DAT-NT-20/ANSSI/SDE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 4 février 2015

N° DAT-NT-20/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 41

# Note technique

# Recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows

**Public visé:**

| | |
|---|---|
| Développeur | |
| Administrateur | ✓ |
| RSSI | ✓ |
| DSI | ✓ |
| Utilisateur | ✓ |

# Informations

**Avertissement**

Ce document rédigé par l'ANSSI présente les **« Recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows »**. Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

**Personnes ayant contribué à la rédaction de ce document:**

| Contributeurs | Rédigé par | Approuvé par | Date |
|---|---|---|---|
| BSS, SIS, LRP | BSS | SDE | 4 février 2015 |

**Évolutions du document :**

| Version | Date | Nature des modifications |
|---|---|---|
| 1.0 | 15 janvier 2015 | Version initiale. |
| 1.1 | 4 février 2015 | - assouplissement de image_src_set et ssl.require_safe_negotiation<br>- complément d'information concernant ESR |

**Pour toute remarque:**

| Contact | Adresse | @mél | Téléphone |
|---|---|---|---|
| Bureau Communication de l'ANSSI | 51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP | communication@ssi.gouv.fr | 01 71 75 84 04 |

# Table des matières

# 1 Préambule

Firefox est le navigateur web en sources ouvertes édité par la fondation Mozilla et dont la première version stable date de 2004. Rapidement devenu l'un des navigateurs les plus utilisés par les internautes [1], il est aujourd'hui soutenu par une importante communauté de développeurs du monde libre.

Firefox dispose d'un mécanisme de mise à jour automatique et peut être configuré de manière centralisée. Il se prête bien à une utilisation professionnelle. De par son haut degré de paramétrage et son code en sources ouvertes, il peut également s'adapter à des environnements au sein desquels les contraintes techniques sont importantes.

Cette note technique vise à sensibiliser le lecteur aux enjeux de sécurité d'un navigateur Web et doit le guider dans la mise en œuvre d'une stratégie de sécurisation spécifique à Firefox dans le cadre d'une configuration centralisée et sécurisée en environnement Active Directory.

# 2 Enjeux de sécurité d'un navigateur Web

Comme tout composant logiciel utilisé pour accéder à Internet, les navigateurs sont une cible privilégiée des attaquants du fait des vulnérabilités qu'ils présentent et de leur utilisation régulière sur Internet. Viennent également s'ajouter les vulnérabilités propres aux différents modules complémentaires intégrés aux navigateurs et dont les processus de mise à jour sont généralement indépendants de ceux du navigateur.

L'atteinte en intégrité d'un poste de travail par le biais de son navigateur Web est intéressante du point de vue d'un attaquant étant donné qu'elle lui permet le plus souvent de contourner les mesures de sécurité liées à l'architecture réseau et aux différentes passerelles de filtrage. L'attaque réussie d'un poste utilisateur suffit généralement à l'établissement d'un canal de contrôle distant qui permettra par la suite de rebondir au sein du système d'information pour atteindre les biens essentiels de l'entité. La navigation Web est donc logiquement devenue un des principaux vecteurs d'attaque utilisés et, plus largement, un problème pour la sécurité des systèmes d'information.

Du point de vue de la sécurité, Firefox pâtit de l'absence de mécanisme de bac à sable (*sandbox* [2]) et d'architecture multi-processus, une vulnérabilité peut alors avoir un impact important. Comme tous les navigateurs, il fait régulièrement l'objet de vulnérabilités critiques [3].

# 3 Firefox versus Firefox ESR

Mozilla publie une version ESR (*Extended Support Release*) [4] de Firefox. Chaque version de Firefox ESR est maintenue pendant environ 1 an et n'a pour seules mises à jour que les correctifs de sécurité et de stabilité. Cette version de Firefox est destinée aux entités qui nécessitent un support étendu pour un déploiement en masse, évitant ainsi d'avoir à gérer des évolutions fréquentes du navigateur.

1. Sources : `www.atinternet.com` et `www.w3schools.com`.
2. Environnement d'exécution contrôlé et restreint.
3. Les multiples avis de sécurité et bulletins d'actualité relatifs aux principaux navigateurs peuvent être consultés sur le site du CERT-FR (`www.cert.ssi.gouv.fr`).
4. Pour plus d'informations : `http://mozilla.org/en-US/firefox/organizations/`.

Le tableau comparatif suivant présente les avantages et inconvénients de chaque version :

| Version | Avantages | Inconvénients |
|---|---|---|
| **Version standard** | Le navigateur évolue régulièrement et les utilisateurs disposent ainsi rapidement des nouvelles fonctionnalités qui font leur apparition. | Les équipes informatiques doivent régulièrement déployer les nouvelles versions de Firefox pour le maintenir en conditions de sécurité. Ces déploiements engendrent une charge de travail non négligeable puisqu'il est nécessaire de vérifier la compatibilité avec les applications Web internes, compléter la configuration centralisée vis-à-vis des nouvelles fonctionnalités, etc. |
| **Version ESR** | Les équipes informatiques n'ont pas à se soucier des évolutions fonctionnelles du navigateur. Une fois la dernière version majeure de Firefox ESR déployée, elles se contentent de garantir sa stabilité et son maintien en conditions de sécurité en déployant les correctifs publiés par Mozilla. Les cycles de vie des versions de Firefox ESR étant d'environ un an, les correctifs de sécurité sont publiés pendant toute cette durée de vie. | ESR ne dispose pas des nouvelles fonctionnalités qui apparaissent dans les versions successives de Firefox standard, le navigateur peut alors paraître pauvre en fonctionnalités du point de vue des utilisateurs. |

Au sein d'un système d'information administré de manière centralisée, il est donc plutôt conseillé de déployer la version ESR de Firefox. La présente note technique s'appuie sur le déploiement et la configuration de Firefox ESR dans sa version 31.

# 4 Maîtrise du navigateur

Les principaux enjeux d'un déploiement de navigateur au sein d'un système d'information sont sa sécurité et sa maîtrise. Pour cela, il est nécessaire de pouvoir contrôler sa configuration de manière centralisée, tout en procédant à des déploiements et à des mises à jour (automatiques ou non) selon la politique de mise à jour de l'entité et sans intervention de l'utilisateur.

Firefox ne prend pas nativement en charge la configuration par stratégies de groupes (GPO) en environnement Active Directory. Il est pour cela nécessaire de recourir à des extensions tierces. Il est en revanche possible de paramétrer le navigateur à l'aide de fichiers de configuration à déployer sur les postes des utilisateurs. Cette méthode présente l'intérêt d'être utilisable simplement, dans nombreux contextes, et aussi bien sous Linux que Windows sans distinction. Ces fichiers de configuration permettent également d'imposer des paramètres verrouillés et non modifiables par les utilisateurs.

| | |
|---|---|
| **R1** | Avant tout déploiement de Firefox au sein d'un système d'information, il est primordial de définir précisément une stratégie de paramétrage qui garantira l'utilisation du navigateur dans une configuration durcie et verrouillée. |

Il est important de commencer par clarifier les termes utilisés par Mozilla et ce qu'ils désignent. Le terme de « module » (*Add-on*) ou de « module complémentaire » inclut :

- les *plugins* ou greffons, qui sont des composants compilés ;
- les extensions (qui sont des composants en langage interprété comme XUL ou JavaScript) ;
- les thèmes (qui ne font l'objet d'aucune recommandation de sécurité) ;
- les modules de moteur de recherche.

Les recommandations de paramétrage figurant dans ce document sont données à titre indicatif dans l'optique d'une configuration durcie. Elles doivent donc être modulées selon les besoins propres à chaque entité et bien entendu selon le périmètre d'utilisation du navigateur (Internet, Intranet, etc.). Leur application ne doit pas se faire sans validation préalable. L'annexe I de ce document précise les paramètres de configuration permettant d'appliquer toutes les recommandations de configuration de Firefox indiquées dans ce document. En environnement professionnel, il est par ailleurs conseillé de déployer une telle configuration par GPP de manière centralisée comme expliqué en annexe II.

## 4.1 Choix des *plugins*

Les *plugins* Firefox ne peuvent être développés qu'à partir de l'interface de programmation NPAPI (*Netscape Plugin Application Programming Interface*). Cette architecture, qui date de Netscape, n'est pas sécurisée et exécute les *plugins* avec le niveau de privilège de l'utilisateur. Bien qu'il soit possible d'exécuter certains *plugins* dans un processus séparé (le *plugin-container*), cette séparation ne protège que le processus du navigateur d'un éventuel arrêt brusque de fonctionnement d'un *plugin*. Une vulnérabilité affectant un *plugin* permet en revanche de compromettre la session ou le système. Le *plugin* Flash Player fait toutefois exception en intégrant un mécanisme de bac à sable qui lui est propre (« Mode Protégé de Flash Player pour Firefox » [5]). Le processus Flash Player exécuté dans le *plugin-container* ne sert alors qu'à instancier des processus enfants auxquels s'appliquent des restrictions de sécurité plus importantes. Le *plugin* Flash continue toutefois de faire l'objet de vulnérabilités critiques [6].

| | |
|---|---|
| **R2** | Tout *plugin* ajouté à Firefox fait courir un risque de sécurité supplémentaire, il est alors important de les limiter au strict nécessaire. |

Note : Le risque induit par l'utilisation du *plugin Flash Player* peut être toléré dès lors que la lecture des contenus Flash constitue un besoin incontournable. Complété par la visionneuse PDF intégrée à Firefox (écrite en JavaScript), la prise en charge de ces deux types de contenus devrait suffire pour la plupart des usages.

L'ajout, la mise à jour, et la suppression de *plugins* pour Firefox de manière centralisée peut se faire simplement par base de registre [7]et par GPP (*Group Policy Preferences*).

## 4.2 Choix des extensions

Le mécanisme d'extension rend possible l'écriture de programmes (extensions) en langage interprété (XUL ou JavaScript entre autres) permettant l'ajout de fonctionnalités ou la personnalisation du navigateur. Contrairement aux *plugins* qui sont des programmes compilés, les extensions s'exécutent dans le processus du navigateur et sans système de permission permettant de restreindre les libertés qui leur sont accordées. Il convient donc d'être particulièrement vigilant étant donné les risques de sécurité non négligeables qu'elles introduisent.

5. http://blogs.adobe.com/security/2012/06/inside-flash-player-protected-mode-for-firefox.html.
6. Les multiples avis de sécurité peuvent être consultés sur le site du CERT-FR (www.cert.ssi.gouv.fr).
7. Un article de Mozilla explique l'ajout, la mise à jour, et la suppression d'extensions et de *plugins* pour Firefox par base de registre : https://developer.mozilla.org/en-US/docs/Adding_Extensions_using_the_Windows_Registry.

Ainsi, une extension malveillante pourrait accéder à des informations sensibles concernant la navigation de l'utilisateur puis les envoyer à un serveur illégitime sur Internet. Une extension peut également introduire de nouveaux comportements indésirables suite à une mise à jour. Rien ne laisse présager qu'une extension aujourd'hui non malveillante ne le sera pas demain. En parallèle, de nombreuses extensions présentent des vulnérabilités qui peuvent être exploitées (par le contenu des pages visitées ou encore, par courriels spécifiquement forgés et consultés par webmail). Ces extensions vulnérables peuvent également servir à exploiter, par rebond, les vulnérabilités d'éventuels *plugins* activés et ainsi obtenir un accès complet au système.

| **R3** | Ne déployer que des extensions de confiance et nécessaires aux besoins métiers. |
|---|---|

Note : Dans le cas d'extensions développées en interne, il convient de prêter une attention particulière à la sécurité de leur code [8].

L'ajout, la mise à jour et la suppression d'extensions pour Firefox de manière centralisée peut se faire simplement dans la base de registre et par GPP (*Group Policy Preferences*).

### 4.2.1 SSL/TLS et certificats

Firefox a comme particularité d'utiliser ses propres bibliothèques de gestion des échanges sécurisés client/serveur développées par la fondation Mozilla (bibliothèques NSS, *Network Security Services*), ce qui lui permet de disposer par exemple de son propre magasin de certificats et de sa propre liste de CRL (listes de révocations de certificats). Il est ainsi possible d'appliquer des restrictions spécifiques au navigateur sur certains certificats sans que cela ne s'applique au système d'exploitation dans son ensemble, ce qui le différencie d'autres navigateurs. Il est également possible de restreindre simplement les versions de protocoles SSL/TLS ainsi que les suites cryptographiques utilisées. Cette indépendance vis-à-vis du mécanisme fourni par le système d'exploitation lui confère une plus grande portabilité et une souplesse dans sa configuration SSL/TLS mais se traduit en contrepartie par une démarche de sécurisation plus complexe.

| **R4** | Désactiver l'utilisation de SSL et n'autoriser que les protocoles TLS v1.1 et supérieures (la v1.0 étant vulnérable). Pour aller plus loin, il est également possible de restreindre les suites cryptographiques utilisables en désactivant celles reposant sur des algorithmes obsolètes comme RC4. |
|---|---|

Note : Pour plus d'informations, le lecteur est invité à se référer à la section correspondante de l'annexe I ainsi qu'aux publications de l'ANSSI [9]. Par ailleurs, les suites n'utilisant pas de mécanismes de PFS (*Perfect Forward Secrecy*) devraient idéalement être désactivées elles aussi mais des difficultés de navigation seraient à prévoir sur Internet du fait de l' incompatibilité avec de nombreux serveurs Web.

Chaque utilisateur d'un poste de travail dispose de son propre profil Firefox. Les informations de sécurité relatives aux certificats sont stockées, pour chaque profil firefox, dans 3 fichiers :

- `cert8.db` (objets accessibles publiquement : certificats, CRLs, enregistrements S/MIME) ;
- `key3.db` (clés privées, mots de passe) ;
- `secmod.db` (informations de configuration des modules de sécurité).

8. L'article *Security best practices in extensions* expose certains fondamentaux à respecter pour le développement d'extension sécurisées : `https://developer.mozilla.org/en-US/Add-ons/Security_best_practices_in_extensions`.

9. La note « Recommandations de sécurité concernant l'analyse des flux HTTPS » est disponible à l'adresse : http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/authentification-et-mecanismes-cryptographiques/recommandations-de-securite-concernant-l-analyse-des-flux-https.html.
L'article « SSL/TLS : état des lieux et recommandations » est disponible à l'adresse : http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/ssl-tls-etat-des-lieux-et-recommandations.html.

