

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

Objectif : Remplacer le serveur DNS par défaut de votre fournisseur d'accès (Orange, SFR, Free, Bouygues, etc.) par Cloudflare (1.1.1.1), Quad9 (9.9.9.9) ou **NextDNS** pour naviguer de manière plus privée, plus rapide, et protégée contre les sites malveillants.

Public visé : Débutant à Intermédiaire (NextDNS nécessite un peu plus d'attention)

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 (Fournisseur d'Accès Internet) enregistre tous les sites que vous visitez	Cloudflare et Quad9 s'engagent à ne pas conserver vos données personnelles (politique de confidentialité stricte)
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 et Quad9 ne censurent pas (sauf option famille)
Vous êtes exposé aux sites de phishing et aux logiciels malveillants	Quad9 bloque automatiquement les sites dangereux grâce à des listes mises à jour en temps réel
Le DNS par défaut n'est pas chiffré : quelqu'un sur votre réseau peut voir vos requêtes	DNS over HTTPS (DoH) ou DNS over TLS (DoT) chiffrent vos requêtes

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

Problème

Solution apportée par un DNS privé

Vous voulez bloquer les publicités, les traqueurs et les sites adultes sur tout votre réseau

NextDNS permet une configuration personnalisée (blocage, logs, liste blanche, etc.)

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

2. Les solutions DNS recommandées

2.1 Pour débutants : Cloudflare ou Quad9 (simples, rapides)

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, excellente confidentialité (suppression des logs en 24h), chiffrement DNS par défaut
Quad9 (9.9.9.9)	9.9.9.9	149.112.112.112	Bloque les sites de phishing et malwares (listes mises à jour toutes les minutes), géré par une fondation à but non lucratif

2.2 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

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

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

NextDNS est un service DNS moderne qui permet une **configuration ultra-personnalisable** (blocage des publicités, des traqueurs, des réseaux sociaux, des sites adultes, logs optionnels, etc.).

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, via navigateur (DoH), ou directement sur le routeur
----------------------	--

Localisation	Serveurs dans le monde entier (dont Europe)
---------------------	---



Pourquoi choisir NextDNS ?

Si vous en avez assez des publicités sur tous vos appareils (ordinateur, téléphone, tablette, TV connectée), NextDNS les bloque **au niveau du réseau**, sans rien installer. Une seule configuration sur votre box (routeur) protège tout le foyer.

3. Comment faire ? (Le pas à pas)

3.1 Méthode A : Changer le DNS sur votre ordinateur (Windows, Mac, Linux)

Sur Windows (changement permanent)

1. Ouvrez les paramètres réseau :

• Démarrer → Panneau de configuration → Réseau et Internet → Centre réseau et partage

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

- Cliquez sur **Connexion au réseau local** ou **Wi-Fi** (selon votre connexion)
- Cliquez sur **Propriétés**

2. Sélectionnez **Protocole Internet version 4 (TCP/IPv4)** → **Propriétés**

3. Cochez **Utiliser les adresses de serveur DNS suivantes**

4. Entrez les adresses selon votre choix :

Solution	Serveur DNS préféré	Serveur DNS auxiliaire
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
Cloudflare famille	1.1.1.3	1.0.0.3

5. Cliquez sur **OK** puis **Fermer**

6. Redémarrez votre ordinateur ou tapez `ipconfig /flushdns` dans l'invite de commandes

Sur macOS

1. Préférences Système → **Réseau**
2. Sélectionnez votre connexion active → **Avancé...** → onglet **DNS**
3. Cliquez sur **+** sous la liste des serveurs DNS
4. Entrez les adresses (1.1.1.1, 1.0.0.1 ou 9.9.9.9, 149.112.112.112)
5. Supprimez les anciens serveurs (ceux de votre FAI)
6. Cliquez sur **OK** puis **Appliquer**

Sur Linux Mint / Ubuntu

Via l'interface graphique :

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

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

3.2 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 (ordinateurs, téléphones, TV, consoles) bénéficieront automatiquement du nouveau DNS.

