BTS S.I.O. option S.I.S.R. - 2025 – 2026

Déploiement d’un VPN Sécurisé

De l’introduction au déploiement d’un VPN en réseau simulé GNS3

Mr Michele Mastrogiacomo

Deploiement d'un VPN Securisé

Sommaire – Guide de déploiement VPN IPsec

Introduction :

Présentation du besoin et objectif du VPN.

Un VPN (Virtual Private Network) peut être défini comme un mécanisme de tunnellisation permettant d'interconnecter de manière sécurisée deux réseaux distants à travers une infrastructure publique, telle qu'Internet. Il garantit la confidentialité, l'intégrité et l'authentification des données échangées.

Ce type de solution est particulièrement adapté aux scénarios de mobilité (travailleurs nomades) et de télétravail, en offrant un accès distant sécurisé aux ressources internes (serveurs, applications, bases de données) d'un réseau d'entreprise ou d'un établissement. Dans ce contexte, il permet notamment au personnel administratif et technique d'accéder au réseau du lycée depuis un site externe, sans présence physique sur le réseau local.

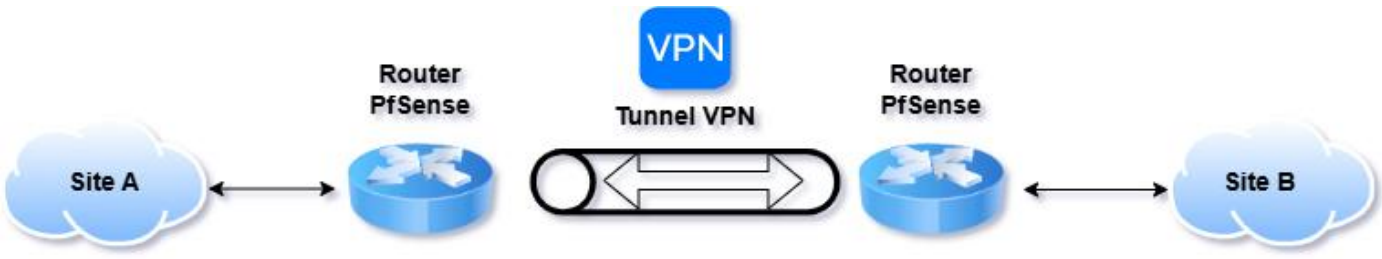
Le fonctionnement d'un VPN repose sur l'utilisation de protocoles de communication sécurisés. Un protocole définit un ensemble de règles et de mécanismes régissant la transmission, le chiffrement et l'authentification des données. Parmi les protocoles les plus répandus figurent IPSec, OpenVPN et WireGuard.

Dans le cadre de ce TP, le protocole utilisé est IPSec (Internet Protocol Security). IPSec opère au niveau de la couche 3 (réseau) du modèle OSI et permet de sécuriser directement les paquets IP via deux mécanismes principaux : AH (Authentication Header) pour l'authentification et ESP (Encapsulating Security Payload) pour le chiffrement et l'intégrité des données. Il est couramment utilisé pour la mise en place de tunnels VPN site-à-site.

À l'inverse, OpenVPN fonctionne au niveau de la couche 7 (application) du modèle OSI et s'appuie sur la bibliothèque SSL/TLS pour établir un tunnel sécurisé, ce qui le rend particulièrement flexible et compatible avec de nombreux environnements.

WireGuard, quant à lui, est un protocole moderne opérant également à la couche 3 (réseau). Il se distingue par une implémentation plus légère et des performances élevées. Il utilise le protocole UDP pour le transport des paquets et repose sur des primitives cryptographiques modernes afin d'assurer la sécurité des communications.

Image 1 – Schema Base VPN



Contexte et architecture réseau

Description de l'infrastructure et des réseaux connectés.

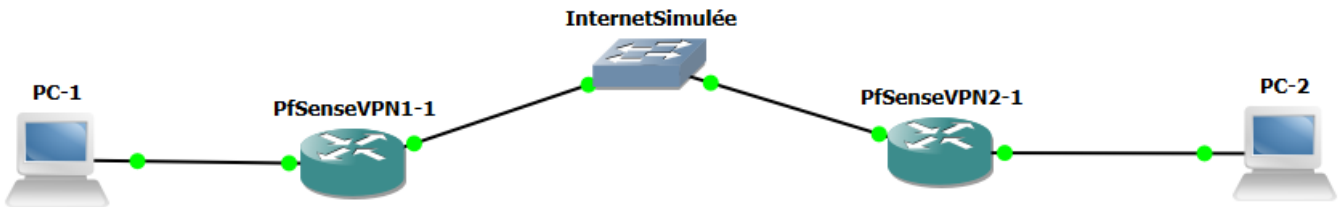
Dans ce TP, j'ai créé une architecture composée de deux sites distants(LAN) interconnectés via un réseau représentant Internet.

