Service de sécurité géré du gouvernement du Canada (SSGGC)

Document joint 2.1 : Données historiques

Date : 8 juin 2012

1 AVANT-PROPOS

(1) Les données historiques qui suivent sont fournies *à titre d'information seulement* et ne doivent pas être interprétées comme étant un engagement de la part du Canada.

2 SERVICES DE SÉCURITÉ GÉRÉS

(2) Services partagés Canada offre actuellement aux ministères clients une suite de services de défense du périmètre entièrement gérés, y compris le portefeuille existant de services de sécurité gérés (SSG).

(3) L'acquisition des SSG se fait actuellement dans le cadre du contrat SA02 de la Voie de communication protégée qui prendra fin en décembre 2013. En conséquence, le lancement du présent projet d'acquisition d'un SSGGC a pour but de soumettre une nouvelle demande de soumissions concurrentielles à l'égard de ces services et d'amener les clients à effectuer la transition des SSG existants aux services du SSGGC d'ici décembre 2013.

(4) Le portefeuille de SSG offre un ensemble complet de solutions visant la sécurité du périmètre, la détection des intrusions et le filtrage de contenu lié au Web et au courriel. Ces services, qui peuvent être jumelés aux solutions existantes que possède le GC aux fins de protection globale des zones d'accès public des ministères, comprennent ce qui suit :

a) Le Service de détection des intrusions géré a pour but la surveillance du trafic du réseau TI, afin de déceler toute activité hostile et d'alerter le client dès qu'il détecte des attaques organisées ou des atteintes à la sécurité. Des détecteurs d'intrusions sont placés de façon stratégique dans le réseau du client et sur Internet. Le trafic émanant du réseau et des hôtes est suivi en temps réel au moyen d'une base de données exhaustive sur les manœuvres d'attaque connues.

b) Le Service de pare-feu géré assure une surveillance permanente par un réseau de sécurité informatique qui joue un rôle de « passerelle » entre le client et Internet, protégeant ainsi le réseau contre les pirates et les attaques.

c) Le Service d'antivirus géré protège le réseau du ministère contre les activités malveillantes en balayant le trafic basé sur le protocole simple de transfert de courrier (SMTP) à la recherche de fichiers soupçonnés de contenir du code nuisible et en filtrant tous les courriels entrants et sortants au niveau de la passerelle. Quand un courriel est désigné comme étant suspect, il est arrêté et mis en quarantaine pour prévenir toute contamination.

d) Le Service antipourriel géré contribue à réduire le nombre de courriels commerciaux non sollicités en filtrant le courriel entrant et sortant au niveau de la passerelle. Ce service bloque les courriels non sollicités à la passerelle, avant qu'ils atteignent les boîtes aux lettres des utilisateurs. Le courrier SMTP externe est acheminé en un point où les pourriels sont détectés et supprimés avant d'être transmis à leur destinataire. Le service recourt à un certain nombre de techniques de détection des pourriels, comme la cote de réputation de SenderBase, la recherche par mots clés, la connaissance heuristique, la comparaison de

signatures de pourriel, les listes noires en temps réel et le filtrage basé sur la langue.

e) Le Filtrage d'URL géré a pour but la surveillance des accès et il empêche les employés d'accéder aux sites Internet jugés indésirables. Fondé sur une base de données dynamique et personnalisée conforme aux politiques du gouvernement du Canada en la matière, ce service bloque l'accès aux sites Internet indésirables en ciblant des contenus et des éléments Web précis. Les utilisateurs d'Internet sont privés de l'accès à certains sites, ce qui réduit le temps passé sur des sites inappropriés et atténue les risques de poursuites judiciaires.

(5) Les SSG sont gérés, contrôlés et entretenus 24 heures sur 24 par une équipe de spécialistes en matière de sécurité de l'information. Ils protègent les données, réduisent les risques de sécurité auxquels le réseau est exposé et s'adaptent rapidement à l'évolution des besoins en matière de sécurité.

