Recommandation

SUR LE DÉPLOIEMENT D'UN SERVEUR MANDATAIRE WEB FILTRANT

Version adoptée le 29 janvier 2026

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Introduction

Objet et contexte

Cette recommandation a pour objectif d'accompagner les responsables de traitement dans la mise en œuvre d'un serveur mandataire web filtrant (filtrage d'URL et détection et blocage des charges malveillantes[1]) conforme au règlement général sur la protection des données (RGPD). Elle vise également à accompagner les fournisseurs de solutions dans la mise en œuvre de bonnes pratiques concernant ces outils de sécurité.

Les solutions de filtrage web visent à répondre à des enjeux cruciaux de cybersécurité, en permettant notamment :

- de prévenir l'accès à des sites illicites ou inappropriés, qu'il s'agisse de contenus illégaux (pédopornographie, terrorisme), frauduleux et malveillants (hameçonnage) ou de sites web dont l'accès serait interdit ou restreint par l'employeur ;
- de réduire les risques liés aux cyberattaques, notamment par hameçonnage ou rançongiciel.

Périmètre d'application de la recommandation

Cette recommandation **s'applique** aux responsables de traitement, employeurs publics ou privés, qui déploient un serveur mandataire web filtrant pour l'accès à Internet professionnel de leurs employés, agents ou prestataires. Elle s'applique également dans le cadre d'un accès Wi-Fi professionnel mis à disposition, dans leurs locaux, au bénéfice de personnes externes (consultants externes ou partenaires), y compris lorsque ces dernières ne peuvent être identifiées (visiteurs par exemple).

Elle **ne s'applique pas** aux accès Internet publics ouverts à tous, mis en place par des commerçants, des médiathèques ou d'autres organismes (publics comme privés) à destination du public.

Portée de la recommandation

Cette recommandation n'a pas de caractère contraignant et ne préjuge pas des obligations légales applicables aux responsables de traitement qui existent par ailleurs, en particulier celles issues du code du travail, notamment les articles L1121-1 et L2312-38.

2. Qu'est-ce qu'un serveur mandataire web filtrant ?

Un serveur mandataire web filtrant, selon le guide de l'ANSSI « *Recommandations relatives à l'interconnexion d'un SI à Internet* »[2], est un dispositif ou un service relais entre l'équipement client (poste de travail) et le serveur web (sur Internet). Son rôle principal est de bloquer ou restreindre l'accès à certains sites web ou catégories de contenus pour des raisons de sécurité du système d'information (SI) et de conformité (par exemple, le blocage des accès aux sites web malveillants, illicites ou non conformes à la politique d'entreprise, le respect des principes de droit commun ou de règlementations sectorielles).

La recommandation ne couvre pas la question de l'analyse de flux sortants et de solutions de prévention des pertes de données (solutions *DLP* pour *Data Loss Prevention* en anglais) ni de

[1] Charge malveillante ou code malveillant : tout programme développé dans le but de nuire à/ou au moyen d'un système informatique ou d'un réseau ; maliciel/logiciel malveillant.

[2] Recommandations relatives à l'interconnexion d'un SI à Internet, v3.0, chapitre 4, cyber.gouv.fr

solutions de protection des applications web exposées sur Internet (tel que les solutions WAF pour *Web Application Firewall*).

Les fonctions généralement constitutives d'un serveur mandataire web filtrant sont :

Filtrage web :

- Bloquer, restreindre ou autoriser l'accès à des sites spécifiques en se basant sur leur catégorisation, celle-ci pouvant notamment être adossée à des listes de blocage (en anglais *blacklists*) ou des listes d'autorisation (en anglais *whitelists*) d'URL.
- Attribuer un profil aux employés avec les catégories (définies et mises à jour régulièrement par l'éditeur telles que commerce en ligne, voyage, réseaux sociaux, plateformes de jeux en ligne, contenu pour adultes) de sites autorisés ou interdits qui leurs sont appliquées, selon les besoins de sécurité et les besoins opérationnels du responsable de traitement. Par exemple, il pourrait être décidé que l'ensemble des employés ne doit pas avoir accès aux sites de vidéos à la demande (*streaming*), ou que seules les équipes « achats » doivent avoir un profil leur autorisant l'accès aux plateformes de vente en ligne.

Détection et blocage :

- Déchiffrer le trafic HTTPS[3] et inspecter les flux HTTP pour pouvoir accéder au contenu des requêtes et des réponses pour détecter les charges malveillantes dans le trafic web chiffré.
- Scanner le trafic web HTTP pour détecter et bloquer les pages web et les fichiers téléchargés malveillants afin de protéger l'utilisateur de menaces émanant du serveur web demandé.