Les deux pares-feux sont reliés via leurs interfaces WAN à un réseau intermédiaire simulant Internet. Le VPN IPsec sera configuré entre ces deux équipements afin de permettre la communication sécurisée entre les réseaux locaux. Le VPN IPsec permettra la communication sécurisée entre les réseaux.

Le plan d'adressage simple pour ce tp est le suivant :

• Site A :
  ○ pfSense: 192.168.50.254
  ○ PC Client : 192.168.50.10
  ○ WAN : 192.168.204.138
	• Site B :
	  ○ pfSense: 192.168.70.254
	  ○ PC Client : 192.168.70.10
	  ○ WAN : 192.168.204.131

Image 2 – Topologie réseau en GNS3 (Switch pour un Internet simulé)



Technologies utilisées

Présentation de pfSense et du protocole IPsec

PfSense

pfSense est une solution open source basée sur FreeBSD qui permet de transformer un ordinateur ou une machine virtuelle en pare-feu et routeur complet.

Elle offre de nombreuses fonctionnalités telles que : la gestion du pare-feu, le routage réseau, la mise en place de VPN, le filtrage du trafic, la surveillance du réseau

IPsec

IPsec (Internet Protocol Security) est une suite de protocoles, dont IKE et ESP, qui permet de sécuriser les communications IP en assurant :

- la confidentialité des données (chiffrement)
- l'intégrité des paquets
- l'authentification des équipements
- la protection contre les attaques de type rejeu

Internet Key Exchange (IKEv2)

Ce protocole gère la connexion entre deux routeurs à travers deux phases :

- **Phase 1** : elle crée un canal sécurisé entre les deux pare-feu afin qu'ils puissent négocier les paramètres du VPN.
- **Phase 2** : elle établit le tunnel qui transportera les données du réseau.

Le protocole IKE est plus sécurisé que L2TP et PPTP.

ESP (Encapsulating Security Payload)

ESP assure la confidentialité, l'intégrité des données et l'authentification de la source. Il modifie le paquet d'origine (qui sera restauré à la réception) :
il chiffre le paquet puis modifie l'en-tête IP

Ce chiffrement rend les attaques et tentatives de piratage plus difficiles.

Image 3 – Terminal principal de PfSense de deux reseau

Pfsense Site A VPN1-1

GNS3VM | PfSenseVPN1 | PfSenseVPN2

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 691df05604fc8c52c787

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.204.138/24
 LAN (lan)       -> em1        -> v4: 192.168.50.254/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Pfsense Site B VPN2-1

GNS3VM | PfSenseVPN1 | PfSenseVPN2

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 2bd296330083c9134ae4

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.204.131/24
 LAN (lan)       -> em1        -> v4: 192.168.70.254/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Configuration du VPN IPsec sur pfSense

Dans cette partie, nous configurons un tunnel VPN IPsec entre deux pare-feu pfSense afin de sécuriser les communications entre deux réseaux distants.
Le choix d'IKEv2 permet une meilleure sécurité et une gestion plus efficace des connexions par rapport à IKEv1.
La configuration d'un VPN IPsec repose sur deux phases :

- **Phase 1 (IKE)** : établissement du canal sécurisé entre les deux équipements
- **Phase 2** : définition des flux de données à chiffrer dans le tunnel

Configuration de la Phase 1 (IKE)

Image 4 – Configuration de la Phase 1 de deux pare-feu

IPsec Tunnels

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
Disable	1	V2	WAN 192.168.204.138	Mutual PSK -	AES256-GCM	SHA256	14 (2048 bit)	Phase1	

Show Phase 2 Entries (1)

IPsec Tunnels

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
Disable	1	V2	WAN 192.168.204.131	Mutual PSK -	AES256-GCM	SHA256	14 (2048 bit)	Phase1	

Show Phase 2 Entries (1)

