



LE PARE-FEU DE CIRA

PRÉPARÉ PAR: PIERRE ROBILLARD

22 OCTOBRE 2026

SITE: [HTTPS://FORMATIO.INFO/CLUB-INFORMATIQUE](https://formatio.info/club-informatique)

COURRIEL: RECEPTION@FORMATIO.INFO



Contenu de la présentation

1. CIRA en bref
2. Qu'est-ce qu'un serveur DNS?
3. Le pare-feu de CIRA en détail
4. Où effectuer la configuration ?
5. L'installation du bouclier de CIRA

Complément d'information

Provenance de la liste d'adresse frauduleuses de CIRA

Tableau comparatif CIRA Cloudflare et Google DNS



Cira est une OBNL, une organisation à but non lucratif canadienne indépendante qui offre une protection contre le hameçonnage et les logiciels malveillants.

Il existe d'autres sites qui offrent cette protection. Son principal intérêt réside à offrir une protection axée sur les Canadiens.

Où peut-on l'installer ?

- * Sur tous vos appareils : cellulaires, tablettes, ordinateurs, portables et routeurs.

Comment ça fonctionne ?

- * Il suffit de modifier seulement deux paramètres.



Où faire la modification ?

- * Dans votre navigateur Web (Firefox, Google, Chrome, Brave, Safari, Bing, etc), dans le système (ex. Windows, macOS, iOS) ou directement sur votre routeur.

Chaque emplacement présente ses avantages et ses inconvénients.

De quelle manière, CIRA protège?

- * C'est via son serveur DNS de CIRA

Qu'est-ce qu'un serveur DNS?



DNS est l'abréviation de Domain Name System (en français, Système de noms de domaine).

C'est l'annuaire d'Internet.

Il traduit les noms de domaines comme Formatio.info, Bell.ca, ou cira.ca, en adresses IP numériques comme 149.112.121.20 indispensables aux ordinateurs pour communiquer entre eux.

Qu'est-ce qu'un serveur DNS? (suite)



Normalement, lorsque vous utilisez les réglages par défaut de votre fournisseur (exemple: Vidéotron, Bell), votre routeur envoie chaque demande d'adresse (ex: google.ca, journaldemontreal.com) directement aux serveurs du fournisseur afin qu'il obtienne l'adresse IP correspondant à ce site.

Le pare-feu de CIRA en détail



Ce pare-feu DNS appelé **Bouclier canadien de CIRA** s'ajoute au pare-feu logiciel comme Windows Defender.

L'autorité canadienne pour les renseignements Internet (ACEI), mieux connu sous l'acronyme anglais **CIRA** (Canadian Internet Registration Authority) opère ce bouclier depuis qu'il a été créé en 2020.

CIRA, un organisme à but non lucratif, a été créée en 1998 pour prendre le relais de l'Université de la Colombie-Britannique (UBC), qui gérait bénévolement l'enregistrement des domaines **.ca** depuis 1987.

En 2000, un accord-cadre conclu avec le ministère de l'Innovation, des Sciences et du Développement économique (ISDE) du gouvernement du Canada a reconnu CIRA par comme opérateur du **.CA**

Le pare-feu de CIRA en détail (suite)



Ce bouclier protège contre le hameçonnage (Phishing), les faux sites. Par exemple, un site malicieux qui a une grande ressemblance avec le vrai site de Bell mais a une adresse IP malicieuse.

Il bloque les logiciels malveillants. Par exemple, il bloque un virus sur votre PC qui tente de contacter son serveur frauduleux.

Il ne surveille pas vos fichiers. Il agit au niveau de votre connexion internet.

En remplaçant les réglages du fournisseur internet par ceux du pare-feu, votre routeur envoie désormais cette question directement aux serveurs de CIRA via une connexion sécurisée. Le bouclier vérifie, valide et retourne ensuite l'adresse IP à votre routeur pour qu'il établisse le lien avec le site voulu.

Le pare-feu de CIRA en détail (suite)

Votre fournisseur ne voit transiter que des paquets de données sans en connaître l'adresse IP.

Le bouclier vérifie si ce domaine est sur sa "liste noire" de sites malveillants qui est continuellement mise à jour.

Il y a 3 niveaux de filtrage :

1. **Privé** : Confidentialité DNS simple.
2. **Sécurisé** : Ajoute la protection contre les malwares et le phishing.
3. **Familial** : Ajoute un filtre pour le contenu adulte (porno).

