

# Rapport Final de Projet – Infrastructure Réseau Sécurisée et Haute Disponibilité avec pfSense

# **1. Contexte Professionnel du Projet**

Dans le cadre d'un projet de transformation numérique, la société Cyberlogix Solutions, une entreprise spécialisée dans le développement de logiciels de cybersécurité pour les TPE et PME, a entrepris une modernisation complète de son infrastructure réseau. Avec une croissance constante de ses effectifs et l'ouverture de nouvelles agences sur le territoire national, l'entreprise fait face à de nouveaux défis en matière de sécurité, de disponibilité des services, de gestion du trafic réseau, et d'accès distant sécurisé pour ses collaborateurs et partenaires.

Les dirigeants de Cyberlogix Solutions ont constaté que l'infrastructure réseau actuelle, initialement conçue pour une petite structure, ne répondait plus aux besoins critiques de l'entreprise en matière de haute disponibilité, de sécurité avancée, de contrôle des flux, et d'accès distant sécurisé. La moindre panne réseau pouvait entraîner un arrêt de la production, des interruptions dans le support client, et des risques élevés liés à la cybersécurité. Pour y remédier, la DSI de l'entreprise a décidé de lancer un projet stratégique visant à concevoir et déployer une infrastructure réseau virtualisée et sécurisée, s'appuyant sur des technologies robustes, éprouvées et open source, avec un objectif de redondance, de segmentation réseau, de sécurité active et de supervision centralisée.

Ce projet, intitulé "Infrastructure Réseau Sécurisée et Haute Disponibilité avec pfSense", s'inscrit dans une logique de continuité d'activité, de conformité aux exigences de sécurité actuelles, et d'évolution vers un modèle d'infrastructure agile et scalable. L'intégralité du projet a été conçue pour être entièrement virtualisée sous Proxmox, tout en reproduisant le plus fidèlement possible un environnement d'entreprise réel, dans une logique de simulation de production.

## **2. Objectifs du Projet**

Les objectifs définis par la DSI de Cyberlogix Solutions pour ce projet sont clairs, ambitieux, et alignés avec les besoins opérationnels de l'entreprise :

- Garantir la haute disponibilité de l'accès réseau par la mise en place d'un cluster pfSense avec le protocole CARP, permettant le basculement automatique en cas de défaillance matérielle ou logicielle.
- Implémenter une solution de Load Balancing et de Failover entre deux connexions Internet redondantes, afin d'assurer une continuité de service même en cas de coupure d'un fournisseur d'accès.
- Mettre en œuvre une infrastructure VPN multi-sites (IPsec pour les interconnexions entre agences et OpenVPN pour les accès distants du personnel) sécurisée et adaptée aux différents profils d'utilisateurs.
- Segmenter le réseau en plusieurs VLAN selon les services (administration, développement, invités) pour isoler les flux et limiter la surface d'exposition.
- Contrôler les accès Internet via un proxy filtrant basé sur Squid et SquidGuard, afin d'appliquer une politique acceptable d'usage (Acceptable Use Policy - AUP).
- Détecter et bloquer en temps réel les tentatives d'intrusion grâce à un système IDS/IPS tel que Suricata, configuré pour intervenir de manière proactive.
- Mettre en place une supervision avancée de l'infrastructure réseau à l'aide de Zabbix (surveillance des ressources), Grafana (visualisation graphique), et ELK Stack (collecte et analyse des logs réseau).

## **3. Architecture Générale du Réseau**

L'architecture de l'infrastructure déployée repose sur des principes éprouvés de sécurité, de segmentation, de redondance, et de haute disponibilité. Tous les éléments réseau critiques sont virtualisés dans l'hyperviseur Proxmox VE, et l'ensemble des services réseau est cloisonné à l'aide de VLANs et de pare-feu inter-VLAN.

### 1. Tableau d'Adressage IP du Projet

Nom de la machine / Service	Interface	VLAN	Adresse IP	Rôle
pfSense (CARP)	LAN	110	192.168.100.1	Passerelle LAN (virtuelle via CARP)
pfSense Master	LAN	110	192.168.100.2	Firewall principal
pfSense Backup	LAN	110	192.168.100.3	Firewall de secours
pfSense (WAN1)	WAN1 (ens18)	-	10.4.0.2	Connexion Internet principale
pfSense (WAN2)	WAN2 (ens19)	-	192.168.200.2	Connexion Internet secondaire simulée
Debian (Docker + ELK + Zabbix)	LAN	110	192.168.100.10	Serveur de supervision & logs
Windows Server (AD + DNS + DHCP)	LAN	110	192.168.100.20	Contrôleur de domaine Active Directory
Windows Client (test)	LAN	120	192.168.100.70	Poste client VLAN Développement
Machine VLAN Invités	LAN	130	192.168.100.130	Accès Internet uniquement

## 2. Tableau des VLANs

VLAN ID	Nom	Adresse Gateway	Plage IP	Description
110	Administration	192.168.100.1	192.168.100.10-50	Serveurs et personnel IT
120	Développement	192.168.100.65	192.168.100.70-90	Postes développeurs
130	Invités	192.168.100.129	192.168.100.130-150	Accès Internet uniquement

## 3. Tableau des Services Docker Déployés

Service	Image Docker	Port d'accès	Fonction
Elasticsearch	docker.elastic.co/elasticsearch/elasticsearch:7.17.0	9200	Indexation des logs
Logstash	docker.elastic.co/logstash/logstash:7.17.0	5044	Réception et parsing des logs
Kibana	docker.elastic.co/kibana/kibana:7.17.0	5601	Interface web pour les logs
Zabbix Server	zabbix/zabbix-server-mysql:alpine-6.0-latest	10051	Serveur de supervision
Zabbix Frontend	zabbix/zabbix-web-apache-mysql:alpine-6.0-latest	8080	Interface web Zabbix
Zabbix Agent	zabbix/zabbix-agent:alpine-6.0-latest	10050	Agent à installer sur les hôtes
Grafana	grafana/grafana:latest	3000	Dashboards personnalisés