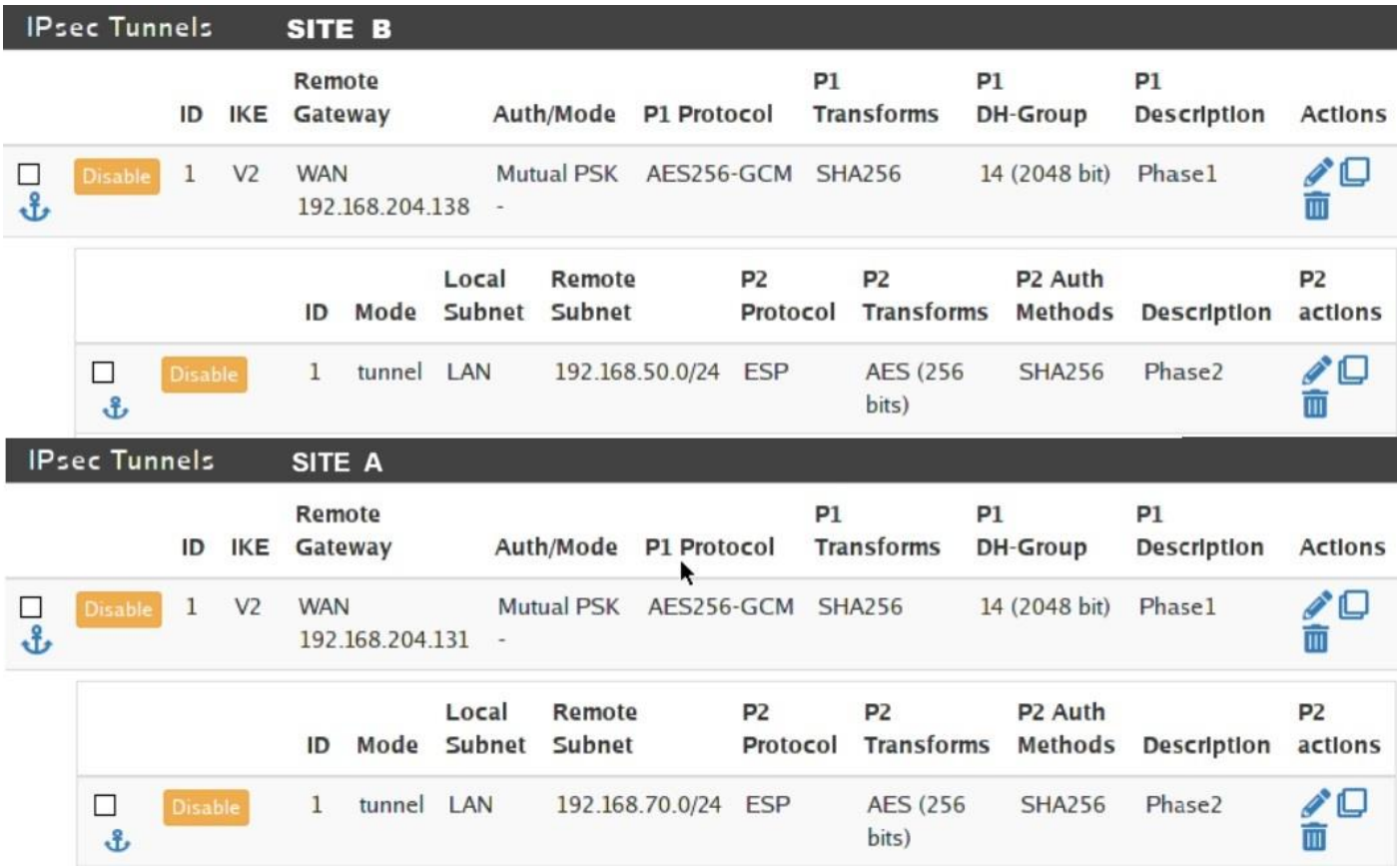
Configuration de la Phase 2

Sur le pare-feu pfSense du Site A, la Phase 2 a été configurée avec les paramètres suivants :

- Mode : Tunnel IPv4
- Protocole : ESP (Encapsulating Security Payload)
- Local Network : LAN Subnet (192.168.50.0/24)
- Remote Network : Network (192.168.70.0/24)
- Type de réseau distant : Network
- Algorithme de chiffrement : AES-256
- Algorithme d'authentification : SHA256

Cette configuration permet d'autoriser les communications entre le réseau local du Site A et le réseau distant du Site B via le tunnel sécurisé.
La configuration de la Phase 2 sur le Site B est symétrique à celle du Site A, avec inversion des réseaux

Image 5 – Configuration de la Phase 2 des deux pare-feu



Configuration des règles firewall

Nous allons configurer les règles de filtrage du pare-feu sont le même sur le deux site avec les adresse des destination de site distante afin de sécuriser les communications entre les différents réseaux.
L'objectif principal est de contrôler le trafic entrant et sortant en appliquant des règles. Les règles mises en place doivent répondre aux objectifs suivants :

- Autoriser uniquement les flux nécessaires
- Bloquer tout trafic non explicitement autorisé (principe du *deny all*)
- Protéger les équipements internes
- Permettre la communication VPN configurée précédemment
- Sécuriser les accès administratifs

Par défaut, pfSense applique une politique de sécurité restrictive sur l'interface WAN. Aucun trafic entrant n'est autorisé sans règle explicite. Cette configuration protège le réseau interne contre les accès non autorisés provenant d'Internet. En ces cas c'est suffisant de bloquer le Bogon.
Enfin La résolution du problème a nécessité l'ajout d'une règle d'exclusion NAT (NO NAT) afin d'éviter la translation des adresses privées, condition indispensable au bon fonctionnement du tunnel IPsec sur GNS3.

Configuration des règles sur l'interface LAN

Afin de permettre aux machines du réseau local d'accéder à Internet, une règle autorisant le trafic sortant doit être mise en place. Normalement sont inséré par défaut. Cette règle permet aux hôtes internes d'émettre des requêtes vers l'extérieur sans restriction.

