continue\*\* : Capture d'écran et procédures détaillées

4. \*\*Sauvegarde systématique\*\* : Backup avant chaque modification majeure

#### Planification du déploiement

* **Phase 1 - Infrastructure de base (Jour 1) :**

- Installation pfSense et configuration réseau initiale

- Configuration du switch avec VLANs

- Tests de connectivité de base

* **Phase 2 - Services d'authentification (Jour 2) :**

- Installation et configuration FreeRADIUS

- Intégration avec Active Directory

- Tests d'authentification RADIUS

* **Phase 3 - Portail captif (Jour 3) :**

- Configuration du portail captif

- Système de vouchers

- Personnalisation de l'interface

* **Phase 4 - Sécurisation (Jour 4) :**

- Règles de pare-feu détaillées

- Limitation de bande passante

- Tests de sécurité

* **Phase 5 - Validation (Jour 5) :**

- Tests fonctionnels complets

- Tests de performance

- Documentation finale

### Installation et configuration pfSense

#### Installation du système

**Préparation du support d'installation :**

```bash

# Téléchargement de l'image pfSense

wget [https://www.pfsense.org/download/](https://www.pfsense.org/download/)

**Vérification de l'intégrité**

sha256sum pfSense-CE-2.7.0-RELEASE-amd64.iso

**Création de la clé USB bootable (Linux)**

sudo dd if=pfSense-CE-2.7.0-RELEASE-amd64.iso of=/dev/sdb bs=4M status=progress

sync