BTS SIO — Option SISR

Session 2026

Épreuve E6 — Support et mise à disposition de services informatiques

Réalisation Professionnelle n°2

Sécurisation et contrôle des accès Internet

Filtrage DNS · Durcissement des postes · Supervision SIEM

Informations	
Candidat	REGNIER David
Numéro de candidat	2541525521
Établissement de formation	CFA INGETIS
Entreprise d'accueil	Tavite (entreprise fictive — infogérance PME Île-de-France)
Date de réalisation	Juin 2026
Environnement technique	Proxmox VE — VLANs — Windows Server 2022 — pfSense

SOMMAIRE

1. Présentation du contexte

1.1 L'entreprise Tavite

Tavite est une entreprise fictive spécialisée dans l'infogérance de PME en Île-de-France, gérée dans le cadre du CFA INGETIS. Elle dispose d'une infrastructure réseau composée de plusieurs serveurs Windows, de postes clients et d'un pare-feu pfSense assurant la connexion Internet de l'ensemble du parc.

1.2 Problématique

L'infrastructure réseau de Tavite utilisait les modules Squid et SquidGuard de pfSense pour le filtrage des accès Internet. Ces modules sont désormais obsolètes et ne répondent plus aux exigences actuelles de sécurité et de traçabilité.

Les lacunes identifiées dans la situation initiale étaient les suivantes :

- Requêtes DNS non chiffrées, exposées à l'interception ou à la manipulation
- Absence de protection contre les domaines malveillants et les contenus inappropriés
- Consommation de bande passante non maîtrisée (services de streaming, réseaux sociaux)
- Aucune traçabilité ni supervision des accès Internet
- Possibilité de contournement du filtrage par changement manuel du serveur DNS

1.3 Objectifs de la réalisation

N°	Objectif	Solution retenue
1	Centraliser et filtrer les accès Internet	DNS Resolver pfSense en forwarding + Cloudflare filtrant 1.1.1.3/1.0.0.3 via DNS over TLS
2	Renforcer la sécurité des postes clients	GPO Active Directory — Defender SmartScreen, protection temps réel, pare-feu forcé
3	Réduire la consommation de bande passante	Filtrage DNS par catégories (streaming, réseaux sociaux, jeux bloqués par Cloudflare)
4	Améliorer la traçabilité et la supervision	Export Syslog pfSense vers Wazuh SIEM (VLAN 99) — dashboards et alertes

2. Architecture de la solution

2.1 Inventaire des équipements

Rôle	Système	Adresse IP	Hostname
Pare-feu / Routeur	pfSense 2.7.x	192.168.2.1	pfSense
Contrôleur de domaine / DNS	Windows Server 2022	192.168.2.10	AD-DNS.tavite.lan
Serveur DHCP / WDS	Windows Server 2022	192.168.2.11	DHCP-WDS.tavite.lan
Poste client (test)	Windows 11 22H2	DHCP (192.168.2.50-250)	PC-TAVITE-001
Supervision SIEM	Debian 12 + Wazuh	192.168.99.20 (VLAN 99)	Wazuh

2.2 Schéma de flux DNS

```
[Postes clients Windows 10/11]
        |
        |  Requêtes DNS  (port 53 - interne uniquement)
        v
[AD-DNS.tavite.lan  192.168.2.10  - Windows Server 2022]
        |
        |  Zones internes tavite.lan --> résolues localement
        |  Domaines externes         --> forwardes vers pfSense
        v
[pfSense DNS Resolver  192.168.2.1]
        |
        |  Mode forwarding + DNS over TLS (port 853)
        v
[Cloudflare  1.1.1.3 / 1.0.0.3]
        |  Filtrage : malware + contenu adulte
        |  Chiffrement : DoT (family.cloudflare-dns.com)
```

2.3 Schéma de supervision

```
VLAN 108  (192.168.2.0/24)                VLAN 99  (192.168.99.0/24)
--------------------------------          ---------------------------
pfSense  192.168.2.1                     Wazuh SIEM  192.168.99.20
  |  Logs DNS + Firewall                    |  Wazuh Manager
  |  Syslog UDP:514 ---------------------> |  Wazuh Indexer
  |                                         |  Dashboard HTTPS:443
AD-DNS  192.168.2.10
Postes clients
  |  Agents Wazuh (optionnel) ------------>  |
```

3. Mise en place du filtrage DNS

3.1 Présentation de Cloudflare DNS filtrant

Cloudflare propose plusieurs niveaux de filtrage accessibles via des adresses IP dédiées :

Adresses IP	Niveau de filtrage	Nom d'hôte TLS
1.1.1.1 / 1.0.0.1	Aucun filtrage (DNS standard)	cloudflare-dns.com
1.1.1.2 / 1.0.0.2	Blocage malware uniquement	security.cloudflare-dns.com
1.1.1.3 / 1.0.0.3	Blocage malware + contenu adulte (retenu)	family.cloudflare-dns.com

Les serveurs 1.1.1.3 et 1.0.0.3 ont été retenus pour leur double niveau de protection. Le DNS over TLS (DoT) sur le port 853 chiffre les échanges entre pfSense et Cloudflare, empêchant toute interception ou modification des requêtes DNS en transit.

