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 3 août 2015

N° DAT-NT-16/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 31

Note technique

Recommandations pour le déploiement sécurisé du navigateur Google Chrome 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 Google Chrome 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, BAI, FRI, BAS, LAM, LRP	BSS	SDE	3 août 2015

Évolutions du document :

Version	Date	Nature des modifications
1.0	02 avril 2014	Version initiale
1.1	3 août 2015	Actualisation de la note

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

Chrome est un navigateur Web gratuit édité par Google dont la première version stable sous Windows date de fin 2008. Il est aujourd'hui devenu l'un des navigateurs les plus utilisés par les internautes [1]. Son système de « bac à sable » [2], ses fonctionnalités de déploiement et de configuration centralisées, et son système de mises à jour automatiques réactif présentent un certain intérêt [3].

Doté de fonctionnalités de déploiement et de configuration centralisées, ainsi que d'un système de mises à jour automatiques réactif, l'usage de ce navigateur en entreprise est tout à fait envisageable.

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 de stratégies de sécurité spécifiques à Google Chrome dans le cadre d'un télé-déploiement 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 massive sur Internet. Viennent également s'ajouter les vulnérabilités propres aux différents greffons intégrés aux navigateurs et dont les processus de mise à jour sont généralement indépendants de ceux du navigateur (le terme anglais *plugins* est utilisé dans la suite du document à la place du terme « greffons » pour des raisons de correspondance avec les modèles d'administration fournis par Google et pour éviter toute confusion du lecteur).

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 le principal vecteur d'attaque utilisé et, plus largement, un problème pour la sécurité des systèmes d'information.

Du point de vue de la sécurité, Google Chrome a comme particularités d'intégrer nativement un plugin *Adobe Flash Player* et une visionneuse PDF, tous deux exécutés en « bac à sable ». Leurs mises à jour de sécurité s'effectuent simultanément avec celles du navigateur, ce qui évite d'avoir à gérer ces mises à jour par ailleurs. Ces plugins sont toutefois désactivables.

3 Préoccupations relatives au respect de la vie privée et à la confidentialité

Un point d'attention à l'encontre de Google Chrome concerne le non respect de la confidentialité du fait de la transmission d'informations à Google. En effet, tout entité se lançant dans le déploiement de ce navigateur est fortement invitée à prendre connaissance du « livre blanc sur la confidentialité dans

1. Sources : www.atinternet.com et www.w3schools.com.
2. Environnement d'exécution contrôlé et restreint.
3. Voir les avis de sécurité et bulletins d'actualité relatifs aux principaux navigateurs sur le site du CERT-FR.

Google Chrome » [4]. Ce livre blanc se veut détailler l'ensemble des informations qui sont communiquées à Google par le navigateur. La plupart ont trait à certaines fonctionnalités et concernent par exemple :

- la recherche prédictive ou instantanée, de manière à fournir des résultats optimisés ;
- les statistiques anonymes d'utilisation des applications, pour mesurer leur popularité ;
- la protection contre le hameçonnage, les logiciels malveillants, ou les attaques par le milieu avec faux certificats SSL.

Certaines fonctionnalités devraient donc être désactivées dès lors qu'elles vont à l'encontre des besoins en confidentialité des utilisateurs. Une entité qui le souhaite pourrait tenter de bloquer tout trafic réseau à destination des serveurs de Google pour se prémunir d'une quelconque transmission d'informations. Néanmoins, une telle démarche, que l'on pourrait juger excessive et qui empêcherait l'utilisation des services de Google, nécessiterait de bien contrôler les flux en sortie des pare-feu mais également de référencer les plages d'adresses publiques appartenant à Google afin de les bloquer.

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 des mises à jour automatiques selon la politique de mise à jour de l'entreprise et sans intervention de l'utilisateur.

Dans cette optique, Google met à disposition des modèles d'administration pour Active Directory qui permettent de définir des stratégies de configuration d'ordinateurs et d'utilisateurs. Ces stratégies reposent sur différents paramètres du navigateur décris dans ce document. Ils présentent l'intérêt de pouvoir être verrouillés et non modifiables par les utilisateurs. Toutes les recommandations permettant de configurer de manière sécurisée Chrome sont détaillées en annexe I.

4.1 Choix des plugins

Les plugins Chrome peuvent être développés en utilisant une des deux interfaces de programmation suivantes :

- NPAPI : architecture datant de Netscape et n'apportant pas de fonction de sécurité convenable du fait de l'exécution des plugins avec le niveau de privilège de l'utilisateur. Une vulnérabilité affectant un plugin permet alors de compromettre la session ou le système. Depuis avril 2015 (Chrome version 42), les plugins NPAPI sont obsolètes et bloqués par défaut mais ré-activables via les paramètres `EnabledPlugins` et `PluginsAllowedForUrls`. Le support des plugins NPAPI sera toutefois complètement supprimé en septembre 2015 avec la version 45 de Chrome ;
- PPAPI : projet lancé en 2009 dont l'objectif est de rendre les plugins davantage portables et sécurisés, notamment par leur exécution en « bac à sable » dans des processus possiblement séparés du navigateur et du moteur de rendu. Lorsqu'elle se produit, l'exploitation de vulnérabilités du plugin reste alors confinée au processus d'exécution de ce dernier et ne permet pas, à moins d'exploitation de vulnérabilités successives du système de « bac à sable », de s'étendre au navigateur.

Sous Google Chrome, l'adresse `chrome://plugins` permet de consulter, en choisissant l'affichage détaillé, la liste des plugins activés et l'API utilisée par chacun d'eux. Aujourd'hui, et malgré la fin

4. Disponible à l'adresse http://www.google.com/intl/fr/chrome/browser/privacy/whitepaper.html.

de support annoncée de NPAPI, quelques plugins continuent d'utiliser cette interface. C'est le cas par exemple de Java, Silverlight et Unity qui ne seront donc plus utilisables à partir de septembre 2014. Les principaux plugins utilisent à présent PPAPI et s'exécutent donc en « bac à sable ».

R1	D'ici à septembre 2014, il est déconseillé de contourner le blocage par défaut des plugins utilisant l'interface NPAPI. Toute activation forcée de plugin basé sur NPAPI apporte un risque non négligeable de compromission du système. Les plugins PPAPI *Flash Player*, *Chrome PDF Viewer*, *Google Update* et *Native Client* devraient suffire à la plupart des usages. Il est donc recommandé de n'autoriser que ceux-là après confirmation qu'ils sont réellement nécessaires.

Note : Les paramètres de configuration relatifs aux plugins sont détaillés en section « Paramètres de contenu » de l'annexe I.

4.2 Choix des extensions

Le mécanisme d'extensions rend possible l'écriture de programmes (extensions) en langage interprété permettant ainsi l'ajout de fonctionnalités ou la personnalisation du navigateur. Les extensions ne s'exécutent pas au niveau système ou dans un processus spécifique mais uniquement au niveau du navigateur via un système de permissions qui leurs sont propres et, en fonction des libertés qui leurs sont accordées. Si elles présentent moins de risques que les plugins, il convient malgré tout d'être vigilant dans leur usage.

Pour commencer, une extension demande, légitimement ou non, certaines permissions qui lui donnent entre autres[5] accès en lecture et en écriture aux cookies, aux données utilisateur, au contenu des pages web visitées, au presse-papier ou encore à la configuration du serveur mandataire (proxy).

Une extension avec d'importantes permissions peut ainsi accéder à des informations sensibles concernant la navigation de l'utilisateur puis les envoyer à un serveur malveillant sur Internet. Une extension peut également introduire de nouveaux comportements indésirables suite à une mise à jour ; rien ne laisse présager qu'une extension qui n'est pas aujourd'hui malveillante ne le sera pas demain.

Par ailleurs, de nombreuses extensions présentent des vulnérabilités qui peuvent être exploitées de différentes manières (par le contenu des pages visitées, par courriels spécifiquement forgés et consultés par webmail, etc.) afin de profiter des autorisations qui leurs sont accordées. Ces extensions vulnérables peuvent également servir à exploiter, par rebond, les vulnérabilités d'éventuels plugins NPAPI activés et ainsi obtenir un accès complet au système.

R2	Dans le cadre d'une configuration durcie, par défaut, il est recommandé de n'autoriser aucune extension hormis celles qui se justifient par un réel besoin métier à satisfaire (extensions spécifiques d'aide au développement Web par exemple).

Note : La plupart des entités pourront toutefois choisir de déployer certaines extensions qu'elles jugeront être de confiance. Une telle décision doit être prise en ayant conscience des conséquences potentielles. Dans le cas d'extensions développées en interne, il conviendra de prêter une attention particulière à la sécurité de leur code et à ne pas leur accorder plus de permissions que nécessaire.

5. Pour plus d'informations sur les permissions et leur criticité, se référer à la page https://support.google.com/chrome_webstore/answer/186213?hl=fr.

4.3 Choix des politiques de sécurité

R3	Avant tout déploiement de Chrome au sein d'un système d'information dont l'administration est centralisée par Active Directory, il est primordial de définir précisément une politique de sécurité (GPO, *Group Policy Object*). Celle-ci devra restreindre l'utilisation des plugins et des extensions et inclure des règles de configuration importantes pour la sécurité de la navigation.

Une telle politique garantira alors l'utilisation du navigateur dans une configuration durcie et verrouillée. Les recommandations de paramétrage qui suivent sont données à titre indicatif dans cette optique. Elles doivent donc être modulées selon les besoins métier 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, principalement pour les applications métier, étant donné qu'elles peuvent être incompatibles avec certains usages ou applications légères (applications Web).

La liste des règles de configuration disponibles est sujette à des évolutions constantes de l'éditeur. Ainsi, les recommandations et leurs indications de mise en œuvre figurant dans ce document sont basées sur les règles de configuration de Chrome dans sa version 44. Ces dernières pourront être adaptées selon la version du navigateur déployé à la date de lecture du document.

Ces règles de configuration peuvent s'appliquer aussi bien aux ordinateurs qu'aux utilisateurs. Il convient donc de choisir un périmètre adéquat et de créer plusieurs GPO spécifiques aux particularités de chaque périmètre.

Les règles de configuration de Chrome sont pour la plupart classées par catégories ; ce document les reprend donc à l'identique. Les règles relatives à ChromeOS, qui figurent également dans les modèles d'administration de Google Chrome et sans distinction claire, sont hors périmètre et ne sont pas traitées dans ce document. Les valeurs recommandées sont données telles qu'indiquées dans le modèle d'administration par GPO. Les termes *Activer* et *Désactiver* peuvent donc être ambigus :

- une valeur *Activer* pour une règle intitulée « Activer telle fonctionnalité » a pour effet d'activer la fonctionnalité ;
- une valeur *Activer* pour une règle intitulée « Désactiver telle fonctionnalité » a pour effet de désactiver la fonctionnalité.

Pour être verrouillée, une règle doit être activée ou désactivée. Par contre, dès lors qu'elle est non configurée, l'utilisateur a toute liberté pour la configurer lui même.

R4	Il est donc fortement conseillé de laisser le minimum de règles non configurées.

L'annexe I de ce document reprend à l'identique les sous-sections qui suivent et indique les paramètres de configuration permettant d'appliquer les recommandations formulées ici.

4.3.1 Options d'accès à distance

L'application de bureau à distance Google Chrome permet à un utilisateur, depuis le navigateur, de partager son bureau ou d'accéder au bureau d'un autre utilisateur à la manière du bureau à distance de Windows. L'accès se fait sur la base d'un code PIN à usage unique généré aléatoirement.

R5	Il est déconseillé d'installer l'application de bureau à distance Google Chrome ou de permettre aux utilisateurs de l'installer.

Les options d'accès à distance seront alors ignorées aussi, toutes les règles de configuration liées à ces options peuvent être laissées à la valeur « *non configuré* ».

4.3.2 Extensions

Conformément à la recommandation R2 toutes les extensions doivent par défaut être interdites. Un attaquant pouvant inciter un utilisateur à installer une extension malveillante, les extensions autorisées doivent explicitement faire partie d'une liste blanche pour être installées.

R6	Par mesure de sécurité, il est fortement recommandé d'interdire toutes les extensions en les mettant en liste noire (à l'aide du caractère « * »), puis de lister exhaustivement les extensions autorisées en les ajoutant en liste blanche qui est prioritaire sur la liste noire.

Note : Si certaines extensions ne sont nécessaires que pour des catégories d'utilisateurs ou d'ordinateurs bien précises, il est dans ce cas pertinent de créer plusieurs GPO avec des listes blanches spécifiques.

4.3.3 Gestionnaire de mots de passe

Le gestionnaire de mots de passe de Chrome permet de mémoriser les mots de passe saisis dans les formulaires Web. Ces derniers sont éventuellement consultables par l'utilisateur.

R7	Il est conseillé de désactiver le gestionnaire de mots de passe de manière à imposer une 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 [6].

4.3.4 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

6. KeePass est un exemple de solution certifiée par l'ANSSI au titre de la CSPN qui peut être utilisée avec Chrome.

moteur de recherche français qui s'appuie sur une connexion chiffrée (en parallèle, l'entité met alors en liste noire les adresses des moteurs de recherche qu'elle souhaite interdire).

R8	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.

R9	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.

4.3.5 Google Chrome Frame

Google Chrome Frame est un module pour Microsoft Internet Explorer permettant d'y afficher des applications Web en HTML5. Son utilisation est donc hors périmètre, et toutes les règles de configuration liées à Google Frame peuvent donc être laissées à la valeur « *non configuré* ».

4.3.6 Page(s) d'accueil

R10	Lors du démarrage du navigateur, il est préférable de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une page connue et de confiance, comme par exemple : – le portail Web de l'Intranet, pour la navigation Intranet ; – le site Internet de l'entité (voire le moteur de recherche par défaut), pour le navigateur Internet.

Note : 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. Il est alors possible de récupérer ces cookies sauvegardés pour s'authentifier à la place de l'utilisateur sans avoir connaissance du mot de passe.

4.3.7 Paramètres de contenu

Les paramètres relatifs aux types de contenus qui peuvent s'afficher sur les sites Web ainsi qu'aux informations qui peuvent être utilisées pour personnaliser ce contenu sont importants pour la sécurité de la navigation. Certains paramètres peuvent avoir une incidence sur la faculté des utilisateurs à naviguer sur certains sites. Comme pour les extensions avec listes blanche et noire, il est globalement recommandé d'interdire par défaut puis d'autoriser une liste de sites spécifiques à effectuer telle ou telle action. Cette liste se construira soit par analyse des journaux sur une période de temps déterminée, soit au fur et à mesure des problèmes de navigation remontés par les utilisateurs.

R11	Il est recommandé d'interdire par défaut les notifications sur le bureau ainsi que les fonctions de géolocalisation (fonctionnalité de localisation géographique du client).

Les « pop-ups » devraient idéalement être désactivées mais certains sites Internet ne pourront alors plus être consultés. Il sera dans ce cas nécessaire d'autoriser les « pop-ups » sur une liste de sites définie au fur et à mesure des problèmes rapportés par les utilisateurs. En fonction des usages qui sont faits

d'Internet au sein de l'entité, cela peut donc s'avérer trop contraignant pour un service informatique manquant de ressources. Un compromis peut alors consister à ne pas configurer cette règle mais à laisser l'utilisateur accepter lui-même les « pop-ups » pour les sites qui les nécessitent. De même, l'interdiction des cookies pouvant empêcher la navigation sur de nombreux sites Internet, les images ainsi que les cookies pourront être autorisés uniquement le temps de la session de navigation.

R12	La machine virtuelle JavaScript de Chrome (de nom de code « `V8` ») offre une surface d'attaque supplémentaire et fait l'objet de vulnérabilités régulières. De ce fait, pour une configuration très durcie et une navigation sur un périmètre précis, il est préférable d'interdire JavaScript pour tous les sites et d'ajouter des exceptions au cas par cas via la règle `JavaScriptAllowedForUrls`.

Note : Dans les autres cas, étant donné que JavaScript est aujourd'hui souvent nécessaire à la navigation Internet, on devra la plupart du temps choisir de l'autoriser.

R13	Il est recommandé d'autoriser les plugins sur tous les sites dans la mesure où seuls les plugins `Adobe Flash Player`, `Chrome PDF Viewer` et `Native Client` sont autorisés (recommandation R1), qu'ils s'exécutent en bac à sable et correspondent à un usage souvent incontournable sur Internet. Malgré tout, il reste préférable qu'ils ne soient exécutés qu'à la demande de l'utilisateur pour la lecture d'un contenu attendu.

4.3.8 Serveur mandataires (proxy)

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 établir un canal de contrôle depuis le poste de travail vers un serveur situé sur Internet. L'utilisation de serveurs mandataires avec authentification peut donc bloquer des connexions sortantes malveillantes. Il s'avère ainsi judicieux de configurer l'utilisation du serveur mandataire par GPO sur les postes d'extrémité.

R14	L'utilisation de serveurs mandataires avec authentification est importante pour la sécurité d'un système d'information.

4.3.9 Authentification HTTP

Les paramètres d'authentification HTTP sont surtout importants pour un navigateur dédié à l'Intranet. La plupart des sites Internet procèdent à de l'authentification par formulaires Web gérés par le code (PHP, ASP, etc.) côté serveur, ce qu'il convient de différencier de l'authentification HTTP opérée par le service Web lui même (Apache, IIS, etc.). Les quatre modes d'authentification HTTP disponibles [7] sont, par ordre croissant de sécurité :

- basic : couple utilisateur/mot de passe transmis en clair au serveur avec un simple encodage en base64 réversible de façon triviale ;
- digest : couple utilisateur/mot de passe envoyé sous forme hachée pouvant être d'un niveau de sécurité dégradé, le serveur peut par exemple choisir d'opérer sans nonce rendant l'échange vulnérable à des attaques par le milieu ;
- NTLM : méthode reposant sur un mécanisme de défi/réponse évitant le rejeu d'authentification ;
- negociate : procède à une authentification par Kerberos si possible, sinon par NTLM.

7. Pour plus d'informations : http://msdn.microsoft.com/en-us/library/Windows/desktop/aa380502.aspx.

R15	Il est recommandé de désactiver les modes d'authentification *basic* et *digest* pour n'autoriser que les modes *NTLM* et *negociate*. Si Kerberos est utilisé par l'ensemble des services accédés par navigateur Web (serveur mandataire compris), le mode *negociate* est dans ce cas le seul à autoriser.

Note : l'utilisation de modes d'authentification faibles est moins risquée dès lors qu'HTTPS est utilisé.
Note : certains services ne prennent en charge que l'authentification HTTP par couple utilisateur/mot de passe. Dans cette éventualité, il conviendra de faire évoluer le système d'authentification des services concernés par formulaires web, certificats voire méthodes d'authentification NTLM ou Kerberos.

R16	Les invites d'authentification de base HTTP (Basic Auth) multi-domaine doivent être désactivées pour se protéger contre les tentatives d'hameçonnage.

Note : À défaut, un contenu tiers peut afficher une boîte d'authentification HTTP qui pourrait tromper l'utilisateur.

4.3.10 Périmètre de navigation

Il est possible de restreindre le périmètre de navigation par le biais des listes blanche et noire d'adresses mais également de schémas d'adresses.

R17	Interdire à 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 Internet 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 abordé en section 5 (« Stratégie de double navigateur »).

4.3.11 Fonctionnalités diverses

La navigateur Google Chrome dispose de fonctionnalités dont la plupart devraient être soit désactivées soit re-configurées. C'est le cas notamment :
- de la connexion à Google Chrome[8] pour la synchronisation des préférences de navigation avec un compte Google ;
- de la saisie automatique ;
- des services *Google Traduction* et *Google Cloud Print*.

La liste complète de ces paramètres figure en annexe I.

8. Pour en savoir plus sur la connexion à Google Chrome, voir `https://support.google.com/chrome/answer/165139`.

4.3.12 Administration système et maintenance

Les paramètres relatifs à l'administration système ont une incidence assez faible sur la sécurité mais certaines précautions peuvent tout de même 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.

4.4 Télé-déploiement initial

Chrome, au même titre que les autres logiciels, devrait idéalement être installé sur les postes de travail par télé-déploiement. Le télé-déploiement est un des fondamentaux d'un système d'information contrôlé et maîtrisé. En effet, il permet de maîtriser les installations, d'homogénéiser les versions et configurations, ainsi que de procéder aux mises à jour de manière réactive et efficace.

Le télé-déploiement peut se faire de plusieurs manières. Les principales et les plus communément utilisées étant :

- le déploiement par GPO (stratégies de groupe pour la gestion centralisée) dans un domaine Microsoft Active Directory ;
- le déploiement à l'aide d'un outil de gestion de parc ou de tout autre produit tiers prévu à cet effet.

L'annexe II de ce document guide le lecteur dans le télé-déploiement et la configuration de Chrome par GPO dans un domaine Active Directory.

4.5 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 exposerait le poste de travail à une attaque. Deux différentes stratégies de mise à jour de Chrome peuvent alors être envisagées :

- la première consiste à simplement laisser la configuration par défaut, le navigateur (ou plutôt le service *Google Update Service*) va alors automatiquement télécharger les mises à jour auprès des serveurs de Google. 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 Google sur Internet, idéalement au travers du proxy d'entreprise qui pourra notamment mettre en cache les binaires.
- la configuration alternative consiste à désactiver le service de mise à jour automatique de Chrome et à réaliser des télé-déploiements manuels des nouvelles versions du navigateur. Il convient dans ce cas d'utiliser le modèle d'administration ADM spécifique à *Google Update*[9] pour désactiver le processus de mise à jour automatique. Cette méthode (détaillée en annexe III) convient davantage aux systèmes d'information de grande taille et lorsque des moyens humains des services informatiques le permettent.

9. lien de téléchargement : `http://dl.google.com/update2/enterprise/GoogleUpdate.adm`.

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 Google par Internet.	- mise en œuvre aisée par les services informatiques ; - haut taux de disponibilité des serveurs de mise à jour de Google.	- 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 ; - peu adapté pour un navigateur dédié à l'Intranet.
contrôlée : la mise à jour automatique de Chrome est désactivée et les services informatiques réalisent des télé-déploiements manuels des nouvelles versions du navigateur.	- permet de tester et valider les mises à jour avant déploiement ; - permet d'adapter les GPO pour tenir compte des éventuelles nouvelles fonctionnalités avant déploiement ; - permet de bloquer tout le trafic à destination des serveurs de Google.	- freine la réactivité des mises à jour ; - nécessite des moyens humains importants.

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 légitimement vouloir en déployer certaines. Dans le scénario d'une mise à jour automatique du navigateur par le *Google Update Service*, les extensions seront elles aussi automatiquement mises à jour. Par contre, dans le contexte de télé-déploiements manuels des nouvelles versions du navigateur, les extensions et applications devront être mises à jour manuellement.

Le cas du plugin Flash PPAPI intégré à Chrome est particulier puisqu'il se met à jour automatiquement et indépendamment du navigateur via le système de *components*, ce qui lui permet d'être rapidement à jour de ses correctifs de sécurité. Les *components* peuvent être mis à jour individuellement et manuellement depuis l'interface accessible en tapant `chrome://components` dans la barre d'adresse.

Concernant le service *Google Update*, 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 Certificats

Google Chrome utilise les certificats du magasin de Windows. Il ne sera donc pas possible d'appliquer des restrictions spécifiques à Chrome sur les certificats sans les appliquer au système d'exploitation dans son ensemble.

R18	Il est par ailleurs recommandé de désactiver l'utilisation de SSL (1, 2 et 3) et de n'autoriser que les protocoles TLS.

Pour aller plus loin, il est également conseillé de restreindre les suites cryptographiques [10] utilisables en désactivant celles reposant sur des algorithmes obsolètes comme RC4, n'utilisant pas de mécanismes de PFS (*Perfect Forward Secrecy*).

Dans les faits, l'application de ces recommandations s'avère compliquée sous Google Chrome au sein d'un système d'information puisque ces restrictions doivent être indiquées en argument de l'exécutable `chrome.exe` [11]. La section suivante traite cette problématique.

6 Arguments de ligne de commande

L'exécutable de Google Chrome prend en charge des arguments de ligne de commande qui ont un effet sur le niveau de sécurité du navigateur. La liste exhaustive des arguments supportés peut être consultée dans le fichier de sources https://src.chromium.org/viewvc/chrome/trunk/src/chrome/common/chrome_switches.cc (sujet à de fréquents changements). Parmi ces arguments figurent entre autres :

- `ssl-min-version` : version minimum de SSL supportée ;
- `ssl-max-version` : version maximum de SSL supportée ;
- `cipher-suite-blacklist` : liste noire de suites cryptographiques ;
- `allow-running-insecure-content` : autoriser des pages HTTPS à exécuter du JavaScript ou du CSS depuis des URLs HTTP ;
- `user-agent` : personnaliser la chaîne *user-agent*.

Au sein d'un système d'informations, il ne sera pas trivial d'interdire certains arguments ou au contraire d'en imposer. Les paramètres de GPO ont priorité sur les options de ligne de commande ayant la même fonction, un utilisateur ne pourra par exemple pas exécuter Chrome en mode *incognito* ou sans serveur mandataire s'il n'y est pas autorisé par GPO.

Des solutions techniques sont envisageables pour imposer des arguments d'exécution, comme par exemple déployer des scripts (PowerShell ou VBScript entre autres) enregistrant un événement WMI empêchant l'exécution de `chrome.exe` sans les arguments définis en central. Une entité qui souhaite maîtriser la sécurité de Google Chrome jusqu'à ces quelques détails devra donc mettre en œuvre une solution imposant les arguments d'exécution de `chrome.exe`.

7 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

10. Les suites cryptographiques supportées par un navigateur peuvent être testées sur le site de l'université de Hannover : https://cc.dcsec.uni-hannover.de. Le registre des suites cryptographiques maintenu par l'IANA est par ailleurs consultable à l'adresse http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml. Pour plus d'informations sur les recommandations de sécurité relatives à SSL/TLS, consulter la note de l'ANSSI datant du 25 juin 2012 : http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/articles-de-conferences/ssl-tls-etat-des-lieux-et-recommandations.html.

11. Arguments `-cipher-suite-blacklist`, `-ssl-version-min` et `-ssl-version-max`.

l'entité à un des vecteurs d'attaque les plus critiques et massivement exploités.

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 une 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 pourrait faire 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 relativement laxiste. Il est alors possible de le configurer pour permettre 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 :

Composant	Action	Valeur
Serveur mandataire	Autoriser	*User-Agent*[12] 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 : - le processus du navigateur Internet (chemin complet de l'exécutable) ; - le processus de mise à jour associé, dans le cas d'une mise à jour automatique par Internet (*GoogleUpdate.exe* pour Google Chrome) ; - tout autre processus autorisé à accéder à Internet via le serveur mandataire.
	Bloquer	TCP en sortie vers le serveur mandataire depuis les autres processus
Pare-feu de passerelle Internet	Autoriser	TCP en sortie vers les ports 443 et 80 depuis : - l'IP source du serveur mandataire ; - 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.

12. Entête HTTP contenant des informations sur le client à l'origine de la requête.

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

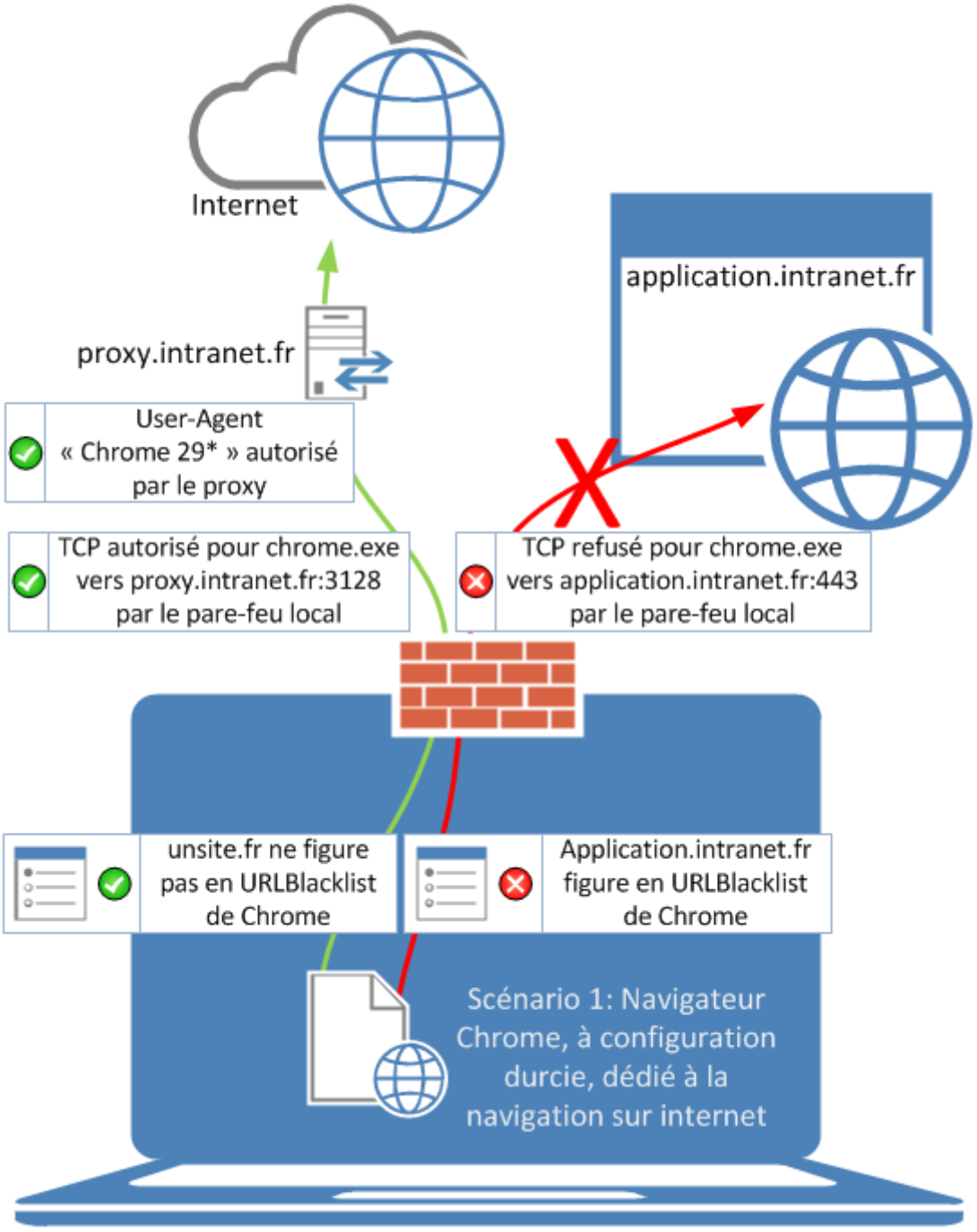

FIGURE 1 – Illustration d'une stratégie de double navigateur, cas où Chrome est utilisé comme navigateur Internet

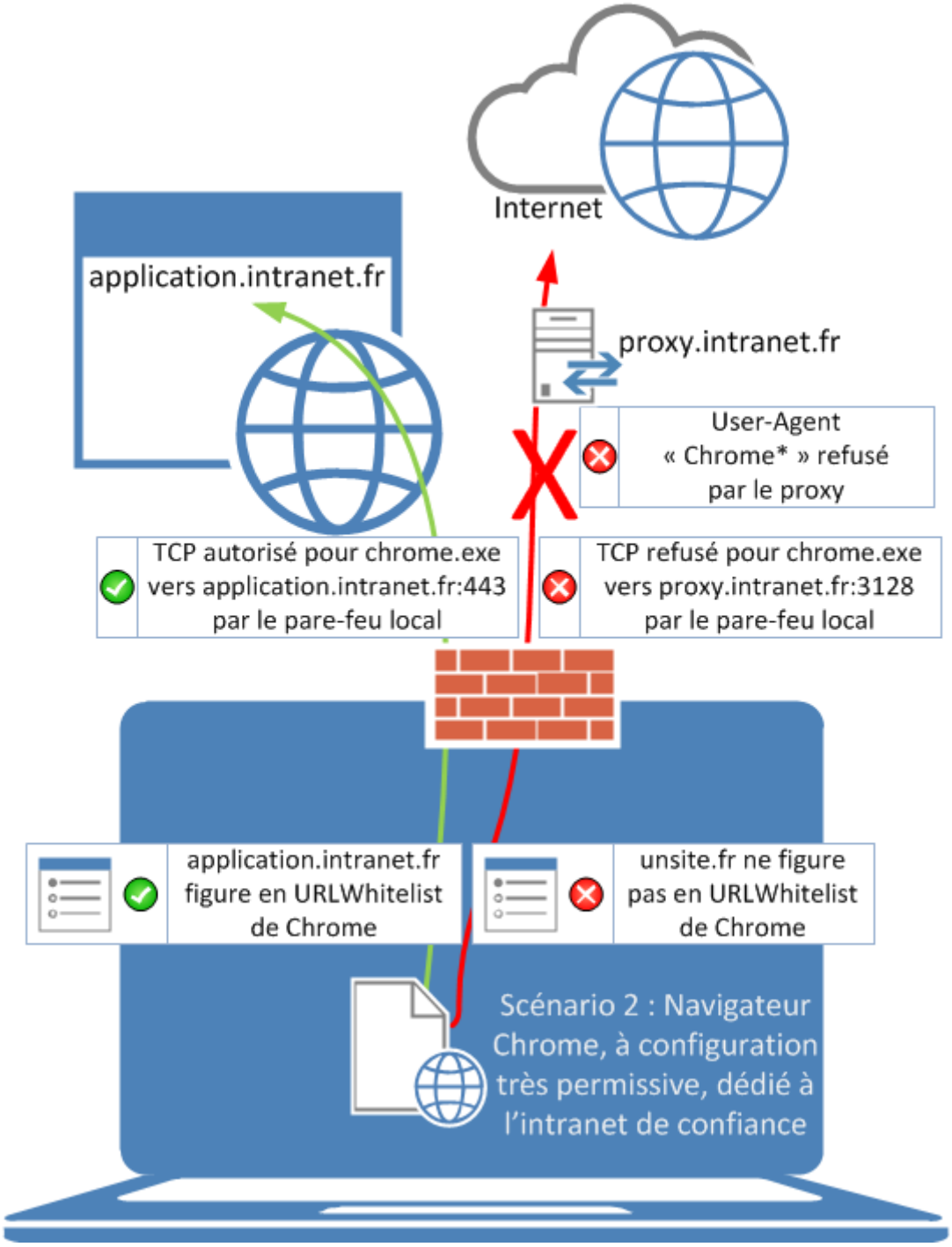

FIGURE 2 – Illustration d'une stratégie de double navigateur, cas où Chrome est utilisé comme navigateur Intranet

Ces figures illustrent deux cas distincts. Le navigateur Chrome 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 Google Chrome

Cette annexe liste les valeurs recommandées permettant de mettre en œuvre les recommandations formulées dans cette note technique. La liste des règles de configuration disponibles est sujette à des évolutions constantes de l'éditeur. Ainsi, les recommandations et leurs indications de mise en œuvre figurant dans ce document sont basées sur les règles de configuration de Chrome dans sa version 44. Ces dernières pourront être adaptées selon la version du navigateur déployé à la date de lecture du document.

Depuis un navigateur Google Chrome, il est possible d'afficher les politiques appliquées et leur valeurs en tapant `chrome://policy` dans la barre d'adresse. Cela peut également être utile au débogage grâce à la colonne « État » qui affiche « OK » ou indique d'éventuelles erreurs dans les valeurs saisies (mauvais format, etc.).

Pour rappel, les valeurs recommandées sont données telles qu'indiquées dans le modèle d'administration par GPO. Les termes *Activer* et *Désactiver* peuvent donc être ambigus :
- une valeur *Activer* pour une règle intitulée « Activer telle fonctionnalité » a pour effet d'activer la fonctionnalité ;
- une valeur *Activer* pour une règle intitulée « Désactiver telle fonctionnalité » a pour effet de désactiver la fonctionnalité.

Pour être verrouillée, une règle doit être activée ou désactivée. Par contre, dès lors qu'elle est non configurée, l'utilisateur a toute liberté pour la configurer lui même. Il est donc fortement conseillé de laisser le moins possible de règles non configurées.

Extensions :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Extensions		
ExtensionAllowedTypes	Configurer les types d'applications ou d'extensions autorisés	*Non configuré*
ExtensionInstallBlacklist	Configurer la liste noire d'installation des extensions	*Activé* avec la valeur *
ExtensionInstallWhitelist	Configurer la liste blanche d'installation des extensions	Cette liste est idéalement vide (paramètre *non configuré*). Dans le cas contraire, le paramètre est *Activé* et la valeur fait figurer de manière exhaustive la liste des identifiants d'extensions autorisés (un identifiant d'extension est une chaîne de 32 caractères)
ExtensionInstallForcelist	Configurer la liste des extensions dont l'installation est forcée	En fonction des besoins, mais idéalement vide donc *non configuré*
ExtensionInstallSources	Configurer les sources d'installation des extensions, des applications et des scripts d'utilisateur	*Non configuré*

Gestionnaire de mots de passe :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Gestionnaire de mots de passe		
PasswordManagerEnabled	Activer le gestionnaire de mots de passe	*Désactivé*
PasswordManagerAllowShowPasswords	Permet aux utilisateurs d'afficher les mots de passe dans le gestionnaire de mots de passe.	*Désactivé*
**Google Chrome **		
ImportSavedPasswords	Importer les mots de passe enregistrés du navigateur par défaut à la première exécution	*Désactivé*

Moteur de recherche par défaut :

Dans ce tableau, la colonne « *valeur recommandée* » est remplacée par un exemple de configuration du moteur de recherche français `https://www.qwant.com` [13] comme celui retenu par défaut. N'importe quel autre moteur de recherche pourrait être utilisé.

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

Nom de stratégie	Description	Exemple
Google Chrome \ Moteur de recherche par défaut		
DefaultSearchProviderSearchURL	URL de recherche du moteur de recherche par défaut	*Activé* avec la valeur : `https://www.qwant.com/?q=searchTerms`
DefaultSearchProviderIconURL	Icône du moteur de recherche par défaut	*Activé* avec la valeur : `https://www.qwant.com/favicon.ico`
DefaultSearchProviderEncodings	Codages du moteur de recherche par défaut	*Non configuré* (utilisera UTF-8 par défaut)
DefaultSearchProviderEnabled	Activer le moteur de recherche par défaut	*Activé*
DefaultSearchProviderName	Nom du moteur de recherche par défaut	*Activé* avec la valeur `Qwant`
DefaultSearchProviderKeyword	Mot clé du moteur de recherche par défaut	*Non configuré*
DefaultSearchProviderSuggestURL	URL de suggestions de recherche du moteur de recherche par défaut	*Désactivé*
DefaultSearchProviderInstantURL	URL de recherche instantanée du moteur de recherche par défaut	*Désactivé*
DefaultSearchProviderAlternateURLs	Liste d'URL alternatives pour le moteur de recherche par défaut	*Désactivé*
DefaultSearchProviderSearchTermsReplacementKey	Paramètre contrôlant le positionnement des termes de recherche pour le moteur de recherche par défaut	*Non configuré*

Viennent ensuite certains paramètres plus généraux relatifs aux fonctionnalités de recherche :

Nom de stratégie	Description	Valeur recommandées
**Google Chrome **		
ImportSearchEngine	Importer les moteurs de recherche du navigateur par défaut à la première exécution	*Désactivé*
SearchSuggestEnabled	Activer les suggestions de recherche	*Désactivé*
ForceSafeSearch	Forcer SafeSearch (contenu pour adultes)	*Désactivé*

Page(s) d'accueil :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Page(s) d'accueil		
HomepageLocation	Configurer l'URL de la page d'accueil	*Activé* avec pour valeur l'adresse du site web choisi par l'entité
HomepageIsNewTabPage	Utiliser la page "Nouvel onglet" comme page d'accueil	*Désactivé*
RestoreOnStartup	Action au démarrage	Il est recommandé d'*Activer* ce paramètre et de choisir d'*ouvrir une liste d'url* (l'Intranet par exemple)
RestoreOnStartupURLs	URL à ouvrir au démarrage	*Activer* avec la même valeur que pour `HomepageLocation`
**Google Chrome **		
ImportHomepage	Importer la page d'accueil du navigateur par défaut à la première exécution	*Désactivé*
ShowHomeButton	Afficher le bouton Accueil sur la barre d'outils	*Activé*

Paramètres de contenu :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Paramètres de contenu		
DefaultCookiesSetting	Paramètre de cookies par défaut	*Activé* avec la valeur *Conserver les cookies pendant toute la durée de la session*
DefaultImagesSetting	Paramètres d'images par défaut	*Activé* avec la valeur *Autoriser tous les sites*
DefaultJavaScriptSetting	Paramètre JavaScript par défaut	*Activé* avec la valeur *Autoriser tous les sites* ou *Interdire tous les sites* en fonction de la marge de manœuvre de l'entité et du durcissement attendu
DefaultPluginsSetting	Paramètre de plug-ins par défaut	*Activé* avec la valeur *Bloquer tous les plug-ins*
DefaultPopupsSetting	Paramètre de fenêtres pop-up par défaut	*Activé* avec la valeur *Interdire tous les sites* ou *Non configuré* en fonction de la marge de manœuvre de l'entité et du durcissement attendu
DefaultNotificationsSetting	Paramètre de notification par défaut	*Activé* avec la valeur *Interdire tous les sites*
DefaultGeolocationSetting	Paramètre de géolocalisation par défaut	*Activé* avec la valeur *Interdire tous les sites*
DefaultMediaStreamSetting	Paramètre MediaStream par défaut	*Activé* avec la valeur *Interdire tous les sites*
AutoSelectCertificateForUrls	Sélectionner automatiquement des certificats client pour ces sites	Lorsque certains sites requièrent une authentification client par certificat, il peut être pertinent d'*activer* ce paramètre pour procéder à une sélection automatique du certificat plutôt que manuelle par l'utilisateur. La valeur de la règle est alors par exemple : `"pattern":"https://monsite.fr", "filter":"ISSUER":"CN":"Mon AC Clients" "pattern":"https://*.monsite.fr", "filter":"ISSUER":"CN":"Mon AC Clients"`
EnableOnlineRevocation Checks	Si des contrôles OCSP/CRL en ligne sont effectués	Au choix de l'entité sachant que Google prévoit de retirer cette fonctionnalité au profit d'une liste locale de certificats révoqués 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).
CookiesAllowedForUrls	Autoriser les cookies sur ces sites	*Non configuré*
CookiesBlockedForUrls	Bloquer les cookies sur ces sites	*Non configuré*

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Paramètres de contenu		
CookiesSessionOnlyForUrls	Autoriser les cookies limités à la session sur ces sites	*Non configuré*, à moins que la règle *DefaultCookiesSetting* interdise les cookies. Dans ce cas textitCookiesSessionOnlyForUrls permet d'indiquer les sites autorisés à créer des cookies le temps de la session.
ImagesAllowedForUrls	Autoriser les images sur ces sites	*Non configuré*
ImagesBlockedForUrls	Bloquer les images sur ces sites	*Non configuré*

JavaScriptAllowedForUrls	Autoriser JavaScript sur ces sites	*Non configuré* si *DefaultJavaScriptSetting* autorise JavaScript sur tous les sites, sinon *Activé* avec comme valeur une liste blanche de sites sous la forme :
		`http://www.exemple.com`
		`[*.].gouv.fr`

JavaScriptBlockedForUrls	Bloquer JavaScript sur ces sites	*Non configuré*
PluginsAllowedForUrls	Autoriser les plug-ins sur ces sites	*Non configuré*, la règle par défaut *DefaultPluginsSetting* s'applique donc : tous les plugins sont bloqués et sur tous les sites.
PluginsBlockedForUrls	Bloquer les plug-ins sur ces sites	*Non configuré*

PopupsAllowedForUrls	Autoriser les fenêtres pop-up sur ces sites	*Non configuré* si *DefaultPopupsSetting* autorise les fenêtres pop-up sur tous les sites, sinon *Activé* avec comme valeur une liste blanche de sites sous la forme :
		`http://www.exemple.com`
		`[*.].gouv.fr`

PopupsBlockedForUrls	Bloquer les fenêtres pop-up sur ces sites	*Non configuré*

NotificationsAllowedForUrls	Autoriser les notifications sur ces sites	*Non configuré* ou *Activé* avec comme valeur une liste blanche de site sous la forme :
		`http://www.exemple.com`
		`[*.].gouv.fr`

NotificationsBlockedForUrls	Bloquer les notifications sur ces sites	*Non configuré*
**Google Chrome **		
AllowOutdatedPlugins	Autoriser l'exécution de plug-ins obsolètes	*Désactivé*
AlwaysAuthorizePlugins	Toujours exécuter les plug-ins qui nécessitent une autorisation	*Désactivé*

EnabledPlugins	Indiquer une liste de plug-ins activés	*Activé*, et listant les seuls plugins autorisés, c'est à dire ceux cités dans la section *Choix des plugins* et basés sur PPAPI :
		`Adobe Flash Player`
		`Chrome PDF Viewer`
		`Native Client`
		`Google Update` (si l'entité opte pour la mise à jour automatique)

Nom de stratégie	Description	Valeur recommandée
Google Chrome \		
DisabledPlugins	Répertorier les plug-ins désactivés	*Activé*, avec la valeur `*` ainsi on désactive tout plugin qui n'est pas explicitement activé par la règle *EnabledPlugins*
DisabledPluginsExceptions	Répertorier les plug-ins pouvant être activés ou désactivés par l'utilisateur	*Désactivé*
DisablePluginFinder	Indiquer si l'outil de recherche de plug-ins doit être désactivé	*Désactivé*
BlockThirdPartyCookies	Bloquer les cookies tiers	*Activé*
AudioCaptureAllowed	Autoriser ou interdire la capture audio	*Désactivé*
VideoCaptureAllowed	Autoriser ou interdire la capture vidéo	*Désactivé*
VideoCaptureAllowedUrls	URL autorisées à accéder aux appareils de capture audio sans avis préalable	*Désactivé*
audioCaptureAllowedUrls	URL autorisées à accéder aux appareils de capture vidéo sans avis préalable	*Désactivé*
Disable3DAPIs	Désactiver la prise en charge des API 3D graphics	*Activé*
AllowFileSelectionDialogs	Autoriser l'appel des boîtes de dialogue de sélection de fichiers	*Activé* avec la valeur *Autoriser*, à moins que l'on veuille volontairement bloquer les téléchargements ou envois de fichier par exemple
SafeBrowsingEnabled	Activer la navigation sécurisée[14]	*Activé*
DisableSafeBrowsingProceedAnyway	Désactiver l'accès au site lors de l'affichage de la page d'avertissement par le service de navigation sécurisée	*Activé*
IncognitoModeAvailability	Disponibilité du mode navigation privée	*Activé* avec le mode `navigation privée disponible` si le navigateur est destiné à la navigation sur Internet, et `navigation privée non disponible` dans le cas contraire

14. La fonctionnalité de navigation sécurisée consiste à synchroniser une liste locale d'adresses de sites maveillants (depuis les serveurs de Google) 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.

Serveur proxy (mandataire) :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Serveur proxy		
ProxyMode	Sélectionner le mode de spécification des paramètres de serveur proxy	*Activé* avec comme valeur *utiliser des paramètres proxy déterminés*
ProxyServer	Adresse ou URL du serveur proxy	*Activé* avec comme valeur l'adresse du proxy à utiliser pour les clients Web sous la forme `ip:port`
ProxyPacUrl	URL d'un fichier .pac de proxy	*Non configuré* et à n'utiliser qu'en cas d'utilisation de serveurs mandataires moins courants (proxy socks par exemple).
ProxyBypassList	Règles de contournement de proxy	*Activé* avec comme valeur les adresses (locales généralement, et séparées par des virgules) pour lesquels l'usage du proxy est contourné. Par exemple : `*.Intranet.fr, 127.0.0.1`
**Google Chrome **		
MaxConnectionsPerProxy	Nombre maximal de connexions simultanées au serveur proxy	*Activé* et à une valeur déterminée (comprise entre 6 et 100, 32 étant une valeur par défaut qui conviendra dans la majorité des cas) en fonction du serveur proxy de l'entité et de sa charge, mais également des usages de navigation (l'utilisation simultanée de plusieurs applications Web pourrait par exemple nécessiter d'augmenter la valeur par défaut)

Authentification HTTP :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Stratégies d'authentification HTTP		
AuthSchemes	Modèles d'authentification compatibles	*Activé* avec comme valeur la liste des modes à autoriser séparés par des virgules. La valeur recommandée est : `ntlm, negociate`.
DisableAuthNegotiateCnameLookup	Désactiver la consultation CNAME lors de la négociation de l'authentification Kerberos	Lors de l'utilisation de Kerberos pour l'authentification auprès du serveur mandataire, et si le SPN (`Service Principal Name`) de ce dernier est construit sur son nom d'hôte original et non sur son CNAME (au sens DNS) alors il est nécessaire que ce paramètre soit *Activé* pour désactiver la consultation CNAME
EnableAuthNegotiatePort	Inclure un port non standard dans le SPN Kerberos	*Non configuré* sauf si le port à utiliser dans le SPN est différent de 80 ou 443, ce paramètre permet alors de renseigner le port approprié.

Nom de stratégie	Description	Valeur recommandée
Google Chrome \ Stratégies d'authentification HTTP		
AuthServerWhitelist	Liste blanche des serveurs d'authentification	Ce paramètre doit être renseigné pour permettre une authentification intégrée utilisant les credentials en cache de la session utilisateur en cours. Chrome ne permet l'authentification intégrée qu'auprès des serveurs envoyant un challenge et figurant dans cette liste blanche. Le serveur proxy est automatiquement en liste blanche. Pour les autres services (de l'Intranet généralement) autorisés à utiliser l'authentification intégrée, il est nécessaire que ce paramètre soit *Activé* avec comme valeur la liste des services sous la forme : `www.Intranet.fr, *.Intranet.fr`
AuthNegotiateDelegateWhitelist	Liste blanche des serveurs de délégation Kerberos	La délégation Kerberos n'est pas prise en charge pour l'authentification au serveur mandataire. Pour les autres serveurs utilisant la délégation kerberos (exemple : un serveur Web IIS accédant à un serveur MSSQL), il est nécessaire que ce paramètre soit *Activé* avec comme valeur la liste des services impliqués dans la délégation sous la forme : `www.Intranet.fr, mssql.Intranet.fr`
AllowCrossOriginAuthPrompt	Invites d'authentification de base HTTP (Basic Auth) multi-domaine	*Désactivé* dans le cadre de la protection contre les tentatives d'hameçonnage.

Périmètre de navigation :

Nom de stratégie	Description	Valeur recommandée
**Google Chrome **		

URLBlacklist	Bloquer l'accès à une liste d'URL	Tout dépend de l'usage fait du navigateur. S'il s'agit d'un navigateur unique pour tous usages, l'entité utilisera de préférence une configuration de listes noires et blanches au niveau des serveurs mandataires (proxy). Par contre, cette règle permet d'interdire à minima certains schémas d'url comme « `file://` » ou « `ftp://` » jugés indésirables au sein du navigateur Internet :
		`file://*`
		`ftp://*`
		
		Si en revanche l'entité met en œuvre une stratégie de double navigateur (un premier réservé pour Internet et un second réservé aux applications légères de l'Intranet par exemple), il peut alors être utile de renseigner cette règle de la manière suivante :
		- si le navigateur est dédié à Internet, on mettra en liste noire l'ensemble des sites de l'Intranet pour s'assurer que l'utilisateur ne s'y connecte pas via ce navigateur ;
		- si le navigateur est dédié à l'Intranet, on bloquera l'accès à tous les sites (valeur `"*"`) et la règle `URLWhitelist` sera utilisée pour renseigner les exceptions (en l'occurence les sites de l'Intranet).
		Exemples de valeurs :
		`*.mondomaine.fr`
		`https://serveur:port/chemin`

URLWhitelist	Permet d'accéder à une liste d'URL	Cette règle sera configurée en fonction de l'`URLBlacklist`

Fonctionnalités diverses :

Viennent ensuite un certain nombre de fonctionnalités qui méritent également d'être configurées :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \		
CloudPrintProxyEnabled	Activer le proxy Google Cloud Print	*Désactivé*
CloudPrintSubmitEnabled	Activer l'envoi de documents à Google Cloud Print	*Désactivé*
HideWebStorePromo	Empêcher la possibilité pour des applications de s'afficher sur la page Nouvel onglet	*Activé*
DeveloperToolsDisabled	Désactiver les outils de développement	*Désactivé*, sauf pour les développeurs web
DisablePrintPreview	Désactiver l'aperçu avant impression	Au choix de l'entité
DisableScreenshots	Désactiver les captures d'écran	*Activé*
AlternateErrorPagesEnabled	Activer les pages d'erreur alternatives	*Activé*
AutoFillEnabled	Activer la saisie automatique	*Activé* avec la valeur *Interdire*
SigninAllowrd	Autoriser la connexion à Chrome	*Désactivé*
RestrictSigninToPattern	Ne pas autoriser certains utilisateurs à se connecter à Google Chrome	*Non configuré*
SyncDisabled	Désactiver la synchronisation des données avec Google	*Activé*
SpellCheckServiceEnabled	Activer ou désactiver le service Web de correction orthographique	*Désactivé*
TranslateEnabled	Activer Google Traduction	*Désactivé*
PrintingEnabled	Activer l'impression	*Activé* sauf si le navigateur est utilisé pour n'accéder qu'à des informations ne devant pas être imprimées
FullscreenAllowed	Autoriser le mode plein écran	Au choix de l'entité

Administration système et maintenance :

Nom de stratégie	Description	Valeur recommandée
Google Chrome \		
DefaultBrowserSettingEnabled	Définir Chrome comme navigateur par défaut	En fonction des besoins
BuiltInDNSClientEnabled	Utiliser le client DNS intégré	*Désactivé*
DnsPrefetchingEnabled	Activer la prédiction réseau	*Désactivé*
DisableSSLRecordSplitting	Désactiver le fractionnement des enregistrements SSL	*Désactivé*
BackgroundModeEnabled	Poursuivre l'exécution des applications en arrière-plan après la fermeture de Google Chrome	*Activé* avec la valeur *Interdire*
DownloadDirectory	Définir le répertoire de téléchargement	*Activé* avec une valeur à définir en fonction de la stratégie d'administration système de l'entité. Il est primordial de le stocker dans un répertoire personnel de l'utilisateur.

Nom de stratégie	Description	Valeur recommandée
Google Chrome \		
UserDataDir	Définir le répertoire de données utilisateur	*Activé* avec une valeur à définir en fonction de la stratégie d'administration système de l'entité. Il est toutefois primordial de stocker le répertoire de données de l'utilisateur dans un répertoire qui lui est personnel. Dans le cas de profils itinérants[15], l'emplacement pourra alors être changé au profit de `roaming_app_data`[16].
DiskCacheDir	Définir le répertoire du cache disque	*Activé* et à définir en fonction de la stratégie d'administration système de l'entité. Il est toutefois primordial de stocker le cache disque de l'utilisateur dans un répertoire qui lui est personnel. Dans le cas de profils itinérants, l'emplacement devrait être changé au profit de `local_app_data`.
MediaCacheSize	Définir la taille du cache du disque de support en octets	*Activé* (il s'agit du cache spécifique aux fichiers multimédia) et à définir selon la stratégie d'administration système[17]
DiskCacheSize	Définir la taille du cache du disque (en octets)	*Activé* et à définir en fonction de la stratégie d'administration système de l'entité
MetricsReportingEnabled	Autoriser l'envoi de statistiques d'utilisation et de rapports d'erreur	*Désactivé*
ImportBookmarks	Importer les favoris du navigateur par défaut à la première exécution	*Désactivé*
ImportHistory	Importer l'historique de navigation du navigateur par défaut à la première exécution	*Désactivé*
SavingBrowserHistoryDisabled	Désactiver l'enregistrement de l'historique du navigateur	*Non configuré*, à moins que l'entité ait des besoins de confidentialité particuliers
EditBookmarksEnabled	Active ou désactive la modification des favoris	*Activé*
ApplicationLocaleValue	Paramètres régionaux de l'application	Au choix, *Activé* avec la valeur *fr-FR* pourrait par exemple être utilisé pour forcer les paramètres régionaux français.
ForceEphemeralProfiles	Profil éphémère	*Désactivé*
DisableSpdy	Désactiver le protocole SPDY[18]	*Activé*, selon le principe de précaution
QuicAllowed	Autoriser le protocole QUIC[19]	*Désactivé*, selon le principe de précaution

15. Pour plus d'informations sur les profils itinérants : technet.microsoft.com/fr-fr/library/cc732275.aspx.
16. Les variables utilisables sont listées à l'adresse http://www.chromium.org/administrators/policy-list-3/user-data-directory-variables.
17. Le compromis entre performance et utilisation de la bande passante Internet dépend du contexte.
18. 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*).
19. QUIC (*Quick UDP Internet Connections*) est un protocole UDP expérimental présenté comme étant un équivalent à TLS + TCP et dont le principe est détaillé à l'adresse http://blog.chromium.org/2013/06/experimenting-with-quic.html.

Annexe II : Déploiement et configuration de Google Chrome par GPO dans un domaine Active Directory

Cette annexe présente de manière synthétique une méthode de télé-deploiement reposant sur GPO.

Téléchargement du paquet MSI

La dernière version de Google Chrome en version entreprise est disponible sur le site Web de Google [20]. Le fichier téléchargé ayant toujours le même nom quelle que soit sa version, il est recommandé de renommer le fichier après téléchargement de manière à faire figurer sa version dans le nom de fichier (la version est affichée dans l'onglet *détails* des propriétés du fichier). Cette bonne pratique de nommage est d'autant plus utile pour les entités qui choisiront de déployer manuellement les mises à jour de Google Chrome.

Règles de configuration

Pour pouvoir définir des règles de configuration de Google Chrome dans une GPO, il est nécessaire de préalablement télécharger les modèles d'administration fournis par Google à l'adresse :
https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.

Ensuite, dans un scénario de déploiement en domaine Active Directory, les modèles ADM et ADMX doivent être déposés dans un dépôt central au sein du dossier SYSVOL présent sur les contrôleurs de domaine et contenant les GPO. Pour plus d'informations, un guide pas à pas de gestion des modèles ADM et ADMX est disponible sur le site technet de Microsoft à l'adresse :
http://technet.microsoft.com/fr-fr/library/cc709647.

Déploiement

Le fichier MSI doit ensuite être déposé dans un partage de fichiers (d'un serveur de fichiers idéalement) accessible en lecture seule par tous les utilisateurs. Le chemin UNC (*Universal Naming Convention*) du partage créé sera utilisé dans la stratégie de groupe (C'est à dire par exemple `"\\serveur\partage\GoogleChromeStandaloneEnterprise.msi"` et non pas `"C:\partage\GoogleChromeStandaloneEnterprise"` puisqu'il s'agit du chemin qui sera utilisé par les postes utilisateurs pour accéder aux fichiers d'installation). Les utilisateurs (ou ordinateurs, en fonction de la GPO) doivent bien entendu avoir les droits de lecture uniquement sur ce partage.

Une simple stratégie de groupe permet pour finir de télédéployer le paquet d'installation. Au niveau de la console de gestion des stratégies de groupe du domaine, cela se fait en créant et modifiant une nouvelle GPO ayant par exemple les paramètres suivants :

20. https://www.google.fr/intl/fr/chrome/business/browser/

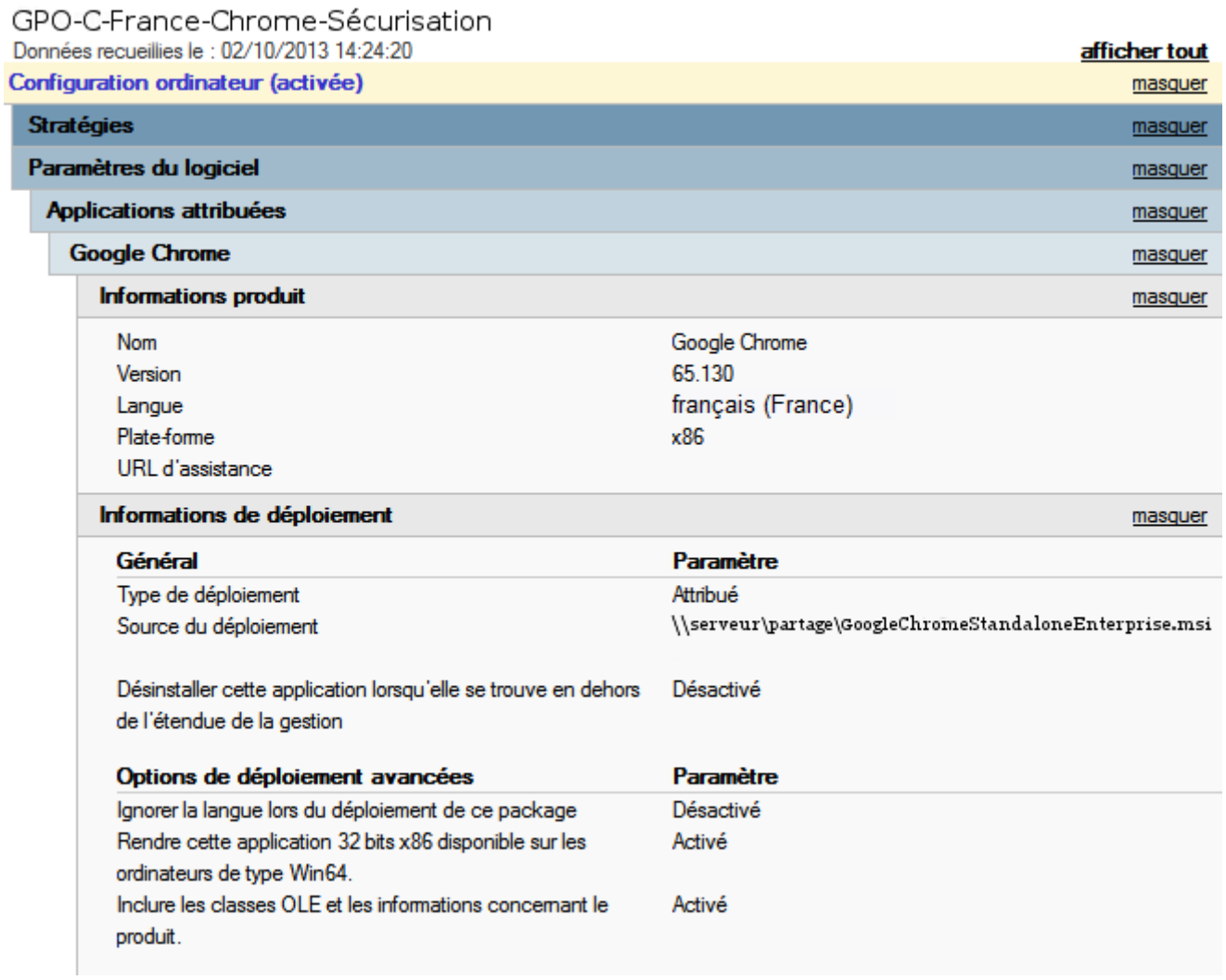
GPO-C-France-Chrome-Sécurisation
Données recueillies le : 02/10/2013 14:24:20 afficher tout
Configuration ordinateur (activée) masquer
Stratégies masquer
Paramètres du logiciel masquer
Applications attribuées masquer
Google Chrome masquer
Informations produit masquer
Nom Google Chrome
Version 65.130
Langue français (France)
Plate-forme x86
URL d'assistance
Informations de déploiement masquer
Général Paramètre
Type de déploiement Attribué
Source du déploiement \\serveur\partage\GoogleChromeStandaloneEnterprise.msi
Désinstaller cette application lorsqu'elle se trouve en dehors de l'étendue de la gestion Désactivé
Options de déploiement avancées Paramètre
Ignorer la langue lors du déploiement de ce package Désactivé
Rendre cette application 32 bits x86 disponible sur les ordinateurs de type Win64. Activé
Inclure les classes OLE et les informations concernant le produit. Activé

FIGURE 3 – GPO de déploiement de paquet d'installation MSI

Le déploiement peut également se faire au niveau de la stratégie utilisateur plutôt que de la stratégie ordinateur. L'étendue d'application de la stratégie de groupe peut également être restreinte à certains groupes d'ordinateurs ou d'utilisateurs. Si le déploiement se fait par stratégie utilisateur, la GPO s'applique par défaut à tous les utilisateurs authentifiés et ce périmètre devra bien souvent être réduit à une population précise.

Une fois les GPO de déploiement et de configuration des règles de Chrome appliquées, celui-ci sera automatiquement installé et configuré selon les règles définies.

Annexe III : Paramétrage du *Google Update Service*

Une fois l'ADM (*GoogleUpdate.adm*) ajouté, il est possible de configurer *Google Update* par GPO, et plus particulièrement de l'activer ou le désactiver :

- Désactiver Google Update

Nom de stratégie	Description	Valeur recommandée
Google \ Google Update \ Préférences		
AutoUpdateCheckPeriod	Fréquence de vérification des mises à jour	*Activé* avec la case à cocher *Disable all auto-update checks (not recommanded)* cochée
Google \ Google Update \ Applications \ Google Chrome		
AllowInstallation	Politique de mise à jour	*Activé* avec la valeur Updates disabled
Google \ Google Update \ Applications \ Google Chrome Binaries		
AllowInstallation	Politique de mise à jour	*Activé* avec la valeur Updates disabled

- Activer et configurer Google Update

Nom de stratégie	Description	Valeur recommandée
Google \ Google Update \ Préférences		
AutoUpdateCheckPeriod	Fréquence de vérification des mises à jour	*Activé* avec comme valeur la fréquence de vérification des mises à jour en minutes et avec la case à cocher *Disable all auto-update checks (not recommanded)* non cochée
Google \ Google Update \ Proxy Server		
ProxyMode	Sélectionner le mode de spécification des paramètres de serveur proxy	*Activé* avec comme valeur *utiliser des paramètres proxy déterminés*
ProxyServer	Adresse ou URL du serveur proxy	*Activé* avec comme valeur l'adresse du proxy à utiliser pour les clients Web sous la forme `ip:port`
ProxyPacUrl	URL d'un fichier .pac de proxy	*Non configuré* et à n'utiliser qu'en cas d'utilisation de serveurs mandataires moins courants (proxy socks par exemple)