PROCÉDURE DE RECONFIGURATION

Tunnel VPN IPsec Site-à-Site

Suite réinstallation pfSense-02 (Site B) — Infrastructure SISR 2026

Auteur	CHADHOULI EL-Anrif
Filière	BTS SIO — option SISR (2ème année)
Établissement	MEWO Metz
Date	Mars 2026
Contexte	Réinstallation pfSense-02 (pertes de paquets) — tunnel IPsec à reconfigurer
Protocole	IKEv2 — IPsec (ESP) — AES-256 — SHA-256 — DH Groupe 14
Site A	PfSense-01 — 10.10.101.3 (WAN) — LAN 10.11.3.16/28
Site B	PfSense-02 — 10.10.101.X (WAN) — LAN 10.11.4.16/28

1. Contexte et Rappel de l'Infrastructure

1.1 Pourquoi cette procédure ?

pfSense-02 (Site B) a été réinstallé à la suite de pertes de paquets importantes qui empêchaient l'installation et le bon fonctionnement des agents (GLPI, Zabbix) ainsi que de Squid. La réinstallation remet pfSense-02 à l'état usine : le tunnel IPsec Site-à-Site qui reliait les deux sites doit donc être entièrement reconfiguré des deux côtés.

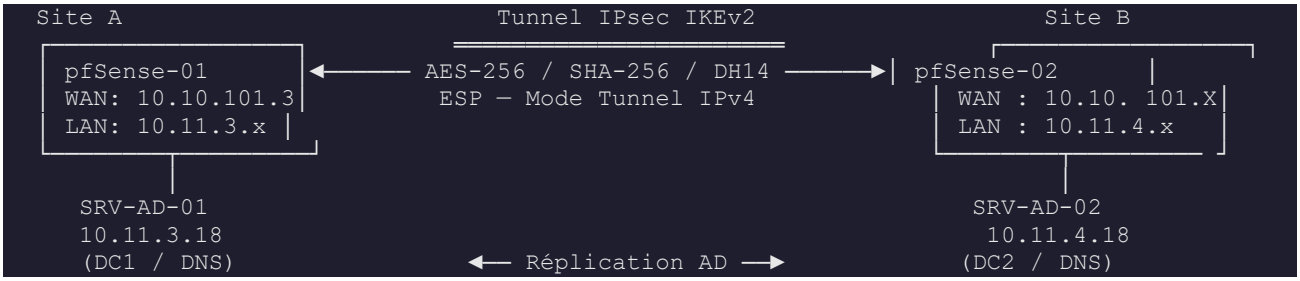
IMPORTANT : Le tunnel IPsec est critique pour l'infrastructure : sans lui, SRV-AD-02 (Site B) ne peut plus répliquer l'Active Directory depuis SRV-AD-01 (Site A), et la sauvegarde inter-sites nocturne est interrompue.

1.2 Architecture réseau

Élément	Adresse IP	Rôle
PfSense-01 (Site A)	WAN : 10.10.101.3	Passerelle Site A — côté initiateur du tunnel

PfSense-02 (Site B)	WAN : 10.10.101.X	Passerelle Site B — vient d'être réinstallée
LAN Site A	10.11.3.16/28	Réseau local Site A (SRV-AD-01, SRV-WEB-01...)
LAN Site B	10.11.4.16/28	Réseau local Site B (SRV-AD-02, CL-WIN11-02)
SRV-AD-01	10.11.3.18	DC1 — source de réplication AD
SRV-AD-02	10.11.4.18	DC2 — destination de réplication AD (Site B)

1.3 Schéma du tunnel



2. Paramètres IPsec de Référence

Ces paramètres sont ceux utilisés dans la configuration d'origine. Ils doivent être identiques sur les deux pfSense pour que le tunnel s'établisse.

2.1 Phase 1 — Canal de contrôle (IKEv2)

Paramètre	Valeur (Site A — pfSense-01)	Valeur (Site B — pfSense-02)
Version IKE	IKEv2	IKEv2
Authentification	Mutual PSK	Mutual PSK
Algorithme chiffrement	AES 256 bits	AES 256 bits
Algorithme hachage	SHA256	SHA256
Groupe Diffie-Hellman	14 (2048 bits)	14 (2048 bits)
Remote Gateway	10.10.101.X (IP WAN pfSense-02)	10.10.101.3 (IP WAN pfSense-01)
Pre-Shared Key	[clé à définir — identique des 2 côtés]	[même clé que Site A]
Lifetime	28800 secondes	28800 secondes

2.2 Phase 2 — Tunnel de données (ESP)

Paramètre	Valeur
Protocole	ESP

Mode	Tunnel IPv4
Réseau local Site A	10.11.3.16/28
Réseau local Site B	10.11.4.16/28
Algorithme chiffrement	AES 256 bits
Algorithme hachage	SHA256
Groupe PFS	14 (2048 bits)
Keep Alive	Ping vers 10.11.3.18 (SRV-AD-01)
Lifetime	3600 secondes

⚠ **ATTENTION :** La Pre-Shared Key (PSK) doit être rigoureusement identique sur les deux pfSense. Une seule différence de caractère empêche le tunnel de s'établir. Notez-la dans un endroit sécurisé avant de commencer.

