

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Objectif : Changer votre serveur DNS pour naviguer de manière plus privée, plus rapide et protégée contre les sites malveillants.

Remarque : Cette nouvelle version de la fiche N°6 est largement augmentée grâce au contenu de la Newsletter Crowdbunker publiée par Matthieu le 19 juin 2026 : *Comment contourner la surveillance (partie 2) : le DNS, l'annuaire secret qui peut censurer Internet.*

Un grand Merci à Matthieu pour ces compléments très utiles.

Les points qui n'avaient pas été traités initialement ont été regroupés dans la section intitulée « **Aller plus loin** »

- **Public visé :** Débutant à Intermédiaire
- **Temps estimé :** 5 à 15 minutes
- **Niveau de difficulté :** ★★☆☆☆ (Facile)

1. Pourquoi changer son serveur DNS ? (Le problème)

Problème	Solution apportée par un DNS privé
Votre FAI enregistre tous les sites que vous visitez	Cloudflare, Quad9 et Mullvad s'engagent à ne pas conserver vos données personnelles
Le DNS de votre FAI est souvent lent et mal optimisé	Cloudflare (1.1.1.1) est l'un des plus rapides au monde
Certains FAI bloquent ou censurent des sites	Cloudflare, Quad9 et Mullvad ne censurent pas (sauf option famille)
Vous êtes exposé aux sites de phishing et malwares	Quad9 bloque automatiquement les sites dangereux
Le DNS par défaut n'est pas chiffré	DNS over HTTPS (DoH) ou DNS over TLS (DoT) chiffrent vos requêtes
Vous voulez bloquer publicités, traqueurs et contenus adultes	NextDNS permet une configuration personnalisée

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Le bénéfice : Navigation plus rapide, plus privée (votre FAI ne voit plus les sites que vous visitez), et protégée contre les sites dangereux.

2. Ce que vos requêtes DNS disent de vous

Avant même de parler d'outils, il faut comprendre ce que vous protégez.

Rien qu'avec vos requêtes DNS, un observateur (votre FAI, un réseau public, un intermédiaire) peut reconstituer :

- Les **sites que vous consultez** (même sans voir la page exacte)
- Les **applications que vous ouvrez** (elles "appellent" des domaines reconnaissables)
- Les **services qui tournent en arrière-plan** sur vos appareils
- Vos **horaires et vos habitudes** : à quelle heure vous vous levez, quand vous travaillez, quand vous dormez
- Les **appareils de votre foyer** (la télé connectée, la console, le téléphone des enfants...)
- Vos **centres d'intérêt sensibles** : santé, opinions politiques, croyances, situation financière...

Nuance importante : Le DNS ne voit pas forcément l'adresse complète d'une page (ex: /article/dossier-secret). Mais il voit `site-tres-sensible.com` — et la plupart du temps, ça suffit largement à savoir ce que vous faites.

Et si votre DNS est réglé sur votre box internet (le cas par défaut chez la majorité des gens), c'est tout le foyer qui est lisible d'un seul coup d'œil.

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

3. "Mais j'ai HTTPS, le petit cadenas... je suis protégé, non ?"

C'est l'une des confusions les plus répandues. Clarifions-la une bonne fois :

- **HTTPS** (le petit cadenas) **chiffre le contenu** de la page : ce que vous lisez, ce que vous tapez, vos mots de passe.
- Mais **HTTPS ne chiffre pas automatiquement la question DNS**. Sans DNS chiffré, quelqu'un sur le trajet (votre FAI, le Wi-Fi d'un hôtel, un réseau public...) peut ne pas voir ce que vous lisez exactement, mais peut très bien voir **quels domaines vous essayez de joindre**.

La bonne image à retenir :

HTTPS cache la conversation que vous avez à l'intérieur de la maison.
Mais sans DNS chiffré, tout le monde dans la rue peut voir devant quelle porte vous vous êtes arrêté.