Le pare-feu de CIRA en détail (suite)



Les avantages majeurs

Souveraineté des données : Contrairement à Google DNS (8.8.8.8) ou Cloudflare (1.1.1.1), les serveurs sont situés **au Canada**. Vos habitudes de navigation restent sous juridiction canadienne et ne sont pas vendues à des tiers.

Rapidité : Comme les serveurs sont locaux (souvent à Montréal ou Toronto), la latence est très faible pour les utilisateurs québécois.

Gratuité : C'est un service public offert par l'ACEI, l'organisme qui gère les domaines **.ca**.

Le pare-feu de CIRA en détail (suite)



Les limites à connaître

Ce n'est pas un antivirus : Il ne peut pas supprimer un virus déjà présent sur votre disque dur ou scanner une clé USB.

Il empêche seulement la *connexion* vers des sites dangereux.

Configuration : Bien qu'il existe une application mobile, pour protéger toute votre maison (consoles, télé intelligente, PC), il est préférable de configurer les adresses DNS directement dans votre routeur, ce qui demande une petite manipulation technique à réaliser une seule fois.

La mise à jour des sites frauduleux se fait sur le site de CIRA

Le pare-feu de CIRA en détail (suite)



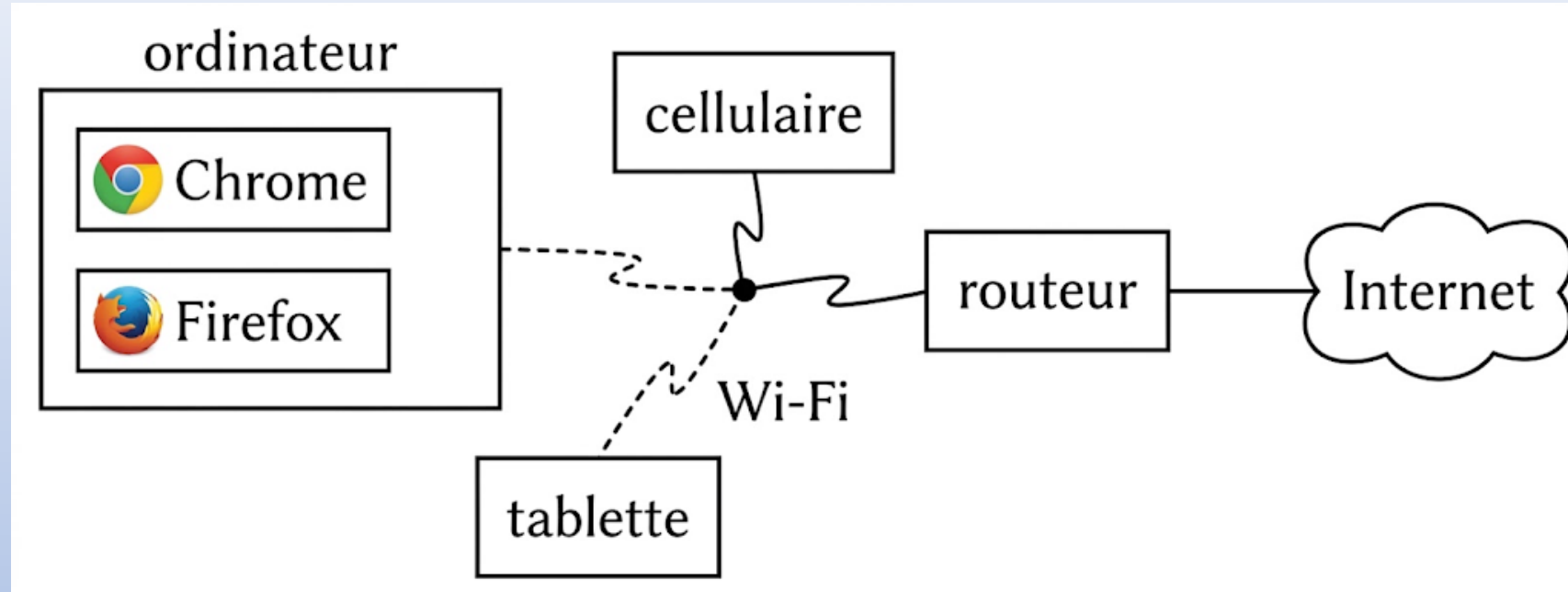
Donc, si vous cherchez à renforcer la sécurité de votre foyer sans ralentir votre connexion, c'est une **excellente couche de protection supplémentaire**.