3. Configuration IPsec sur pfSense-02 (Site B — NOUVEAU)

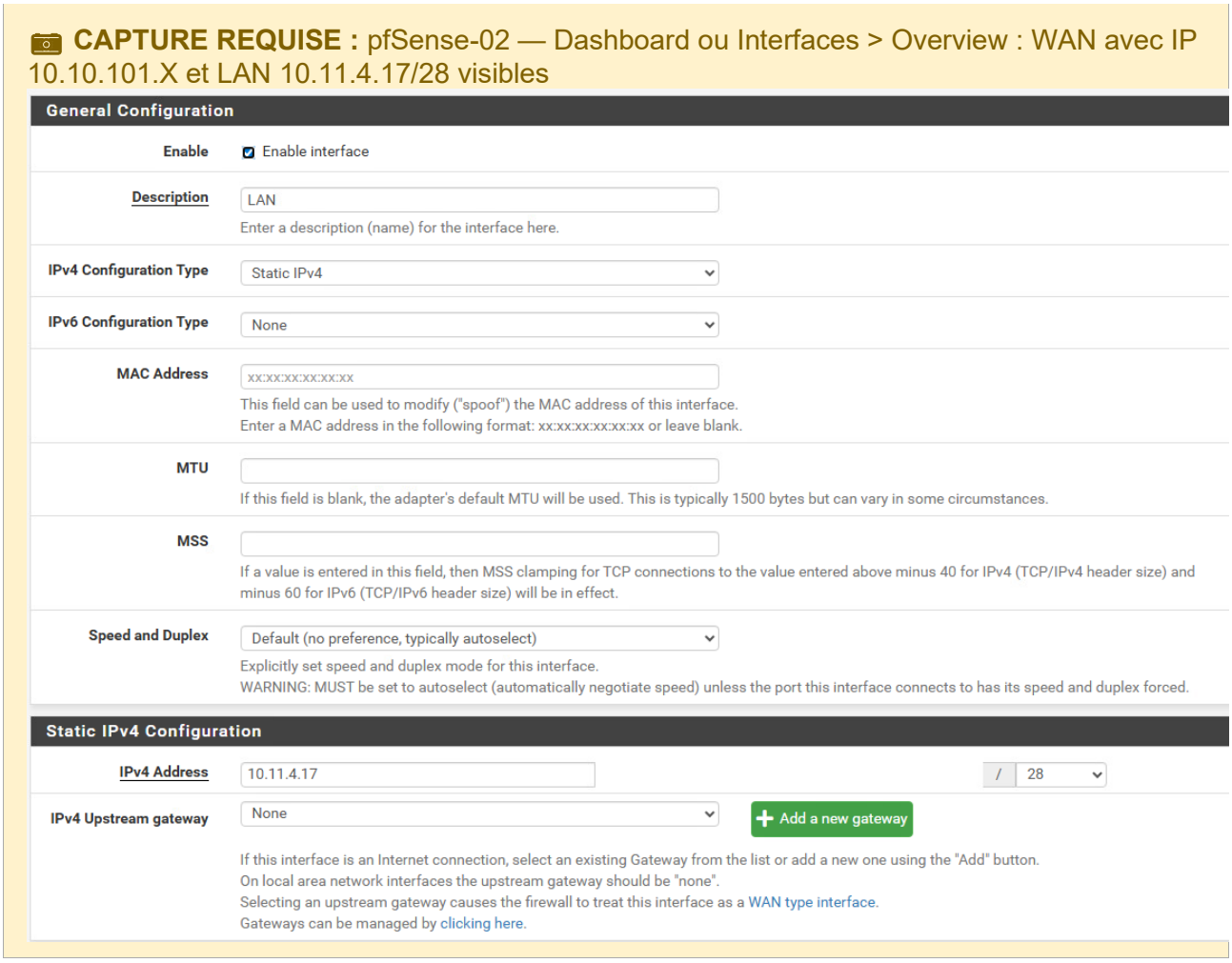
PfSense-02 vient d'être réinstallé. On commence par configurer le tunnel sur le côté Site B, puis on vérifiera/adaptera le Site A.

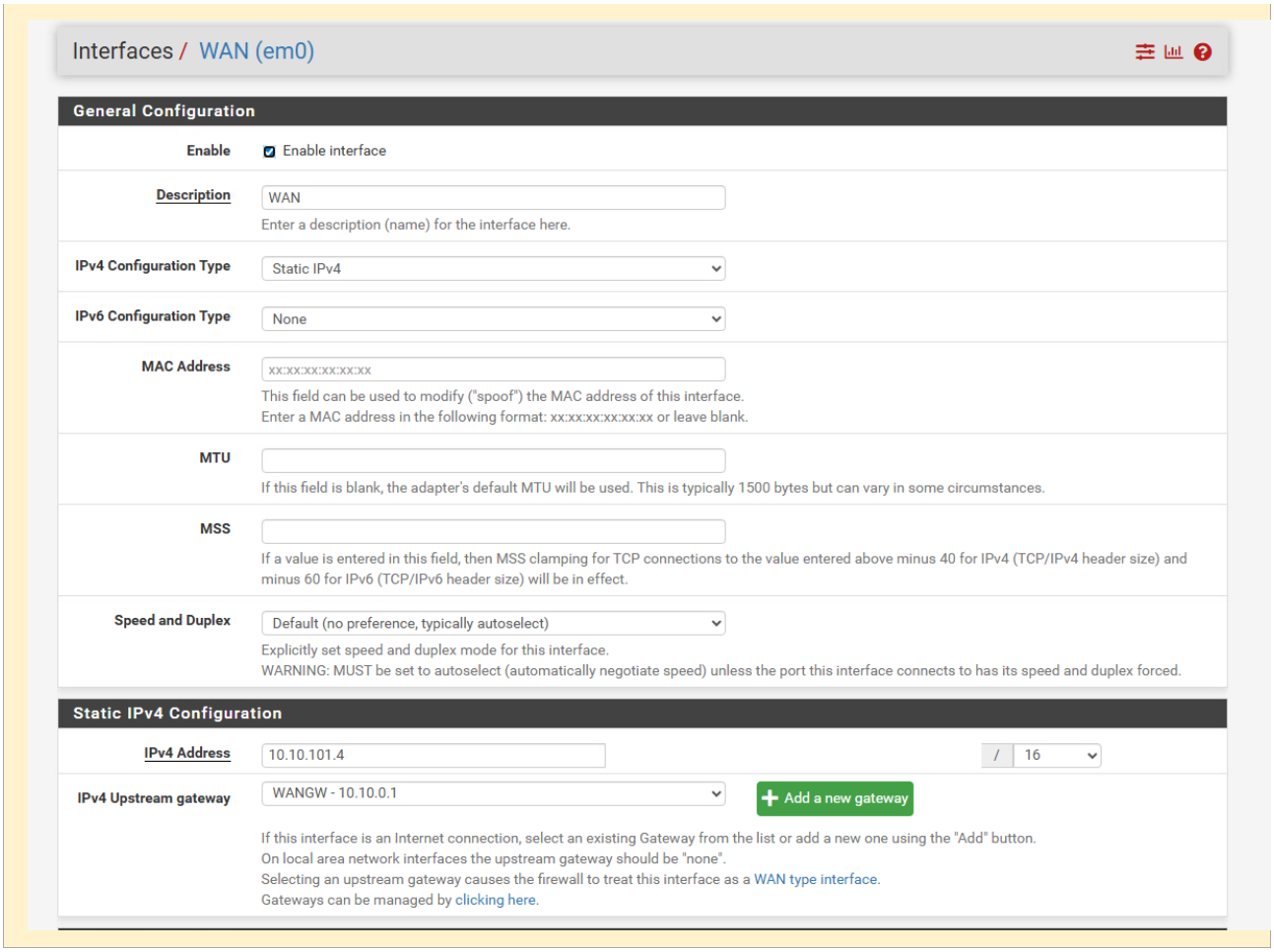
3.1 Vérification préalable des interfaces

Avant de configurer IPsec, s'assurer que les interfaces LAN et WAN de pfSense-02 sont bien configurées :

1. Se connecter à l'interface web de pfSense-02 (depuis un poste du Site B ou via vSphere)
2. Aller dans Interfaces → Overview
3. Vérifier que l'interface WAN affiche bien une IP dans la plage 10.10.101.x
4. Vérifier que l'interface LAN est sur 10.11.4.17/28

CAPTURE REQUISE : pfSense-02 — Dashboard ou Interfaces > Overview : WAN avec IP 10.10.101.X et LAN 10.11.4.17/28 visibles





