Service de sécurité géré du gouvernement du Canada (SSGGC)

Document joint 2.2 : Modèle de service

Date : 8 juin 2012

TABLE DES MATIÈRES

INDEX DES FIGURES

1 AVANT-PROPOS

(1) Le modèle de service qui suit est fourni à titre d'information seulement et ne doit pas être interprété comme étant un engagement de la part du gouvernement du Canada (GC) de privilégier un quelconque modèle de déploiement, ou de s'y limiter.

2 MODÈLE THÉORIQUE

(2) Le modèle théorique du SSGGC, illustré dans la figure 1, propose une distribution des services de gestion des menaces qui est quelque peu semblable à celle adoptée par les services de sécurité gérés actuels. Les services de gestion des menaces sont répartis dans deux catégories :

a) Les services hébergés centralement – sur des appareils partagés ou communs, à disponibilité élevée, situés à un point de contrôle Internet dont le Canada est propriétaire;

b) Les services distribués – sur des appareils dédiés, standard ou à disponibilité élevée, situés dans les locaux de l'organisation cliente.

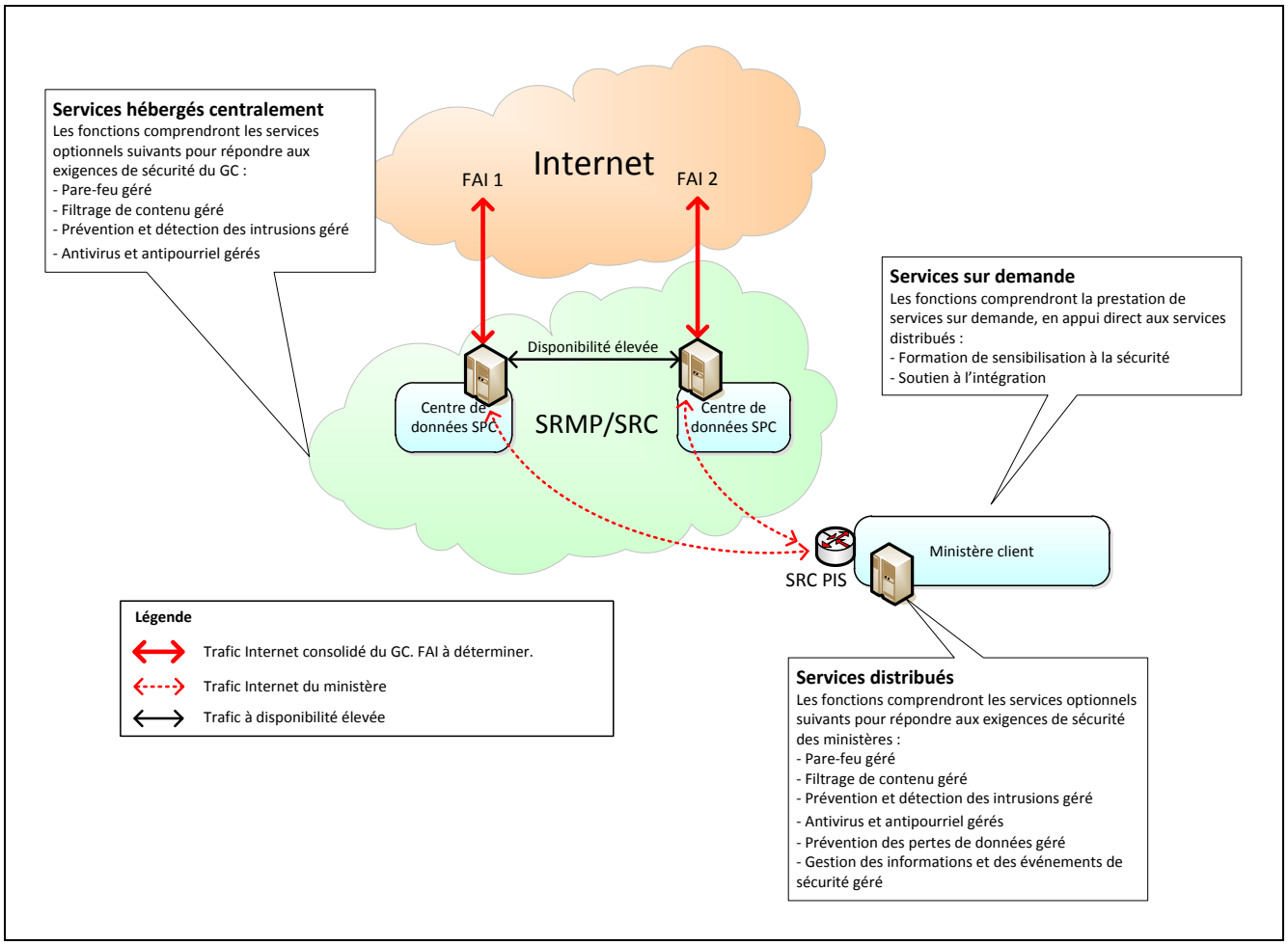

Figure 1 – Modèle théorique du SSGGC

(3) Afin de faciliter la transition, tous les services de gestion des menaces doivent être en mesure de fonctionner les uns avec les autres, ainsi qu'avec les services de sécurité préexistants que possède l'organisation cliente et (ou) Services partagés Canada.

