DNS over HTTPS en Entreprise avec Microsoft 2026 : Déploiement et Sécurité

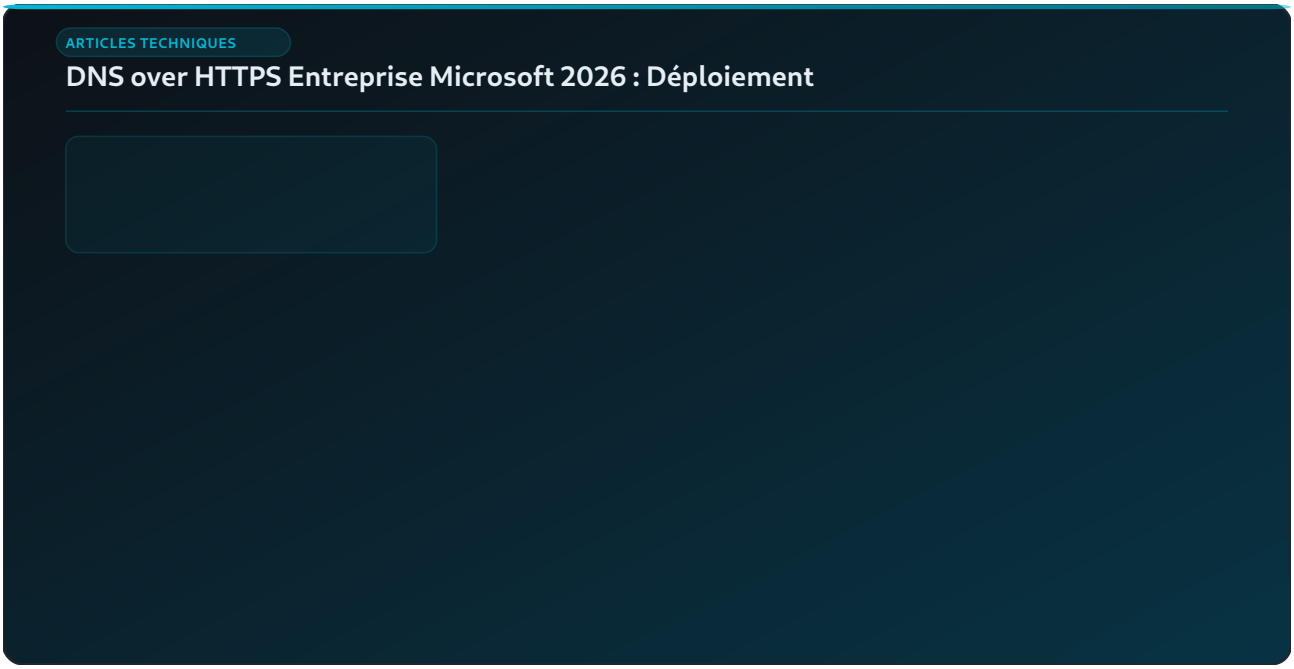
Déployez DNS over HTTPS en entreprise Windows Server 2025 : résolveur interne, GPO, blocage DoH public, conformité NIS 2 et ANSSI pour administrateurs.

📋 EN BREF

- DNS over HTTPS (DoH) chiffre les requêtes DNS dans du trafic HTTPS (port 443), rendant l'inspection DNS traditionnelle inefficace en entreprise.
- Windows 11 et Windows Server 2025 intègrent nativement DoH, configurable via PowerShell et GPO sans logiciel tiers.
- Windows Server 2025 peut servir de résolveur DoH interne, permettant de conserver l'inspection DNS tout en chiffrant le trafic client-serveur.
- Le contrôle du DoH en entreprise passe par le blocage des résolveurs publics (Cloudflare 1.1.1.1, Google 8.8.8.8) et le forçage vers le résolveur interne approuvé.
- Le DoH non contrôlé représente un vecteur de contournement DLP et de communications C2, détectable via JA3/JA4 fingerprinting et analyse Zeek.

La sécurité DNS est devenue un enjeu stratégique pour les entreprises françaises, notamment depuis l'entrée en vigueur de la directive NIS 2 transposée en droit français en octobre 2024. Dans les grandes métropoles comme Paris, Lyon ou Bordeaux, les RSSI font face à une double contrainte : garantir la confidentialité des requêtes DNS de leurs collaborateurs — souvent exposées en clair sur le réseau — tout en maintenant une capacité d'inspection et de filtrage indispensable à la sécurité du système d'information. DNS over HTTPS (DoH), standardisé par la RFC 8484 et désormais intégré nativement dans Windows 11 et Windows Server 2025, apporte une réponse technique à la première exigence, mais complexifie considérablement la

seconde. Cet article propose un guide complet de déploiement et de gouvernance du DoH en environnement Microsoft d'entreprise, en couvrant la configuration native, la mise en place d'un résolveur DoH interne, le contrôle du trafic DoH non autorisé, et les implications réglementaires pour les entreprises soumises à NIS 2 ou aux recommandations de l'ANSSI. La maîtrise de DNS over HTTPS représente aujourd'hui un prérequis pour tout RSSI souhaitant maintenir une visibilité complète sur les flux réseau de son organisation tout en renforçant la protection des postes nomades et des télétravailleurs contre les attaques par empoisonnement DNS.