#### 4. Tableau des GPOs Appliquées

Nom de la GPO	Description	Cible / OU	Effet attendu
GPO-Mot de Passe Expiration	Forcer changement de mot de passe tous les 90 jours	Utilisateurs	Renforcement sécurité des comptes
GPO-Firewall	Activation et configuration du pare-feu Windows	Tous les postes	Filtrage du trafic réseau local
GPO-Limitation-RDP	Restreindre RDP aux admins uniquement	Utilisateurs standard	Blocage des accès RDP non autorisés
GPO-Désactivation USB	Empêcher usage de clés USB	Utilisateurs standard	Prévention de la fuite de données
GPO-Imprimantes	Mappage automatique des imprimantes réseau	Tous les utilisateurs	Simplification de l'accès à l'impression

## **4. Déploiement du Cluster pfSense en Haute Disponibilité (CARP)**

Afin de garantir la continuité de service en cas de défaillance d'un des équipements réseau, l'entreprise Cyberlogix Solutions a choisi de mettre en place une solution de haute disponibilité pour le cœur de son infrastructure : la passerelle réseau. Pour cela, deux pare-feux pfSense ont été configurés en mode redondant, à l'aide du protocole CARP (Common Address Redundancy Protocol), un protocole open source permettant à plusieurs hôtes sur le même réseau local de partager une ou plusieurs adresses IP virtuelles.

Cette solution repose sur un mécanisme de redondance active-passive, dans lequel un pfSense joue le rôle de maître (Master), tandis que le second agit en secours (Backup). En cas de défaillance du maître (crash système, perte de connectivité, coupure de service), le serveur de secours prend automatiquement le relais, en assumant la même adresse IP virtuelle, ce qui garantit la continuité de service pour tous les clients du réseau, sans interruption perceptible.

### **4.1 Prérequis à la mise en place de CARP**

Avant de configurer la haute disponibilité, plusieurs prérequis ont été vérifiés :

Les deux instances pfSense ont été installées en tant que machines virtuelles sous Proxmox, chacune disposant de trois interfaces réseau : une pour le WAN, une pour le LAN, et une dédiée à la synchronisation (pfsync).

Les interfaces ont été affectées comme suit :

- Vmb0 : WAN
- Vmb4 : LAN

em2 : SYNC (interface privée dédiée uniquement à la synchronisation de l'état du pare-feu et des sessions)

L'interface SYNC a été configurée avec un adressage réseau privé spécifique :

- pfSense Master : 172.16.0.1/24
- pfSense Backup : 172.16.0.2/24

### **4.2 Configuration du cluster CARP sur pfSense**

Une fois les interfaces configurées, la haute disponibilité a été activée via les étapes suivantes sur le pfSense principal (Master) :

Dans **System > High Availability Sync**, les cases **Synchronize Config** to Backup ont été cochées, et l'adresse IP du pare-feu secondaire (172.16.0.2) a été renseignée.

Le mot de passe d'administration de l'interface Web a été défini de manière identique sur les deux nœuds pfSense.

Dans le même menu, les services à synchroniser ont été activés :


Firewall Rules

Virtual IPs

DHCP Leases


IPsec Tunnels

OpenVPN settings

 Capture d'écran à insérer : Menu "High Availability Sync" du pfSense principal avec tous les services synchronisés.

Ensuite, dans **Firewall > Virtual IPs**, un nouvel alias de type CARP a été créé avec l'adresse 192.168.100.1 pour le VLAN Admin. Cette adresse sera la passerelle par défaut des clients de ce VLAN, et sera utilisée par les deux pfSense, mais uniquement le Master répondra lorsqu'il est en fonctionnement normal.


- Type : CARP
- Interface : LAN
- IP Address : 192.168.100.1/24
- VHID Group : 1 (unique pour chaque IP virtuelle)
- Password : mot de passe sécurisé commun aux deux pare-feu
- Advskew : 0 pour le Master, 100 pour le Backup

 Capture d'écran à insérer : Détail de la configuration de l'IP virtuelle CARP sur le VLAN Administration.

Cette étape a été répétée pour chaque VLAN (Développement, Invités), ainsi que pour les interfaces WAN si nécessaire. Il est recommandé d'utiliser des VHID différents pour chaque IP virtuelle (ex. VHID 2 pour VLAN 20, VHID 3 pour VLAN 30, etc.).

### **4.3 Vérification de la synchronisation d'état (pfsync)**

Dans **System > Advanced > Miscellaneous**, l'option **Synchronize States** a été activée. Cela permet au pare-feu secondaire de reprendre immédiatement les sessions en cours lors d'un basculement, sans perte de connexion utilisateur, ce qui est crucial pour la disponibilité des services tels que les VPN, les sessions SSH, ou les accès à distance.

 Capture d'écran à insérer : Activation de la synchronisation d'état (pfsync) dans les paramètres avancés.

### **4.4 Tests de basculement (Failover)**



Afin de s'assurer de la fiabilité du cluster, plusieurs tests de basculement ont été effectués :  
Extinction volontaire du pfSense principal : constat immédiat du transfert de l'adresse IP virtuelle vers le secondaire.


Simulation d'une coupure réseau : le Backup a pris le relais sans délai notable pour les utilisateurs.

Vérification de l'adresse MAC associée à l'IP virtuelle via un client connecté :

Commande utilisée sur un poste client Linux :

`- arp -a`

Cette commande permet de visualiser les adresses MAC associées aux IPs connues. Lors du basculement, la MAC associée à l'IP 192.168.100.1 change, signe que la prise de relais est effective.

 Capture d'écran à insérer : Résultat de la commande arp -a avant et après basculement pour prouver le fonctionnement de CARP.

## **5. Mise en Place de l'Équilibrage de Charge (Load Balancing) et du Basculement Automatique (Failover)**

L'un des objectifs majeurs du projet était de garantir une connectivité Internet continue et sans interruption, même en cas de panne ou d'instabilité d'un fournisseur d'accès. Pour cela, l'équipe informatique de Cyberlogix Solutions a décidé de mettre en œuvre une architecture multi-WAN, avec deux connexions Internet distinctes fournies par deux opérateurs différents. Ces deux liens Internet sont connectés physiquement aux deux pare-feux pfSense du cluster, l'un étant désigné comme WAN1 (primaire) et l'autre comme WAN2 (secondaire).