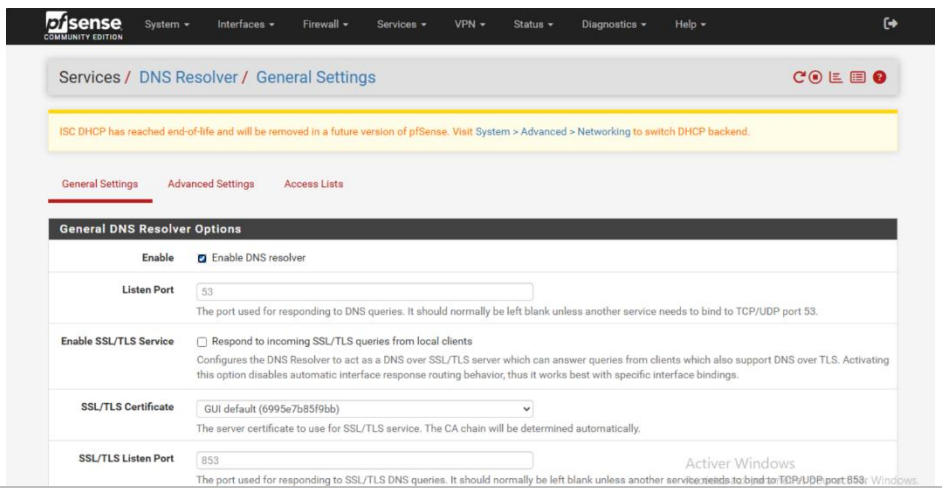
3.2 Configuration du DNS Resolver pfSense

3.2.1 Paramètres généraux

Configuration effectuée depuis l'interface web pfSense (Services > DNS Resolver) :

Paramètre	Valeur configurée	Justification
Enable DNS Resolver	Activé	Active le service Unbound sur pfSense
Network Interfaces	All	Requis car pfSense utilise son propre DNS Resolver
Outgoing Network Interfaces	WAN	Les requêtes sortantes transitent par l'interface WAN
Enable Forwarding Mode	Activé	Transmet les requêtes vers les serveurs Cloudflare
Use SSL/TLS for outgoing DNS Queries	Activé	Active le chiffrement DoT vers Cloudflare (port 853)

Services > DNS Resolver > General Settings => Enable Forwarding Mode + SSL/TLS activés



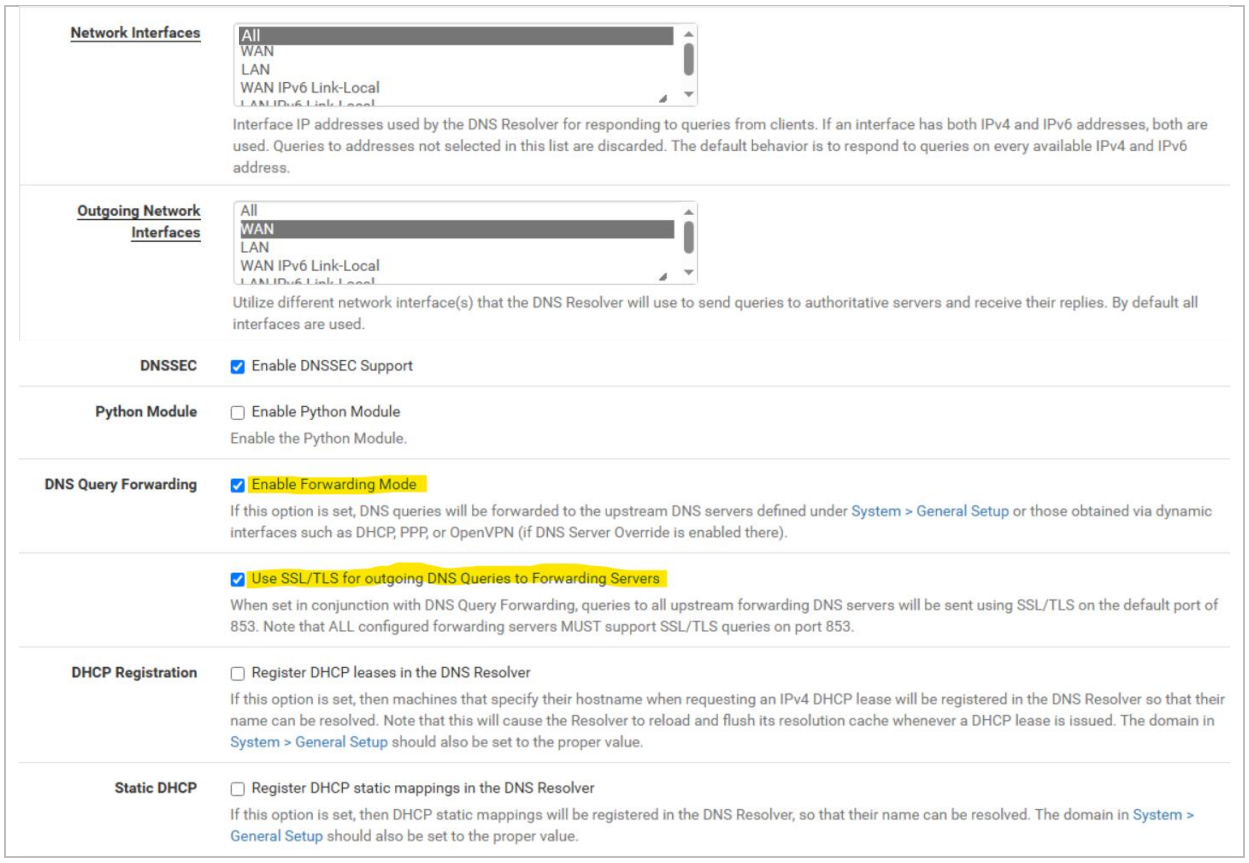


Figure 1 — Configuration du DNS Resolver pfSense

3.2.2 Ajout des serveurs Cloudflare filtrants

Les serveurs Cloudflare ont été déclarés dans le champ Custom Options du DNS Resolver.
Cette configuration indique à Unbound de transmettre toutes les requêtes vers Cloudflare via DoT :

```
forward-zone:
    name: "."
    forward-ssl-upstream: yes
    forward-addr: 1.1.1.3@853#family.cloudflare-dns.com
    forward-addr: 1.0.0.3@853#family.cloudflare-dns.com
```

Le suffixe #family.cloudflare-dns.com est le nom d'hôte TLS utilisé pour valider le certificat Cloudflare lors de la connexion DoT. @853 indique le port DoT. Sans ces paramètres, le chiffrement ne peut pas être vérifié.

