BTS SIO — Option SISR — Procédure Technique

Preuve de chiffrement des flux de réplication Active Directory inter-sites

Analyse Wireshark — IPsec ESP / AES-256 — SRV-AD-01 ↔ SRV-AD-02

Objectif

Démontrer, capture Wireshark à l'appui, que les flux de réplication Active Directory entre `SRV-AD-01 (10.11.3.18)` (Site A) et `SRV-AD-02 (10.11.4.18)` (Site B) sont **totalement chiffrés et illisibles** pour tout tiers qui intercepterait le trafic sur le réseau public. La preuve repose sur l'observation de paquets `ESP (Encapsulating Security Payload)` dont le contenu est mathématiquement opaque sans la clé de session IPsec.

Prérequis

- **Tunnel IPsec IKEv2 opérationnel** entre pfSense-01 et pfSense-02 (état « Established » visible dans `Status > IPsec`)
- **SRV-AD-01** (10.11.3.18) et **SRV-AD-02** (10.11.4.18) — Réplication AD active (vérifiée via `repadmin /showrepl`)
- **Wireshark** installé sur `CL-WIN11-01` (poste d'analyse)
- **Accès administrateur** à l'interface web pfSense-01 (`https://10.11.3.17`)
- Ouvrir `Services > Active Directory Sites and Services` sur SRV-AD-01 pour vérifier que le site « Site-B » existe bien

> **Rappel d'architecture IPsec**
> **pfSense-01 WAN :** `10.10.101.3` ↔ **pfSense-02 WAN :** `10.10.101.4`
> Phase 1 IKEv2 : `AES-256 / SHA-256 / DH Groupe 14 (2048 bits)` — Phase 2 ESP : `AES-256 / SHA-256 / PFS Groupe 14`
> Réseaux tunnelés : `10.11.3.16/28 ↔ 10.11.4.16/28`

Étape 1 — Initialisation du flux (Le « Trigger »)

Pour rendre le trafic AD visible dans Wireshark, il faut forcer des échanges réseau entre les deux sites. Un **ping continu** depuis SRV-AD-01 vers SRV-AD-02 génère du trafic ICMP encapsulé dans le tunnel IPsec — ce trafic sera capturé sous forme de paquets ESP opaques.

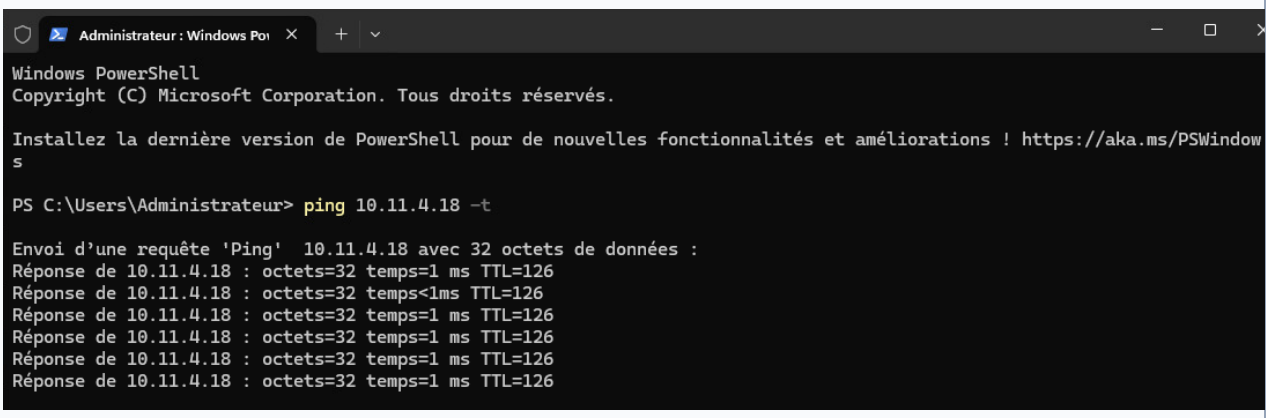
Action — Sur SRV-AD-01

Ouvrir une invite de commandes en tant qu'Administrateur et exécuter :

```
# Ping continu vers SRV-AD-02 (Site B) pour générer du trafic inter-sites
ping 10.11.4.18 -t
```

Le résultat attendu est une réponse `Reply from 10.11.4.18: bytes=32 time<1ms TTL=127` à chaque ligne. Ce retour prouve que le lien logique inter-sites fonctionne et que les paquets transitent bien par le tunnel.

CAPTURE D'ÉCRAN N°1 — Terminal SRV-AD-01 — ping 10.11.4.18 -t avec des réponses continues. La résolution et le TTL prouvent le transit via le tunnel IPsec.