(4) Chaque PPS centralisé doit avoir une capacité suffisante pour traiter tout le trafic Internet au cas où il y aurait perte d'un FAI (c'est-à-dire qu'il doit prendre en charge l'architecture d'accès Internet à disponibilité élevée).

3 SCÉNARIOS DE DÉPLOIEMENT POSSIBLES

(5) Le déploiement réel du SSGGC pourrait être réalisé en appliquant de multiples scénarios de déploiement. Le Canada a identifié trois scénarios qui pourraient permettre la mise en œuvre du SSGGC tout en reconnaissant que l'approche distribuée conviendrait mieux à certaines organisations clientes, alors que l'approche centralisée serait mieux adaptée pour d'autres.

(6) Les principaux éléments du modèle de déploiement distribué comprennent ce qui suit:

a) La politique de sécurité du GC relative au trafic Internet entrant est appliquée au PPS centralisé tandis que la politique de sécurité du ministère l'est au PPS d'une organisation cliente.

b) Chaque organisation cliente doit déployer le SSGGC dans un PPS qui lui est propre.

c) Chaque PPS centralisé doit avoir une capacité suffisante pour traiter tout le trafic Internet au cas où il y aurait perte d'un FAI (c'est-à-dire qu'il doit prendre en charge l'architecture d'accès Internet à disponibilité élevée).

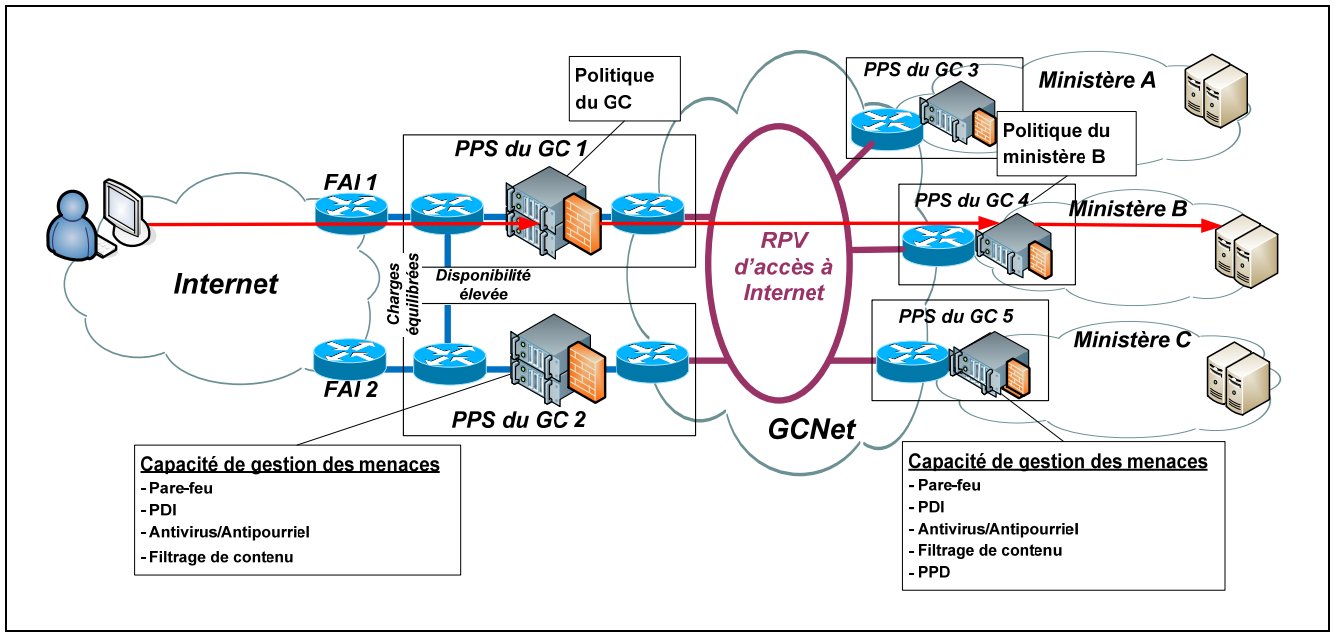

Figure 2 – Modèle de déploiement distribué du SSGGC

(7) La figure 2 illustre l'application de la politique de sécurité du GC au PPS centralisé pour le trafic entrant, puis l'application de la politique de sécurité du ministère au PPS d'une organisation cliente (c.-à-d. ministère B).