Étapes générales :

1. Connectez-vous à l'interface d'administration de votre box :

- Tapez 192.168.1.1 ou 192.168.0.1 dans votre navigateur
- Le mot de passe administrateur est souvent sur une étiquette sous la box

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 (voir section suivante pour NextDNS)

5. Sauvegardez et redémarrez la box

3.3 Méthode C : NextDNS – Configuration avancée (recommandé)

Étape 1 : Créez un compte NextDNS

1. Rendez-vous sur <https://nextdns.io>
2. Cliquez sur "**Get Started**" (gratuit pour 300 000 requêtes/mois)
3. Créez un compte (email + mot de passe)

Étape 2 : Configurez vos paramètres de blocage

Une fois connecté, vous arrivez sur votre tableau de bord. Vous pouvez personnaliser :

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

Paramètre	Recommandation	Explication
Blocage publicités	✓ Activer	Bloque les publicités sur tous vos appareils
Blocage traqueurs	✓ Activer	Bloque les traqueurs publicitaires
Blocage malwares	✓ Activer (High)	Bloque les sites dangereux
Blocage adultes	Selon besoin	Bloque les contenus pour adultes
Blocage réseaux sociaux	Selon besoin	Bloque Facebook, Twitter, etc.
SafeSearch	✓ Activer	Filtre les résultats de recherche explicites
Logs	Désactivés (ou 24h max)	Pour préserver votre vie privée

Étape 3 : Choisissez vos listes de blocage

Dans l'onglet "**Privacy**" (Denylist), choisissez des listes de blocage.
Recommandations pour débutants :

Liste	Ce qu'elle bloque
OISD Full	Publicités + traqueurs + malwares (la plus complète)
AdGuard DNS filter	Publicités (complément)

💡 **Astuce** : Ne prenez pas trop de listes au début – commencez par **OISD Full**.

Étape 4 : Récupérez votre adresse DNS personnalisée

Chaque compte NextDNS génère une **adresse DNS unique** (ou un identifiant). Vous la trouverez dans l'onglet "**Setup**".

Exemple : 45.90.28.xxx et 45.90.28.xxx (deux adresses)

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

Étape 5 : Configurez NextDNS sur vos appareils

Option 1 – Sur votre box (routeur) :

Entrez les deux adresses IP uniques dans les champs DNS de votre box. Tous vos appareils seront protégés automatiquement.

Option 2 – Sur votre ordinateur (Windows/Mac/Linux) :

Entrez les deux adresses IP comme vous le feriez pour Cloudflare ou Quad9.

Option 3 – Application mobile (Android/iOS) :

Installez l'application "**NextDNS**" depuis le Play Store ou l'App Store. Elle vous guidera pour configurer le DNS chiffré.

Option 4 – DNS over HTTPS dans Firefox :

- 1.Paramètres → Vie privée et sécurité → DNS sécurisé
- 2.Cochez "Augmenter la protection"
- 3.Choisissez "Personnalisé" → entrez : <https://dns.nextdns.io/votre-identifiant>

Étape 6 : Vérifiez que ça fonctionne

Rendez-vous sur <https://test.nextdns.io>

Le site vous confirmera si vous utilisez bien NextDNS et vous montrera quels blocages sont actifs.

Limites de la version gratuite

Version gratuite	Version payante (1,99 \$/mois)
300 000 requêtes/mois	Requêtes illimitées
Toutes les fonctionnalités	Toutes les fonctionnalités
Parfait pour un foyer de 2-3 personnes	Pour les gros consommateurs

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

4. Tableau comparatif des solutions DNS

Critère	Cloudflare (1.1.1.1)	Quad9 (9.9.9.9)	NextDNS
Gratuit	✔ Oui	✔ Oui	✔ 300k req/mois
Rapide	✔ Très rapide	✔ Rapide	✔ Très rapide
Confidentialité	Logs supprimés en 24h	Pas de logs IP	Logs optionnels (désactivables)
Blocage malwares	✘ Non	✔ Oui (listes mises à jour)	✔ Oui (configurable)
Blocage publicités	✘ Non	✘ Non	✔ Oui (listes personnalisables)
Blocage adultes	✔ (1.1.1.3)	✔ (9.9.9.11)	✔ Oui (optionnel)
Filtrage personnalisé	✘ Non	✘ Non	✔ Oui (listes noires/blanches)
Logs consultables	✘ Non	✘ Non	✔ Oui (optionnel, limité)
DNS over HTTPS/TLS	✔ Oui	✔ Oui	✔ Oui
Idéal pour	Vitesse et simplicitéSécurité anti-malware		Contrôle total + blocage pubs