3.2 Création de la Phase 1 sur pfSense-02

5. Naviguer vers VPN → IPsec
6. Cliquer Add P1 (ajouter une Phase 1)
7. Renseigner les paramètres suivants :

Onglet General Information

Champ	Valeur à saisir
Key Exchange version	IKEv2
Internet Protocol	IPv4
Interface	WAN
Remote Gateway	10.10.101.3 (IP WAN de pfSense-01 Site A)
Description	IPsec Site B vers Site A

Onglet Phase 1 Proposal (Authentication)

Champ	Valeur à saisir
Authentication Method	Mutual PSK
My identifier	My IP address

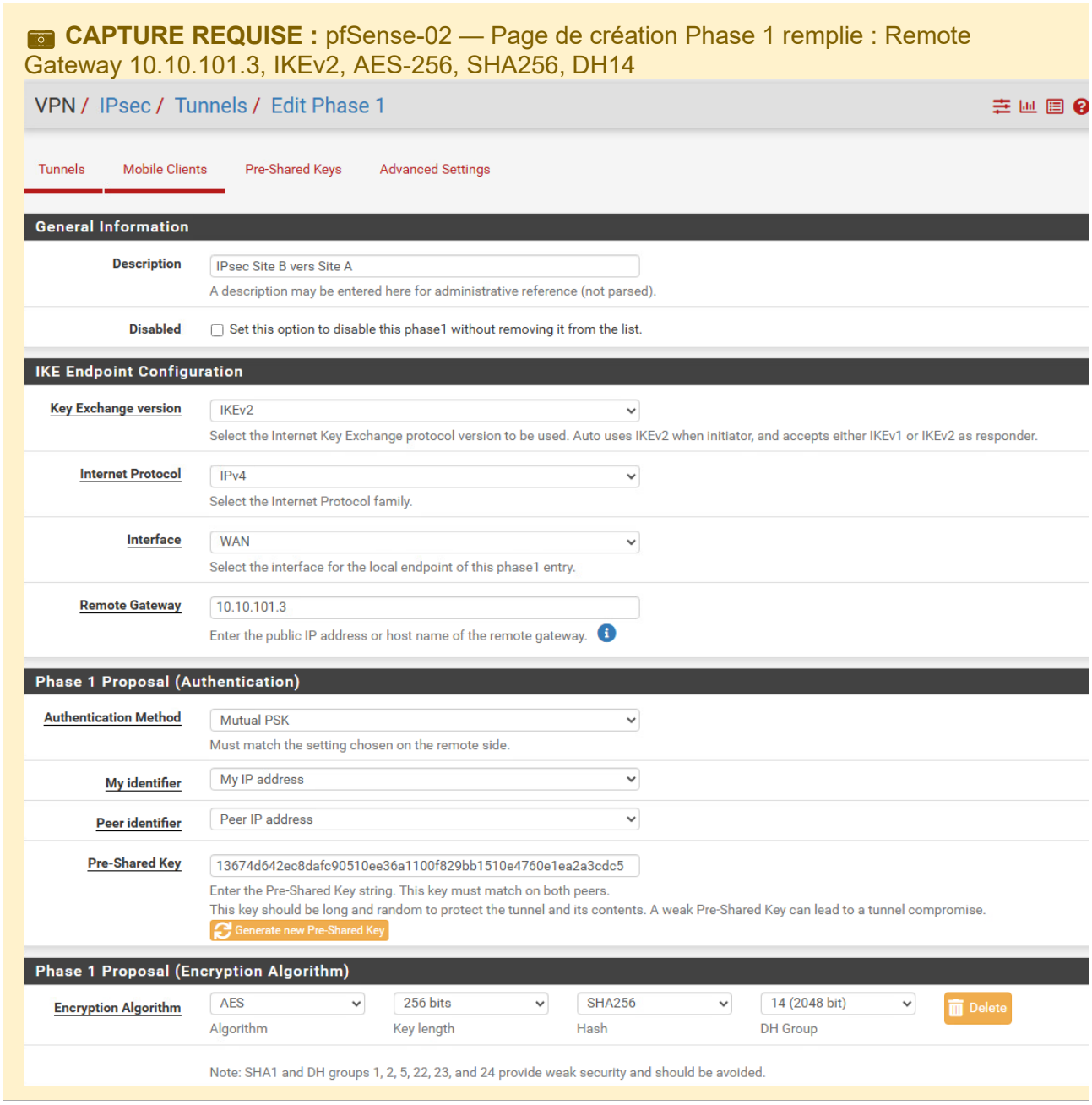
Peer identifier	Peer IP address
Pre-Shared Key	13674d642ec8dafc90510ee36a1100f829bb1510e4760e1ea2a3cdc5

Onglet Phase 1 Proposal (Encryption)

Champ	Valeur à saisir
Encryption Algorithm	AES — 256 bits
Hash Algorithm	SHA256
DH Group	14 (2048 bit)
Lifetime	28800

8. Cliquer Save

CAPTURE REQUISE : pfSense-02 — Page de création Phase 1 remplie : Remote Gateway 10.10.101.3, IKEv2, AES-256, SHA256, DH14



3.3 Création de la Phase 2 sur pfSense-02

9. Depuis la liste IPsec, cliquer sur Show Phase 2 Entries sous la Phase 1 créée
10. Cliquer Add P2
11. Renseigner les paramètres suivants :

Onglet General Information

Champ	Valeur à saisir
Mode	Tunnel IPv4
Local Network	Network — 10.11.4.16/28 (LAN Site B)
Remote Network	Network — 10.11.3.16/28 (LAN Site A)
Description	LAN Site B vers LAN Site A

Onglet Phase 2 Proposal (SA/Key Exchange)

