Government of Canada Managed Security Service (GCMSS)

Annex A-3: Statement of Work - Content Filtering

Date: June 8, 2012

TABLE OF CONTENTS

REFERENCE

Please refer to Annex A - Appendix C: Definitions and Acronyms for a definition of terms and acronyms utilized throughout this annex.

1 CONTENT FILTERING

(1) The Content Filtering is one of the GCMSS Threat Management Services. When ordered by Canada, by issuing a Task Authorization, the Content Filtering, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this annex, in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period of the Contract.

1.1 Quality of Service

(2) The Contractor must categorize uncategorized URLs within 7 days of the first automatic detection.

(3) The Contractor must re-categorize miss-categorized URLs within 7 days of a request by Canada.

1.2 Detection and Response

(4) The Content Filtering must block and allow access to the Internet based on the Acceptable Use Policy in real-time.

(5) The Content Filtering must give precedence to user-specific Acceptable Use Policy.

(6) The Content Filtering must display a Content Filtering blocked-site web page when the Internet access violates the Acceptable Use Policy.

(7) The Content Filtering must block the outgoing Internet access by executing the subset of the Acceptable Use Policy that applies to the request.

(8) The Content Filtering must block the incoming Internet access by executing the subset of the Acceptable Use Policy that applies to the response.

(9) The Content Filtering must block content containing viruses and malicious code (refer to GCMSS Annex A-4: Statement of Work - Antivirus).

(10) The Content Filtering must automatically determine the URL category and URL reputation.

(11) The Content Filtering must return up to 5 categories per URL.

(12) The Content Filtering must be language and content agnostic.

(13) The Content Filtering fail-safe state must be configurable to open or close as specified by Canada.

1.3 Acceptable Use Policy

(14) The Content Filtering Acceptable Use Policy must include, at minimum, policies to block requests by:

a) destination IP address or range of IP addresses;

b) domain;

c) sub-domain;

d) URL;

e) sub-URL;

f) time of day;

g) file type;

h) keyword;

i) URL reputation;

j) URL category;

k) content signature;

l) User;

m) source IP address or range of IP addresses;

n) protocol;

o) time quota per category per day (optional);

p) volume quota per category per day (optional);

q) web content (Active X, Java Applets, Cookies, etc.);

r) web page metadata; and

s) MIME Header.

(15) The Content Filtering Acceptable Use Policy must allow for the configuration of blocking exceptions.

(16) The URL categories must include, but not be limited to, the following:

a) pornography/sex sites;

b) hatred sites;

c) racism sites;

d) illegal sites;

e) violence sites;

f) gambling sites;

g) games sites;

h) sites known to distribute viruses and malware;

i) free email sites;

j) anonymizer sites;

k) news sites;

l) bank and financial service sites;

m) sports sites;

n) entertainment sites;

o) auction sites;

p) shopping sites;

q) lifestyles sites;

r) social networking;

s) Internet communications;

t) audio/video streaming sites such as Internet radio and Internet tv;

u) websites which can download the following files:

i) MP3 files; and

ii) MPEG and other video files which consume high bandwidth.

(17) The Contractor must provide the categorization and reputation of URLs.

(18) The Content Filtering Acceptable Use Policy must be enforceable for one or more of the following categories:

a) all requests;

b) Client Organization;

c) User;

d) source IP address;

e) User group;

f) protocol; and

g) originating network.

(19) The Content Filtering must allow for the construction of an Acceptable Use Policy from a combination of one or many policies.

(20) The Content Filtering must allow the management of Acceptable Use Policy by creating logical groups of policies where a logical group can contain any number of policies as well as logical groups.

1.4 Configuration

1.4.1 Blocked-site Web Page

(21) The Content Filtering must allow for the configuration of the blocked-site web page that the service displays when access to a site is blocked.

(22) The Content Filtering blocked-site web page must be Client Organization specific.

(23) Canada must approve the Content Filtering blocked-site web page.

1.4.2 Customized Categories

(24) The Content Filtering must allow the management of customized URL categories.

(25) The Content Filtering must allow the management of URLs within customized URL categories.

1.4.3 User-based Acceptable Use Policy

(26) The Content Filtering must find the groups a user belongs to using the following methods, as specified by Canada for the Client Organization:

a) a query to a Canada provided directory for the Client Organization; or

b) a query to the GCMSS repository.

(27) The Service Portal must allow an authorized User to manage group-specific Acceptable Use Policies that include:

a) viewing Acceptable Use Policies by user group;

b) searching Acceptable Use Policies by any available field;

c) searching Acceptable Use Policies by user groups;

d) assign and unassign Acceptable Use Policies to user groups; and

e) applying modifications to the GCMSS Content Filtering.

(28) The Service Portal must allow an authorized User to manage user groups that include:

a) viewing user groups;

b) searching user groups by any available field;

c) adding, deleting Users in user groups; and

d) applying modifications to the GCMSS Content Filtering.

(29) The Content Filtering must apply the Acceptable Use Policies according to the user groups the user belongs to, if any.

(30) The Content Filtering must select the directory to retrieve the User information based on a policy specified by Canada.

(31) The Contractor must implement the interface between the Content Filtering and the Client Organization provided LDAP directories.

1.5 Automatic Security Updates

(32) The Content Filtering must support automatic URL updates directly over the public Internet (ie no dependency of any intermediate device) at maximum every hour.

(33) The Contractor must provide automatic URL updates within 15 minutes of availability from their supplier.

(34) The Content Filtering must apply URL updates without rebooting within 15 minutes of receiving the updates.

1.6 Authentication

(35) The Content Filtering must authenticate requests to access the Internet using the source IP address.