Avant de déployer DNS over HTTPS en entreprise, il est essentiel de comprendre les différences fondamentales entre les trois approches de résolution DNS disponibles aujourd'hui. Chacune présente des avantages et des inconvénients distincts selon le contexte d'utilisation.

Protocole	Port	Chiffrement	Support entreprise Windows	Bypass firewall
DNS classique (Do53)	53/UDP, 53/TCP	Aucun	Natif depuis Windows NT	Non (port dédié, filtrable)
DNS over TLS (DoT)	853/TCP	TLS 1.2/1.3	Partiel (via stub resolver tiers)	Faible (port distinct, détectable)
DNS over HTTPS (DoH)	443/TCP	TLS 1.2/1.3 (dans HTTPS)	Natif Windows 11 / Server 2025	Élevé (se fond dans le trafic HTTPS)

Le DNS classique (Do53) reste le protocole le plus répandu en entreprise, mais il expose toutes les requêtes en clair sur le réseau. Un simple sniffing réseau ou une attaque Man-in-the-Middle permet d'observer l'intégralité des sites et services consultés par les collaborateurs. DNS over TLS (DoT) résout ce problème en encapsulant le DNS dans une session TLS, mais utilise le port 853, facilement identifiable et filtrable par les firewalls d'entreprise.

DNS over HTTPS va plus loin : les requêtes DNS sont encapsulées dans des requêtes HTTPS standard sur le port 443. Du point de vue réseau, le trafic DoH est indiscernable du trafic HTTPS vers n'importe quel site web. C'est précisément ce qui pose problème en entreprise.

Pourquoi DoH pose problème en entreprise

L'inspection DNS est un pilier de la sécurité des systèmes d'information en entreprise. Les solutions de filtrage DNS (Cisco Umbrella, Infoblox, Windows DNS avec RPZ) permettent de bloquer les domaines malveillants, de détecter les communications C2, d'appliquer des politiques d'utilisation acceptable et d'alimenter les SIEM en logs de requêtes DNS. Lorsqu'un poste Windows 11 configure DoH vers un résolveur public comme Cloudflare (1.1.1.1) ou Google (8.8.8.8), il contourne l'intégralité de cette infrastructure :

Les requêtes DNS ne transitent plus par le résolveur interne de l'entreprise

Les politiques de filtrage DNS ne s'appliquent plus

Les logs DNS du résolveur interne sont incomplets

Les outils de détection basés sur les requêtes DNS (Zeek, Suricata) deviennent aveugles

Les acteurs malveillants peuvent utiliser DoH vers des résolveurs publics pour faire communiquer leurs malwares (C2 over DoH)

La bonne approche n'est donc pas d'interdire DoH — ce qui est techniquement difficile sur le port 443 — mais de le contrôler en déployant un résolveur DoH interne approuvé et en bloquant les résolveurs DoH publics.

DoH sur Windows 11 / Server 2025 : Configuration Native

Microsoft a introduit le support natif de DoH dans Windows 10 version 19628 (build Insider) et l'a généralisé dans Windows 11. Windows Server 2025 étend ce support côté serveur. La configuration peut se faire manuellement, par PowerShell ou via GPO en environnement d'entreprise.

> ⚡ **Retour terrain**
>
> Pour un éditeur SaaS RH qui migrait vers Kubernetes, la première mise en production a révélé des pods qui consommaient 10× plus de mémoire que prévu — sans limits configurées, ils saturaient les nodes. J'avais prévenu que les limits et requests devaient être calibrées avant le départ en production. La leçon retenue : dans un cluster mutualisé, un pod sans limite est une bombe à retardement pour les voisins.