Étape 2 — Capture de paquets sur pfSense-01 (Interface WAN)

On va intercepter les paquets au moment précis où ils quittent l'interface WAN de pfSense-01 vers Internet. À ce stade, si le chiffrement fonctionne, on ne doit voir **aucun protocole interne lisible** — uniquement des enveloppes ESP.

Action — Sur pfSense-01

Se connecter à l'interface web pfSense-01 : `https://10.11.3.17` puis naviguer dans `Diagnostics > Packet Capture`

Interface	`WAN (interface publique, sortie vers Internet)`
Protocol	`ESP (Encapsulating Security Payload)`
Host Address	`10.10.101.4 (IP WAN de pfSense-02, Site B)`
Count	`0 (capture illimitée, on l'arrête manuellement)`

Buffer Size	1 Mo (suffisant pour 10 secondes de trafic)

CAPTURE D'ÉCRAN N°2 — Page Diagnostics > Packet Capture de pfSense-01 — configuration remplie (WAN, ESP, 10.10.101.4) avant de cliquer sur Start.

Packet Capture Output: /tmp/packetcapture-vmx1-20260506170358.pcap

```
15:03:59.391976 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ee8), length 104
15:03:59.392620 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x1855), length 104
15:03:59.392700 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ee9), length 104
15:03:59.392722 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eea), length 136
15:03:59.393497 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x1856), length 120
15:03:59.393510 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x1857), length 104
15:03:59.393612 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eeb), length 104
15:03:59.393641 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eec), length 104
15:03:59.393868 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x1858), length 104
15:03:59.842443 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eed), length 104
15:03:59.843047 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x1859), length 104
15:03:59.843297 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eee), length 88
15:03:59.843549 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1eef), length 88
15:03:59.843566 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ef0), length 120
15:03:59.843907 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x185a), length 88
15:04:00.391702 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ef1), length 104
15:04:00.392742 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x185b), length 104
15:04:00.392864 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ef2), length 104
15:04:00.392880 IP 10.10.101.3 > 10.10.101.4: ESP(spi=0xc6d2b689,seq=0x1ef3), length 152
15:04:00.393750 IP 10.10.101.4 > 10.10.101.3: ESP(spi=0xcd261ac6,seq=0x185c), length 120
```

Cliquer sur **Start**. Laisser la capture tourner **10 à 15 secondes** (le ping doit continuer sur SRV-AD-01 pendant ce temps). Cliquer sur **Stop**, puis sur **Download Capture** pour récupérer le fichier `.pcap` sur `SRV-AD-01`.

Pourquoi filtrer sur ESP et non sur TCP/UDP ?

Le protocole ESP (IP Protocol 50) est le protocole de transport d'IPsec en mode tunnel. Tout paquet chiffré par IPsec arrive au niveau WAN sous cette forme. En filtrant sur ESP + IP WAN du Site B, on s'assure de ne capturer que le trafic IPsec sortant vers pfSense-02, sans bruit parasite.

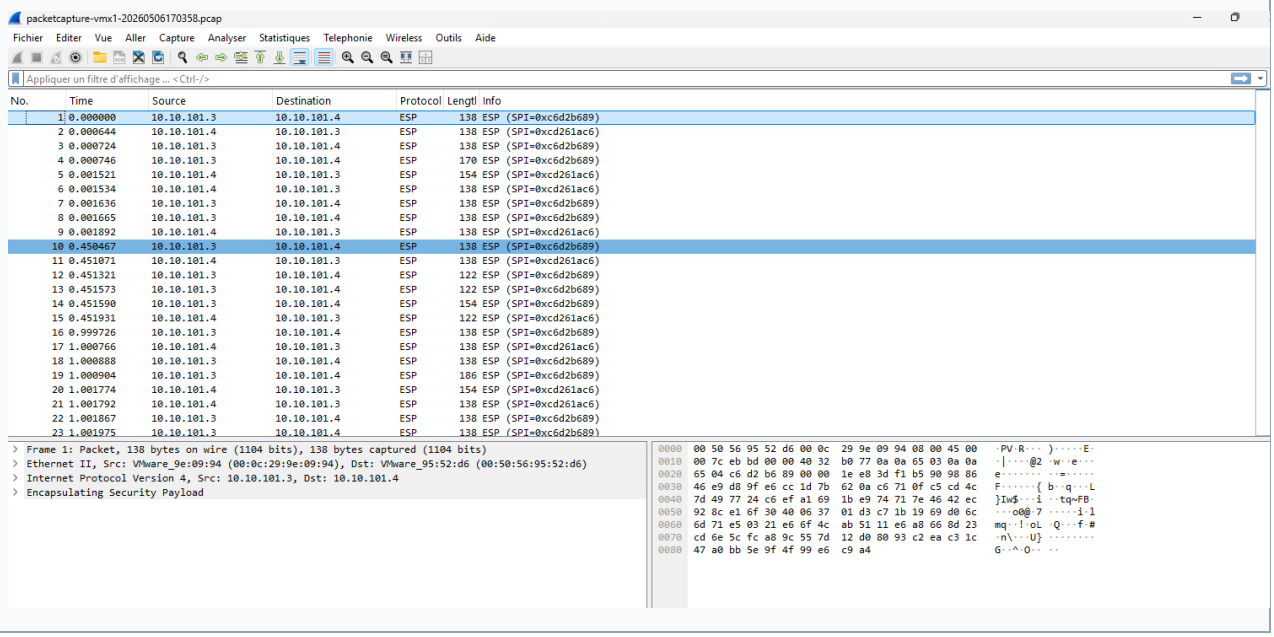
Étape 3 — Analyse dans Wireshark : première preuve (colonne Protocol)

