PROJET DE MISE EN PLACE DE DEUX RÉSEAUX LAN COMMUNICANTS AVEC ACCÈS INTERNET SÉCURISÉ.

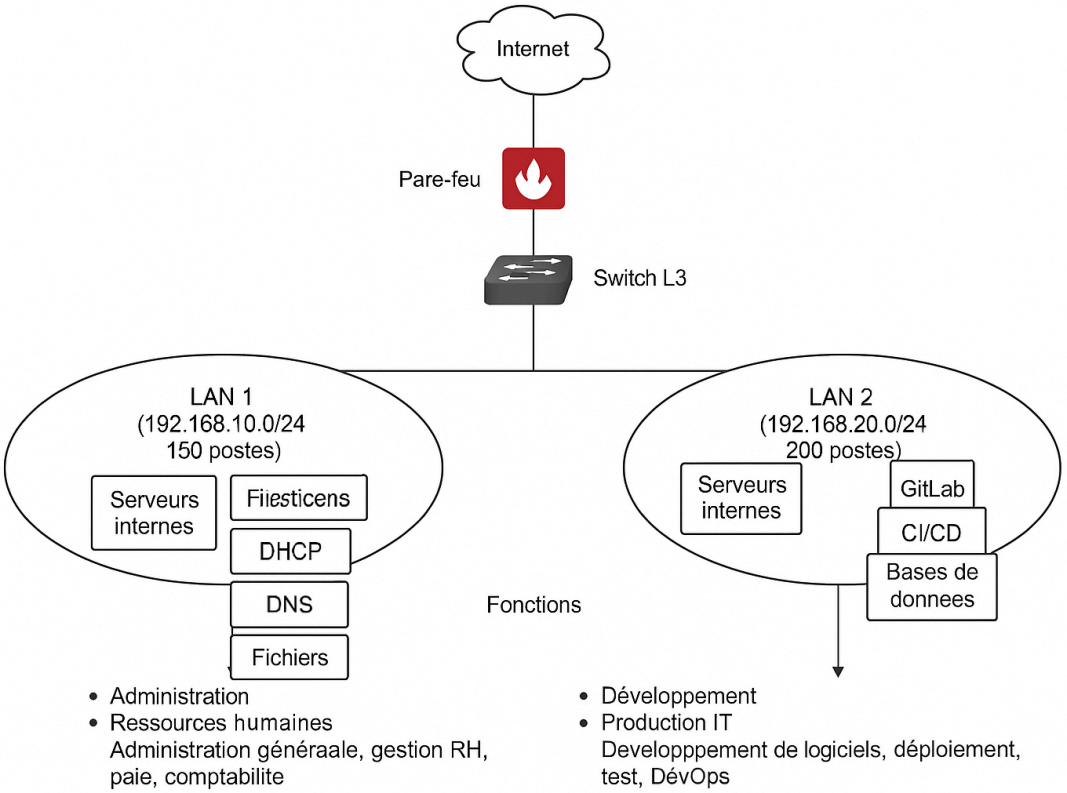
1. Objectif du Projet

L'objectif de ce projet est de concevoir, mettre en place et sécuriser deux réseaux LAN (LAN 1 et LAN 2) interconnectés,
capables de communiquer entre eux, d'accéder à internet, tout en intégrant un pare-feu open source robuste pour garantir la sécurité, la scalabilité et la haute disponibilité du système informatique d'une grande entreprise.

2. Architecture Générale du Réseau

2.1 Schéma Logique du Réseau

- Deux LANs : LAN1 (192.168.10.0/24), LAN2 (192.168.20.0/24)
- Un switch L3 assurant le routage inter-VLAN
- Un pare-feu pfSense
- Accès Internet
- Serveurs DHCP, DNS, fichiers pour LAN1
- GitLab, CI/CD, base de données pour LAN2



3. Description Technique

3.1 LAN 1 (Département A)

. Plage IP : 192.168.10.0/24
. Utilisateurs : Environ 150 postes
. Rôles : Administration, Ressources humaines
. Serveurs internes : DHCP, DNS, fichiers
. Fonctions principales : Administration générale, gestion RH, paie, comptabilité.

3.2 LAN 2 (Département B)

. Plage IP : 192.168.20.0/24
. Utilisateurs : Environ 200 postes
. Roles : Développement, Production IT
. Serveurs internes : GitLab, CI/CD, bases de données internes
. Fonctions principales : Développement de logiciels, déploiement, test, DevOps

Installer GitLab Community Edition (CE)

Mettre à jour le système

sudo apt update && sudo apt upgrade -y

Installer curl, openssh, ca-certificates

sudo apt install -y curl openssh-server ca-certificates tzdata perl

Ajouter le dépôt GitLab

curl
https://packages.gitlab.com/install/repositories/gitlab/gitlab-ce/script.deb.sh |
sudo bash

# Installer GitLab (en remplaçant l'URL par l'IP de ton serveur)
sudo EXTERNAL_URL="http://192.168.20.10" apt install gitlab-ce -y

http://192.168.20.10 Pour aller sur le navigateur.