C'est pour ça que "chiffrer le DNS" est l'une des améliorations de vie privée les plus rentables, et l'une des plus simples à mettre en place.

4. Les solutions DNS recommandées

4.1 Pour débutants : Cloudflare, Quad9 ou Mullvad DNS

Solution	Adresse IP principale	Adresse IP secondaire	Pourquoi la choisir ?
Cloudflare (1.1.1.1)	1.1.1.1	1.0.0.1	Ultra-rapide, logs supprimés en 24h, chiffrement DNS par défaut

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Solution	Adresse IP principale	Adresse IP secondaire	Pourquoi la choisir ?
Quad9 (9.9.9.9)	9.9.9.9	149.112.112.112	Bloque les sites de phishing et malwares, fondation suisse à but non lucratif, pas de logs IP
Mullvad DNS	Voir site	Voir site	DNS public chiffré, pas besoin d'être client VPN, politique de confidentialité exemplaire

4.2 Options famille (filtrage de contenu)

Solution	Adresse IP	Blocage
Cloudflare famille	1.1.1.3 / 1.0.0.3	Bloque les contenus malveillants et adultes
Quad9 famille	9.9.9.11	Bloque les malwares + contenus litigieux

4.3 Solution avancée : NextDNS (recommandé pour le contrôle total)

NextDNS est un service DNS moderne qui permet une configuration ultra-personnalisable.

Caractéristique Détail

Modèle	Gratuit (300 000 requêtes/mois) puis payant (1,99 \$/mois illimité)
Blocage intégré	Publicités, traqueurs, malwares, sites adultes, réseaux sociaux, etc.
Personnalisation	Listes noires/blanches, profils multiples, logs consultables
Chiffrement	DNS over HTTPS (DoH), DNS over TLS (DoT)
Configuration	Via application, navigateur (DoH), ou routeur

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Pourquoi choisir NextDNS ? Si vous en avez assez des publicités sur tous vos appareils, NextDNS les bloque au niveau du réseau, sans rien installer. Une seule configuration sur votre box protège tout le foyer.

5. Comment faire ? (Le pas à pas)

5.1 Méthode A : Changer le DNS sur votre ordinateur

Sur Windows 11

1. Paramètres → Réseau et Internet → (votre connexion) → Modifier l'attribution du serveur DNS
2. Passez en **Manuel**, activez IPv4 (et IPv6 si vous l'utilisez)
3. Entrez les adresses de votre résolveur
4. Réglez le chiffrement DNS sur "**Chiffré uniquement (DNS over HTTPS)**" quand l'option apparaît
5. N'oubliez pas IPv6 : c'est l'erreur n°1 (voir plus bas)

Sur macOS

Le réglage DNS de base (Réglages → Réseau → DNS) n'active pas le chiffrement. Le plus fiable : un profil de configuration DNS chiffré ou l'application de votre résolveur (Mullvad, NextDNS, Cloudflare WARP...).

Sur Linux Mint / Ubuntu

Via l'interface graphique :

1. Menu → Paramètres → Réseau

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

2. Sélectionnez votre connexion → cliquez sur l'icône engrenage
3. Onglet **Paramètres IPv4** → changez la méthode "Automatique (DHCP)" en **"Automatique (DHCP) uniquement des adresses"**
4. Dans le champ "Serveurs DNS", entrez : 1.1.1.1, 1.0.0.1 ou 9.9.9.9, 149.112.112.112
5. Cliquez sur **Enregistrer**

⚠ **Important** : sur Linux, le DNS est souvent géré par NetworkManager. Après modification, redémarrez NetworkManager ou votre connexion.

5.2 Méthode B : Changer le DNS sur votre box (recommandé pour tout le foyer)

Si vous changez le DNS directement sur votre box (routeur), tous les appareils de votre maison seront protégés en une seule manipulation.