C'est particulièrement efficace pour :

Protéger les membres de la famille moins technophiles contre les liens frauduleux.

Améliorer la confidentialité face à votre fournisseur d'accès internet (Vidéotron, Bell, Ebox, etc.). En ne voyant pas vos requêtes, il ne connaît pas les sites que vous visitez.

Où effectuer la configuration ?



Configurer le bouclier au niveau du **routeur de la maison** est la méthode la plus efficace, car il protège automatiquement tous les appareils connectés à votre Wi-Fi (téléphones, ordinateurs, tablettes et même vos objets connectés).

Où effectuer la configuration ?



1. Directement dans le navigateur (ex. Brave, Firefox, Chrome)

Le principe : La protection s'applique uniquement à la navigation Web dans ce logiciel spécifique.

Avantages :

- Facile et rapide à configurer.

- Permet d'activer facilement le chiffrement des requêtes (DoH / DNS sécurisé).

Inconvénient : Ne protège pas les autres applications de l'appareil (ex. vos courriels, applications d'arrière-plan, mises à jour).

Où effectuer la configuration ? (suite)



2. Dans le système d'exploitation (ex. Windows, iOS, Android)

Le principe : On configure la protection directement dans les paramètres réseau de l'ordinateur, du téléphone ou de la tablette.

Avantages :

Protège **toutes** les applications de cet appareil (navigateurs, logiciels de courriel, jeux, etc.).

Suit l'appareil même lorsqu'il se connecte à un réseau Wi-Fi public à l'extérieur.

Inconvénient : Il faut répéter la configuration individuelle sur chaque appareil de la maison.

Où effectuer la configuration ? (suite)



3. le cas d'un portable

Dans le cas d'un **portable**, l'approche diffère puisque sa portabilité fait en sorte qu'il peut se connecter sur des réseaux dont on a peu d'information.

La protection s'installe soit au niveau des **navigateurs** ou mieux, au niveau du **chiffrement DoT / DoH** que nous verrons un peu plus loin.

Précaution importante : Prenez une capture d'écran et/ou notez vos adresses DNS avant d'inscrire celles de CIRA car s'il a erreur, vous n'aurez plus accès à internet!

Où effectuer la configuration ? (suite)



4. Directement dans le routeur résidentiel

Le principe : On modifie les paramètres à la source, au niveau de la boîte Internet principale.

Avantages : Une seule configuration protège instantanément tous les appareils connectés au Wi-Fi de la maison (ordinateurs, téléphones, télévisions intelligentes, objets connectés).

Inconvénient : La protection ne suit plus les appareils mobiles dès qu'ils quittent la maison ou passent sur les données cellulaires (LTE/5G).

La configuration peut être plus difficile à réaliser à cause de la variété des routeurs.

Précaution importante : Prenez une capture d'écran et/ou notez vos adresses DNS avant d'inscrire celles de CIRA car s'il y a erreur, vous n'aurez plus accès à internet!

Où effectuer la configuration ? (suite)

En résumé:

1. De préférence, configurer le routeur de la maison pour une protection complète de tous les équipements reliés au réseau Wifi de la maison;
2. Configurer les équipements mobiles que vous utilisez à l'extérieur de la maison: cellulaire, tablette, portable.

L'installation du bouclier de CIRA

On peut configurer le Bouclier canadien sur une variété d'appareils ou de plateformes suivantes accessibles à:

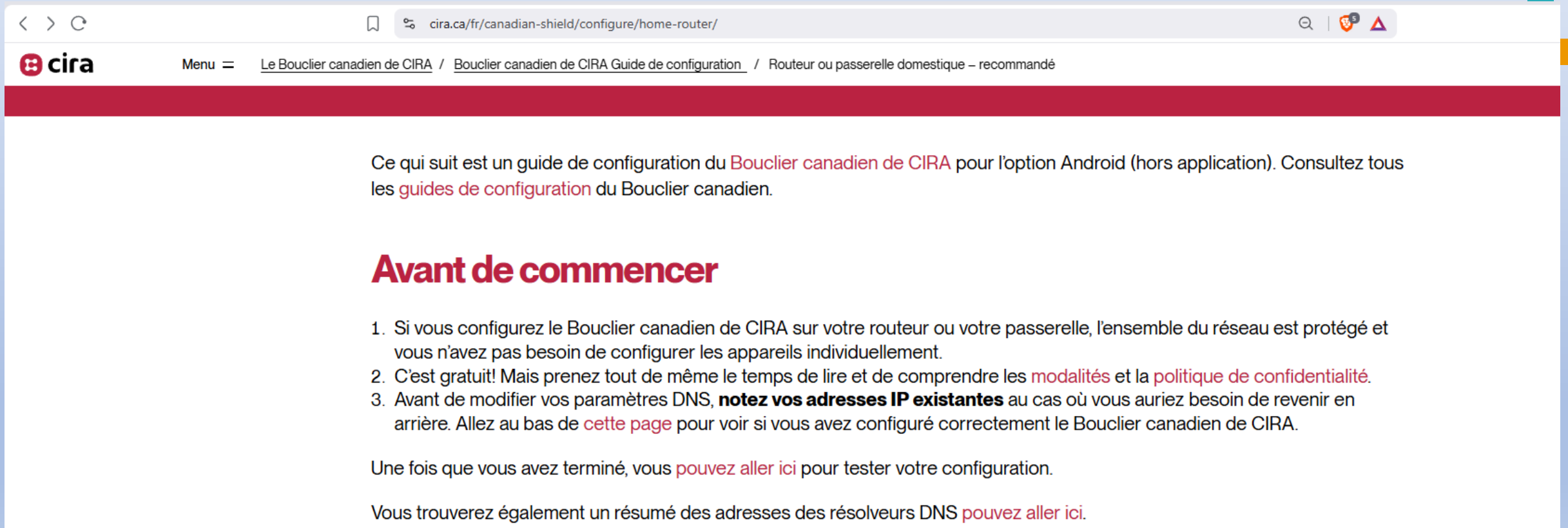
<https://www.cira.ca/fr/canadian-shield/configure/>

Résumé des adresses des résolveurs DNS du Bouclier canadien de CIRA	→	Routeur ou passerelle domestique – recommandé	→
Extension de navigateur	→	Système d'exploitation Microsoft Windows	→
Apple MacOS	→	Version mobile sur iOS ou Android (App Store ou Google Play)	→
Sony Playstation 4	→	Microsoft Xbox One	→
Nintendo Switch	→	Nintendo 3DS	→
Ubuntu Desktop	→	Debian	→
Chiffrement DNS avec DNS sur HTTPS (DoH) sur Chrome	→	Chiffrement DNS avec DNS sur HTTPS (DoH) sur Firefox	→
Chiffrement DNS avec HTTPS sur Microsoft Edge	→	Chiffrement DNS avec DNS sur TLS (DoT)	→
Android (hors application)	→		

L'installation du bouclier au niveau du routeur

L'installation du bouclier au niveau du routeur

CIRA offre un guide de configuration à cette adresse: <https://www.cira.ca/fr/canadian-shield/configure/home-router/>



The screenshot shows a web browser window with the URL [cira.ca/fr/canadian-shield/configure/home-router/](https://www.cira.ca/fr/canadian-shield/configure/home-router/). The page header includes the CIRA logo and a navigation menu with the following items: "Le Bouclier canadien de CIRA", "Bouclier canadien de CIRA Guide de configuration", and "Routeur ou passerelle domestique – recommandé". The main content area has a red header bar and the following text:

Ce qui suit est un guide de configuration du **Bouclier canadien de CIRA** pour l'option Android (hors application). Consultez tous les **guides de configuration** du Bouclier canadien.

Avant de commencer

1. Si vous configurez le Bouclier canadien de CIRA sur votre routeur ou votre passerelle, l'ensemble du réseau est protégé et vous n'avez pas besoin de configurer les appareils individuellement.
2. C'est gratuit! Mais prenez tout de même le temps de lire et de comprendre les **modalités** et la **politique de confidentialité**.
3. Avant de modifier vos paramètres DNS, **notez vos adresses IP existantes** au cas où vous auriez besoin de revenir en arrière. Allez au bas de **cette page** pour voir si vous avez configuré correctement le Bouclier canadien de CIRA.

Une fois que vous avez terminé, vous **pouvez aller ici** pour tester votre configuration.

Vous trouverez également un résumé des adresses des résolveurs DNS **pouvez aller ici**.