Afin d'optimiser l'usage de ces deux connexions et de renforcer la disponibilité, deux mécanismes complémentaires ont été mis en œuvre dans pfSense :

L'équilibrage de charge, qui permet de répartir les connexions sortantes entre WAN1 et WAN2 pour mieux gérer la bande passante disponible.


Le basculement automatique (Failover), qui permet de transférer automatiquement tout le trafic sur la seconde connexion en cas de panne de la première.

## **5.1 Ajout des interfaces WAN1 et WAN2**

Dans un premier temps, les deux interfaces WAN ont été correctement ajoutées et configurées sur chaque pfSense, avec des adresses IP publiques distinctes fournies par chaque opérateur. Chaque interface WAN est connectée à un switch virtuel distinct dans Proxmox pour simuler deux connexions extérieures différentes.

WAN1 est connecté au bridge principal **vmbr0**, qui correspond à l'interface physique de l'hôte Proxmox disposant d'un accès Internet réel. Ce bridge utilise un plan d'adressage en base 16, soit le réseau 10.4.0.0/16. L'adresse IP de la passerelle de ce réseau est 10.4.0.253, qui permet d'accéder à Internet. L'interface WAN1 de pfSense reçoit l'adresse 10.4.0.2/16, configurée manuellement, avec 10.4.0.253 comme passerelle par défaut.

WAN2 est relié à un second bridge Proxmox, **vmbr5**, configuré comme un réseau isolé ou de test. Ce réseau est utilisé pour simuler une seconde connexion externe. Dans ce cas, une IP fixe, par exemple 192.168.100.2/24, a été attribuée à l'interface WAN2 de pfSense, avec une passerelle fictive 192.168.100.1, qui peut être simulée par une petite VM NAT ou un routage interne.

 Capture d'écran à insérer : Tableau de bord pfSense montrant les deux interfaces WAN connectées avec leurs adresses IP publiques respectives.

## **5.2 Création des Gateway Groups pour Load Balancing et Failover**

L'élément central de cette configuration repose sur la création d'un groupe de passerelles (Gateway Group). Ce groupe permet de définir une politique de basculement et d'équilibrage de charge entre les deux interfaces WAN. L'objectif est que WAN1 soit utilisé en priorité, et que WAN2 prenne le relais uniquement si WAN1 devient inaccessible.

Pour cela, dans le **menu System > Routing > Gateway Groups**, un nouveau groupe a été créé avec les paramètres suivants :


Nom du groupe : WAN\_FAILOVER

WAN1 : Tier 1 (priorité haute)

WAN2 : Tier 2 (priorité basse)

Trigger Level : Member Down

Ce paramètre indique que pfSense basculera automatiquement vers WAN2 dès que WAN1 ne répond plus aux pings de surveillance configurés.

 Capture d'écran à insérer : Écran de création du Gateway Group montrant les priorités Tier 1 (WAN1) et Tier 2 (WAN2).


### 5.3 Configuration de la surveillance des gateways (Monitoring)

Pour détecter l'état de chaque lien Internet, pfSense utilise un mécanisme de ping de surveillance vers une adresse IP fiable (souvent un serveur DNS public comme 8.8.8.8 ou 1.1.1.1). Ces adresses sont configurées dans **System > Routing > Gateways**, dans la colonne Monitor IP.

Monitor IP WAN1 : 8.8.8.8 (Google DNS)

Monitor IP WAN2 : 1.1.1.1 (Cloudflare DNS)

Cela permet à pfSense de détecter une coupure de manière fiable, même si l'interface réseau est toujours physiquement active.

 Capture d'écran à insérer : Détail de la configuration de la surveillance (Monitor IP) pour chaque gateway.

### 5.4 Création des règles de routage (Policy-Based Routing)

Une fois le groupe de passerelles créé, il est nécessaire de configurer les règles de pare-feu pour que le trafic sortant passe par ce groupe. Cela se fait dans **Firewall > Rules > LAN** (et sur chaque interface VLAN concernée).

Une règle générale a été créée :


Action : Pass

Interface : LAN (ou VLAN XX)

Protocol : any

Gateway : WAN\_FAILOVER (le groupe de passerelles créé)

Cela signifie que tout le trafic sortant depuis le réseau LAN ou VLAN utilisera WAN1 en priorité, et basculera automatiquement vers WAN2 en cas de panne.

 Capture d'écran à insérer : Règle de pare-feu avec Policy-Based Routing sélectionnant le groupe de passerelles.

### 5.5 Tests de basculement WAN

Pour valider le bon fonctionnement du système de failover, plusieurs tests ont été réalisés :


Coupure du câble WAN1 dans Proxmox : Le ping vers une IP externe (comme 8.8.8.8) depuis un poste client a été relancé automatiquement via WAN2 en moins de 5 secondes.

Commande utilisée pour vérifier le routage :

Sur un poste client Linux ou Windows : `tracert www.google.com` ou `tracert www.google.com`

Cela permet de voir la route empruntée et l'adresse IP source du WAN utilisée.

Dans le tableau de bord de pfSense, l'état de WAN1 est passé à Offline, et la bascule vers WAN2 a été observée immédiatement.

 Capture d'écran à insérer : Traceroute avant et après coupure WAN1 montrant la redirection automatique du trafic vers WAN2.

## **6. Mise en Place des VPN OpenVPN et IPsec pour l'Accès Distant Sécurisé**

Dans un contexte professionnel moderne, où la mobilité des collaborateurs et les interconnexions inter-sites sont devenues incontournables, il était indispensable pour l'entreprise Cyberlogix Solutions de proposer des solutions d'accès distant sécurisées et fiables, répondant aux exigences de confidentialité des données, d'intégrité des échanges et de compatibilité avec les systèmes d'authentification centralisée. Pour cela, deux technologies complémentaires ont été mises en place sur les pare-feux pfSense : OpenVPN pour l'accès distant des employés, et IPsec Site-to-Site VPN pour l'interconnexion des agences distantes.

## **6.1 Mise en place d'OpenVPN pour les employés**

La solution OpenVPN a été choisie en raison de sa compatibilité multiplateforme, de son chiffrement robuste basé sur SSL/TLS, et de sa souplesse de configuration. Elle permet à un employé, où qu'il se trouve dans le monde, de se connecter de manière chiffrée et authentifiée au réseau de l'entreprise en utilisant une application cliente compatible.