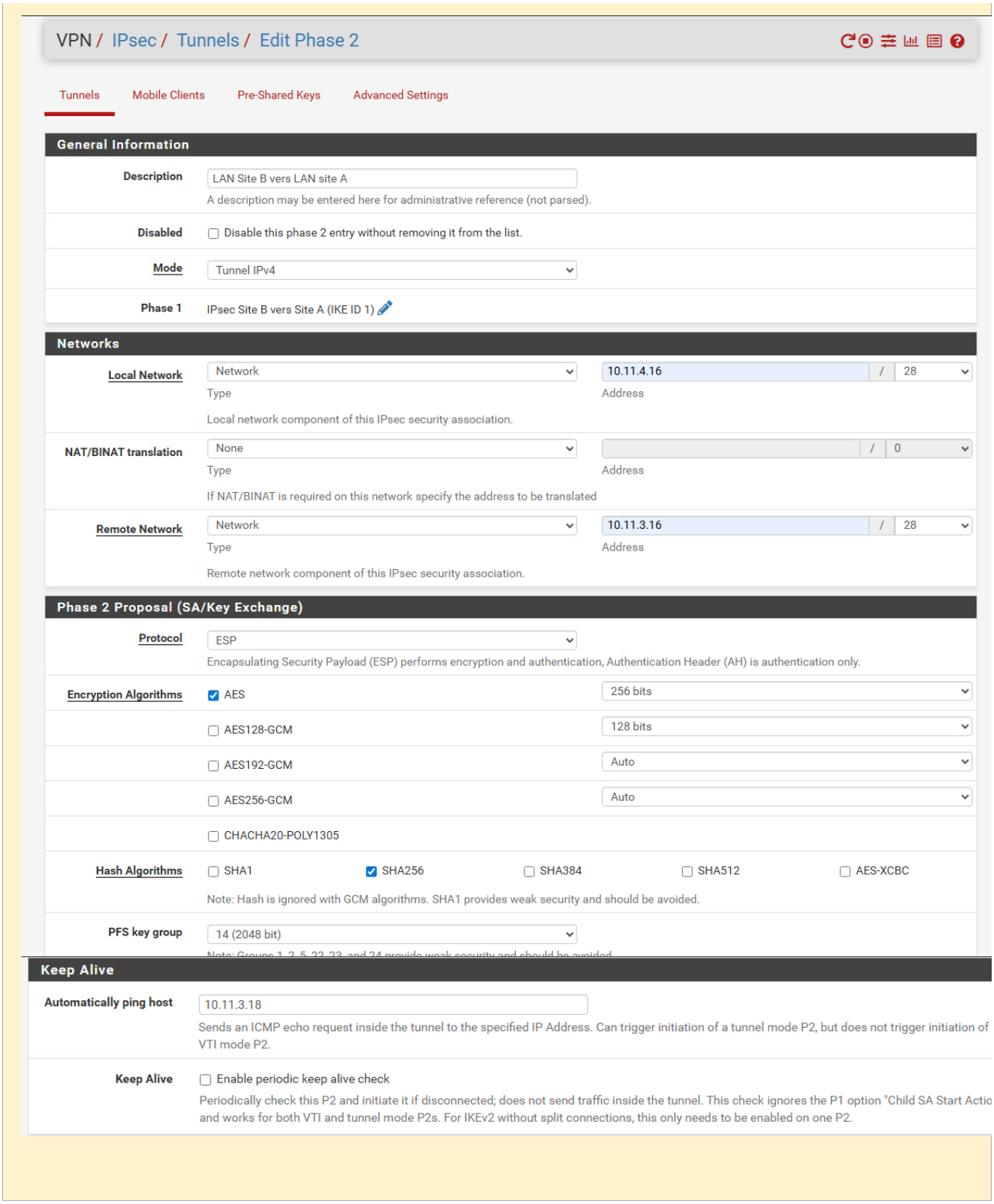
Champ	Valeur à saisir
Protocol	ESP
Encryption Algorithm	AES — 256 bits
Hash Algorithm	SHA256
PFS Key Group	14 (2048 bit)
Lifetime	3600

Onglet Advanced Configuration (Keep Alive)

Champ	Valeur à saisir
Automatically ping host	10.11.3.18 (SRV-AD-01 — pour maintenir le tunnel actif)

12. Cliquer Save

CAPTURE REQUISE : pfSense-02 — Page Phase 2 remplie : Local 10.11.4.16/28, Remote 10.11.3.16/28, ESP, AES-256, SHA256, DH14, Keep Alive 10.11.3.18



3.4 Règle pare-feu IPsec sur pfSense-02

pfSense ne crée pas automatiquement les règles pour autoriser le trafic dans le tunnel. Il faut les créer manuellement.

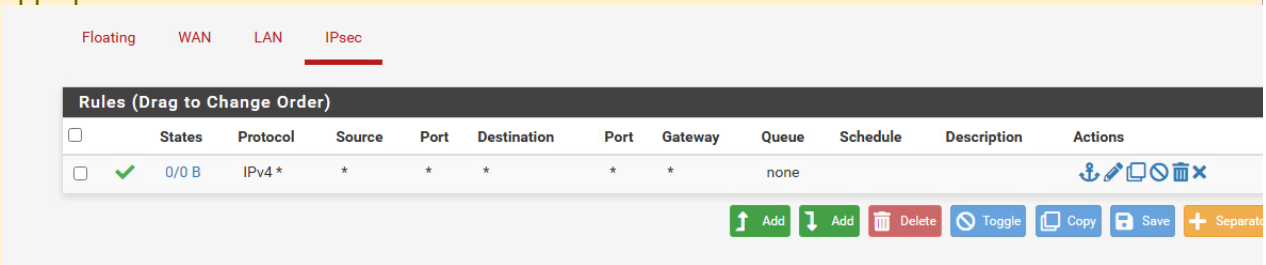
13. Aller dans Firewall → Rules → onglet IPsec
14. Cliquer Add
15. Renseigner :

- Action : Pass
- Interface : IPsec
- Protocol : any
- Source : any
- Destination : any
- Description : Autoriser tout trafic IPsec inter-sites

16. Cliquer Save puis Apply Changes

> **INFO :** Cette règle 'Pass any' sur l'interface IPsec est suffisante en environnement de lab/examen. En production, on restreindrait aux seuls flux nécessaires (réplication AD, sauvegardes).

> **CAPTURE REQUISE :** pfSense-02 — Règle Firewall > IPsec : Pass any créée et appliquée



4. Vérification/Mise à jour sur pfSense-01 (Site A)

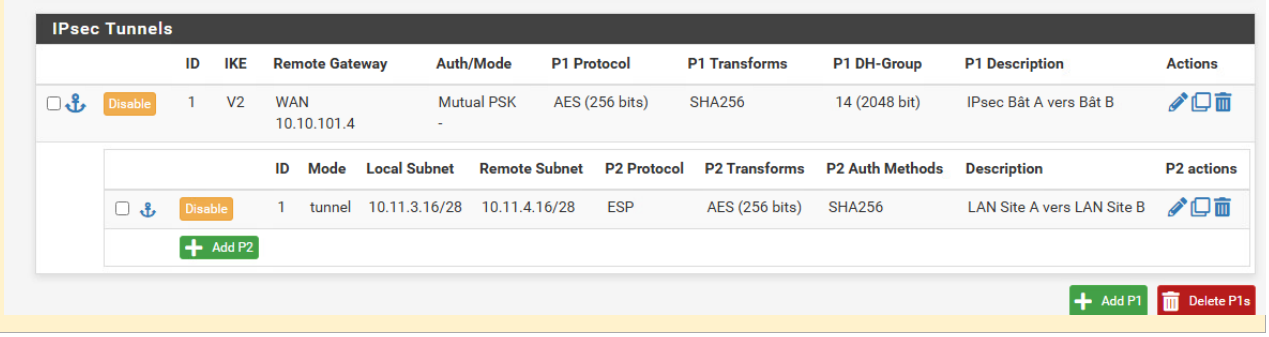
PfSense-01 (Site A) avait déjà le tunnel configuré. Il faut vérifier que les paramètres correspondent bien à la nouvelle configuration de pfSense-02, et s'assurer que l'IP WAN de pfSense-02 n'a pas changé après la réinstallation.