3.3 Nettoyage de la configuration DNS système

La configuration système de pfSense a été nettoyée (System > General Setup) pour éliminer tout contournement involontaire par un DNS externe :

Paramètre	Avant	Après configuration
DNS Servers	1.1.1.1	Vide — aucun serveur DNS externe
DNS Server Override	Activé (FAI peut remplacer les DNS)	Désactivé
DNS Resolution Behavior	Fallback vers DNS distants	Use local DNS (127.0.0.1) only

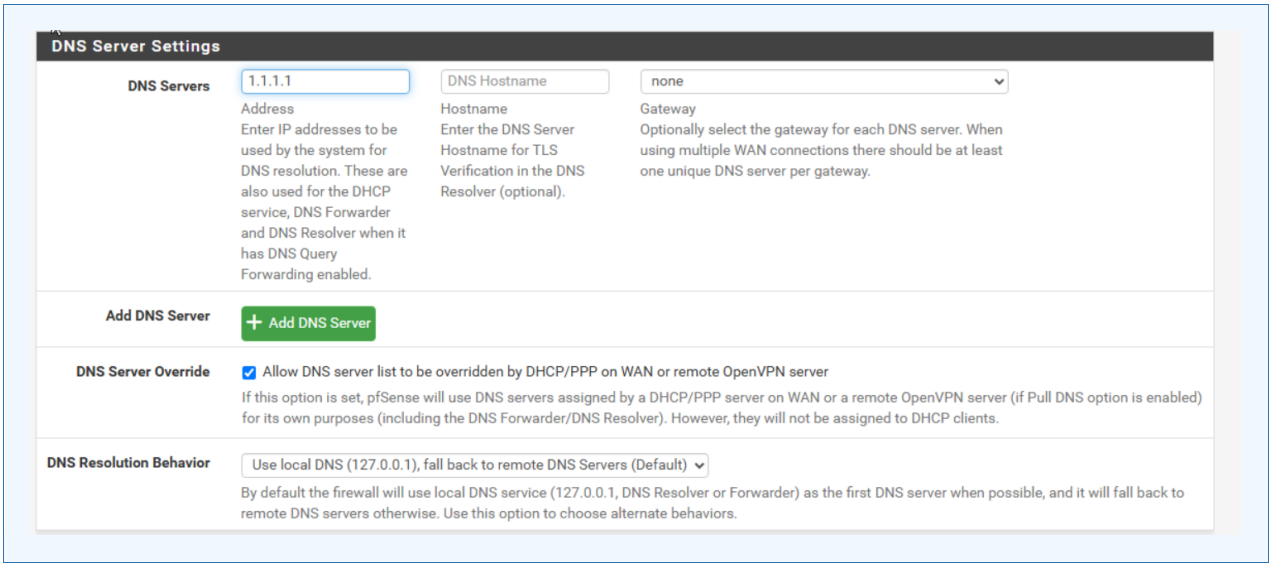


Figure 2 — Configuration DNS système pfSense après nettoyage

3.4 Configuration du redirecteur sur le serveur AD-DNS

Le serveur DNS (AD-DNS.tavite.lan, 192.168.2.10) a été configuré pour transmettre toutes les requêtes externes vers pfSense. Cette configuration est accessible depuis le Gestionnaire DNS (dnsmgmt.msc) > Propriétés du serveur > onglet Redirecteurs.

Paramètre	Valeur
Redirecteur configuré	192.168.2.1 (pfSense DNS Resolver)
Utiliser les indications de racine si aucun redirecteur disponible	Désactivé — pour éviter toute résolution directe sans filtrage

Gestionnaire DNS — Propriétés AD-DNS.tavite.lan — Onglet Redirecteurs (192.168.2.1 configuré)

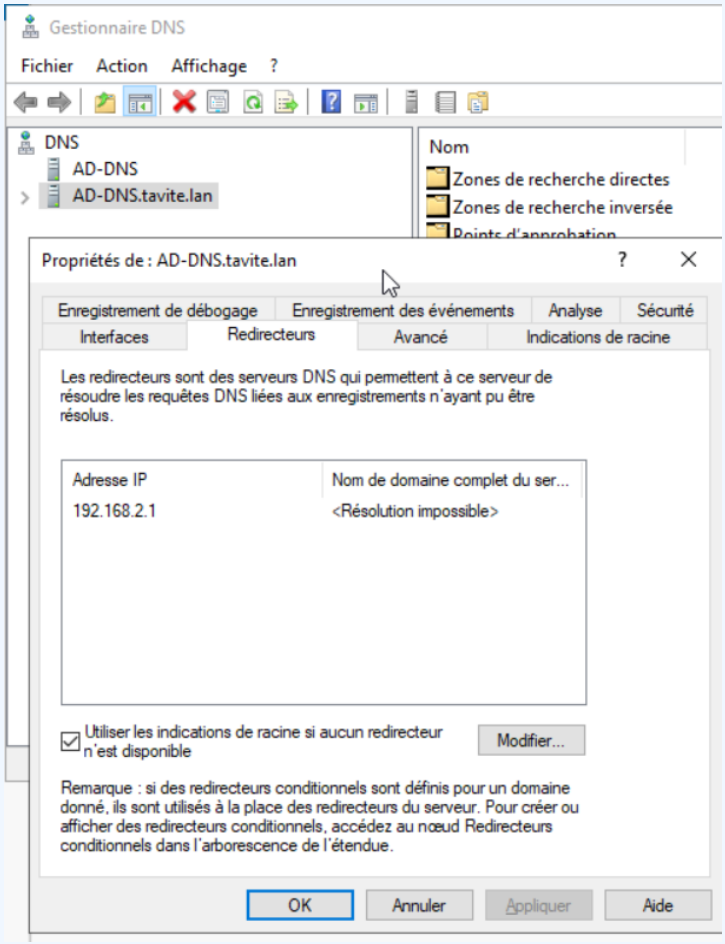


Figure 3 — Redirecteur DNS Windows Server pointant vers pfSense

La désactivation des indications de racine est critique : si elle était active, en cas d'indisponibilité de pfSense, le serveur DNS résoudrait directement vers Internet sans aucun filtrage, créant une faille de sécurité.