Étapes générales :

1. Connectez-vous à l'interface d'administration de votre box (généralement 192.168.1.1 ou 192.168.0.1)
2. Cherchez une section nommée "Réseau", "Paramètres Internet", "DNS" ou "DHCP"
3. Changez les DNS en mode manuel (ou "statique")
4. Entrez les adresses de Cloudflare, Quad9 ou NextDNS
5. Sauvegardez et redémarrez la box

FAI	Interface Administrateur
Orange / Sosh	192.168.1.1 ou http://livebox
SFR / RED by SFR	192.168.1.1, 192.168.0.1 ou http://monmodem
Free	http://mafreebox.freebox.fr (ou IP 192.168.0.254)
Bouygues Telecom	192.168.1.254 ou https://mabbox.bytel.fr

⚠ **Limites selon les box :**

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

FAI Possibilité de modifier les DNS

Free	✓ Oui (via Freebox OS)
Bouygues	✓ Oui (sur les modèles récents)
SFR	⚠ Oui, mais pas sur les box les plus récentes (Box 7 fibre, Box 8)
Orange	✗ Non (Livebox récentes bloquent la modification)

Si la modification sur votre box n'est pas possible, configurez les DNS manuellement sur chaque appareil.

5.3 Méthode C : Configuration sur vos mobiles (Android et iOS)

La configuration sur un mobile est cruciale car vous naviguez via le Wi-Fi **et** les données mobiles.

Sur Android (9 et +)

- 1.Paramètres → Réseau et Internet → DNS privé
- 2.Choisissez "**Nom d'hôte du fournisseur DNS privé**"
- 3.Entrez le hostname de votre résolveur

Sur iOS (14 et +)

- 1.Réglages → Général → VPN et gestion de l'appareil → DNS privé
- 2.Activez le DNS privé
- 3.Choisissez **Manuel** et ajoutez un serveur
- 4.Entrez le hostname de votre résolveur

Noms d'hôte à utiliser :

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Service	Nom d'hôte	Fonction
Quad9	dns.quad9.net	Bloque les malwares
Cloudflare	one.one.one.one	Rapide, sans blocage
Cloudflare (malware)	security.cloudflare-dns.com	Bloque les malwares
Cloudflare (famille)	family.cloudflare-dns.com	Bloque malwares + adultes
NextDNS	votre-identifiant.dns.nextdns.io	Configuration personnalisée
Mullvad	adblock.dns.mullvad.net	Bloque pubs et traqueurs

À savoir : Le DNS Privé protège à la fois en Wi-Fi et en 4G/5G. C'est la méthode la plus efficace pour les mobiles.

5.4 Méthode D : Dans le navigateur (Firefox, Brave, Chrome)

- **Firefox** : Paramètres → Vie privée et sécurité → DNS via HTTPS
- **Brave / Chrome / Edge** : Paramètres → Confidentialité/Sécurité → Utiliser un DNS sécurisé

⚠ Piège fréquent : si vous activez un DNS dans le navigateur ET un autre au niveau du système, le navigateur peut imposer le sien. Choisissez votre stratégie et restez cohérent.

6. Vérifier que ça marche vraiment (la mini-checklist)

Changer un réglage, c'est bien. Vérifier qu'il est appliqué, c'est indispensable.

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Le test simple :

1. Ouvrez votre navigateur et allez sur dnsleaktest.com (ou ipleak.net)

2. Cliquez sur **"Extended test"** (test étendu)

3. Le site affiche la liste des résolveurs DNS qui ont traité vos requêtes

4. Lisez le nom qui apparaît :

- ☒ S'il indique votre résolveur choisi (Mullvad, Quad9, Cloudflare, NextDNS...) → **c'est gagné**
- ☒ S'il affiche le nom de votre FAI (Orange, SFR, Free, Bouygues...) → **votre réglage n'est pas pris en compte**

La checklist complète :

- ☒ Mon DNS est-il bien celui que j'ai choisi, et pas celui de mon FAI ?
- ☒ Mes requêtes passent-elles chiffrées (et non en clair) ?
- ☒ Si j'utilise un VPN, laisse-t-il fuiter mon DNS vers mon FAI ?
- ☒ L'IPv6 part-il par un autre résolveur que celui que j'ai configuré ?
- ☒ Mon navigateur utilise-t-il un DNS différent de celui du système ?
- ☒ Mon téléphone utilise-t-il le même DNS en Wi-Fi et en 4G/5G ?