Ouvrir le fichier `.pcap` téléchargé avec Wireshark sur `CL-WIN11-01`. L'observation de la colonne **Protocol** constitue la première preuve formelle de chiffrement.

Observation attendue

- La colonne **Protocol** affiche **ESP** sur toutes les lignes — Wireshark est incapable d'identifier un protocole de couche applicative (pas de « ICMP », « RPC », « LDAP », « DNS »)
- La colonne **Info** affiche seulement `Encapsulated Security Payload`, sans aucun détail de contenu
- Les adresses `Source` et `Destination` affichent les IP WAN : `10.10.101.3` → `10.10.101.4` (et inversement pour les réponses)

CAPTURE D'ÉCRAN N°3 — Fenêtre principale de Wireshark — colonne Protocol remplie uniquement de lignes « ESP ». Aucun protocole applicatif visible. C'est la première preuve de chiffrement.



Interprétation pour l'oral

Wireshark ne peut pas disséquer le contenu de ces paquets car il n'a pas accès à la clé de session IKEv2 négociée entre les deux pfSense. Sans cette clé, les octets du payload sont mathématiquement indistinguables d'une suite aléatoire.

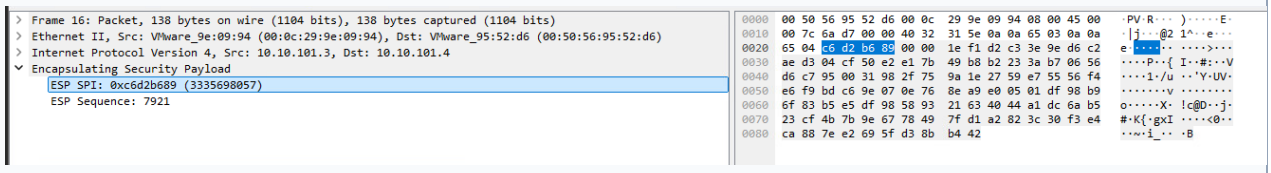
Étape 4 — La preuve par l'échec : analyse du payload (Data hexadécimal)

C'est l'étape qui apporte la preuve **irréfutable**. En cliquant sur un paquet ESP et en observant la zone **Data / Payload** dans le panneau inférieur de Wireshark, on visualise directement l'impossibilité de lire le contenu.

Procédure

1. Sélectionner un paquet ESP au hasard dans la liste
2. Dans le panneau du milieu (arbre de dissection), déplier la section `Encapsulating Security Payload`
3. Observer la ligne `Data:` — elle affiche une suite hexadécimale sans structure identifiable
4. Dans le panneau du bas (dump hexadécimal), aucune chaîne ASCII lisible n'apparaît — pas de `ICMP`, pas de `ping`, pas de `LDAP`, pas de `Kerberos`

CAPTURE D'ÉCRAN N°4 — Wireshark — zoom sur la zone Data/Payload d'un paquet ESP sélectionné. La suite hexadécimale opaque prouve que le contenu est chiffré AES-256. Aucun protocole interne identifiable.



Commentaire technique pour l'oral

"Ici, on voit que Wireshark est **incapable d'identifier le protocole** transporté à l'intérieur du paquet (ICMP, Kerberos, RPC de réplication AD...).

Les données sont **encapsulées et chiffrées en AES-256 bits**. Sans la clé de session IKEv2, qui n'existe que sur les deux pfSense, le contenu est **mathématiquement illisible**.

Un attaquant interceptant ce trafic sur le réseau public ne verrait que des blocs de données aléatoires — il ne pourrait même pas déterminer qu'il s'agit de trafic Active Directory. C'est exactement l'objectif de l'architecture IPsec."

