FICHE PROCÉDURE

Configuration d'un DNS Sinkhole (Menteur) sous Windows Server 2025

Blocage de domaines par manipulation de la résolution DNS au niveau du contrôleur de domaine

Auteur : CHADHOULI EL-Anrif — BTS SIO SISR 2026 — MEWO Metz

Champ	Valeur
Auteur	CHADHOULI EL-Anrif — BTS SIO SISR 2026
Établissement	MEWO Metz
Domaine AD	sio.local
Serveur DNS	SRV-AD-01 — Windows Server 2025 — 10.11.3.18
Poste de test	CL-WIN11-01 — Windows 11 Pro — 10.11.3.25
Domaine bloqué	facebook.com (exemple)
Technique	DNS Sinkhole — Zone primaire AD intégrée — redirection 127.0.0.1

1. CONTEXTE ET ENJEUX DE SÉCURITÉ

1.1 Qu'est-ce qu'un DNS Sinkhole ?

Un DNS Sinkhole (ou DNS menteur) est une technique de sécurité réseau qui consiste à créer une fausse zone DNS autoritaire sur le contrôleur de domaine. Lorsqu'un poste client interroge le serveur DNS pour résoudre un domaine bloqué, le DNS répond avec une adresse IP locale fictive (127.0.0.1) au lieu de l'IP réelle du serveur distant. Le trafic est ainsi court-circuité dès la résolution de noms, avant même d'atteindre le pare-feu ou le proxy.

ℹ INFO — Le DNS Sinkhole opère à la couche 7 (Application) avant toute décision de routage. C'est la méthode la plus efficace et la plus légère pour bloquer massivement des domaines malveillants ou indésirables.

1.2 Pourquoi cette méthode complète le proxy Squid ?

Méthode	Niveau d'action	Avantage	Limite
Proxy Squid	HTTP/HTTPS (couche 7)	Filtrage des URLs, inspection TLS	Requiert config proxy sur le client
Règle pfSense	Réseau (couche 3/4)	Bloque IP/port	Contournable via DNS alternatif
DNS Sinkhole ✓	Résolution DNS (couche 7)	Bloque avant connexion, transparent	Ne bloque que si DNS AD utilisé

Combiné avec le proxy Squid et les règles pfSense, le DNS Sinkhole forme une défense en profondeur à trois niveaux : les domaines bloqués ne sont jamais résolus, donc aucun trafic ne se propage sur le réseau.

⚠ SÉCURITÉ — Cette technique est efficace uniquement pour les postes qui utilisent SRV-AD-01 comme résolveur DNS (ce qui est le cas de tous les postes joints au domaine sio.local via DHCP). Un poste configuré avec un DNS externe (8.8.8.8) contournerait le sinkhole.

1.3 Flux de fonctionnement

```
SANS Sinkhole :
CL-WIN11-01 → DNS SRV-AD-01 → "facebook.com = 157.240.x.x" → Connexion réussie

AVEC Sinkhole :
CL-WIN11-01 → DNS SRV-AD-01 → "facebook.com = 127.0.0.1" → Connexion échouée
                                ↑
                Zone primaire fictive créée sur SRV-AD-01
                Répliquée automatiquement sur SRV-AD-02 (AD intégré)
```

