Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

7 nov, 2026 · @Gabriel

Objectif : *Changer votre serveur DNS pour naviguer de manière plus privée, plus rapide et protégée contre les sites malveillants, en privilégiant des résolveurs européens ou suisses.*

Remarque : *cette fiche a été largement augmentée grâce à 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 sont regroupés dans la section « Aller plus loin ».*

⚠️ ***Changement important (novembre 2026) :*** *Mullvad a fermé son service DNS public chiffré le 2 novembre 2026 et soutient désormais Quad9. Si vous aviez configuré dns.mullvad.net, adblock.dns.mullvad.net ou un profil Mullvad, remplacez-les par Quad9 (ou par DNS4EU avec blocage des publicités). Le VPN Mullvad, lui, continue de fonctionner avec son propre DNS.*

- ***Public visé :*** *Débutant à Intermédiaire*
- ***Temps estimé :*** *5 à 15 minutes*
- ***Difficulté :*** *★★☆☆☆ (Facile)*
- ***Prérequis :*** *accès aux réglages réseau de vos appareils (et de votre box, si possible)*
- ***Fiches associées :*** *N°3 (YouTube), N°5 (Mullvad), N°20c (AdGuard Home), N°38 (Pi-hole), N°44 (limites du VPN)*

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

Problème	Solution apportée par un DNS privé
Votre FAI enregistre tous les sites que vous visitez	Un résolveur respectueux (Quad9, DNS4EU) s'engage à ne pas exploiter vos requêtes ; avec le DNS chiffré, votre FAI ne les lit plus
Le DNS de votre FAI est parfois lent	Les résolveurs publics sont généralement rapides
Certains FAI bloquent ou censurent des sites	Les résolveurs publics ne bloquent pas par défaut (hors options anti-malware, famille ou publicité), mais une décision de justice peut aussi les contraindre (voir § 9.3)
Vous êtes exposé aux sites d'hameçonnage et aux logiciels malveillants	Quad9 et DNS4EU (option « Protective ») bloquent 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 pour adultes	DNS4EU propose des options « blocage publicitaire » et « protection des enfants » ; NextDNS permet une configuration personnalisée

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

Le bénéfice : une navigation plus privée (votre FAI ne voit plus les sites que vous visitez si le DNS est chiffré), protégée contre les sites dangereux, et des requêtes traitées en Europe ou en Suisse plutôt qu'aux États-Unis.

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 (télévision connectée, console, 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 (par exemple /article/dossier-secret). Mais il voit site-tres-sensible.com, et la plupart du temps cela suffit à savoir ce que vous faites.

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

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

C'est l'une des confusions les plus répandues :

- **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 la question DNS.** Sans DNS chiffré, quelqu'un sur le trajet (votre FAI, le Wi-Fi d'un hôtel, un réseau public…) ne voit pas ce que vous lisez, mais voit très bien 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 pourquoi chiffrer le DNS est l'une des améliorations de vie privée les plus rentables, et l'une des plus simples à mettre en place.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

4. Les solutions DNS recommandées

4.1. Pour débutants : Quad9 ou DNS4EU

Solution	Adresse IP principale	Adresse IP secondaire	Pourquoi la choisir ?
Quad9	`9.9.9.9`	`149.112.112.112`	Fondation suisse à but non lucratif ; bloque l'hameçonnage et les logiciels malveillants ; n'enregistre pas votre adresse IP ; DoH/DoT disponibles
DNS4EU « Protective »	`86.54.11.1`	IPv6 : `2a13:1001::86:54:11:1`	Résolveur public européen cofinancé par l'UE (consortium mené par Whalebone, Tchéquie) ; résolution dans l'UE, conforme au RGPD ; bloque les sites malveillants
Quad9 sans filtrage	`9.9.9.10`	`149.112.112.10`	Sans blocage des logiciels malveillants : réservé aux utilisateurs avertis
DNS4EU sans filtrage	`86.54.11.100`	IPv6 : `2a13:1001::86:54:11:100`	Résolution sans aucun blocage

Et Cloudflare (1.1.1.1) ? C'est un résolveur très rapide, qui s'engage à effacer ses journaux sous 25 heures. Mais Cloudflare est une **entreprise américaine soumise au Cloud Act** : dans l'esprit de ce guide, préférez Quad9 ou DNS4EU. Cloudflare reste préférable au DNS de Google ou à celui de votre FAI sur un réseau public.