Image 6 - Règle autorisant le trafic LAN vers * (en ce cas Tous)

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	1/2.05 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
☐ ✓	46/833 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule
☐ ✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule

Autorisation du trafic VPN

Afin de permettre le fonctionnement du tunnel VPN (IKEv2), il est nécessaire d'autoriser les protocoles suivants :

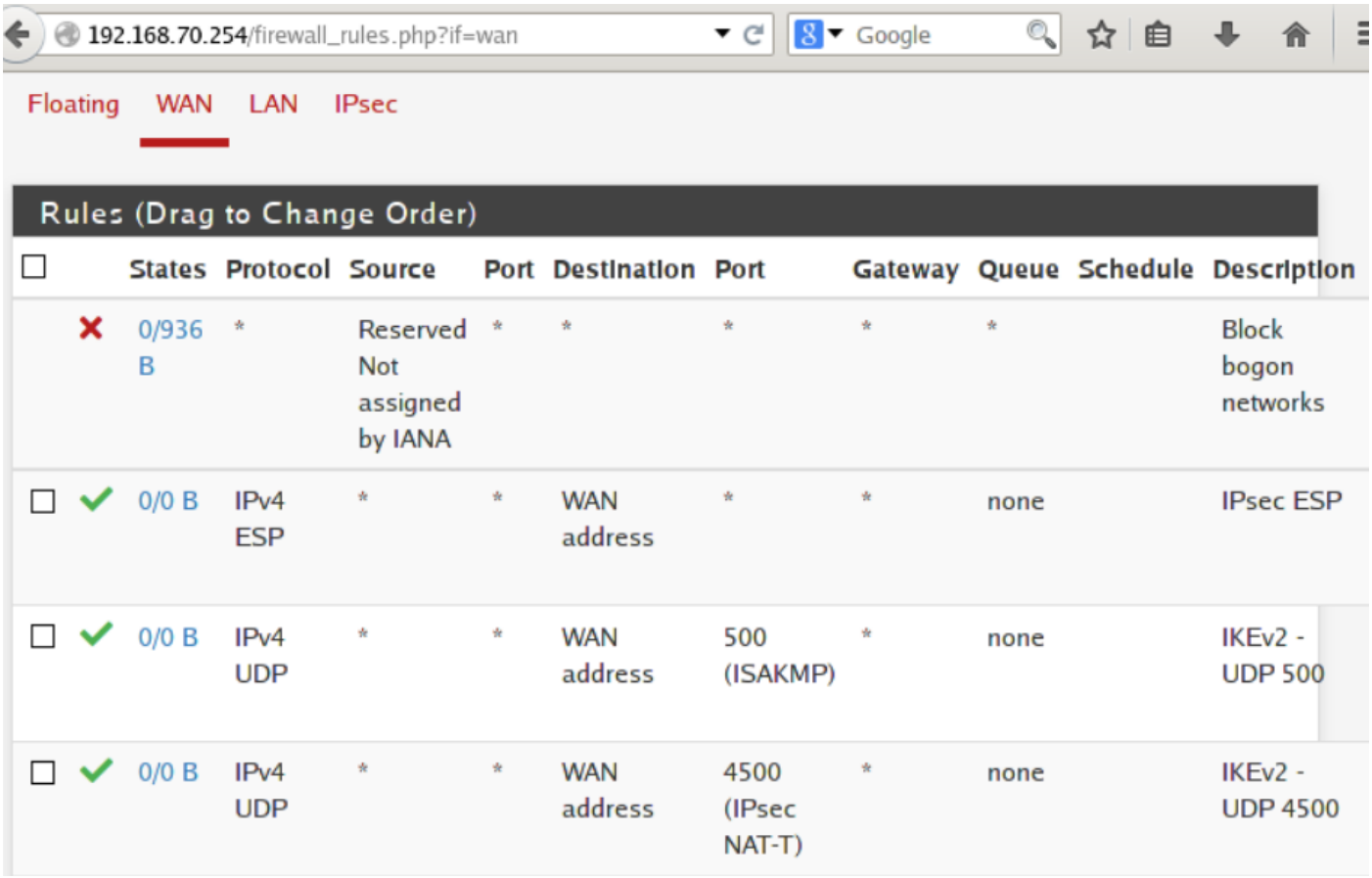
- UDP 500 (IKEv2 - Phase 1) Autorisation du protocole IKE
- UDP 4500 (IKEv2 - NAT-T) Autorisation du NAT Traversal
- ESP (Encapsulating Security Payload) Autorisation du protocole ESP

Ces règles sont indispensables pour permettre l'établissement et le bon fonctionnement du tunnel VPN.