Faites le test chez vous, mais aussi sur un Wi-Fi public : c'est là que la protection compte le plus.

7. Les erreurs fréquentes (ne tombez pas dedans)

- ☒ Changer seulement l'IPv4 et oublier l'IPv6 (qui continue alors de fuiter)
- ☒ Croire que 1.1.1.1 = anonymat (non : c'est juste un bon résolveur)
- ☒ Croire que DNS chiffré = VPN (non : ça ne masque pas votre adresse IP au site)
- ☒ Croire qu'un VPN garantit zéro fuite DNS (à vérifier systématiquement)
- ☒ Activer un DNS filtrant sans jamais lire ce qu'il bloque

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

- ❌ Activer le DNS sécurisé dans le navigateur tout en croyant utiliser celui du VPN
- ❌ Utiliser le DNS de Google par réflexe
- ❌ Installer cinq outils qui se contredisent
- ❌ Laisser les logs activés dans NextDNS
- ❌ Ne jamais tester après avoir configuré
- ❌ Utiliser le DNS de son FAI sur un réseau hostile (Wi-Fi public, etc.)

8. Tableau comparatif des solutions DNS

Critère	Cloudflare (1.1.1.1)	Quad9 (9.9.9.9)	Mullvad DNS	NextDNS
Gratuit	✅ Oui	✅ Oui	✅ Oui	300k req/mois
Rapide	Très rapide	Rapide	Rapide	Très rapide
Confidentialité	Logs supprimés en 24h	Pas de logs IP	Pas de logs	Logs optionnels
Blocage malwares	✅ Oui	✅ Oui	❌ Non	✅ Oui
Blocage publicités	❌ Non	❌ Non	✅ Oui	✅ Oui
Blocage adultes	✅ Option famille	✅ Option famille	❌ Non	✅ Optionnel
Filtrage personnalisé	❌ Non	❌ Non	❌ Non	✅ Oui
Juridiction	USA	Suisse	Suède	Europe
Idéal pour	Vitesse et simplicité	Sécurité antimalware	Vie privée maximale	Contrôle total + blocage

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

9. ALLER PLUS LOIN

Cette section s'adresse à ceux qui veulent comprendre l'architecture du contrôle DNS et aller au-delà du simple changement de résolveur.

9.1 Les protocoles : DNS classique, DoT, DoH, DoQ, ODoH

Tous les "DNS chiffrés" ne se valent pas.

Protocole	Description	Force	Limite
DNS classique (port 53)	Non chiffré	Compatible universel	Facile à observer, bloquer, détourner
DoT (DNS over TLS)	Chiffré dans TLS, port 853	Standardisé (RFC 7858)	Port identifiable, facile à bloquer
DoH (DNS over HTTPS)	Chiffré dans HTTPS, port 443	Se fond dans le trafic web, difficile à bloquer	Souvent configuré uniquement dans le navigateur
DoQ (DNS over QUIC)	Chiffré via QUIC	Latence améliorée	Encore peu déployé
ODoH	Proxy chiffré entre vous et le résolveur	Proxy connaît votre IP, résolveur connaît votre question, aucun ne voit tout	Encore expérimental

9.2 DNSSEC, QNAME minimization, ECH

Trois mécanismes peu connus qui changent beaucoup de choses :

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Mécanisme	Fonction	Ce qu'il apporte
DNSSEC	Vérifie que la réponse DNS est authentique	Intégrité (la réponse n'a pas été falsifiée)
QNAME minimization	N'envoie à chaque serveur que le strict nécessaire	Réduit ce que les serveurs amont apprennent de vous
ECH (Encrypted Client Hello)	Chiffre le SNI du handshake TLS	Masque le domaine visité même avec HTTPS
Important : DNSSEC ≠ confidentialité. DNSSEC authentifie, il ne chiffre pas. ECH est le complément indispensable au DNS chiffré.		