(8) Les principaux éléments de l'approche centralisée comprennent ce qui suit :

a) La politique du GC et celles de l'organisation cliente sont appliquées à une capacité de gestion des menaces située à un PPS centralisé.

b) Les possibilités de virtualisation ou de partage de la capacité de gestion des menaces située au PPS centralisé font en sorte que les appareils de gestion unifiée des menaces puissent être partagés et ainsi contribuer à réduire les besoins en électricité et en espace au PPS en question.

c) Chaque PPS centralisé doit avoir une capacité suffisante pour traiter tout le trafic Internet au cas où il y aurait perte d'un FAI (c'est-à-dire qu'il doit prendre en charge l'architecture d'accès Internet à disponibilité élevée).

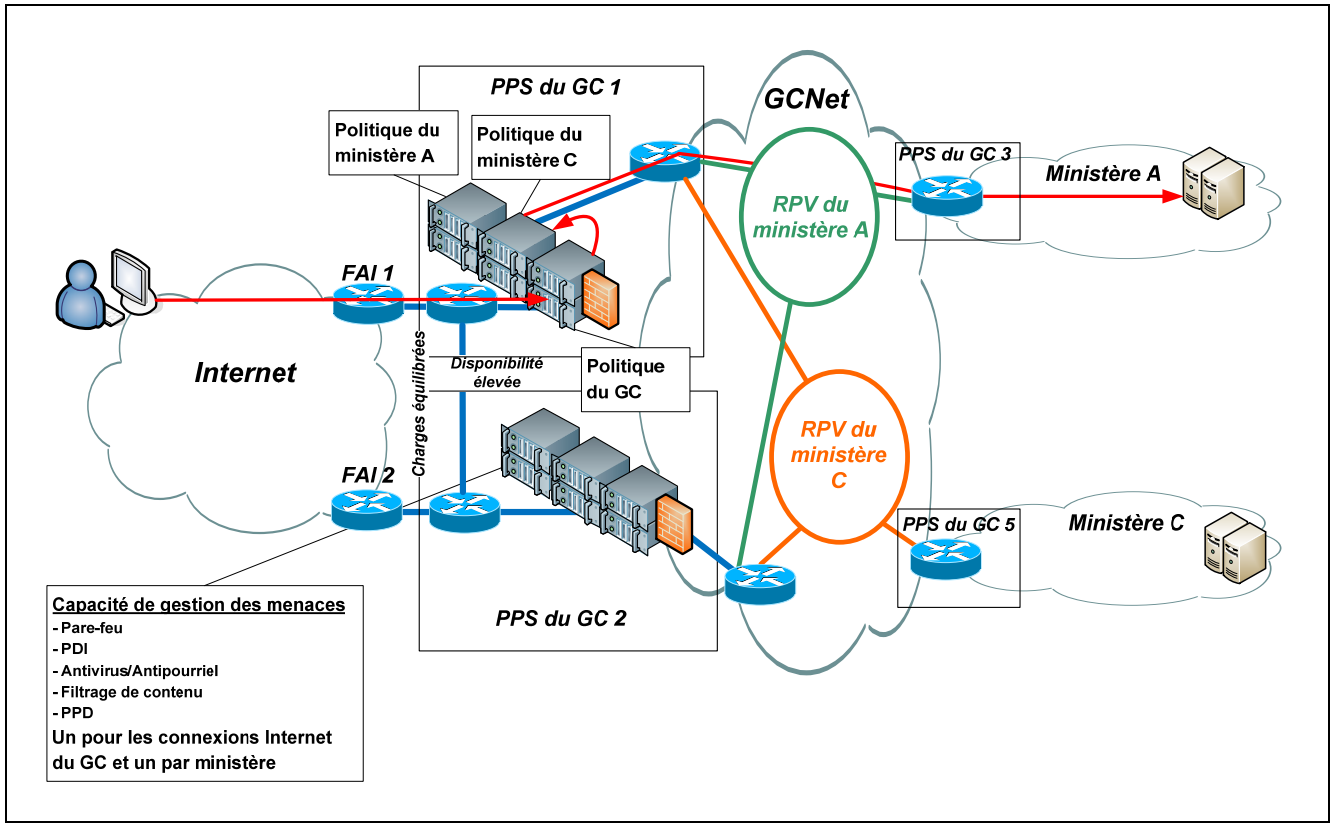

Figure 3 – Modèle de déploiement centralisé du SSGGC

(9) La figure 3 illustre les étapes de l'application de la politique de sécurité (c.-à-d. la politique du GC d'abord, puis celle de la politique propre à l'organisation cliente) pour un flux type de données entrantes depuis Internet.