2. PRÉREQUIS

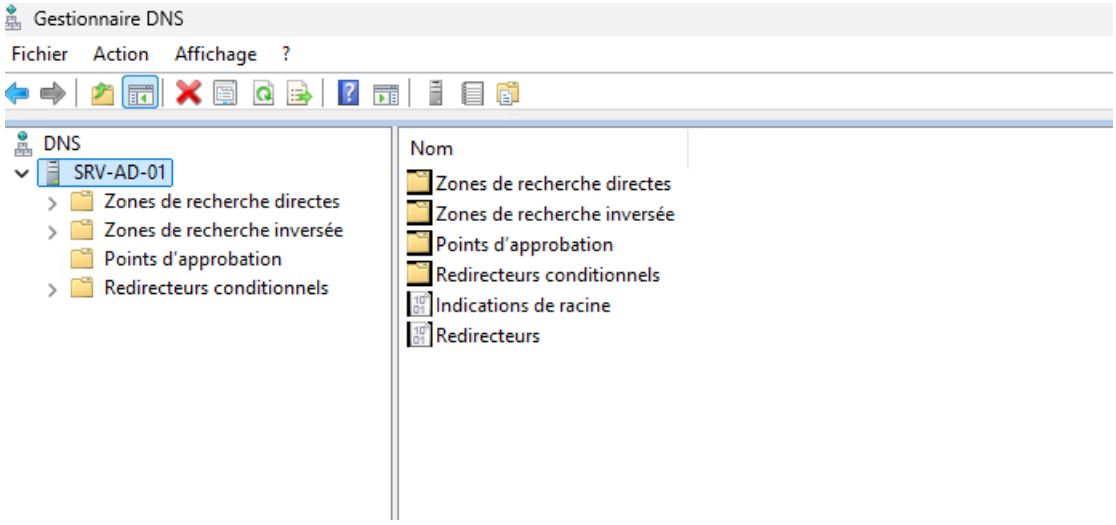
- Accès administrateur du domaine sur SRV-AD-01 (10.11.3.18).
- Rôle DNS Server installé et actif sur SRV-AD-01.
- CL-WIN11-01 joint au domaine sio.local — DNS configuré sur 10.11.3.18.
- Snapshot VMware SRV-AD-01 pris avant manipulation (recommandé).

Vérification	Commande / Emplacement	Résultat attendu
DNS actif sur AD1	services.msc → DNS Server	En cours d'exécution
DNS client CL-WIN11-01	ipconfig /all → DNS Servers	10.11.3.18 (primaire)
Poste joint au domaine	systeminfo | findstr /i "domain"	sio.local

ÉTAPE 1 — CRÉATION DE LA FAUSSE ZONE DNS

1.1 Ouverture de la console DNS

- Se connecter sur SRV-AD-01 avec un compte Administrateur du domaine.
- Ouvrir le Gestionnaire de serveur.
- Cliquer sur Outils → DNS.
- Dans l'arborescence de gauche, dérouler SRV-AD-01.



1.2 Création de la nouvelle zone

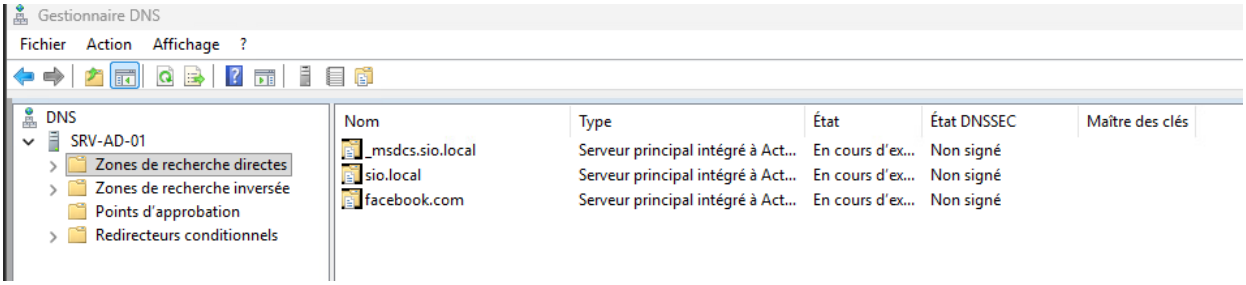
- Clic droit sur Zones de recherche directe → Nouvelle zone...
- L'assistant Nouvelle zone s'ouvre — cliquer sur Suivant.

```
Type de zone : Zone principale
               ✓ Stocker la zone dans Active Directory
               (réplication automatique sur SRV-AD-02)
```

- Cliquer sur Suivant.
- Étendue de réplication AD : sélectionner "À tous les serveurs DNS exécutant Windows Server dans ce domaine : sio.local" → Suivant.
- Nom de la zone : saisir exactement le domaine à bloquer :

```
facebook.com
```

- Cliquer sur Suivant.
- Mises à jour dynamiques: laisser le choix par défaut → Suivant → Terminer.



ℹ INFO — En cochant "Stocker la zone dans Active Directory", la règle de sinkhole sera automatiquement répliquée sur SRV-AD-02 (Site B) via le tunnel IPsec. Aucune configuration manuelle supplémentaire n'est nécessaire sur AD2.

