

MIPIH ÉDITEUR ET UN HÉBERGEUR DU MONDE DE LA SANTÉ

Le petit Chaperon Rouge (feat. Le petit Poucet)



Réalisé Par:
INVINCIBLE_ ISITCOM

INSTITUT SUPÉRIEUR D'INFORMATIQUE ET DES TECHNOLOGIES DE COMMUNICATION

Année Universitaire : 2022-2023

1 Introduction

Aujourd'hui, il y a de plus en plus de systèmes d'information dans les entreprises qui sont importants et compliqués. La nécessité de maintenir et de gérer ces systèmes représente une priorité.

Un système d'information se représente par un ensemble des ressources matériels, logiciels et aussi des données. Le SI est toujours mis en face à plusieurs types d'attaques. Elles ne ciblent plus seulement les systèmes techniques, mais ciblent aussi directement les personnes. Face à ces attaques, les solutions de sécurité informatique protègent les systèmes et les réseaux informatiques pour garantir l'intégrité, la confidentialité et la disponibilité des données, pour garantir ces services il vaut mieux adopter le model Zero trust.

Zero Trust est un modèle de sécurité réseau selon lequel aucune personne, ni aucun terminal à l'intérieur ou à l'extérieur du réseau d'une entreprise ne doit avoir accès à nos systèmes. Le modèle Zero Trust repose sur une authentification et une autorisation renforcée pour chaque terminal et chaque personne, empêchant tout accès ou transfert de données sur un réseau privé, que ce soit à l'intérieur ou à l'extérieur de ce périmètre réseau ou services informatiques tant qu'il n'est pas authentifié et vérifié en permanence.

2 Problématique

Dans le cas de transfert des données sensibles (exemple : des résultats d'analyses de VIH) vers une destination précise on a le chemin de transmission des données est plein des dangers et des attaques.

3 Spécifications de besoins

Pour remédier à ces problèmes étudiés, on a besoin de :

- 1- Il faut assurer que les données arrivent bien à notre destination :il faut que les données ne soient pas interceptées par un hacker (vole des données)
- 2- Le hacker ne doit pas avoir un accès sur les données cad, assurer l'intégrité de donnée (les données ne doit être modifier par le hacker)
- 3- On doit garantir une trace du chemin parcouru pour assurer la traçabilité.

4 Les solutions

Pour prévenir le problème étudié. Nous avons choisi d'assurer la mise en place d'un pare-feu open source efficace dans lequel on va activer des fonctionnalités qui ont pour but de garantir la sécurité du réseau entre un émetteur et un récepteur vu les différentes menaces qui peuvent le toucher. La solution mise en place doit répondre aux attentes suivantes tout en gardant la

simplicité de cette solution :

- L'authenticité : authentication + identification.
- garantir l'authentification par jeton.
- garantir la traçabilité.

Selon le model Zero trust (Never trust always verify) on doit sécuriser tous (device, data, lien de transmission ...), Les appareils ne doivent pas être approuvés par défaut, on doit suivre tout changements sur le comportement de paquet, de device, des user

Une vérification d'identité solide doit être appliquée (authentification mutuelle, authentification a deux facteurs + reconnaissance faciale + empreinte digital, rotation des mots de passe ...) aussi on doit valider la conformité de l'appareil avant d'accorder l'accès.