Dans l'image suivante :

Les ports UDP 500 et 4500 sont ouverts pour IPsec (IKEv2)
Le protocole ESP est autorisé
Le blocage des réseaux bogon est activé ce qui est une bonne pratique de sécurité
Pour les règles VPN (UDP 500, 4500, ESP) c'est possible de restreindre la source aux IP publiques des sites distants pour renforcer la sécurité.
Les mêmes réglages sont faits sur le site distant. Le Bogon Network peut donner de soucis pour le réglages et fonctionnement du VPN sur GNS3 faut temporairement modifier en autorisant le plage d'adresse ou déshabiliter.

Image 7 : Règles autorisant le trafic VPN sur l'interface WAN



Autorisation du trafic interne (règles sur l'interface IPsec)

Une fois le tunnel VPN établi, il est nécessaire d'autoriser les communications entre les réseaux distants. Cette règle permet aux machines situées sur des sites distants de communiquer avec le réseau local de manière sécurisée. Le réglage en ce cas autorisant le réseau du site B au Site A sont faites sur le réseau A

Image 8 : Règle de filtrage sur l'interface IPsec du Site A

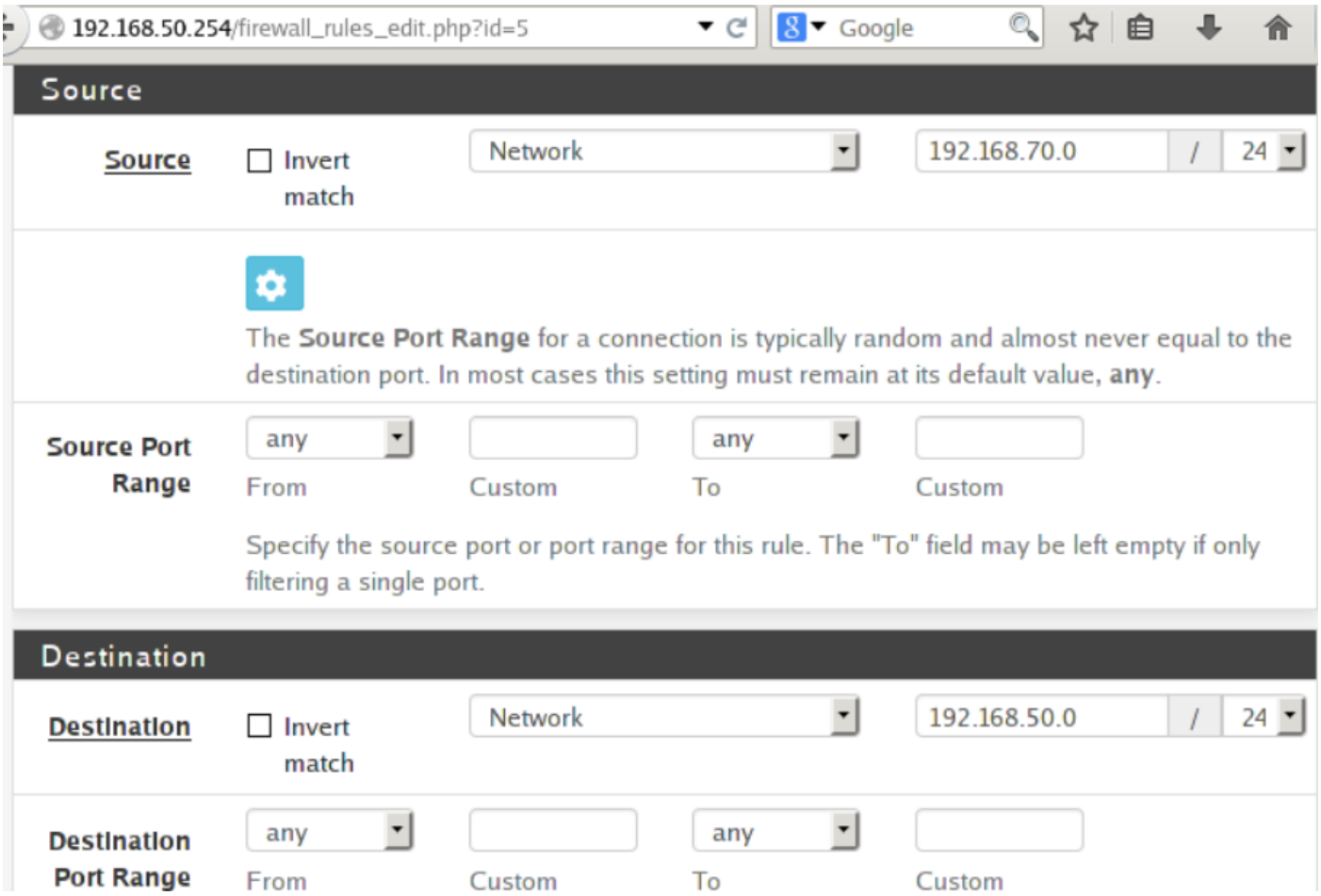
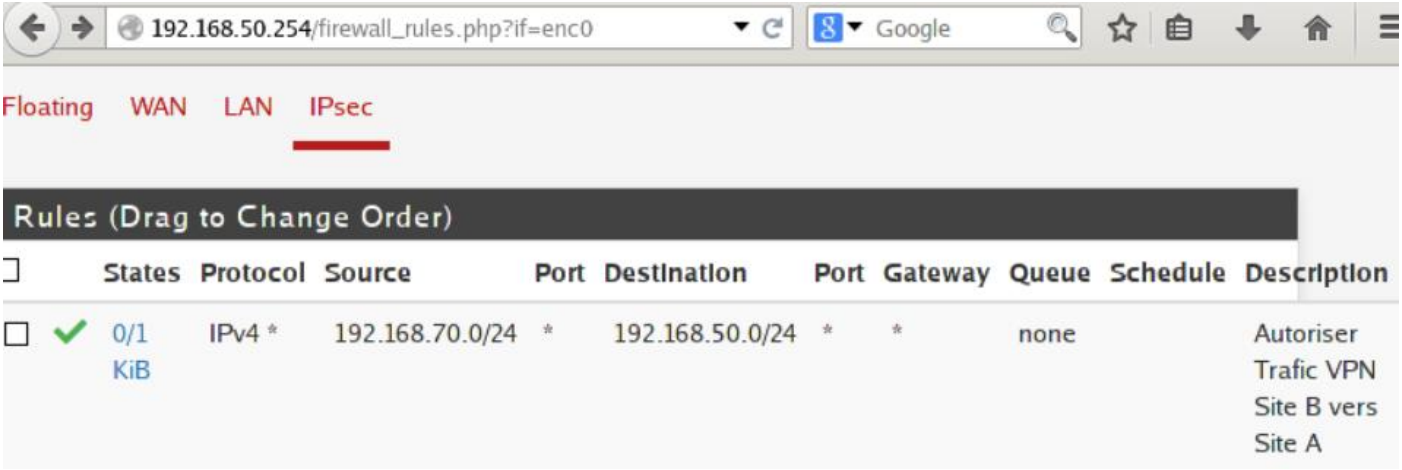