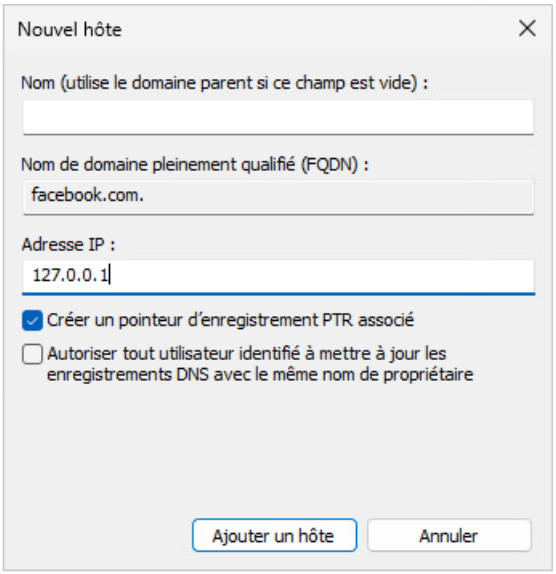
ÉTAPE 2 — CRÉATION DE L'ENREGISTREMENT DE REDIRECTION (FAUX POINTEUR)

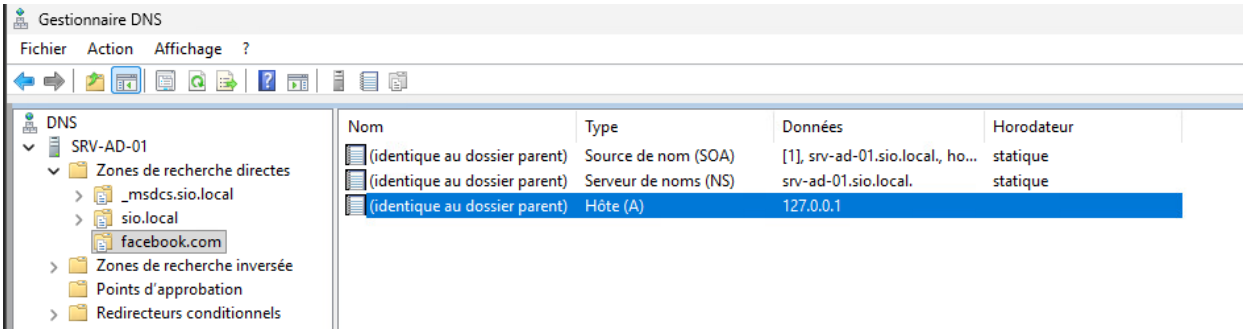
2.1 Création de l'enregistrement A (hôte)

- Dans la console DNS, cliquer sur la zone facebook.com dans le panneau gauche.
- Clic droit dans l'espace vide du panneau central → Nouvel hôte (A ou AAAA)...

```
Champ "Nom"          : laisser VIDE
                       (s'applique au domaine parent facebook.com lui-même)
Champ "Adresse IP"   : 127.0.0.1
                       (boucle locale — le paquet ne quitte jamais le poste client)
```

- Cliquer sur Ajouter un hôte.
- Cliquer sur OK sur le message de confirmation.
- Cliquer sur Terminé.





2.2 Enregistrement SOA et NS — vérification

La zone crée automatiquement deux enregistrements supplémentaires : un enregistrement SOA (Start Of Authority) et un enregistrement NS (Name Server) pointant vers SRV-AD-01. Ces enregistrements sont normaux et n'ont pas besoin d'être modifiés.

Enregistrement	Valeur	Rôle
SOA	SRV-AD-01.sio.local	Serveur autoritaire de la zone
NS	SRV-AD-01.sio.local	Serveur de noms de la zone
A	127.0.0.1 (nom vide)	Faux pointeur — cœur du sinkhole

⚠ SÉCURITÉ — Utiliser 127.0.0.1 et non 0.0.0.0. L'adresse 127.0.0.1 est la boucle locale du poste client lui-même — la connexion échoue immédiatement sans générer de trafic réseau. L'adresse 0.0.0.0 peut provoquer des comportements indéfinis selon les OS.

