TP\_INTERCONNEXION\_VPN

CCI CAMPUS STRASBOURG |BTS SIO SISR 2ème Année

U4\_Concevoir\_Solution\_Infra

FEVRE & HUBER & YILMAZ

2022

Table des matières

[**1. Savoir installer et configurer un serveur PfSense.** 2](#_Toc115783545)

[1.1 Installation de pfsense freeBSD 2](#_Toc115783546)

[1.2 Configuration sur pfsense 5](#_Toc115783547)

[1.3 Configuration depuis client Windows 10 Pro 6](#_Toc115783548)

[**2. Installer et configurer un VPN site à site (IPsec)** 6](#_Toc115783549)

[2.1 Prérequis 6](#_Toc115783550)

[2.2 IPSEC 7](#_Toc115783551)

[2.3 Phase 2 9](#_Toc115783552)

[2.4 RULES 10](#_Toc115783553)

[2.5 Test de connexion 11](#_Toc115783554)

[3. Installer et configurer un VPN distant (OpenVPN) 12](#_Toc115783555)

[4. Problèmes / Résolutions 13](#_Toc115783556)

# **1. Savoir installer et configurer un serveur PfSense.**

**Prérequis**

- Une vm Pfsense FreeBSD sur VMware avec 2 cartes réseaux, une pour le WAN et une pour le LAN.

- Un client Windows 10 (ici c’est un PRO)

## 

## 1.1 Installation de pfsense freeBSD

|  |
| --- |
|  |
| Choisir « Auto ZFS » puis choisir le clavier\* |
|  |
| Sélectionnez « pool Type/Disks » et choisir « No Redundancy » parce qu’on n’a pas besoin de  Mettre en place de redondance dans ce tp. |
|  |
|  |
|  |
| Cocher la case avec la touche « espace » |
|  |

|  |
| --- |
| Puis « ok »  Validez |
|  |
|  |
|  |

|  |
| --- |
|  |

## 1.2 Configuration sur pfsense

|  |
| --- |
| On va configurer l’adresse ip de la carte réseau « LAN » |
|  |

|  |
| --- |
| Choix « 2 » |
| Une image contenant texte  Description générée automatiquement |
| Choisir l’interface « LAN » choix « 2 » puis renseignez les réglages de l’adresse ip suivant  IP: 192.168.30.5  Subnet bit count: 24  DHCP: n |

## 1.3 Configuration depuis client Windows 10 Pro

Configuration de base = carte réseau avec l’ip sur le même réseau que pfsense et mettre l’ip de

pfsense en passerelle (8.8.8.8 en dns pour internet).

Par défaut le login est : admin et le MDP est : pfsense

# **2. Installer et configurer un VPN site à site (IPsec)**

## 2.1 Prérequis

Deux machines virtuelles PFSENSE sur la même connexion (ex partage de connexion) avec l’adressage IP suivant :

Serveur 1 : WAN 192.168.125.113/24

LAN 192.168.30.5

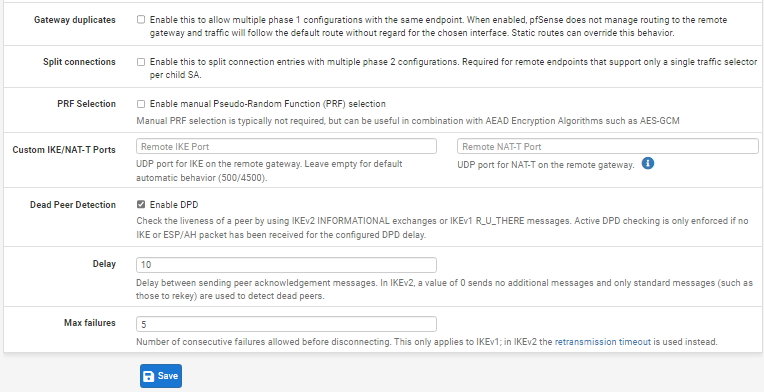
Serveur 2 : WAN 192.168.125.14/24

LAN 192.168.20.5

## 2.2 IPSEC

|  |
| --- |
| Aller dans l’onglet VPN/IPSEC |
|  |
| Cliquez sur le bouton « add P1 » pour ajouter la phase 1 |
|  |
| Remplissez selon la photo ci-dessous  Dans « Remote Gateway » mettre l’addresse ip WAN de l’autre PFSENSE  Dans preshared key, mettez un mot (ex : test vpn) ou générez une clef (il faudra absoluent mettre le même dans l’autre pfsense) |

|  |
| --- |
|  |
|  |



## 2.3 Phase 2

|  |
| --- |
| Cliquez sur « add P2 » pour renseigner la phase 2 |
|  |
| Remplir selon la photo ci-dessus. Dans le remote Network, bien renseignez l’adresse réseau de la LAN de l’autre pfsense |
|  |

|  |
| --- |
|  |

## 2.4 RULES

|  |
| --- |
| Allez dans « Interfaces/WAN » descendre tout en bas de la page puis décochez les 2 cases dans la partie « Reserved Networks » |
|  |
| Ensuite, allez dans l’onglet « Firewall / Rules » Commencez par la partie WAN, modifier la règle en changeant le protocole par « Any » puis sauvegardez |

|  |
| --- |
| Une image contenant texte  Description générée automatiquement |
| Faites pareil pour la partie LAN et IPSEC puis rajoutez une règle en autorisant le protocole ICMP dans IPSEC |
|  |

## 2.5 Test de connexion

|  |
| --- |
|  |

|  |
| --- |
|  |
|  |

# 3. Installer et configurer un VPN distant (OpenVPN)

# 4. Problèmes / Résolutions

|  |  |
| --- | --- |
| Problème de connexion | Pensez à bien être sur le même réseau pour les machines virtuelles |
| Problème de connexion | Bien paramétrer les règles pare-feu |
| Problème de connexion | Désactiver les pare-feu Windows sur les machines hôtes + virtuelles |
| Phase 2 | Bien penser à mettre l’adresse réseau de l’adresse LAN et non l’adresse LAN directement |
|  |  |

Un seul livrable par groupe (nommé sous la forme TP\_VPN\_NOM1\_NOM2.PDF).•Le livrable doit être complet, nomenclaturé et détaillé.•La présentation, la lisibilité, les explications, ainsi que le chapitrage est important.•Pensez à une section débug / résolution de problème / incidents rencontrés et solutions.