Image 9 : Règles présent sur l'onglet IPsec de règles pare-feu du Site A



Tests et validation du tunnel VPN

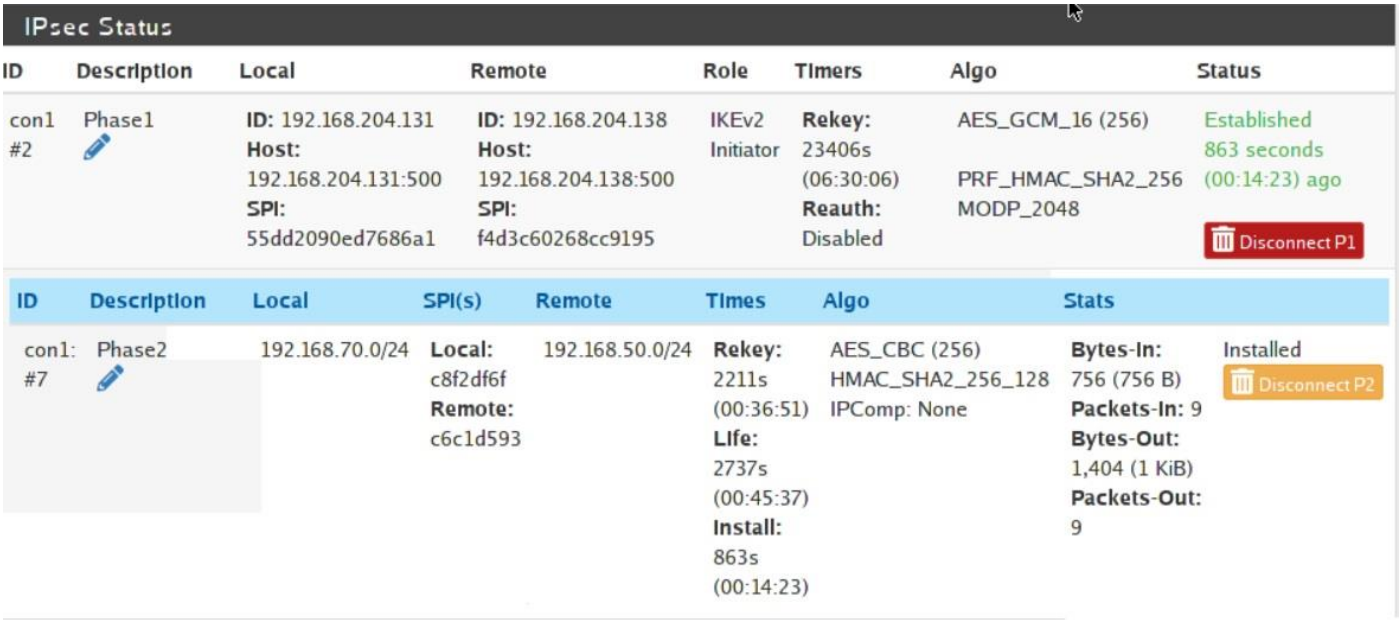
Maintenant on vérifie le bon fonctionnement du tunnel VPN IPsec configuré précédemment. Il s'agit de valider :

- l'établissement du tunnel, la communication entre les réseaux distants, la sécurité des échanges

Vérification de l'état du tunnel VPN

La première étape consiste à vérifier que le tunnel IPsec est bien établi.