Journalisation de la navigation web :

- Enregistrer les requêtes web des utilisateurs pour des raisons de conformité et de sécurité.
- Analyser en temps réel les traces pour prévenir et bloquer des cyberattaques ou conserver les journaux afin de permettre la réalisation d'une analyse suite à un incident de sécurité.

3. Finalités du Traitement

La finalité du traitement est l'objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime. Les opérations relevant des fonctionnalités réalisées dans le cadre du serveur mandataire web filtrant, décrites ci-dessus, sont considérées comme déterminées et légitimes si elles ont pour finalités :

- le respect des exigences réglementaires en matière de cybersécurité (notamment l'article 32 du RGPD) ;
- la protection des systèmes d'information contre les cybermenaces ;
- la prévention des accès à des sites web illégaux, non conformes à la politique de l'organisme ou à des sites malveillants.

Les données traitées à ces fins ne doivent pas être réutilisées pour de nouvelles finalités qui seraient incompatibles avec ces objectifs initiaux.

La CNIL rappelle que la mise en œuvre de ces traitements ne doit pas conduire à une surveillance excessive de l'activité des salariés qui serait contraire, notamment, au RGPD.

[3] Analyse de flux https : bonnes pratiques et questions, 31 mars 2015, cnil.fr

4. Base légale du traitement

Pour pouvoir être mis en œuvre, tout traitement de données à caractère personnel doit se fonder sur l'une des bases légales prévues par le RGPD. Dans ce cadre, les bases légales suivantes pourront notamment être retenues.

Le traitement qui vise à garantir les finalités décrites ci-dessus peut reposer sur l'**intérêt légitime** du responsable de traitement (article 6.1.f du RGPD). Il appartiendra alors notamment au responsable de traitement de mettre en balance ses intérêts propres et ceux des personnes concernées.

Il est important de souligner que la base légale de l'obligation légale n'est mobilisable que pour des textes prévoyant cette obligation de manière explicite. En particulier, les articles 5.1.f et 32 du RGPD qui prévoient une obligation de sécurité ne devraient pas engendrer à eux seuls une obligation légale de mettre en place un serveur mandataire web filtrant dans le cadre de traitements de données à caractère personnel.

5. Réalisation d'une AIPD

La nécessité d'une analyse d'impact relative à la protection des données (AIPD) pour une solution de serveur mandataire web filtrant dépend de plusieurs facteurs liés aux fonctionnalités retenues et à leurs usages. Il convient de se référer aux lignes directrices du Comité européen de la protection des données (CEPD) pour déterminer les cas où la réalisation d'une AIPD est obligatoire[4].

Le responsable de traitement devrait réaliser une AIPD si les traitements du serveur mandataire web filtrant remplissent au moins deux des critères suivants :

- collecte de données sensibles ou données à caractère hautement personnel ;
- collecte de données personnelles à large échelle ;
- personnes vulnérables5 ;
- surveillance systématique.

Au-delà de son caractère obligatoire, la CNIL estime que la réalisation d'une AIPD devrait être une bonne pratique permettant de formaliser la justification des choix réalisés et, ainsi, d'identifier et traiter les risques juridiques et techniques. La réalisation d'une AIPD permettra de recueillir l'avis du délégué à la protection des données (DPO), lorsqu'il a été désigné, avant la mise en place du dispositif.

6. Proportionnalité du traitement

Il incombe au responsable de traitement de s'assurer de la proportionnalité des opérations envisagées au regard des finalités poursuivies.

Par ailleurs, afin de garantir la transparence et une prise en compte équilibrée des intérêts en jeu, la CNIL recommande aux responsables de traitement d'associer systématiquement les comités sociaux (CSE/CSA), y compris dans les cas où elle n'est pas obligatoire et le DPO, à ce questionnement. Une information/consultation préalable de ces derniers dans le cadre d'une analyse concertée de la

[4] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 octobre 2017, cnil.fr

[5] Les lignes directrices du CEPD précisent que les employés peuvent être considérés comme des personnes concernées vulnérables en raison du déséquilibre des pouvoirs accru qui existe entre elles et le responsable du traitement (l'employeur).

solution de filtrage web envisagée (et de conservation des journaux d'accès) favorise l'évaluation de la proportionnalité du dispositif préalablement à sa mise en œuvre. Elle contribue également à identifier les éventuels risques, à déterminer les mesures d'atténuation appropriées (mise en place de listes noires, listes blanches et listes d'exceptions) et identifier les modalités d'information des personnes concernées.

7. Minimisation des données

Conformément aux articles 5 et 25 du RGPD notamment, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

En l'espèce, les données collectées devraient être strictement limitées aux éléments nécessaires aux fonctionnalités de filtrage et de journalisation.

