Government of Canada Managed Security Service (GCMSS)

Attachment 2.1: Historical Information

Date: June 8, 2012

1 FOREWORD

(1) The following historical data is provided for *information purposes only* and should not be construed as commitments from Canada.

2 MANAGED SECURITY SERVICES

(2) Shared Services Canada (SSC) currently delivers a suite of fully managed perimeter defence services including the existing Managed Security Services (MSS) portfolio to client departments.

(3) MSS is presently procured under the Secure Channel SA02 contract that will end in December 2013. Consequently, this GCMSS procurement initiative has been initiated to competitively retender these services and transition existing MSS clients to GCMSS by December 2013.

(4) The MSS portfolio of services provides a comprehensive set of solutions covering perimeter security, intrusion detection and content filtering for web and email. These services, that can be combined with existing GC-owned solutions for holistic protection of departmental public access zones, include:

a) Managed Intrusion Detection Service (IDS) to monitor Information Technology (IT) network traffic for hostile activity and alerts the client to organized attacks or security breaches at the earliest stage. The intrusion detection sensors are strategically placed within the client network and on the Internet. Network and host traffic are monitored in real time using a comprehensive database of known attack sequences.

b) Managed Firewall Service (MFS) to provide continuous monitoring by an IT security network that serves as a gateway between the client and the Internet, protecting the network from hackers and attacks.

c) Managed Anti-Virus Service to protect the departmental network against malicious activity by scanning Simple Mail Transfer Protocol (SMTP) traffic for files suspected of containing untrustworthy code, and by filtering all inbound and outbound e-mail traffic at the gateway. Once identified as suspicious, the suspect mail is stopped and quarantined to prevent further infection.

d) Managed Anti-Spam Service to help reduce unsolicited commercial e-mail by filtering e-mail messages for both inbound and outbound spam at the gateway, before it reaches the user's inbox. External Simple Mail Transfer Protocol (SMTP) mail is routed to where the spam is detected and dropped before being forwarded to their destination. The service uses a number of spam detection techniques such as sender base reputation, keyword search, heuristics, spam signature comparison, real-time black lists, language-based filtering and other methods.

e) Managed URL Filtering to monitor and restrict employee access to undesirable Internet sites. A customized and dynamic database that conforms to Government of Canada (GC) policies obstructs access to undesirable Internet sites by targeting specific Web content and elements. Internet users are restricted from certain Web sites; thereby reducing time spent inappropriately "surfing", and reducing exposure to potential legal liabilities.

(5) MSS is managed, monitored and maintained by Information Security specialists around-the-clock to protect data, reduce network security risks and respond to rapidly changing security needs.

3 MSS Deployment Architecture

(6) The MSS deployment architecture is comprised of centralized and distributed solutions as shown in Figure 1. The centralized solution is located into the Contractor's data center and delivers the Anti-Virus and the Anti-Spam services to the subscribing client departments using department's specific policies. The centralized solution is based on Cisco IronPort Email Security Appliances. The distributed solution is located into individual departments Public Access Zone (PAZ) within their data center. The distributed solution is based on Fortinet Fortigate and Cisco ASA UTM appliances to deliver Firewall and Intrusion Detection services and WebSense Web Filter to deliver content filtering.