Configurer DoH via PowerShell : Add-DnsClientDohServerAddress

La cmdlet `Add-DnsClientDohServerAddress` permet d'enregistrer un serveur DoH dans la liste des résolveurs DoH approuvés de Windows. Voici la syntaxe de base :

```
 # Ajouter un résolveur DoH interne approuvé
Add-DnsClientDohServerAddress `
    -ServerAddress "10.0.0.53" `
    -DohTemplate "https://dns.interne.entreprise.fr/dns-query" `
    -AllowFallbackToUdp $false `
    -AutoUpgrade $true

# Vérifier les résolveurs DoH enregistrés
Get-DnsClientDohServerAddress

# Configurer l'interface réseau pour utiliser DoH
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "10.0.0.53"
```

Le paramètre `-AllowFallbackToUdp $false` est critique en entreprise : il empêche le client de basculer vers DNS classique non chiffré si DoH échoue. Le paramètre `-AutoUpgrade $true` configure Windows pour utiliser automatiquement DoH lorsque le serveur DNS assigné supporte DoH.

Configuration via GPO

Pour déployer DoH sur une flotte de postes Windows via Group Policy Object, naviguez vers :

`Computer Configuration > Administrative Templates > Network > DNS Client`

Les paramètres GPO pertinents sont :

Configure DNS over HTTPS (DoH) name resolution : Définit le comportement DoH (Désactivé, Autorisé, Obligatoire)

Configure DNS over HTTPS (DoH) server : Spécifie le template URL du résolveur DoH

Turn off smart multi-homed name resolution : Évite les fuites DNS sur d'autres interfaces

La politique GPO s'applique à tous les postes membres du domaine Active Directory dès le prochain rafraîchissement des stratégies de groupe (par défaut toutes les 90 minutes, ou forçable via `gpupdate /force`). Il est recommandé de tester le déploiement dans une OU pilote avant de le généraliser à toute la flotte.

Script PowerShell de déploiement DoH en flotte

```
 # Script de déploiement DoH - Flotte Windows 11 Entreprise
# A executer via GPO Startup Script ou SCCM/Intune

param(
    [string]$DohServerIP = "10.0.0.53",
    [string]$DohTemplate = "https://dns.interne.entreprise.fr/dns-query",
    [string]$NetworkAdapter = "Ethernet"
)

# Verifier que le serveur DoH interne est joignable
$pingResult = Test-NetConnection -ComputerName $DohServerIP -Port 443 -WarningAction SilentlyConti
if (-not $pingResult.TcpTestSucceeded) {
    Write-Error "Resolveur DoH interne $DohServerIP inaccessible sur port 443"
    exit 1
}

# Supprimer les anciens resolveurs DoH publics potentiellement enregistres
$existingDoh = Get-DnsClientDohServerAddress
foreach ($doh in $existingDoh) {
    if ($doh.ServerAddress -notin @($DohServerIP)) {
        Remove-DnsClientDohServerAddress -ServerAddress $doh.ServerAddress
        Write-Host "Resolveur DoH supprime : $($doh.ServerAddress)"
    }
}

# Enregistrer le resolveur DoH interne approuve
Add-DnsClientDohServerAddress `
    -ServerAddress $DohServerIP `
    -DohTemplate $DohTemplate `
    -AllowFallbackToUdp $false `
    -AutoUpgrade $true `
    -ErrorAction SilentlyContinue

# Configurer l'interface reseau
Set-DnsClientServerAddress `
    -InterfaceAlias $NetworkAdapter `
    -ServerAddresses $DohServerIP

Write-Host "DoH configure avec succes. Resolveur : $DohServerIP"
Write-Host "Template : $DohTemplate"

# Journaliser dans le journal d'evenements Windows
New-EventLog -LogName Application -Source "DNS-DoH-Deploy" -ErrorAction SilentlyContinue
Write-EventLog -LogName Application -Source "DNS-DoH-Deploy" -EventId 1001 `
```

```
    -EntryType Information `
    -Message "DoH configure vers $DohServerIP ($DohTemplate)"
```

Ce script vérifie la connectivité avant d'appliquer la configuration, supprime les résolveurs DoH publics préexistants et enregistre l'opération dans le journal d'événements Windows pour la traçabilité. Il peut être intégré dans SCCM/MECM comme package de déploiement ou dans Intune comme script PowerShell de remédiation.

Windows Server 2025 comme Résolveur DoH Interne

L'approche recommandée par Microsoft et l'ANSSI pour les entreprises est de déployer un résolveur DoH interne plutôt que de s'appuyer sur des résolveurs publics. Windows Server 2025 intègre cette fonctionnalité nativement dans son rôle DNS Server, sans nécessiter de logiciel tiers.