L'accès aux fichiers `key3.db` et `cert8.db` non chiffrés d'un profil Firefox permet la récupération et la réutilisation des certificats utilisateurs qu'ils contiennent. Tout compte disposant de droits administrateurs sur un ordinateur a la possibilité de récupérer l'ensemble des fichiers `key3.db` et `cert8.db` qui y sont stockés (voire tout utilisateur non privilégié dans le cas d'un système de fichiers FAT32). La confidentialité des données utilisateurs n'est donc pas assurée dès lors que ces fichiers ne sont pas chiffrés. La définition d'un mot de passe principal déclenche le chiffrement du fichier `key3.db` par algorithme 3DES-CBC avec une clé dérivée de ce mot de passe. La sécurité apportée par une telle mesure reste modérée, des outils performants permettent de rapidement retrouver ce mot de passe maître par force brute. Le stockage du profil Firefox dans un conteneur chiffré par une solution qualifiée par l'ANSSI peut être, dans certains cas, la solution à privilégier.

| | |
|---|---|
| **R5** | Dès lors que des certificats utilisateurs sont stockés dans les magasins de certificats de Firefox, il est recommandé d'assurer la sécurité de leurs conteneurs de clés privées (fichiers `key3.db`) par chiffrement. |

Tout utilisateur de Firefox peut aussi ajouter des certificats serveurs et des autorités de confiance dans son propre magasin de certificats. Selon le contexte d'utilisation du navigateur, il peut donc être important de mettre en œuvre des mesures techniques permettant de maîtriser les magasins de certificats des profils Firefox et de s'assurer de leur conformité vis à vis de la stratégie de l'entité.

| | |
|---|---|
| **R6** | Maîtriser les magasins de certificats des profils Firefox et notamment les autorités de certification racines de confiance et les certificats serveurs qui y sont configurés. |

Note : l'application de cette recommandation est simple dès lors que les utilisateurs ne stockent pas de certificats utilisateurs dans leurs magasins de certificats Firefox, mais cela devient plus compliqué dans le cas contraire. La problématique est abordée plus en détail en annexe III.

Il à noter également que, depuis sa version 24, Firefox se détourne de l'usage classique des CRLs en ligne au profit d'une liste de révocations mise à jour régulièrement pour consultation locale. Les bibliothèques NSS supportent toujours la gestion des CRLs classiques (modifiables par l'outil `crlutil` et non plus par interface graphique) mais il est prévu qu'elles ne soient plus utilisées dans un avenir proche. Les autorités de certification sont d'ailleurs invitées à envoyer leurs certificats révoqués à Mozilla pour être intégrés à la liste de révocation maintenue par Mozilla [10].

### 4.2.2 Gestionnaire de mots de passe

Le gestionnaire de mots de passe de Firefox permet de mémoriser les mots de passe saisis dans les formulaires Web. Tout comme pour les magasins de certificats, l'utilisation d'un « mot de passe principal » [11] permet de chiffrer les mots de passe stockés par un algorithme 3DES-CBC avec une clé dérivée du mot de passe principal. La sécurité apportée par une telle mesure reste modérée, des outils performants permettent de rapidement retrouver ce mot de passe maître par force brute. L'utilisation d'un gestionnaire de mots de passe alternatif sécurisé est donc conseillé.

| | |
|---|---|
| **R7** | Il est conseillé de désactiver le gestionnaire de mots de passe pour imposer la saisie systématique de ces derniers. L'application d'un tel durcissement est légitime sur un réseau amené à traiter des données sensibles ou confidentielles, mais peut toutefois être difficile à imposer aux utilisateurs sur des réseaux moins sensibles. Sa désactivation pourrait alors s'accompagner du déploiement d'un gestionnaire de mots de passe alternatif et sécurisé [12]. |

10. Le Wiki de Mozilla détaille la problématique de révocation de certificats au sein de Firefox : https://wiki.mozilla.org/CA:ImprovingRevocation.

11. https://support.mozilla.org/fr/kb/utiliser-mot-passe-principal-proteger-identifiants.

#### 4.2.3 Confidentialité

Le lecteur est invité à prendre connaissance de la « déclaration de confidentialité de Firefox » [13]. Selon les fonctionnalités activées, diverses informations sont susceptibles d'être envoyées à Mozilla. La plupart sont en rapport avec :

- les informations liées aux modules complémentaires installés et le blocage automatique des modules en liste noire ;
- les rapports de plantage ;
- le service de mise à jour automatique ;
- le service de protection contre les sites malveillants ;
- le service de synchronisation *Firefox Sync*.

Il est donc important de désactiver certaines de ces fonctionnalités pour limiter les données envoyées à Mozilla.

| | |
|---|---|
| **R8** | Désactiver les divers rapports disponibles de plantage, de performance, etc. |

| | |
|---|---|
| **R9** | Désactiver le service de synchronisation *Firefox Sync*. |

| | |
|---|---|
| **R10** | La fonctionnalité de blocage des sites contrefaits envoie à des fournisseurs tiers de Mozilla les adresses Web des sites visités pour vérifier qu'ils ne soient pas connus comme étant malveillants et en bloquer l'accès si nécessaire. Bien qu'il soit conseillé de laisser ce filtre activé pour des raisons de sécurité, une entité pourra juger suffisamment confidentielles les adresses des pages Web visitées pour qu'une désactivation de ce mécanisme s'impose. |

La navigation privée ainsi que la protection contre le pistage (*Do Not Track*) sont des fonctionnalités intéressantes du point de vue du respect de la vie privée lors de la navigation sur Internet et qui pourraient être désactivées pour de la navigation en Intranet. La stratégie de configuration des paramètres de confidentialité dépendra donc du périmètre d'utilisation du navigateur. Dès lors que le navigateur Firefox dispose d'une connectivité à Internet, les recommandations suivantes s'appliquent.

| | |
|---|---|
| **R11** | Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, suppression des données privées, etc.) lorsque le navigateur n'est pas dédié à une navigation Intranet. |

Note : Le nouveau standard de protection contre le-pistage (*Do Not Track*) n'est qu'une sollicitation du client. Sa prise en compte par les serveurs Web ne dépend donc que de leurs pratiques de confidentialité respectives et n'apporte aucune garantie au client.

| | |
|---|---|
| **R12** | Interdire les fonctions de géolocalisation. |

| | |
|---|---|
| **R13** | Dès lors que la confidentialité des recherches est jugée primordiale, il conviendra d'imposer un moteur de recherche de confiance et de désactiver les fonctionnalités de recherche instantanée ou de suggestion de recherche. |

12. KeePass est un exemple de solution disposant d'un certificat de sécurité de premier niveau (CSPN) délivré par l'ANSSI qui peut être utilisée avec Firefox.
13. Déclaration disponible en anglais à l'adresse :
http://www.mozilla.org/en-US/legal/privacy/firefox.html.

#### 4.2.4 Moteur de recherche par défaut

Imposer un moteur de recherche et certains paramètres de recherche peut avoir un sens dans certains contextes. C'est le cas principalement lorsque le navigateur se trouve dédié à l'Intranet. L'entité pourra alors imposer et configurer le moteur de recherche de l'Intranet. Ces règles de configuration peuvent également avoir une utilité pour la recherche sur Internet si, par exemple, l'entité veut imposer un moteur de recherche français qui s'appuie sur une connexion chiffrée. En parallèle, l'entité peut alors bloquer l'accès aux adresses des moteurs de recherche qu'elle souhaite interdire.

| | |
|---|---|
| **R14** | Pour des questions de respect de la vie privée, il est conseillé d'imposer un moteur de recherche s'appuyant sur une connexion chiffrée (HTTPS). |

Note : Cela n'empêche pas l'interception des données par le moteur de recherche, ce dernier étant dans tous les cas destinataire des données de recherche en clair.

#### 4.2.5 Filtrage de contenu

Le filtrage du contenu participe à renforcer la sécurité de la navigation en bloquant les contenus potentiellement malveillants. Certains mécanismes de filtrage peuvent toutefois avoir une incidence sur la faculté des utilisateurs à naviguer sur certains sites.

| | |
|---|---|
| **R15** | Activer les fonctionnalités de filtrage de contenu telles que la navigation sécurisée (protection contre le hameçonnage et les logiciels malveillants) ou la *Content Security Policy*[14]. |

| | |
|---|---|
| **R16** | Interdire ou, a minima, restreindre les scripts, les contenus mixtes actifs [15], les cookies tiers, etc. |

La section correspondante de l'annexe I liste en détail le paramétrage recommandé pour ces types de contenus.

#### 4.2.6 Page(s) d'accueil

Si le navigateur est configuré pour restaurer la session précédente, les données ainsi que les cookies de session seront sauvegardés puis restaurés au prochain démarrage du navigateur (sauf en mode de navigation privée). Il est alors possible de récupérer ces cookies sauvegardés pour s'authentifier à la place de l'utilisateur sans mot de passe, voire de récupérer une session HTTPS préalablement initiée.

| | |
|---|---|
| **R17** | Il est préférable que le navigateur n'enregistre pas les sessions de navigation. Lors du démarrage du navigateur (après un arrêt normal ou brusque), il est en effet conseillé de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une(des) page(s) connue(s) et de confiance. |

#### 4.2.7 Serveur mandataire

Il est primordial de contrôler les flux non seulement en entrée mais également en sortie. Lorsqu'un individu malveillant atteint en intégrité un poste de travail, il peut ensuite procéder à l'établissement d'un canal de contrôle depuis le poste de travail vers un serveur situé sur Internet. L'utilisation de

14. Cette couche de sécurité, qui permet de se prémunir contre certains types d'attaques, est détaillée dans un article du *Mozilla Developer Network* : https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy.

15. https://developer.mozilla.org/en-US/docs/Security/MixedContent.

serveurs mandataires avec authentification peut donc bloquer des connexions sortantes malveillantes. Il s'avère alors judicieux d'imposer l'utilisation du serveur mandataire (*proxy*) par configuration centralisée sur les postes utilisateurs.

| | |
|---|---|
| **R18** | Privilégier l'utilisation de serveurs mandataires avec authentification. |

Note : Cette recommandation peut être renforcée par des règles de filtrage de pare-feu.

#### 4.2.8 Authentification HTTP

Il est possible de durcir la sécurité des authentifications utilisant NTLM [16] ou SPNEGO [17] sur Firefox dès lors que l'une d'entre elles est utilisée par l'entité qui le déploie. Il est par exemple recommandé de spécifier la liste des serveurs autorisés à engager une authentification SPNEGO ou une authentification NTLM automatique.

| | |
|---|---|
| **R19** | Spécifier la liste des serveurs autorisés à engager une authentification SPNEGO ou une authentification NTLM automatique. |

Note : L'utilisation de NTLM n'est pas conseillée, Kerberos étant le protocole d'authentification à privilégier.

#### 4.2.9 Périmètre de navigation

Il est recommandé de restreindre le périmètre de navigation en interdisant certains schémas d'adresses avec les *protocol-handlers*.

| | |
|---|---|
| **R20** | Interdire a minima le schéma d'adresses `file://` pour un navigateur dédié à la navigation sur Internet de manière à éviter des accès arbitraires au système de fichiers. Le schéma `ftp://` pourrait également être interdit au profit de l'utilisation d'un client FTP tiers. |

Note : L'utilisation du navigateur Firefox ne sera alors plus possible pour afficher des pages html directement depuis un système de fichiers (CD-ROM, disque local ou distant via un partage réseau, etc.).

Ces listes présentent également un intérêt particulier dans le cadre d'une stratégie de double navigateur. Ce sujet est détaillé en section « Stratégie de double navigateur ».

#### 4.2.10 Administration système et maintenance

Divers paramètres de Firefox relèvent de sa maintenance et certaines précautions doivent être prises pour éviter des problèmes de compatibilité, de confidentialité des données utilisateurs voire de disponibilité des postes de travail. La liste complète de ces paramètres figure en annexe I.

### 4.3 Télé-déploiement initial

Firefox, au même titre que les autres logiciels, devrait idéalement être installé sur les postes de travail par télé-déploiement. Une telle méthode de déploiement est un des fondamentaux d'un système d'information contrôlé et maîtrisé. En effet, il permet de maîtriser les installations, d'homogénéiser les

16. NTLM (*NT Lan Manager*) est une suite de protocoles d'authentification de Microsoft qui ne supporte pas les méthodes cryptographiques récentes comme AES ou SHA-256.

17. SPNEGO (*Simple and Protected GSSAPI Negociation Mechanism*) est un standard qui permet de négocier de l'authentification Kerberos, NTLM, ainsi que d'autres protocoles supportés pour le système. SPNEGO est également connu sous le nom du protocole d'authentification « negociate ». Pour plus d'informations : `https://developer.mozilla.org/en-US/docs/Integrated_Authentication`.

versions et configurations mais aussi, de procéder aux mises à jour de manière réactive et efficace.

Le télé-déploiement de logiciel peut se faire de plusieurs manières :
- au format MSI par GPO (stratégies de groupe pour la gestion centralisée) dans un domaine Microsoft Active Directory. Attention toutefois, puisque Mozilla ne fournit Firefox qu'au format exécutable, il sera donc nécessaire de construire un *package* Firefox au format MSI. Des éditeurs tiers proposent de tels paquets mais ces éditeurs n'offrent pas de garantie forte de l'intégrité des logiciels qu'ils fournissent. Il est par conséquent préférable que l'organisation utilisatrice génère ses propres fichiers MSI ;
- au format exécutable à l'aide d'un outil de gestion de parc ou de tout autre produit tiers prévu à cet effet.

## 4.4 Gestion des mises à jour

La mise à jour réactive du navigateur est primordiale pour se prémunir des vulnérabilités régulièrement détectées et corrigées. L'utilisation d'un navigateur présentant des vulnérabilités connues par des personnes malveillantes expose le poste de travail à une attaque. Deux stratégies différentes de mise à jour de Firefox peuvent alors être envisagées :
- la première consiste à simplement laisser la configuration par défaut, le navigateur va alors automatiquement télécharger les mises à jour auprès des serveurs de Mozilla. Il convient dans ce cas de s'assurer que les postes de travail sont en mesure d'accéder aux serveurs de mise à jour de Mozilla sur Internet, idéalement au travers du proxy d'entreprise qui pourra notamment mettre en cache les binaires.
- la configuration alternative consiste à remplacer l'URL de mise à jour (à l'aide du paramètre de configuration `app.update.url.override`)[18] par une URL locale qui mettra les mises à jour à disposition des postes de travail.