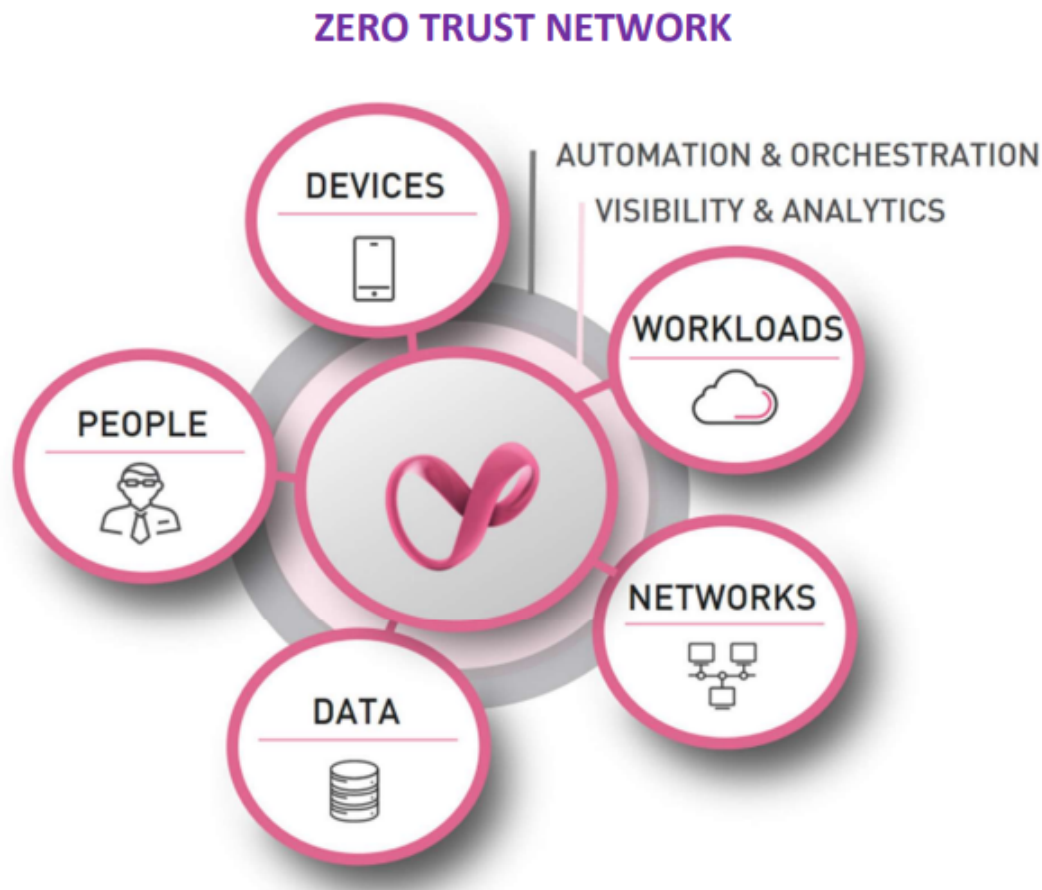


Figure 1: Modèle ZERO TRUST

Dans notre solution nous avons choisi d'utiliser le pare-feu pfSense vue qu'il est open source et garantie ces fonctionnalités :

- Du côté des fonctionnalités VPN, pfSense propose quatre modes de connexion : OpenVPN, VPN PPTP, VPN IPSEC et VPN L2TP.
- Création de portail captif
- IDS/IPS

- Rapport et monitoring (SIEM).
- Systèmes de provisioning rapide
- Des outils de protection des appareils
- Contrôle des accès adaptatif
- Security Orchestration, Automation, and Response
- Un système de configuration d'alias qui simplifie la création des règles complexes.
- Autorité de certificat qui délivre et gère des certificats internes.

Aussi on a choisi d'utiliser OpenVPN vue qu'il est open source et garantie ces fonctionnalités

:

- Chiffrement fort qui exploite openssl.
- Algorithmes utilisés : 3DES, AES, RC5, Blowfish.
- Chiffrement 128 bits avec clé 1024 bits.
- Offre une grande stabilité et fiabilité.
- Sa configuration est simple.
- audité et testé de manière approfondie.
- Compatible avec plusieurs logiciels et pratiquement tous les fournisseurs VPN modernes.

Aussi on a choisi d'utiliser la solution squid implémenté dans pfSense pour enregistrer les

logs :

Squid est un serveur cache proxy, il stocke les pages souvent visitées pour éviter de les télécharger à chaque connexion