3.5 Validation du filtrage

3.5.1 Test depuis pfSense (Diagnostics > DNS Lookup)

Domaine testé	Résultat attendu	Résultat obtenu	Statut
google.com	IP valide (non filtré)	172.217.22.46	OK
pornhub.com	Blocage par Cloudflare	Host could not be resolved	BLOQUE

Diagnostics > DNS Lookup — pornhub.com : Host could not be resolved

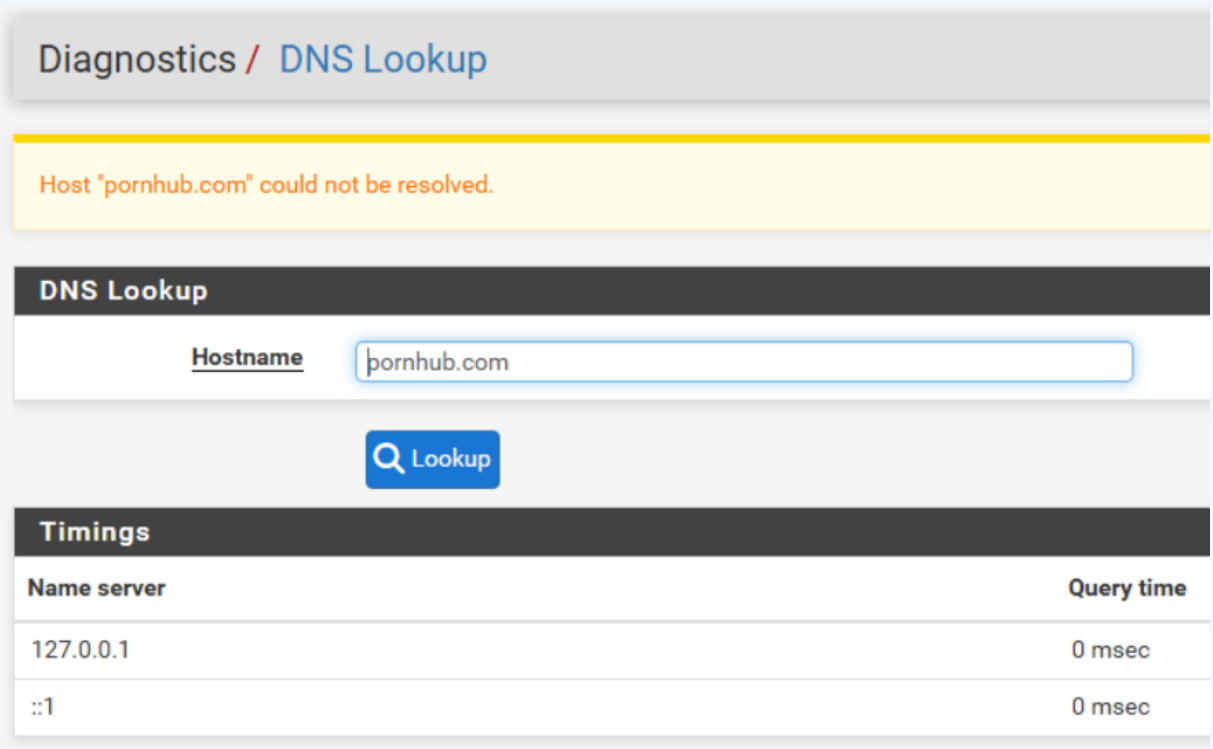


Figure 4 — Filtrage Cloudflare actif depuis pfSense

3.5.2 Test depuis un poste client Windows (PC-TAVITE-001)

```
PS C:\> Resolve-DnsName google.com
Name         Type  TTL   IPAddress
google.com   A     105   172.217.22.110   --> RESOLU (normal)

PS C:\> Resolve-DnsName pornhub.com
Resolve-DnsName : Defaillance du serveur DNS
RCODE_SERVER_FAILURE              --> BLOQUE PAR CLOUDFLARE
```

PowerShell client — Resolve-DnsName google.com (résolu) et pornhub.com (échec DNS)