5. À savoir avant de se lancer

Crainte fréquente	La réalité
"Je vais perdre ma	Non. Si les adresses sont incorrectes, les sites n'ouvriront plus,

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

Crainte fréquente	La réalité
connexion Internet si je me trompe."	mais il suffit de remettre "Obtenir automatiquement" pour revenir à la normale.
"Mon FAI va me facturer quelque chose ?"	Non. Changer de DNS est totalement gratuit et autorisé.
"Cloudflare et Quad9 me traquent-ils ?"	Cloudflare supprime les logs en 24h ; Quad9 ne conserve aucun log d'adresse IP. Tous deux sont transparents et audités.
"NextDNS est-il vraiment privé ?"	Oui – vous pouvez désactiver les logs. Le service a été audité et respecte le RGPD.
"Est-ce que les sites web vont s'afficher différemment ?"	Non. Le DNS ne modifie pas le contenu des sites, uniquement "l'annuaire" qui transforme google.com en adresse IP.
"Comment vérifier que ça a bien fonctionné ?"	Pour Cloudflare : 1.1.1.1/help . Pour Quad9 : quad9.net/connect . Pour NextDNS : test.nextdns.io .
"NextDNS, c'est compliqué à configurer ?"	La configuration de base prend 5 minutes. Vous pouvez ensuite l'oublier.
"300 000 requêtes par mois, c'est suffisant ?"	Pour un foyer de 2-3 personnes utilisant Internet normalement, c'est très large. Le streaming vidéo génère peu de requêtes DNS (une par minute environ).

6. Challenge 7 jours

Challenge : Pendant 7 jours, utilisez **NextDNS** (ou Cloudflare/Quad9) sur tous vos appareils.

Vous allez constater :

- Moins de publicités (avec NextDNS)

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

- Une navigation plus rapide (surtout si votre FAI a un DNS lent)
- Votre FAI ne voit plus les sites que vous visitez
- Les sites de phishing sont bloqués (avec Quad9 ou NextDNS)

Test à faire :

1. Configurez NextDNS sur votre box (ou sur votre ordinateur)
2. Allez sur test.nextdns.io – vérifiez que vous êtes bien protégé
3. Essayez d'accéder à un site de test de phishing (exemple : <https://nextdns.io/phishing-test> – NextDNS bloque normalement)
4. Au bout de 7 jours, consultez les statistiques NextDNS pour voir combien de requêtes ont été bloquées

7. 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, sans logs
Changer pour NextDNS	Blocage des publicités et traqueurs sur tout le réseau, logs optionnels, personnalisation infinie
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

Fiche Pratique N°6 : Changez votre serveur DNS pour plus de confidentialité et de sécurité V1.1

8. 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)
Contrôle total + blocage des publicités	NextDNS (recommandé pour les utilisateurs exigeants)
Protection pour toute la famille	NextDNS configuré sur la box + blocage adulte activé

À retenir absolument :

- Les DNS par défaut de votre FAI sont lents et vous espionnent. Changez-les !
- **Cloudflare** et **Quad9** sont gratuits, simples et respectueux de votre vie privée.
- **NextDNS** est plus technique mais offre un **blocage des publicités** et une **personnalisation** inégalés.
- Une fois configuré sur votre **box**, vous n'avez plus rien à faire – tous vos appareils sont protégés.

Test final :

1. ☒ Configurez NextDNS (ou Cloudflare) sur votre ordinateur
2. ☒ Vérifiez sur test.nextdns.io (ou 1.1.1.1/help) que ça fonctionne
3. ☒ Naviguez normalement pendant une semaine
4. ☒ Vérifiez que vous voyez moins de publicités (NextDNS)
5. ☒ Si tout fonctionne, configurez-le sur votre **box** pour protéger tout le foyer