Activer DoH sur Windows DNS Server

```
 # Sur le serveur Windows Server 2025 hebergeant le role DNS
# Activer DoH sur le serveur DNS
Set-DnsServerDohServerConfiguration -Enable $true

# Recuperer l'empreinte du certificat TLS pour le resolveur DoH
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
    $_.Subject -like "*dns.interne.entreprise.fr*" -and
    $_.NotAfter -gt (Get-Date)
} | Sort-Object NotAfter -Descending | Select-Object -First 1

# Configurer le serveur DoH avec le certificat
Set-DnsServerDohServerConfiguration `
    -Enable $true `
    -CertificateThumbprint $cert.Thumbprint

# Verifier la configuration
Get-DnsServerDohServerConfiguration
```

Une fois activé, le serveur DNS Windows Server 2025 écoute les requêtes DoH sur le port 443/TCP en plus du port 53/UDP classique. Les clients Windows configurés pour utiliser ce résolveur en mode DoH enverront leurs requêtes DNS encapsulées dans des requêtes HTTPS vers `https://dns.interne.entreprise.fr/dns-query`.

Certificat TLS pour le résolveur DoH interne via ADCS

Le résolveur DoH interne doit présenter un certificat TLS valide reconnu par les clients. En environnement Active Directory, l'autorité de certification d'entreprise (ADCS — Active Directory Certificate Services) est idéale car ses certificats sont automatiquement approuvés par tous les postes membres du domaine.

```
 # Demander un certificat serveur Web aupres de l'ADCS
# Executer sur le serveur DNS ou depuis un poste d'administration PKI

# Methode 1 : Via Get-Certificate PowerShell PKI
Get-Certificate `
    -Template "WebServer" `
    -SubjectName "CN=dns.interne.entreprise.fr" `
    -DnsName "dns.interne.entreprise.fr","dns.entreprise.fr" `
    -CertStoreLocation "Cert:\LocalMachine\My" `
    -CertificateAuthority "NomServeurCA\NomCA"

# Methode 2 : Via certreq avec fichier .inf
# [NewRequest]
# Subject = "CN=dns.interne.entreprise.fr"
# KeySpec = 1
# KeyLength = 2048
# Exportable = False
# MachineKeySet = True
# RequestType = PKCS10
# [Extensions]
# 2.5.29.17 = "{text}dns=dns.interne.entreprise.fr&dns=dns.entreprise.fr"
```

Le certificat doit avoir une durée de validité d'au moins 1 an et être renouvelé avant expiration (configurer une alerte sur la date d'expiration). L'ADCS peut être configuré pour l'auto-enrollment, permettant le renouvellement automatique des certificats serveur. Pour les clients Windows, le certificat ADCS est distribué automatiquement via Group Policy.

Clients Windows pointant vers le résolveur DoH interne

Une fois le résolveur DoH interne opérationnel, les clients doivent être reconfigurés pour l'utiliser. La méthode recommandée en environnement Active Directory est la combinaison GPO + DHCP :

```
 # Option DHCP 6 : distribuer l'IP du resolveur DoH via DHCP
Set-DhcpServerv4OptionValue -ScopeId "192.168.1.0" -OptionId 6 -Value "10.0.0.53"

# Sur le client Windows 11, verifier la configuration DoH active
Resolve-DnsName "test.entreprise.fr" -Type A -Server "10.0.0.53"
Get-DnsClientDohServerAddress | Format-Table ServerAddress, DohTemplate, AutoUpgrade
```

Pour une couverture complète sur la sécurisation du DHCP en lien avec le DNS, consultez notre guide sur le DHCP sécurisé sous Windows Server 2025.

Contrôle du DoH en Entreprise : Politique de DNS

Le déploiement d'un résolveur DoH interne n'est pas suffisant si les postes peuvent toujours atteindre des résolveurs DoH publics. Une stratégie de gouvernance DNS complète implique plusieurs niveaux de contrôle complémentaires.

Bloquer les résolveurs DoH publics au firewall

Les résolveurs DoH publics les plus courants doivent être bloqués au niveau du firewall périmétrique. Voici les cibles prioritaires :

Cloudflare : 1.1.1.1, 1.0.0.1 — `https://cloudflare-dns.com/dns-query`, `https://1.1.1.1/dns-query`

Google : 8.8.8.8, 8.8.4.4 — `https://dns.google/dns-query`

Quad9 : 9.9.9.9 — `https://dns.quad9.net/dns-query`

AdGuard : 94.140.14.14 — `https://dns.adguard.com/dns-query`

OpenDNS : 208.67.222.222 — `https://doh.opendns.com/dns-query`

Le blocage doit cibler à la fois les adresses IP (pour les connexions directes) et les noms de domaine (nécessite un filtrage DNS préalable via le résolveur interne). Sur un firewall Next-Generation (Fortinet FortiGate, Palo Alto Networks, Check Point), créer une règle bloquant les connexions HTTPS vers ces IP sur le port 443/TCP depuis les postes internes.

Il faut également bloquer le port 53/UDP et 53/TCP sortant vers toutes les IP sauf le résolveur DNS interne, pour empêcher l'utilisation de DNS classique non chiffré vers des résolveurs externes. Cette mesure est indépendante du DoH mais complémentaire.