Le tableau suivant synthétise les avantages et inconvénients des deux méthodes :

| Méthode | Avantages | Inconvénients |
|---|---|---|
| **classique** : par défaut, les navigateurs se mettent à jour automatiquement auprès des serveurs de Mozilla par Internet. | - mise en œuvre aisée par les services informatiques ;<br>- haut taux de disponibilité des serveurs de mise à jour de Mozilla. | - ne permet pas aux services informatiques de tester et valider les mises à jour avant leur déploiement, notamment lors de l'utilisation d'applications Web métier peu répandues ;<br>- peu adapté pour un navigateur dédié à l'Intranet. |
| **contrôlée** : la mise à jour automatique de Firefox est désactivée et les services informatiques mettent les mises à jour à disposition des postes de travail depuis un serveur local. | - permet de tester et valider les mises à jour avant déploiement ;<br>- permet d'adapter les configurations centralisées du navigateur pour tenir compte des éventuelles nouvelles fonctionnalités avant déploiement ;<br>- permet de bloquer tout le trafic à destination des serveurs de Mozilla. | - freine la réactivité des mises à jour ;<br>- nécessite des moyens humains importants. |

18. Pour plus d'informations sur la mise en œuvre d'un serveur de mises à jour local : https://developer.mozilla.org/en-US/docs/Mozilla/Setting_an_update_server.

Il sera nettement moins risqué (du point de la compatibilité) de retenir le mode classique (automatique) pour les versions ESR de Firefox étant donné que les mises à jour concernent des correctifs de sécurité à haut risque et n'apportent aucune nouvelle fonctionnalité. En revanche, les versions standards de Firefox peuvent recevoir des mises à jour fonctionnelles importantes qu'il serait plus pertinent de contrôler préalablement.

La problématique des mises à jour concerne également les extensions. Bien qu'il soit recommandé de les interdire dans le cadre d'une configuration durcie, une entité peut vouloir en déployer certaines pour de bonnes raisons. La mise à jour des extensions est indépendante du mécanisme de mise à jour du navigateur. Elles peuvent être mises à jour automatiquement (comportement par défaut) ou manuellement quelle que soit la stratégie de mise à jour choisie pour le navigateur.

Le maintien en conditions de sécurité des *plugins* devra par ailleurs être géré indépendamment du navigateur, chaque *plugin* ayant ses spécificités quant aux mécanismes de mise à jour utilisés.

Concernant le service *Mozilla Maintenance Service* (service chargé des mises à jour de Firefox), ce dernier s'exécute avec les droits qui lui sont propres pour la mise à jour du navigateur et ce, quels que soient les droits de l'utilisateur.

# 5 Stratégie de double navigateur

La sécurité des systèmes d'information impose souvent un navigateur qui doit être durci pour l'accès à Internet mais plus permissif pour l'accès aux applications internes. Lorsque certains serveurs Web internes utilisent des appliquettes Java par exemple, nécessitant le déploiement de modules complémentaires Java, le navigateur finit par avoir une surface d'attaque très importante et expose ainsi l'entité à un des vecteurs d'attaque les plus critiques et massivement exploités [19].

Pour traiter cette problématique, lorsqu'elles disposent des ressources nécessaires, en particulier pour en assurer le maintien en conditions de sécurité, de plus en plus d'entités s'orientent vers l'usage de deux navigateurs différents. Il devient alors possible :

- d'en dédier un à la navigation sur Internet. De par sa configuration durcie, sa surface d'attaque est réduite au maximum. Il est maintenu en conditions de sécurité avec la plus grande attention. Les équipes de veille scrutent la moindre vulnérabilité dont le navigateur Internet fait l'objet. Les équipements de filtrage et d'analyse du trafic sont utilisés pour repérer tout comportement suspect de navigation sur Internet ;
- d'en dédier un deuxième à l'accès aux serveurs internes, nécessitant par exemple un module complémentaire qui peut faire l'objet de vulnérabilités fréquentes ou qui nécessite une configuration plus permissive. Il est alors possible de le configurer pour permettre uniquement l'accès et l'usage de l'ensemble des sites et applications légères de l'Intranet.

Une telle stratégie de double navigateur doit nécessairement s'accompagner de mesures de sécurité techniques permettant de garantir le périmètre d'utilisation de chaque navigateur par des paramètres de configuration verrouillés. Le tableau suivant en donne quelques exemples :

19. Voir les recommandations de sécurité publiées par l'ANSSI relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows à l'adresse http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-aux-environnements-d-execution-java-sur.html

| Composant | Action | Valeur |
|---|---|---|
| Serveur mandataire | Autoriser | *User-Agent* du navigateur Internet (ou plus strictement de la dernière version de ce dernier) |
| | Bloquer | Tout autre *User-Agent* non autorisé |
| Pare-feu locaux des postes de travail | Autoriser | TCP en sortie vers le serveur mandataire depuis :<br>- le processus du navigateur Internet (chemin complet de l'exécutable) ;<br>- les autres processus éventuels autorisés à accéder à Internet via le serveur mandataire. |
| | Bloquer | TCP en sortie vers le serveur mandataire depuis tout autre processus |
| Pare-feu de passerelle Internet | Autoriser | TCP en sortie vers les ports 443 et 80 depuis :<br>- l'IP source du serveur mandataire ;<br>- les autres IP sources éventuelles autorisées à sortir en direct sur Internet sans passer par le serveur mandataire. |
| | Bloquer | TCP en sortie vers ports 443 et 80 depuis toute autre IP source |
| Applocker (ou SRP) sur les postes de travail | Autoriser l'exécution | Chemin complet de l'exécutable des navigateurs autorisés |
| | Bloquer l'exécution | Tout autre exécutable de navigateur interdit |

Les règles de configuration décrites en annexe I, section « Périmètre de navigation », permettent alors de mettre en œuvre une partie de ces mesures de sécurité et de restreindre le périmètre de navigation possible de chacun des navigateurs.

Les figures suivantes illustrent de manière synthétique les mesures de sécurité appliquées à une stratégie de double navigateur :

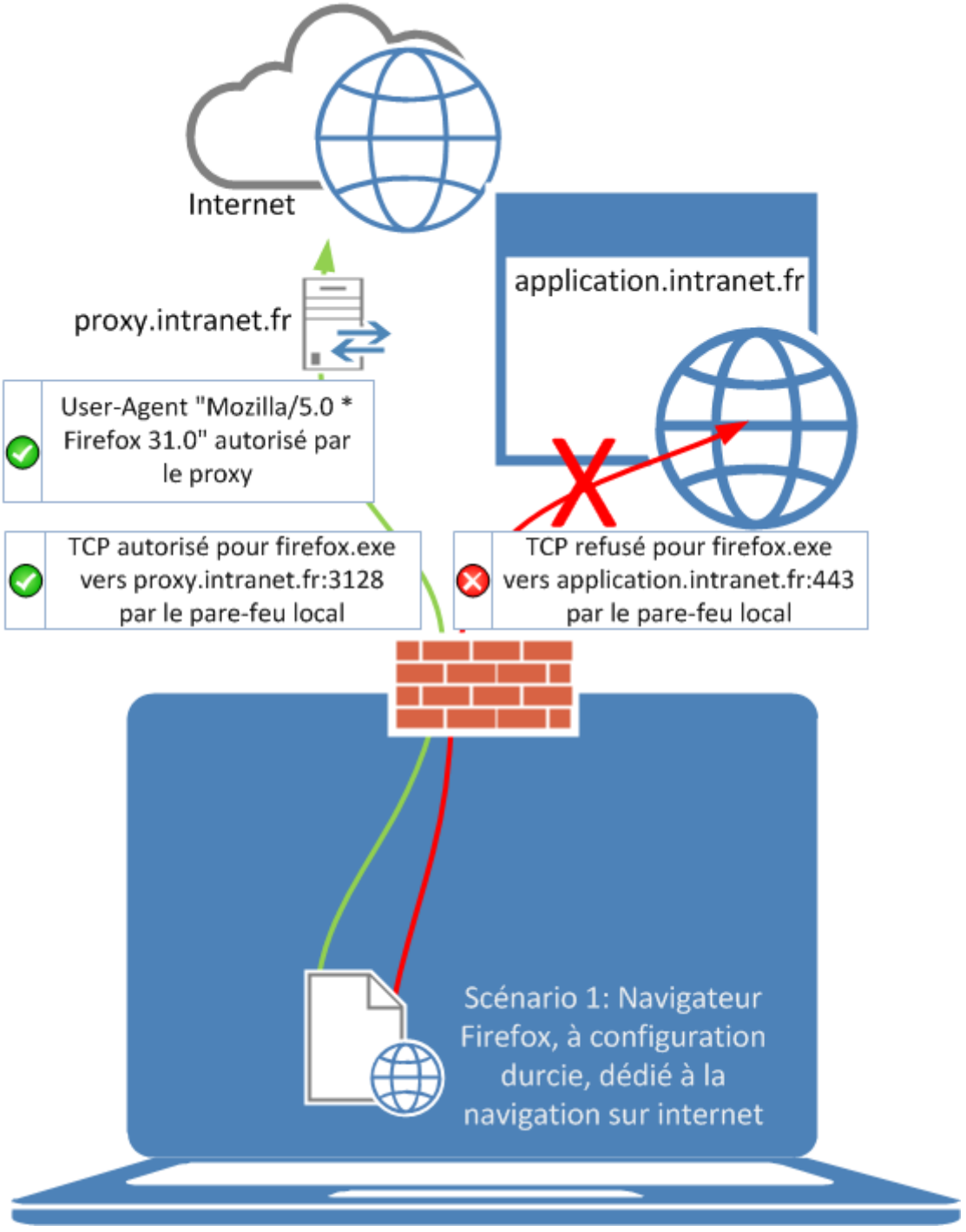


FIGURE 1 – Illustration d'une stratégie de double navigateur, cas où Firefox est utilisé comme navigateur Internet.

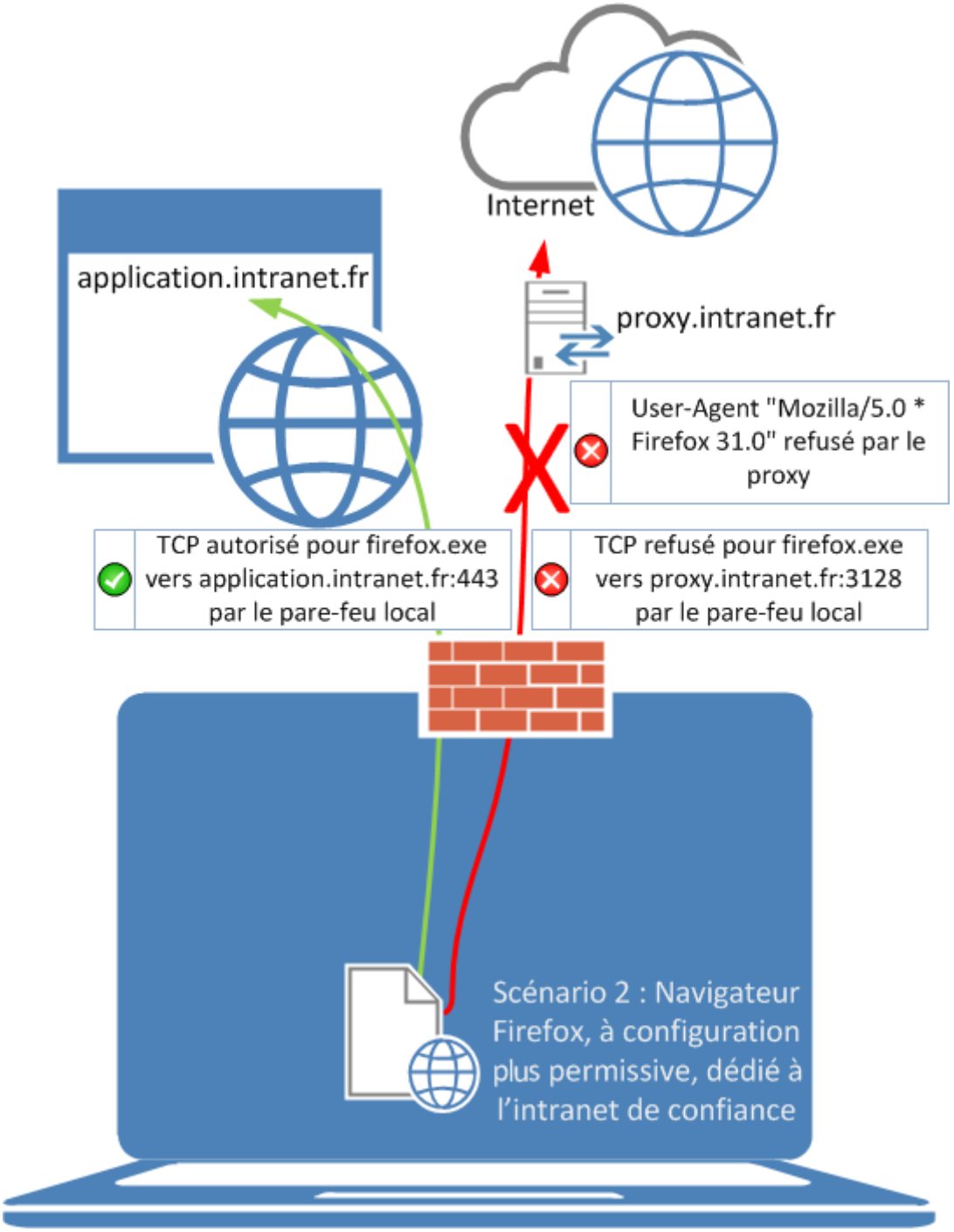


FIGURE 2 – Illustration d'une stratégie de double navigateur, cas où Firefox est utilisé comme navigateur Intranet.

Ces figures illustrent deux cas distincts. Le navigateur Firefox y est représenté mais la stratégie serait équivalente avec d'autres navigateurs.

Les règles de configuration recommandées en annexe I se prêtent à un contexte où le navigateur est dédié à la navigation sur Internet.

# Annexe I : Stratégies de sécurisation de Firefox

Cette annexe liste, sous forme de tableaux, les valeurs recommandées permettant de mettre en œuvre les recommandations formulées dans cette note technique. La liste des paramètres de configuration disponibles est sujette à des évolutions fréquentes et certains sont peu, voire pas documentés. Les recommandations et leurs indications de mise en œuvre figurant dans ce document sont basées sur les paramètres de configuration de Firefox dans sa version ESR 31. Ces derniers pourront être adaptés selon la version du navigateur déployée à la date de lecture du document.

Depuis un navigateur Firefox, il est possible d'afficher et de modifier les paramètres de configuration appliqués en tapant `about:config` dans la barre d'adresse. Les paramètres verrouillés sont affichés en italique. La page `about:support` affiche, quant à elle, un récapitulatif des informations systèmes et de version ainsi que les modifications importantes apportées à la configuration par défaut du navigateur.

En environnement professionnel, il est conseillé de déployer une configuration de manière centralisée comme expliqué en annexe II. Pour un usage personnel de Firefox, il est également possible de s'inspirer de tout ou partie des paramètres indiqués dans ce document à partir de la page `about:config`.

### Sécurité des modules complémentaires :

Les règles de configuration préfixées par le terme « extensions » ne s'appliquent pas toujours uniquement aux extensions comme elles pourraient le laisser entendre mais parfois, plus largement aux *plugins* voire aux modules complémentaires dans leur ensemble. Il convient donc d'être vigilant quant au périmètre réel d'application des règles de configuration dont les noms pourraient prêter à confusion.

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| extensions.autoDisableScopes | Les extensions peuvent être désactivées automatiquement en fonction de leur localisation. | `3` (les extensions déposées dans le profil Firefox de l'utilisateur ou dans le profil utilisateur Windows seront automatiquement désactivées[20]) |
| extensions.enabledScopes | Les extensions peuvent être activées automatiquement en fonction de leur localisation[21]. | `12` (seules les extensions référencées par une entrée en base de registres[22] ou déposées dans le sous-dossier d'extensions à l'emplacement de l'exécutable FireFox seront activées. Attention, ce paramètre a priorité sur *extensions.autoDisableScopes* |

20. Contrairement à ce qu'indique la *MozillaZine Knownledge Base*, le paramètre *extensions.autoDisableScopes* ne permet pas de désactiver un plugin, pour ce faire il convient d'utiliser les paramètres *plugin.state.x*.

21. Pour plus d'informations sur le paramètre *extensions.enabledScopes* : https://developer.mozilla.org/en-US/Add-ons/Installing_extensions.

22. Article de Mozilla expliquant l'ajout, la mise à jour, et la suppression d'extensions ou de *plugins* pour Firefox par base de registre : https://developer.mozilla.org/en-US/docs/Adding_Extensions_using_the_Windows_Registry.

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| extensions.blocklist.enabled | Téléchargement régulier d'une liste noire de modules référencés comme étant malveillants | `false` si seuls les modules télé-déployés par les équipes informatique sont installés, ou `true` si l'utilisateur est en mesure d'installer des modules lui-même |
| extensions.blocklist.detailsURL | URL de la page qu'un utilisateur peut visiter pour en savoir plus sur la liste noire de modules | Celle par défaut (`https://www.mozilla.org/%LOCALE%/blocklist/`) |
| extensions.blocklist.itemURL | URL de la page qu'un utilisateur peut visiter pour en savoir plus sur la liste noire de modules (variante) | Celle par défaut (`https://addons.mozilla.org/%LOCALE%/%APP%/blocked/%blockID%`) |
| extensions.blocklist.interval | Intervalle de téléchargement de la liste noire de modules, en secondes | `86400` (soit 1 fois par jour) |
| extensions.blocklist.level | Niveau de blocage | `2` (pour bloquer les extensions de la liste) |
| extensions.blocklist.url | Adresse de téléchargement de la liste noire de modules | Celle par défaut (`https://addons.mozilla.org/blocklist/3/%APP_ID%/%APP_VERSION%/%PRODUCT%/%BUILD_ID%/%BUILD_TARGET%/%LOCALE%/%CHANNEL%/%OS_VERSION%/%DISTRIBUTION%/%DISTRIBUTION_VERSION%/%PING_COUNT%/%TOTAL_PING_COUNT%/%DAYS_SINCE_LAST_PING%/`) |
| extensions.enabledAddons | Modules activés au démarrage de Firefox | Mettre à vide |
| pdfjs.disabled | Désactiver la visionneuse PDF intégrée à Firefox (*pdf.js*) | `true` pour que l'utilisateur télécharge les PDF et les visionne via un lecteur PDF tiers maintenu en conditions de sécurité par l'entité et ne faisant pas l'objet de vulnérabilités fréquentes, ou `false` pour autoriser l'usage du lecteur de PDF intégré. |
| plugin.state.flash | Configuration d'activation du *plugin* Flash | `1` (demander l'autorisation à l'utilisateur avant chaque exécution du *plugin* Flash) ou `2` (toujours activer) au choix de l'entité et en fonction des utilisateurs et des contraintes de sécurité |
| plugin.state.java | Configuration d'activation du *plugin* Java | `0` pour ne jamais activer le *plugin* Java (à moins que l'entité souhaite utiliser ce *plugin* malgré les risques de sécurité encourus, auquel cas la valeur à donner serait `1` pour demander l'autorisation à l'utilisateur à chaque exécution du *plugin* Java) |
| plugin.state.*x* | Configuration d'activation du *plugin* *x*, où *x* est à remplacer par le nom court du *plugin* à désactiver (exemple : npctrl pour Microsoft Silverlight. Les noms courts des *plugins* sont indiqués en affichant leurs informations détaillées depuis l'interface graphique) | `0` pour ne jamais activer le plugin, ou `1` pour demander l'autorisation à l'utilisateur avant chaque exécution du *plugin* |
| plugin.default.state | Configuration d'activation des autres *plugins* | `0` pour ne jamais activer un *plugin* non explicitement autorisé par les règles précédentes |
| plugin.defaultXpi.state | Configuration d'activation des autres *plugins* au format XPI | `0` pour ne jamais activer un *plugin* au format XPI non explicitement autorisé par les règles précédentes |
| plugins.click_to_play | Cliquer pour lire le contenu nécessitant un *plugin* | `true` pour activer le mode « Cliquer pour lire » |
| plugins.load_appdir_plugins | Chargement automatique des *plugins* depuis des emplacements utilisés avant Firefox 21 | `false` |

Étant donné que seuls les modules complémentaires télé-déployés par les équipes informatiques sont autorisés, il est recommandé de bloquer toute possibilité d'ajout de modules complémentaires par l'utilisateur.

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| extensions.getAddons. getWithPerformance.url | URL de récupération d'un module complémentaire | Mettre à vide |
| extensions.getAddons.maxResults | Nombre de résultats maximum | 0 |
| extensions.getAddons.get.url | URL de consultation d'un module complémentaire | Mettre à vide |
| extensions.getAddons. recommended.browseURL | URL de consultation des modules complémentaires recommandés | Mettre à vide |
| extensions.getAddons. recommended.url | URL de consultation des modules complémentaires recommandés, par API | Mettre à vide |
| extensions.getAddons. search.browseURL | URL de recherche de modules complémentaires | Mettre à vide |
| extensions.getAddons.search.url | URL de recherche de modules complémentaires, par API | Mettre à vide |
| extensions.getAddons.showPane | Afficher le panneau d'ajout de modules complémentaires | `false` |
| extensions.hideInstallButton | Cacher le bouton d'installation manuelle d'extensions | `true` |
| extensions.webservice.discoverURL | URL du catalogue d'extensions | Mettre à vide |
| xpinstall.enabled | Autoriser l'installation manuelle de modules au format XPI | `false` |
| xpinstall.whitelist.required | Obligation pour une archive XPI d'être en liste blanche pour être installée manuellement | `true` |
| xpinstall.whitelist.add xpinstall.whitelist.add.* | Liste blanche d'archives XPI pouvant être installées manuellement | Mettre à vide |

Pour finir, l'entité devra choisir sa stratégie de mise à jour des extensions télé-déployées. L'entité qui voudra télé-déployer elle-même les versions à jour des modules complémentaires après une phase de validation optera pour le paramétrage donné ci-dessous, la responsabilité du maintien en conditions de sécurité sera alors déportée sur les services informatiques en charge du déploiement de ces mises à jour. Dans le cas contraire, les valeurs par défaut permettent une mise à jour automatique des extensions par Internet.

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| extensions.hotfix.cert. checkAttributes | Vérifie les attributs du certificat de signature des correctifs téléchargés | `true` |
| extensions.hotfix.certs.1. sha1Fingerprint | Empreintes attendues du certificat de signature des correctifs téléchargés | Laisser la valeur par défaut (`91:53:98:0C:C1:86:DF:47 :8F:35:22:9E:11:C9:A7:31 :04:49:A1:AA` en date de rédaction de ce document). |
| extensions.update. autoUpdateDefault | Télécharger et installer automatiquement les mises à jour d'extensions | `false` |
| extensions.update.background. URL | URL de téléchargement des mises à jour d'extensions en arrière plan | Mettre à vide |
| extensions.update.enabled | Activer la mise à jour des extensions | `false` |
| extensions.update.interval | Intervalle de téléchargement des mises à jour des extensions | `86400` (soit 1 fois par jour) |
| plugins.update.notifyUser | Notifier l'utilisateur de la présence d'une mise à jour pour ses modules complémentaires | `false` |
| plugins.update.url | URL de mise à jour des modules complémentaires | Mettre à vide |

### SSL/TLS et certificats :

Le paramétrage des suites cryptographiques autorisées peut engendrer des problèmes de compatibilité selon le contexte. Il est donc légitime de préférer ne pas modifier la configuration par défaut. Dans un soucis de durcissement, les recommandations suivantes pourraient toutefois être appliquées :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| security.ssl3.dhe_dss_aes_128_sha | Autoriser ssl3.dhe_dss_aes_128_sha | `false` |
| security.ssl3.dhe_dss_aes_256_sha | Autoriser ssl3.dhe_dss_aes_256_sha | `false` |
| security.ssl3.dhe_dss_camellia_128_sha | Autoriser ssl3.dhe_dss_camellia_128_sha | `false` |
| security.ssl3.dhe_dss_camellia_256_sha | Autoriser ssl3.dhe_dss_camellia_256_sha | `false` |
| security.ssl3.dhe_rsa_aes_128_sha | Autoriser ssl3.dhe_rsa_aes_128_sha | `true` |
| security.ssl3.dhe_rsa_aes_256_sha | Autoriser ssl3.dhe_rsa_aes_256_sha | `true` |
| security.ssl3.dhe_rsa_camellia_128_sha | Autoriser ssl3.dhe_rsa_camellia_128_sha | `false` |
| security.ssl3.dhe_rsa_camellia_256_sha | Autoriser ssl3.dhe_rsa_camellia_256_sha | `false` |
| security.ssl3.dhe_rsa_des_ede3_sha | Autoriser ssl3.dhe_rsa_des_ede3_sha | `false` |
| security.ssl3.ecdhe_ecdsa_aes_128_gcm _sha256 | Autoriser ssl3.ecdhe_ecdsa_aes_128_gcm _sha256 | `true` |
| security.ssl3.ecdhe_ecdsa_aes_128_sha | Autoriser ssl3.ecdhe_ecdsa_aes_128_sha | `true` |
| security.ssl3.ecdhe_ecdsa_aes_256_sha | Autoriser ssl3.ecdhe_ecdsa_aes_256_sha | `true` |
| security.ssl3.ecdhe_ecdsa_rc4_128_sha | Autoriser ssl3.ecdhe_ecdsa_rc4_128_sha | `false` |
| security.ssl3.ecdhe_rsa_aes_128_gcm _sha256 | Autoriser ssl3.ecdhe_rsa_aes_128_gcm _sha256 | `true` |
| security.ssl3.ecdhe_rsa_aes_128_sha | Autoriser ssl3.ecdhe_rsa_aes_128_sha | `true` |
| security.ssl3.ecdhe_rsa_aes_256_sha | Autoriser ssl3.ecdhe_rsa_aes_256_sha | `true` |
| security.ssl3.ecdhe_rsa_des_ede3_sha | Autoriser ssl3.ecdhe_rsa_des_ede3_sha | `false` |
| security.ssl3.ecdhe_rsa_rc4_128_sha | Autoriser ssl3.ecdhe_rsa_rc4_128_sha | `false` |
| security.ssl3.rsa_aes_128_sha | Autoriser ssl3.rsa_aes_128_sha | `true` |
| security.ssl3.rsa_aes_256_sha | Autoriser ssl3.rsa_aes_256_sha | `true` |
| security.ssl3.rsa_camellia_128_sha | Autoriser ssl3.rsa_camellia_128_sha | `false` |
| security.ssl3.rsa_camellia_256_sha | Autoriser ssl3.rsa_camellia_256_sha | `false` |
| security.ssl3.rsa_des_ede3_sha | Autoriser ssl3.rsa_des_ede3_sha | `false` |
| security.ssl3.rsa_fips_des_ede3_sha | Autoriser ssl3.rsa_fips_des_ede3_sha | `false` |
| security.ssl3.rsa_rc4_128_md5 | Autoriser ssl3.rsa_rc4_128_md5 | `false` |
| security.ssl3.rsa_rc4_128_sha | Autoriser ssl3.rsa_rc4_128_sha | `false` |
| security.ssl3.rsa_seed_sha | Autoriser ssl3.rsa_seed_sha | `false` |

Autres paramètres :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| security.tls.version.max | Version maximum de SSL/TLS | `3` (ce qui correspond à TLS 1.2) |
| security.tls.version.min | Version minimum de SSL/TLS | `2` (ce qui correspond à TLS 1.1) |
| security.ssl.allow_unrestricted_renego_ everywhere__temporarily_available_pref | Activer la renégociation SSL | `false` pour remédier à une attaque par le milieu connue |
| security.ssl.enable_false_start | Activer « SSL False Start » | `false` car non standardisé et amenant de potentielles vulnérabilités |
| security.ssl.enable_ocsp_stapling | Activer l'OCSP stapling[23] | `true` |

23. https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| security.ssl.require_safe_ negotiation | Nécessite une négociation SSL qui n'utilise pas une ancienne version SSL/TLS vulnérable à des attaques par le milieu | `true` est la valeur idéale en termes de sécurité, mais `false` reste conseillé pour éviter que de nombreux sites couramment visités ne soient plus utilisables |
| security.ssl.renego_ unrestricted_hosts | Liste d'hôtes autorisés à faire de la renégociation SSL avec d'anciennes versions vulnérables du protocole | Liste d'hôtes séparés par des virgules (ne supportant pas les *wildcards*) et qu'il est utile de renseigner si security.ssl.require_safe_negotiation est configuré à `true` |
| security.ssl.treat_unsafe_ negotiation_as_broken | Informer l'utilisateur (cadenas cassé rouge dans la barre de status) lorsque les négociations SSL/TLS sont non sécurisées | `true` |
| network.stricttransportsecurity. preloadlist | Charger la liste de sites déclarés comme utilisant HSTS (*HTTP Strict Transport Security*[24]) | `true` |
| network.websocket. allowInsecureFromHTTPS | Autoriser les WebSockets non sécurisée pour un site consulté en HTTPS | `false` |
| security.OCSP.enabled | Activer OCSP | `2` pour vérifier le certificat à partir de l'URL de service OCSP et de l'autorité de certification ayant signé le certificat. Notons que cette fonctionnalité est critiquée pour des questions de latence des répondeurs OCSP (de l'ordre de 300ms pour les plus rapides à plus d'une seconde pour les plus lents). OCSP tend donc à être remplacé par des listes locales de certificats révoqués dans d'autres navigateurs, mais Firefox ne dispose pas encore d'une telle liste. Une entité ayant des contraintes particulières quant à la latence induite par OSCP pourrait opter pour une désactivation d'OCSP avec la valeur `0` |
| security.OCSP.require | Nécessite la validation du certificat par OCSP avant de continuer la navigation sur le site | `true` si *security.OCSP.enabled* a été configuré à `true`, ou `false` dans le cas contraire. |
| security.cert_pinning. enforcement_level | Niveau de *certificate pinning* (épinglage de certificats)[25](à partir de Firefox 32) | `2` pour utiliser l'épinglage strict. |

## Gestionnaire de mots de passe :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| privacy.clearOnShutdown.passwords | Effacer les mots de passe enregistrés à la fermeture du navigateur | `true` |
| signon.rememberSignons | Active le gestionnaire de mots de passe | `false` |
| signon.autofillForms | Remplissage automatique des formulaires de login | `false` |

24. https://developer.mozilla.org/fr/docs/S%C3%A9curit%C3%A9/HTTP_Strict_Transport_Security.

25. L'épinglage de certificats permet d'avoir une base locale de certificats connus et attendus pour certains sites Web consultés en HTTPS. Ainsi, si le certificat présenté par le serveur est valide en tous points de vue mais n'est pas le certificat attendu, la connexion sera coupée. Ce mécanisme permet d'éviter une attaque par le milieu présentant un faux certificat issu d'une autorité de certification de confiance.

**Confidentialité :**

Il n'existe pas, en date de rédaction de cette note, de règle globale pour la désactivation de *Firefox Sync*. Sa désactivation se fait par conséquent à travers plusieurs règles de configuration.

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| services.sync.engine.addons | Synchronisation des modules complémentaires | `false` |
| services.sync.engine.bookmarks | Synchronisation des marque-pages | `false` |
| services.sync.engine.history | Synchronisation de l'historique de navigation | `false` |
| services.sync.engine.passwords | Synchronisation des mots de passe stockés | `false` |
| services.sync.engine.prefs | Synchronisation des préférences | `false` |
| services.sync.engine.tabs | Synchronisation des onglets ouverts | `false` |
| services.sync.registerEngines | Moteurs de synchronisation enregistrés | Mettre à vide |
| services.sync.jpake.serverURL | URL du serveur synchronisation jpake | Mettre à vide |
| services.sync.serverURL | URL du serveur de synchronisation | Mettre à vide |
| services.sync.serverURL | URL du serveur de synchronisation | Mettre à vide |
| services.sync.tokenServerURI | URI du serveur de jetons | Mettre à vide |
| services.sync.nextSync | Planification de la prochaine synchronisation | `0` |

Il convient également de désactiver les différents rapports à Mozilla :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| datareporting.healthreport.about.reportUrl | URL de rapport de santé | Mettre à vide |
| datareporting.healthreport.<br>logging.consoleEnabled | Activer la journalisation (console) du service de rapports de santé | `false` |
| datareporting.healthreport.<br>logging.dumpEnabled | Activer la journalisation (dumps) du service de rapports de santé | `false` |
| datareporting.healthreport.<br>nextDataSubmissionTime | Date de prochaine soumission de rapport de santé | Mettre à vide |
| datareporting.healthreport.service.enabled | Activer le service de rapport de santé | `false` |
| datareporting.healthreport.uploadEnabled | Autoriser l'envoi de données au serveur de rapports de santé | `false` |
| datareporting.policy.dataSubmissionEnabled | Activer l'envoi de données à Mozilla à des fins d'amélioration | `false` |
| datareporting.policy.<br>dataSubmissionPolicyAccepted | Accepter les conditions d'envoi de données à Mozilla à des fins d'amélioration | `false` |
| datareporting.policy.<br>dataSubmissionPolicyBypassAcceptance | Contourner l'acceptation des conditions d'envoi de données à Mozilla à des fins d'amélioration | `false` |
| datareporting.policy.<br>dataSubmissionPolicyResponseType | Réponse aux conditions d'envoi de données à Mozilla à des fins d'amélioration | `accepted-info`<br>`-bar-dismissed` |
| dom.ipc.plugins.reportCrashURL | Intégrer l'URL au rapport de crash de *plugins* | `false` |
| dom.ipc.plugins.flash.subprocess.<br>crashreporter.enabled | Activer le rapport de crash du sous-processus flash | `false` |
| toolkit.telemetry.enabled | Activer la fonctionnalité de télémétrie | `false` |
| toolkit.telemetry.server | Adresse du serveur de télémétrie | Mettre à vide |
| breakpad.reportURL | URL du rapport de crash | Mettre à vide |

Il peut également être utile de configurer l'option de suppression des données privées (*Clear Private Data*) en sélectionnant les éléments qui seront supprimés. L'entité pourra par exemple permettre aux utilisateurs de supprimer leurs données privées dans le cadre d'une navigation sur internet ou bien, de l'interdire s'il s'agit d'un navigateur dédié à l'intranet. Une entité pourrait également vouloir toujours garder les historiques et le cache à des fins d'investigation (cela n'empêchera toutefois pas l'utilisateur de les supprimer directement au niveau du système de fichiers dans son profil utilisateur).

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| privacy.cpd.cache | Supprimer le cache lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.cookies | Supprimer les cookies lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.downloads | Supprimer l'historique des téléchargements lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.formdata | Supprimer l'historique de remplissage automatique des formulaire lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.history | Supprimer l'historique lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.offlineApps | Supprimer les applications disponibles hors connexion lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.passwords | Supprimer les mots de passe enregistrés lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.sessions | Supprimer les sessions en cours enregistrées lors d'une suppression des données privées | Au choix de l'entité |
| privacy.cpd.siteSettings | Supprimer les paramètres par site lors d'une suppression des données privées | Au choix de l'entité |
| privacy.sanitize.<br>sanitizeOnShutdown | Supprimer les données privées à la fermeture du navigateur | En cas de besoin spécifique de l'entité |

Viennent pour finir divers autres paramètres liés à la confidentialité :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| privacy.clearOnShutdown.sessions | effacer les sessions de navigation en cours lors de la fermeture du navigateur | `true` |
| privacy.clearOnShutdown.cookies | effacer les cookies de navigation lors de la fermeture du navigateur | `true` |
| privacy.donottrackheader.enabled | Activer *Do-Not-Track* | `true` |
| geo.enabled | activer la géolocalisation | `false` |
| geo.wifi.uri | URI du service de géolocalisation à utiliser | Mettre à vide |
| network.prefetch-next | Téléchargement prédictif anticipé des documents liés à la page Web visités (*link prefetching*)[26] | `false` pour éviter l'établissement de connexions et le téléchargement de contenu non sollicités |
| media.navigator.permission.disabled | Contourne la permission d'accéder à la webcam | `false` |
| network.http.sendRefererHeader | Activer l'envoi de l'entête *referer* | `0` pour plus d'anonymat, ou `2` pour ne pas empêcher le fonctionnement de certains sites |
| browser.send_pings | Activer l'envoi de requête POST lors du clic sur un lien (fonctionnalité souvent utilisée pour tracer les clics) | `false` |

26. Le *link prefetching* permet d'accélérer le surf en anticipant le chargement des documents liés à la page visités. L'implémentation de ce mécanisme dans Firefox ne transmet aucune information à Mozilla. Pour plus d'informations : https://developer.mozilla.org/en-US/docs/Web/HTTP/Link_prefetching_FAQ.

### Filtrage de contenu :

Actions autorisées aux les scripts :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| dom.allow_scripts_to_close_windows | Autoriser les scripts à fermer une fenêtre | `false` |
| dom.disable_image_src_set | Interdire la modification des images sources par script | `false` |
| dom.disable_window_flip | Interdire le changement de fenêtre active par script | `true` |
| dom.disable_window_move_resize | Détermine si les fenêtres peuvent être bougées or redimensionnées par script | `false` |
| dom.disable_window_open_feature.close | Interdire la création de fenêtre sans bouton de fermeture | `true` pour éviter les popups invasifs |
| dom.disable_window_open_feature.location | Interdire la création de fenêtre sans barre d'adresse | `true` pour que l'utilisateur puisse toujours vérifier être à l'adresse prévue |
| dom.disable_window_open_feature.status | Interdire la création de fenêtre sans barre de status | `true` pour que l'utilisateur puisse se rendre contre plus facilement des tentatives de spoofing |
| dom.disable_window_open_feature.titlebar | Interdire la création de fenêtre sans barre de titre | `true` pour que l'utilisateur puisse bien voir qu'il s'agit d'un popup Firefox |
| dom.disable_window_open_feature.toolbar | Interdire la création de fenêtre sans barre d'outils | `false` |
| dom.event.clipboardevents.enabled | Permettre à un script de saisir les événements du presse papier | `false` |
| dom.event.contextmenu.enabled | Permettre à un script de saisir les événements d'accès au menu contextuel (clic droit) | `false` |
| dom.inter-app-communication-api.enabled | Activer la communication par API entre applications | `false` |
| dom.ipc.plugins.enabled | Activation du *plugin* container | `true` pour exécuter les *plugins* dans le *plugin-container* |
| dom.ipc.plugins.java.enabled | Exécuter Java au sein du *plugin-container* | `false` pour éviter des problèmes de stabilité |

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| browser.safebrowsing.enabled | Utiliser la navigation sécurisée (protection contre le phishing et les logiciels malveillants)[27] | `true` |
| javascript.enabled | Activation de Javascript | `true` |
| security.xpconnect.plugin.unrestricted | Autoriser le scripting de *plugins* par des scripts qui ne sont pas de confiance | `false` à moins d'une incompatibilité avec des *plugins* et/ou pages Web nécessaires à l'entité |
| security.mixed_content.<br>block_active_content | Bloquer le contenu mixte actif | `true` |
| security.mixed_content.<br>block_display_content | Bloquer le contenu mixte passif | `false` |
| security.fileuri.<br>strict_origin_policy | Politique d'origine stricte pour les URi de type fichiers | `true` sauf pour les populations de développeurs qu'un tel paramètre pourrait bloquer pour le développement en local |
| network.cookie.cookieBehavior | Politique de gestion des cookies | `1` pour n'autoriser que les cookies du serveur d'origine, et bloquer les cookies tiers |
| network.cookie.lifetimePolicy | Politique d'expiration des cookies | `2` pour conserver les cookies pendant toute la durée de la session seulement |
| network.cookie.thirdparty.sessionOnly | Restreindre les cookies tiers à la durée de la session seulement | `true` |
| network.jar.open-unsafe-types | N'ouvrir que les *.jar* servis avec un *content-type* adéquat | `false` |
| privacy.popups.policy | Politique de popups | `1` pour activer les popups, ou `2` pour les rejeter mais cela rendrait la navigation difficile voire impossible sur une quantité de sites Internet non négligeable |
| privacy.popups.showBrowserMessage | Afficher un message lorsqu'un popup a été bloqué | `true` |
| browser.popups.showPopupBlocker | Afficher l'icône du bloqueur de popups dans la barre de status | `true` |
| security.csp.enable | Activer la *Content Security Policy* (politique de sécurité des contenus) qui permet de détecter et de limiter l'impact de certains types d'attaques | `true` |
| full-screen-api.enabled | Activer l'API permettant d'afficher du contenu en plein écran pour les modules complémentaires | `false` |
| notification.feature.enabled | Permettre les notifications sur le bureau | `false` |

27. La fonctionnalité de navigation sécurisée consiste à synchroniser une liste locale d'adresses de sites maveillants (depuis les serveurs de Google par défaut, depuis que Firefox utilise leur service) pour alerter l'utilisateur s'il s'apprête à en visiter un. Elle consiste également à analyser le contenu des pages pour repérer d'éventuelles tentatives d'hameçonnage.

### Moteur de recherche par défaut :

La configuration d'un moteur de recherche personnalisé ne peut pas se faire simplement par fichier de configuration et nécessite le déploiement d'un module de recherche (*search engine plugin*). L'annexe IV illustre la télé-déploiement d'un module de recherche utilisant le moteur français `https://www.qwant.com` [28].

| Nom de paramètre | Description | Exemple |
|---|---|---|
| browser.search.defaultenginename | Moteur de recherche par défaut | `Qwant.com` |
| browser.search.defaulturl | URL du moteur de recherche par défaut | `https://www.qwant.com/?q=searchTerms` |
| browser.search.log | Journalisation de l'utilisation des services de recherche à des fins de déboggage | `false` |
| browser.search.openintab | Ouvrir les résultats de recherche dans un nouvel onglet | `false` |
| browser.search.order.1 | Moteur de recherche à utiliser en priorité 1 | `Qwant.com` |
| browser.search.suggest.enabled | activer les suggestions | `false` |
| browser.search.update | Recherche de mises à jour pour les modules de recherche | `false` |
| keyword.enabled | Permettre de faire une recherche depuis la barre d'adresse | `true` |

## Page(s) d'accueil

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| startup.homepage_override_url | Page d'accueil après une mise à jour de Firefox | En fonction du choix de l'entité |
| startup.homepage_welcome_url | Page d'accueil au premier démarrage | En fonction du choix de l'entité |
| browser.startup.homepage | Page d'accueil | *about :blank* pour une page vide, ou l'adresse d'un site Web ou intranet selon le choix de l'entité |
| browser.startup.page | Page d'accueil | `1` pour ouvrir la page d'accueil indiquée par le paramètre *browser.startup.homepage* |
| browser.sessionstore.resume_from_crash | Restauration de session après crash | `false` |
| browser.sessionstore.enabled | Activer le service de restauration de session | `false` |
| browser.newtab.url | Page ouverte par défaut lors de la création d'un nouvel onglet de navigation | *about :blank* pour une page vide, ou l'adresse d'un site Web ou intranet selon le choix de l'entité |

28. Ceci n'est en aucun cas une recommandation ni une incitation à son utilisation mais un simple exemple.

### Authentification HTTP :

| Nom de stratégie | Description | Valeur recommandée |
|---|---|---|
| network.auth.force-generic-ntlm | Utiliser le module d'authentification NTLM de Firefox plutôt que celui fourni par les APIs du système | `false` |
| network.auth.use-sspi | Utiliser SSPI plutôt que GSSAPI pour l'authentification Kerberos | `true` sous Windows |
| network.ntlm.send-lm-response | Envoyer le LM Hash dans la réponse NTLM | `false` |
| network.automatic-ntlm-auth.allow-proxies | Authentification par NTLM automatique avec les serveurs proxy | Au choix de l'entité en fonction du système d'authentification utilisé par le serveur proxy d'entreprise |
| network.automatic-ntlm-auth.trusted-uris | Liste des URIs autorisées pour l'authentification par NTLM automatique | Liste de valeurs séparées par des virgules (exemple : `monsite.fr, https://monsite.fr`. L'entité y fera figurer les adresses de tous les sites ayant recours à une authentification NTLM automatique |
| network.automatic-ntlm-auth.allow-non-fqdn | Autoriser l'authentification NTLM automatique avec des sites sans FQDN | `false` à moins que la liste *network.automatic-ntlm-auth.trusted-uris* comporte des adresses sans FQDN |
| network.negotiate-auth.allow-non-fqdn | Autoriser l'authentification SPNEGO avec des sites sans FQDN | En fonction de l'entité |
| network.negotiate-auth.allow-proxies | Autoriser SPNEGO[29]si demandé par un serveur proxy | Au choix de l'entité en fonction du système d'authentification utilisé par le serveur proxy d'entreprise |
| network.negotiate-auth.delegation-uris | Liste des URIs autorisées pour lesquels le navigateur peut déléguer l'autorisation de l'utilisateur | Liste de valeurs séparées par des virgules (exemple : `monsite.fr, https://monsite.fr`. L'entité y fera figurer les adresses de tous les sites auxquels elle souhaite permettre la délégation SPNEGO |
| network.negotiate-auth.trusted-uris | Liste des URIs autorisées pour engager une authentification SPNEGO | Liste de valeurs séparées par des virgules (exemple : `monsite.fr, https://monsite.fr`. L'entité y fera figurer les adresses de tous les sites ayant recours à une authentification SPNEGO |
| network.negotiate-auth.gsslib | Chemin vers une librairie GSSLIB spécifique | Mettre à vide |
| network.negotiate-auth.using-native-gsslib | Utiliser la librairie GSSLIB native du système | `true` |
| security.default_personal_cert | Choix du certificat d'authentification client | `Ask Every Time` |

29. SPNEGO est un standard qui permet de négocier de l'authentification Kerberos, NTLM, ainsi que d'autres protocoles supportés pour le système. SPNEGO est également connu sous le nom du protocole d'authentification « negociate ». Pour plus d'informations : https://developer.mozilla.org/en-US/docs/Integrated_Authentication.

### Serveur mandataire :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| network.proxy.autoconfig_url | URL de configuration automatique du proxy | Laisser à vide |
| network.proxy.ftp | Adresse du proxy FTP | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.ftp_port | port du proxy FTP | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.http | Adresse du proxy proxy HTTP | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.http_port | port du proxy HTTP | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.no_proxies_on | Liste d'exceptions à l'utilisation du serveur proxy | A minima `localhost, 127.0.0.1` et davantage en fonction de l'entité et du périmètre d'utilisation du navigateur |
| network.proxy.share_proxy_settings | Utiliser le même proxy pour tous les protocoles | `false` |
| network.proxy.socks | Adresse du proxy socks | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.socks_port | port du proxy socks | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.socks_remote_dns | Réaliser les requêtes DNS via le proxy socks | `false` |
| network.proxy.socks_version | Version du proxy socks | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.ssl | Adresse du proxy HTTPS | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.ssl_port | port du proxy HTTPS | À renseigner selon la configuration de l'entité et si un tel proxy est utilisé |
| network.proxy.type | Type d'utilisation du proxy | `1` pour utiliser les valeurs indiquées par les paramètres ci-dessus (`network.proxy.*`) |
| network.http.proxy.version | version de proxy | `1.1` par défaut et en fonction du serveur proxy de l'entité |
| network.http.proxy.pipelining | Activer le pipelining[30]par proxy | `false` pour des raisons de compatibilité. L'entité peut choisir de l'activer si le pipelining est supporté par son serveur proxy d'entreprise |
| signon.autologin.proxy | Saisie automatique du mot de passe de proxy | `false` |

30. Le pipelining permet de faire plusieurs requêtes HTTP simultanément plutôt que de les faire séquentiellement en attendant les réponses de chacune d'entre elles. Pour plus d'informations : http://www-archive.mozilla.org/projects/netlib/http/pipelining-faq.html.

### Périmètre de navigation :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| network.protocol-handler.expose-all | Détermine si le navigateur essaye d'ouvrir les liens cliqués dans le navigateur en priorité avant de laisser le système s'en charger en cas d'échec (si le protocole du lien en question n'est pas supporté par le navigateur) | `true` |
| network.protocol-handler.warn-external-default | Avertir l'utilisateur avant de charger un gestionnaire de protocole tiers | `true` |
| network.protocol-handler.external-default | Action pour l'ouverture d'un protocole non pris en charge par le navigateur | `false` de manière à ne pas essayer de charger des protocoles non pris en charge nativement par le navigateur. L'entité renseignera éventuellement des gestionnaires de protocoles tiers pour des protocoles qu'elle souhaite explicitement permettre, tels que *NNTP :*, *Mailto :*, etc. Pour illustrer par l'exemple avec *Mailto :*, le paramètre *network.protocol-handler.external.mailto* aurait pour valeur `true` et le paramètre network.protocol-handler.app.mailto avec pour valeur le chemin d'un exécutable comme Mozilla Thunderbird ou Microsoft Outlook |
| network.protocol-handler.external.file | Gestionnaire de protocole `file://` sous Firefox | `false` |
| network.protocol-handler.external.ftp | Gestionnaire de protocole `ftp://` sous Firefox | `false` |
| gecko.handlerService. allowRegisterFromDifferentHost | Autoriser les sites Web à installer des gestionnaires de protocoles ou de contenus utilisable pour des hôtes tiers | `false` |

### Administration système, maintenance, et options diverses :

Paramétrage des mises à jour :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| app.update.enabled | Activation de la mise à jour automatique | `true` |
| app.update.auto | Téléchargement et installation automatiques (nécessite que le paramètre `app.update.enabled` ait pour valeur `true`) | `true` |
| app.update.cert.checkAttributes | Vérifie les attributs du certificat du serveur de mise à jour | `false` |
| app.update.cert.requireBuiltIn | Requiert l'intégration des certificats du serveur de mise à jour et de toutes les redirections intermédiaires | `false` |
| app.update.channel | Canal de mise à jour | `esr` pour la version ESR de Firefox |
| app.update.download .backgroundInterval | Temps de pause (en secondes) entre chaque téléchargement, en arrière plan, d'un morceau de 300 Kb de mise à jour | Au choix de l'entité |
| app.update.idletime | Temps de pause (en secondes) entre chaque téléchargement, à la demande de l'utilisateur) d'un morceau de 300 Kb de mise à jour | 60 |
| app.update.interval | Intervalle de temps entre chaque vérification de disponibilité de nouvelles mises à jour | 43200 |
| app.update.mode | Détermine quelles mises à jour sont téléchargées en arrière plan | `0` pour télécharger toutes les mises à jour sans intervention de l'utilisateur |
| app.update.service.enabled | Active le service de mise à jour de Firefox | `true` |
| app.update.showInstalledUI | Détermine si, après installation de mise à jour, une boîte de dialogue informe l'utilisateur qu'une mise à jour a été installée | Au choix de l'entité |
| app.update.silent | Active le mode de mise à jour silencieux | `true` pour une mise à jour silencieuse en arrière plan |
| app.update.url | URL de récupération des mises à jour de Firefox | En fonction de la stratégie de mise à jour de l'entité. Pour une mise à jour depuis les serveurs de Mozilla : `https://aus3.mozilla.org/update/3/%PRODUCT%/%VERSION%/%BUILD_ID%/%BUILD_TARGET%/%LOCALE%/%CHANNEL%/%OS_VERSION%/%DISTRIBUTION%/%DISTRIBUTION_VERSION%/update.xml`, sinon l'URL du serveur de mise à jour interne de l'entité (qu'il faudra également renseigner dans le paramètre `app.update.url.override`) |
| app.update.url.override | URL de récupération des mises à jour de Firefox | Paramètre à renseigner uniquement dans le cas ou la mise à jour de Firefox se fait depuis l'URL d'un serveur de mise à jour interne de l'entité (à renseigner en plus du paramètre `app.update.url`) |
| app.update.url.details | URL de consultation des informations relatives aux mises à jour disponibles | Laisser la valeur par défautr `https://www.mozilla.org/%LOCALE%/firefox/notes` |

Configuration du cache :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| browser.cache.check_doc_frequency | Quand vérifier la mise à jour d'une page en cache disque | `3` (vérifier quand la page est périmée) |
| browser.cache.compression_level | Niveau de compression du cache disque | Au choix de l'entité, de `0` (pas de compression) à `9` (haut taux de compression avec forte sollicitation du processeur) |
| browser.cache.disk.capacity | Espace disque alloué au cache disque, en Kb | Au choix de l'entité |
| browser.cache.disk.enable | Utiliser le cache disque | `true` |
| browser.cache.disk.max_entry_size | Taille maximum (en Kb) d'une entrée en cache disque | Au choix de l'entité |
| browser.cache.disk.smart_size.enabled | Allocation intelligente de l'espace disque alloué au cache en fonction de l'espace disponible | Au choix de l'entité |
| browser.cache.disk_cache_ssl | Mettre en cache disque les pages visitées en HTTPS | `False` de manière à ne pas mettre en cache le contenu SSL |
| browser.cache.memory.enable | Utiliser le cache mémoire | `true` |
| browser.cache.memory.max_entry_size | Taille maximum (en Kb) d'une entrée en cache mémoire | Au choix de l'entité |
| browser.cache.memory_limit | Mémoire maximum utilisée pour le cache mémoire, en Kb | Au choix de l'entité |
| browser.cache.offline.capacity | Espace disque alloué au cache des applications Web | Au choix de l'entité |
| browser.cache.offline.enable | Utiliser le cache des applications Web permettant une utilisation hors ligne | Au choix de l'entité |
| browser.cache.use_new_backend | Utilisation du nouveau système de cache | `0` (ne pas utiliser pour des questions de stabilité) |
| network.http.use-cache | Utiliser le cache des documents HTTP | `true` |
| media.cache_size | Taille du cache pour les fichiers multimedia | Au choix de l'entité, par défaut `512000` |
| dom.storage.default_quota | Quota de stockage côté client pour les pages Web | `5120`, taille par défaut |
| dom.storage.enabled | Active le stockage côté client pour les pages Web | `true` à défaut de vulnérabilités connues pour cette fonctionnalité |

Désactiver les options de développement (sauf pour les populations de développeurs) :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| devtools.appmanager.enabled | Activation des outils de développement, module appmanager | `false` |
| devtools.debugger.enabled | Activation des outils de développement, module débogueur | `false` |
| devtools.errorconsole.enabled | Activation des outils de développement, module console d'erreurs | `false` |
| devtools.fontinspector.enabled | Activation des outils de développement, module inspecteur de polices | `false` |
| devtools.inspector.enabled | Activation des outils de développement, module inspecteur | `false` |
| devtools.netmonitor.enabled | Activation des outils de développement, module réseau | `false` |
| devtools.profiler.enabled | Activation des outils de développement, module profileur | `false` |
| devtools.shadereditor.enabled | Activation des outils de développement, module vue adaptive | `false` |
| devtools.styleeditor.enabled | Activation des outils de développement, module editeur de styles | `false` |
| devtools.tilt.enabled | Activation des outils de développement, module tilt | `false` |
| devtools.toolbar.enabled | Activation des outils de développement, module barre de développement | `false` |

Configurations diverses :

| Nom de paramètre | Description | Valeur recommandée |
|---|---|---|
| network.seer.enable-hover-on-ssl | Activer *seer* sur SSL | `false` |
| network.seer.enabled | Activer *seer* | `false` |
| network.http.pipelining | Activer le pipelining pour le surf HTTP/1.1 | `false` pour des raisons de compatibilité avec les serveurs Web. Le pipelining peut éventuellement être utilisé pour un navigateur dédié à l'intranet si l'entité sait l'ensemble de ses serveurs compatibles |
| network.http.pipelining.ssl | Activer le pipelining pour le surf HTTPS/1.1 | `false` pour des raisons de compatibilité avec les serveurs Web. Le pipelining peut éventuellement être utilisé pour un navigateur dédié à l'intranet si l'entité sait l'ensemble de ses serveurs compatibles |
| network.http.spdy.enabled | Activer SPDY[31] | `false` |
| network.http.spdy.enabled.v2 | Activer SPDY v2 | `false` |
| network.http.spdy.enabled.v3 | Activer SPDY v3 | `false` |
| network.http.spdy.enabled.v3-1 | Activer SPDY v3.1 | `false` |
| browser.shell.checkDefaultBrowser | Vérifier si Firefox est configuré comme navigateur par défaut | `false` dans le cadre de double navigateurs. |
| browser.download.manager.scanWhenDone | Scan antivirus d'un fichier lorsque son téléchargement est terminé | `true` |
| browser.download.useDownloadDir | Utiliser le répertoire de téléchargement par défaut | `false` pour que l'utilisateur indique à quel emplacement il souhaite télécharger le fichier |
| browser.fullscreen.autohide | Cacher la barre d'outils et d'onglets en mode plein écran | `false` |

31. SPDY est un protocole réseau expérimental de Google visant à augmenter les capacités du protocole HTTP pour réduire le temps de chargement des pages Web en classant les objets par ordre de priorité et en multiplexant les transferts pour ne nécessiter qu'une seule connexion. Ce protocole est vulnérable aux attaques CRIME (*Compression Ratio Info-leak Made Easy*) lorsqu'il est utilisé avec HTTPS (ce qui est généralement le cas).

# Annexe II : Déploiement et configuration centralisée dans un domaine Active Directory par GPP

Cette annexe présente de manière synthétique une méthode de configuration centralisée reposant sur Active Directory.

## Téléchargement de l'exécutable d'installation

La dernière version de Firefox est disponible sur le site Web de Mozilla [32].

Le téléchargement n'est proposé qu'au format exécutable. Son déploiement sera effectué selon les méthodes utilisées par chaque entité. Pour un déploiement par GPO au format MSI, un repaquettage de l'exécutable est nécessaire mais cela nécessite l'usage d'outils tiers.

## Fichiers de configuration

La méthode de configuration centralisée et verrouillée de Firefox présentée dans cette annexe consiste en la création d'un minimum de deux fichiers texte :

- un fichier `local-settings.js` à déposer dans le sous dossier `defaults\pref\` du répertoire d'installation de Firefox. Ce fichier, par convention, se contente de référencer un deuxième fichier de configuration plus complet ;
- un fichier `mozilla.cfg` (ou quelconque autre nom à la discrétion de l'entité) à déposer directement dans le répertoire d'installation de Firefox et qui contient l'ensemble des paramètres de configuration souhaités.

Fichier `local-settings.js` :

```
pref("general.config_obscure_value", 0); // fichier de configuration sans encodage
pref("general.config.filename","mozilla.cfg");
```

Fichier `mozilla.cfg` qui contient tous les paramètres de configuration souhaités :

```
// Configuration de Firefox
try {
// Options de configuration de proxy
lockPref("network.proxy.http","192.168.0.100");
lockPref("network.proxy.http_port",3128);
lockPref("network.proxy.ssl","192.168.0.100");
lockPref("network.proxy.ssl_port",3128);
// Autres options de configuration...
// ...
} catch(e) {
displayError("Erreur dans le fichier de configuration local :", e);
}
```

32. Version ESR : https://www.mozilla.org/en-US/firefox/organizations/all. Version standard : https://www.mozilla.org/en-US/firefox/new/.

Il est précisé que pour davantage de flexibilité, il est également possible de centraliser ce dernier fichier de configuration sur un espace partagé[33] comme un site Web interne. Dans ce cas, le fichier `mozilla.cfg` devient un simple chargeur d'URL vers un troisième fichier de configuration :

```
// Configuration de Firefox - Chargeur URL
try {
// Options de configuration de proxy
lockPref("autoadmin.global_config_url", "http://intranet.local/config.cfg");
lockPref("autoadmin.append_emailaddr",false);
// Autres options de configuration...
// ...
} catch(e) {
displayError("Erreur dans le fichier de configuration local :", e);
}
```

Le fichier `config.cfg` (ou un quelconque autre nom à la discrétion de l'entité) précédemment référencé et déposé à l'URL indiquée devient alors le fichier contenant tous les paramètres de configuration souhaités. Ce fichier est chargé à chaque lancement de Firefox :

```
// Configuration de Firefox
try {
// Options de configuration de proxy
lockPref("network.proxy.http","192.168.0.100");
lockPref("network.proxy.http_port",3128);
lockPref("network.proxy.ssl","192.168.0.100");
lockPref("network.proxy.ssl_port",3128);
// Autres options de configuration...
// ...
} catch(e) {
displayError("Erreur dans le fichier de configuration distant :", e);
}
```

En suivant cette méthode, la configuration Firefox sera commune à tous les comptes utilisateurs d'un poste de travail où la configuration est télé-déployée.

### Télé-déploiement des fichiers de configuration par GPP/GPO

Les fichiers de configuration requis sur les postes (`mozilla.cfg` et `local-settings.js` dans l'exemple donné précédemment) peuvent être déployés simplement par GPP (*Group Policy Preferences*). Étant donné que Firefox n'est pas installé dans un dossier identique sur les systèmes 32 et 64 bits, il est donc nécessaire de réaliser le déploiement de manière distincte en fonction du type de système d'exploitation.

Pour appliquer une GPO aux seuls postes utilisateurs 64 bits, il est possible d'utiliser la fonctionnalité de filtre WMI des stratégies de groupes (dans l'espace de noms `"root\CIMV2"` avec la requête « `Select * from Win32_Processor where AddressWidth = '64'` »). Pour appliquer une GPO aux seuls postes utilisateurs 32 bits, la requête devient « `Select * from Win32_Processor where AddressWidth = '32'` »). Ce filtre WMI permet alors d'appliquer chacune des deux GPP de déploiement des fichiers de configuration aux postes 32 ou 64 bits respectivement.

33. L'entité veillera à la sécurité d'accès de cet espace, pour éviter que le fichier de configuration puisse être modifié par un utilisateur non privilégié. Elle étudiera également la compatibilité avec ses postes nomades. Lorsque l'espace partagé est temporairement indisponible, le lancement de Firefox est retardé d'environ trois secondes, mais la configuration obtenue au dernier chargement réussi reste appliquée.

Au niveau de la console de gestion des stratégies de groupe du domaine, ces deux GPO auront les paramètres suivants :

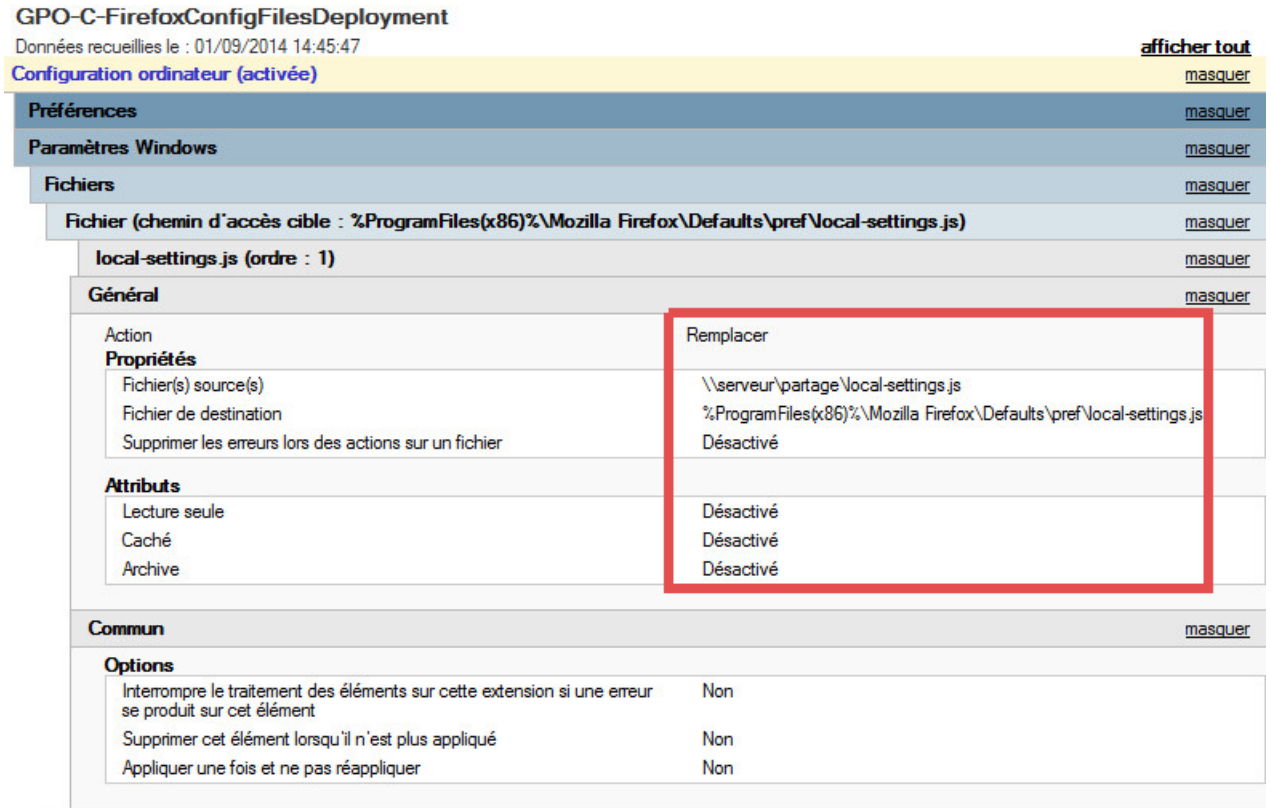


FIGURE 3 – GPO de déploiement du fichier `local-settings.js` sur les systèmes 64 bits.

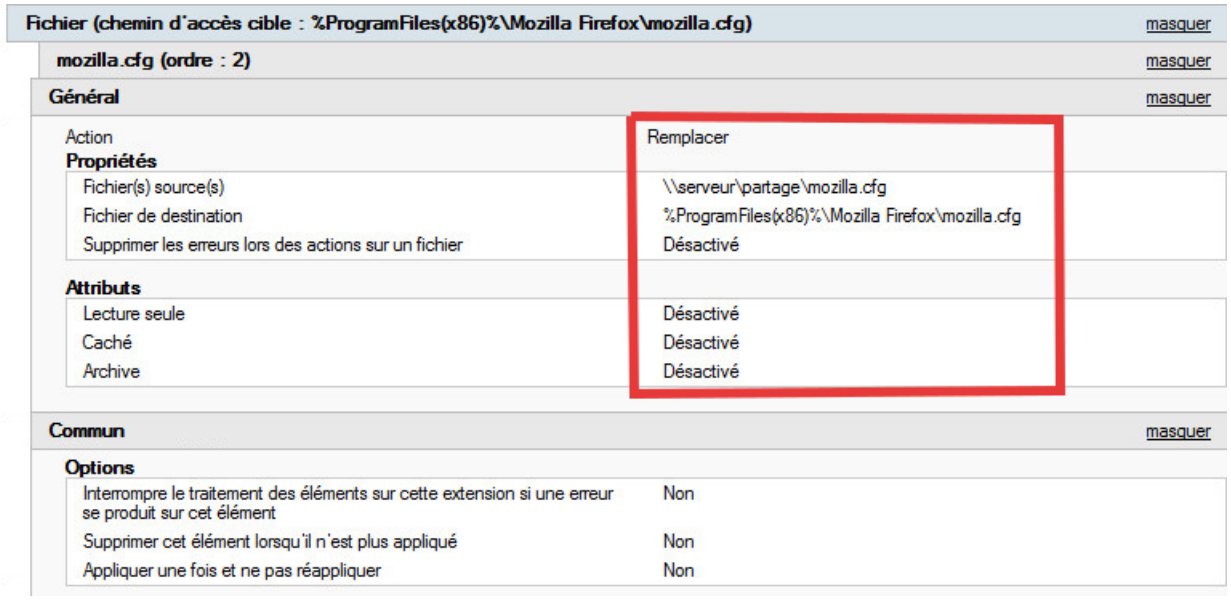


FIGURE 4 – GPO de déploiement du fichier `mozilla.cfg` sur les systèmes 64 bits.

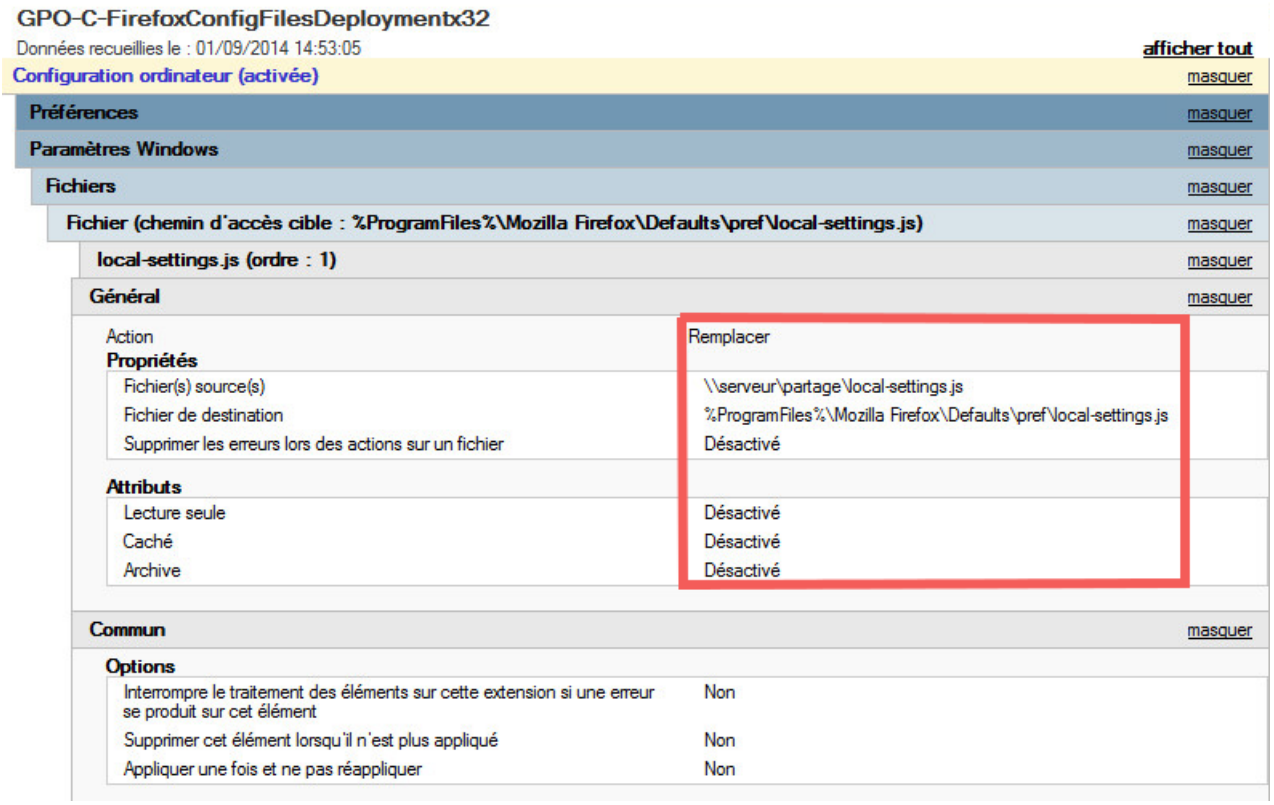


FIGURE 5 – GPO de déploiement du fichier `local-settings.js` sur les systèmes 32 bits.

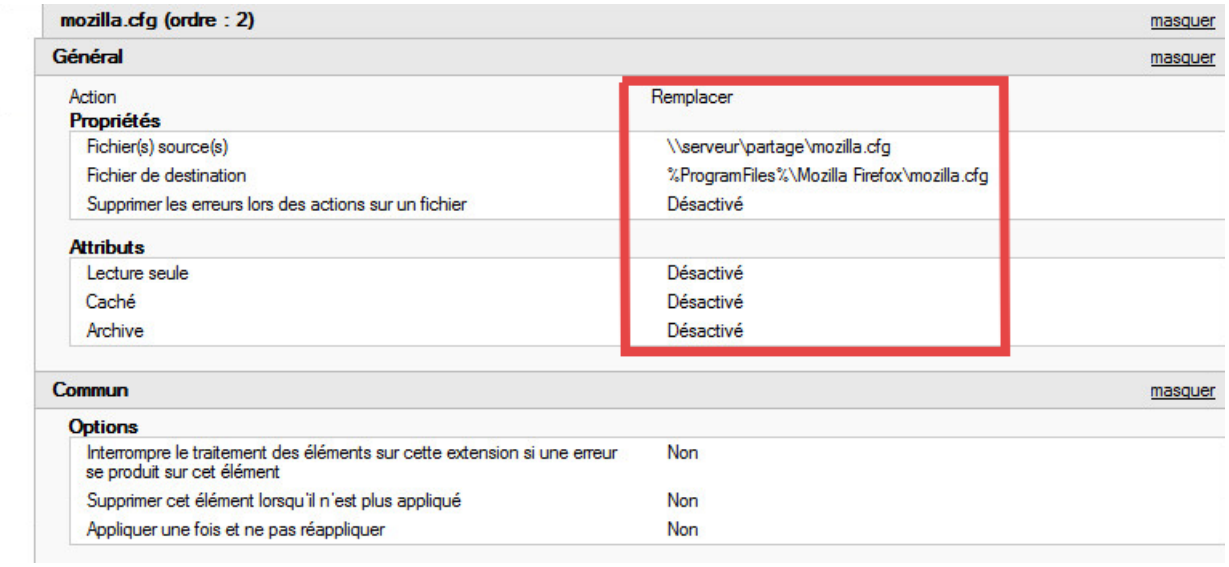


FIGURE 6 – GPO de déploiement du fichier `mozilla.cfg` sur les systèmes 32 bits.

# Annexe III : Déploiement et maîtrise des magasins de certificats des profils utilisateurs Firefox

Tout d'abord, il est précisé qu'un écrasement du fichier `cert8.db` d'un profil Firefox a pour résultat de supprimer les certificats utilisateurs qu'il contient (il ne restera alors plus que les clés privées associées à ces derniers dans le fichier `key3.db`). La complexité de déploiement et de maîtrise des magasins de certificats des profils utilisateurs varie donc en fonction du contexte d'utilisation du navigateur.

Il à noter également que les certificats d'autorités racines de confiance pré-intégrés à Firefox sont présents en dur dans l'exécutable Firefox et non pas dans les magasins de certificats `cert8.db`. Il n'est donc pas possible de les supprimer à moins de recompiler Firefox à partir des sources [34] (ces certificats sont renseignés dans le fichier `certdata.txt` à l'emplacement `security/nss/lib/ckfw/builtins/` de l'arborescence des sources).

## Scénario 1 : les utilisateurs de Firefox n'ajoutent pas de certificats utilisateurs à leur magasin de certificats Firefox

Dans ce cas, une solution simple consiste à copier régulièrement un fichier `cert8.db` de référence dans les profils Firefox des utilisateurs. Comme le nom des sous dossiers de profils Firefox ne peuvent pas être déterminés à l'avance, il n'est pas possible de copier ce fichier par GPP (*Group Policy Preferences*). Par contre, cela peut être fait simplement par GPO via un script d'ouverture de session. Le script PowerShell suivant illustre une manière de procéder :

```
# Répertoire contenant le fichier à copier
$sFFCertLocation = 'chemin_vers_le_répertoire_local_ou_le_partage_réseau_contenant_cert8.db'

# Fichier cert8.db à copier
$sFFCertDB = "$sFFCertLocation\cert8.db"

# Chemin complet vers les profils Firefox
$sFFProfiles = $env:APPDATA + '\Mozilla\Firefox\Profiles'
$lFFProfiles = Get-ChildItem -Path $sFFProfiles |
Where-Object { $_.Attributes -band [System.IO.FileAttributes]::Directory }

# Copie et remplacement du fichier dans les profils Firefox
foreach ($oProfile in $lFFProfiles) {
  Copy-Item -Path $sFFCertDB -Destination $oProfile.FullName -Force
}
```

Le fichier de référence à déployer peut être récupéré sur un profil Firefox existant dont le magasin de certificats à été configuré, ou bien encore créé en utilisant l'outil de gestion de magasins certificats de Mozilla `certutil.exe` [35].

34. Les sources de Firefox sont disponibles sur le site de Mozilla à l'adresse https://developer.mozilla.org/fr/docs/Téléchargement_du_code_source_de_Mozilla.

35. Voici un article expliquant l'utilisation de `certutil.exe` sur le site de Mozilla : https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil. L'outil compilé n'est plus proposé au téléchargement par Mozilla, mais les sources sont disponibles à l'adresse https://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/ et un article de Mozilla explique la procédure de compilation à suivre : https://developer.mozilla.org/en-US/docs/Mozilla/Developer_guide/Build_Instructions/Windows_Prerequisites.

## Scénario 2 : les utilisateurs de Firefox sont susceptibles d'ajouter des certificats utilisateurs à leur magasin de certificats Firefox

Dans ce cas, le fichier `cert8.db` ne doit pas être écrasé. Les magasins de certificats devront alors être mis à jour par lignes de commandes en utilisant l'outil de Mozilla `certutil.exe`. La première étape consiste à déployer l'outil `certutil.exe` et ses dépendances sur les postes utilisateurs. Cela peut être réalisé par GPP avec la méthode illustrée en annexe II. Le dossier de destination est sans importance et au choix de l'entité. Les fichiers à copier sont :

- `certutil.exe` ;
- `libnspr4.dll` ;
- `libplc4.dll` ;
- `libplds4.dll` ;
- `nss3.dll` ;
- `nssutil3.dll` ;
- `msvcr100.dll` ;
- `smime3.dll`.

Par la suite, différents scripts d'ouverture de session permettraient de maîtriser les magasins de certificats des profils utilisateurs Firefox. Voici quelques exemples de scripts PowerShell. Ces scripts sont des illustrations permettant au lecteur de mieux appréhender la problématique de maîtrise des magasins de certificats Firefox. Ils nécessitent une adaptation à l'environnement de l'entité avant tout test et passage en production.

Script permettant de supprimer tous les certificats ajoutés aux magasins de certificats des profils utilisateurs Firefox, tout en y préservant les certificats utilisateurs :

```
# Script de suppression des certificats ajoutés aux magasins des
# profiles Firefox, à l'exception des certificats utilisateurs.
#
# Attention :
# Ce script est sensible au format de sortie de l'outil certutil.exe
# S'il venait à changer, ce script serait à réadapter.
# Il est primordial de tester ce script dans l'environnement
# de l'entité avant son exécution en production sur les postes de travail

Set-StrictMode -Version 2.0

# Répertoire de certutil à changer par celui de l'entité
$sPathToCertutil = 'E:\PROJETS\Firefox\NSS-3.14.2\NSS-3.14.2\certutil.exe'

# Chemin complet vers les profils Firefox
$sFFProfiles = $env:APPDATA + '\Mozilla\Firefox\Profiles'
$lFFProfiles = Get-ChildItem -Path $sFFProfiles | Where-Object { $_.Attributes -band [
    System.IO.FileAttributes]::Directory }

# Pour chaque profil Firefox :
foreach ($oProfile in $lFFProfiles) {
    $sPathToDB = $oProfile.FullName

    # Exécution de certutil pour lister les certificats
    $sCertutilOutput = &"$sPathToCertutil" -L -d "$sPathToDB"
    $aLines = $sCertutilOutput -Split '[\r\n]'

    # Attributs des certificats à ne pas supprimer
    # ("u,u,u" pour les certificats utilisateurs)
    $sAttributesToKeep = @('u,u,u')

    foreach ($sLine in $aLines) {
        $sAttributes = ''
        $sNickName = ''
```

```
        # Supression des lignes vides et de l'en-tête
        $sLine = $sLine.Trim()
        if ([string]::IsNullOrEmpty($sLine) -Or
            ($sLine -match '^\s*Certificate Nickname\s+Trust Attributes\s*$') -Or
            ($sLine -match '^\s*SSL,S/MIME,JAR/XPI\s*$')) {
            continue
        }

        # Récupération des attributs en fin de ligne
        for ($i = $sLine.Length - 1; $i -ge 0; $i--) {
            if ($sLine[$i].ToString() -match '^\s$') {
                break
            }
            $sAttributes = $sLine[$i] + $sAttributes
        }

        # Récupération du nom convivial
        if ($i -gt 0) {
            $sNickName = $sLine.Substring(0, $i).Trim()
        }
        if ($sAttributes -notcontains $sAttributesToKeep) {
            &"$sPathToCertutil" -D -n "$sNickName" -d "$sPathToDB"
            if (!$?) {
                Write-Output "Le certificat $sNickName n'a pas été supprimé."
            }
        }
    }
}
```

Script permettant d'ajouter[36] des certificats serveurs ou d'autorités de certification racines de confiance de l'entité :

```
# Script d'ajout de certificats dans les magasins de certificats des
# profils Firefox
#
# Attention :
# Il est primordial de tester ce script dans l'environnement
# de l'entité avant son exécution en production sur les postes de travail

# Liste de certificats à importer
# Chemin complet de certutil.ex (à changer par celui de l'entité)
$sPathToCertutil = 'E:\PROJETS\Firefox\NSS-3.14.2\NSS-3.14.2\certutil.exe'

# Certificats à importer, sous forme de triplets (chemin du .cer, nom convivial, attributs)
$aCerts = @(

# Autorités de certification
('E:\PROJETS\Firefox\CACerts\MONAC.cer','MONAC','c,c,c'),

# Certificats serveurs
('E:\PROJETS\Firefox\SSLSrvCerts\MONSERVER.cer','MONSERVER','P,,')
)

# Chemin complet vers les profils Firefox
$sFFProfiles = $env:APPDATA + '\Mozilla\Firefox\Profiles'
$lFFProfiles = Get-ChildItem -Path $sFFProfiles |
Where-Object { $_.Attributes -band [System.IO.FileAttributes]::Directory }

# Pour chaque profil Firefox
foreach ($oProfile in $lFFProfiles) {
    $PathToDB = $oProfile.FullName

    # Exécution de certutil pour importer les certificats
    foreach ($aCert in $aCerts) {
```

36. L'ajout de certificats nécessite le positionnement d'attributs de confiance pour chacun des 3 périmètres (SSL/TLS, S/MIME, JAR/XPI). La liste des attributs possibles est consultable à l'adresse https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/tools/NSS_Tools_certutil.

```
        &"$sPathToCertutil" -A -n $aCert[1] -t $aCert[2] -i $aCert[0] -d "$PathToDB"
    }
}
```

# Annexe IV : Télé-déploiement par GPO d'un module de recherche personnalisé

Un module de recherche consiste en un fichier XML stocké dans le sous dossier `searchplugins` d'un profil Firefox (pour un utilisateur) ou bien du répertoire d'installation de Firefox (pour tous les utilisateurs de la machine). L'obtention de nouveaux modules de recherche peut se faire simplement à l'adresse https://addons.mozilla.org/fr/firefox/search/?atype=4, chaque moteur ajouté se verra alors stocké dans le profil Firefox sous la forme d'un fichier XML pré-configuré. Un administrateur qui souhaite télé-déployer un module de recherche personnalisé (moteur de recherche en intranet par exemple) pourra alors aisément adapter un de ces fichiers XML à ses besoins.

Pour l'ajout du moteur de recherche « moteur.intranet.com », le contenu du fichier XML serait le suivant :

```
<SearchPlugin xmlns="http://www.mozilla.org/2006/browser/search/"
xmlns:os="http://a9.com/-/spec/opensearch/1.1/">
<os:ShortName>moteur.intranet.fr</os:ShortName>
<os:Description>moteur de recherche intranet</os:Description>
<os:InputEncoding>UTF-8</os:InputEncoding>
<os:Image width="16" height="16"> au format png en
    base64</os:Image>
<SearchForm>https://moteur.intranet.fr/</SearchForm>
<os:Url type="application/x-suggestions+json" method="GET"
template="http://moteur.intranet.fr/suggest">
  <os:Param name="q" value="{searchTerms}"/>
  <os:Param name="client" value="firefox"/>
</os:Url><os:Url type="text/html" method="GET" template="https://moteur.intranet.fr/">
  <os:Param name="q" value="{searchTerms}"/>
  <os:Param name="client" value="firefox"/>
</os:Url>
</SearchPlugin>
```

Dans ce fichier, il convient de remplacer les termes « image au format png en base64 » par une image au format PNG d'une taille de 16*16 pixels et encodée en base64.

Pour déployer ces fichiers XML sur les postes utilisateurs dans le sous dossier `searchplugins` du répertoire d'installation de Firefox, il est possible d'utiliser les GPP (*Group Policy Preferences*) avec la méthode illustrée en annexe II.