4.2. Option famille et blocage des publicités

Solution	Adresse IPv4	Blocage
DNS4EU « Protective + Child Protection »	`86.54.11.12`	Sites malveillants + contenus pour adultes
DNS4EU « Protective + Ad Blocking »	`86.54.11.13`	Sites malveillants + publicités
DNS4EU « Child Protection & Ad Blocking »	`86.54.11.11`	Les trois

Attention : Quad9 ne propose pas de filtrage « famille ». L'adresse 9.9.9.11 est la variante avec ECS (elle transmet une partie de votre adresse IP aux sites pour améliorer la géolocalisation des contenus) : moins bonne pour la vie privée.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

4.3. Solution avancée : NextDNS (configuration personnalisée)

NextDNS est un service DNS très personnalisable.

Caractéristique	Détail
Modèle	Gratuit jusqu'à 300 000 requêtes par mois (au-delà, le filtrage s'arrête jusqu'au mois suivant), puis 1,99 $/mois ou 19,90 $/an en illimité
Blocage intégré	Publicités, traqueurs, logiciels malveillants, sites pour adultes, réseaux sociaux, etc.
Personnalisation	Listes noires et blanches, profils multiples, journaux consultables
Chiffrement	DNS over HTTPS (DoH), DNS over TLS (DoT)
Société	NextDNS Inc., **société américaine** ; vous choisissez où sont stockés les journaux (Union européenne, Suisse, États-Unis…)
Configuration	Application, navigateur (DoH) ou routeur

Pourquoi NextDNS ? Pour ses profils et ses listes de blocage sur mesure (par exemple un profil enfant).
Alternative souveraine : AdGuard Home ou Pi-hole auto-hébergés (fiches N°20c et N°38), ou DNS4EU avec blocage des publicités.

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 (section 7).

Sur macOS

Le réglage DNS de base (**Réglages Système** › **Réseau** › votre connexion › **Détails** › **DNS**) n'active pas le chiffrement. Le plus fiable : un profil de configuration DNS chiffré (Quad9 en propose, de même que NextDNS) ou l'application de votre résolveur.

Sur Linux Mint / Ubuntu

1. **Menu** › **Paramètres système** › **Réseau** (ou clic droit sur l'icône réseau › **Modifier les connexions**).
2. Sélectionnez votre connexion › cliquez sur l'icône engrenage.
3. Onglet **IPv4** : choisissez la méthode **Automatique (DHCP), adresses uniquement**.

gabriel.ananda@mailo.com
CC BY SA

4. Dans le champ **Serveurs DNS**, entrez par exemple `9.9.9.9, 149.112.112.112` (Quad9) ou `86.54.11.1` (DNS4EU).
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 (pour tout le foyer)

Si vous changez le DNS directement sur votre box, tous les appareils de la maison sont protégés en une seule manipulation.

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 **Réseau**, **Paramètres Internet**, **DNS** ou **DHCP**.
3. Passez les DNS en mode manuel (ou « statique »).
4. Entrez les adresses de Quad9 ou de DNS4EU.
5. Enregistrez et redémarrez la box.

FAI	Interface d'administration
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 192.168.0.254)
Bouygues Telecom	192.168.1.254 ou https://mabbox.bytel.fr

Limites selon les box :

FAI	Modification des 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 (les Livebox récentes bloquent la modification)

Si la modification sur votre box n'est pas possible, configurez les DNS sur chaque appareil, ou installez Pi-hole en serveur DHCP (fiche N°38).