### *6.1.1 Préparation de l'infrastructure PKI*

Avant de configurer OpenVPN, il est indispensable de mettre en place une infrastructure à clé publique (PKI) afin de générer les certificats nécessaires à l'authentification du serveur VPN et des clients.

Dans **System > Cert. Manager > CAs**, une nouvelle autorité de certification (CA) a été créée :

Name : Cyberlogix-CA

Key length : 2048 bits

Digest Algorithm : SHA256

Lifetime : 3650 jours

Ensuite, dans **System > Cert. Manager > Certificates**, un certificat serveur a été généré à partir de cette CA, avec l'usage Server Certificate.



Capture d'écran à insérer : Création de l'autorité de certification Cyberlogix-CA.

### *6.1.2 Configuration du serveur OpenVPN*

Dans le menu **VPN > OpenVPN > Servers**, un nouveau serveur a été configuré avec les paramètres suivants :

Protocol : UDP

Port : 1194

Tunnel Network : 10.8.0.0/24 (plage d'adresses interne au VPN)

Local Network : 192.168.100.0/24, 192.168.200.0/24 (accès aux VLAN internes)

Client Authentication : SSL/TLS + User Auth (login/mot de passe via LDAP)

Certificate : Cyberlogix-Server

Encryption algorithm : AES-256-CBC

Auth digest algorithm : SHA256



Capture d'écran à insérer : Paramètres du serveur OpenVPN dans pfSense.

### *6.1.3 Intégration avec l'annuaire LDAP / Active Directory*

Pour éviter de devoir gérer manuellement les comptes VPN, une connexion au contrôleur Active Directory de l'entreprise a été mise en place.

Dans **System > User Manager > Authentication Servers**, un nouveau serveur LDAP a été ajouté :

Hostname or IP address : IP du serveur AD (ex : 192.168.100.10)

Base DN : dc=cyberlogix,dc=local

Authentication containers : ou=Employés,dc=cyberlogix,dc=local

Une fois ce serveur LDAP ajouté, il a été sélectionné comme backend d'authentification dans la configuration du serveur OpenVPN.



Capture d'écran à insérer : Configuration du serveur LDAP dans pfSense.

### *6.1.4 Exportation et distribution des profils VPN*

Pour faciliter la connexion des utilisateurs, le paquet OpenVPN Client Export a été installé via **System > Package Manager**. Ensuite, dans **VPN > OpenVPN > Client Export**, chaque utilisateur a pu générer un profil de configuration complet (.ovpn) à importer dans le client OpenVPN.



Capture d'écran à insérer : Génération et exportation des fichiers de configuration client OpenVPN.

## *6.2 Mise en place d'un tunnel IPsec Site-to-Site entre agences*

Pour interconnecter les différents sites distants de l'entreprise sans exposer les services sur Internet, une liaison VPN IPsec a été établie entre le siège principal (serveur pfSense 1) et l'agence secondaire (serveur pfSense 2). IPsec a été préféré à OpenVPN pour les liaisons site-à-site, en raison de sa standardisation, sa compatibilité avec la majorité des équipements réseau professionnels, et sa capacité à fonctionner même en environnement NAT.

### *6.2.1 Configuration de Phase 1*

Dans **VPN > IPsec > Tunnels**, une phase 1 a été ajoutée avec les paramètres suivants :

Key Exchange version : IKEv2

Internet Protocol : IPv4

Interface : WAN

Remote Gateway : Adresse IP publique de l'agence distante

Authentication Method : Pre-Shared Key (clé commune forte)

My identifier : My IP address

Encryption Algorithm : AES-256-GCM

DH Group : 14 (2048-bit MODP)



Capture d'écran à insérer : Détail de la configuration Phase 1 du tunnel IPsec.

### *6.2.2 Configuration de Phase 2*

Une Phase 2 a ensuite été ajoutée pour définir les sous-réseaux concernés par le tunnel :

Local Network : 192.168.100.0/24 (siège)

Remote Network : 192.168.50.0/24 (agence distante)

Protocol : ESP

Encryption Algorithms : AES-256

PFS Key Group : 14



Capture d'écran à insérer : Configuration de la Phase 2 du tunnel IPsec.

Une règle de pare-feu a été ajoutée dans Firewall > Rules > IPsec pour permettre le trafic entre les deux sites.

### *6.2.3 Vérification de la connectivité*

Une fois les deux tunnels configurés sur les deux sites, les tests de connectivité ont été réalisés à l'aide des commandes suivantes :

Depuis un poste client :

**ping 192.168.50.1 (depuis le siège vers un hôte de l'agence distante)**  
**tracert 192.168.50.1 pour vérifier le chemin du trafic**



Capture d'écran à insérer : État du tunnel IPsec dans le menu "Status > IPsec" avec le message "Connected".

## **7. Segmentation Réseau par VLANs et Configuration des Règles de Pare-feu Inter-VLAN**

Dans une architecture réseau professionnelle, il est indispensable de segmenter les flux afin de réduire la surface d'attaque, limiter les communications inutiles, renforcer la sécurité des données sensibles, et isoler les différents environnements métiers. Pour répondre à cette exigence, l'entreprise Cyberlogix Solutions a mis en place une segmentation réseau complète reposant sur des VLANs (Virtual Local Area Networks) configurés dans pfSense, et sur des switchs managés compatibles VLAN (simulés dans l'environnement Proxmox).

Chaque VLAN est associé à une unité organisationnelle (service) distincte de l'entreprise, avec des plages d'adresses IP privées dédiées, un routage contrôlé par pfSense, et des règles de pare-feu strictes empêchant la communication inter-VLAN par défaut, sauf exceptions autorisées.