4.1 Vérifier la Phase 1 côté Site A

17. Se connecter à l'interface web de pfSense-01 : https://10.11.3.17
18. Aller dans VPN → IPsec
19. Vérifier les paramètres de la Phase 1 existante :
    - Remote Gateway = IP WAN de pfSense-02 (adapter si elle a changé après réinstallation)
    - Key Exchange = IKEv2
    - Encryption = AES 256 bits
    - Hash = SHA256
    - DH Group = 14
    - Pre-Shared Key = identique à celle saisie sur pfSense-02

> **ATTENTION :** Si l'IP WAN de pfSense-02 a changé après la réinstallation, mettre à jour le champ 'Remote Gateway' sur pfSense-01 avec la nouvelle IP. C'est souvent la cause n°1 d'échec lors d'une réinstallation.

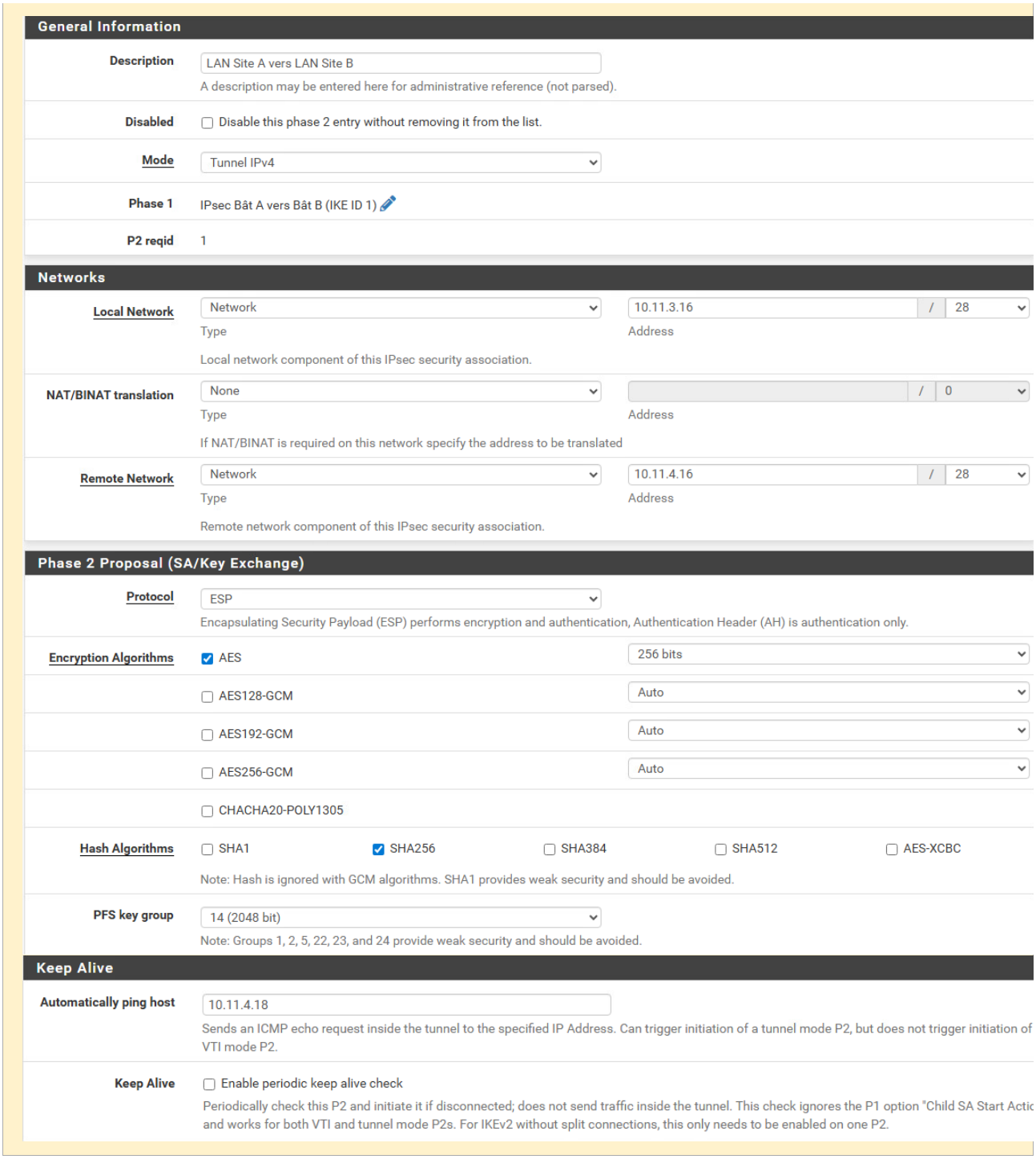
CAPTURE REQUISE : pfSense-01 — VPN > IPsec : Phase 1 existante avec Remote Gateway pointant vers la nouvelle IP WAN de pfSense-02



4.2 Vérifier la Phase 2 côté Site A

20. Cliquer Show Phase 2 Entries sur la Phase 1
21. Vérifier :
    - Local Network = 10.11.3.16/28 (LAN Site A)
    - Remote Network = 10.11.4.16/28 (LAN Site B)
    - Protocol = ESP, AES-256, SHA256, DH14
    - Keep Alive = 10.11.4.18 (SRV-AD-02)

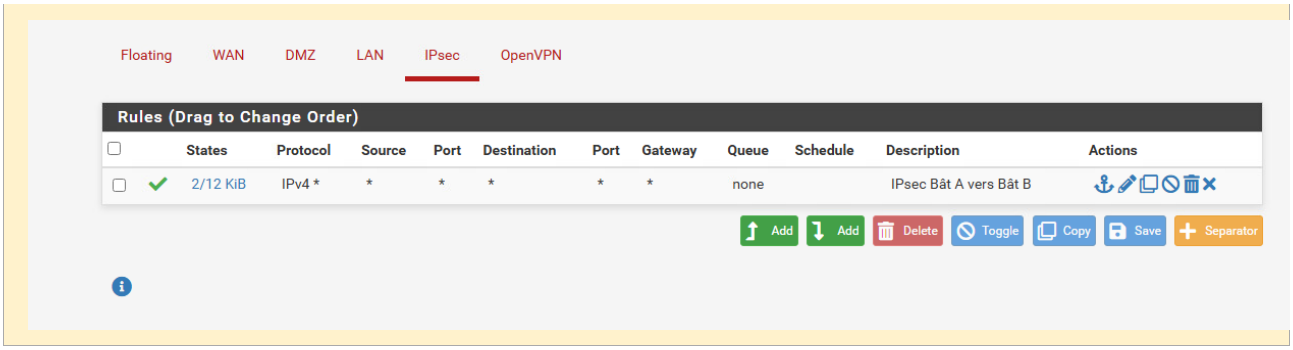
CAPTURE REQUISE : pfSense-01 — Phase 2 : Local 10.11.3.16/28, Remote 10.11.4.16/28, paramètres chiffrement visibles