2.3 Méthode PowerShell (alternative)

La même configuration peut être réalisée en PowerShell sur SRV-AD-01 :

```
# Créer la zone sinkhole intégrée AD
Add-DnsServerPrimaryZone -Name "facebook.com" `
  -ReplicationScope "Domain" `
  -DynamicUpdate "None"

# Créer l'enregistrement A de redirection
Add-DnsServerResourceRecordA -ZoneName "facebook.com" `
  -Name "@" `
  -IPv4Address "127.0.0.1" `
  -TimeToLive 00:05:00

# Vérification
Get-DnsServerZone -Name "facebook.com"
Resolve-DnsName facebook.com -Server 127.0.0.1
```

ÉTAPE 3 — TESTS ET VALIDATION DEPUIS LE POSTE CLIENT

3.1 Préparation du test sur CL-WIN11-01

- Se connecter sur CL-WIN11-01 (10.11.3.25) avec un compte du domaine sio.local.
- Ouvrir une invite de commande (cmd.exe) en tant qu'utilisateur standard.

3.2 Vidage du cache DNS

Vider le cache DNS local pour forcer une nouvelle requête vers SRV-AD-01 :

```
ipconfig /flushdns
```

Résultat attendu :

```
Configuration IP de Windows


Vidage réussi du cache de résolution DNS.
```

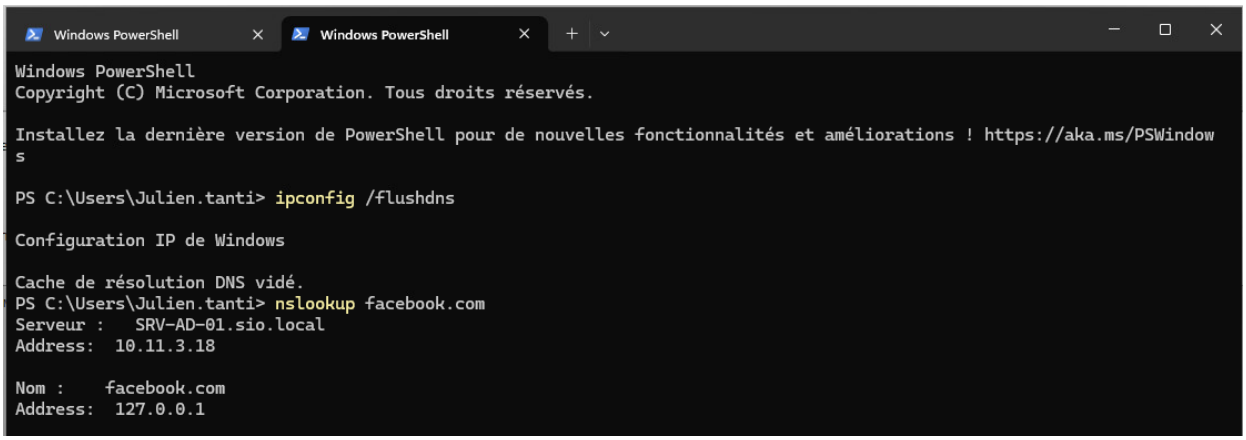
3.3 Test de résolution DNS avec nslookup

Vérifier que le DNS Sinkhole répond correctement avant de tester la connectivité :

```
nslookup facebook.com

→ Résultat attendu :
   Serveur :  SRV-AD-01.sio.local
   Address:   10.11.3.18

   Nom :      facebook.com
   Address:   127.0.0.1    ← Sinkhole actif
```