Si une charge malveillante est détectée, la conservation du contenu des requêtes initiales peut être justifiée par le besoin d'identification de la menace afin de protéger le système d'information du responsable de traitement. À titre d'exemple, les données suivantes peuvent en principe être collectées et traitées :

Catégories de données collectées :

- l'identité de l'utilisateur (gestion des accès web des utilisateurs ou authentification sur le proxy web filtrant) ;
- l'adresse IP du poste de l'utilisateur ;
- tout ou partie de l'URL consultée ;
- l'horodatage de l'accès ;
- la catégorie de site visité ;
- l'action (autorisé, bloqué, forcé et/ou ajout demandé – si ces dernières possibilités sont offertes aux utilisateurs).

La CNIL attire l'attention des responsables de traitement et des sous-traitants sur le fait que l'URL complète, accessible lors d'un déchiffrement HTTPS, est susceptible de donner accès à des données à caractère personnel. En conséquence, ces opérations nécessitent la mise en œuvre de garanties particulières (cf. infra).

S'agissant des données d'accès remontées à l'offreur de solution dans un but de catégorisation, celles-ci devraient être limitées au nom de domaine et non à l'adresse URL en intégralité.

Listes d'exceptions et déchiffrement HTTPS

Les responsables de traitement devraient configurer des listes d'exceptions excluant le déchiffrement HTTPS des sites ne présentant pas de risques spécifiques en vue de limiter les données à caractère personnel qui pourraient être conservées lors de la journalisation des accès par la solution de filtrage (par exemple les sites de banques, de santé et les administrations publiques). En complément de la création d'une telle liste statique, un processus de validation et d'ajout de nouvelles URL faisant suite à une demande d'un employé (par exemple, pour le besoin d'ajout d'une URL spécifique nécessaire à l'exercice de ses fonctions) pourra être mis en place.

Déchiffrement HTTPS

Les solutions de filtrage d'URL peuvent nécessiter le déchiffrement HTTPS pour détecter des fichiers malveillants.

Ces opérations présentent des risques pour la vie privée dans la mesure où elles entraînent la rupture d'un canal sécurisé et exposent des données en clair au niveau de l'équipement en charge de l'opération. Elles doivent, à ce titre, faire l'objet d'une attention particulière.

Ainsi, lorsqu'un déchiffrement est nécessaire, celui-ci ne devrait être réalisé que sur les domaines non listés dans les listes d'exceptions et les données échangées dans les requêtes HTTPS ne devraient pas être conservées (à moins qu'une charge malveillante soit détectée).

Enfin, sa mise en œuvre doit s'accompagner de nombreuses précautions de sécurité, telles que listées dans les recommandations[1] de sécurité concernant l'analyse de flux HTTPS proposées par l'ANSSI.

8. Durée de conservation et journalisation

Le responsable de traitement devra définir une durée de conservation des journaux proportionnée au besoin. Une durée supérieure aux préconisations de la CNIL[6] (6 mois à 1 an) doit être justifiée et documentée.

9. Information et droits des personnes concernées

Le responsable de traitement doit informer les personnes concernées (employés ou visiteurs) des traitements mis en œuvre conformément à l'article 13 du RGPD.

S'agissant des serveurs mandataires web filtrant, cette information pourrait notamment venir alimenter le règlement intérieur de l'organisme employeur, par exemple sous forme d'une charte informatique annexée, après un passage devant les comités sociaux (CSE/CSA) et le DPO, s'il existe.

L'information devant être individuelle, il est recommandé aux organismes de la porter à la connaissance de chaque utilisateur du SI, *a minima* à son arrivée. Cette information peut être réalisée par voie de messagerie électronique professionnelle, lorsque celle-ci est disponible, pour faciliter la preuve de sa réalisation. Cette preuve peut également se matérialiser par la signature de la charte informatique.

Les informations à communiquer doivent comprendre l'ensemble des éléments énumérés à l'article 13 du RGPD[7] dans un langage accessible. Cette information pourra être renouvelée régulièrement, notamment en cas de modification substantielle.

Par ailleurs et étant donné les spécificités des serveurs mandataires web filtrant, le responsable de traitement devrait s'assurer, au titre de l'article 12-1 du RGPD, de porter à la connaissance des personnes concernées non seulement l'existence du traitement de filtrage web, mais aussi des précisions sur le fonctionnement pratique du dispositif et notamment :

---

[6] Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, cnil.fr

[7] Plusieurs contenus ont été mis en ligne sur le site de la CNIL afin d'accompagner les responsables de traitement dans la rédaction de tels contenus tel que : Conformité RGPD : comment informer les personnes et assurer la transparence ? 29 juillet 2019, cnil.fr

- les catégories de sites exclus du déchiffrement HTTPS via des listes d'exceptions ;
- le fait que, dans une situation de télétravail, l'utilisateur est également amené à passer par le serveur mandataire web filtrant ;
- l'absence de conservation des contenus échangés (requêtes HTTP, données à caractère personnel contenues dans les URL telles que mot de passe, identifiant, etc.) excepté dans le cas de la détection d'une charge malveillante.