9.3 Comment le DNS sert à censurer

Le DNS est l'outil de censure le plus utilisé au monde, parce qu'il est simple et peu coûteux à actionner :

Méthode	Description
"Ce domaine n'existe pas" (NXDOMAIN)	Le résolveur ment et prétend que le site n'existe pas
Réponse vide ou refusée	Le résolveur renvoie une erreur ou ne répond jamais
Redirection	Vous êtes envoyé vers une page d'avertissement
Sinkhole	Redirection vers une adresse contrôlée qui observe les tentatives d'accès
Filtrage par catégories	Malware, contenu adulte, "désinformation", contenus politiques
Blocage dynamique	Des listes de domaines bloqués sont mises à jour en quasi temps réel

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

En France, l'Arcom a déjà fait bloquer des centaines de domaines, et a publié des modèles d'accords visant explicitement les résolveurs DNS et les VPN comme intermédiaires techniques à enrôler dans la censure.

Enseignement : un outil créé "contre le piratage" devient vite une infrastructure de contrôle généralisée.

9.4 Pourquoi "changer de DNS" ne suffit plus toujours

Changer de DNS est une brique, pas une armure complète.

Changer de DNS peut :

-  Contourner un blocage DNS basique (le plus courant)
-  Empêcher votre FAI de lire directement vos requêtes DNS
-  Améliorer la sécurité contre phishing et malware
-  Éviter certains détournements DNS

Mais changer de DNS ne protège pas contre :

-  Le blocage par IP (on bloque l'adresse du serveur, pas le nom)
-  Le blocage par SNI (sans ECH)
-  Le DPI (Deep Packet Inspection)
-  Le blocage au niveau du registrar ou du registre (.fr, .com...)
-  La suppression pure et simple du domaine
-  Les logs du résolveur que vous avez choisi
-  Une obligation légale imposée à ce résolveur

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

9.5 DNS, VPN, Tor — qui voit quoi ?

Configuration	Votre FAI voit	Le résolveur voit	Le site visité voit
DNS seul (non chiffré)	Vos requêtes DNS	Vos requêtes DNS	Votre IP réelle
DNS chiffré seul	Que vous faites du DNS	Vos requêtes DNS	Votre IP réelle
VPN seul	Que vous êtes sur un VPN	Les requêtes du VPN	L'IP du VPN
DNS chiffré + VPN	Que vous êtes sur un VPN	Les requêtes du VPN	L'IP du VPN
Tor	Que vous utilisez Tor	Aucun acteur unique ne voit tout	L'IP de sortie Tor

9.6 Le cas italien : Piracy Shield, ou comment un outil "anti-piratage" devient une infrastructure de contrôle

L'Italie a déployé **Piracy Shield**, un système où des noms de domaine et des adresses IP peuvent être transmis pour blocage en **30 minutes**.

Les enseignements :

- La censure technique déborde presque toujours son objectif initial
- Les blocages automatisés font des dégâts collatéraux massifs
- Un outil créé "contre le piratage" devient vite une infrastructure de contrôle généralisée

C'est exactement le scénario qu'on voit se dessiner à l'échelle européenne.

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

9.7 Recommandations selon votre profil

Profil	Recommandation DNS
Profil 1 — Vie privée simple	Mullvad DNS ou Quad9, activé au niveau du système. Test de fuite DNS. C'est tout.
Profil 2 — Famille	NextDNS filtré. Créez un profil enfant séparé. Réduisez les logs au minimum.
Profil 3 — Contourner un blocage	1. Changez de DNS. 2. Activez DoH/DoT. 3. Testez plusieurs résolveurs. 4. Si ça ne suffit pas : VPN.
Profil 4 — Journaliste / militant	DNS chiffré + VPN sérieux (Mullvad). Vérification systématique des fuites. Navigateur durci. ECH si disponible. Pas de comptes personnels dans l'environnement "anonyme".
Profil 5 — Utilisateur avancé / auto-hébergement	Unbound local + DNSSEC + QNAME minimization. Pi-hole ou AdGuard Home pour le filtrage réseau.