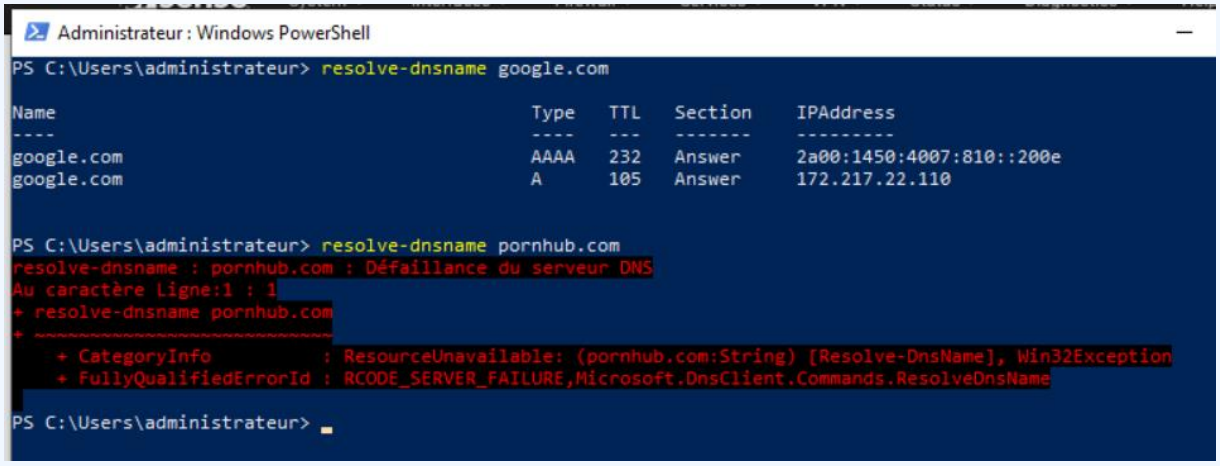


Figure 5 — Validation du filtrage Cloudflare depuis le poste client

4. Blocage des contournements DNS

4.1 Objectif

Sans règle de pare-feu complémentaire, un utilisateur peut contourner le filtrage en configurant manuellement un serveur DNS externe (ex. 8.8.8.8 ou 9.9.9.9) directement sur son poste. Les règles créées sur pfSense empêchent ce type de contournement en bloquant tout trafic DNS direct vers Internet sur les ports 53 (DNS standard) et 853 (DNS over TLS).

4.2 Règles de pare-feu créées

Les règles suivantes ont été créées dans Firewall > Rules > LAN, dans l'ordre de priorité (pfSense applique la première règle correspondante, de haut en bas) :

Priorité	Action	Source	Destination	Port	Description
1	PASS	192.168.2.10	192.168.2.1	53 / TCP+UDP	AD-DNS vers pfSense DNS Resolver
2	PASS	LAN subnets	192.168.2.10	53 / TCP+UDP	Clients vers AD-DNS (flux légitime)
3	BLOCK	LAN subnets	Any	53 / TCP+UDP	Bloquer tout DNS direct externe
4	BLOCK	LAN subnets	Any	853 / TCP+UDP	Bloquer tout DoT direct externe

Les règles 1 et 2 autorisent les flux DNS légitimes : clients > AD-DNS (192.168.2.10) > pfSense (192.168.2.1). Le blocage du port 853 empêche un utilisateur d'utiliser un client DoT configuré manuellement vers un serveur externe non filtrant.

Firewall > Rules > LAN — Les 4 règles DNS dans l'ordre correct

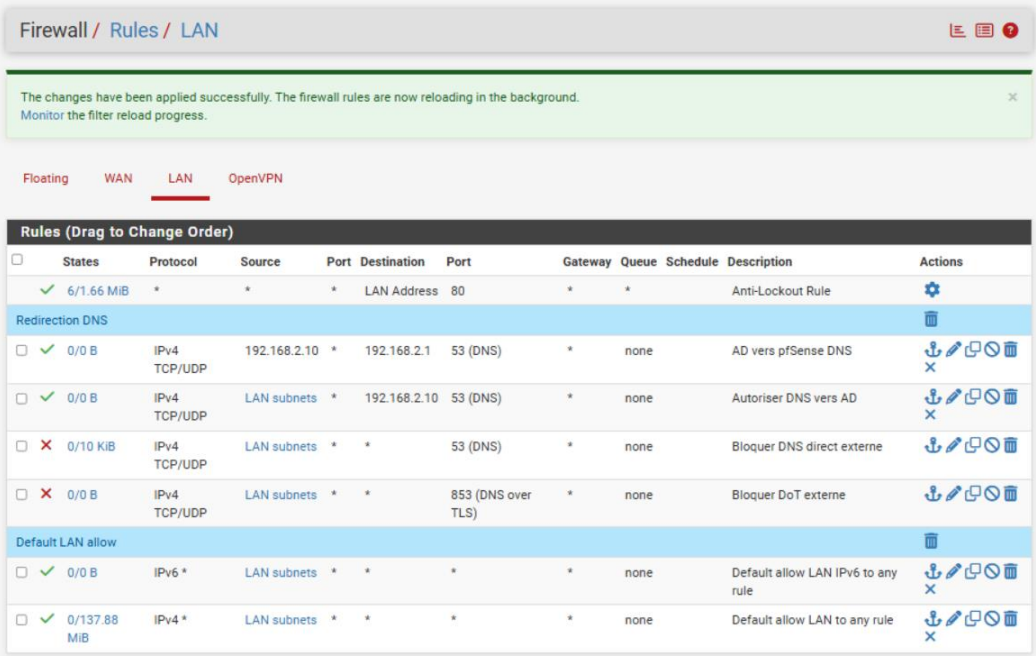


Figure 6 — Règles firewall pfSense bloquant les contournements DNS

4.3 Validation du blocage

Le test de contournement a été réalisé depuis le poste client en forçant l'utilisation de 8.8.8.8 comme serveur DNS via le paramètre -Server de PowerShell :

```
PS C:\> Resolve-DnsName google.com -Server 8.8.8.8
Resolve-DnsName : Cette operation s'est terminee car le delai d'attente a expire
ERROR_TIMEOUT

FullyQualifiedErrorId :
OperationTimeout,Microsoft.DnsClient.Commands.ResolveNameCommand

--> BLOQUE : les paquets DNS vers 8.8.8.8 sont silencieusement droppes par pfSense
```

PowerShell client — Resolve-DnsName google.com -Server 8.8.8.8 (ERROR_TIMEOUT)

Figure 7 — Tentative de bypass DNS bloquée par la règle firewall

Le timeout (ERROR_TIMEOUT) confirme que les paquets DNS à destination de 8.8.8.8:53 sont silencieusement supprimés (action Block) par pfSense avant d'atteindre Internet. L'action Block drop les paquets sans notifier l'expéditeur, contrairement à Reject qui renverrait un refus.