4.3 Vérifier la règle pare-feu IPsec côté Site A

22. Firewall → Rules → onglet IPsec
23. Vérifier qu'une règle Pass any existe (ou la recréer si elle a disparu)

CAPTURE REQUISE : pfSense-01 — Firewall > Rules > IPsec : règle Pass any présente



5. Établissement et Vérification du Tunnel

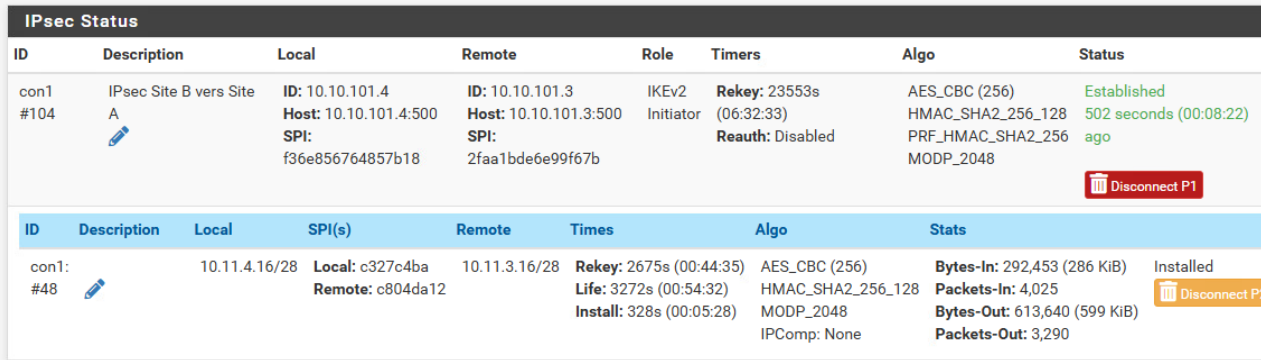
5.1 Initier le tunnel depuis pfSense-02 (Site B)

Le tunnel IPsec doit être initié manuellement la première fois après configuration :

24. Sur pfSense-02 : aller dans Status → IPsec
25. Localiser le tunnel dans la liste
26. Cliquer sur le bouton Connect (▶) pour initier la Phase 1
27. Attendre quelques secondes et observer le statut

☑ **RÉSULTAT ATTENDU :** Phase 1 : statut 'Established' en vert. Phase 2 : statut 'Established' en vert. Les deux phases doivent être vertes pour que le tunnel soit opérationnel.

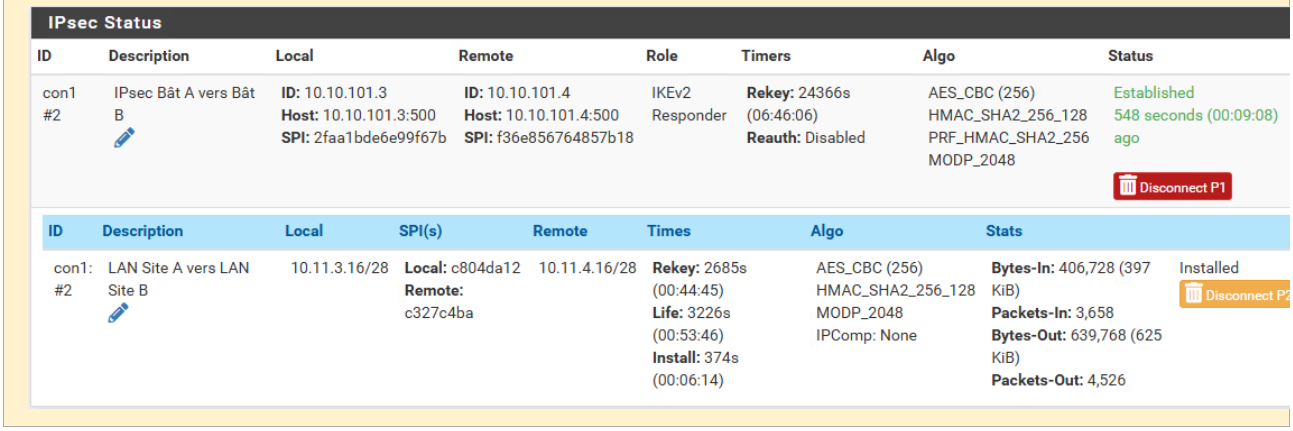
CAPTURE REQUISE : pfSense-02 — Status > IPsec : Phase 1 ET Phase 2 affichant le statut 'Established' en vert



5.2 Vérification côté pfSense-01 (Site A)

28. Sur pfSense-01 : aller dans Status → IPsec
29. Vérifier que le tunnel apparaît également comme 'Established'

CAPTURE REQUISE : pfSense-01 — Status > IPsec : tunnel affiché 'Established' des deux côtés



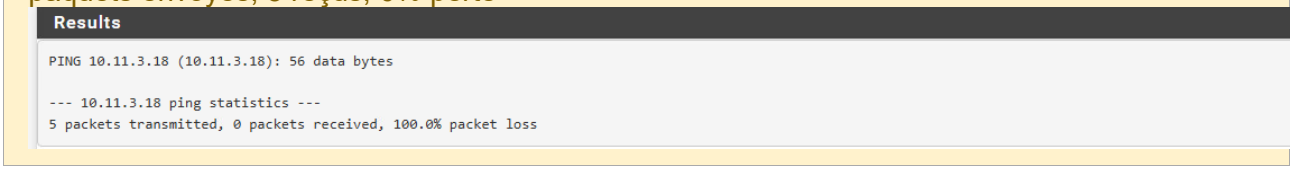
5.3 Test de connectivité — Ping inter-sites

Le test fondamental : vérifier que les deux réseaux LAN peuvent se joindre à travers le tunnel.

Depuis pfSense-02 (Site B) — Diagnostics → Ping

```
# Ping depuis pfSense-02 vers SRV-AD-01 (Site A)
# Diagnostics → Ping
# Host : 10.11.3.18
# Source IP : 10.11.4.17 (interface LAN de pfSense-02)
# Count : 5
```

CAPTURE REQUISE : pfSense-02 — Diagnostics > Ping vers 10.11.3.18 (SRV-AD-01) : 5 paquets envoyés, 5 reçus, 0% perte