## 7.1 Tableau de Répartition des VLANs et Adressage IP

### 7.2 Configuration des VLANs dans pfSense

La configuration des VLANs dans pfSense s'est déroulée en plusieurs étapes :

Création des VLANs dans **Interfaces > Assignments > VLANs**

Chaque VLAN a été créé sur l'interface physique LAN (par exemple vmx1) en attribuant un VLAN tag :


- VLAN 110 → tag 110
- VLAN 120 → tag 120
- VLAN 130 → tag 130

Affectation d'une interface virtuelle à chaque VLAN

Après avoir créé les VLANs, ils ont été assignés comme interfaces dans Interfaces > Assignments, renommés pour plus de clarté :

- OPT1 → VLAN\_Admin (192.168.100.1/24)
- OPT2 → VLAN\_Dev (192.168.100.65/26)
- OPT3 → VLAN\_Invites (192.168.100.129/26)

Activation du DHCP Server sur chaque interface VLAN (menu Services > DHCP Server) pour distribuer automatiquement les IPs aux postes selon leur VLAN.


 Capture d'écran à insérer : Configuration d'un VLAN dans pfSense (ex. VLAN 120) avec IP statique et DHCP activé.

### 7.3 Configuration des ports sur les switchs (ou dans Proxmox)

Dans un environnement réel, les ports des switchs doivent être configurés en mode trunk (vers pfSense) et en mode access (vers les machines clientes). Dans notre cas virtualisé sous Proxmox :

Un Linux Bridge par VLAN est défini (vmbr110, vmbr120, vmbr130)

Chaque VM est reliée à son VLAN par une interface connectée au bridge correspondant

 Capture d'écran à insérer : Configuration réseau d'une VM dans Proxmox reliée à un bridge VLAN spécifique.

### 7.4 Règles de Pare-feu inter-VLAN dans pfSense

Par défaut, pfSense ne permet aucune communication entre les VLANs, sauf si une règle explicite est ajoutée. L'objectif de Cyberlogix Solutions étant de cloisonner les flux au maximum, les règles suivantes ont été définies :

 VLAN 110 - Administration (192.168.100.0/24)

Accès complet à tous les VLANs

Règle : Allow Any vers tous les réseaux internes (utilisateurs IT uniquement)

## VLAN 120 - Développement (192.168.100.64/26)

Accès uniquement à certains serveurs internes dans VLAN 110 (par exemple : GitLab, Base de données)


Règle : Allow TCP vers IP serveur GitLab : 192.168.100.10 port 22, 80, 443

Blocage de tout autre trafic inter-VLAN

## VLAN 130 - Invités (192.168.100.128/26)

Accès uniquement à Internet (NAT)

Blocage total des communications avec les autres VLANs


 Capture d'écran à insérer : Exemple de règles de pare-feu dans Firewall > Rules > VLAN\_Dev avec accès limité uniquement aux serveurs internes.

## 7.5 Commandes pour tester la segmentation

Afin de valider la bonne isolation réseau, plusieurs tests ont été réalisés depuis des postes situés dans chaque VLAN. Par exemple :

Depuis un poste en VLAN 130 (Invités) : ping 192.168.100.1 → Réussite (gateway) ping 192.168.100.10 → Échec (serveur Git interdit)

Depuis VLAN 120 (Dev) : telnet 192.168.100.10 443 → Succès (serveur Git autorisé) telnet 192.168.100.1 22 → Échec (SSH interdit sur pfSense)

 Capture d'écran à insérer : Console d'un poste en VLAN invité montrant échec du ping vers un serveur interne.

## 8. Déploiement d'un Proxy HTTP/HTTPS avec Filtrage Web (Squid + SquidGuard)

Dans un environnement professionnel, il est fondamental de contrôler les usages d'Internet afin de garantir un comportement conforme aux politiques de sécurité de l'entreprise, d'optimiser la bande passante, et de prévenir l'accès à des contenus inappropriés ou malveillants. Pour répondre à cette exigence, Cyberlogix Solutions a décidé d'implémenter une solution de proxy transparent avec filtrage web, en s'appuyant sur deux outils puissants et largement utilisés dans le monde professionnel : Squid, qui joue le rôle de proxy HTTP/HTTPS, et SquidGuard, qui permet de filtrer les sites en fonction de catégories (blacklists).


L'objectif était de rediriger tout le trafic HTTP/HTTPS sortant à travers le serveur pfSense pour le contrôler, tout en définissant des politiques d'accès distinctes selon les VLANs et groupes d'utilisateurs (grâce à l'authentification LDAP).

### 8.1 Installation des paquets Squid et SquidGuard

Dans l'interface pfSense, le déploiement s'est fait via le gestionnaire de paquets intégré : Aller dans System > Package Manager > Available Packages  
Rechercher puis installer successivement :

Squid  
SquidGuard

Une fois installés, les deux modules sont apparus dans le menu **Services > Proxy Server et Proxy Filter**.

 Capture d'écran à insérer : Interface pfSense montrant Squid et SquidGuard comme paquets installés.

## 8.2 Configuration de Squid en proxy transparent

Pour éviter de devoir configurer manuellement chaque poste utilisateur, Squid a été configuré en mode transparent, ce qui permet d'intercepter automatiquement le trafic HTTP (et HTTPS avec SSL bumping) sortant des clients.


Dans **Services > Proxy Server > General**, les paramètres suivants ont été appliqués :  
Proxy Interface : **VLAN\_Dev, VLAN\_Invites (interfaces concernées)**

Allow Users on Interface : ☒

Transparent HTTP Proxy : ☒ activé

SSL Man In the Middle Filtering (SSL Bump) : ☒ activé pour HTTPS

HTTPS/SSL Interception : enable, avec un certificat local généré via le Cert. Manager

 Capture d'écran à insérer : Paramétrage du proxy transparent dans l'onglet General Settings de Squid.

Une autorité de certification (CA) locale a été créée dans **System > Cert. Manager > CAs** pour signer les certificats SSL internes utilisés par Squid pour décrypter le trafic HTTPS.

Les utilisateurs des **VLANs 120** (Dev) et **130** (Invités) ont reçu ce certificat via GPO ou script d'import, afin que leurs navigateurs ne détectent pas d'alerte de sécurité SSL.

## 8.3 Configuration du filtrage web avec SquidGuard

Dans **Services > SquidGuard** Proxy Filter, SquidGuard a été activé avec les options suivantes :

Blacklist source : Liste gratuite Shalla's ou Université de Toulouse (catégories de sites par URL)

Règles globales :

**Bloquer : pornographie, jeux en ligne, réseaux sociaux, sites malveillants**


**Autoriser : moteurs de recherche, sites professionnels, outils de développement**

Des groupes d'accès ont été créés selon l'origine des requêtes (adresse IP ou VLAN) :

**Groupe DEV (192.168.100.64/26)** : accès large mais filtrage jeux et réseaux sociaux

Groupe INVITES (192.168.100.128/26) : accès restreint à une liste blanche uniquement (moteurs de recherche et pages institutionnelles)

Dans l'onglet Common ACL, des messages personnalisés ont été configurés pour informer les utilisateurs du blocage d'une page.

