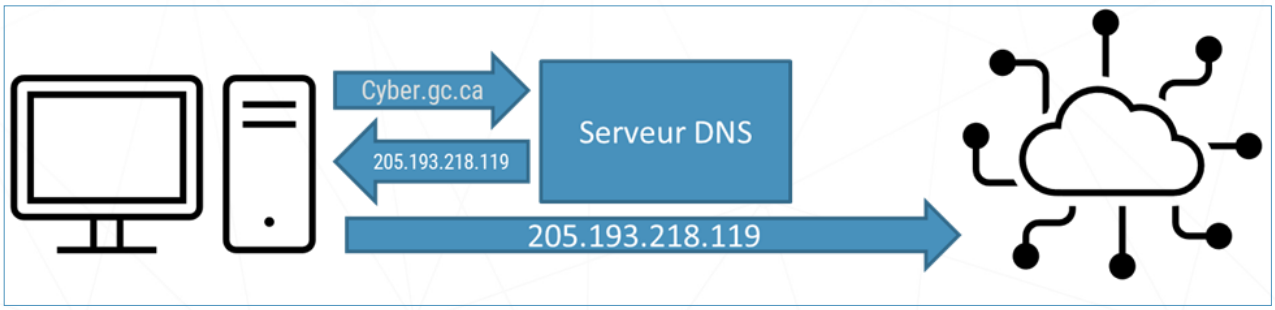
# SYSTÈME D'ADRESSAGE PAR DOMAINE (DNS) DE PROTECTION

MARS 2022 ITSAP.40.019

Les auteurs de menace utilisent fréquemment les connexions à des domaines Web malveillants pour compromettre davantage les systèmes et les données d'une victime. Selon des rapports de l'industrie, il est estimé que de 80 à 90 % des cyberattaques exploitent le système d'adressage par domaine (DNS pour Domain Name System). Si un auteur de menace parvient à vous convaincre, ou à convaincre un membre de votre organisation, de vous connecter à un site Web malveillant, il peut infecter votre réseau et vos appareils à l'aide d'un maliciel ou voler vos données.

## EN QUOI CONSISTE LE DNS?

Le DNS est un protocole qui traduit des adresses Web conviviales, comme « cyber.gc.ca », en adresses IP lisibles par machine. Il est souvent appelé le carnet d'adresses d'Internet. Le DNS est utilisé à la fois pour les actions lancées par l'humain (comme consulter un site Web) et pour les actions lancées par la machine (comme exécuter une mise à jour). Ce processus de traduction se nomme la résolution DNS. Les requêtes DNS sont nécessaires pour réaliser presque toutes les activités en ligne ou sur les applications réseau de votre organisation. Un DNS de protection peut être utile à votre organisation autant qu'à vous, à titre d'utilisateur public.




## QU'EST-CE QU'UN DNS DE PROTECTION?

Un DNS de protection (PDNS pour *Protective Domain Name System*) ou coupe-feu DNS (*DNS Firewall*) est un outil que votre organisation peut déployer pour empêcher les employés d'accéder par mégarde à des domaines potentiellement malveillants sur Internet. Les domaines malveillants figurant sur les listes de rejet d'une PDNS sont établis à partir d'une grande variété de sources de renseignement sur les cybermenaces. Ces listes de rejet contiennent tous les domaines auxquels les utilisateurs ne peuvent pas accéder lorsqu'ils utilisent des actifs TI organisationnels ou lorsqu'ils sont connectés à des réseaux de votre organisation. Un PDNS assure normalement une protection contre les quatre types de domaines suivants les domaines d'hameçonnage, les domaines de commandement et de contrôle de maliciel, les domaines d'algorithme de génération de noms de domaine, et les domaines de filtrage de contenu.

## NORMES DE CHIFFREMENT DNS

Dans le protocole DNS, deux options sont offertes pour chiffrer le trafic et les requêtes DNS : DNS par HTTPS (DoH pour *DNS over HTTPS*) et DNS par TLS (DoT pour *DNS over TLS*). Ces deux protocoles visent à augmenter la confidentialité des données des utilisateurs et à prévenir la consultation et la manipulation des données DNS. Ils peuvent tous deux fournir une protection contre certaines cyberattaques, comme les attaques de l'intercepteur. Pour déterminer lequel de ces deux protocoles, DoT ou DoH, sera mis en œuvre dans votre organisation, vous devriez comparer les risques et les avantages de chacun.

### DoT

Protocole permettant de chiffrer la résolution DNS par l'intermédiaire du protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*).