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

La configuration sur un mobile est essentielle, car vous naviguez en Wi-Fi et en données mobiles.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

Sur Android (9 et plus récent)

1. **Paramètres** › **Réseau et Internet** › **DNS privé**.
2. Choisissez **Nom d'hôte du fournisseur DNS privé**.
3. Entrez le nom d'hôte de votre résolveur (tableau ci-dessous).

Sur iOS (14 et plus récent)

iOS n'a pas de champ « DNS privé » comme Android. Il faut passer par un profil de configuration ou par l'application du résolveur :

1. Téléchargez le profil DNS chiffré depuis le site du résolveur (pages d'aide de Quad9, joindns4.eu pour DNS4EU).
2. **Réglages** › **Général** › **VPN et gestion de l'appareil** › touchez le profil téléchargé › **Installer**.
3. Vérifiez dans **Réglages** › **Général** › **VPN et gestion de l'appareil** › **DNS** que le bon résolveur est sélectionné.

Noms d'hôte à utiliser :

Service	Nom d'hôte (DNS privé) ou adresse DoH	Fonction
Quad9	`dns.quad9.net`	Bloque les logiciels malveillants
DNS4EU Protective	`protective.joindns4.eu`	Bloque les sites malveillants
DNS4EU blocage publicitaire	`noads.joindns4.eu`	Sites malveillants + publicités
DNS4EU protection des enfants	`child.joindns4.eu`	Sites malveillants + contenus pour adultes
NextDNS	`votre-identifiant.dns.nextdns.io`	Configuration personnalisée (société américaine)

À savoir : le DNS privé (Android) ou le profil DNS (iOS) 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** › **Personnalisé**, puis l'adresse DoH (par exemple `https://dns.quad9.net/dns-query` ou `https://protective.joindns4.eu/dns-query`).
- **Brave / Chrome / Edge : Paramètres** › **Confidentialité et 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.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

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

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

Le test simple :

1. Ouvrez votre navigateur et allez sur dnsleaktest.com (ou ipleak.net).
2. Cliquez sur **Extended test** (test étendu).
3. Lisez les noms des résolveurs qui ont traité vos requêtes.

Vous devez voir :

- ✅ le résolveur que vous avez choisi (Quad9, Whalebone pour DNS4EU, NextDNS…) ;
- ❌ si le nom de votre FAI apparaît (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 ?
- ✅ Si j'utilise un VPN, laisse-t-il fuiter mon DNS vers mon FAI ?
- ✅ L'IPv6 passe-t-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 qu'un DNS public = anonymat (non : c'est seulement un bon résolveur).
- ❌ Croire que DNS chiffré = VPN (non : cela 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 regarder ce qu'il bloque.
- ❌ 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 journaux 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	Quad9	DNS4EU	NextDNS	Cloudflare
Gratuit	✅ Oui	✅ Oui	300 000 requêtes/mois	✅ Oui

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

Critère	Quad9	DNS4EU	NextDNS	Cloudflare
Confidentialité	Pas d'adresse IP enregistrée	Conforme au RGPD, résolution dans l'UE	Journaux optionnels	Journaux effacés sous 25 h
Blocage malwares	✅ Oui	✅ Oui (Protective)	✅ Oui	✅ Option
Blocage publicités	❌ Non	✅ Option	✅ Oui	❌ Non
Blocage adultes	❌ Non	✅ Option	✅ Option	✅ Option famille
Filtrage personnalisé	❌ Non	❌ Non	✅ Oui	❌ Non
Juridiction	🇨🇭 Suisse	🇪🇺 Union européenne	🇺🇸 États-Unis (journaux stockables en UE ou en Suisse)	🇺🇸 États-Unis
Idéal pour	Sécurité, vie privée	Souveraineté européenne, famille, publicités	Contrôle total	Vitesse (à défaut d'alternative)

9. Aller plus loin

Cette section s'adresse à ceux qui veulent comprendre l'architecture du contrôle par le 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 partout	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

gabriel.ananda@mailo.com
CC BY SA

Protocole	Description	Force	Limite
ODoH	Proxy chiffré entre vous et le résolveur	Le proxy connaît votre IP, le résolveur votre question : aucun ne voit tout	Encore expérimental