 Capture d'écran à insérer : Page d'erreur personnalisée SquidGuard affichant "Site interdit par la politique de sécurité de Cyberlogix Solutions".

## 8.4 Redirection du trafic via règles de pare-feu


Même si Squid est configuré en mode transparent, il est essentiel de s'assurer que les ports 80 et 443 sont bien redirigés depuis les VLANs concernés.

Dans Firewall > Rules > VLAN\_Dev et VLAN\_Invites, les règles suivantes ont été définies :

Pass : TCP → ports 80, 443 → Destination : any → Gateway : default

Redirect vers Squid local (en proxy interceptant)

Optionnellement, pour les VLANs non concernés (comme VLAN\_110 Admin), ces ports ne sont pas redirigés, afin de garantir un accès Internet direct aux administrateurs.

 Capture d'écran à insérer : Règles de redirection des ports HTTP/HTTPS vers Squid depuis VLAN\_130.

## 8.5 Tests fonctionnels du proxy et du filtrage

Des tests ont été effectués depuis différents postes dans les VLANs pour vérifier :

Navigation autorisée : vers <https://www.google.com> et <https://www.cyberlogix.fr>

Blocage : tentative d'accès à <https://www.facebook.com>, <https://www.jeuxvideo.com> → page de blocage affichée

Commandes de test :

Sur un poste Linux :

curl -I <http://www.facebook.com>

→ Résultat : redirection vers la page de blocage du proxy.

## **9. Mise en Place d'un Système de Détection et de Prévention d'Intrusion (IDS/IPS) avec Suricata**

Dans le contexte d'une cybersécurité proactive et d'une supervision avancée des menaces réseau, l'entreprise Cyberlogix Solutions a souhaité intégrer un IDS/IPS (Intrusion Detection and Prevention System) capable de surveiller en temps réel l'ensemble du trafic réseau, d'analyser les paquets, de détecter les comportements anormaux, et surtout de bloquer automatiquement les attaques potentielles en provenance d'Internet ou d'un poste compromis à l'intérieur du réseau.

Après étude comparative des principales solutions open source disponibles, le choix s'est naturellement porté sur Suricata, en raison de sa compatibilité native avec pfSense, de sa capacité à effectuer de l'inspection profonde des paquets (DPI), de son support multithread, et de sa prise en charge complète des protocoles réseau modernes.


### **9.1 Installation de Suricata sur pfSense**

L'installation s'est effectuée directement via le gestionnaire de paquets de pfSense :

**System > Package Manager > Available Packages**

Recherche du paquet Suricata

Installation sur le système pfSense principal (Master)

 Capture d'écran à insérer : Menu de gestion des paquets de pfSense montrant Suricata installé.

## 9.2 Configuration initiale de Suricata

Une fois installé, Suricata est accessible via Services > Suricata. La configuration initiale a été appliquée comme suit :

Enable Interface : Oui

Interface sélectionnée : VLAN\_Admin (192.168.100.0/24) et WAN

Blocking Mode : activé (IPS actif)


IPS Policy : "Security" (politique agressive)

Log to System Log : activé

Interface Setup :

Promiscuous Mode : Oui (pour capturer tous les paquets)

Checksum Validation : désactivé pour compatibilité

 Capture d'écran à insérer : Écran principal de configuration de l'interface Suricata sur VLAN\_Admin et WAN.


## 9.3 Téléchargement et gestion des règles (rule sets)

Pour détecter les intrusions, Suricata s'appuie sur un ensemble de règles d'analyse réseau. Les sources activées incluent :

- ET Open Ruleset (Emerging Threats Open)
- Snort VRT Ruleset (si enregistré)
- SSLBL, DShield, SSL-FP : listes IP malveillantes

Dans l'onglet Global Settings, les options suivantes ont été activées :

- Automatically Update Rules : ☒
- Update Frequency : Every 12 hours
- Dans l'onglet Categories, les catégories suivantes ont été activées :
- trojan-activity
- web-server-attack
- exploit-kit
- sql-injection
- dns-attack

 Capture d'écran à insérer : Liste des catégories de règles activées dans l'interface Suricata.

## 9.4 Activation du mode blocage (IPS)


Pour passer du mode détection (IDS) à un mode prévention (IPS) actif, Suricata a été configuré pour bloquer automatiquement les connexions malveillantes détectées, via l'option :

**Block Offenders : activé**

**Kill States on Block : Oui (termine les connexions actives)**

**Suppress List : utilisée pour éviter les faux positifs récurrents**

Cela permet de répondre immédiatement à une attaque détectée, par exemple un port scanning ou une tentative d'exploitation de faille.

 Capture d'écran à insérer : Activation du mode blocage IPS dans l'onglet interface de Suricata.

## 9.5 Analyse des alertes et suivi des événements

Les alertes générées par Suricata sont visibles dans Services > Suricata > Alerts, où chaque événement est affiché avec :

Signature de la règle

Adresse source/destination

Protocole

Port

Catégorie de menace

Exemple d'alerte détectée :

ET POLICY External IP accessing SSH on non-standard port

Dans le cas d'un faux positif, l'option Suppress this Alert a été utilisée pour éviter le blocage à l'avenir.

 Capture d'écran à insérer : Interface "Alerts" de Suricata montrant une alerte détectée avec action de blocage automatique.