GPO pour forcer le résolveur DoH interne

```
 # Deploiement via GPO - Preferences de registre
# Chemin : Computer Configuration > Preferences > Windows Settings > Registry

# Forcer DoH obligatoire
# EnableAutoDoh : 0=Desactive, 1=Autorise, 2=Prefere, 3=Obligatoire
$regPath = "HKLM:\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters"
New-ItemProperty -Path $regPath `
    -Name "EnableAutoDoh" `
    -Value 3 `
    -PropertyType DWORD `
    -Force

# Configurer le template DoH pour le resolveur interne
$dohPath = "$regPath\DohWellknownServers\10.0.0.53"
New-Item -Path $dohPath -Force | Out-Null
New-ItemProperty -Path $dohPath `
    -Name "DohTemplate" `
    -Value "https://dns.interne.entreprise.fr/dns-query" `
    -PropertyType String `
    -Force

# Definir si le fallback UDP est autorise (0 = interdit, 1 = autorise)
New-ItemProperty -Path $dohPath `
    -Name "DohFlags" `
    -Value 0 `
    -PropertyType DWORD `
    -Force
```

Inspection DoH via proxy HTTPS transparent

Pour les entreprises disposant d'un proxy HTTPS avec inspection SSL (Break and Inspect), il est possible d'inspecter le trafic DoH vers les résolveurs publics non bloqués. Le proxy intercepte la session TLS, déchiffre la requête DoH, peut l'analyser ou la bloquer, puis la rechiffre vers le résolveur. Cette approche nécessite que les postes clients approuvent le certificat racine du proxy (déployé via GPO en environnement AD). Les solutions Squid avec ssl-bump, Bluecoat/ Symantec ProxySG ou Zscaler supportent cette fonctionnalité.

DoH et Sécurité : Avantages et Risques

DNS over HTTPS est souvent présenté comme une amélioration de la sécurité, et c'est vrai pour les utilisateurs individuels. En entreprise, le tableau est plus nuancé et nécessite une analyse approfondie des risques avant déploiement.

Avantages du DoH en entreprise

Confidentialité des requêtes DNS : Sur les réseaux WiFi publics (hôtels, aéroports, espaces de coworking), le DoH protège les collaborateurs en télétravail contre l'espionnage de leurs requêtes DNS par d'autres usagers du réseau

Protection contre le MITM DNS : Un attaquant intermédiaire ne peut pas falsifier les réponses DNS (combiné avec DNSSEC pour une protection complète)

Résistance au DNS spoofing : L'encapsulation TLS empêche l'injection de fausses réponses DNS dans le flux réseau

Protection des télétravailleurs : Les requêtes DNS des postes nomades ne sont plus exposées sur les réseaux non maîtrisés

Conformité réglementaire : Répond aux exigences NIS 2 et ANSSI sur la sécurité des résolutions de noms

Risques du DoH non contrôlé

Le DoH non gouverné représente un risque de sécurité significatif pour les entreprises. Ces risques sont documentés par des organismes comme l'ANSSI, l'ENISA et de nombreux éditeurs de sécurité :

Bypass DLP : Les outils de prévention des fuites de données basés sur le filtrage DNS (blocage des domaines de partage non autorisés) deviennent inefficaces face au DoH vers résolveurs publics

C2 over DoH : Des frameworks d'attaque comme Cobalt Strike, Sliver et des APT documentés (APT32, APT41) utilisent DoH vers des résolveurs publics pour faire communiquer leurs implants en contournant les systèmes de détection DNS

Exfiltration DNS chiffrée : L'exfiltration de données par encodage en sous-domaines DNS (technique classique) peut utiliser DoH pour chiffrer le canal d'exfiltration et éviter la détection

Perte de visibilité SIEM : Les corrélations basées sur les logs DNS deviennent incomplètes, affectant la qualité de la détection des menaces

Contournement des politiques de sécurité : Des applications malveillantes ou des utilisateurs mal intentionnés peuvent contourner les politiques de filtrage web basées sur le DNS