Image 10 : État du tunnel IPsec (Phase 1 et Phase 2 actives)



Test de connectivité entre les réseaux

Une fois le tunnel établi, il est nécessaire de tester la communication entre les deux réseaux. Le méthode est celui d'effectuer un ping vers une machine du réseau distant. Ce test confirme que le trafic passe bien par le tunnel VPN.

Image 11 : Test de ping réussi entre les réseaux de Site B vers A

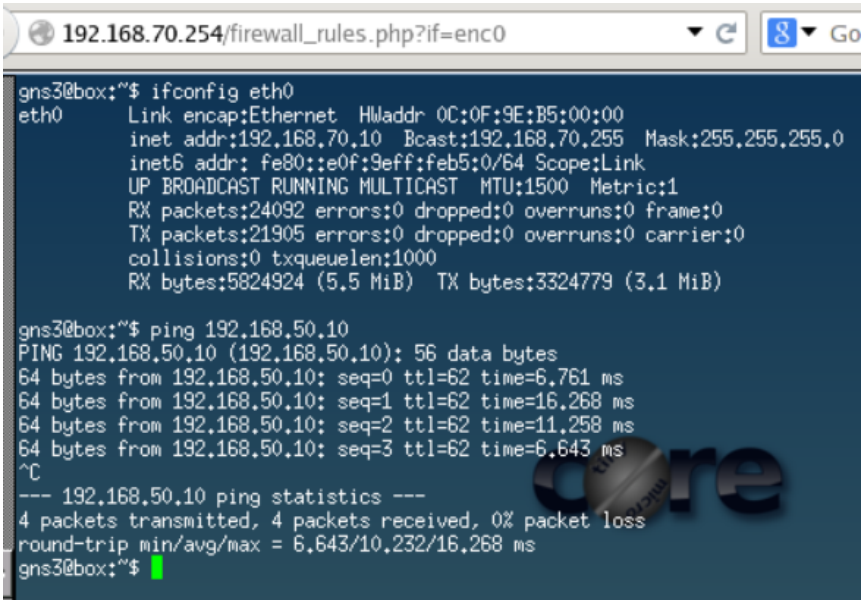
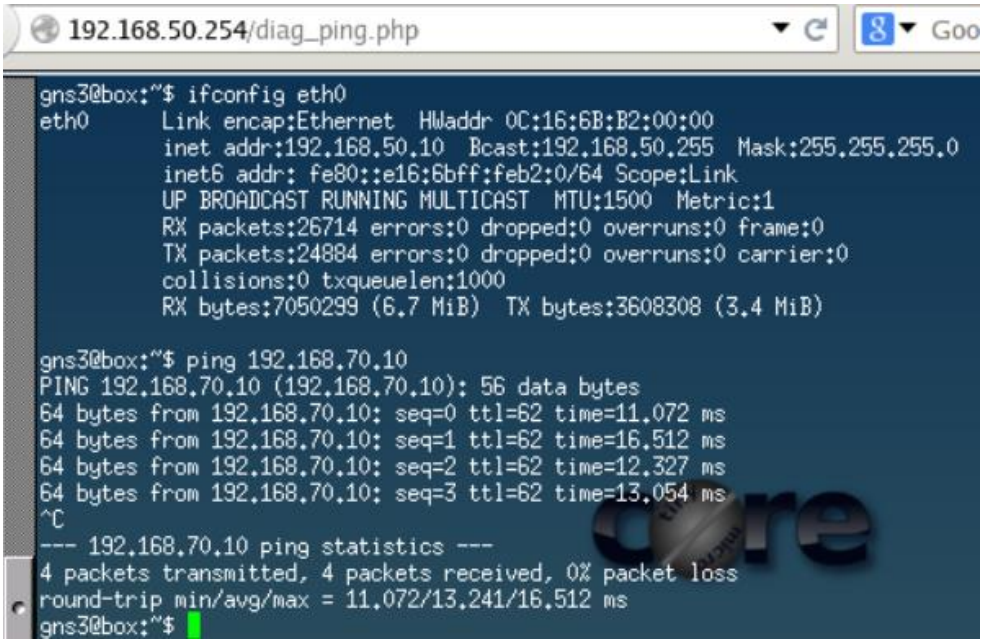