## 9.6 Vérification du bon fonctionnement

Plusieurs tests ont été réalisés pour s'assurer de l'efficacité de Suricata :

Scan de port simulé depuis une VM externe :

Commande :

**nmap -sS -p 1-1000 192.168.100.10**

Résultat : détection par Suricata et blocage de l'IP source

Navigation vers site malveillant volontairement listé (test) :

Blocage immédiat du site

## **10. Mise en Place d'un Système de Supervision Avancée avec Zabbix, Grafana et la Stack ELK**

Dans une infrastructure réseau moderne, la visibilité en temps réel sur l'état des équipements, la collecte centralisée des événements, la détection proactive des anomalies et l'analyse historique des performances sont des exigences fondamentales pour assurer une exploitation fiable, sécurisée et optimisée du système d'information. Consciente de ces enjeux, l'entreprise Cyberlogix Solutions a déployé une solution de monitoring multi-niveaux, combinant à la fois la surveillance technique, la visualisation graphique, et la centralisation des logs, en s'appuyant sur des outils open source puissants et interopérables : Zabbix, Grafana, et ELK.

### **10.1 Déploiement de Zabbix pour la supervision technique**

#### *10.1.1 Présentation de Zabbix*

Zabbix est une solution de monitoring centralisé permettant de surveiller la disponibilité, les performances, l'utilisation des ressources (CPU, RAM, réseau, disque) de serveurs, de services et d'équipements réseau. Il permet également de définir des seuils d'alerte, de recevoir des notifications, et de visualiser les métriques collectées sur le long terme. Dans notre projet, Zabbix a été utilisé pour surveiller les VMs critiques (pfSense, Suricata, proxy, serveur AD), ainsi que les services déployés en production.

#### *10.1.2 Installation via Docker sur la VM Debian*

Sur une machine Debian (192.168.100.10), Docker a été utilisé pour déployer les conteneurs Zabbix de manière isolée et reproductible.

Voici les commandes utilisées :

```
**apt update && apt install -y docker.io docker-compose**
```

Cette commande permet d'installer Docker, l'outil de conteneurisation utilisé pour déployer Zabbix et ses services associés.

Un fichier docker-compose.yml a été rédigé contenant les services suivants :

- zabbix-server-mysql



- mysql-server (avec base zabbix préconfigurée)
- zabbix-frontend-apache
- zabbix-agent

Une fois les conteneurs démarrés :

**\*\*docker-compose up -d\*\***

Zabbix a été accessible à l'adresse : <http://192.168.100.10:8080>

### *10.1.3 Ajout d'hôtes et définition des seuils*

Les hôtes suivants ont été ajoutés dans l'interface Zabbix :

pfSense (via SNMP)

VM Debian (via Zabbix Agent)

Serveur AD (via ping + agent)

Interface OpenVPN (check disponibilité)


Des seuils d'alerte ont été définis :

CPU > 90% pendant 2 minutes

Espace disque < 10%

Interface WAN inaccessible

Perte de connectivité sur un VLAN

 Capture d'écran à insérer : Tableau de supervision des hôtes dans Zabbix avec statut (OK, Warning, High).

## 10.2 Intégration avec Grafana pour la visualisation graphique

### *10.2.1 Pourquoi Grafana ?*

Zabbix intègre ses propres tableaux, mais Grafana offre une expérience utilisateur supérieure, avec des dashboards dynamiques, une personnalisation graphique avancée, et une interopérabilité avec plusieurs sources de données. Il a été utilisé pour créer des tableaux de bord clairs, consultables par l'équipe IT en un coup d'œil.

### *10.2.2 Connexion de Grafana à Zabbix*

Grafana a été installé sur la même VM Debian, également via Docker :

**\*\*docker run -d -p 3000:3000 --name grafana grafana/grafana\*\***

Ensuite, via l'interface Web <http://192.168.100.10:3000>, le plugin Zabbix datasource a été ajouté.

Des dashboards ont été créés :

- Utilisation CPU/RAM des hôtes
- Bande passante WAN/WAN2
- Historique des alertes
- Connexion VPN en temps réel

## 10.3 Collecte des logs réseau avec la Stack ELK (Elasticsearch, Logstash, Kibana)

### *10.3.1 Objectif de la stack ELK*

Alors que Zabbix et Grafana surveillent des métriques, ELK est dédié à la centralisation et l'analyse des logs, particulièrement utile pour identifier des comportements suspects, retracer des événements de sécurité, et effectuer des recherches historiques sur incidents.

### *10.3.2 Déploiement sur Debian via Docker*

La stack ELK a été installée en tant que service Docker :

```
**docker-compose up -d**
```

Avec les services :

- Elasticsearch : moteur d'indexation des logs
- Logstash : pipeline d'ingestion
- Kibana : interface d'exploration visuelle

Les logs envoyés par pfSense, Suricata, et le proxy (via syslog) sont centralisés ici.

## *10.4 Alertes et Notifications Automatisées*

Des alertes mail ont été configurées dans Zabbix et Suricata pour informer immédiatement l'équipe IT :

- Mail en cas de montée en charge CPU
- Mail si l'interface WAN2 prend le relais (failover actif)
- Alerte si Suricata détecte un scan massif

## **11. Tests Fonctionnels, Scénarios de Panne et Mesures Correctives**

Afin de garantir que l'infrastructure réseau mise en place réponde bien aux objectifs définis initialement par Cyberlogix Solutions, une série de tests fonctionnels complets et de scénarios de panne a été élaborée, mise en œuvre, et analysée. L'objectif de ces tests était de valider la résilience, la sécurité, la continuité de service, ainsi que la capacité des systèmes à détecter, bloquer, rediriger ou restaurer les services en cas de défaillance partielle ou totale d'un composant de l'architecture.

### **11.1 Test de basculement du cluster pfSense (CARP)**


Objectif du test : Vérifier que le basculement automatique entre le pfSense Master et le Backup se fait de manière transparente pour les utilisateurs.

Procédure :

- Extinction brutale de la VM pfSense Master via Proxmox.
- Observation du comportement de l'IP virtuelle CARP (192.168.100.1).
- Vérification de la continuité réseau sur un client connecté (ping, navigation).

Résultat :

- Le pfSense Backup a immédiatement repris l'adresse CARP.
- Aucune interruption de connectivité pour les clients.
- L'alerte de basculement a été enregistrée dans Zabbix et affichée dans Grafana.

 Capture d'écran à insérer : Dashboard Zabbix montrant l'état "DOWN" du Master et "UP" du Backup avec timestamp précis.

### **11.2 Test du Failover WAN (perte du lien principal)**

Objectif du test : S'assurer que le groupe de passerelles WAN\_FAILOVER redirige automatiquement le trafic vers WAN2 en cas de perte de WAN1.