Détection du DoH non autorisé : JA3/JA4 Fingerprinting

Le blocage strict des résolveurs publics n'est pas toujours possible (partage de plages IP avec d'autres services légitimes, CDN, etc.). La détection devient alors essentielle. JA3 et son successeur JA4 permettent de fingerprinter les clients TLS sur la base des paramètres de la négociation TLS (cipher suites, extensions TLS, courbes elliptiques, compression). Les bibliothèques DoH courantes (go-doh, dnscrypt-proxy, Firefox DoH intégré) ont des signatures JA3/JA4 caractéristiques, différentes d'un navigateur web standard accédant à un site HTTPS ordinaire.

```
 # Exemple de regle Suricata pour detecter DoH suspect via JA3
# Adapter les hashes JA3 selon les clients DoH cibles dans votre environnement
alert tls any any -> any 443 (msg:"Possible DoH client suspect - JA3 connu";
    ja3.hash; content:"c7d38f8432b7bcd63a5699cd91ce0ac1";
    threshold: type threshold, track by_src, count 20, seconds 60;
    classtype:policy-violation; sid:9000001; rev:1;)

alert tls any any -> $KNOWN_DOH_PUBLIC_IPS 443 (msg:"Connexion DoH vers resolveur public";
    classtype:policy-violation; sid:9000002; rev:1;)
```

Intégration DoH avec DNSSEC

DoH et DNSSEC sont des protocoles complémentaires qui adressent des problèmes différents mais liés. DoH assure la **confidentialité** du transport DNS (les requêtes et réponses sont chiffrées et ne peuvent pas être observées par un tiers), tandis que DNSSEC assure l'**intégrité et l'authenticité** des réponses DNS (les réponses sont signées cryptographiquement et ne peuvent pas être falsifiées). Ensemble, ils constituent une défense en profondeur robuste contre les attaques DNS.

DoH + DNSSEC : double protection en pratique

Lorsqu'un client Windows 11 résout un nom via DoH vers un résolveur qui effectue la validation DNSSEC, la réponse inclut le bit AD (Authenticated Data) dans l'en-tête DNS. Ce bit indique que le résolveur a validé la chaîne de signatures DNSSEC jusqu'à la racine DNS. Le client peut être configuré pour ne traiter que les réponses avec le bit AD positionné pour les zones critiques.

```
 # Verifier la configuration DNSSEC du resolveur Windows Server
Get-DnsServerDnsSecSetting

# Activer la validation DNSSEC sur le resolveur Windows Server 2025
Set-DnsServerDnsSecSetting -DnsSecMode Auto

# Tester la validation DNSSEC depuis un client
# La reponse doit contenir "AD" (Authentic Data) pour les zones signees
Resolve-DnsName "www.gouvernement.fr" -Type A -DnssecOk | Format-List

# Configurer Windows pour signaler les echecs de validation DNSSEC
Set-DnsClientGlobalSetting -QueryAdapterSettings @{
    UseDnssecValidation = $true
}
```

Pour une couverture complète de la configuration DNSSEC sur Windows Server 2025, consultez notre guide dédié : DNSSEC sur Windows Server 2025 : configuration complète. Les deux protocoles sont conçus pour fonctionner ensemble, et leur déploiement conjoint est recommandé par l'ANSSI dans son guide de sécurisation des serveurs DNS (ANSSI-PA-079).

Le bit AD dans les réponses DoH : validation DNSSEC préservée

Un point important souvent négligé : la validation DNSSEC est effectuée par le **résolveur récursif**, pas par le client final. En mode DoH, le résolveur DoH interne Windows Server 2025 effectue la validation DNSSEC et transmet le résultat via le bit AD dans la réponse DoH. Le client n'a pas besoin de connaître les détails DNSSEC : il peut simplement faire confiance au résolveur interne pour la validation, grâce au chiffrement DoH qui protège l'intégrité du transport entre client et résolveur interne.

Monitoring du Trafic DoH en Entreprise

La supervision du trafic DoH est indispensable pour détecter les usages non autorisés, maintenir la visibilité sur la résolution de noms et alimenter correctement le SIEM d'entreprise avec des logs DNS complets.

Logs Windows DNS Server pour le trafic DoH

Windows Server 2025 DNS Server logue nativement les requêtes DoH reçues dans les mêmes journaux que les requêtes DNS classiques. Activer le logging analytique du DNS :

```
 # Activer le logging des requetes DNS (incluant DoH)
Set-DnsServerDiagnostics `
    -All $true `
    -EnableLoggingForLocalLookupEvent $true `
    -EnableLoggingForRecursiveLookupEvent $true `
    -EnableLoggingToFile $true `
    -LogFilePath "C:\DNS\dns.log" `
    -MaxMBFileSize 100

# Verifier que le logging est actif
Get-DnsServerDiagnostics | Select-Object *Logging*

# Filtrer les requetes DoH dans les evenements Windows
Get-WinEvent -LogName "Microsoft-Windows-DNSServer/Analytical" |
    Where-Object { $_.Message -like "*DoH*" -or $_.Message -like "*HTTPS*" } |
    Select-Object TimeCreated, Message |
    Format-List
```

Les logs DNS peuvent être forwarded vers le SIEM via Windows Event Forwarding (WEF) ou un agent Wazuh/Elastic Beats. Pour une vue complète des événements Windows à surveiller côté DNS et Active Directory, voir notre article sur l'audit des permissions DNS Active Directory et notre guide sur les événements Windows à surveiller sur le contrôleur de domaine.