9.8 Aller encore plus loin : auto-hébergement

Pour les utilisateurs avancés :

- **Unbound** : serveur DNS récursif local, avec DNSSEC activé et QNAME minimization, puis forward vers un résolveur DoT/DoH fiable
- **Pi-hole** ou **AdGuard Home** : sur un Raspberry Pi ou un petit serveur, pour bloquer pubs et traqueurs à l'échelle du réseau

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

10. Challenge 7 jours

Challenge : Pendant 7 jours, utilisez un DNS privé (Mullvad, Quad9 ou NextDNS) sur tous vos appareils.

Jour	Action
Jour 1	Configurez NextDNS/Cloudflare/Quad9 sur votre ordinateur
Jour 2	Configurez sur votre box (routeur) pour protéger tout le foyer
Jour 3	Configurez le DNS Privé sur votre mobile Android ou iOS
Jour 4	Vérifiez sur test.nextdns.io que la protection fonctionne sur tous vos appareils
Jour 5	Vérifiez que ça fonctionne aussi en 4G/5G sur votre mobile
Jour 6	Consultez les statistiques NextDNS pour voir combien de requêtes ont été bloquées
Jour 7	Naviguez normalement et observez la différence

Vous allez constater :

- Moins de publicités (avec NextDNS ou Mullvad)
- Une navigation plus rapide
- Votre FAI ne voit plus les sites que vous visitez
- Les sites de phishing sont bloqués

11. En résumé – ce que vous gagnez

Action	Gagné
Changer le DNS de votre FAI pour Cloudflare (1.1.1.1)	Navigation plus rapide, meilleure confidentialité, gratuit
Changer pour Quad9 (9.9.9.9)	Protection contre les sites de phishing et malwares,

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

Action	Gagné
	pas de logs
Changer pour Mullvad DNS	DNS public chiffré, pas de logs, pas besoin d'être client VPN
Changer pour NextDNS	Blocage des publicités et traqueurs sur tout le réseau, logs optionnels
Changer sur votre box	Tous les appareils du foyer protégés en une manipulation
Activer DNS over HTTPS (Firefox)	Requêtes DNS chiffrées, invisibles pour votre FAI
Configurer le DNS Privé sur votre mobile	Protection sur le Wi-Fi ET les données mobiles

12. Conclusion

Si vous voulez...	Choisissez...
Simple, rapide, sans prise de tête	Cloudflare (1.1.1.1)
Protection contre les sites dangereux	Quad9 (9.9.9.9)
Vie privée maximale, pas de logs	Mullvad DNS
Contrôle total + blocage des publicités	NextDNS
Protection pour toute la famille	NextDNS configuré sur la box + blocage adulte activé

À retenir absolument :

1. Les DNS par défaut de votre FAI sont lents et vous espionnent. Changez-les.
2. HTTPS cache la conversation, pas la porte à laquelle vous frappez.

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.0

3.Cloudflare, Quad9, Mullvad et NextDNS sont gratuits, simples et respectueux de votre vie privée.

4.Une fois configuré sur votre box, vous n'avez plus rien à faire.

5.N'oubliez pas vos mobiles : configurez le DNS Privé pour une protection totale.

6.Testez toujours après configuration.

Test final :

-  Configurez votre nouveau DNS sur votre ordinateur
-  Vérifiez sur dnsleaktest.com que ça fonctionne
-  Configurez le DNS Privé sur votre mobile
-  Vérifiez sur test.nextdns.io que ça fonctionne aussi en 4G/5G
-  Naviguez normalement pendant une semaine
-  Si tout fonctionne, configurez-le sur votre box pour protéger tout le foyer