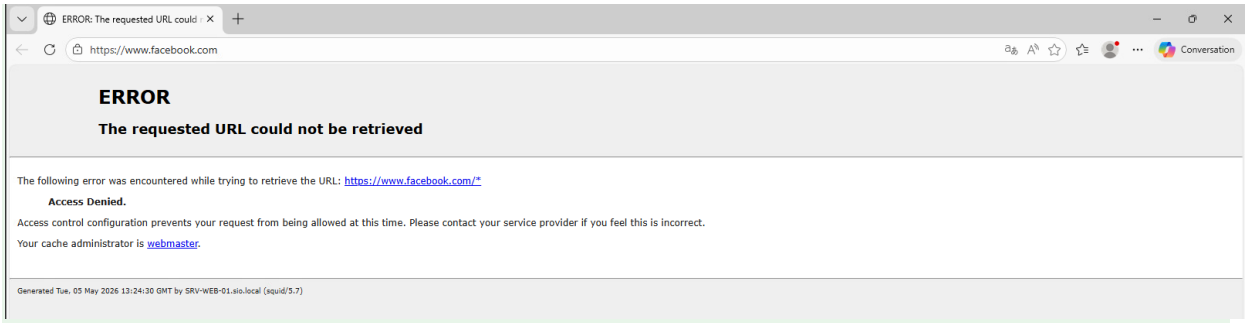
3.4 Vérification du blocage DNS via curl depuis un poste client

```
PS C:\Users\Julien.tanti> curl -v  https://facebook.com
COMMENTAIRES : GET with 0-byte payload
curl : ERROR
The requested URL could not be retrieved
The following error was encountered while trying to retrieve the URL: https://facebook.com/*
Access Denied.
Access control configuration prevents your request from being allowed at this time. Please contact your service
provider if you feel this is incorrect.
Your cache administrator is webmaster.
Generated Tue, 05 May 2026 13:42:06 GMT by SRV-WEB-01.sio.local (squid/5.7)
Au caractère Ligne:1 : 1
+ curl -v  https://facebook.com
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation : (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebEx
   ception
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\Users\Julien.tanti>
```

INFO — La commande curl -v https://facebook.com tente une connexion HTTPS réelle vers le site. Si le DNS Sinkhole est actif, facebook.com est résolu en 127.0.0.1 et curl retourne une erreur de connexion refusée, prouvant qu'aucun accès applicatif n'est possible.

3.5 Test de navigation web (preuve finale)

- Ouvrir Microsoft Edge ou Firefox sur CL-WIN11-01.
- Saisir https://facebook.com dans la barre d'adresse.
- Résultat attendu : page d'erreur du navigateur : ERROR: The requested URL could not be retrieved — Access Denied" générée par SRV-WEB-01.sio.local (squid/5.7) — Double blocage confirmé : DNS Sinkhole + filtrage proxy Squid.
-



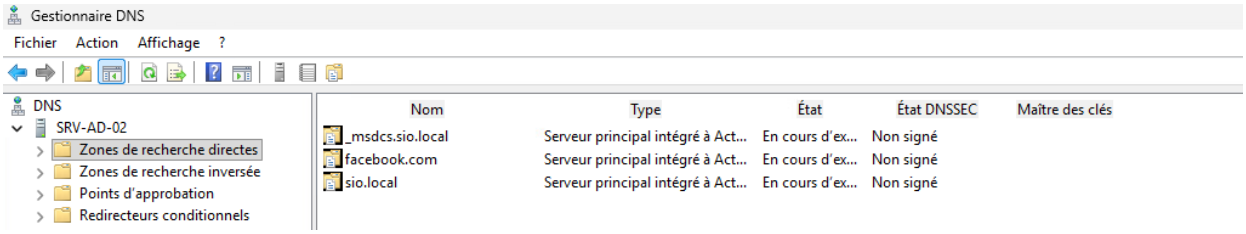
INFO — Le message "Access Denied" est généré par le proxy Squid (SRV-WEB-01.sio.local). Cela confirme que même si un utilisateur tentait de contourner le DNS, le proxy intercepte et bloque la requête au niveau HTTP/HTTPS. Le blocage est donc opéré en double couche.

ÉTAPE 4 — VÉRIFICATION DE LA RÉPLICATION SUR SRV-AD-02

4.1 Vérification côté SRV-AD-02

La zone facebook.com étant intégrée à Active Directory, elle se réplique automatiquement sur SRV-AD-02 (10.11.4.18) via le tunnel IPsec IKEv2. Vérifier la réplication depuis SRV-AD-02 :

- Se connecter sur SRV-AD-02.
- Ouvrir la console DNS.
- Vérifier que la zone facebook.com apparaît dans Zones de recherche directe.




```
# Forcer la réplication AD si nécessaire (depuis SRV-AD-01)
repadmin /syncall /AdeP

# Vérification PowerShell depuis SRV-AD-02
Get-DnsServerZone -Name "facebook.com"
Resolve-DnsName facebook.com -Server 10.11.4.18
→ Address: 127.0.0.1  ← Réplication confirmée
```

ℹ INFO — CL-WIN11-02 (Site B — 10.11.4.24) utilise SRV-AD-02 comme DNS secondaire. Grâce à la réplication AD, le sinkhole s'applique automatiquement au Site B sans aucune configuration supplémentaire.