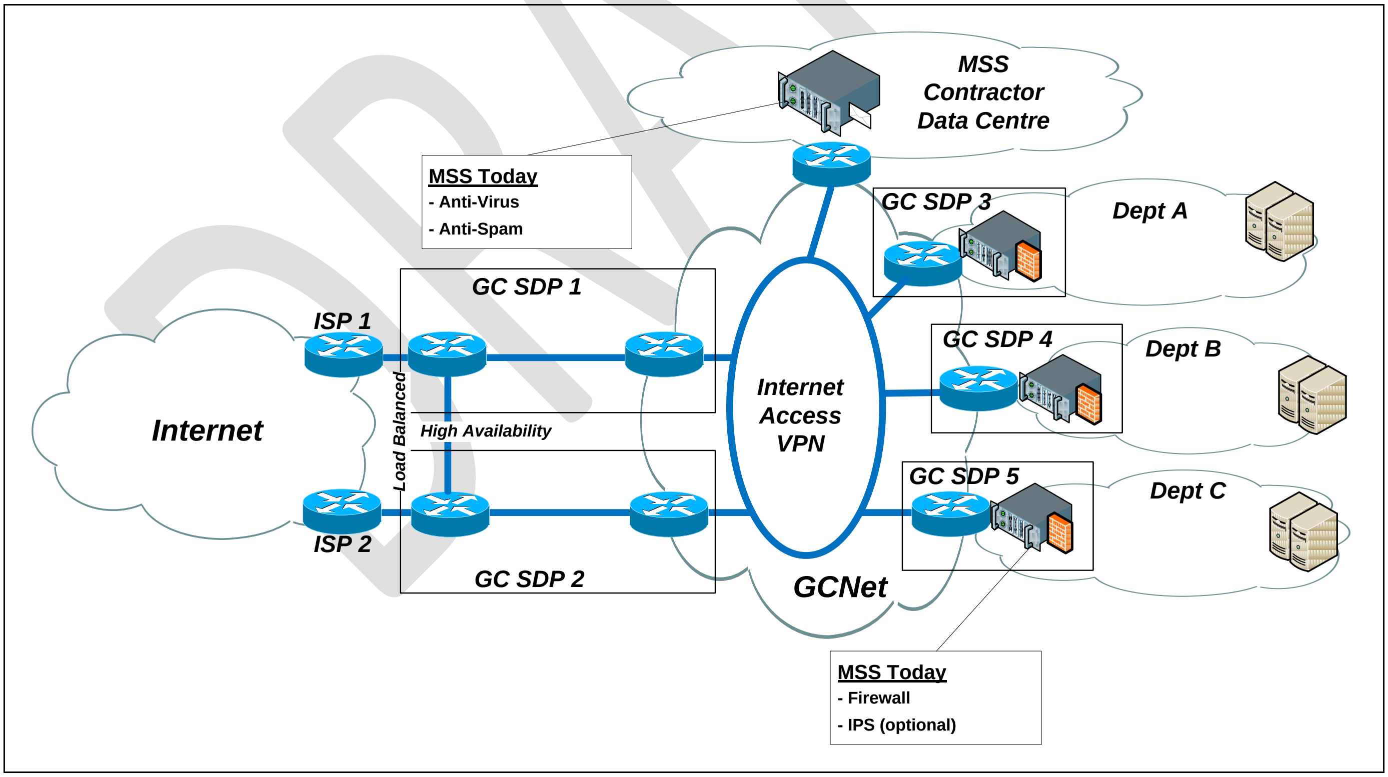

Figure 1 - MSS Deployment Architecture

4 DEPLOYED MSS

(7) Table 1 below lists the equipments that are deployed, as of April 2012, to deliver the managed security services to the subscribing Client Organizations. The table does not include infrastructure related equipments such as aggregation switches; it only includes equipments directly delivering MSS. All SDPs are located in Ottawa and each SPD represents a different Client Organization to the exception of the Contractor SDP that handles multiple clients.

SDP in Ottawa	QTY	Service	Device Type	Manufacturer	Product Name	Product Model/Version	Description
SDP1	1	ITM/UTM	Appliance	Fortinet	Fortigate	FG-110C-BDL-950-DD	FG-110c-FW, FG-110c-DDoS, FG-110c-IDP, FG-110c-WF
SDP2	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco 4240 IPS Sensor
	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	Catalyst	WS-C2960G-24TC-L	Cisco Gigabit Aggregation Switch - Cisco 2960G-24 - 24 10/100/1000, 4 T/SFP LAN Base Image
	2	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Copper Tap
SDP3	2	Firewall	Appliance	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PROD Primary + Secondary FW
	1	Firewall	Appliance	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PRE-PROD FW
	1	Firewall	Server	IBM	xSeries System x	x3350	IBM SYSTEM X3350 Syslog Server
	3	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	11	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 Pre-Prod REZ
SDP4	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	Catalyst	WS-C2950T-24	IDS Aggregation Switch WS-C2950T-24
	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9
	2	ITM/UTM	Appliance	Fortinet	Fortigate	FG-200B	FG-200b-FW, FG-200b-WF, FG-200b-IDP Primary + Secondary
SDP5	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	3	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 OZ
SDP6	2	Firewall	Appliance	Cisco Systems	ASA	5550	Cisco ASA5550-BUN-K9 Firewall
	2	Firewall	Server	IBM	xSeries System x	x3350	IBM SYSTEM X3350 Model 4192-B2U Syslog Server
	2	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4255-K9	Cisco IPS-4255-K9 Network Sensor
	8	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 VPN-OZ
	3	Web Content Filtering	Server	IBM	xSeries_System x	x3550	IBM SYSTEM X3550 Model 7946-AC1 794692U Websense Log and Reporting Server
SDP7	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS 4240

SDP in Ottawa	QTY	Service	Device Type	Manufacturer	Product Name	Product Model/Version	Description
	3	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics TP-CU3 10/100/1000 for MSS.NCC
SDP8	2	Firewall	Appliance	Cisco Systems	ASA	5550	Cisco ASA5550-BUN-K9 PROD Primary + Secondary FW
	1	Firewall	Server	IBM	xSeries System x	x3550	IBM SYSTEM X3550 M2 794652U Syslog Server
	8	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT ByPass	BP-HBCU3	NetOptics 10/100/1000 Bypass Switch with Heartbeat
	4	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
SDP9	2	Firewall	Appliance	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PROD Primary + Secondary FW
	1	Firewall	Server	IBM	xSeries System x	x3250	IBM SYSTEM x3250 M3 4251C2U Syslog Server
SDP10	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	7	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 OZ P
SDP11	1	Firewall	Appliance	Cisco Systems	PIX 500 Series Security Appliances	515E	Cisco PIX 515e
	1	Firewall	Appliance	Cisco Systems	ASA	5505	Cisco ASA5505-BUN-K9
	1	Firewall	Server	SYSTEM (GENERIC)	Other UNIX Server		Syslog Server
	1	Firewall	Server	IBM	xSeries System x	x3250	IBM SYSTEM x3250 M3 4251C2U Syslog Server
	2	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	9	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3
SDP12	1	IDS (NIDS/NIPS)	Appliance	Cisco Systems	IPS	IPS-4255-K9	Cisco IPS-4255-K9 Network Sensor
	7	IDS (NIDS/NIPS)	Appliance	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 Prod OZ1
Contractor	4	Antispam/Antivirus Gateway	Appliance	IronPort	E-mail Security Appliance	X1060-R-NA	Centralized IronPort appliances for Anti-Spam / Anti-Virus services Support a current total of **78,839** users across 25 client departments
	2	Antispam/Antivirus Gateway	Appliance	IronPort	E-mail Security Appliance	C650	
	1	Antispam/Antivirus Gateway	Appliance	IronPort	E-mail Security Appliance	X1070	

Table 1 - MSS Equipment Inventory and Location

5 OPERATIONAL STATISTICS

(8) From May 2011 to April 2012, the MSS contractor handled approximately:

a) 204 Requests for Change; and

b) 512 Incident Tickets.