### DoH

Protocole permettant d'assurer la résolution DNS à distance par l'intermédiaire du protocole de transfert hypertexte sécurisé (HTTPS pour *Hypertext Transport Protocol Secure*).

Pour plus de détails sur les normes de chiffrement DNS, veuillez consulter la page Web *Protective DNS for the private sector* (en anglais seulement) du National Cyber Security Centre.

**SÉRIE SENSIBILISATION**



No de cat. D97-1/40-019-2022F-PDF
ISBN 978-0-660-42361-6

## AVANTAGES D'UN DNS DE PROTECTION

En déployant un DNS de protection dans votre organisation, vous ajoutez une couche de défense contre les domaines malveillants et les cyberattaques, y compris l'hameçonnage et les rançongiciels. Un PDNS procurera également à votre organisation les avantages suivants :

- Informer les utilisateurs au sujet des liens potentiellement malveillants afin qu'ils soient en mesure de les repérer et de les éviter.
- Détecter les menaces possibles pour vos réseaux, systèmes et appareils, et vous donner plus de temps pour mettre en place desmesures d'atténuation appropriées.
- Protéger les appareils mobiles là où la protection antivirus et antimaliciel traditionnelle ne s'applique peut-être pas.
- Offrir une meilleure protection si votre organisation a adopté le modèle « prenez vos appareils personnels (PAP).
- Protéger les utilisateurs contre les sites malveillants lorsqu'ils insèrent une erreur typographique dans une adresse URL de navigateur Web.
- Protéger les utilisateurs contre les sites Web qui ont été compromis par des auteurs de menace à l'insu des propriétaires de domaine, à condition que les domaines aient été signalés comme malveillants.

## SERVICES DNS DE PROTECTION GRATUITS ET PAYANTS

Au Canada, on retrouve des services PDNS gratuits et payants. Les services PDNS gratuits sont généralement commercialisés pour un usage personnel et à domicile. L'Autorité canadienne pour les enregistrements Internet (ACEI) offre un service DNS de protection public et gratuit, le Bouclier canadien, pour veiller à ce que les appareils personnels utilisent toujours un DNS fiable qui filtre les domaines Web malveillants. Le Bouclier canadien peut être configuré sur votre routeur ou votre passerelle à la maison afin d'assurer une meilleure protection de votre réseau.

Les services PDNS payants sont habituellement conçus et commercialisés pour les organisations. Les petites et moyennes organisations peuvent se procurer ces services auprès de fournisseurs canadiens.

## COMMENT CHOISIR UN FOURNISSEUR?

Lorsque vous choisissez un fournisseur de services PDNS pour votre réseau domiciliaire ou organisationnel, vous devriez prendre en considération les aspects suivants.

- Faites vos recherches au sujet des fournisseurs pour vous assurer qu'ils ont une solide réputation et peuvent démontrer leur expérience en cybersécurité.
- Procurez-vous des services PDNS auprès de fournisseurs qui vous permettent de voir les domaines qui sont placés sur les listes de rejet dans votre organisation.
- Demandez aux fournisseurs de vous fournir des études de cas ou des exemples où leurs services ont permis de protéger une organisation contre une cybermenace.
- Vérifier si le fournisseur ou un tiers exécute régulièrement des tests de sécurité sur son infrastructure.
- Vérifiez si le fournisseur donne accès à vos données de requêtes DNS à une interface de programmation d'application (API pour *Application Programming Interface*), y compris s'il offre l'intégration de la sécurité à l'aide de produits tels que les systèmes de gestion des informations et des événements de sécurité (GIES).
- Assurez-vous que le service du fournisseur sera compatible avec de multiples systèmes et appareils, particulièrement les appareils mobiles et PAP (au besoin).
- Établir si le fournisseur publie ses propres résultats et rapports de certification et de tests de sécurité.
- Renseignez-vous au sujet des analyses des services PDNS du fournisseur et de ses sources de renseignement sur les menaces.

Pour en savoir plus sur la sélection d'un fournisseur de services PDNS, veuillez consulter le document intitulé *Selecting a Protective DNS Service* (en anglais seulement) de la National Security Agency (NSA) et de la Cybersecurity & Infrastructure Security Agency (CISA).

### RENSEIGNEMENTS SUPPLÉMENTAIRES

- *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)*
- *Reconnaître les courriels malveillants (ITSAP.00.100)*
- *Avez-vous été victime de cybercriminalité? (ITSAP.00.037)*
- *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)*

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.