9.2. DNSSEC, QNAME minimization, ECH

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 en amont apprennent de vous
ECH (Encrypted Client Hello)	Chiffre le nom du site dans l'établissement de la connexion TLS	Masque le domaine visité, en complément du DNS chiffré

Important : DNSSEC n'apporte pas la confidentialité : il authentifie, il ne chiffre pas. ECH est le complément indispensable du 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 prétend que le site n'existe pas
Réponse vide ou refusée	Le résolveur renvoie une erreur ou ne répond pas
Redirection	Vous êtes envoyé vers une page d'avertissement
Sinkhole	Redirection vers une adresse contrôlée qui observe les tentatives d'accès
Filtrage par catégories	Logiciels malveillants, contenu pour adultes, « désinformation », contenus politiques
Blocage dynamique	Des listes de domaines bloqués sont mises à jour en quasi temps réel

En France, l'Arcom revendique le blocage de plus de 15 000 noms de domaine depuis 2022. Le 22 mai 2026, elle a publié une notice et deux modèles d'accords visant explicitement les moteurs de recherche, les services DNS alternatifs et les VPN, présentés comme des outils de contournement des blocages.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

Enseignement : un outil créé « contre le piratage » peut devenir une infrastructure de contrôle généralisée. Un résolveur européen comme DNS4EU est lui aussi soumis à ces obligations : changer de DNS ne doit pas servir à accéder à des contenus illicites.

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 l'hameçonnage et les logiciels malveillants ;
- ✅ éviter certains détournements DNS.

Mais changer de DNS ne protège pas contre :

- ❌ le blocage par adresse IP ;
- ❌ le blocage par SNI (sans ECH) ;
- ❌ l'inspection profonde des paquets (DPI) ;
- ❌ le blocage au niveau du registrar ou du registre (.fr, .com…) ;
- ❌ la suppression pure et simple du domaine ;
- ❌ les journaux du résolveur que vous avez choisi ;
- ❌ une obligation légale imposée à ce résolveur.

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 utilisez un VPN	Les requêtes du VPN	L'IP du VPN
DNS chiffré + VPN	Que vous utilisez 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

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 :

gabriel.ananda@mailo.com
CC BY SA

- la censure technique déborde presque toujours son objectif initial ;
- les blocages automatisés font des dégâts collatéraux importants ;
- un outil créé « contre le piratage » peut devenir une infrastructure de contrôle généralisée.

C'est le scénario qui se dessine à l'échelle européenne.

9.7. Recommandations selon votre profil

Profil	Recommandation DNS
Vie privée simple	Quad9 ou DNS4EU, activé au niveau du système avec DoH/DoT. Test de fuite DNS. C'est tout.
Famille	DNS4EU « Child Protection » (avec ou sans blocage des publicités) sur la box ; ou NextDNS avec un profil enfant, journaux réduits au minimum.
Contourner un blocage abusif	1. Changez de DNS. 2. Activez DoH/DoT. 3. Testez plusieurs résolveurs. 4. Si cela ne suffit pas : VPN.
Journaliste / militant	DNS chiffré + VPN sérieux (Mullvad). Vérification systématique des fuites. Navigateur durci. ECH si disponible. Pas de comptes personnels dans l'environnement dédié (fiche N°44).
Utilisateur avancé / auto-hébergement	Unbound local + DNSSEC + QNAME minimization. Pi-hole ou AdGuard Home pour le filtrage réseau.

9.8. Aller encore plus loin : l'auto-hébergement

- **Unbound :** serveur DNS récursif local, avec DNSSEC et QNAME minimization, éventuellement relayé vers un résolveur DoT/DoH fiable.
- **Pi-hole ou AdGuard Home :** sur un Raspberry Pi ou un petit serveur, pour bloquer publicités et traqueurs à l'échelle du réseau (fiches N°38 et N°20c).