3.3 Interconnexion

. Un switch L3 assurera le routage inter-VLAN entre les deux LAN.

. ACLs (Listes de Controle d'Acces) seront configurées pour filtrer les flux selon les besoins métiers.

3.4 Accès Internet

. Le pare-feu open source fera office de passerelle sécurisée vers internet.
. Le NAT (Network Address Translation) sera activé pour masquer les IP internes.
. Le proxy et le filtrage URL seront activés pour contrôler les accès web.

4. Sécurité Pare-feu Open Source

4.1 Solution Recommandée :
pfSense

Pourquoi pfSense ?

. Distribution FreeBSD spécialisée dans le routage/filtrage réseau.
. Interface Web complète et facile à administrer.
. Fonctionnalités d'entreprise sans coût de licence :
. Stateful firewall
. VPN (IPSec, OpenVPN)
. IDS/IPS (Snort, Suricata)
. Haute disponibilité (CARP)
. Captive Portal
. Filtrage web avec Squid + SquidGuard

Déploiement

. Mode Bare Metal ou VM sur Hyperviseur (VMware)
. Deux interfaces réseau :
.WAN vers Internet
.LAN vers switch L3
. Redondance possible avec configuration CARP (failover entre deux pare-feux)

5. Sécurité Avancée

. VLANs segmentés avec politiques de sécurité inter-VLAN restrictives.
. IDS/IPS avec Suricata pour détection d'intrusions en temps réel.
. Logs centralisés avec export vers un serveur Syslog sécurisé (Graylog/ELK).
. Filtrage Web via SquidGuard (blocage)
catégories : réseaux sociaux, sites malveillants, etc...
Contrôle d'accès via règles ACL basées sur les rôles métiers.
. VPN sécurisé (OpenVPN ou WireGuard) pour accès distant au réseau.

6. Scalabilité & Evolutivité

. L'architecture est modulaire : ajout de LAN/VLAN simple via configuration du switch L3 et du pfSense.
. Le pare-feu pfSense supporte le clustering pour haute disponibilité.
. Possibilité de passer à une solution SD-WAN ou de migrer vers un datacenter privé/cloud hybride si besoin.

. Intégration possible avec Active Directory ou LDAP pour la gestion centralisée des utilisateurs.

7. Supervision & Monitoring

Outils recommandés :
. Zabbix pour monitoring réseau, charge CPU, RAM, disques, etc.
. NetFlow/ntopng pour analyse des flux réseau.
. Alerting par email/SMS en cas de panne ou surcharge.

8 . Configuration des VLANs (sur Switch L3)

Création des VLANs

```
enable
configure terminal
vlan 10
 name LAN1
exit
vlan 20
 name LAN2
exit
```

Bonnes pratiques:

Séparer clairement les ports d'accès et les trunks.
Utiliser des noms de VLAN clairs.
Activer DHCP snooping, port security, et BPDU Guard pour la sécurité réseau.

9 . Configuration pfSense

Étapes de base (interface web)

1. connexion à l'interface web (https://192.168.1.1)
2. Configurer les interfaces:

.WAN : IP dynamique ou statique selon FAI
. LAN : 192.168.1.1/24 temporaire, à modifier ensuite

Ajout des VLANs dans pfSense
Via Interfaces > Assignments > VLANs:
. VLAN 10 sur l'interface LAN physique
. VLAN 20 idem

Puis assigner les interfaces et leur attribuer les IP:
. LAN1 : 192.168.10.254/24
. LAN2 : 192.168.20.254/24

DHCP Server

Activer un serveur DHCP par VLAN via
Services > DHCP Server :
. LAN1 : 192.168.10.50 - 192.168.10.200
. LAN2 : 192.168.20.50 - 192.168.20.250

Règles de Pare-feu

Aller dans Firewall > Rules :
. Créer des règles par interfaces (LAN1 et LAN2)
. Autoriser le trafic inter-LAN uniquement si nécessaire :

Action : Pass
Interface : LAN1
Protocol : TCP/UDP
Source : LAN1 subnet
Destination : LAN2 subnet

NAT (masquerading)
Activé par défaut pour chaque interface sortante vers le WAN.

