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 28 août 2014

N° DAT-NT-18/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 42

Note technique

Recommandations pour le déploiement sécurisé du navigateur Microsoft Internet Explorer

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les **« Recommandations pour le déploiement sécurisé du navigateur Microsoft Internet Explorer »**. 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, BAS, BAI, LAM, LRP	BSS	SDE	28 août 2014

Évolutions du document :

Version	Date	Nature des modifications
1.0	28 août 2014	Version initiale

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

Microsoft Internet Explorer est le navigateur Web édité par Microsoft. Historiquement le plus utilisé des navigateurs de par sa gratuité et son intégration native à Windows, il cohabite désormais avec des navigateurs alternatifs comme Google Chrome ou Mozilla Firefox.

Depuis sa version 10 sortie le 26 octobre 2012, Microsoft Internet Explorer dispose de mécanismes de sécurité robustes. En plus d'être pré installé, il est également doté de fonctionnalités de configuration centralisée ainsi que de mises à jour automatiques intégrées au système d'exploitation, ce qui facilite son déploiement et son utilisation en entreprise. Néanmoins, entre les changements radicaux opérés par chaque nouvelle version majeure du navigateur et les incompatibilités d'une version à l'autre, la sécurisation de Microsoft Internet Explorer sur un parc hétérogène revêt quelques subtilités.

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 Microsoft Internet Explorer dans le cadre d'un télé-déploiement en environnement Active Directory.

Les recommandations et leurs indications de mise en œuvre figurant dans ce document sont basées sur les règles de configuration de Microsoft Internet Explorer dans sa version 11. Elles peuvent être appliquées aux versions antérieures du navigateur éventuellement maintenues pour les postes de travail anciens, ou pour des raisons de compatibilité avec des applications Web spécifiques. Dans ce cas, seuls les éléments de configuration compatibles seront alors appliqués. L'usage d'anciennes versions du navigateur reste toutefois déconseillé.

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 modules complémentaires intégrés aux navigateurs et dont les processus de mise à jour sont généralement indépendants de ceux du navigateur.

L'atteinte en sécurité 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. La navigation Web est donc logiquement devenue un des principaux vecteurs d'attaque utilisés et, plus largement, un problème pour la sécurité des système d'information.

Du point de vue de la sécurité, Internet Explorer intègre, depuis sa version 10, de nouvelles fonctionnalités de filtrage et des mécanismes de protection avancés qui lui confèrent un niveau de sécurité accru. Comme ses concurrents, il n'en fait pas moins l'objet de vulnérabilités critiques [1]

1. Les multiples avis de sécurité et bulletins d'actualité relatifs aux principaux navigateurs peuvent être consultés sur le site du CERT-FR à l'adresse `http://www.cert.ssi.gouv.fr`.

3 Compatibilité des différentes versions de Microsoft Internet Explorer

Le navigateur de Microsoft évolue considérablement d'une version majeure à l'autre, apportant de nouveaux mécanismes de sécurité ainsi que de nouvelles fonctionnalités. Mais ces nouvelles versions ne sont compatibles qu'avec les versions récentes de Microsoft Windows. Avant d'élaborer une stratégie de déploiement sur un parc hétérogène, il est alors préférable de prendre connaissance du tableau de compatibilité suivant :

Système d'exploitation	IE6	IE7	IE8	IE9	IE10	IE11
Windows XP	Oui	Oui (SP2+)	Oui (SP2+)	Non	Non	Non
Windows Vista	Non	Oui	Oui	Oui (SP2+)	Non	Non
Windows 7	Non	Non	Oui	Oui	Oui (SP1+)	Oui (SP1+)
Windows 8	Non	Non	Non	Non	Oui	Non
Windows 8.1	Non	Non	Non	Non	Non	Oui

En fonction du parc informatique sur lequel le navigateur sera déployé, il est souvent difficile de déployer et maintenir une seule et unique version de Microsoft Internet Explorer. Dès lors qu'il subsiste des postes sous Windows Vista ou Windows XP (qui pour rappel n'est plus supporté par Microsoft depuis le 8 avril 2014), le déploiement de Microsoft Internet Explorer sur ces derniers ne peut se faire au mieux qu'en version 8 ou 9. Ces anciennes versions sont toutefois dépourvues de certains mécanismes de sécurité importants.

4 Mécanismes de sécurité pris en charge par les différentes versions de Microsoft Internet Explorer

Différents mécanismes de sécurité sont mis en œuvre par Microsoft Internet Explorer, les principaux sont décrits ci-dessous par ordre chronologique d'apparition :

- **Protected Mode** (Mode Protégé), apparu avec Microsoft Internet Explorer 7 et qui utilise des mécanismes de sécurité datant de Windows Vista : l'UAC (*User Account Control*), les niveaux d'intégrité et l'UIPI (*User Interface Privilege Isolation*) ;
- **LCIE** (*Loosely-Coupled IE*), terme utilisé pour désigner une architecture multi-processus. Cette approche, qui date de Microsoft Internet Explorer 8, consiste à séparer d'une part les processus de pilotage du navigateur (interface graphique, fenêtres, etc.) et, d'autre part, les processus d'affichage de contenu (contenu HTML, contrôles ActiveX, extensions de barre d'outil, etc.). Cela permet de réduire la surface d'attaque des processus et ainsi de limiter les conséquences d'une exploitation de vulnérabilité. Depuis Windows Vista, ces processus s'exécutent d'ailleurs avec des niveaux d'intégrité [2] plus faibles. Ce mécanisme de séparation n'est pas désactivable et fait partie intégrante de la conception du navigateur ;
- **Filtre Smartscreen**, mécanisme de protection contre le hameçonnage et les logiciels malveillants signalés. Apparu sous Microsoft Internet Explorer 8, il s'agit d'une liste noire de sites et de fichiers hébergée et maintenue par Microsoft. Cette liste est dynamique et mise à jour en temps réel. Dès lors que ce mécanisme est activé, cette liste est consultée par le navigateur à chaque téléchargement ou visite d'un site Web ;

2. Article présentant la notion de niveaux d'intégrité sous Windows : http://msdn.microsoft.com/fr-FR/library/bb625957.aspx.

– **Filtrage XSS**[3] (anti-scripts de site à site), système de filtrage qui vise à repérer et bloquer le contenu malveillant injecté dans des pages Web par le biais de vulnérabilités. Ce filtre heuristique, à l'efficacité variable, est disponible depuis Microsoft Internet Explorer 8 ;
– **Filtrage ActiveX**, système de filtrage qui permet de n'autoriser l'exécution de contrôles ActiveX que sur les sites de confiance. Ce filtre est disponible depuis Microsoft Internet Explorer 9 et est activé par défaut ;
– **EPM** (*Enhanced Protected Mode*, à ne pas confondre avec le Mode Protégé simple), nom de la mesure de sécurité apparue avec Microsoft Internet Explorer 10 et qui englobe les deux mécanismes suivants :
- **AppContainer**, conteneur applicatif qui empêche les pages Web d'accéder en lecture/écriture au système d'exploitation. Il s'agit d'un mécanisme apparu avec Windows 8 (et donc indisponible sur les versions antérieures de Windows) et qui ajoute aux niveaux d'intégrité une notion de *capabilities* (capacités) ;
- **64-bits Tabs**, pour l'exécution des processus de contenu en 64 bits. Cette fonctionnalité permet de forcer l'utilisation de processus 64 bits pour le rendu des pages Internet. L'augmentation de la taille de l'espace d'adressage améliore l'efficacité de l'*ALSR* (mécanisme de distribution de l'espace d'adressage mémoire), rendant ainsi l'exploitation de vulnérabilité logicielle plus difficile[4]. Cette fonctionnalité n'est par définition disponible que sur les systèmes d'exploitation 64 bits ;

EPM est donc un mécanisme de protection fondamental pour une navigation sécurisée sur Internet. Une fois activé, il empêche l'exécution des modules complémentaires non compatibles. Ce mode peut toutefois être désactivé par noms de domaines de manière à autoriser certains sites à s'afficher au travers de processus 32 bits permettant le chargement de modules complémentaires non compatibles. Comme très peu de modules sont actuellement compatibles EPM, Microsoft a décidé de désactiver ce mode par défaut lors d'une mise à jour cumulative[5]. Notons également qu'EPM n'est pas utilisable si l'UAC (*User Account Control*) de Windows est désactivé.

Le tableau synthétique suivant récapitule les mécanismes de sécurité pris en charge par chaque système d'exploitation et par version de Microsoft Internet Explorer :

Mécanisme de sécurité	IE6	IE7	IE8	IE9	IE10		IE11	
Protected Mode	Non	Oui	Oui	Oui	Oui		Oui	
LCIE	Non	Non	Oui	Oui	Oui		Oui	
Filtre SmartScreen	Non	Non	Oui	Oui	Oui		Oui	
Filtre XSS	Non	Non	Non	Oui	Oui		Oui	
Filtre ActiveX	Non	Non	Non	Oui	Oui		Oui	
EPM AppContainer	Non	Non	Non	Non	Win 8 Oui	Win 7 Non	Win 8.1 Oui	Win 7 Non
EPM 64-bits tabs	Non	Non	Non	Non	OS 64 bits Oui	OS 32 bits Non	OS 64 bits Oui	OS 32 bits Non

3. Détails techniques d'implémentation du filtrage XSS : http://blogs.technet.com/b/srd/archive/2008/08/19/ie-8-xss-architecture-implementation.aspx.
4. Pour plus d'informations sur les onglets 64 bits et sur EPM en général : http://blogs.msdn.com/b/ie/archive/2012/03/14/enhanced-protected-mode.aspx.
5. Pour plus d'informations sur la désactivation d'EPM par mise à jour cumulative : https://support.microsoft.com/kb/2907803.

5 Principe des zones de sécurité

Microsoft Internet Explorer a comme particularité de proposer une configuration flexible par zones de sécurité. Cette fonctionnalité permet l'application de configurations distinctes par zone, auxquelles sont alors affectés les différents sites Web. Il est par exemple possible d'appliquer une configuration moins contraignante pour l'intranet et plus stricte pour un extranet dont les niveaux de confiance et de maîtrise seraient inférieurs. Pour un navigateur Internet, il est également possible de définir des sites de confiance (tels que les services externalisés) auxquels s'applique une configuration plus permissive que les autres sites Internet. Les zones mises à disposition par le navigateur sont :

- zone « Internet » ;
- zone « intranet », généralement utilisée pour les sites hébergés sur le réseau interne de l'entité. Cette zone peut être automatiquement peuplée des sites qui n'utilisent pas le serveur mandataire, de tous les chemins d'accès réseau UNC [6] ainsi que des sites locaux (même plan d'adressage IP) qui ne sont pas explicitement associés à une autre zone ;
- zone « ordinateur local » ;
- zone « sites approuvés » et de confiance, qui servira le plus souvent d'exceptions sous forme de liste blanche pour la zone Internet ;
- zone « sites sensibles » potentiellement dangereux, qui servira également le plus souvent d'exceptions sous forme de liste noire de sites à bloquer pour la zone Internet.

Définir des configurations adaptées par zone et affecter de manière réfléchie les sites Web au sein des différentes zones sont donc des moyens de débuter la sécurisation du navigateur mais également d'assurer la compatibilité avec les applications Web de l'entité (internes ou externalisées). Par défaut, un site Web devra être affecté à la zone Internet.

R1	Établir des listes de sites pour chaque niveau de confiance (zone intranet et zone des sites approuvés) auxquelles seront appliquées des configurations de sécurité spécifiques aux besoins de chaque zone. La zone Internet contiendra alors les sites non répertoriés.

Note 1 : Attention toutefois à ne pas faire aveuglément confiance au système de cloisonnement des zones de sécurité. L'élévation de privilèges fait partie des vulnérabilités les plus exploitées dans le but d'exécuter du code malveillant dans la zone « ordinateur local » [7].
Note 2 : La probabilité qu'un site Web Internet a priori légitime héberge involontairement du contenu malveillant n'est pas négligeable. Les attaques de type point d'eau (ou trou d'eau) [8] sont d'ailleurs une méthode que peuvent privilégier des individus malveillants pour contourner les moyens de protection de leur véritable cible. Les règles de cette zone ne doivent donc pas être trop permissives et les sites y figurant doivent être choisis de manière pertinente.

6 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 selon la politique

6. Il s'agit d'une convention de nommage qui consiste à indiquer les chemins réseaux sous la forme : `\\nom\chemin\fichier`.
7. Pour plus d'informations : http://technet.microsoft.com/en-us/library/cc757200.aspx.
8. Attaque qui consiste à identifier les sites Web fréquemment visités par une entité ciblée, puis à en exploiter les vulnérabilités pour y ajouter du contenu malveillant qui infectera indirectement l'entité.

de mise à jour de l'entité. Dans cette optique, Microsoft met à disposition des modèles d'administration pour Active Directory qui permettent de définir des stratégies de configuration des comptes d'ordinateurs et des comptes utilisateurs pour Internet Explorer. Ces stratégies reposent sur différents paramètres du navigateur décrits dans ce document et présentent l'intérêt de pouvoir être verrouillés et non modifiables par les utilisateurs (ce qui est conseillé). Toutes les recommandations de configuration de Microsoft Internet Explorer indiquées dans ce document sont détaillées en annexe I.

Les modèles d'administration d'Internet Explorer par GPO (*Group Policy Object*) fournis par Microsoft ne suffisent toutefois pas au paramétrage de l'ensemble des éléments de configuration. Jusqu'à la version 9 (incluse) du navigateur, un sous-ensemble de paramètres comme ceux relatifs à l'utilisation de serveurs mandataires se configuraient par GPP (*Group Policy Preferences*) via les options IEM (*Internet Explorer Maintenance*). Depuis Windows 8 et donc depuis Microsoft Internet Explorer 10, IEM est déprécié au profit d'IEAK [9] (*Internet Explorer Administration Kit*). Les versions 10 et 11 du navigateur ignoreront donc les paramètres IEM, ce qui nécessitera de changer quelque peu les pratiques d'administration.

R2	Avant tout déploiement de Microsoft Internet Explorer au sein d'un système d'information dont l'administration est centralisée par Active Directory, il est primordial de définir précisément des stratégies de groupe. Celles-ci consisteront à restreindre l'utilisation des modules complémentaires, ainsi qu'à définir les règles de configuration importantes pour la sécurité de la navigation. De telles politiques garantiront alors l'utilisation du navigateur dans une configuration durcie et verrouillée.

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 (des applications métier principalement) étant donné qu'elles peuvent être incompatibles avec certains usages ou certaines applications légères (applications Web) voire lourdes (applications intégrant un objet COM Internet Explorer).

Ces règles de configuration, à l'exception de quelques unes, peuvent s'appliquer aussi bien aux ordinateurs qu'aux utilisateurs. Il convient donc de choisir un périmètre d'application adéquat et de créer plusieurs GPO spécifiques aux particularités de chaque périmètre. D'autre part, certains paramétrages s'appliquent au navigateur de manière globale, tandis que d'autres s'appliquent de manière plus précise aux différentes zones de sécurité. Ces deux grandes catégories de paramètres sont donc présentées de manière séparée dans l'annexe I. Les valeurs recommandées sont par ailleurs données telles qu'indiquées dans les modèles d'administration. 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.

R3	Il est fortement conseillé de laisser le minimum possible de règles non configurées.

9. http://technet.microsoft.com/fr-fr/ie/bb219517.aspx.

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.

6.1 Configurations générales

Les configurations générales s'appliquent au navigateur dans son ensemble et pour toutes les zones de sécurité.

6.1.1 Sécurité des modules complémentaires

Les modules complémentaires sont des applications utilisées par Microsoft Internet Explorer pour interagir avec du contenu Web ou l'interface du navigateur. Les barres d'outils et les extensions sont considérées comme des modules complémentaires au même titre que les contrôles ActiveX.

Lorsqu'EPM est désactivé, aucun mécanisme ne vient véritablement contrôler l'exécution des modules complémentaires. Chaque module activé amène donc ses vulnérabilités potentielles et nécessite une veille pour son maintien en conditions de sécurité. Il est dans ce cas pertinent d'interdire ceux qui font l'objet de vulnérabilités critiques régulières. Pour ces raisons de sécurité, la navigation sans EPM et avec avec des modules complémentaires ne convient généralement qu'en intranet.

Lorsque Microsoft Internet Explorer est déployé pour la navigation sur Internet, l'activation d'EPM est donc fortement recommandée sans quoi la sécurité du navigateur s'en trouverait fortement affaiblie. Malheureusement, les modules complémentaires compatibles EPM sont encore rares. Pour un navigateur tout-usage, EPM peut par contre n'être activé que pour la zone Internet et éventuellement celle des sites sensibles.

Le tableau suivant indique la compatibilité des principaux types de contenus et leurs modules complémentaires correspondants avec EPM (à la date de publication du présent document) :

documents PDF	Le module complémentaire Adobe Reader supporte EPM depuis ses versions 10.1.9 et 11.0.06[10]
appliquettes Java	Aucun module compatible EPM
Javascript	Nativement supporté
contenu Flash Player	Shockwave Flash Player ActiveX[11] est compatible EPM.
contenu HTML5	Compatible et déjà intégré au navigateur par défaut
contenu Microsoft Silverlight	Aucun module compatible EPM

Rien ne devrait donc justifier la désactivation d'EPM pour une navigation sur Internet en entreprise :

- les modules complémentaires Java sont déconseillés sur Internet pour des raisons de sécurité ;
- Microsoft Silverlight reste très peu répandu ;
- HTML5 et Flash ainsi que les documents PDF représentent la majorité des contenus actuels.

Microsoft Internet Explorer en version 10 et 11 avec EPM activé se prête donc raisonnablement à une navigation sécurisée sur Internet. En outre, il présente l'avantage d'imposer une configuration durcie en ne permettant aucun laxisme.

10. http://helpx.adobe.com/acrobat/reader/kb/epm-support-acrobat-products.html.
11. Paquet d'installation MSI téléchargeable à l'adresse https://www.adobe.com/products/flashplayer/distribution3.html.

R4	Pour la navigation sur Internet, l'activation d'EPM est fortement recommandée sans quoi le niveau de sécurité atteint sera insuffisant. Il en va de même pour le filtrage ActiveX et les autres fonctions visant à renforcer la sécurité d'exécution des modules complémentaires. L'activation des onglets 64 bits sur les systèmes d'exploitation 64 bits apporte par ailleurs une protection contre les attaques visant les espaces mémoire. Ce mécanisme qui fait partie d'EPM doit donc être activé dès lors que le système d'exploitation le permet.

R5	D'une manière générale, il est préférable de réduire la surface d'attaque du navigateur (principe de moindre fonctionnalité). Aucune brique logicielle tierce venant se greffer au navigateur ne devrait être autorisée, sauf exceptions liées à des besoins bien spécifiques. Les modules nécessaires et autorisés devraient donc être automatiquement déployés et les utilisateurs ne devraient en aucun cas pouvoir en ajouter de nouveaux. Cette recommandation vaut pour tous les modules complémentaires, qu'ils soient accélérateurs, contrôles ActiveX ou barres d'outils entre autres. Le principe d'application de cette règle est donc de tout interdire puis de renseigner exhaustivement par GPO une liste blanche de briques logicielles tierces autorisées.

6.1.2 SSL et Certificats

Microsoft Internet Explorer utilise les certificats du magasin de Windows. Il ne sera donc pas possible d'appliquer des restrictions spécifiques au navigateur sur certains certificats sans les appliquer au système d'exploitation dans son ensemble. En revanche, il est possible de restreindre les versions de protocoles SSL/TLS ainsi que les suites cryptographiques utilisées.

R6	Il est recommandé de désactiver l'utilisation de SSL et de n'autoriser que les protocoles TLS (les dernières versions de TLS ne sont pas activées par défaut sur toutes les versions de Microsoft Internet Explorer). Pour aller plus loin, il est également possible de restreindre les suites cryptographiques utilisables en désactivant celles reposant sur des algorithmes obsolètes comme RC4. Les suites n'utilisant pas de mécanismes de PFS (*Perfect Forward Secrecy*) doivent idéalement être désactivées elles-aussi mais de nombreux effets de bords sont à prévoir sur Internet du fait que de nombreux serveurs Web sont encore incompatibles.

Note : se référer à la section correspondante de l'annexe I ainsi qu'aux publications de l'ANSSI sur la « sécurité SSL/TLS » disponibles sur le site `http://www.ssi.gouv.fr`.

6.1.3 Gestionnaire de mots de passe

Le gestionnaire de mots de passe d'Internet Explorer permet de mémoriser les mots de passe saisis dans les formulaires Web.

R7	Il est conseillé de désactiver le gestionnaire de mots de passe. L'application d'un tel durcissement est légitime sur un réseau amené à traiter des données sensibles ou confidentielles. Sur des réseaux moins sensibles, il peut en revanche être difficile d'imposer aux utilisateurs une saisie systématique des mots de passe, sans compter les risques de hameçonnage que cela implique. La désactivation du gestionnaire de mots de passe devrait s'accompagner du déploiement d'un gestionnaire alternatif et sécurisé [12].

12. KeePass, dans sa version 2.10, est un exemple de solution certifiée d'un point de vue sécurité au premier niveau (CSPN) par l'ANSSI qui peut être utilisée avec Internet Explorer.

6.1.4 Fonctionnalités de sécurité touchant d'autres processus

Des fonctionnalités de sécurité permettent d'empêcher certains scénarios d'attaque qui pourraient affecter la sécurité du navigateur. Elles apportent par exemple :

- une meilleure sécurité dans la gestion des informations MIME ;
- la protection des accès au presse-papiers (supprimer, copier, coller) par script ;
- une protection contre l'élévation de privilèges ou la mise en cache d'objets ;
- des restrictions de sécurité relatives au téléchargement de fichiers, aux contrôles ActiveX ou aux modules complémentaires.

Il est pertinent d'appliquer certaines de ces fonctionnalités de sécurité aux applications tierces intégrant un objet COM Internet Explorer (c'est à dire un navigateur Internet Explorer intégré de manière transparente dans une application lourde). Ces applications affichent et exécutent du contenu actif d'une façon non sécurisée et peuvent ainsi se retrouver utilisées comme vecteurs d'attaque. Dès lors que ces applications sont bien identifiées et que le durcissement a fait l'objet d'une vérification préalable, le périmètre d'application des fonctionnalités de sécurité devrait donc leur être étendu (ce qui n'est pas le cas par défaut). Il est également possible d'établir des listes blanches d'objets COM instanciés au niveau du système, mais cela reste difficile à mettre en œuvre à cause des nombreux effets de bord.

Certaines de ces « fonctionnalités de sécurité » facultatives (ainsi intitulées dans les modèles d'administration de Microsoft Internet Explorer) peuvent être appliquées :

- aux processus Internet Explorer (`iexplore.exe` mais également l'explorateur de fichiers de Windows `explorer.exe`) et tous leurs processus enfants. Il s'agit du périmètre d'application minimal recommandé pour ces fonctionnalités de sécurité ;
- à une liste de processus définie par les administrateurs, pour étendre l'application de ces fonctionnalités et ainsi renforcer la sécurité d'applications tierces ou développées en interne et qui intègrent un objet COM Internet Explorer (composant logiciel réutilisable par les développeurs) ;
- à tous les processus, de manière plus stricte. Dès lors, la liste de processus ci-dessus fait office de liste blanche et est prioritaire.

R8	Il est recommandé d'activer toutes les « fonctionnalités de sécurité » facultatives. Ces dernières doivent s'appliquer à minima pour les processus Internet Explorer et tel que détaillé en annexe I. Dans l'idéal, leur mise en œuvre devrait être étendue aux processus de toute application tierce intégrant un objet COM Internet Explorer.

6.1.5 Confidentialité

Le lecteur est invité à prendre connaissance de la « déclaration de confidentialité d'Internet Explorer 11 » [13].

13. La déclaration de confidentialité d'Internet Explorer 11 est disponible à l'adresse `http://windows.microsoft.com/fr-fr/internet-explorer/ie11-win8-privacy-statement` pour Windows 8 et `http://windows.microsoft.com/fr-fr/internet-explorer/ie11-win7-privacy-statement` pour Windows 7.

En fonction des fonctionnalités activées, des données sont susceptibles d'être envoyées à Microsoft :

- les adresses complètes des sites Web visités ;
- un identifiant unique aléatoire généré à l'installation d'Internet Explorer et permettant de garder un historique des données envoyées (un nouvel identifiant non lié à l'ancien est généré lors de la suppression de l'historique de navigation ou de la réactivation de la fonctionnalité des sites suggérés) ;
- de nombreuses données de navigation telles que : historique de navigation, éléments contenus dans les pages Web visitées (images, vidéos), statistiques de temps de consultation par page, temps de chargement, pages de provenance, modèle de périphérique utilisé, entre autres ;
- etc.

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

R9	Désactiver la fonctionnalité d'avance rapide avec prédiction de page.

R10	La fonctionnalité de filtre SmartScreen envoie à Microsoft les adresses Web des sites visités et des fichiers téléchargés pour vérifier qu'il ne soient pas connus comme étant malveillants et, si nécessaire, en bloquer l'accès. Bien qu'il soit conseillé de laisser ce filtre activé pour des raisons de sécurité, une entité pourra légitimement juger suffisamment confidentielles les adresses des pages Web visitées pour qu'une désactivation du filtre SmartScreen s'impose sur la zone intranet.

La navigation privée (mode *InPrivate*) 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 Microsoft Internet Explorer dispose d'une connectivité à Internet, les recommandations suivantes s'appliquent.

R11	Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, etc.) dès lors que le navigateur n'est pas dédié à une navigation en Intranet.

Note : Le nouveau standard de protection contre le-pistage (*Do Not Track*) a fait son apparition dans Microsoft Internet Explorer 9 mais celui-ci n'est qu'une déclaration d'intention auprès des sites Web. Sa prise en compte ne dépend donc que des pratiques de confidentialité individuelles des sites Web visités et n'apporte aucune garantie.

R12	Il est recommandé d'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.

6.1.6 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 l'entité veut par exemple imposer un 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.

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.

6.1.7 Filtrage de contenu

Le filtrage du contenu participe au renforcement de la sécurité de navigation. Ces mécanismes de filtrage peuvent toutefois avoir une incidence sur la faculté des utilisateurs à naviguer sur certains sites.

R15	Il est recommandé d'activer les fonctionnalités de filtrage de contenu telles que le filtre SmartScreen (voir recommandation R10), l'anti-hameçonnage ou le bloqueur de fenêtres publicitaires (« pops-ups ») sur la zone Internet.

Les « pop-ups » devraient idéalement être désactivés 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. Cela peut donc s'avérer trop contraignant pour un service informatique manquant de ressources et en fonction des usages qui sont faits d'Internet au sein de l'entité. Un compromis peut alors consister à ne pas configurer cette règle, de manière à laisser l'utilisateur accepter lui-même les « pop-ups » pour les sites qui les nécessitent.

6.1.8 Page(s) d'accueil

R16	Lors du démarrage du navigateur, il est préférable de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une(des) page(s) connue(s) 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 (sauf en navigation *InPrivate*). 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.

6.1.9 Serveur mandataire (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 procède ensuite à l'établissement d'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, mais permettra principalement une journalisation dans un but d'analyse inforensique. Il s'avère alors judicieux de configurer l'utilisation du serveur mandataire par GPO sur les postes d'extrémité.

R17	L'utilisation de serveurs mandataires avec authentification (idéalement par certificat ou kerberos, sinon par NTLM) est importante pour la sécurité d'un système d'information.

Note : Les paramètres de serveurs mandataires ne sont pas configurables via les modèles d'administration. IEM étant aujourd'hui déprécié, le plus simple reste de configurer ces paramètres par clés de registre via les stratégies de groupe de préférences (GPP) tel que détaillé en annexe I dans la section correspondante.
Note : Comme détaillé en annexe III, la restriction du User-Agent sur les serveurs mandataires doit prendre en compte les changements opérés avec Microsoft Internet Explorer 11.

6.1.10 Périmètre de navigation

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

R18	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 qui pourraient être réalisés par du contenu malveillant. 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.).

6.1.11 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.

6.2 Configurations spécifiques aux zones de sécurité

6.2.1 Affectation des sites aux zones

Une fois le travail préliminaire de répartition des sites par zones réalisé, il est nécessaire de mettre en œuvre cette affectation par GPO et de la verrouiller pour s'assurer que les utilisateurs n'ont pas la possibilité de manipuler cette répartition.

R19	L'affectation des sites aux différentes zones de sécurité doit être faite par GPO. Ces listes d'affectation doivent être verrouillées et non modifiables par les utilisateurs.

6.2.2 Zone des sites sensibles

R20	Il est recommandé d'appliquer le modèle « niveau de sécurité haut » à la « zone de sites sensibles ».

6.2.3 Zone Internet

Dans certains contextes, il pourrait être envisagé d'appliquer à la « zone Internet » le modèle de « niveau de sécurité haut » adapté à la consultation de sites sensibles. Ce niveau apporte une sécurité maximale et les différentes fonctionnalités à risque sont désactivées. Néanmoins, il paraît peu probable qu'un utilisateur tolère ce niveau de sécurité dans la mesure ou la consultation de certains contenus (animations Flash par exemple) ne sera alors pas possible. On privilégiera donc l'application de paramètres de configurations manuels et affinés en fonction des besoins plutôt que l'application d'un niveau de sécurité rigide. L'idéal est alors de calquer manuellement les paramètres de sécurité sur le « niveau de sécurité haut » puis d'assouplir certains paramètres de manière à faire un compromis entre sécurité et besoins. L'annexe I donne un exemple de configuration de sécurité pour la « zone Internet ».

R21	Il est recommandé d'appliquer à la « zone Internet » un paramétrage manuel dérivé du modèle de « niveau de sécurité haut » et qui sera un compromis entre haut niveau de sécurité et besoins des utilisateurs pour la consultation des sites Internet qui ne sont pas de confiance. En revanche, si le navigateur est dédié à la navigation en intranet, il est plus pertinent d'appliquer directement le modèle de « niveau de sécurité haut » à la « zone Internet ».

6.2.4 Zone intranet

R22	Il est recommandé d'appliquer à la « zone intranet » un paramétrage manuel durci au maximum et n'autorisant que les fonctionnalités réellement nécessaires à la consultation des sites et applications Web internes. En revanche, si le navigateur est dédié à la navigation sur Internet, il est plus pertinent d'appliquer le modèle de « niveau de sécurité haut » à la « zone intranet ».

6.2.5 Zone des sites de confiance

Si le navigateur est dédié à la navigation en intranet et que le niveau de sécurité de la « zone Internet » est correctement paramétré, la « zone des sites confiance » n'a alors aucune utilité.

En revanche, dans le cadre d'un navigateur dédié à la navigation sur Internet, la « zone des sites de confiance » pourrait servir à rendre consultables des applications Web externalisées ou des sites Internet consultés dans un cadre professionnel mais non compatibles avec le haut niveau de sécurité de la « zone Internet ». Dans ce cas, on veillera encore une fois à n'autoriser que les fonctionnalités réellement nécessaires à la consultation de ces sites et applications Web.

R23	N'octroyer à la « zone des sites de confiance » que les droits réellement nécessaires à la consultation des sites et applications Web qu'elle contient.

6.3 Télé-déploiement initial

Microsoft Internet Explorer, au même titre que les autres logiciels, devrait idéalement être installé sur les postes de travail par télé-déploiement, du moins pour les versions non pré-installées en fonction de la version du système d'exploitation. 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. Celles recommandées par Microsoft sont :
- le déploiement par WSUS dans le cadre des mises à jour Windows ;
- le déploiement par Microsoft System Center 2012 Configuration Manager (SCCM) ;
- le déploiement par Microsoft System Center Essentials 2010 ;
- l'utilisation de Windows Intune.

Il reste bien entendu possible d'utiliser un outil de gestion de parc ou tout autre produit tiers de télé-déploiement.

6.4 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 ou organisations malveillantes exposent le poste de travail à une attaque.

Il est préférable de gérer le maintien en conditions de sécurité de Microsoft Internet Explorer dans le cadre des mises à jour Windows à l'aide de Microsoft WSUS (*Windows Server Update Services*) actuellement en version 3.0 SP2. Pour plus d'information sur WSUS, un guide de prise en main est disponible sur le site `TechNet` de Microsoft à l'adresse suivante :
`http://technet.microsoft.com/fr-fr/technet-techcenter-windows-server-update-services.aspx`.

La problématique des mises à jour concerne également les modules complémentaires (contrôles ActiveX, etc.). Bien qu'il soit recommandé de les interdire dans le cadre d'une configuration durcie, une entité peut légitimement vouloir en déployer. Puisque ces derniers ne seront pas mis à jour par le biais de WSUS, il sera alors nécessaire de prendre en charge leur mise à jour de manière spécifique.

Notons qu'après le 9 septembre 2014, Internet Explorer (versions 8 à 11) bloquera automatiquement les contrôles ActiveX obsolètes, hormis pour la navigation sur des sites Web des zones « Intranet » et « sites de confiance » [14]. S'inscrire aux flux RSS du CERT-FR [15] permet de se tenir informé des alertes de sécurité en cours.

7 Stratégie de double navigateur

La sécurité des systèmes d'information requiert un navigateur qui soit à la fois durci pour l'accès à Internet et souple pour l'accès aux applications internes. Lorsque certains serveurs Web internes utilisent des appliquettes Java par exemple, nécessitant le déploiement de modules complémentaires

14. Pour plus d'information sur le blocage des ActiveX obsolètes : `https://blogs.msdn.com/b/ie/archive/2014/08/06/internet-explorer-begins-blocking-out-of-date-activex-controls.aspx`
15. `http://www.cert.ssi.gouv.fr/site/index.html`.

Java, la surface d'attaque du navigateur devient alors trop importante, exposant ainsi l'entité à un des vecteurs d'attaque les plus critiques et massivement exploités [16].

Pour traiter cette problématique, de plus en plus d'entités s'orientent vers l'usage de deux navigateurs différents dès lors qu'elles disposent des ressources nécessaires pour les maintenir en conditions de sécurité. 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 faisant l'objet de vulnérabilités fréquentes ou une configuration relativement laxiste. Il est donc configuré 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, par des paramètres de configuration verrouillés, le périmètre d'utilisation de chaque navigateur. Le tableau suivant en donne quelques exemples :

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 sur le port approprié et depuis : - le processus du navigateur Internet (chemin complet de l'exécutable) ; - 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 : - 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

16. Les recommandations de sécurité publiées par l'ANSSI relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows peuvent être consultées 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.

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 d'emploi possible de chacun des navigateurs. Plus généralement, les règles de configuration recommandées en annexe I se prêtent à un contexte où le navigateur est dédié à la navigation sur Internet.

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

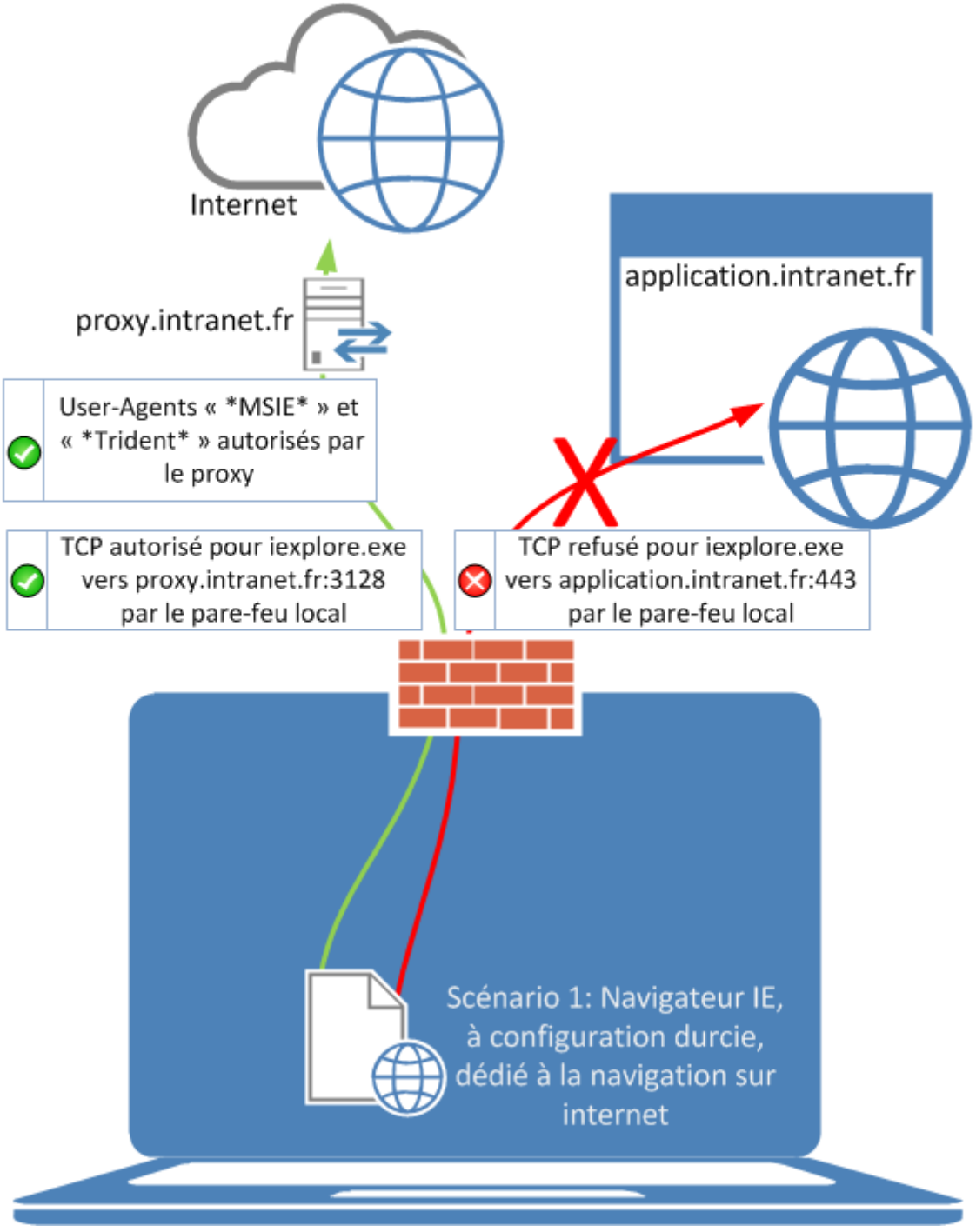

FIGURE 1 – Illustration d'une stratégie de double navigateur - cas ou Microsoft Internet Explorer est utilisé comme navigateur Internet.

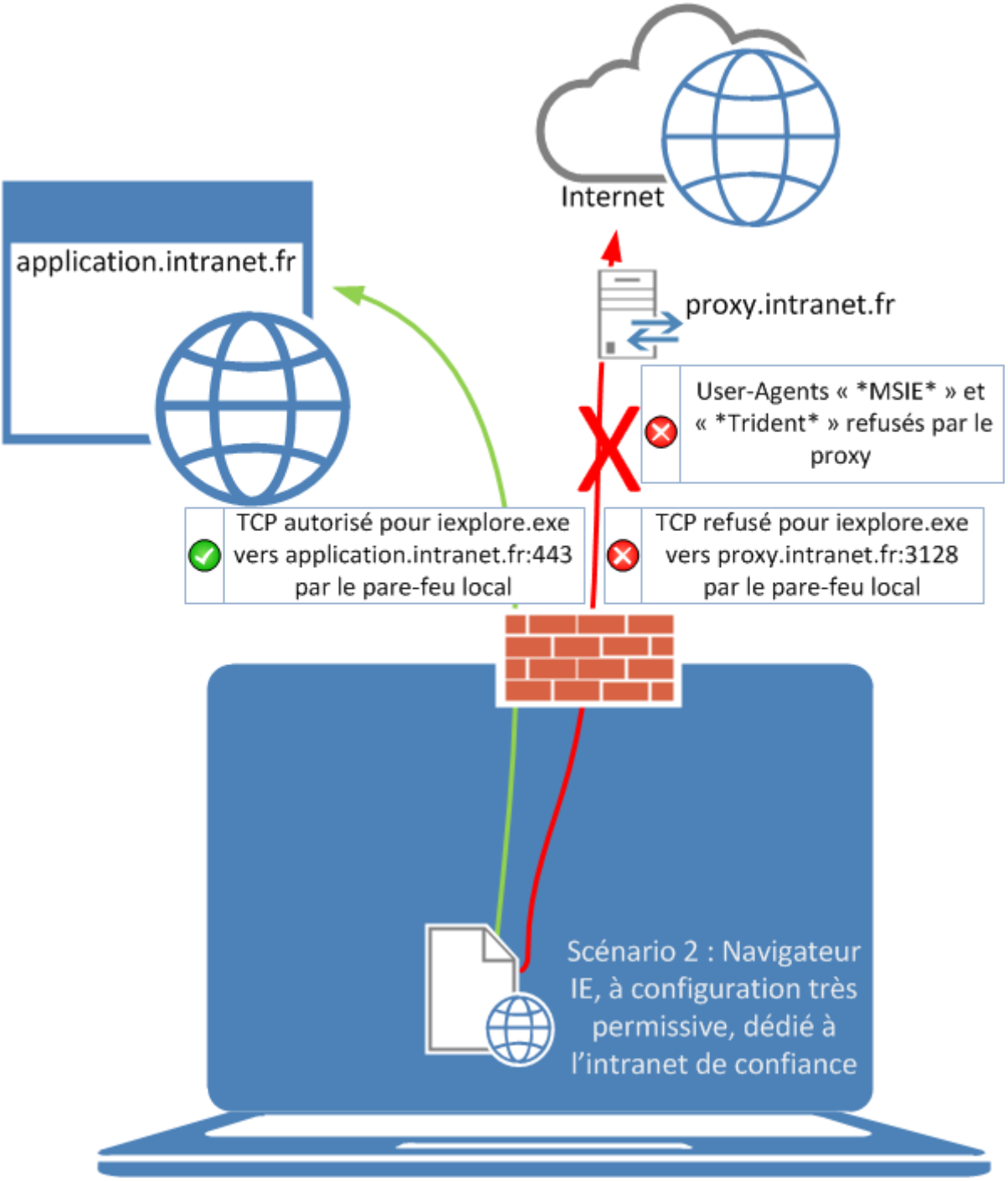

FIGURE 2 – Illustration d'une stratégie de double navigateur - cas ou Microsoft Internet Explorer est utilisé comme navigateur Intranet.

Ces figures illustrent deux cas distincts. Le navigateur Microsoft Internet Explorer y est représenté mais la stratégie est équivalente pour Google Chrome ou Mozilla Firefox, entre autres.

Notons pour finir que les fonctions de compatibilité d'affichage de Microsoft Internet Explorer abordées en annexe III sont à connaître dès lors qu'une entité dédie ce navigateur à la navigation sur un périmètre défini.

Sur Windows 8, Internet Explorer est disponible :
- en version de bureau (*Desktop*), c'est à dire sous sa forme traditionnelle ;
- en version *ModernUI* (anciennement appelé *Metro Style*), c'est à dire sous la forme d'application tactile à l'interface épurée destinée à une utilisation sur périphérique de type tablette ou ordiphone.

La version *ModernUI* se distingue principalement de la version *Desktop* par le fait qu'elle est dépourvue de modules complémentaires (à l'exception de *Flash Player* intégré par défaut). Les stratégies de sécurité mises en œuvre par GPO s'appliquent aux deux versions du navigateur sans distinction. L'entité pourra éventuellement forcer l'ouverture d'Internet Explorer dans un mode ou l'autre.

Annexe I :
Stratégies de sécurisation de Microsoft Internet Explorer

Cette annexe liste les valeurs recommandées permettant de mettre en œuvre les recommandations formulées dans cette note technique. Quelques rares descriptions de fonctionnalités récentes n'ont pas été traduites dans la dernière version des modèles d'administration de Microsoft Internet Explorer 11 et y figurent donc en anglais. Ces dernières apparaissent en français dans cette annexe.

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.

Sécurité des modules complémentaires :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Accélérateurs		
DeployAccelerators	Ajouter d'autres accélérateurs que ceux par défaut	*Désactivé*
DeployDefaultAccelerators	Ajouter les accélérateurs par défaut	*Désactivé*
TurnOffAccelerators	Désactiver les accélérateurs	*Activé*
UsePolicyAccelerators	Restreindre les accélérateurs à ceux déployés via une stratégie de groupe	*Activé*
Internet Explorer \ Contrôles approuvés par l'administrateur		
Flash	Shockwave Flash	Généralement *Activé*.
Toutes les autres	-	*Désactivé* sauf besoin bien spécifique pour certains applicatifs en Intranet.
Internet Explorer		
AddonManagement_DisableAddonLoadTime PerformanceNotifications	Désactiver les notifications de performances des modules complémentaires	*Activé*
AddonManagement_IgnoreAddon ApprovalStatus	Activer automatiquement les modules complémentaires récemment installés	*Désactivé*
AddonManagement_Restrict CrashDetection	Désactiver la détection d'arrêts intempestifs	*Activé*
AddonManagement_Restrict ExtensionManagement	Ne pas autoriser les utilisateurs à activer ou désactiver les modules complémentaires	*Activé*
DisableActiveXFirstPrompt	Désactiver l'invite d'exécution d'ActiveX	*Désactivé*
DisablePerUserActiveXInstall	Empêcher l'installation par utilisateur des contrôles ActiveX	*Activé*
OnlyUseAXISForActiveXInstall	Spécifier l'utilisation du service de l'installateur ActiveX pour l'installation des contrôles ActiveX	*Activé*
TurnOnActiveXFiltering	Activer le filtrage ActiveX	*Activé*
NoJITSetup	Désactiver l'installation automatique de composants Internet Explorer	*Activé*
Internet Explorer \ Panneau de configuration Internet		
Advanced_EnableBrowserExtensions	Autoriser les extensions de navigateurs tierce partie	*Désactivé*

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_DisableEPMCompat	Ne pas autoriser les contrôles ActiveX à s'exécuter en mode protégé lorsque le mode protégé étendu est activé	*Activé*
Advanced_EnableEnhancedProtectedMode	Activer le mode protégé étendu	*Activé*
Advanced_EnableEnhanced ProtectedMode64Bit	Désactiver les onglets 64 bits lorsqu'EPM est activé sur les systèmes 64 bits	*Désactivé*, les onglets 64 bits offrant une protection fondamentale vis vis à d'un contenu potentiellement malveillant
Advanced_InvalidSignatureBlock	Autoriser le logiciel à s'exécuter ou à s'installer même si la signature n'est pas valide	*Désactivé*

SSL et certificats :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet		
NoCertError	Empêcher la non-prise en compte des erreurs de certificat	*Activé*
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_CertificateRevocation	Vérifier la révocation du certificat serveur	*Activé* (cela peut poser des problèmes de temps d'accès si les serveurs de révocation interrogés ne sont pas joignables)
Advanced_SetWinInetProtocols	Désactiver la prise en charge du chiffrement	*Activé* avec pour valeur `Utiliser TLS 1.0, TLS 1.1 et TLS 1.2`[17]
Advanced_EnableSPDY3_0	Autoriser Internet Explorer à utiliser le protocole réseau SPDY/3	*Désactivé*
Internet Explorer \ Panneau de configuration Internet \ Onglet Sécurité		
IZ_PolicyWarnCertMismatch	Activer l'avertissement relatif aux incohérences d'adresses de certificats	*Activé*

Il est ensuite possible de restreindre les suites cryptographiques autorisées à l'aide de la valeur de clé de registre `Functions` de type `REG_SZ` à créer dans `HKCU\Software\Policies\Microsoft\Cryptography\Configuration\SSL\00010002`. Il est également possible de les restreindre par GPO via le modèle d'administration présent par défaut dans `Configuration Ordinateur\Modèles d'administration\Réseau\Paramètres de configuration SSL`.

Cette restriction des suites cryptographiques s'applique à l'ensemble du système d'exploitation et pourrait avoir des effets de bord indésirables avec des applications utilisant la librairie schannel de Microsoft ou avec des serveurs Web anciens ne gérant que des suites cryptographiques obsolètes.

Gestionnaire de mots de passe :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer		
RestrictFormSuggestPW	Désactiver la fonctionnalité de saisie semi-automatique des noms d'utilisateurs et des mots de passe sur les formulaires	*Activé*
Internet Explorer \ Fonctionnalités de sécurité		
IESF_DisablePasswordRevealButton	Ne pas afficher le bouton permettant de révéler le mot de passe	*Activé*

17. Consulter la note technique « Sécurité SSL/TLS » pour plus d'informations.

Fonctionnalités de sécurité extensibles à d'autres processus :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Fonctionnalités de sécurité \ Gestion des modules complémentaires		
AddOnList	Liste des modules complémentaires	*Activé* avec pour valeurs une liste de modules complémentaires sous la forme « CLSID + Valeur ». « CLSID » représente l'identifiant de classe d'objet du module complémentaire « Valeur » est un chiffre indiquant si le module est : - désactivé (0) ; - activé (1) ; - contrôlé par l'utilisateur (2). Ce qui donne pour l'activation du module Flash Player 12.0.0.44 : Nom de valeur = `{D27CDB6E-AE6D-11CF-96B8-444553540000}` Valeur = `1`
AddonManagement_ ManagementMode	Interdire tous les modules complémentaires, sauf s'ils sont explicitement autorisés dans la liste des modules complémentaires	*Activé*
DisableFlashInIE	Désactiver Adobe Flash dans Internet Explorer et empêcher les applications d'utiliser la technologie Internet Explorer pour instancier des objets Flash	*Non configuré* (Flash est activé via la règle `AddOnList` étant donné que l'interdiction `AddonManagement_ManagementMode` prend le pas sur la règle `DisableFlashInIE`)
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ AJAX		
Tous	Tous	*Non configuré*
Internet Explorer \ Fonctionnalités de sécurité \ Barre de notification		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (sans vulnérabilité connue à ce jour, la barre de notification permet d'informer l'utilisateur de certaines restrictions)
IESF_PolicyProcessList	Liste des processus	*Non configuré*
Internet Explorer \ Fonctionnalités de sécurité \ Fonctionnalité de sécurité de détection MIME		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (pour se protéger du MIME spoofing)
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité, sous la forme : Nom de valeur = Nom du processus auquel étendre l'application de la fonctionnalité de sécurité Valeur = 1 (activé) ou 0 (désactivé)

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Fonctionnalités de sécurité \ Gestion MIME cohérente		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (pour se protéger du MIME spoofing)
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Protection contre l'élévation de zone		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé*
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Protection de mise en cache d'objets		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (ce paramètre peut causer des problèmes de compatibilité avec certaines pages lorsque les objets ne sont pas remis en cache avant accès par script)
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Restreindre l'installation ActiveX		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé*
IESF_PolicyProcessList	Liste des processus	*Non configuré*
Internet Explorer \ Fonctionnalités de sécurité \ Restreindre le téléchargement de fichiers		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (le téléchargement de fichier doit alors être initié par une action utilisateur)
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Restriction de sécurité de comportement binaire		
Tous	Tous	*Non configuré* donc interdit à moins de besoins spécifiques en intranet
Internet Explorer \ Fonctionnalités de sécurité \ Restriction de sécurité du protocole MK		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé* (le protocole MK est déprécié et très peu utilisé)
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Restrictions de sécurité de scripts de fenêtres		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé*
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Fonctionnalités de sécurité \ Sécurité du verrouillage de la zone Ordinateur local		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*, ou idéalement *Activé* si le paramètre `IESF_PolicyProcessList` est activé
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé*
IESF_PolicyProcessList	Liste des processus	A minima *Non configuré*, ou idéalement *Activé* en spécifiant une liste de processus tiers auxquels étendre ou non l'application de cette fonctionnalité de sécurité.
Internet Explorer \ Fonctionnalités de sécurité \ Verrouillage des protocoles réseau		
IESF_PolicyAllProcesses	Tous les processus	*Non configuré*
IESF_PolicyExplorerProcesses	Processus Internet Explorer	*Activé*
IESF_PolicyProcessList	Liste des processus	*Non configuré*
Internet Explorer \ Compatibilité des applications \ Accès au presse-papiers		
IESF_PolicyScriptPasteAllProcesses	Ignorer les invites liées à l'accès au Presse-papiers pour les scripts qui s'exécutent dans un processus	*Désactivé*, sauf lorsque le navigateur est utilisé en Intranet et que des applications utilisent le presse-papier
IESF_PolicyScriptPasteExplorerProcesses	Ignorer les invites liées à l'accès au Presse-papiers pour les scripts qui s'exécutent dans le processus Internet Explorer	*Désactivé*, sauf lorsque le navigateur est utilisé en Intranet et que des applications utilisent le presse-papier
IESF_PolicyScriptPasteProcessList	Définir les applications et les processus qui peuvent accéder au Presse-papiers sans avertissement	*Désactivé*, sauf lorsque le navigateur est utilisé en Intranet et que des applications utilisent le presse-papier. Dans ce cas le paramètre doit être *Activé* avec comme valeur une liste de processus (noms d'exécutables) autorisés.

Confidentialité :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Confidentialité		
DisableInPrivateBlockingV8	Désactiver le filtrage InPrivate	*Activé* si le navigateur est destiné à la navigation sur Intranet, et *Désactivé* dans le cas contraire.
DisableInPrivateBlockingV9	Désactiver la protection contre le tracking	*Activé* si le navigateur est destiné à la navigation sur Intranet, et *Désactivé* dans le cas contraire.
DisableInPrivateBrowsing	Désactiver la navigation InPrivate	*Activé* si le navigateur est destiné à la navigation sur Intranet, et *Désactivé* dans le cas contraire.
DisableInPrivateLogging	Désactiver la collecte de données de filtrage InPrivate	*Activé*
DisableInPrivateToolbars	Empêcher l'ordinateur de charger des barres d'outils et des objets application d'assistance du navigateur lorsque la navigation InPrivate démarre	*Activé*
InPrivateBlockingThresholdV8	Établir le seuil de filtrage InPrivate	Au choix de l'entité
InPrivateBlockingThresholdV9	Établir le seuil de protection contre le tracking	Au choix de l'entité
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_SaveEncryptedPages	Ne pas enregistrer les pages chiffrées sur le disque	*Activé*
Advanced_AlwaysSend DoNotTrack	Toujours envoyer l'en-tête Do Not Track	*Activé*

Moteur de recherche par défaut :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer		
AddSearchProvider	Ajouter une liste spécifique de moteurs de recherche à la liste des moteurs de recherche de l'utilisateur	*Activé*
AllowServicePoweredQSA	Autoriser les services Microsoft à proposer des suggestions améliorées lorsque l'utilisateur écrit dans la barre d'adresses	*Désactivé*
EnableSuggestedSites	Activer Sites suggérés	*Désactivé*
SearchDisableUserSuggestions	Désactiver les suggestions de tous les moteurs de recherche installés par l'utilisateur	*Activé*
SpecificSearchProvider	Restreindre les moteurs de recherche à une liste spécifique	*Activé*
NoIESearchBox	Empêcher l'affichage de la liste de recherche d'Internet Explorer	*Activé*
SearchTurnOffQuickPick	Désactiver le menu de recherche rapide	Au choix de l'entité
Search_NoFindFiles	Rechercher : désactiver la recherche de fichiers à l'aide de la touche F3 dans le navigateur	Au choix de l'entité
Search_NoSearchCustomization	Rechercher : désactiver la personnalisation des paramètres de recherche	*Activé*
Internet Explorer \ Paramètres Internet \ Saisie semie-automatique		
RestrictWSAutoComplete	Désactiver la saisie semi-automatique de recherche Windows	À définir en fonction de la stratégie d'administration système de l'entité
RestrictDomainSuggestion	Désactiver les suggestions d'URL	À définir en fonction de la stratégie d'administration système de l'entité (la liste des URL usuelles est stockée localement et est mise à jour une fois par mois. Aucune donnée utilisateur n'est envoyée sur Internet par cette fonctionnalité)
Internet Explorer \ Paramètres Internet \ Paramètres avancés \ Lors de la recherche		
Tous	Tous	À définir en fonction de la stratégie d'administration système de l'entité

Ensuite, la liste des moteurs de recherche peut être configurée par stratégie de groupe de préférences (GPP) à l'aide de clés de registre situées dans :
`HKCU\Software\Microsoft\Internet Explorer\SearchScopes\Internet Settings`.

Dans cet exemple, le moteur de recherche français `https://www.qwant.com` [18] est configuré comme moteur de recherche par défaut. N'importe quel autre moteur de recherche peut être utilisé. Chaque moteur doit être ajouté dans une sous clé GUID (clé unique à chaque moteur). Si le moteur de recherche souhaité est disponible en configuration automatique sur le site Web `www.iegallery.com` de Microsoft, il est dans ce cas recommandé de l'ajouter à un navigateur Internet Explorer depuis ce site afin de récupérer en base de registres le GUID correspondant. À défaut, il suffit de générer un GUID aléatoire et unique par moteur (sous la forme : `12345678-1234-1234-1234-123456789012` à la manière du moteur *Bing* déjà présent par défaut en base de registre). Une fois la clé GUID créée, le moteur se configure par les valeurs de clé de registre suivantes :

- : `DisplayName`, clé de type `REG_SZ` dont la valeur serait `Qwant` ;
- : `URL`, clé de type `REG_SZ` dont la valeur serait `https://www.qwant.com/?q=searchTerms`.
- : `FaviconURLFallback`, clé de type `REG_SZ` dont la valeur serait `https://www.qwant.com/favicon.ico`.

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

Paramètres de contenu :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_EnableHttp1_1	Utiliser HTTP 1.1	*Activé*
Advanced_PlayAnimations	Lire les animations dans les pages Web	Au choix de l'entité
Advanced_PlaySounds	Lire les sons dans les pages Web	Au choix de l'entité
Advanced_PlayVideos	Lire les vidéos dans les pages Web	Au choix de l'entité
Internet Explorer \ Paramètres Internet		
Tous	Tous	Au choix de l'entité
Internet Explorer \ Paramètres Internet \ Paramètres avancés \ Navigation		
Tous	Tous	Au choix de l'entité
Internet Explorer \ Paramètres Internet \ Paramètres avancés \ Multimédia		
EnableAlternativeCodec	Autoriser Internet Explorer à lire les fichiers multimédias qui utilisent des codecs de remplacement	*Désactivé*
Internet Explorer		
DisablePopupFilterLevel	Empêcher la modification du niveau de filtrage des fenêtres publicitaires	*Activé*
DisableSafetyFilterOverride	Empêcher le contournement des avertissements du filtre SmartScreen	*Activé*
DisableSafetyFilterOverride ForAppRepUnknown	Empêcher le contournement des avertissements du filtre SmartScreen pour les fichiers qui ne sont pas fréquemment téléchargés à partir d'Internet	*Activé*
Disable_Managing_ Phishing_Filter	Empêcher la gestion du filtre anti-hameçonnage	*Activé* avec la valeur `Automatique` (les adresses des sites Web ne figurant pas dans la liste locale de sites autorisée sont alors envoyées à Microsoft pour vérification sans demande à l'utilisateur).
Disable_Managing_ Safety_Filter_IE8	Désactiver la gestion du filtre SmartScreen pour Internet Explorer 8	*Activé* avec la valeur `Activé`
Disable_Managing_ Safety_Filter_IE9	Empêcher la gestion du filtre SmartScreen	*Activé* avec la valeur `Activé`
GeolocationDisable	Désactiver la géolocalisation du navigateur	*Activé*
NoTabBrowsingPopups	Désactiver la configuration des fenêtres publicitaires dans la navigation par onglets	Au choix de l'entité
PopupBlocker_AllowList	Liste des fenêtres publicitaires autorisées	*Non configuré* si *RestrictPopupExceptionList* autorise les fenêtres pop-up sur tous les sites et que le gestionnaire de fenêtres publicitaires est activé, sinon *Activé* avec comme valeur une liste blanche de sites sous la forme : `http://www.exemple.com` `[*].gouv.fr`
RestrictPopupExceptionList	Empêcher la gestion de la liste des exceptions du bloqueur de fenêtres publicitaires	*Activé* ou *Non configuré* en fonction de la marge de manœuvre de l'entité et du durcissement attendu
RestrictPopupManagement	Désactiver la gestion des fenêtres publicitaires	*Désactivé*
RestrictFormSuggest	Désactiver la saisie semi-automatique dans les formulaires	Au choix de l'entité

Page(s) d'accueil

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Général		
ContinuousBrowsing	Démarrer Internet Explorer avec les onglets de la dernière session de navigation	*Désactivé*
Internet Explorer		
RestrictHomePage	Désactiver la modification de la page d'accueil	*Activé* avec pour valeur l'url de la page d'accueil souhaitée
DisableReopenLastBrowsingSession	Désactiver Rouvrir la dernière session de navigation	*Activé*
NoSplash	Désactiver l'affichage de l'écran de démarrage	*Activé*
RestrictWebAddressSuggest	Désactiver la fonctionnalité de saisie semi-automatique des adresses Web	*Activé*

Serveur mandataire (proxy) :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer		
AutoProxyCache	Désactiver la mise en cache des scripts de proxy automatiques	Au choix de l'entité
DisplayScriptFailureUI	Afficher un message d'erreur lors d'échecs de téléchargement de scripts de proxy	Au choix de l'entité
RestrictProxy	Empêcher la modification des paramètres de proxy	*Activé*
UserProxy	Paramètres machine du serveur proxy (plutôt que les paramètres individualisés)	*Activé*
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_ProxyHttp1_1	Utiliser HTTP 1.1 avec une connexion par proxy	*Activé* sauf contrainte technique contraire

Les paramètres de proxy peuvent être simplement configurés par stratégie de groupe de préférences (GPP) à l'aide de valeurs de clé de registre situées dans `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings` :

- `ProxyEnable`, clé de type `DWORD` dont la valeur doit être `1` pour activer l'utilisation d'un serveur mandataire ;
- `ProxyServer`, clé de type `REG_SZ` dont la valeur doit indiquer les serveurs proxy à utiliser (exemple : `192.168.0.100:3128`).

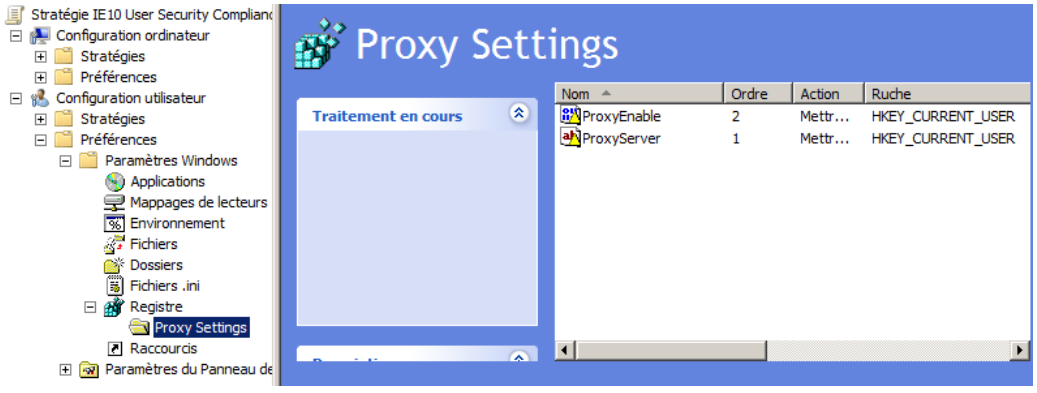

FIGURE 3 – GPP de configuration du serveur mandataire

Cette méthode a l'avantage de fonctionner pour toutes les versions du navigateur.

Administration système, maintenance, et options diverses :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Paramètres Entreprise \ Téléchargement de code		
CodeDownloadPol	Empêcher la spécification du chemin d'accès de téléchargement du code pour chaque ordinateur	*Activé* avec la valeur `CODEBASE`, dans la mesure ou les seuls contrôles ActiveX autorisés auront été pré-installés dans le navigateur par les administrateurs
Internet Explorer \ Supprimer l'historique de navigation		
Tous	Tous	À définir en fonction de la stratégie d'administration système de l'entité
Internet Explorer \ Panneau de configuration Internet \ Onglet Général \ Historique de navigation		
Tous	Tous	En fonction de la stratégie système de l'entité
Internet Explorer \ Panneau de configuration Internet \ Onglet Contenu		
Content_Show ContentAdvisor	Afficher le gestionnaire d'accès dans les Options Internet	*Désactivé*
Internet Explorer \ Panneau de configuration Internet \ Onglet Avancé		
Advanced_TemporaryInternetFiles	Vider le dossier Fichiers Internet temporaires lorsque le navigateur est fermé	*Désactivé*
Advanced_DisablePrefetchPrerender	Désactiver le chargement des pages Web en arrière plan pour optimiser les performances	*Non configuré*
Advanced_InternetExplorerUpdates	Vérifier automatiquement les mises à jour d'Internet Explorer	*Désactivé* puisque les mises à jour sont gérées en central par les équipes d'administration système
Advanced_InstallOnDemand_Other	Activer l'installation à la demande (sauf Internet Explorer)	*Désactivé*
Advanced_EnableCaretBrowsing	Activer la prise en charge de la navigation au clavier	*Non configuré*
Advanced_InstallOnDemand_IE	Autoriser l'installation à la demande (Internet Explorer)	*Désactivé*
Advanced_CDUnlock	Autoriser le contenu actif des CD à s'exécuter sur les ordinateurs des utilisateurs	*Désactivé*
Advanced_DisableClearType	Désactiver ClearType	*Non configuré*
Advanced_ProfileAssistant	Désactiver l'Assistant Profil	*Non configuré*
Advanced_DisableRIED	Ne pas autoriser la réinitialisation des paramètres d'Internet Explorer	*Non configuré*
ControlPanel_UTF8URLQuery	Désactiver l'encodage au format UTF-8 des chaînes de requêtes dans les URLs	*Non configuré*
Advanced_DisableFlipAhead	Désactiver la fonctionnalité d'avance rapide avec prédiction de page	*Activé* (fonctionnalité n'existant que sous Windows 8)
Advanced_DownloadSignatures	Vérifier les signatures des programmes téléchargés	*Activé*

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet		
ControlPanel_ RestrictAdvancedTab	Désactiver l'onglet Avancé	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictConnectionsTab	Désactiver l'onglet Connexions	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictContentTab	Désactiver l'onglet Contenu	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictGeneralTab	Désactiver l'onglet Général	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictPrivacyTab	Désactiver l'onglet Confidentialité	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictProgramsTab	Désactiver l'onglet Programmes	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_ RestrictSecurityTab	Désactiver l'onglet Sécurité	Au choix de l'entité (l'onglet peut être affiché dans la mesure ou les paramètres de configuration sont verrouillés)
ControlPanel_Send IDNNames	Envoyer des noms IDN	*Activé*
ControlPanel_Send UTF8Query	Utiliser UTF-8 pour les liens mailto	*Non configuré*
Internet Explorer \ Paramètres Internet \ Mise à jour des composants \ Vérification périodique		
Tous	Tous	*Activé* avec valeur par défaut étant donné que la mise à jour du navigateur sera effectuée de manière centralisée par l'équipe d'administration système
Internet Explorer \ Paramètres Internet \ Mise à jour des composants \ Menu Aide		
Tous	Tous	Au choix de l'entité
Internet Explorer \ Paramètres Internet		
DefaultTilesView	Ouvrir les vignettes Internet Explorer sur le Bureau	Au choix de l'entité (Internet explorer en version *Desktop* ou *ModernUI*)
DefaultLinksView	Définir le mode d'ouverture des liens dans Internet Explorer	Au choix de l'entité (Internet explorer en version *Desktop* ou *ModernUI*)
Internet Explorer \ Persistance		
Tous	Tous	Il est bon de limiter la taille de la persistance DHTML du point de vue de l'administration système, mais ceci n'affecte en rien la sécurité des postes utilisateurs.
Internet Explorer \ Fonctionnalités de sécurité		
IESF_DisableDEP	Désactiver la prévention de l'exécution des données	*Désactivé*
IESF_DisableDataURI	Désactiver la prise en charge d'URI des données	*Activé*

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Barres d'outils		
DisableDeveloperTools	Désactiver les outils de développement	*Désactivé*, sauf pour les développeurs Web ou pour un navigateur dédié à la navigation sur Internet
DisableToolbarUpgrader	Désactiver l'outil de mise à niveau des barres d'outils	*Activé*
HideCommandBar	Masquer la barre de commandes	Au choix de l'entité
HideStatusBar	Masquer la barre d'état	Au choix de l'entité
LockToolbars	Verrouiller toutes les barres d'outils	*Activé*
MoveStopRefresh	Verrouiller l'emplacement des boutons Arrêter et Actualiser	*Activé*
MoveTabBand	Afficher les onglets sur une ligne distincte	Au choix de l'entité
NoBandCustomize	Désactiver la personnalisation des barres d'outils du navigateur	Au choix de l'entité
NoToolbarCustomize	Désactiver la personnalisation des boutons de la barre d'outils du navigateur	Au choix de l'entité
SetCommandLabels	Personnaliser les étiquettes des commandes	Au choix de l'entité
ToolbarButtons	Configurer les boutons de la barre d'outils	Au choix de l'entité
UseLargeIcons	Utiliser de grandes icônes pour les boutons de commande	Au choix de l'entité
Internet Explorer		
AlwaysShowMenu	Activer la barre de menus par défaut	Au choix de l'entité
DisableFavoritesBar	Désactiver le Volet des Favoris	Au choix de l'entité
DisableInterchanging MenuBarNavBar	Placer la barre de menus au-dessus de la barre de navigation	Au choix de l'entité
DisableTabGrouping	Désactiver le regroupement des onglets	Au choix de l'entité
EnforceFullscreen	Appliquer le mode plein écran	Au choix de l'entité
General_Zooming	Désactiver la fonction de zoom	Au choix de l'entité
NoQuickTabs	Désactiver la fonctionnalité Aperçu mosaïque	Au choix de l'entité
DialupSettings	Désactiver la modification des paramètres de l'onglet Avancé	*Activé*
DisableACRPrompt	Désactiver la récupération automatique après blocage	*Activé*
NotifyNotDefaultBrowser	Avertir les utilisateurs si Internet Explorer n'est pas le navigateur Web par Défaut	*Désactivé*
RestrictAutoconfig	Désactiver la modification des paramètres de la configuration automatique	*Activé*
RestrictCache	Désactiver la modification des paramètres des fichiers Internet temporaires	*Activé*
RestrictCertificates	Désactiver la modification des paramètres des certificats	*Activé*
RestrictCheckBrowser	Désactiver la modification du navigateur par défaut	*Activé*
RestrictConnectionSettings	Désactiver la modification des paramètres de connexion	*Activé*
RestrictConnectionWizard	Désactiver l'Assistant Connexion Internet	*Activé*
RestrictFormSuggest	Désactiver la modification des paramètres des polices	*Activé*
RestrictMessaging	Désactiver la modification des paramètres de la messagerie	*Activé*
RestrictProfiles	Désactiver la modification des paramètres de l'Assistant Profil	*Activé*
RestrictRatings	Désactiver la modification des paramètres du contrôle d'accès	*Activé*
RestrictResetWebSettings	Désactiver la fonctionnalité Rétablir les paramètres Web	Au choix de l'entité

Nom de stratégie	Description	Valeur recommandée
Branding_NoExternalBranding	Désactiver la personnalisation d'Internet Explorer par des tiers	*Activé*
ControlPanel_RestrictAdvanced	Utiliser la détection automatique pour les connexions par numérotation	Au choix de l'entité
FavImportExport	Désactiver l'Assistant Importer/Exporter les paramètres	Au choix de l'entité
NoFirstRunCustomise	Empêcher l'exécution de l'Assistant Première exécution	Au choix de l'entité
OESettings	Configurer Outlook Express	*Désactivé*
Enable_Compat_Logging	Activer l'enregistrement de la compatibilité	En fonction des besoins
SQM_DisableCEIP	Empêcher la participation au Programme d'amélioration de l'expérience utilisateur	*Activé*
NoUpdateCheck	Désactiver la vérification périodique des mises à jour de logiciels Internet Explorer	*Activé* au profit d'une mise à jour poussée par WSUS
EnableAutoUpgrade	Installer automatiquement les nouvelles versions d'Internet Explorer	*Désactivé*
Customized_UserAgent_String	Personnaliser la chaîne de l'agent utilisateur	Au choix de l'entité si nécessaire
Disable_Fix_Security_Settings	Interdire la fonctionnalité « Corriger les paramètres »	*Désactivé*
Disable_Security_Settings_Check	Désactiver la fonctionnalité de vérification des paramètres de sécurité	*Désactivé*
FastShutdownOnUnload	Autoriser le comportement d'arrêt d'Internet Explorer 8	*Désactivé*
Identities	Gestionnaire d'identifications : empêcher les utilisateurs d'utiliser des identifications	*Activé*
MediaSettings	Configurer le volet d'exploration du média	*Activé* avec pour valeur `Désactiver le volet d'exploration et ne pas lire automatiquement les fichiers du média`
NewTabAction	Spécifier le comportement par défaut d'un nouvel onglet	Au choix de l'entité
NoHelpMenu	Empêcher l'accès à l'aide d'Internet Explorer	Au choix de l'entité
NoTabBrowsing	Désactiver la navigation par onglets	Au choix de l'entité
NoWindowReuse	Empêcher la configuration du mode d'ouverture des fenêtres	Au choix de l'entité
RestrictAccessibility	Désactiver la modification des paramètres d'accessibilité	Au choix de l'entité
RestrictCalendarContact	Désactiver la modification des paramètres du Calendrier et de la Liste des contacts	Au choix de l'entité
RestrictColors	Désactiver la modification des paramètres de couleurs	Au choix de l'entité
RestrictLanguages	Désactiver la modification des paramètres de langue	Au choix de l'entité
RestrictLinks	Désactiver la modification des paramètres de couleurs des liens	Au choix de l'entité
SecondaryHomePages	Désactiver la modification des paramètres des pages d'accueil secondaires	*Activé* avec pour valeur `about:blank` par exemple
ShellNotifications	Désactiver les notifications de mise à jour de logiciels provenant de l'interface intégrée, lors du lancement du programme	*Désactivé*
TabOpenInFgndBgnd	Empêcher la configuration de la création d'un onglet	Au choix de l'entité
TabProcGrowth	Définir le développement de processus d'onglet	*Désactivé* (le paramètre par défaut étant optimal vis à vis de la mémoire physique du poste de travail)
TurnOffPinnedSites	Désactiver la capacité à épingler les sites dans Internet Explorer sur le Bureau.	Au choix de l'entité

Affichage de compatibilité :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Affichage de compatibilité		
CompatView_AllSites	Activer le mode standard d'Internet Explorer 7	En fonction des besoins (*Activé* pour davantage de compatibilité mais au détriment du contenu utilisant les dernières normes)
CompatView_DisableList	Désactiver l'affichage de compatibilité	En fonction du périmètre d'utilisation du navigateur. *Activé* pour la navigation en Intranet étant donné que des listes prédéfinies devraient indiquer le mode d'affichage optimal des différents sites sans que l'utilisateur ait à intervenir, et *Désactivé* pour la navigation sur Internet.
CompatView_ShowButton	Bouton Désactiver l'affichage de compatibilité	Idéalement identique à la stratégie `CompatView_DisableList`
CompatView_IntranetSites	Activer le mode standard d'Internet Explorer pour l'intranet local	Il est plus fréquent de nécessiter un affichage en mode IE7 ou Quirks sur l'intranet plutôt qu'un affichage standard pour du contenu dernière génération. Ce paramètre sera donc défini en fonction du besoin.
CompatView_UseMSList	Inclure des listes de sites Web mises à jour à partir de Microsoft	Au choix en fonction du périmètre d'utilisation du navigateur et de la stratégie de l'entité

CompatView_UsePolicyList	Utiliser la liste des sites d'Internet Explorer 7	*Activé* avec pour valeur une liste de sites à afficher en mode IE7 sous la forme :
		`http://www.intranet.fr`
		`[*.].intranet.fr`

CompatView_UseQuirksPolicyList	Utiliser la liste des sites en mode Quirks	*Activé* avec pour valeur une liste de sites à afficher en mode IE7 sous la forme :
		`http://www.intranet.fr`
		`[*.].intranet.fr`

Paramétrages spécifiques aux différentes zones de sécurité :

Affectation des sites aux zones :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Sécurité		
SecurityPage_AutoDetect	Activer la détection automatique du réseau intranet	*Désactivée*, au profit d'un renseignement manuel exhaustif des sites dans la zone intranet
SecurityPage_WarnOnIntranet	Activer la notification de contenu intranet dans la Barre de notification	*Non configuré*
IZ_Zonemaps	Liste des attributions de sites aux zones	*Activé* en spécifiant une liste sous la forme « Site + Valeur » où : « Site » est un nom de domaine ou une adresse ip ; « Valeur » est un chiffre indiquant la zone d'affectation : - 1 : intranet ; - 2 : sites approuvés ; - 3 : internet ; - 4 : sites sensibles.
Tous modèles de zones	Tous modèles de zones	*Non configuré*, au profit d'un paramétrage manuel et explicite du niveau de sécurité des différentes zones
IZ_IncludeUnspecifiedLocalSites	Sites intranet : inclure tous les sites locaux (intranet) non mentionnés dans d'autres zones	*Désactivé*, au profit d'une liste explicite
IZ_ProxyByPass	Sites intranet : inclure tous les sites qui n'utilisent pas de serveur proxy	*Désactivé*, au profit d'une liste explicite
IZ_UNCAsIntranet	Sites intranet : inclure tous les chemins d'accès réseau UNC	*Désactivé*, au profit d'une liste explicite
Internet Explorer		
Security_HKLM_only	Zones de sécurité : utiliser uniquement les paramètres ordinateur	*Activé* à moins que les paramètres de zones soient distribués par GPO Utilisateurs
Security_options_edit	Zones de sécurité : ne pas autoriser les utilisateurs à modifier les stratégies	*Activé*
Security_zones_map_edit	Zones de sécurité : ne pas autoriser les utilisateurs à ajouter/supprimer des sites	*Activé*

Zone Sites Sensibles :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Sécurité		
IZ_PolicyRestrictedSitesZoneTemplate	Modèle de zones Sites sensibles	*Activé* avec la valeur `Haute`
IZ_PolicyRestrictedSitesZoneLockdownTemplate	Modèle de zones Sites sensibles verrouillées	*Activé* avec la valeur `Haute`

Zone Internet :

Nom de stratégie	Description	Valeur recommandée
Internet Explorer \ Panneau de configuration Internet \ Onglet Sécurité \ Zone Internet verrouillée et **Internet Explorer \ Panneau de configuration Internet \ Onglet Sécurité \ Zone Internet**		
IZ_PolicyAccessDataSourcesAcrossDomains	Accès aux sources de données sur plusieurs domaines	*Activé* avec la valeur `Désactivé`
IZ_Policy_Phishing	Activer l'analyse par le filtre SmartScreen	*Activé* avec la valeur `Activé`
IZ_PolicyMimeSniffingURLaction	Activer la détection MIME	*Activé* avec la valeur `Activé`
IZ_PolicyTurnOnXSSFilter	Activer le filtre anti-script de site à site	*Activé* avec la valeur `Activé`
IZ_Policy_TurnOnProtectedMode	Activer le mode protégé	*Activé* avec la valeur `Activé`
IZ_Policy_UnsafeFiles	Afficher un avertissement de sécurité pour les fichiers potentiellement dangereux	*Activé* avec la valeur `Demander`
IZ_PolicyDisplayMixedContent	Afficher un contenu mixte	*Activé* avec la valeur `Demander`
IZ_PolicyJavaPermissions	Autorisations Java	*Activé* avec la valeur `Désactiver Java`
IZ_PolicySoftwareChannelPermissions	Autorisations pour les chaînes du logiciel	*Activé* avec la valeur `Haute sécurité`
IZ_PolicyAllowMETAREFRESH	Autoriser l'actualisation des métafichiers	*Non configuré*
IZ_PolicyInstallDesktopItems	Autoriser l'installation des éléments du Bureau	*Activé* avec la valeur `Désactiver`
IZ_Policy_WebBrowserControl	Autoriser la création de scripts basés sur des contrôles WebBrowser pour Internet Explorer	*Activé* avec la valeur `Désactiver`
IZ_Policy_WebBrowserApps	Autoriser le chargement des applications du navigateur XAML	*Activé* avec la valeur `Désactiver`
IZ_Policy_XAML	Autoriser le chargement des fichiers XAML	*Activé* avec la valeur `Désactiver`
IZ_Policy_XPS	Autoriser le chargement des fichiers XPS	*Activé* avec la valeur `Désactiver`
IZ_PolicyDropOrPasteFiles	Autoriser le glisser-déplacer ou le copier-coller des fichiers	*Activé* avec la valeur `Demander`
IZ_PolicyBinaryBehaviors	Autoriser les comportements des fichiers binaires et des scripts	*Non configuré*
IZ_PolicyWindowsRestrictionsURLaction	Autoriser les fenêtres initiées par des scripts sans contrainte de taille ou de position	*Activé* avec la valeur `Désactiver`
IZ_Policy_ScriptStatusBar	Autoriser les mises à jour de la barre d'état via le script	*Activé* avec la valeur `Désactivé`
IZ_PolicyAllowPasteViaScript	Autoriser les opérations couper, copier ou coller dans le Presse-papiers à l'aide d'un script	*Activé* avec la valeur `Désactiver`
IZ_Policy_AllowScriptlets	Autoriser les scriptlets	*Activé* avec la valeur `Désactiver`
IZ_PolicyActiveScripting	Autoriser les scripts actifs	*Activé* avec la valeur `Désactiver`

Nom de stratégie	Description	Valeur recommandée
IZ_Policy_ScriptPrompt	Autoriser les sites Web à demander des informations à l'aide de fenêtres scriptées	*Activé* avec la valeur `Désactiver`
IZ_Policy_AddressStatusBar	Autoriser les sites Web à ouvrir des fenêtres sans barre d'état ni barre d'adresses	*Activé* avec la valeur `Désactiver`
IZ_PolicyFileDownload	Autoriser les téléchargements de fichiers	Au choix de l'entité
IZ_PolicyFontDownload	Autoriser les téléchargements de polices	*Activé* avec la valeur `Désactiver`
IZ_Policy_AllowDynsrcPlayback	Autoriser les vidéos et les animations sur une page Web qui utilise un ancien lecteur multimédia	*Activé* avec la valeur `Désactiver`
IZ_PolicyOnlyAllowApprovedDomains ToUseActiveXWithoutPrompt	Autoriser uniquement les domaines approuvés à utiliser les contrôles ActiveX sans invite	*Activé* avec la valeur `Activé`
IZ_PolicyScriptActiveXMarkedSafe	Contrôles ActiveX reconnus sûrs pour l'écriture de scripts	*Activé* avec la valeur `Désactivé`
IZ_PolicyScriptActiveXNotMarkedSafe	Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés	*Activé* avec la valeur `Désactivé`
IZ_PolicyNotificationBar ActiveXURLaction	Demander confirmation pour les contrôles ActiveX	*Activé* avec la valeur `Désactivé`
IZ_PolicyNotificationBar DownloadURLaction	Demander confirmation pour les téléchargements de fichiers	*Activé* avec la valeur `Désactivé`
IZ_Policy_WinFXRuntimeComponent	Désactiver l'installation du .NET Framework	*Activé* avec la valeur `Activé`
IZ_Policy_FirstRunOptInDefaultEnable	Désactiver l'invite de première exécution	*Non configuré*
IZ_PolicyAntiMalwareCheckingOf ActiveXControls	Ne pas exécuter les anti-malwares contrôle les contrôles ActiveX	*Non configuré*
IZ_PolicyRenderLegacyFilters	Effectuer le rendu des filtres hérités	*Non configuré*
IZ_PolicySubmitNonencryptedFormData	Envoyer les données de formulaire non chiffrées	*Non configuré*
IZ_PolicyUnsignedFramework ComponentsURLaction	Exécuter les composants dépendant du .NET Framework non signés avec Authenticode	*Activé* avec la valeur `Désactivé`
IZ_PolicySignedFramework ComponentsURLaction	Exécuter les composants dépendant du .NET Framework signés avec Authenticode	*Activé* avec la valeur `Désactivé`
IZ_PolicyRunActiveXControls	Exécuter les contrôles ActiveX et les plug-ins	*Activé* avec la valeur `Demander` si les seuls contrôles et plug-ins installés sont ceux déployés par l'entité.
IZ_Policy_LocalPathForUpload	Inclure le chemin d'accès local lorsque l'utilisateur télécharge des fichiers sur un serveur	*Activé* avec la valeur `Désactivé`
IZ_PolicyLaunchAppsAndFilesInIFRAME	Lancement des applications et des fichiers dans un cadre IFRAME	*Activé* avec la valeur `Désactivé`
IZ_PolicyZoneElevationURLaction	Les sites Web des zones de contenu de moindre privilège peuvent naviguer dans cette zone	*Activé* avec la valeur `Désactivé`
IZ_PolicyNavigateSubframesAcrossDomains	Naviguer dans des fenêtres et des cadres sur différents domaines	*Activé* avec la valeur `Désactivé`

Nom de stratégie	Description	Valeur recommandée
IZ_PolicyNoPromptForOneOrNoClient Certificate	Ne pas proposer la sélection d'un certificat client lorsqu'il n'en existe qu'un ou aucun	*Désactivé*
IZ_PolicyLogon	Options d'ouverture de session	*Activé* avec la valeur `Demander le nom d'utilisateur et le mot de passe`
IZ_PolicyUserdataPersistence	Permanence des données utilisateur	*Activé* avec la valeur `Activé`
IZ_PolicyDragDropAcrossDomains WithinWindow	Permettre de faire glisser du contenu entre des domaines dans la même fenêtre	*Activé* avec la valeur `Désactivé`
IZ_PolicyDragDropAcrossDomains AcrossWindows	Permettre de faire glisser du contenu entre les domaines dans des fenêtres distinctes	*Activé* avec la valeur `Désactivé`
IZ_PolicyScriptingOfJavaApplets	Script des applets Java	*Non configuré*
IZ_PolicyDownloadSignedActiveX	Télécharger les contrôles ActiveX signés	*Activé* avec la valeur `Désactivé`
IZ_PolicyDownloadUnsignedActiveX	Télécharger les contrôles ActiveX non signés	*Activé* avec la valeur `Désactivé`
IZ_PolicyBlockPopupWindows	Utiliser le bloqueur de fenêtres publicitaires	*Activé* avec la valeur `Activé`

Annexe II :
Déploiement et configuration de Microsoft Internet Explorer par GPO dans un domaine Active Directory

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

Téléchargement de l'exécutable d'installation

La dernière version de Microsoft Internet Explorer est disponible sur le site Web de Microsoft [19]. Au moment de la rédaction de cette note, elle nécessite l'installation préalable de mises à jour Windows sans lesquelles l'installation échouera [20].

Le téléchargement n'est proposé qu'au format exécutable. L'utilisation de Microsoft IEAK [21] permet en revanche la construction de paquets d'installation personnalisés au format MSI.

Dans la plupart des scénarios de déploiement, Microsoft Internet Explorer sera téléchargé directement par WSUS et proposé au déploiement aux administrateurs systèmes. L'exécutable d'installation pourrait par exemple faire l'objet d'une règle AppLocker [22] spécifique ou globale de manière à en autoriser l'exécution ainsi qu'à en assurer l'intégrité.

Règles de configuration

Pour pouvoir définir des règles de configuration de Microsoft Internet Explorer 11 à l'aide d'une GPO, il convient d'avoir préalablement ajouté les modèles d'administration adéquats. Ces modèles d'administration sont compatibles avec toutes les versions du navigateur. Pour chaque élément de configuration, il est en effet précisé à quelles versions ils s'appliquent :

19. http://windows.microsoft.com/fr-fr/internet-explorer/ie-11-worldwide-languages.
20. http://support.microsoft.com/kb/2847882.
21. http://technet.microsoft.com/fr-fr/ie/bb219517.aspx.
22. Pour plus d'informations, se référer aux recommandations de l'ANSSI pour la mise en oeuvre d'une politique de restrictions logicielles sous 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-pour-la-mise-en-oeuvre-d-une-politique-de-restrictions.html.

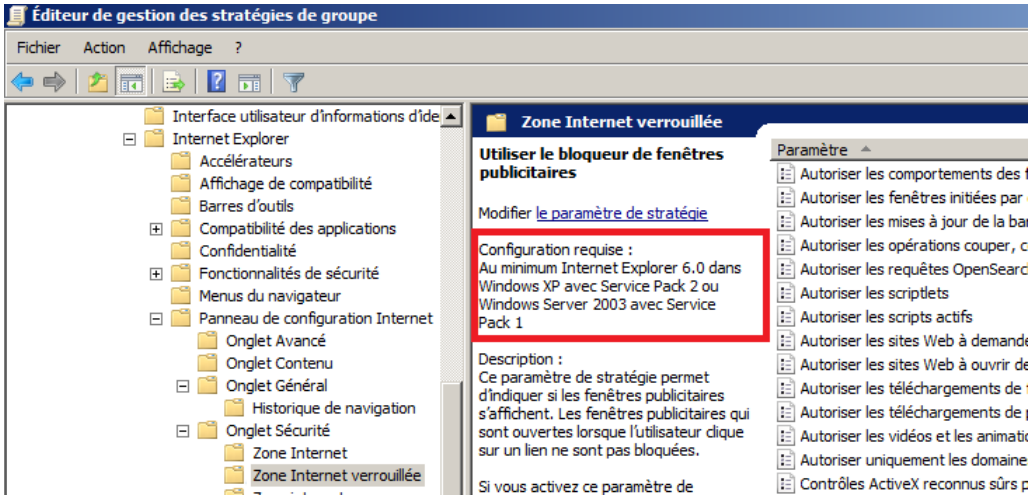

FIGURE 4 – Configuration requise d'un paramètre de GPO

Sans mise à jour des modèles d'administration, seuls les éléments de configuration hérités des anciennes versions du navigateur pourront être contrôlés.

Windows Server 2012 R2 et Windows 8.1

Sur un contrôleur de domaine Windows Server 2012 R2 et sur Windows 8.1, les modèles d'administration de Microsoft Internet Explorer 11 sont déjà présents.

Versions antérieures de Windows Server

Sur un contrôleur de domaine en version Windows Server 2012 ou antérieur, il est nécessaire d'ajouter les modèles d'administration manuellement. Ces derniers sont fournis par Microsoft au format `ADM` à l'adresse https://www.microsoft.com/en-us/download/details.aspx?id=40905. Ils peuvent également être récupérés au format `ADMX` (à compléter de la traduction française au format `ADML`) sur tout poste de travail où Microsoft Internet Explorer 11 a été installé. Ces 2 fichiers se trouvent aux emplacements suivants :

- `%systemroot%\PolicyDefinitions\inetres.admx` ;
- `%systemroot%\PolicyDefinitions\fr-FR\inetres.adml`.

Ensuite, dans un scénario de déploiement en domaine Active Directory, les modèles ADMX ou ADM doivent être déposés 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 suivante :
http://technet.microsoft.com/fr-fr/library/cc709647.

GPO pré-configurées

Microsoft fournit un outil gratuit de gestion des conformités de sécurité (SCM, *Security Compliance Manager*) disponible sur le site `TechNet` de Microsoft à l'adresse http://technet.microsoft.com/fr-fr/solutionaccelerators/cc835245.aspx. Cet outil permet, entre autres, de générer automatiquement des GPO pré-configurées pour les versions 8, 9 et 10 de Microsoft Internet Explorer et intègre les paramétrages de sécurité recommandés par Microsoft. Au moment de la rédaction de cette

note, l'outil n'intègre pas encore Microsoft Internet Explorer 11 [23]. Néanmoins, seule une dizaine d'éléments de configuration ont fait leur apparition avec la version 11. Les recommandations indiquées pour la version 10 pourront donc être utilisées comme base de configuration pour la version 11 du navigateur.

L'installation de Microsoft SCM ne doit en aucun cas se faire sur un contrôleur de domaine ou un serveur en production, mais sur un poste de travail d'administration par exemple. Une fois installé, l'outil permet d'exporter les paramètres Ordinateur (*Computer Security*) et Utilisateur (*User Security*) au format « GPO Backup » (il est préférable de renommer chaque dossier après export, pour davantage de clarté). Ces sauvegardes peuvent ensuite être importées dans une GPO du domaine Active directory via la console de gestion des stratégies de groupe, comme illustré à la figure 5.

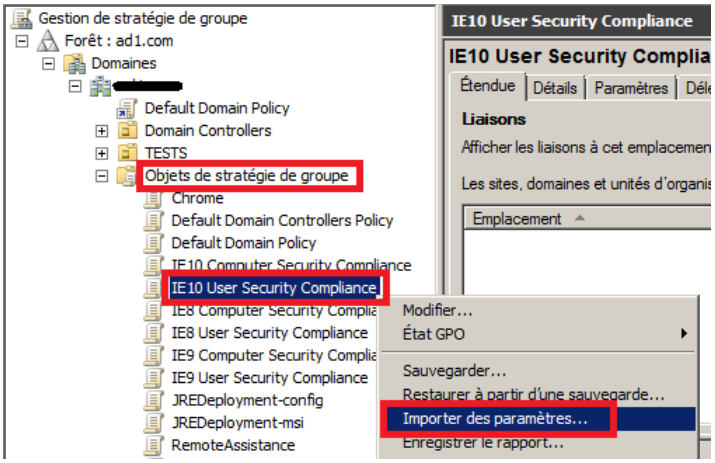

FIGURE 5 – Import de GPO

Ces GPO n'ont alors plus qu'à être complétées et adaptées aux besoins spécifiques de l'entité. Notons toutefois que la plupart des paramètres de ces GPO pré-configurées sont appliqués au niveau utilisateur et non pas au niveau machine.

Cette méthode nécessite que la GPO existe et ses paramètres seront alors écrasés. Il est également possible d'importer directement la GPO sans qu'elle existe préalablement en utilisant PowerShell et son module GroupPolicy.

23. Microsoft a publié la version finale de leurs recommandations de sécurité pour Internet Explorer 11 en date du 13 août 2014. En attendant leur intégration à SCM, il est toutefois possible d'en prendre connaissance à l'adresse https://blogs.technet.com/b/secguide/archive/2014/08/13/security-baselines-for-windows-8-1-windows-server-2012-r2-and-internet-explorer-11-final.aspx. Ces documents abordent de manière plus générale la sécurité des systèmes Windows 8.1 et Windows Server 2012 R2, et ne traitent pas uniquement de la sécurité d'Internet Explorer 11.

Annexe III :
Compatibilité d'affichage et respect des standards

Une critique souvent formulée à l'encontre de Microsoft Internet Explorer concerne les incompatibilités d'affichage d'une version à l'autre du navigateur. Les changements radicaux entre versions entraînent ainsi des incompatibilités avec les applications Web. Il en résulte alors souvent le maintien d'anciennes versions de Microsoft Internet Explorer au sein des systèmes d'information pour de simples raisons de compatibilité.

Si les paramètres d'affichage de compatibilité n'ont pas une grande incidence sur la sécurité, ils en ont par contre du point de vue de l'administration du système d'information. En effet, dès lors que Microsoft Internet Explorer est utilisé pour la navigation en Intranet, il est primordial qu'il permette d'afficher correctement l'ensemble des sites et applications Web accessibles. Les modes d'affichage supportés depuis Microsoft Internet Explorer 8 sont :

- le mode *Quirks* correspondant au mode d'affichage de Microsoft Internet Explorer 5 ;
- le mode *Internet Explorer 7* correspondant comme son nom l'indique au mode d'affichage de Microsoft Internet Explorer 7 ;
- le mode *standard* correspondant au mode d'affichage le plus récent pris en charge par la version installée.

Des paramètres de « listes de sites » permettent de prédéfinir, par site, le mode d'affichage à utiliser. Il est également possible de changer le mode d'affichage par défaut du navigateur.

Deux points de vigilance sont par ailleurs à noter :

- Microsoft Internet Explorer 11 a comme particularité de présenter un *User-Agent*[24] différent de toutes les versions précédentes puisqu'il ne contient plus la chaîne « `MSIE` ». en effet, il présente désormais une chaîne ressemblant à celle d'un navigateur alternatif (« `Mozilla/5.0 (Windows NT 6.x; Trident/7.0; rv:11.0) like Gecko` »). Les nombreux sites Web qui cherchent à afficher du contenu compatible Microsoft Internet Explorer en se basant sur cette chaîne de caractères se trouvent alors trompés et ne le considérèrent pas comme un navigateur Microsoft Internet Explorer mais comme un navigateur alternatif.
- la restriction des *User-Agent* en sortie au niveau des passerelles d'interconnexion (sur serveurs mandataires par exemple) doit donc prendre en compte l'utilisation possible de multiples *User-Agent* pour Microsoft Internet Explorer.

Certains sites ou applicatifs Web pourront alors ne plus détecter correctement les navigateurs Microsoft Internet Explorer. Notons qu'il n'est pas recommandé de se fier aux chaînes User-Agent pour les détecter et qu'il est préférable d'insérer des commentaires conditionnels dans le code HTML ou de tester la présence de fonctionnalités JavaScript qui leur sont spécifiques. Sur les équipements de filtrage ne pouvant filtrer que les chaînes User-Agent, il sera alors possible de chercher l'un des termes « `*MSIE*` » ou « `*Trident*` » pour juger être en présence d'un navigateur Microsoft Internet Explorer. Dans le cas ou il ne serait pas possible d'intervenir facilement côté serveurs ou équipements, une autre option consisterait à modifier la chaîne User-Agent du navigateur par GPO (voir annexe I) et de spécifier une chaîne personnalisée comme par exemple « `Mozilla/5.0 (compatible; MSIE 11.0; Trident/7.0; rv:11.0) like Gecko` » qui devrait permettre d' identifier un navigateur Microsoft Internet Explorer 11 dans de nombreux cas.

24. Le *User-Agent* est une entête HTTP qui contient des informations sur le client à l'origine de la requête.