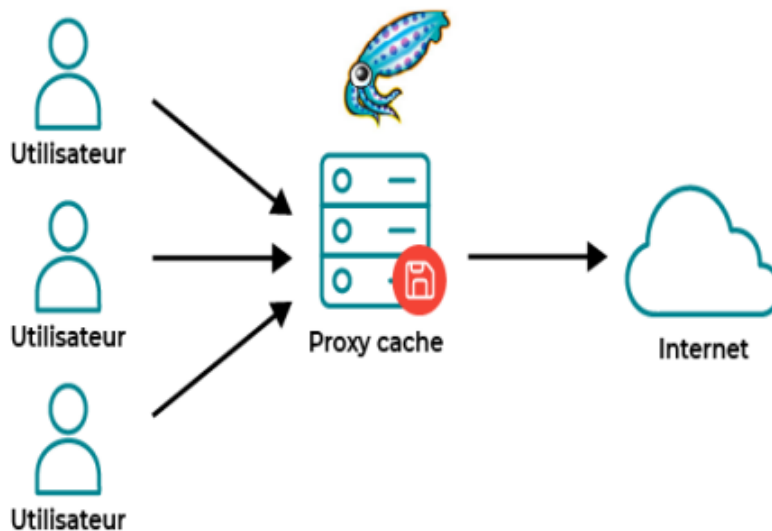


Figure 2: Proxy squid

Pour assurer une architecture d'une organisation à haut niveau de sécurité, on propose cette architecture qu'on a modéliser à l'aide de l'outil Microsoft Visio qui assure la sécurité réseau, des équipements, workload, identités des utilisateurs, des données :