L'installation du bouclier au niveau du routeur (suite)



En résumé:

- 1) Accédez à l'interface de votre routeur
- 2) Trouvez les paramètres DNS

Cherchez une section nommée "Paramètres de base", "Internet", ou "LAN/Réseau". Vous y trouverez une option pour les serveurs DNS (souvent réglée sur "Automatique" par défaut).

- 3) Notez les adresses actuelles ou prenez une capture d'écran
- 4) Entrez les adresses du Bouclier canadien

Modifiez le réglage en "Manuel" et entrez les adresses suivantes selon le niveau de protection que vous avez choisi :

Niveau	Serveur DNS Primaire	Serveur DNS Secondaire
Privé (Confidentialité seulement)	149.112.121.10	149.112.122.10
Sécurisé (Malware + Phishing)	149.112.121.20	149.112.122.20
Familial (Sécurisé + Pornographique)	149.112.121.30	149.112.122.30

L'installation du bouclier au niveau du routeur (suite)



L'installation du bouclier au niveau du routeur (suite)

5) Vous sauvegardez et redémarrez

Une fois les adresses enregistrées, cliquez sur **Appliquer** ou **Sauvegarder**. Il est parfois nécessaire de redémarrer le routeur (ou simplement de désactiver et réactiver le Wi-Fi sur vos appareils) pour que le changement soit pris en compte.

6) Vous vérifiez le fonctionnement

Une fois la configuration terminée, visitez le site officiel de CIRA pour confirmer instantanément si votre réseau utilise bien leurs serveurs.

<https://www.cira.ca/fr/canadian-shield/configure/canadian-shield-configuration-test-2/>

L'installation du bouclier au niveau du routeur (suite)



Étant donné les nombreuses marques et modèles de routeur, en cas d'insuccès, je vous suggère d'utiliser votre IA préféré pour obtenir les instructions spécifiques à votre routeur. **Voici une suggestion pour l'invite (le prompt) : Routeur XX modèle YY (ou photo de la plaque signalétique) : Fournir les instructions pour changer l'adresse primaire et secondaire**

Au besoin, fournissez des captures d'écran à votre IA et lui demander de clarifier les étapes suivantes.