Procédure :

- Simulation d'une coupure de l'interface WAN1 (désactivation dans Proxmox).
- Lancement d'un ping continu vers une IP externe depuis un poste client.
- Observation du changement de route via traceroute.

Résultat :

- Coupure détectée par pfSense via le système de monitoring.
- Bascutage automatique vers WAN2 sans perte de session notable.

- L'alerte "WAN1 gateway down" a été générée dans Zabbix.

 Capture d'écran à insérer : Traceroute avant/après montrant la bascule de route, et alerte dans pfSense.

### 11.3 Test de montée en charge réseau

Objectif du test : Vérifier le comportement de l'infrastructure sous forte sollicitation réseau.

Procédure :

- Lancement d'un stress test réseau depuis plusieurs machines (scripts de téléchargement simultané + navigation).
- Observation en temps réel de la bande passante dans Grafana.
- Surveillance des ressources dans Zabbix.

Résultat :

- Pic de trafic bien visible sur l'interface WAN.
- L'utilisation CPU/RAM de pfSense et de la VM proxy est restée stable.
- Aucune latence excessive, preuve d'une bonne répartition de charge.

 Capture d'écran à insérer : Graphique Grafana montrant le pic de bande passante avec stabilisation.

### 11.4 Simulation d'attaque réseau détectée par Suricata

Objectif du test : Tester la détection active d'une attaque réseau (ex. scan de ports, attaque brute force) et la réaction automatique du système IDS/IPS.

Procédure :

Lancement d'un scan Nmap depuis une machine externe vers une IP du réseau

192.168.100.0/24 :

```
nmap -sS -p- 192.168.100.10
```

Observation du log dans Suricata.

Vérification de l'adresse source dans la liste des IP bloquées.

Résultat :

- Alerte générée par Suricata : "ET SCAN Nmap Scripting Engine User-Agent Detected".
- L'IP source a été automatiquement bloquée.
- Notification email envoyée via Zabbix.

 Capture d'écran à insérer : Alertes Suricata avec blocage IPS actif et email reçu.

## 11.5 Vérification du fonctionnement du filtrage Squid/SquidGuard

Objectif du test : Contrôler que les politiques d'accès Internet par VLAN sont bien appliquées.

Procédure :

- Connexion à Internet depuis un poste en VLAN 130 (Invités).
- Tentative d'accès à un site bloqué (<https://facebook.com>).
- Tentative d'accès à un site autorisé (<https://fr.wikipedia.org>).

Résultat :

- Accès refusé vers site interdit, page de blocage affichée.
- Accès autorisé vers site permis.
- Logs disponibles dans Kibana.

 Capture d'écran à insérer : Page de blocage proxy et log correspondant dans Kibana.

## 11.6 Simulation de panne du serveur Zabbix

Objectif du test : Vérifier que l'indisponibilité du serveur de supervision n'impacte pas la continuité des autres services.

Procédure :

- Arrêt de la VM contenant Zabbix.
- Vérification de la continuité du trafic réseau, des tunnels VPN, des accès proxy.

Résultat :

- Aucun impact sur les services réseau.
- Seules les alertes automatiques ont été suspendues.
- Notification d'indisponibilité de la supervision par mail dès son retour.

 Capture d'écran à insérer : Email de reprise de service de Zabbix après indisponibilité

## **12. Conclusion Générale du Projet**

À l'issue de ce projet intitulé "Infrastructure Réseau Sécurisée et Haute Disponibilité avec pfSense", l'entreprise Cyberlogix Solutions dispose désormais d'une architecture réseau professionnelle, robuste, sécurisée et hautement disponible, parfaitement adaptée à ses besoins actuels, et dimensionnée pour accompagner sa croissance future. Ce projet, conduit dans un environnement virtualisé sous Proxmox VE afin de simuler les conditions réelles d'un déploiement en production, a permis de mettre en œuvre une infrastructure cohérente, répondant aux standards modernes de cybersécurité, de résilience réseau, d'administration centralisée et de supervision.

Grâce à la mise en place d'un cluster pfSense en haute disponibilité (CARP), l'entreprise bénéficie d'une continuité de service assurée, même en cas de défaillance de l'un des pare-feux. L'intégration de deux connexions WAN redondantes avec basculement automatique permet de maintenir l'accès à Internet sans interruption, garantissant la productivité des utilisateurs et la disponibilité des services en ligne.

La segmentation réseau par VLAN a permis d'isoler les flux internes selon les services (Administration, Développement, Invités), renforçant ainsi la sécurité des échanges et la maîtrise des accès. Cette segmentation a été accompagnée de règles de pare-feu strictes, définies sur mesure pour chaque environnement, assurant une circulation des données contrôlée et conforme aux exigences métiers.

La mise en œuvre d'un proxy filtrant avec Squid et SquidGuard permet aujourd'hui à l'entreprise de contrôler avec précision les usages d'Internet en fonction des profils d'utilisateurs, tout en bloquant l'accès à des sites inappropriés ou à risque. Cette solution a été renforcée par l'intégration de Suricata, un IDS/IPS actif, capable de détecter et bloquer en temps réel les tentatives d'intrusion, les scans de ports, les activités suspectes, contribuant à une sécurité réseau dynamique et intelligente.

Enfin, le déploiement d'un système de supervision avancée multi-outils, combinant Zabbix pour la surveillance technique, Grafana pour la visualisation des métriques, et ELK pour la centralisation et l'analyse des logs, offre à l'équipe informatique une visibilité complète, en temps réel et historique, sur l'ensemble de l'infrastructure, permettant une réaction rapide en cas d'incident et un pilotage optimal de l'environnement réseau.

Ce projet a également permis de mettre en œuvre de nombreux tests fonctionnels et scénarios de panne, qui ont démontré la fiabilité et la résilience de l'architecture en place. Chaque élément critique de l'infrastructure a été testé, monitoré, et documenté, garantissant la stabilité du système dans les conditions les plus exigeantes.

En plus de ses résultats techniques, ce projet a permis de développer des compétences concrètes en administration réseau, en cybersécurité, en gestion d'infrastructure virtualisée, en automatisation et en supervision, offrant ainsi une base solide pour la gestion continue du système d'information.