10. Challenge 7 jours

Challenge : pendant 7 jours, utilisez un DNS privé (Quad9 ou DNS4EU) sur tous vos appareils.

Jour	Action
Jour 1	Configurez Quad9 ou DNS4EU sur votre ordinateur
Jour 2	Configurez-le sur votre box pour protéger tout le foyer
Jour 3	Configurez le DNS privé sur votre mobile Android ou iOS
Jour 4	Vérifiez sur dnsleaktest.com que la protection fonctionne sur tous vos appareils
Jour 5	Vérifiez que cela fonctionne aussi en 4G/5G sur votre mobile

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

Jour	Action
Jour 6	Si vous avez choisi le blocage publicitaire, observez les sites que vous visitez souvent
Jour 7	Naviguez normalement et observez la différence

Vous allez constater :

- moins de publicités (avec l'option de blocage de DNS4EU) ;
- une navigation aussi rapide, voire plus ;
- votre FAI ne voit plus les sites que vous visitez (avec le DNS chiffré) ;
- les sites d'hameçonnage sont bloqués.

11. En résumé (ce que vous gagnez)

Action	Gagné
Passer à Quad9 (9.9.9.9)	Protection contre l'hameçonnage et les logiciels malveillants, pas d'IP enregistrée, juridiction suisse
Passer à DNS4EU	Résolution dans l'UE, options famille et blocage des publicités, gratuit
Passer à NextDNS	Blocage personnalisé sur tout le réseau (société américaine, journaux optionnels)
Changer le DNS de votre box	Tous les appareils du foyer protégés en une manipulation
Activer DNS over HTTPS (Firefox)	Requêtes DNS chiffrées, illisibles pour votre FAI
Configurer le DNS privé sur votre mobile	Protection en Wi-Fi et en données mobiles

12. Conclusion

Si vous voulez…	Choisissez…
Simple, sûr, sans prise de tête	Quad9 (9.9.9.9)
Un résolveur européen	DNS4EU (86.54.11.1)
Vie privée maximale	Quad9, ou votre propre résolveur Unbound
Bloquer les publicités sans installer de serveur	DNS4EU « Ad Blocking » (86.54.11.13), ou NextDNS
Protéger toute la famille	DNS4EU « Child Protection » sur la box, ou NextDNS avec profil enfant

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V2.2

À retenir absolument

1. Le DNS de votre FAI voit tous les domaines que vous consultez et applique les blocages imposés. Changez-le.
2. HTTPS cache la conversation, pas la porte à laquelle vous frappez.
3. **Quad9 (Suisse) et DNS4EU (Union européenne)** sont gratuits, simples et respectueux de votre vie privée. Cloudflare et NextDNS sont américains.
4. Une fois configuré sur votre box, vous n'avez plus rien à faire.
5. N'oubliez pas vos mobiles : configurez le DNS privé.
6. Testez toujours après configuration.

Test final :

1. Configurez votre nouveau DNS sur votre ordinateur.
2. Vérifiez sur dnsleaktest.com que cela fonctionne.
3. Configurez le DNS privé sur votre mobile.
4. Vérifiez qu'il fonctionne aussi en 4G/5G.
5. Naviguez normalement pendant une semaine.
6. Si tout fonctionne, configurez-le sur votre box pour protéger tout le foyer ✅

Références

- Mullvad – Fermeture des serveurs DNS publics chiffrés et soutien à Quad9 (3 septembre 2026)
- Quad9 – Adresses et fonctions des services
- DNS4EU – Lancement du service public (adresses et options)
- Help Net Security – Lancement de DNS4EU, résolveur européen (juin 2025)
- Cloudflare – Engagement de confidentialité du résolveur 1.1.1.1
- DNS Robot – NextDNS : limite gratuite et tarifs (guide détaillé)
- Arcom – Notice et deux modèles d'accords contre le piratage sportif (22 mai 2026)
- Next – L'Arcom revendique plus de 15 000 noms de domaine bloqués depuis 2022

gabriel.ananda@mailo.com
CC BY SA