Image 12 : Test de ping réussi entre les réseaux de Site A vers B



Test de stabilité du tunnel

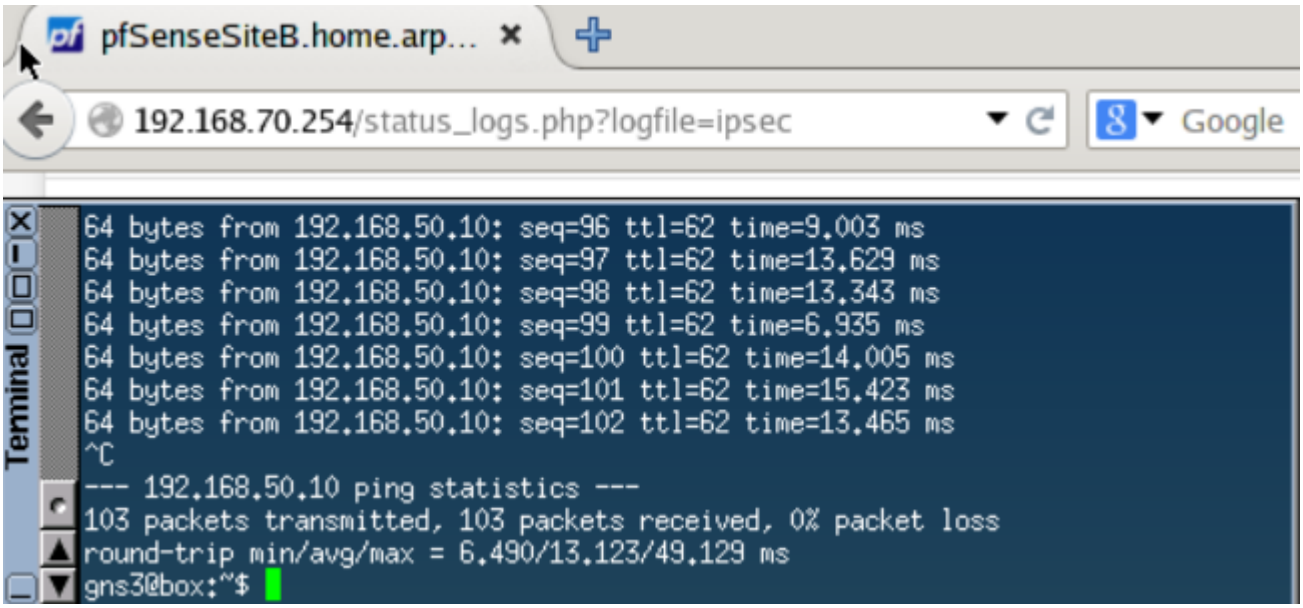
Un test de continuité permet de vérifier la stabilité du VPN.

Le méthode est de lancer un ping en continu : ping 192.168.50.10 -t 10

Résultat attendu :

- aucune perte de paquets, temps de réponse stable

Image 13 : Ping continu sans perte de paquets



Conclusion, contraintes et solutions

Les tests réalisés ont permis de valider le bon fonctionnement du tunnel VPN IPsec. Le tunnel est correctement établi, les communications entre les réseaux distants sont opérationnelles, et les règles de filtrage assurent un niveau de sécurité satisfaisant.

Lors de la mise en place du tunnel VPN IPsec sous pfSense, plusieurs contraintes techniques ont été rencontrées, nécessitant des ajustements spécifiques au niveau du pare-feu et de la configuration réseau.

Lors de la configuration de la Phase 2, la gestion du NAT (Network Address Translation) a constitué un point critique. Par défaut, pfSense applique une translation d'adresses sur les flux sortants, ce qui empêche le bon fonctionnement du VPN. En effet, le protocole IPsec repose sur les adresses IP réelles des réseaux locaux. Il a donc été nécessaire d'utiliser les réseaux LAN, et non les adresses WAN, dans la configuration. Afin de résoudre ce problème, une règle d'exclusion NAT (NO NAT) a été mise en place afin d'autoriser la communication directe entre les sous-réseaux 192.168.50.0/24 et 192.168.70.0/24 sans modification des adresses IP.

Ensuite, le mécanisme de blocage des réseaux dits « bogon » a également posé problème dans le cadre de cette simulation sous GNS3. Ces règles, destinées à bloquer des plages d'adresses non routables sur Internet, ont empêché la communication entre les interfaces WAN configurées en adresses privées (192.168.204.0/24). Il a donc été nécessaire de désactiver ce filtrage afin de permettre l'établissement du tunnel VPN dans un environnement de laboratoire.

Par ailleurs, la configuration des règles de filtrage sur l'interface WAN a nécessité une adaptation afin d'autoriser les flux nécessaires au fonctionnement du VPN, notamment les protocoles utilisés par IPsec.

Ces ajustements ont permis d'aboutir à une infrastructure fonctionnelle, sécurisée et conforme aux objectifs du projet.