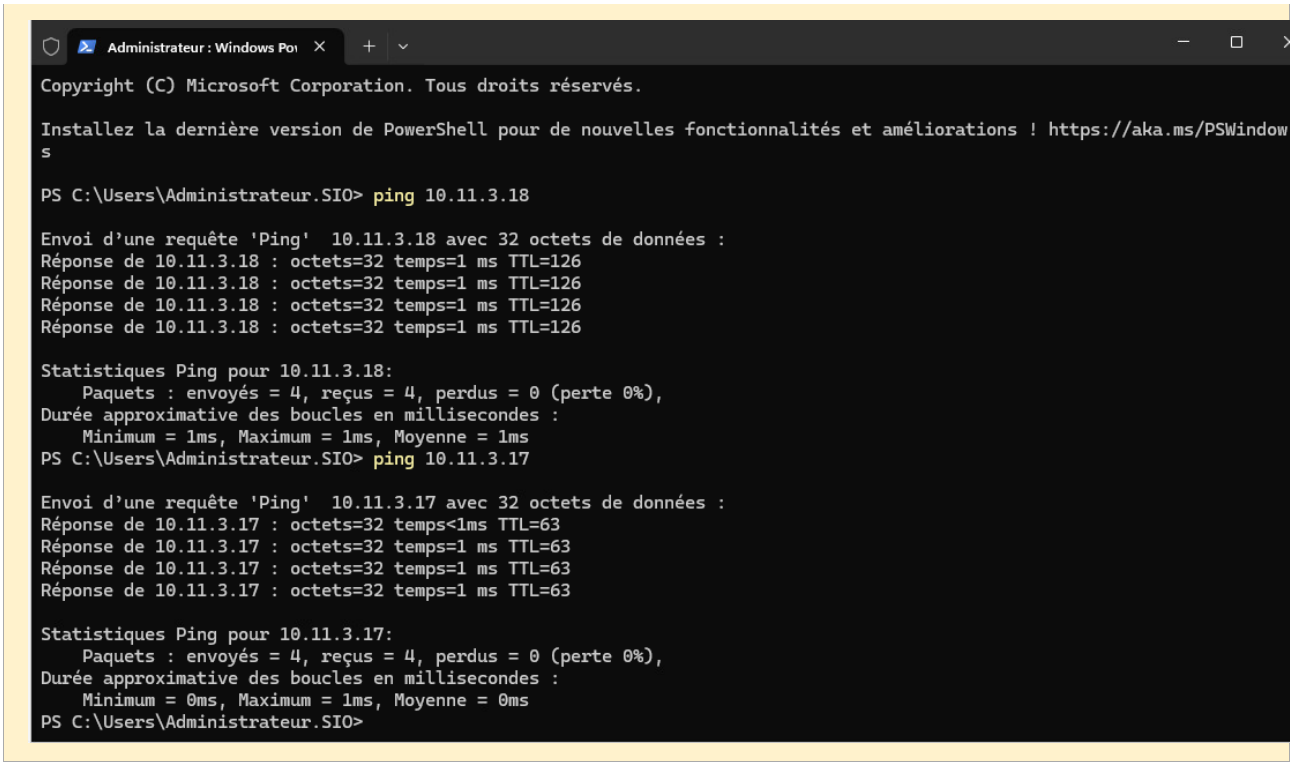


Note : Le ping depuis l'outil Diagnostics de pfSense affiche 100% de perte car pfSense source le ping depuis son interface WAN (10.10.101.4) et non depuis le LAN (10.11.4.17). Le trafic ICMP sortant par le WAN ne passe pas dans le tunnel IPsec qui est configuré pour les réseaux LAN (10.11.4.16/28 ↔ 10.11.3.16/28). La connectivité inter-sites est néanmoins confirmée par les pings réussis depuis SRV-AD-02 (10.11.4.18) vers SRV-AD-01 (10.11.3.18) visibles en section 5.3, ainsi que par le statut **Established** du tunnel et la réplication AD fonctionnelle.

Depuis SRV-AD-02 (Site B) — Test depuis la VM

```
# Sur SRV-AD-02 (10.11.4.18) — PowerShell ou cmd :
ping 10.11.3.18    # → SRV-AD-01 (DC1 Site A)
ping 10.11.3.17    # → pfSense-01 (passerelle Site A)
```

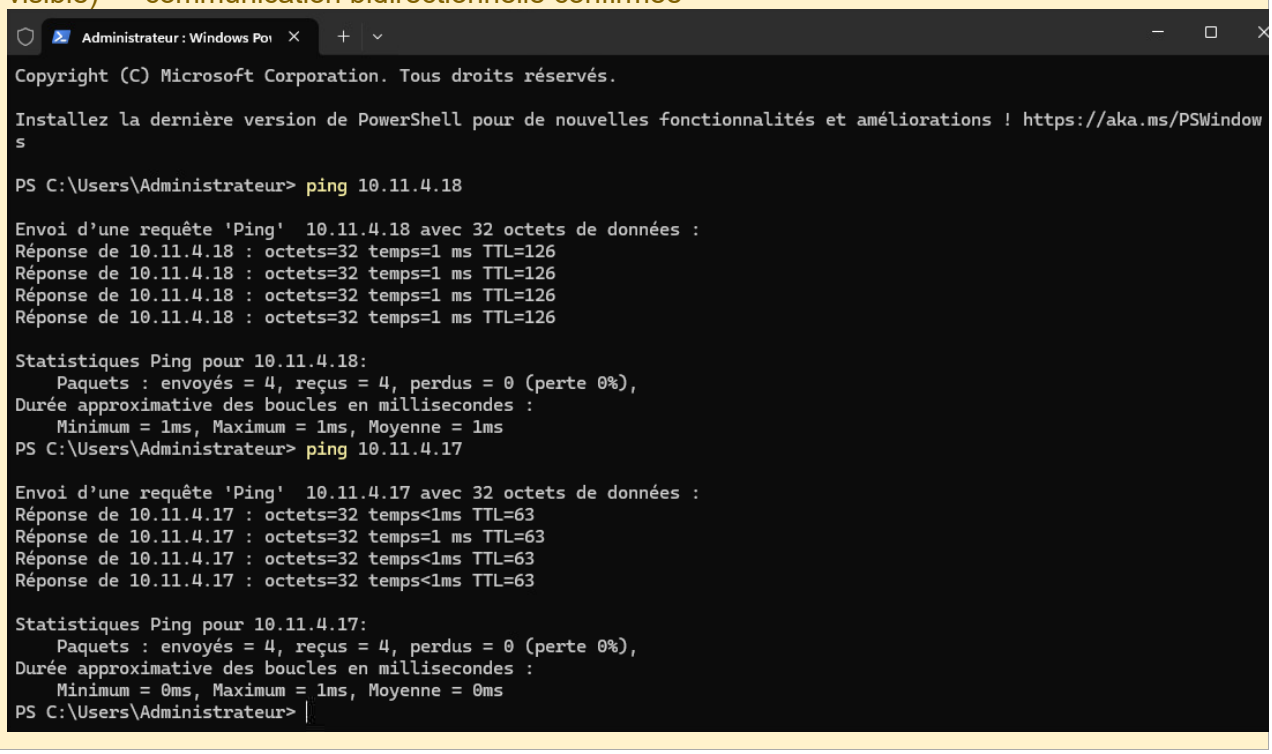
CAPTURE REQUISE : SRV-AD-02 — cmd/PowerShell : ping 10.11.3.18 réussi (Reply from 10.11.3.18 : TTL visible)



Depuis SRV-AD-01 (Site A) — Test retour

```
# Sur SRV-AD-01 (10.11.3.18) — PowerShell ou cmd :
ping 10.11.4.18     # → SRV-AD-02 (DC2 Site B)
ping 10.11.4.17     # → pfSense-02 (passerelle Site B)
```

CAPTURE REQUISE : SRV-AD-01 — ping 10.11.4.18 réussi (Reply from 10.11.4.18 : TTL visible) — communication bidirectionnelle confirmée



6. Validation de la Réplication Active Directory

La réplication AD est le service le plus critique qui transite par ce tunnel. Vérifier qu'elle fonctionne à nouveau correctement.