5. Renforcement des postes clients par stratégie de groupe (GPO)

5.1 Structure Active Directory

Le domaine tavite.lan dispose d'une Unité d'Organisation Ordi_Deploye dans laquelle sont automatiquement placés les postes déployés via WDS/MDT. La GPO de sécurité a été liée directement à cette OU.

```
tavite.lan
 |-- Builtin
 |-- Computers            (conteneur par defaut)
 |-- Domain Controllers
 |-- Managed Service Accounts
 |-- Ordi_Deploye         <-- GPO Securite_Postes_Tavite liee ici
 |    |-- PC-TAVITE-001
 |-- Users
```

5.2 Création et liaison de la GPO

La GPO a été créée depuis la console Gestion de stratégie de groupe (gpmc.msc) par un clic droit sur l'OU Ordi_Deploye > Créer un objet GPO dans ce domaine, et le lier ici.

Paramètre	Valeur
Nom de la GPO	Securite_Postes_Tavite
OU cible	Ordi_Deploye (DC=tavite, DC=lan)
Lien activé	Oui
État GPO	Activé
Étendue d'application	Configuration ordinateur (s'applique au compte machine, pas à l'utilisateur)

Gestion de stratégie de groupe (gpmc.msc) — Securite_Postes_Tavite liée à Ordi_Deploye

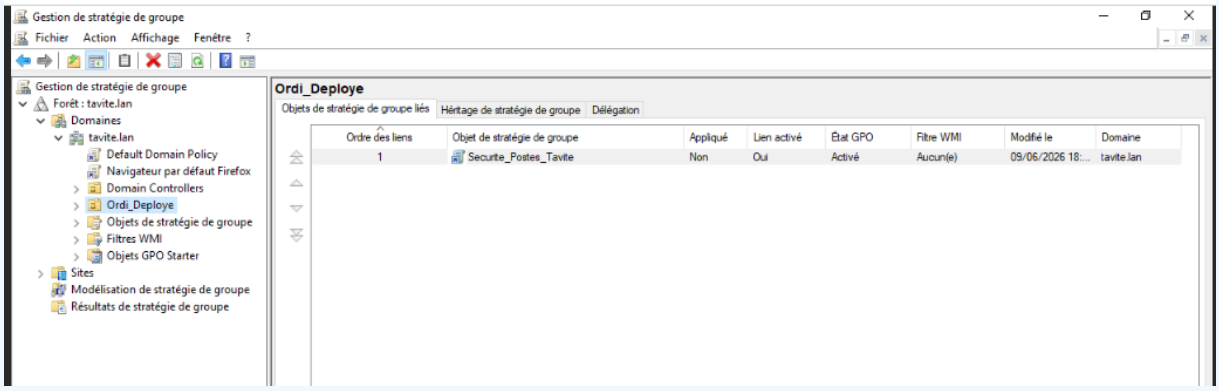


Figure 8 — GPO créée et liée à l'OU Ordi_Deploye

5.3 Paramètres de sécurité configurés

5.3.1 Microsoft Defender SmartScreen — Explorateur de fichiers

Chemin : Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Explorateur de fichiers

Paramètre GPO	Valeur	Effet sur le poste
Configurer Windows Defender SmartScreen	Activé — Avertir et empêcher tout contournement	Bloque l'exécution de fichiers non reconnus téléchargés depuis Internet. L'utilisateur ne peut pas ignorer l'avertissement.

Éditeur GPO — Configurer Windows Defender SmartScreen (Activé + Avertir et empêcher tout contournement)

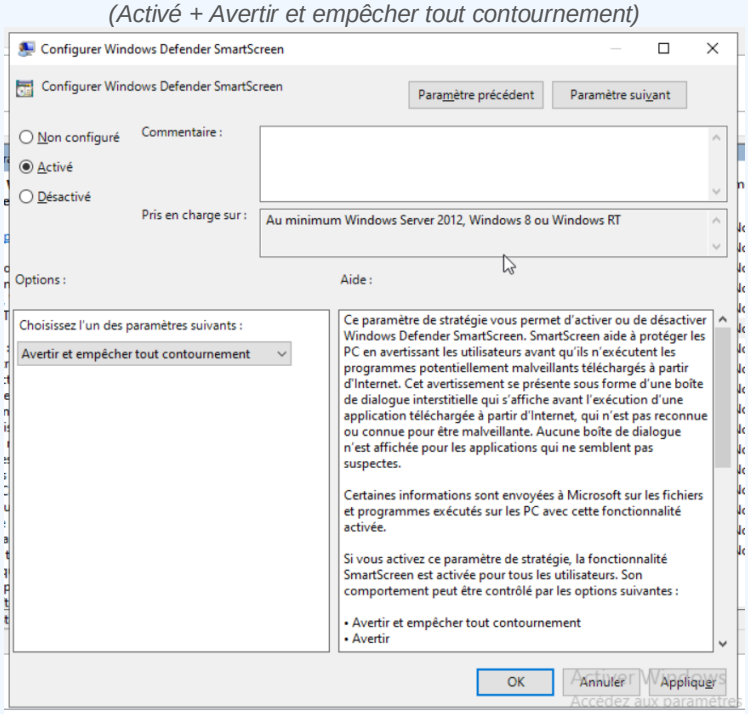


Figure 9 — Paramètre SmartScreen dans l'Explorateur de fichiers

5.3.2 Microsoft Defender Antivirus — Protection en temps réel

Chemin : Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Antivirus Microsoft Defender > Protection en temps réel