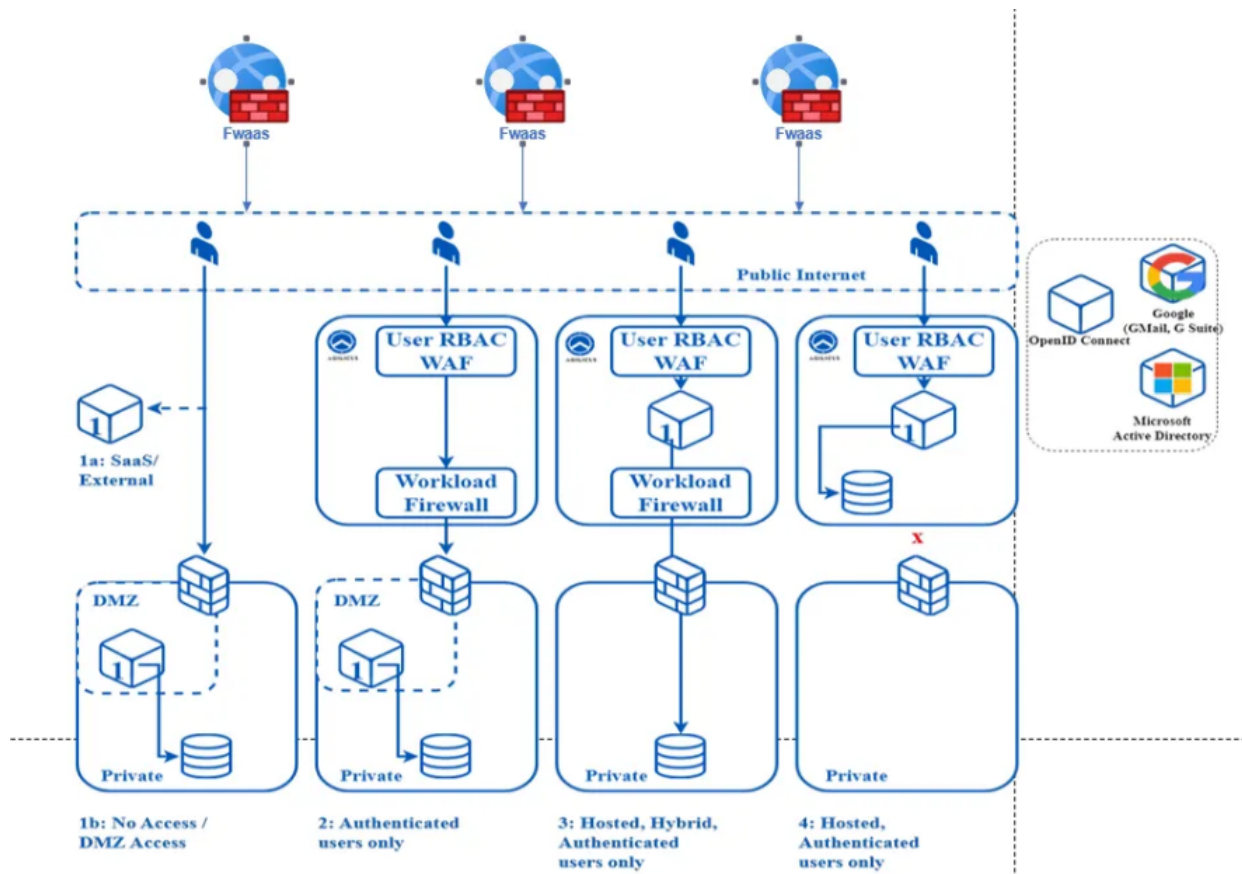


Figure 3: Architecture complète du modèle ZERO TRUST

5 Configuration de VPN au niveau pfSense

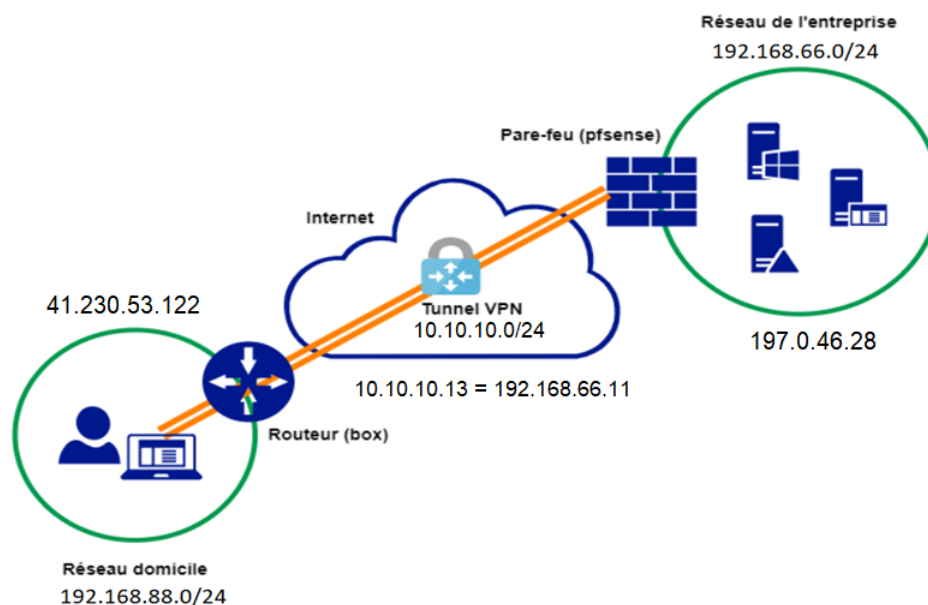


Figure 4: Configuration VPN

Au cours de cette configuration, nous avons configuré openVPN au niveau pfSense pour assurer l'authenticité des utilisateurs

Nous sommes placés dans le réseau LAN 192.168.88.0/24 et nous avons une adresse IP publique : 41.230.53.122 et nous allons essayer de nous connecter à un hôte qui se trouve dans le réseau LAN 192.168.66.0/24 d'adresse IP publique : 197.0.46.28 via le VPN.

Pour l'authentification j'ai utilisé un compte utilisateur locale au Pare-feu pfsense et pour le mode de connexion au serveur VPN, j'ai utilisé l'Accès à distance (SSL/TLS + authentification de l'utilisateur basée sur un nom d'utilisateur et un mot de passe client lors de la connexion).

Etape 1 : Création d'autorité de certification et Certificat de serveur Open VPN

Pour les paramètres de serveur, nous avons spécifié l'adresse du réseau VPN : 10.10.10.0/24, ainsi, lorsqu'un client se connecte en VPN, il obtiendra une adresse IP dans ce réseau.

Ensuite, nous avons spécifié l'adresse de réseau LAN que nous souhaitons rendre accessibles via ce tunnel VPN : 192.168.66.0/24.

Dans les paramètres des clients, nous avons coché l'option « Dynamic IP » : si l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN.

VPN / OpenVPN / Servers						
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export						
OpenVPN Servers						
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions	
WAN2	UDP4 / 1194 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	accès distant openVPN		

Figure 5: Certificat du serveur OpenVPN

Etape 2 : Exportation de la configuration OpenVPN et Création des règles de pare-feu pour OpenVPN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	1 / 76 KiB	IPv4 UDP	*	*	WAN2 address	1194 (OpenVPN)	*	none	accès distant openVPN	

Figure 6: Règles VPN

Etape 3 : Test d'accès distant depuis un poste client

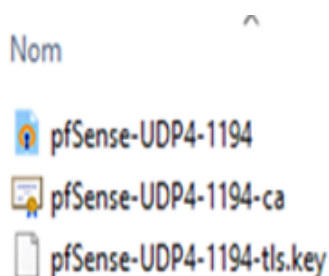


Figure 7: Fichier de config VPN

pfSense-UDP4-1194

Utilisateur:

Mot de passe:

☐ Se souvenir du mot de passe

Figure 8: Authentification VPN

```

Carte inconnue OpenVPN TAP-Windows6 :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::2c82:f553:c76f:1ed2%15
Adresse IPv4. . . . . : 10.10.10.13
Masque de sous-réseau. . . . . : 255.255.255.0

```

Figure 9: Test de connexion VPN

6 Authentification avec jeton

Plusieurs méthodes d'authentification telles que l'authentification basée sur Push, les mots de passe logiciels à usage unique (OTP), les jetons, les codes de contournement et les mots de passe à usage unique par e-mail garantissent que les utilisateurs finaux peuvent toujours se connecter en toute sécurité. Pour assurer cette étape on va activer la prise en charge de Mobile-One-Time-Password (mOTP) avec le package FreeRADIUS . Au cours de lequel on génération de jeton toutes les 60 secondes par exemple.

Le mécanisme d'authentification RSA SecurID consiste en un jeton qui est attribué à un utilisateur d'ordinateur et qui crée un code d'authentification à intervalles fixes (60 secondes par exemple), à l'aide une horloge intégrée et la clé presque aléatoire codée en usine de la carte (connue sous le nom de graine).

La graine est différente pour chaque jeton et est chargée dans le serveur RSA SecurID correspondant (RSA Authentication Manager).

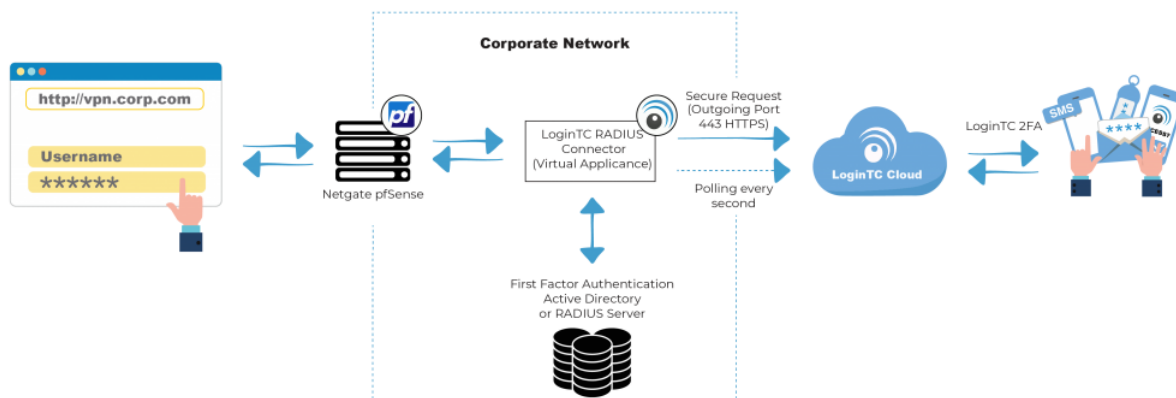


Figure 10: Exemple de configuration OTP

7 Configuration de squid au niveau pfSense

Notre autorité de certification de proxy est sous le nom de « proxy-CA ».



Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
proxy-CA	✓	self-signed	0	CN=internal-ca 		   

Figure 11: Certificat Proxy

Ensuite, nous avons procédé à l'activation du proxy squid sur l'interface LAN via le menu « services ». En activant l'option « Allow users on interface », nous avons obligé tous les utilisateurs de réseau LAN à passer par notre proxy.

De même nous avons activé le mode transparent pour que nous ne soyons pas obligés à installer le certificat sur les postes de travail des utilisateurs.

- Configuration de Lightsquid

Cette étape s'effectue dans l'onglet « Statut > Squid Proxy Reports ». Le port d'écoute de Lightsquid par défaut est 7445.

La figure illustre respectivement le rapport d'accès utilisateur qui est organisé par adresse IP



#	Temps	Utilisateur	Real Name	Connexion(s)	Octets	%
00. Pas dans un groupe						
1		192.168.66.10	?	4 915	30.7 M	73.8%
2		192.168.66.11	?	819	10.9 M	26.1%
					41.6 M	100.0%

Figure 12: Lightsquid

8 Conclusion et perspectives

Dans le cadre de ce défi, on a proposé une solution qui répond aux besoins demandés (L'authenticité de la donnée du début à la fin, garantir l'authentification par jeton, garantir la traçabilité).

Comme perspectives : Utiliser des API pour automatiser les tâches de sécurité et la réponse aux incidents et pour réduire la charge de travail de l'administrateur de sécurité.