L'installation du bouclier sur un portable ou ordinateur Windows

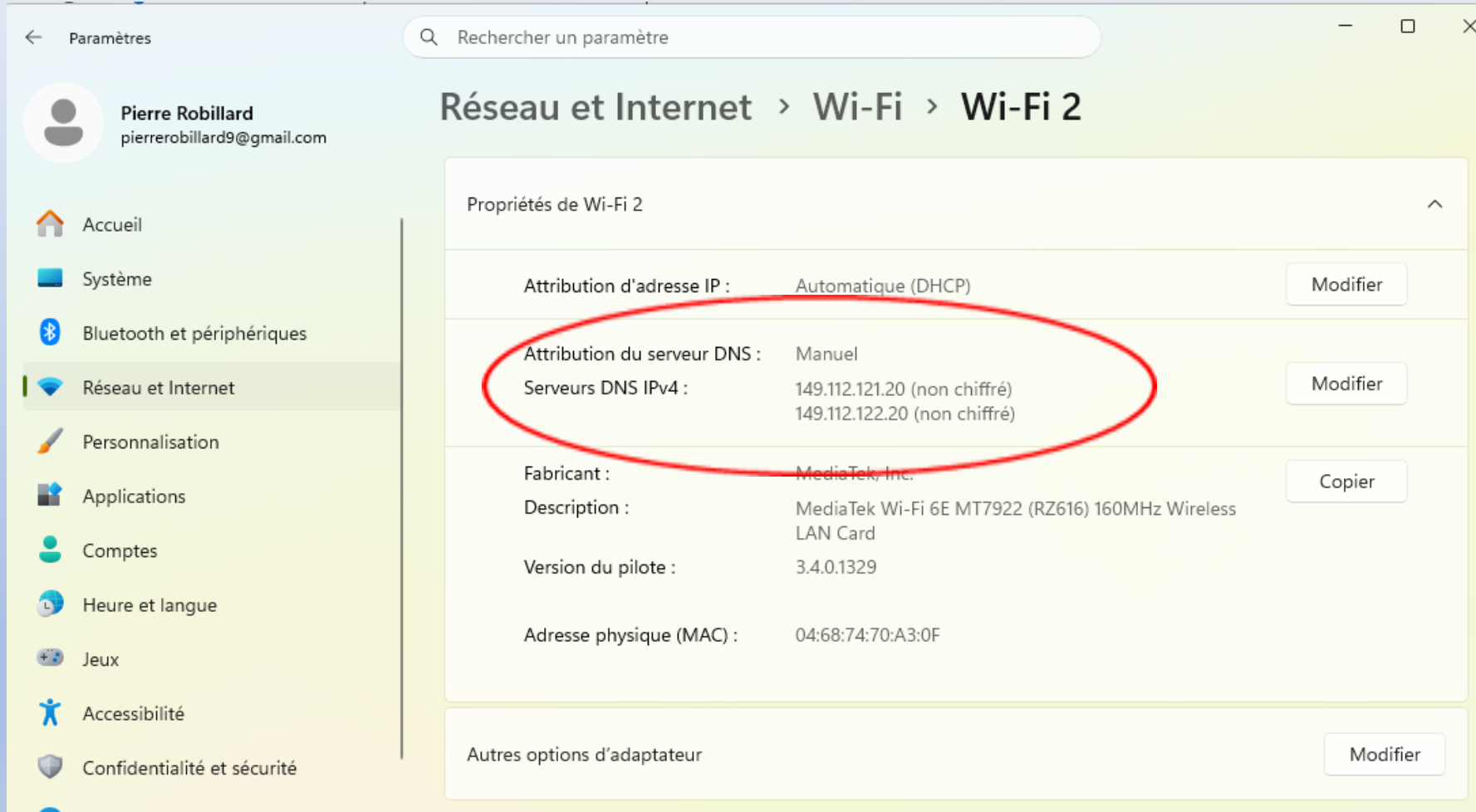


Cette méthode protège toutes les applications de votre PC Windows.

1. Cliquez sur le menu **Démarrer** puis ouvrez les **Paramètres** (icône d'engrenage).
2. Dans le menu de gauche, sélectionnez **Réseau et Internet**.
3. Cliquez sur votre type de connexion actuelle : **Wi-Fi** ou **Ethernet** (par câble).
4. Cliquez sur **Propriétés du matériel**.
5. Recherchez la ligne **Attribution de serveur DNS** et cliquez sur le bouton **Modifier**.
6. Dans le menu déroulant, passez de *Automatique (DHCP)* à **Manuel**.
7. Activez l'option **IPv4**.
8. Saisissez les deux adresses dans les cases :
 1. **DNS préféré** : 149.112.121.20 (*ou 1.1.1.2*)
 2. **DNS secondaire** : 149.112.122.20 (*ou 1.0.0.2*)
9. Cliquez sur **Enregistrer**.

L'installation du bouclier sur un portable ou ordinateur Windows

Vous obtenez une fenêtre comme celle-ci:



L'installation du bouclier sur un portable ou ordinateur Mac



Cette méthode protège toutes les applications de votre Mac.

1. Cliquez sur le **menu Pomme ()** en haut à gauche de l'écran.
2. Ouvrez les **Réglages système** (ou *Préférences système*).
3. Cliquez sur **Réseau** dans le menu latéral.
4. Sélectionnez votre réseau connecté (**Wi-Fi** ou **Ethernet**), puis cliquez sur **Détails...**
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **DNS** dans la colonne de gauche.
6. Sous la liste des *Serveurs DNS*, cliquez sur le bouton « + » en bas à gauche :
 1. Tapez la première adresse : 149.112.121.20
 2. Cliquez à nouveau sur « + » et tapez la seconde adresse : 149.112.122.20
7. Cliquez sur **OK**, puis sur **Appliquer**.

L'installation du bouclier sur un navigateur Web Brave / Chrome



Dans Brave / Chrome :

1. Ouvrez les **Paramètres** du navigateur (les 3 petits points ou barres en haut à droite).
2. Allez dans **Confidentialité et sécurité** \flèche droite **Sécurité**.
3. Faites défiler jusqu'à la section **Utiliser un DNS sécurisé**.
4. Sélectionnez **Avec : Personnalisé**.
5. Entrez l'adresse Web sécurisée (DoH) du service (ex. pour CIRA : <https://protected.canadianshield.cira.ca/dns-query>)

L'installation du bouclier sur un navigateur Mozilla Firefox



Au Canada, il est installé par défaut dans Mozilla Firefox.