Enfin, l'ensemble des personnes dont les données seront traitées, doivent disposer de droits prévus par le RGPD, en particulier celui d'accès[8].

10. Modalités de déploiement et recommandations

Il est possible d'envisager le déploiement de la solution de serveur mandataire web filtrant selon différentes modalités :

- Infrastructure à la main exclusive du responsable de traitement (déploiement sur site ou sur un espace d'informatique en nuage (*cloud*) privé) ;
- *Software as a Service* (*SaaS*) qui permet d'utiliser des applications logicielles en ligne sans en avoir à en gérer l'infrastructure ;
- Hybride (requêtes dans l'informatique en nuage (*cloud*) de la solution déployée en interne pour bénéficier en temps réel des dernières URL catégorisées par l'éditeur seulement dans le cas où une URL requêtée par l'employé ne serait pas présente dans la base locale). Cette solution est pertinente notamment pour obtenir les dernières URL des sites d'hameçonnage, très fréquemment dupliquées en masse.

Le déploiement d'une solution de serveur mandataire web filtrant dans ces différentes modalités peut entraîner des différences notables en termes de protection des données et de conformité au RGPD.

En particulier, si **une solution en *SaaS*** peut présenter un certain nombre d'avantages, elle est susceptible d'entraîner des risques spécifiques qu'il revient au responsable de traitement de maîtriser via des mesures adéquates au titre de la protection des données dès la conception et par défaut (article 25 du RGPD), notamment dans les phases de configuration de la solution ainsi déployée.

À cet égard, la CNIL recommande en particulier de :

- prévoir les clauses prévues à l'article 28 pour encadrer le traitement des données par le fournisseur, agissant comme sous-traitant au sens du RGPD ;
- vérifier et encadrer les transferts éventuels de données hors de l'UE, liés notamment à l'accès par le sous-traitant aux données à caractère personnel résultant d'un déchiffrement HTTPS le cas échéant ;
- s'assurer de la possibilité de récupérer les *logs* en cas d'audit ;
- s'assurer de la sécurité du fournisseur pour prévenir le risque de violations de données (par exemple : fuite de *logs* contenant des informations personnelles d'utilisateurs) ;
- vérifier que les *logs* collectés en local et les informations envoyées à l'éditeur respectent la minimisation des données. Notamment, en cas de déploiement d'un client sur les postes des utilisateurs : mettre en place des mesures de pseudonymisation des données envoyées au sous-traitant, comme l'obfuscation des identifiants, ou des mécanismes de tokenisation des *logs* avant transmission dans l'informatique en nuage (*cloud*) ;

[8] CEPD, « Lignes directrices 01/2022 sur les droits des personnes concernées — Droit d'accès » du 28 mars 2023.

- clarifier dans la documentation interne les flux de données et les responsabilités entre l'entreprise et le fournisseur *SaaS*.

S'agissant d'un **déploiement hybride**, la CNIL recommande en outre de sécuriser les échanges entre la solution déployée par le responsable de traitement sur son système d'information et l'éditeur de la solution (notamment dans le cas d'échanges nécessités par la récupération des mises à jour d'URL) en veillant à s'appuyer sur un chiffrement des flux.

11. Sécurité de la solution de filtrage et de journalisation des accès

En vue de sécuriser la solution de filtrage web et la solution de journalisation des accès, le responsable de traitement devra notamment tenir compte des recommandations ci-dessous.

Filtrage web

S'agissant du filtrage, la CNIL recommande :

- pour une solution déployée sur site, que seuls les noms de domaine des sites web bloqués et non catégorisés soient remontés à l'éditeur en vue de leur analyse, sans rattachement à la personne concernée par la tentative d'accès au site ;
- de limiter la possibilité pour le fournisseur d'identifier les utilisateurs de la solution de filtrage, cette capacité devant être autant que possible réservée au responsable de traitement lui-même. La pseudonymisation des données des utilisateurs peut permettre de répondre à cet enjeu, notamment lorsque la solution est déployée en mode *SaaS*.

Journalisation de la navigation web

S'agissant de la journalisation, la CNIL recommande de mettre en place, en plus de la recommandation journalisation[9] émise par la CNIL :

- la signature d'une clause de confidentialité des administrateurs de la solution ;
- un stockage des journaux dans un environnement garantissant leur intégrité et leur confidentialité ;
- un accès aux journaux restreint à des administrateurs dûment habilités ;
- une authentification multifacteur[10] pour les accès administrateurs à la solution.

[9] Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, cnil.fr

[10] Recommandation relative à l'authentification multifacteur, 20 mars 2025, cnil.fr