6.1 Forcer une réplication depuis SRV-AD-01

Sur SRV-AD-01 (10.11.3.18), ouvrir PowerShell en administrateur :

```
# Forcer la réplication vers SRV-AD-02
repadmin /syncall /AdeP

# Vérifier l'état de la réplication (doit être sans erreur)
repadmin /showrepl

# Alternative graphique : Sites et services Active Directory
# → NTDS Settings sur SRV-AD-02 → clic droit → Répliquer maintenant
```

☑ **RÉSULTAT ATTENDU :** repadmin /showrepl doit afficher 'Last attempt ... was successful' sans aucune ligne en rouge. Toute erreur indique un problème de connectivité réseau via le tunnel.

CAPTURE REQUISE : SRV-AD-01 — PowerShell : repadmin /showrepl sans erreur, statut 'successful' pour SRV-AD-02 (10.11.4.18)

```
PS C:\Users\Administrateur> repadmin /showrepl

Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Default-First-Site-Name\SRV-AD-01
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 76a2ed84-f0af-4985-a6c5-0a3716bfa372
ID de l'invocation DSA : 71ece5c0-33cc-4d38-89b3-91b4f54556f7

=== INSTANCES VOISINES ENTRANTES ==================================

DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-03-24 22:06:10, a réussi.

CN=Configuration,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-03-24 22:02:01, a réussi.

CN=Schema,CN=Configuration,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-03-24 21:56:20, a réussi.

DC=DomainDnsZones,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-03-24 22:07:06, a réussi.

DC=ForestDnsZones,DC=sio,DC=local
    Default-First-Site-Name\SRV-AD-02 via RPC
        GUID de l'objet DSA : 91cf05c1-7bcd-4593-9e90-da79a8f20e74
        La dernière tentative, le 2026-03-24 22:07:05, a réussi.
```

6.2 Vérification DNS inter-sites

Vérifier que la résolution DNS fonctionne entre les deux sites via le tunnel :

```
# Sur SRV-AD-02 (Site B) :
nslookup srv-ad-01.sio.local 10.11.3.18
# → doit retourner 10.11.3.18

# Sur SRV-AD-01 (Site A) :
nslookup srv-ad-02.sio.local 10.11.4.18
# → doit retourner 10.11.4.18
```

📷 **CAPTURE REQUISE :** SRV-AD-02 — nslookup srv-ad-01.sio.local : réponse 10.11.3.18 retournée correctement

```
PS C:\Users\Administrateur.SIO> nslookup srv-ad-01.sio.local 10.11.3.18
Serveur :   UnKnown
Address:  10.11.3.18

Nom :    srv-ad-01.sio.local
Address:  10.11.3.18

PS C:\Users\Administrateur.SIO>
```

7. Vérification de la Sauvegarde Inter-Sites

La sauvegarde nocturne automatique de SRV-AD-02 vers SRV-AD-01 transite par le tunnel IPsec. Vérifier que le partage réseau est à nouveau accessible.

7.1 Test d'accès au partage de sauvegarde

Depuis SRV-AD-02 (Site B), vérifier l'accès au partage de destination sur SRV-AD-01 :

```
# Sur SRV-AD-02 — PowerShell :
Test-Path '\\10.11.3.18\Backup'
# → doit retourner True

# Ou tester en montant le partage :
net use Z: \\10.11.3.18\Backup
```

📷 **CAPTURE REQUISE :** SRV-AD-02 — Test-Path ou net use : accès au partage \\10.11.3.18\Backup confirmé (True / commande réussie)

```
PS C:\Users\Administrateur.SIO> Test-Path '\\10.11.3.18\Backup'
True
PS C:\Users\Administrateur.SIO>
```

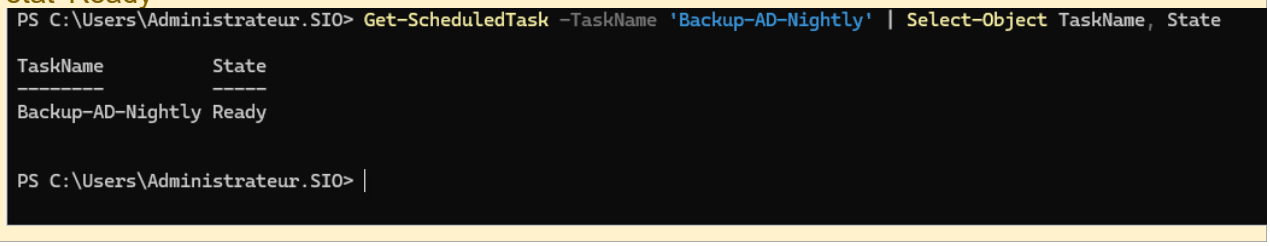
7.2 Vérification de la tâche planifiée

Vérifier que la tâche de sauvegarde automatique est toujours active sur SRV-AD-02 :

```
# Sur SRV-AD-02 — PowerShell :
```

```
Get-ScheduledTask -TaskName 'Backup-AD-Nightly' | Select-Object TaskName, State
# → State doit être 'Ready'
```

CAPTURE REQUISE : SRV-AD-02 — Get-ScheduledTask : tâche 'Backup-AD-Nightly' en état 'Ready'



8. Tableau de Validation Finale

Récapitulatif de tous les tests à valider après reconfiguration du tunnel :

Test de validation	Résultat attendu	Résultat obtenu	Statut
Interfaces pfSense-02 (WAN/LAN)	WAN 10.10.101.X + LAN 10.11.4.17	✅ OK	✅ OK
Phase 1 IPsec établie (pfSense-02)	Statut : Established	✅ OK	✅ OK
Phase 2 IPsec établie (pfSense-02)	Statut : Established	✅ OK	✅ OK
Phase 1 visible côté pfSense-01	Statut : Established	✅ OK	✅ OK
Ping pfSense-02 → SRV-AD-01	5/5 paquets reçus, 0% perte	✅ OK	✅ OK
Ping SRV-AD-02 → SRV-AD-01	Reply from 10.11.3.18	✅ OK	✅ OK
Ping SRV-AD-01 → SRV-AD-02	Reply from 10.11.4.18	✅ OK	✅ OK
Réplication AD (repadmin /showrepl)	Successful, aucune erreur	✅ OK	✅ OK
DNS inter-sites fonctionnel	nslookup résout les deux DCs	✅ OK	✅ OK
Accès partage \\10.11.3.18\Backup	Test-Path retourne True	✅ OK	✅ OK
Tâche Backup-AD-Nightly	État : Ready	✅ OK	✅ OK