Pour vous en assurer, faite ce test : <https://www.cira.ca/fr/canadian-shield/configure/canadian-shield-configuration-test-2/>

Si le test échoue:

1. Ouvrez les **Paramètres** de Firefox.
2. Dans l'onglet **Vie privée et sécurité**, faites défiler vers le bas jusqu'à: **DNS via HTTPS** et cliquez sur **Paramètres avancés**
3. Cliquez sur **Personnalisé**
4. Choisissez le fournisseur **CIRA Canadian Shield**.

L'installation du bouclier sur un iPhone/iPad



Option A : Manuellement (via un profil de configuration)

1. Téléchargez le fichier de profil depuis le site web officiel de CIRA via Safari.
2. Allez dans l'application **Réglages** de votre iPhone/iPad. Un message « **Profil téléchargé** » apparaîtra tout en haut.
3. Appuyez dessus, puis touchez **Installer** (votre code de déverrouillage vous sera demandé).
4. Suivez les étapes pour valider.

Le système d'exploitation de l'iPhone gère la protection de manière purement native. En étant installée dans les réglages, il n'y a d'application qui tourne en arrière-plan ou qui occupe de l'espace visuel sur votre écran d'accueil.

C'est parfait pour les personnes qui n'aiment pas accumuler les applications sur leur téléphone.

Option B : Via l'application officielle

1. Ouvrez l'**App Store** sur votre iPhone ou iPad.
2. Recherchez l'application **CIRA Canadian Shield**.
3. Téléchargez et installez l'application.
4. Ouvrez l'application, suivez les instructions à l'écran pour l'activer et l'autoriser à installer son **profil de configuration VPN/DNS** dans les réglages.

Recommandé pour sa facilité. Elle se configure toute seule.

Dans les 2 options, vous êtes protégés dès l'ouverture du iPhone et même lorsqu'il est verrouillés. Si vous cliquez sur un lien frauduleux présent dans un texto vous êtes protégés.

L'installation du bouclier sur une tablette ou un cellulaire Android



Les menus sur Android peuvent légèrement varier selon la marque (Samsung, Google Pixel, Motorola, etc.) et la version du système, mais le chemin d'accès général reste le même.

1. Ouvrez les **Paramètres** (l'application avec l'icône d'engrenage) de votre téléphone ou de votre tablette Android.
2. Appuyez sur **Réseau et Internet** (ou *Connexions / Sans fil et réseaux* selon les fabricants).
3. Recherchez et appuyez sur **DNS privé** (souvent situé dans les paramètres avancés ou de liaison).
4. Par défaut, l'option est souvent sur *Automatique*. Sélectionnez plutôt **Nom d'hôte du fournisseur DNS privé**.

L'installation du bouclier sur une tablette/cellulaire Android (suite)



5. Dans la case qui apparaît, entrez l'adresse web sécurisée:
« protected.canadianshield.cira.ca »
6. Appuyez sur **Enregistrer**. La protection est immédiatement active sur toutes vos applications et navigateurs mobiles.

L'option « **DNS privé** » par nom d'hôte est très utile car elle s'applique en quelques secondes à tout l'appareil, sans avoir à manipuler de complexes adresses IP chiffrées.

Sources pour cette présentation



Mes sources ont été Gemini et le site du bouclier canadien de CIRA:

<https://www.pensezcybersecurite.gc.ca/fr/blogues/le-bouclier-canadien-de-cira-enfiler-votre-armure-de-cybersecurite>

Et également: <https://www.cira.ca/fr/> (Note: Si vous êtes sur la version anglaise, faite défiler vers le bas pour voir apparaître le bouton de la version française)

<https://www.cira.ca/fr/canadian-shield/>

Suggestion : Pour plus d'information : Questionnez votre IA en commençant avec un prompt similaire à celui-ci :

"internet: que penses tu du pare-feu nommé "bouclier canadien" conçu par CIRA?"

Complément d'Informations



Pour les personnes intéressées en connaître un peu plus, j'ai joint aux pages suivantes diverses informations sur le sujet.

Provenance de la liste d'adresse frauduleuses de CIRA



Pour constituer sa liste de blocage, l'organisme s'appuie sur :

- **Le Centre canadien pour la cybersécurité (CCCS) :** Des renseignements canadiens sur les arnaques et menaces ciblant spécifiquement le Canada (ex. faux SMS d'Impôt Canada, hameçonnage des banques canadiennes).
- **Des bases de données de cybersécurité internationales :** Pour bloquer les maliciels, rançongiciels mondiaux connus à travers le monde.