Tests et Validation finale

Critères de succès — Checklist jury

☑ **Critère 1 :** Le ping depuis SRV-AD-01 vers SRV-AD-02 répond avec succès (preuve de connectivité via tunnel)

☑ **Critère 2 :** La capture pfSense sur l'interface WAN ne contient que des paquets ESP — aucun protocole interne en clair

☑ **Critère 3 :** Wireshark affiche uniquement « ESP » en colonne Protocol — preuve que le chiffrement est actif

☑ **Critère 4 :** Le payload hexadécimal est opaque — aucune donnée Active Directory lisible en clair sur le réseau public

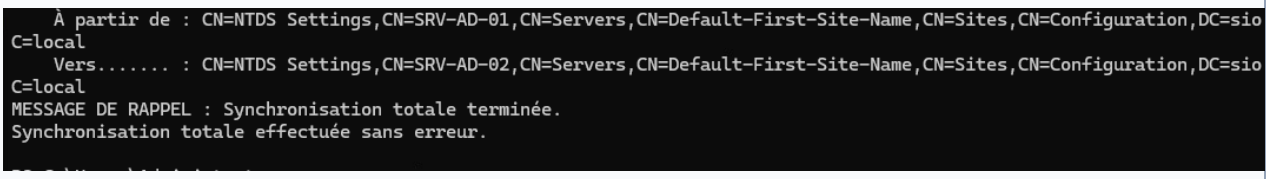
Test complémentaire — Vérification de la réplication AD

Sur **SRV-AD-01**, vérifier que la réplication fonctionne correctement :

```
# Vérification complète de la réplication inter-sites
repadmin /showrepl

# Résultat attendu :
# DC=sio,DC=local
#    Default-First-Site-Name\SRV-AD-02 via RPC
#       GUID du domaine : <GUID>
#       La dernière tentative le <date> a réussi.
```

CAPTURE D'ÉCRAN N°5 — Résultat de repadmin /showrepl sur SRV-AD-01 — La dernière réplication avec SRV-AD-02 est marquée « a réussi ». Preuve que les données AD transitent correctement via le tunnel chiffré.

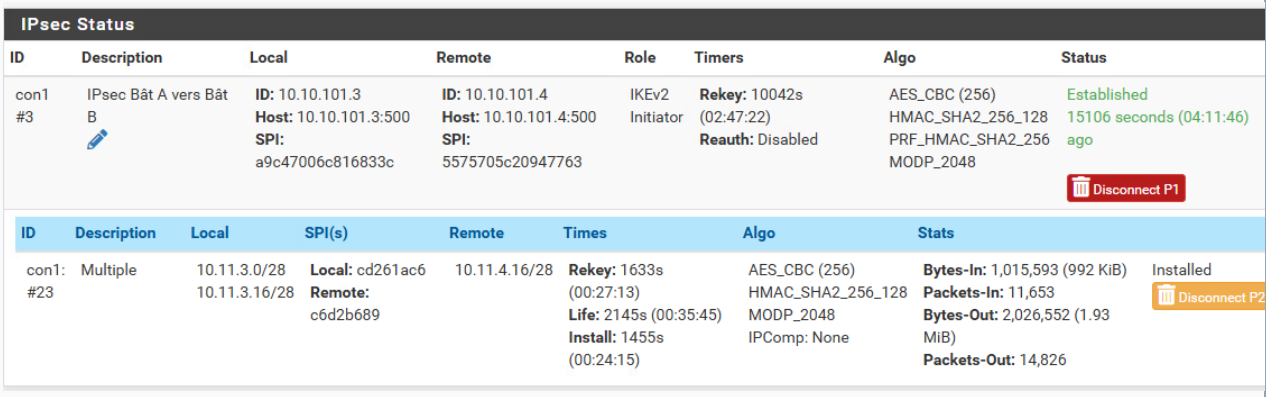


Test complémentaire — Statut IPsec sur pfSense-01

Dans l'interface web pfSense-01, naviguer dans `Status > IPsec`. Le tunnel doit afficher :

État	ESTABLISHED
Local	10.10.101.3 / 10.11.3.16/28
Remote	10.10.101.4 / 10.11.4.16/28
Algorithme	AES-CBC (256) / HMAC-SHA2-256 / MODP-2048
Bytes-In	Valeur > 0 (trafic reçu depuis Site B)
Bytes-Out	Valeur > 0 (trafic envoyé vers Site B)

CAPTURE D'ÉCRAN N°6 — Interface Status > IPsec de pfSense-01 — Tunnel en état ESTABLISHED avec les compteurs Bytes-In et Bytes-Out non nuls, confirmant un trafic actif et chiffré.



Conclusion technique

La démonstration prouve, de manière empirique et non théorique, que l'architecture IPsec IKEv2 déployée sur la PME Sio-sisr garantit la **confidentialité totale** des flux de réplication Active Directory.

Toute interception du trafic sur le réseau public entre les IPs WAN `10.10.101.3` et `10.10.101.4` ne révèle que des paquets ESP dont le contenu est **mathématiquement indéchiffrable** sans la clé de session — conformément aux spécifications `RFC 4303 (ESP)` et `RFC 7296 (IKEv2)`.