10 . Configuration d'OpenVPN (accès distant)

Création du serveur VPN

via VPN > OpenVPN > Wizards :
Générer CA interne
Générer certificat serveur
Créer le serveur VPN (UDP, port 1194)
Definir la page IP VPN (ex: 10.8.0.0/24)

Règles firewall VPN

Autoriser trafic sur l'interface OpenVPN

Téléchargement des fichiers de configuration client
depuis VPN > OpenVPN > Client Export

11 . Installation d'un IDS/IPS (Suricata)

Installation
via System > Package manager > Available Packages

Installer Suricata

Configuration

Affecter suricata aux interfaces LAN1, LAN2
choisir des règles (ET Open, Snort VRT)
Activer l'inspection en ligne (inline mode)

Bonnes pratiques :

Ne pas activer toutes les règles, trier par usage
activer les logs vers Syslog/Graylog
Mettre à jour régulièrement les signatures

12. Bonnes Pratiques Globales

sécurité

utiliser des ACLs sur le switch L3 pour limiter les communications inter-VLAN
configurer des règles strictes sur pfsense (deny all par défaut)

utiliser le DNS over TLS (DoT) ou DNSSEC si possible

Supervision & Sauvegarde

planifier des sauvegardes automatiques de la configuration pfSense
monitorer via Zabbix
Sauvegarder les configurations du switch (tftp ou scp)

Redondance

installer un second pfSense avec carp pour haute disponibilité
Alimenter tout via onduleur (UPS)
Réseau en étoile pour limiter les SPOF

13. Annexes : Scripts & aides

Ecrire un Script de sauvegardes automatique sur pfsense

Configuration NAT manuelle (si besoin)

via Firewall > NAT > Outbound :
. Passer en mode “Hybrid”
. Ajouter des règles explicites si plusieurs sous-réseaux

14. Sécurisation avancée de l’infrastructure

14.1 Segmentation réseau poussée (micro-segmentation)

Objectif

limiter les mouvements latéraux d’un attaquant dans le réseau interne.

Chaque VLAN peut être subdiviser par fonction :

. LAN1

- VLAN 10: RH
- VLAN 11 : Direction
- VLAN 12 : Finance

. LAN2

- VLAN 20 : Développement
- VLAN 21 : Production
- VLAN 22 : Test

Mise en oeuvre
Configuration de VLANs supplémentaires sur le switch L3
Routage inter-VLAN avec des ACLs restrictives.

14.2 Politique de filtrage firewall stricte (pfSense)

Principe Zéro Trust

Tout trafic est bloqué par défaut
Chaque règle doit être justifiée et tracée

Mise en place

créer une règle finale “Block All” sur chaque interface LAN.

Bonnes pratiques

activer logging sur toutes les règles critiques
regrouper les règles en “groupes logiques” avec des alias d’IP/services
Utiliser des alias dynamiques (pfblockerNG) pour bloquer les IPs malveillants.

14.3 Surveillance réseau centralisée

Solutions recommandées

Zabbix : pour surveillance hôte, services, pings, SNMP

ELK Stack (Elasticsearch, Logstash, Kibana) : analyse des logs
firewall, VPN, serveurs

ntopng : visualisation du trafic réseau en temps réel

Sur serveur Zabbix :

Ajouter un hôte
Associer le template pfSense SNMP interface

15. VPN Entreprise-Haute sécurité

15.1 Configuration OpenVPN avancée

Algorithme de chiffrement : AES-256-GCM, TLS 1.3
Authentification à deux facteurs (OTP)
Restrictions de réseau par utilisateur (client-specific override)

15.2 Intégration LDAP/ Active Directory

Authentification centralisée des utilisateurs
via le plugin pfSense > System > User Manager > Authentication Servers

Protocole : LDAP ou RADIUS

Sécurisation avec StartTLS

16. Redondance et haute disponibilité

16.1 pfSense en HA (CARP)

Matériel requis
Deux machines pfSense avec 3 interfaces minimum
Une interface synchronisation (SYNC)
Une IP virtuelle partagée (VIP)

Étapes principales

Créer une interface SYNC entre les deux pare-feux
configurer le pfSync pour synchroniser les règles, utilisateurs, etc.
configurer carp vip :
VIP LAN : 192.168.10.254
VIP WAN : IP publique flottante
Priorité : pfSense maître = 100, backup = 50

16.2 Redondance au niveau du switch

Stacking/Virtual Chassis
Utiliser deux switchs L3 (ex: Cisco 9300) empilés
Configuration automatique d’un switch maître et esclave.
interconnexion avec LAG (Link Aggregation Group)

Spanning Tree Protocol (STP)

Rapid PVST ou MSTP pour éviter les boucles réseau
Activer Root Guard et BPDU Filter pour plus de sécurité

—----------FIN—----------