Tableau comparatif CIRA Cloudflare et Google DNS



Voici un **comparatif sommaire**

CIRA (Bouclier canadien) : Exploité par l'Autorité canadienne pour les noms de domaine (.CA). C'est une solution axée sur la **souveraineté des données au Canada**, la **confidentialité** et la **sécurité proactive** (blocage des menaces).

Cloudflare (1.1.1.1) : Axé sur la **vitesse ultra-rapide** et la **confidentialité**. Il dispose également de déclinaisons pour filtrer les maliciels (1.1.1.2) ou le contenu adulte (1.1.1.3).

Google Public DNS (8.8.8.8) : Axé sur la **stabilité globale** et le **temps de disponibilité (uptime)**, mais sans aucun filtrage de sécurité natif et avec une collecte de données d'usage sous l'écosystème Google.

Tableau comparatif CIRA Cloudflare et Google DNS



Critère	CIRA (Bouclier canadien)	Cloudflare (1.1.1.1)	Google DNS (8.8.8.8)
Souveraineté des données	Strictement canadienne (Serveurs et données maintenus au Canada)	Mondiale (Réseau CDN mondial)	Mondiale (Infrastructures Google)
Confidentialité / Logs	Excellente (OBNL canadien, aucune vente de données)	Excellente (Journaux effacés/anonymisés sous 24h, audité)	Moyenne (Utilisé pour l'analyse technique, conservé selon leurs politiques)
Sécurité & Filtrage	Inclus par défaut (Protégé : Phishing/Malware ; Famille : Contenu adulte)	Optionnel via des IP dédiées (1.1.1.2 / 1.1.1.3)	Aucun filtrage (Ne bloque ni phishing ni maliciels)
Performance / Latence	Très rapide au Canada (Nœuds canadiens)	Ultra-rapide (Souvent le plus rapide mondialement)	Très rapide et extrêmement stable
Chiffrement (DoH / DoT)	Oui (DoH et DoT supportés)	Oui (DoH et DoT supportés)	Oui (DoH et DoT supportés)

Tableau comparatif CIRA Cloudflare et Google DNS (Suite)



Confidentialité et Juridiction

CIRA : C'est le point fort du Bouclier canadien. Vos requêtes DNS restent soumises aux lois canadiennes sur la protection de la vie privée. Comme CIRA est un organisme à but non lucratif, il n'a aucun modèle d'affaires axé sur la publicité ou la monétisation de données.

Cloudflare : S'engage à ne pas conserver de données permettant d'identifier votre IP personnelle au-delà de 24 heures et fait auditer ses pratiques de confidentialité. Cependant, les données passent par une infrastructure internationale basée aux États-Unis.

Google : Bien que Google n'utilise pas directement le trafic de son DNS public pour cibler des publicités personnalisées, l'entreprise collecte des données télémétriques et d'utilisation. Pour la confidentialité stricte, c'est généralement le choix le moins recommandé.

Tableau comparatif CIRA Cloudflare et Google DNS (Suite)



Détection et pertinence des menaces

CIRA Protégé (149.112.121.20) Utilise des données de cyber-renseignement internationales (comme Canadian Centre for Cyber Security / Centre canadien pour la cybersécurité). Il est particulièrement efficace contre les **escroqueries et attaques d'hameçonnage ciblant spécifiquement les Canadiens** (ex. faux sites d'institutions financières canadiennes, fausses alertes d'impôts).

Cloudflare 1.1.1.2 : S'appuie sur le réseau mondial géant de Cloudflare (qui protège une grande partie du Web mondial). Sa force réside dans la détection en temps réel des **menaces mondiales à très grande échelle** (botnets internationaux, attaques de maliciels mondiales).

Google : Ne réalise aucun filtrage préventif (8.8.8.8 résoudra la requête même s'il s'agit d'un site d'hameçonnage connu).



Protocole de chiffrement (DoH / DoT)

Les trois services DNS supportent **DNS-over-HTTPS (DoH)** et **DNS-over-TLS (DoT)**, ce qui permet de chiffrer le trafic entre votre appareil/routeur et le serveur DNS, empêchant votre fournisseur d'accès Internet (FAI) de lire vos requêtes.

Des questions?