Paramètre GPO	Valeur	Effet sur le poste
Activer la surveillance du comportement	Activé	Surveille les comportements suspects des processus en temps réel
Analyser tous les fichiers et pièces jointes téléchargés	Activé	Analyse automatique de tout fichier téléchargé avant exécution

Éditeur GPO > Connexion Réseau > Pare-feu Windows Defender > Profil du domaine
⇨ Pare-feu Windows Defender : protéger toutes les connexions réseau
⇨

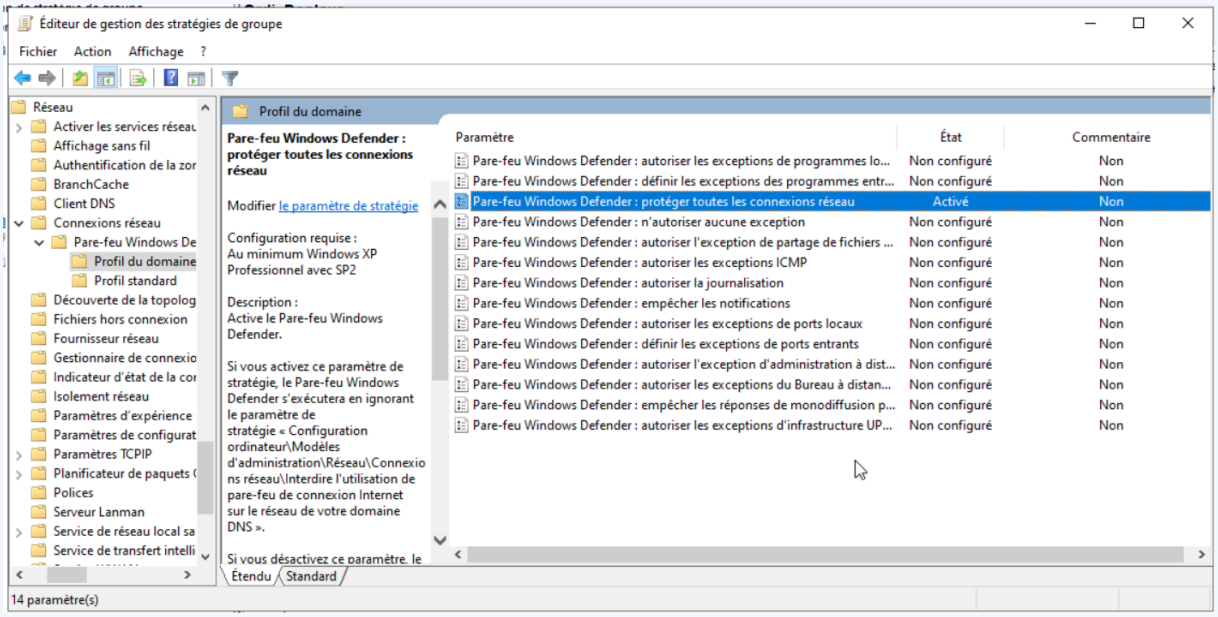


Figure 9.1 — Activation de la protection en temps réel

5.3.3 Pare-feu Windows

Chemin : Configuration ordinateur > Stratégies > Modèles d'administration > Réseau > Connexions réseau > Pare-feu Windows

Paramètre GPO	Profil	Valeur
Pare-feu Windows : protéger toutes les connexions réseau	Profil de domaine	Activé — garantit l'activation du pare-feu en environnement AD
Pare-feu Windows : protéger toutes les connexions réseau	Profil standard	Activé — garantit l'activation hors domaine (déconnecté)

5.4 Validation de l'application de la GPO

La validation a été effectuée sur le poste PC-TAVITE-001, membre de l'OU Ordi_Deploye, en session ouverte avec un compte du domaine TAVITE.

```
C:\> gpresult /r /scope computer
CN=PC-TAVITE-001, OU=Ordi_Deploye, DC=tavite, DC=lan
Strategie de groupe appliquee depuis : AD-DNS.tavite.lan

Objets Strategie de groupe appliques
  Securite_Postes_Tavite     <-- CONFIRME
  Default Domain Policy
  Navigateur par defaut Firefox
```

gpresult /r /scope computer — Securite_Postes_Tavite listée dans les GPO appliquées

```
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

```
C:\Users\angelo.test>gpresult /r /scope computer

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© Microsoft Corporation. Tous droits réservés.

Créé le 10/06/2026 à 15:25:00


Données RSOP pour  sur PC-TAVITE-001 : mode journalisation
-----------------------------------------------------------

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.26200
Nom du site........................... : Default-First-Site-Name
Profil itinérant :
Profil local.......................... :
Connexion via une liaison lente ? : Non


Paramètre de l'ordinateur
--------------------------
    CN=PC-TAVITE-001,OU=Ordi_Deploye,DC=tavite,DC=lan
    Heure de la dernière application de la stratégie de groupe : 10/06/2026 à 15:16:46
    Stratégie de groupe appliquée depuis :      AD-DNS.tavite.lan
    Seuil de liaison lente dans la stratégie de groupe :   500 kbps
    Nom du domaine..................... : TAVITE
    Type de domaine.................... : Windows 2008 ou supérieur
    Objets Stratégie de groupe appliqués
    ------------------------------------
        Securite_Postes_Tavite
        Default Domain Policy
        Navigateur par défaut Firefox

    Les objets stratégie de groupe n'ont pas été appliqués
    car ils ont été refusés
    -----------------------------------------------------------------------------------------
        Stratégie de groupe locale
          Filtrage :  Non appliqué (vide)