3 ARCHITECTURE DE DÉPLOIEMENT DES SSG

(6) L'architecture de déploiement des SSG est formée de solutions centralisées et distribuées, comme l'illustre la figure 1. Située dans le centre de données de l'entrepreneur, la solution centralisée offre au ministère client abonné les services d'antivirus et d'antipourriel en recourant aux politiques ministérielles en la matière. Cette solution est basée sur les appareils Cisco IronPort Email Security Appliances. La solution distribuée est située dans les zones d'accès public des ministères, à l'intérieur de leur centre de données. Elle s'appuie sur les serveurs Fortinet Fortigate et Cisco ASA UTM pour offrir les services de pare-feu et de détection des intrusions, et sur la solution de filtrage Web WebSense pour assurer le filtrage de contenu.

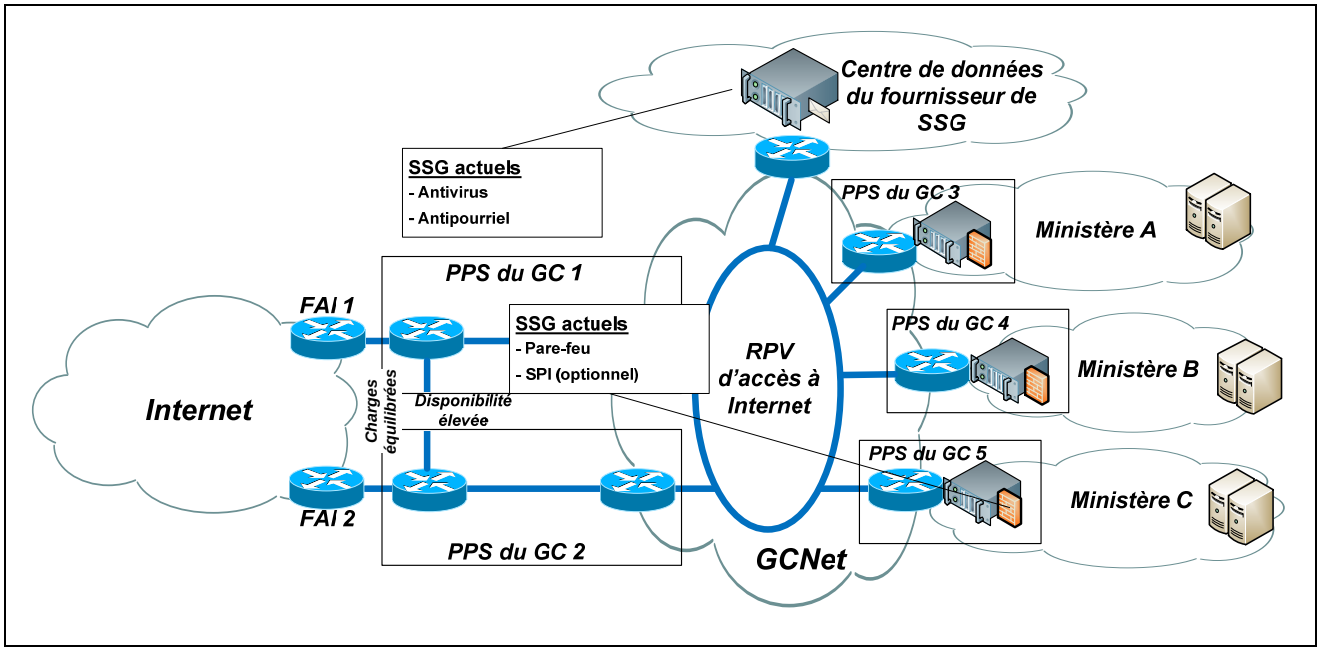

Figure 1 – Architecture de déploiement de SSG

4 SSG DÉPLOYÉS

(7) Le tableau 1 ci-dessous dresse la liste des équipements qui avaient été déployés en avril 2012 pour offrir les SSG aux organisations clients abonnées. Il ne comprend pas les équipements d'infrastructure comme les commutateurs de regroupement; seuls les équipements permettant de livrer directement les SSG y figurent. Tous les PPS sont situés à Ottawa, et chacun d'entre eux représente une organisation cliente différente; le PPS de l'entrepreneur fait exception, car il s'occupe de multiples clients.

PPS à Ottawa	Qtée	Service	Type de dispositif	Fabricant	Nom du produit	Modèle/Version du produit	Description
PPS1	1	GIM/GUM	Appareil	Fortinet	Fortigate	FG-110C-BDL-950-DD	FG-110c-FW, FG-110c-DDoS, FG-110c-IDP, FG-110c-WF
PPS2	1	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco 4240 IPS Sensor
	1	SDI (SRDI/SRPI)	Appareil	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	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Copper Tap
PPS3	2	Pare-feu	Appareil	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PROD Primary + Secondary FW
	1	Pare-feu	Appareil	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PRE-PROD FW
	1	Pare-feu	Serveur	IBM	xSeries System x	x3350	IBM SYSTEM X3350 Syslog Server
	3	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	11	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 Pre-Prod REZ
PPS4	1	SDI (SRDI/SRPI)	Appareil	Cisco Systems	Catalyst	WS-C2950T-24	IDS Aggregation Switch WS-C2950T-24
	1	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9
	2	GIM/GUM	Appareil	Fortinet	Fortigate	FG-200B	FG-200b-FW, FG-200b-WF, FG-200b-IDP Primary + Secondary
PPS5	1	IDS (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	3	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 OZ
PPS6	2	Pare-feu	Appareil	Cisco Systems	ASA	5550	Cisco ASA5550-BUN-K9 Firewall
	2	Pare-feu	Serveur	IBM	xSeries System x	x3350	IBM SYSTEM X3350 Model 4192-B2U Syslog Server
	2	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4255-K9	Cisco IPS-4255-K9 Network Sensor
	8	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 VPN-OZ
	3	Filtrage de contenu Web	Serveur	IBM	xSeries_System x	x3550	IBM SYSTEM X3550 Model 7946-AC1 794692U Websense Log and Reporting Server
PPS7	1	SDI	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS 4240

PPS à Ottawa	Qtée	Service	Type de dispositif	Fabricant	Nom du produit	Modèle/Version du produit	Description
		(SRDI/SRPI)					
	3	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics TP-CU3 10/100/1000 for MSS.NCC
PPS8	2	Pare-feu	Appareil	Cisco Systems	ASA	5550	Cisco ASA5550-BUN-K9 PROD Primary + Secondary FW
	1	Pare-feu	Serveur	IBM	xSeries System x	x3550	IBM SYSTEM X3550 M2 794652U Syslog Server
	8	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT ByPass	BP-HBCU3	NetOptics 10/100/1000 Bypass Switch with Heartbeat
	4	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
PPS9	2	Pare-feu	Appareil	Cisco Systems	ASA	5520	Cisco ASA5520-BUN-K9 PROD Primary + Secondary FW
	1	Pare-feu	Serveur	IBM	xSeries System x	x3250	IBM SYSTEM x3250 M3 4251C2U Syslog Server
PPS10	1	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	7	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 OZ P
PPS11	1	Pare-feu	Appareil	Cisco Systems	PIX 500 Series Security Appliances	515E	Cisco PIX 515e
	1	Pare-feu	Appareil	Cisco Systems	ASA	5505	Cisco ASA5505-BUN-K9
	1	Pare-feu	Serveur	SYSTEM (GENERIC)	Other UNIX Server		Syslog Server
	1	Pare-feu	Serveur	IBM	xSeries System x	x3250	IBM SYSTEM x3250 M3 4251C2U Syslog Server
	2	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4240-K9	Cisco IPS-4240-K9 Network Sensor
	9	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3
PPS12	1	SDI (SRDI/SRPI)	Appareil	Cisco Systems	IPS	IPS-4255-K9	Cisco IPS-4255-K9 Network Sensor
	7	SDI (SRDI/SRPI)	Appareil	Net Optics	10/100/1000BaseT	TP-CU3	NetOptics 10/100/1000 Ethernet Tap P/N TP-CU3 Prod OZ1
Entrepreneur	4	Passerelle antipourriel/ antivirus	Appareil	IronPort	E-mail Security Appliance	X1060-R-NA	Appareil IronPort centralisé pour services d'antipourriel et d'antivirus Prend en charge un nombre total actuel de 78 839 utilisateurs répartis dans 25 ministères clients
	2	Passerelle antipourriel/ antivirus	Appareil	IronPort	E-mail Security Appliance	C650	
	1	Passerelle antipourriel/ antivirus	Appareil	IronPort	E-mail Security Appliance	X1070	

Table 1 – Emplacement et inventaire des équipements des SSG

5 STATISTIQUES OPÉRATIONNELLES

(8) De mai 2011 à avril 2012, l'entrepreneur offrant les SSG a traité environ :

a) 204 demandes de changement;

b) 512 billets d’incident.