Wazuh + Zeek pour l'analyse du trafic DNS/DoH

Zeek (anciennement Bro) analyse le trafic réseau en mode passif et peut identifier le trafic DoH en combinant plusieurs indicateurs : analyse du SNI TLS, de l'ALPN (Application-Layer Protocol Negotiation), des flux vers des IP connues de résolveurs DoH, et du fingerprinting JA3/JA4.

```
 # Script Zeek pour detecter DoH suspect
# /usr/local/share/zeek/site/doh-detect.zeek

@load base/frameworks/notice

module DoHDetect;

export {
    redef enum Notice::Type += { DoH_Detected };

    const known_doh_resolvers: set[string] = {
        "cloudflare-dns.com",
        "dns.google",
        "dns.quad9.net",
        "doh.opendns.com",
        "dns.adguard.com"
    } &redef;
}

event ssl_established(c: connection) {
    if (c$id$resp_p == 443/tcp && c$ssl?$server_name) {
        if (c$ssl$server_name in known_doh_resolvers) {
            NOTICE([$note=DoH_Detected,
                    $conn=c,
                    $msg=fmt("DoH vers resolveur public detecte : %s depuis %s",
                             c$ssl$server_name, c$id$orig_h),
                    $identifier=cat(c$id$orig_h, c$ssl$server_name)]);
        }
    }
}
```

Les alertes Zeek sont intégrées dans Wazuh via le module d'intégration Zeek (`/var/ossec/etc/ossec.conf`), permettant de créer des règles de corrélation qui génèrent des alertes de sécurité de niveau élevé lorsque des requêtes DoH vers des résolveurs non autorisés sont détectées depuis des postes du parc informatique.

DoH et Conformité NIS 2 en France

La directive NIS 2 (Network and Information Security 2), transposée en France par la loi n°2024-1186 du 17 décembre 2024, impose des obligations de sécurité renforcées aux entreprises des secteurs essentiels (énergie, transport, santé, eau) et importants (services postaux, gestion des déchets, fabrication, distribution alimentaire, numérique). DNS over HTTPS s'inscrit directement dans plusieurs exigences de cette directive.

NIS 2 Article 21§2.d : Authenticité et intégrité DNS

L'article 21§2.d de NIS 2 impose des mesures pour assurer l'authenticité et l'intégrité des données et des configurations nécessaires à la continuité de service. Le DNS est une infrastructure critique dont la compromission peut entraîner une interruption complète des services numériques d'une organisation. DoH, combiné à DNSSEC, contribue directement à satisfaire cette exigence en protégeant :

La confidentialité des requêtes DNS (évite la reconnaissance du système d'information par un attaquant réseau)

L'intégrité des réponses DNS (DNSSEC empêche l'empoisonnement DNS)

La disponibilité de la résolution de noms (résolveur DoH interne redondant)

Les entreprises soumises à NIS 2 doivent documenter leurs mesures de sécurité DNS dans leur politique de sécurité des systèmes d'information (PSSI) et être en mesure de les justifier lors d'un audit par l'ANSSI ou un organisme de certification reconnu.

Recommandations ANSSI sur DNS over TLS/HTTPS

L'Agence Nationale de la Sécurité des Systèmes d'Information recommande dans son guide « Sécurisation des architectures DNS » le déploiement de DNS chiffré (DoT ou DoH) pour les résolveurs exposés sur Internet ou dans des zones non maîtrisées. Pour les entreprises françaises, les grandes lignes des recommandations ANSSI en matière de DNS chiffré sont :

Déployer un résolveur DNS interne supportant DoH ou DoT pour les postes nomades et télétravailleurs

Forcer le chiffrement DNS pour toutes les communications DNS sortant du périmètre maîtrisé

Bloquer l'accès direct aux résolveurs publics depuis le réseau interne pour maintenir la visibilité DNS

Combiner DoH et DNSSEC pour une protection maximale (confidentialité + intégrité)

Journaliser et superviser les requêtes DNS dans le cadre du SOC ou de la supervision sécurité

CNIL : traitement des logs DNS comme données personnelles

Les logs DNS contiennent des données à caractère personnel au sens du RGPD : ils permettent de reconstituer les sites et services consultés par chaque collaborateur, identifié par son adresse IP interne ou son nom d'hôte. La CNIL rappelle que ces logs doivent être traités dans le respect du RGPD, avec les précautions suivantes :