    L'ordinateur fait partie des groupes de sécurité suivants
    ---------------------------------------------------------
        Administrateurs
        Tout le monde
        Utilisateurs
        RESEAU
        Utilisateurs authentifiés
        Cette organisation
        PC-TAVITE-001$
        Ordinateurs du domaine
        Identité déclarée par une autorité d'authentification
        Niveau obligatoire système
```

Figure 10 — Validation de l'application de la GPO sur PC-TAVITE-001

6. Supervision et traçabilité — Wazuh SIEM

6.1 Présentation de Wazuh

Wazuh est une plateforme SIEM (Security Information and Event Management) open source. Elle assure la collecte, la corrélation et l'analyse en temps réel des événements de sécurité provenant de multiples sources. Dans ce projet, Wazuh est déployé sur une VM Debian 12 dédiée, accessible sur le VLAN de supervision (VLAN 99, réseau isolé).

Composant	Rôle	Port
Wazuh Manager	Reçoit et traite les logs des agents et sources Syslog	1514/1515 (agents), 514 UDP (Syslog)
Wazuh Indexer	Stocke et indexe les événements (basé sur OpenSearch)	9200 (interne)
Wazuh Dashboard	Interface web de visualisation, alertes et tableaux de bord	443 (HTTPS)

6.2 Configuration de l'export Syslog sur pfSense

pfSense a été configuré pour transmettre ses logs DNS et les événements de pare-feu vers Wazuh via le protocole Syslog UDP. La configuration est accessible depuis Status > System Logs > Settings > Remote Logging Options :

Paramètre	Valeur configurée
Enable Remote Logging	Activé
Remote log servers	192.168.99.20:514 (Wazuh SIEM, VLAN 99)
Remote Syslog Contents — DNS logs	Activé — transmet toutes les requêtes DNS résolues et bloquées
Remote Syslog Contents — Firewall events	Activé — transmet les événements de filtrage (règles BLOCK)

[CAPTURE D'ECRAN A INSERER]

pfSense — Status > System Logs > Settings — Remote Logging Options configuré vers 192.168.99.20:514

Figure 11 — Configuration Syslog pfSense vers Wazuh

Note de déploiement : La VM Wazuh est sur le VLAN 99 (réseau de supervision isolé), séparé du réseau principal (VLAN 2). Une règle inter-VLAN sur pfSense permettra d'acheminer le flux Syslog UDP:514 de 192.168.2.1 vers 192.168.99.20. Cette configuration sera finalisée lors de l'ouverture du VLAN 99 en environnement de production.

6.3 Flux de données et alertes

Une fois la connectivité VLAN établie, Wazuh reçoit en temps réel les événements de pfSense et permet de détecter les scénarios suivants :

Scénario de sécurité	Indicateur dans Wazuh	Action recommandée
Tentative de bypass DNS (ex. 8.8.8.8)	Alertes répétées sur règle BLOCK port 53, même IP source	Identifier le poste, vérifier la configuration réseau
Accès à domaine malveillant (bloqué)	SERVFAIL sur domaine catégorisé malware par Cloudflare	Analyser le poste source, rechercher présence de malware
Volume DNS anormal (exfiltration)	Nombre de requêtes DNS/h > seuil sur une IP source	Suspicion d'exfiltration DNS, isoler le poste concerné
Accès à catégorie hors politique	Requête DNS vers domaine de streaming ou jeux bloqué	Rappel de la charte informatique à l'utilisateur

7. Bilan de la réalisation

7.1 Objectifs atteints

Objectif	Statut	Preuve de validation
Filtrage DNS via Cloudflare filtrant (DoT)	Atteint	Resolve-DnsName pornhub.com : SERVFAIL depuis client Windows
Blocage des contournements DNS (ports 53/853)	Atteint	Resolve-DnsName -Server 8.8.8.8 : ERROR_TIMEOUT
GPO de sécurité sur les postes (SmartScreen, Defender, FW)	Atteint	gpresult confirme Securite_Postes_Tavite sur PC-TAVITE-001
Export Syslog pfSense vers Wazuh SIEM	Partiellement atteint	Configuration pfSense effectuée — connectivité VLAN 99 en attente

7.2 Difficultés rencontrées et solutions apportées

- Paramètre Network Interfaces du DNS Resolver configuré sur LAN au lieu de All, provoquant une erreur au démarrage du service (pfSense a besoin d'écouter sur localhost pour ses propres résolutions). Solution : passage sur All.
- Règle firewall BLOCK LAN subnets > Any:53 bloquant également le trafic légitime du serveur AD-DNS (192.168.2.10) vers pfSense (192.168.2.1:53). Solution : ajout d'une règle PASS explicite prioritaire pour ce flux.
- Échec de gpupdate /force sur un poste de test en raison d'une désynchronisation NTP (service w32time non configuré). Solution : w32tm /config /manualpeerlist:"192.168.2.10,0x8" suivi de w32tm /resync /force.
- Accès au VLAN 99 de supervision non disponible dans l'environnement Proxmox scolaire, empêchant la finalisation du déploiement Wazuh. Solution : configuration pfSense effectuée en attente d'ouverture inter-VLAN par l'administrateur.

7.3 Améliorations possibles

- Installation des templates ADMX Microsoft Edge pour étendre la GPO SmartScreen au navigateur Edge (non disponibles par défaut sur Windows Server 2022).
- Déploiement d'agents Wazuh sur les postes Windows pour une supervision enrichie (processus, fichiers système, registre, connexions réseau).
- Création de règles de corrélation personnalisées dans Wazuh pour détecter automatiquement les tentatives répétées de bypass DNS et déclencher des alertes.
- Configuration d'alertes email ou webhook dans Wazuh pour notifier l'administrateur en temps réel lors de détection d'incident de sécurité.
- Mise en place d'une politique de mot de passe renforcée via GPO (longueur minimale, complexité, historique) en complément des politiques de sécurité déjà déployées.