(36) When the IP address authentication fails, the Content Filtering must authenticate requests to access the Internet using one or more of the following Authentication Services provided by Canada, and as specified by Canada for each Client Organization:

a) X.509 Certificate;

b) RADIUS Server;

c) LDAP Server;

d) SecurID Server; and

e) Active Directory.

(37) The Content Filtering must allow access to the Internet with default policies if the request cannot be authenticated.

(38) The Contractor must implement the interface between the Content Filtering and the Authentication Services specified by Canada for each Client Organization.

(39) The Contractor must ensure that authentication processes used by the Content Filtering do not affect or impair any additional authentication processes implemented by Canada.

1.7 Interoperability

(40) The Content Filtering must not require configuration changes to the end device that accesses the Internet.

1.8 Interface

(41) When a proxy machine is required, the Content Filtering must redirect the request on layer 4 switches via transparent mode proxy.

(42) The Content Filtering must process all requests for websites to pass through any type of Internet control point, such as firewall, server or caching device which is configurable based on criteria defined by Canada.

(43) The Content Filtering must support configuration of traffic shaping on a per policy basis including:

a) specific applications;

b) specific networks;

c) guaranteed bandwidth; and

d) maximum bandwidth.

1.9 Logging

(44) The Content Filtering must log all requests and responses that resulted in a violation of the Acceptable Use Policy, including, at minimum, the following:

a) failed policies along with actual values that caused the failure;

b) URL;

c) URL Categories;

d) URL Reputation;

e) content type (i.e. Adobe Flash, ActiveX, etc.);

f) date and time;

g) User;

h) source IP address;

i) Group;

j) Client Organization;

k) Network; and

l) keywords.

(45) The Content Filtering must log all requests that resulted in an uncategorized URL or unreputated URL including, at minimum, the following:

a) URL;

b) URL Categories;

c) URL Reputation;

d) date and time;

e) User;

f) source IP address;

g) Group; and

h) Client Organization.

1.10 Reporting

1.10.1 Monthly Reports

(46) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 blocked URL categories;

i) URL categories on the x axis; and

ii) total number of blocked requests on the y axis;

b) top 10 blocked URL categories in tabular format with totals;

i) URL category; and

ii) total number of blocked requests.

(47) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 blocked URLs;

i) URL on the x axis; and

ii) total number of blocked requests on the y axis;

b) top 10 blocked URLs in tabular format with totals;

i) URL; and

ii) total number of blocked requests.

(48) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 visited URL categories;

i) URL categories on the x axis; and

ii) total number of visit requests on the y axis;

b) top 10 visited URL categories in tabular format with totals;

i) URL category; and

ii) total number of visit requests.

(49) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 visited URL categories by bandwidth;

i) URL categories on the x axis; and

ii) total bandwidth (KB) of visit requests on the y axis;

b) top 10 visited URL categories by bandwidth in tabular format with totals;

i) URL category; and

ii) total bandwidth (KB) of visit requests.

(50) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 protocols by bandwidth;

i) protocols on the x axis; and

ii) total bandwidth (KB) of visit requests on the y axis;

b) top 10 protocols by bandwidth in tabular format with totals;

i) protocol; and

ii) total bandwidth (KB) of visit requests.

(51) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 risk categories by bandwidth;

i) risk categories on the x axis; and

ii) total number of visit requests on the y axis;

b) top 10 risk categories by bandwidth in tabular format with totals;

i) risk category; and

ii) total number of visit requests.

(52) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 visited URLs;

i) URL on the x axis; and

ii) total number of visit requests on the y axis;

b) top 10 visited URLs in tabular format with totals;

i) URL; and

ii) total number of visit requests.

(53) The Contractor must provide a monthly Content Filtering report to Canada in tabular and graphical format by Client Organization that includes:

a) a summary in column-chart format for the top 10 visited URLs by bandwidth;

i) URL on the x axis; and

ii) total bandwidth (KB) of visit requests on the y axis;

b) top 10 visited URLs by bandwidth in tabular format with totals;

i) URL; and

ii) total bandwidth (KB) of visit requests.

(54) The Contractor must provide a monthly Content Filtering report to Canada in tabular format by Client Organization that includes:

a) Uncategorized URLs;

i) total number of URLs requested;

ii) total number of uncategorized URLs; and

iii) percentage of uncategorized URLs;

b) top 10 uncategorized URLs in tabular format with totals;

i) URL; and

ii) total number of visit requests;

c) Unreputated URLs;

i) total number of URLs requested;

ii) total number of unreputated URLs; and

iii) percentage of unreputated URLs;

d) top 10 unreputated URLs in tabular format with totals;

i) URL; and

ii) total number of visit requests.

1.11 Implementation

(55) The Contractor must inventory, review, optimize and implement, in GCMSS, existing rules, policies, and any other configuration of the existing content filtering solution of the Client Organization.

(56) The Contractor must document, review, optimize and implement in GCMSS configuration requirements of the Client Organization for the Content Filtering.

(57) The Contractor must configure the interface with the Client Organization directory as specified by Canada.

1.12 Change Management

(58) The Contractor must update the blocked-site web page when requested by Canada within 2 FGWDs.

(59) The Contractor must update Acceptable Use Policies, as requested by Canada, in accordance with priority levels as specified by Canada.

(60) The Contractor must configure Acceptable Use Policies, as requested by Canada, in accordance with priority levels as specified by Canada.

(61) The Contractor must add customized URL categories, as requested by Canada, in accordance with priority levels as specified by Canada.

(62) The Contractor must add URLs to customized categories, as requested by Canada, in accordance with priority levels as specified by Canada.