Base légale : Intérêt légitime de l'employeur (sécurité du SI, conformité NIS 2) ou obligation légale

Durée de conservation : Limitée au nécessaire pour l'objectif de sécurité (recommandation : 6 mois maximum pour les logs DNS bruts)

Information des salariés : Via la charte informatique et le registre des traitements (article 30 RGPD)

Accès restreint : Seul le personnel de sécurité (RSSI, SOC) peut accéder aux logs DNS individuels dans le cadre de leur mission

Analyse en masse : Préférer l'analyse agrégée ou pseudonymisée pour la supervision quotidienne

La mise en place d'un résolveur DoH interne augmente le volume de logs DNS collectés — les requêtes qui passaient par des résolveurs publics (et donc invisibles) deviennent maintenant visibles et loguées. Une analyse juridique préalable avec le DPO (Délégué à la Protection des Données) est recommandée avant tout déploiement à grande échelle.

Questions fréquentes sur DNS over HTTPS en entreprise

DoH est-il compatible avec le filtrage DNS d'entreprise ?

Oui, à condition d'utiliser un résolveur DoH interne qui applique les mêmes politiques de filtrage que le résolveur DNS classique. Les solutions comme Windows Server 2025 DNS, Infoblox ou BlueCat supportent DoH tout en maintenant le filtrage par DNS Response Policy Zones (RPZ). Le DoH vers des résolveurs publics est incompatible avec le filtrage DNS d'entreprise et doit être bloqué au firewall.

Windows 11 active-t-il DoH automatiquement ?

Depuis Windows 11 22H2, Windows peut activer DoH automatiquement (AutoUpgrade) si le serveur DNS configuré sur l'interface réseau est reconnu comme supportant DoH et figure dans la liste des résolveurs DoH approuvés par Microsoft. Ce comportement est contrôlable via GPO. Un résolveur interne non référencé par Microsoft ne déclenchera pas l'AutoUpgrade sans configuration explicite via PowerShell ou registre.

Peut-on détecter le DoH sur le réseau sans proxy d'inspection SSL ?

Oui, partiellement. Sans déchiffrement SSL, on peut détecter le DoH via l'analyse du SNI (Server Name Indication) dans la négociation TLS, le JA3/JA4 fingerprinting du client TLS, et les flux vers des adresses IP connues de résolveurs DoH publics. Des outils comme Zeek permettent cette détection passive sans déchiffrement. La détection est plus difficile pour les résolveurs DoH hébergés sur des CDN partagés.

DoH fonctionne-t-il avec Active Directory et Kerberos ?

Oui, sous réserve que le résolveur DoH interne resolve correctement les enregistrements SRV (_kerberos._tcp.domaine.local, _ldap._tcp.dc._msdcs.domaine.local, etc.) utilisés par Active Directory. Le résolveur DoH interne Windows Server 2025 est authoritative pour les zones AD internes et résout tous les enregistrements AD requis. Kerberos lui-même ne dépend pas du

protocole utilisé pour la résolution DNS, seulement de la qualité et de la complétude des réponses.

Quelle est la différence entre DoH et ESNI/ECH pour la confidentialité ?

DoH protège la confidentialité des requêtes DNS (quels noms sont résolus), tandis qu'ESNI (Encrypted SNI) et son successeur ECH (Encrypted Client Hello, RFC 9001) protègent le SNI dans la négociation TLS (vers quel serveur on se connecte réellement). Ces deux technologies sont complémentaires : un attaquant réseau peut voir le SNI même si DoH est utilisé, et inversement. La combinaison DoH + ECH offre une confidentialité maximale des communications depuis un poste Windows.

À RETENIR

À retenir

Windows Server 2025 peut servir de résolveur DoH interne via `Set-DnsServerDohServerConfiguration`, permettant de conserver la visibilité et le filtrage DNS tout en chiffrant le transport entre clients et résolveur.

Bloquer impérativement les résolveurs DoH publics (Cloudflare 1.1.1.1, Google 8.8.8.8) au firewall périmétrique pour éviter le contournement des politiques DNS d'entreprise.

Déployer DoH via GPO sur toute la flotte Windows 11 (`Computer Configuration > Administrative Templates > Network > DNS Client`) en pointant vers le résolveur interne approuvé muni d'un certificat ADCS.

Combiner DoH avec DNSSEC pour une double protection : confidentialité du transport (DoH) et intégrité des réponses DNS (DNSSEC), conformément aux recommandations ANSSI pour les entreprises soumises à NIS 2.

Les logs DNS d'un résolveur DoH interne constituent des données personnelles soumises au RGPD : informer les salariés via la charte informatique, limiter la conservation à 6 mois maximum et restreindre l'accès au RSSI et au SOC.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité