Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A-3 : Énoncé des travaux – Filtrage de contenu

Date : 8 juin 2012

TABLE DES MATIÈRES

RÉFÉRENCE

Voir l'appendice C : Définitions et acronymes de l'annexe A pour obtenir une définition des termes et des acronymes utilisés dans la présente annexe.

1 FILTRAGE DE CONTENU

(1) Le filtrage de contenu constitue un des services de gestion des menaces du SSGGC. Lorsque le Canada en fait la commande par l'émission d'une autorisation de tâches, le filtrage de contenu, tel qu'il est géré et mis en œuvre par l'entrepreneur, doit respecter ou dépasser toutes les exigences mentionnées dans la présente annexe et dans le reste de l'Énoncé des travaux, ainsi qu'ailleurs dans le contrat, et ce, avant son acceptation par le Canada et tout au long de la durée du contrat.

1.1 Qualité de service

(2) L'entrepreneur doit catégoriser les adresses URL qui ne le sont pas dans les sept jours en suivant la première détection automatique.

(3) L'entrepreneur doit catégoriser de nouveau les adresses URL qui ne l'ont pas été dans les sept jours suivant une demande présentée par le Canada.

1.2 Détection et réponse

(4) Le filtrage de contenu doit bloquer et autoriser, en temps réel, l'accès à Internet en fonction des dispositions de la politique d'utilisation acceptable.

(5) Le filtrage de contenu doit privilégier la politique d'utilisation acceptable s'adressant particulièrement aux utilisateurs.

(6) Le filtrage de contenu doit afficher une page Web indiquant le blocage du site par filtrage de contenu lorsque l'accès à Internet contrevient à la politique d'utilisation acceptable.

(7) Le filtrage de contenu doit bloquer l'accès sortant à Internet en exécutant le sous-ensemble de la politique d'utilisation acceptable qui s'applique à la demande en question.

(8) Le filtrage de contenu doit bloquer l'accès entrant à Internet en exécutant le sous-ensemble de la politique d'utilisation acceptable qui s'applique à la réponse en question.

(9) Le filtrage de contenu doit bloquer le contenu infecté de virus ou de codes malveillants (voir l'annexe A-4 : Énoncé des travaux – Antivirus).

(10) Le filtrage de contenu doit automatiquement déterminer la catégorie d'URL et la réputation de celle-ci.

(11) Le filtrage de contenu doit retourner jusqu'à cinq catégories par URL.

(12) Le filtrage de contenu doit s'exécuter sans égard à la langue et au contenu.

(13) L'état à sécurité intégrée du filtrage de contenu doit être configurable à la position ouverte ou fermée, tel que le précise le Canada.

1.3 Politique d'utilisation acceptable

(14) La politique d'utilisation acceptable en matière de filtrage de contenu doit comprendre, au minimum, des politiques visant le blocage des demandes en fonction de ce qui suit :

a) L'adresse IP de destination ou la gamme d'adresses IP;

b) Le domaine;

c) Le sous-domaine;

d) L'adresse URL;

e) L'adresse URL secondaire;

f) L'heure du jour;

g) Le type de fichier;

h) Le mot-clé;

i) La réputation de l'URL;

j) La catégorie d'URL;

k) La signature du contenu;

l) L'utilisateur;

m) L'adresse IP source ou la gamme d'adresses IP;

n) Le protocole;

o) Les quotas horaires par catégorie par jour (facultatif);

p) Les quotas en volume par catégorie par jour (facultatif);

q) Le contenu Web (contrôle Active X, applets Java, témoins, etc.);

r) Les métadonnées de pages Web;

s) L'en-tête MIME.

(15) La politique d'utilisation acceptable en matière de filtrage de contenu doit permettre la configuration des exceptions de blocage.

(16) Les catégories d'URL doivent comprendre ce qui suit, sans s'y limiter :

a) Les sites pornographiques ou de sexe;

b) Les sites haineux;

c) Les sites racistes;

d) Les sites illégaux;

e) Les sites violents;

f) Les sites de jeu;

g) Les sites de jeux;

h) Les sites connus pour diffuser des virus ou des codes malveillants;

i) Les sites de courriel gratuit;

j) Les sites anonymiseurs;

k) Les sites de nouvelles;

l) Les sites des services bancaires et financiers;

m) Les sites de sports;

n) Les sites de divertissement;

o) Les sites de vente aux enchères;

p) Les sites de magasinage;

q) Les sites axés sur les styles de vie;

r) Les sites de réseautage social;

s) Les sites de communications Internet;

t) Les sites de contenu audio ou vidéo sur Internet, comme les sites de radio ou de télévisions sur Internet;

u) Les sites permettant le téléchargement du type de fichiers suivant :

i) MP3;

ii) MPEG et autres fichiers vidéo utilisant beaucoup de bande passante.

(17) L'entrepreneur doit fournir les catégories d'URL et indiquer la réputation rattachée à celles-ci.

(18) La politique d'utilisation acceptable en matière de filtrage de contenu doit s'appliquer à au moins une des catégories suivantes :

a) Toutes les demandes;

b) L'organisation cliente;

c) L'utilisateur;

d) L'adresse IP source;

e) Le groupe d'utilisateurs;

f) Le protocole;

g) Le réseau de départ.

(19) Le filtrage de contenu doit permettre l'élaboration d'une politique d'utilisation acceptable à partir de la combinaison d'une ou de plusieurs politiques.

(20) Le filtrage de contenu doit permettre la gestion de la politique d'utilisation acceptable grâce à la création de groupes logiques de politiques, où un groupe logique peut contenir un certain nombre de politiques, ainsi que des groupes logiques.

1.4 Configuration

1.4.1 Page Web indiquant le blocage du site

(21) Le filtrage de contenu doit permettre la configuration de la page Web indiquant le blocage du site; le service affiche cette page lorsque l'accès au site est bloqué.

(22) Le page Web indiquant le blocage du site par filtrage de contenu doit être propre à l'organisation cliente.

(23) Le Canada doit approuver ladite page Web.

1.4.2 Catégories personnalisées

(24) Le filtrage de contenu doit permettre la gestion des catégories personnalisées d'URL.

(25) Le filtrage de contenu doit permettre la gestion des URL figurant dans les catégories

personnalisées d'URL.

1.4.3 Politique d'utilisation acceptable axée sur l'utilisateur

(26) Le filtrage de contenu doit trouver les groupes auxquels appartient un utilisateur en appliquant l'une ou l'autre des méthodes qui suivent, selon ce que précise le Canada à l'égard de l'organisation cliente :

a) L'interrogation d'un annuaire fourni par le Canada pour l'organisation cliente;

b) L'interrogation du référentiel du SSGGC.

(27) Le portail de services doit permettre à un utilisateur autorisé de gérer les politiques d'utilisation acceptable propres à un groupe, notamment :

a) Visualiser les politiques d'utilisation acceptable par groupe d'utilisateurs;

b) Rechercher les politiques d'utilisation acceptable par champ disponible;

c) Rechercher les politiques d'utilisation acceptable par groupe d'utilisateurs;

d) Attribuer les politiques d'utilisation acceptable aux groupes d'utilisateurs, et les dissocier;

e) Appliquer les modifications apportées au filtrage de contenu du SSGGC.

(28) Le portail de services doit permettre à un utilisateur autorisé de gérer des groupes d'utilisateurs, notamment :

a) Visualiser les groupes d'utilisateurs;

b) Rechercher les groupes d'utilisateurs par champ disponible;

c) Ajouter et supprimer des utilisateurs faisant partie de groupes d'utilisateurs;

d) Appliquer les modifications apportées au filtrage de contenu du SSGGC.

(29) Le filtrage de contenu doit appliquer les politiques d'utilisation acceptable en fonction des groupes d'utilisateurs auxquels appartient l'utilisateur, le cas échéant.

(30) Le filtrage de contenu doit sélectionner l'annuaire afin d'extraire l'information concernant l'utilisateur, selon une politique précisée par le Canada.

(31) L'entrepreneur doit mettre en œuvre l'interface entre le filtrage de contenu et les annuaires LDAP fournis par l'organisation cliente.

1.5 Mises à jour de sécurité automatiques

(32) Le filtrage de contenu doit prendre en charge les mises à jour automatiques d'URL exécutées directement depuis Internet (c'est-à-dire sans dépendre d'un dispositif intermédiaire) toutes les heures, au plus.

(33) L'entrepreneur doit fournir les mises à jour automatiques d'URL dans les 15 minutes suivant le moment où le fournisseur les rend disponibles.

(34) Le filtrage de contenu doit appliquer les mises à jour d'URL sans redémarrage dans les 15 minutes suivant leur réception.

1.6 Authentification

(35) Le filtrage de contenu doit authentifier les demandes d'accès à Internet au moyen de

l'adresse IP source.

(36) Lorsque l'authentification de l'adresse IP échoue, le filtrage de contenu doit authentifier les demandes d'accès à Internet en recourant à au moins un des services d'authentification suivants fournis par le Canada, selon ce que celui-ci précise pour chaque organisation cliente :

a) Un certificat X.509;

b) Un serveur RADIUS;

c) Un serveur LDAP;

d) Un serveur SecurID;

e) Un service d'annuaire Active Directory.

(37) Le filtrage de contenu doit permettre l'accès à Internet au moyen des politiques par défaut, si la demande ne peut être authentifiée.

(38) L'entrepreneur doit mettre en œuvre l'interface entre le filtrage de contenu et les services d'authentification précisés par le Canada pour chaque organisation cliente.

(39) L'entrepreneur doit s'assurer que les processus d'authentification utilisés par le filtrage de contenu n'ont pas d'incidence sur les autres processus d'authentification mis en œuvre par le Canada, ou ne les entravent pas.

1.7 Interopérabilité

(40) Le filtrage de contenu ne doit pas nécessiter de modifications de la configuration du dispositif d'extrémité qui accède à Internet.

1.8 Interface

(41) Lorsqu'un mandataire est requis, le filtrage de contenu doit rediriger la demande sur des commutateurs de couche 4 au moyen d'un mandataire fonctionnant en mode transparent.

(42) Le filtrage de contenu doit traiter toutes les demandes visant à faire passer les sites Web au travers de tout type de point de contrôle Internet, comme les pare-feu, les serveurs ou des dispositifs de mise en cache, qui est configurable en fonction des critères définis par le Canada.

(43) Le filtrage de contenu doit prendre en charge les configurations liées au lissage du trafic, en fonction de chaque politique; cette pratique vise notamment :

a) Des applications particulières;

b) Des réseaux particuliers;

c) Une bande passante garantie;

d) Une bande passante maximale.

1.9 Journalisation

(44) Le filtrage de contenu doit enregistrer toutes les demandes et réponses qui ont donné lieu à une infraction à la politique d'utilisation acceptable, dont les renseignements qui suivent :

a) Les politiques échouées, ainsi que les valeurs réelles qui ont causé l'échec;

b) L'URL;

c) Les catégories d'URL;

d) La réputation de l'URL;

e) Le type de contenu (c'est-à-dire Adobe Flash, ActiveX, etc.);

f) La date et l'heure;

g) Le nom de l'utilisateur;

h) L'adresse IP source;

i) Le groupe;

j) Le nom de l'organisation cliente;

k) Le réseau;

l) Les mots-clés.

(45) Le filtrage de contenu doit enregistrer toutes les demandes qui se sont soldées par une URL non catégorisée ou non réputée, dont, au minimum, les renseignements qui suivent :

a) L'URL;

b) Les catégories d'URL;

c) La réputation de l'URL;

d) La date et l'heure;

e) Le nom de l'utilisateur;

f) L'adresse IP source;

g) Le groupe;

h) Le nom de l'organisation cliente.

1.10 Rapports

1.10.1 Rapports mensuels

(46) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales catégories d'URL bloquées, où :

i) Les catégories d'URL figurent sur l'axe x;

ii) Le nombre total de demandes bloquées figure sur l'axe y;

b) Les 10 principales catégories d'URL bloquées, présentées sous forme de tableau, indiquant :

i) Les totaux par catégorie d'URL;

ii) Le nombre total de demandes bloquées.

(47) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales URL bloquées, où :

i) Les URL figurent sur l'axe x;

ii) Le nombre total de demandes bloquées figure sur l'axe y;

b) Les 10 principales URL bloquées, présentées sous forme de tableau, indiquant :

i) Les totaux par URL;

ii) Le nombre total de demandes bloquées.

(48) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales catégories d'URL visitées, où :

i) Les catégories d'URL figurent sur l'axe x;

ii) Le nombre total de demandes de visite figure sur l'axe y;

b) Les 10 principales catégories d'URL visitées, présentées sous forme de tableau, indiquant :

i) Les totaux par catégorie d'URL;

ii) Le nombre total de demandes de visite.

(49) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales catégories d'URL visitées selon la bande passante utilisée, où :

i) Les catégories d'URL figurent sur l'axe x;

ii) La bande passante totale associée aux demandes de visite figure sur l'axe y;

b) Les 10 principales catégories d'URL visitées selon la bande passante utilisée, présentées sous forme de tableau, indiquant :

i) Les totaux par catégorie d'URL;

ii) La bande passante totale associée aux demandes de visite.

(50) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principaux protocoles selon la bande passante utilisée, où :

i) Les protocoles figurent sur l'axe x;

ii) La bande passante totale associée aux demandes de visite figure sur l'axe y;

b) Les 10 principaux protocoles selon la bande passante utilisée, présentés sous forme de tableau, indiquant :

i) Les totaux par protocole;

ii) La bande passante totale associée aux demandes de visite.

(51) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales catégories de risque selon la bande passante utilisée, où :

i) Les catégories de risque figurent sur l'axe x;

ii) Le nombre total de demandes de visite figure sur l'axe y;

b) Les 10 principales catégories de risque selon la bande passante utilisée, présentées sous forme de tableau, indiquant :

i) Les totaux par catégorie de risque;

ii) Le nombre total de demandes de visite.

(52) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales URL visitées, où :

i) Les URL figurent sur l'axe x;

ii) Le nombre total de demandes de visite figure sur l'axe y;

b) Les 10 principales URL visitées, présentées sous forme de tableau, indiquant :

i) Les totaux par URL;

ii) Le nombre total de demandes de visite.

(53) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau ou de graphique; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Un résumé, sous forme de graphique à colonnes, des 10 principales URL visitées selon la bande passante utilisée, où :

i) Les URL figurent sur l'axe x;

ii) La bande passante totale associée aux demandes de visite figure sur l'axe y;

b) Les 10 principales URL visitées selon la bande passante utilisée, présentées sous forme de tableau, indiquant :

i) Les totaux par URL;

ii) La bande passante totale associée aux demandes de visite.

(54) L'entrepreneur doit fournir au Canada un rapport mensuel concernant le filtrage de contenu, sous forme de tableau; les données sont ventilées par organisation cliente et portent sur ce qui suit :

a) Les URL non catégorisées;

   i) Le nombre total d'URL demandées;

   ii) Le nombre total d'URL non catégorisées;

   iii) Le pourcentage d'URL non catégorisées;

b) Les 10 principales URL non catégorisées, présentées sous forme de tableau, indiquant :

   i) Les totaux par URL;

   ii) Le nombre total de demandes de visite;

c) Les URL non réputées;

   i) Le nombre total d'URL demandées;

   ii) Le nombre total d'URL non réputées;

   iii) Le pourcentage d'URL non réputées;

d) Les 10 principales URL non réputées, présentées sous forme de tableau, indiquant :

   i) Les totaux par URL;

   ii) Le nombre total de demandes de visite.

1.11 Mise en œuvre

(55) L'entrepreneur doit inventorier, examiner, optimiser et mettre en œuvre, dans le SSGGC, les règles, politiques et toute autre configuration existantes de la solution existante de filtrage de contenu de l'organisation cliente.

(56) L'entrepreneur doit documenter, examiner, optimiser et mettre en œuvre, dans le SSGGC, les exigences de l'organisation cliente relatives à la configuration du filtrage de contenu.

(57) L'entrepreneur doit configurer l'interface avec l'annuaire de l'organisation cliente, selon ce que précise le Canada.

1.12 Gestion des changements

(58) L'entrepreneur doit mettre à jour la page Web indiquant le blocage du site, dans les deux JOFPF suivant la demande présentée par le Canada à ce sujet.

(59) L'entrepreneur doit mettre à jour les politiques d'utilisation acceptable, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(60) L'entrepreneur doit configurer les politiques d'utilisation acceptable, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(61) L'entrepreneur doit ajouter des catégories personnalisées d'URL, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.

(62) L'entrepreneur doit ajouter des URL aux catégories personnalisées, selon ce que demande le Canada, en fonction des niveaux de priorisation qu'il précise.