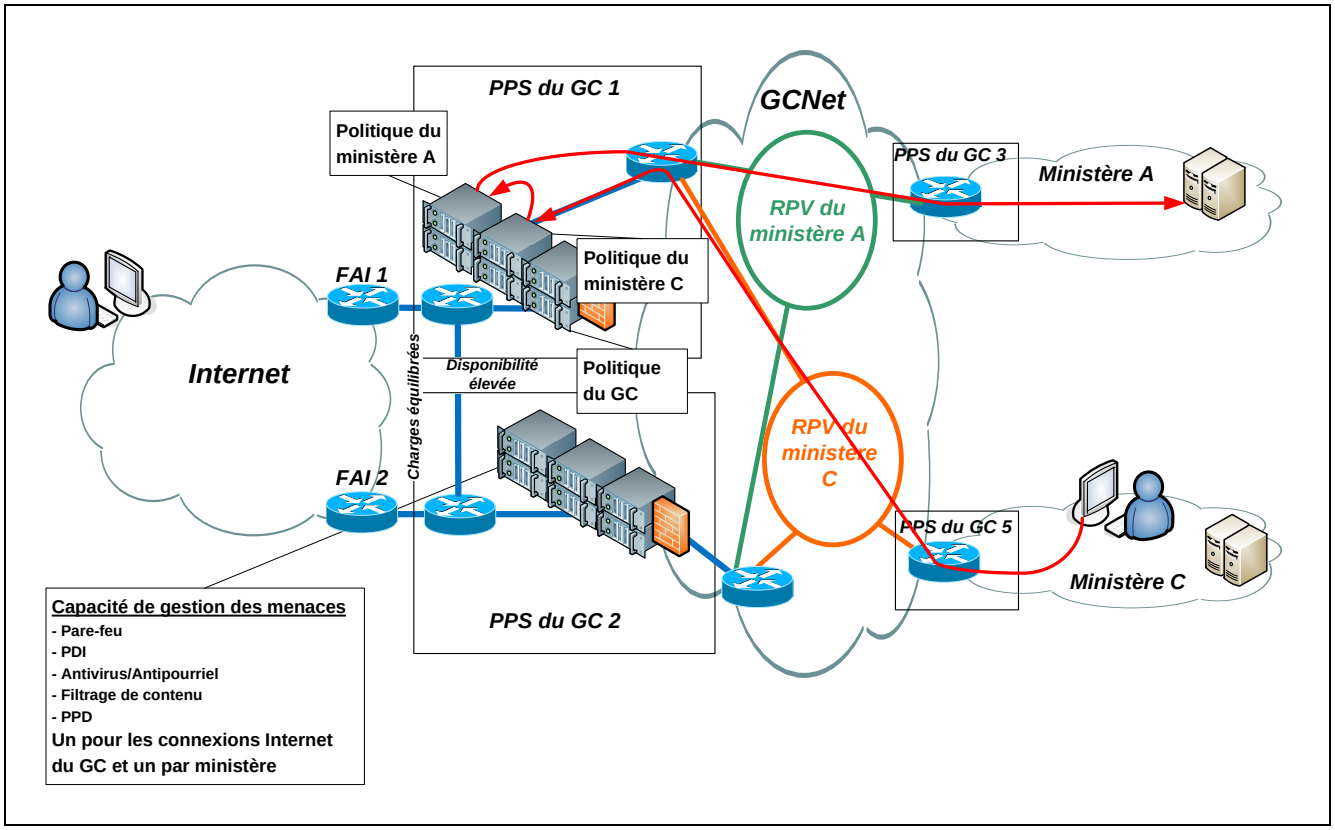

Figure 4 - Modèle de déploiement centralisé du SSGGC

(10) La figure 4 illustre l'application de la politique de sécurité de l'organisation cliente lorsqu'il y a communications entre deux organisations clientes (c.-à-d. trafic entre ministères plutôt que trafic Internet entrant).

(11) Les principaux éléments du modèle de déploiement mixte comprennent ce qui suit :

a) La politique du GC et certaines politiques de l'organisation cliente sont appliquées à une capacité de gestion des menaces située à un PPS centralisé.

b) Certaines politiques de l'organisation cliente sont appliquées à une capacité de gestion des menaces située à un PPS de l'organisation cliente.

c) Les possibilités de virtualisation ou de partage de la capacité de gestion des menaces située au PPS centralisé font en sorte que les appareils de gestion unifiée des menaces puissent être partagés et ainsi contribuer à réduire les besoins en électricité et en espace au PPS en question.

d) Chaque PPS centralisé doit avoir une capacité suffisante pour traiter tout le trafic Internet au cas où il y aurait perte d'un FAI (c'est-à-dire qu'il doit prendre en charge l'architecture d'accès Internet à disponibilité élevée).

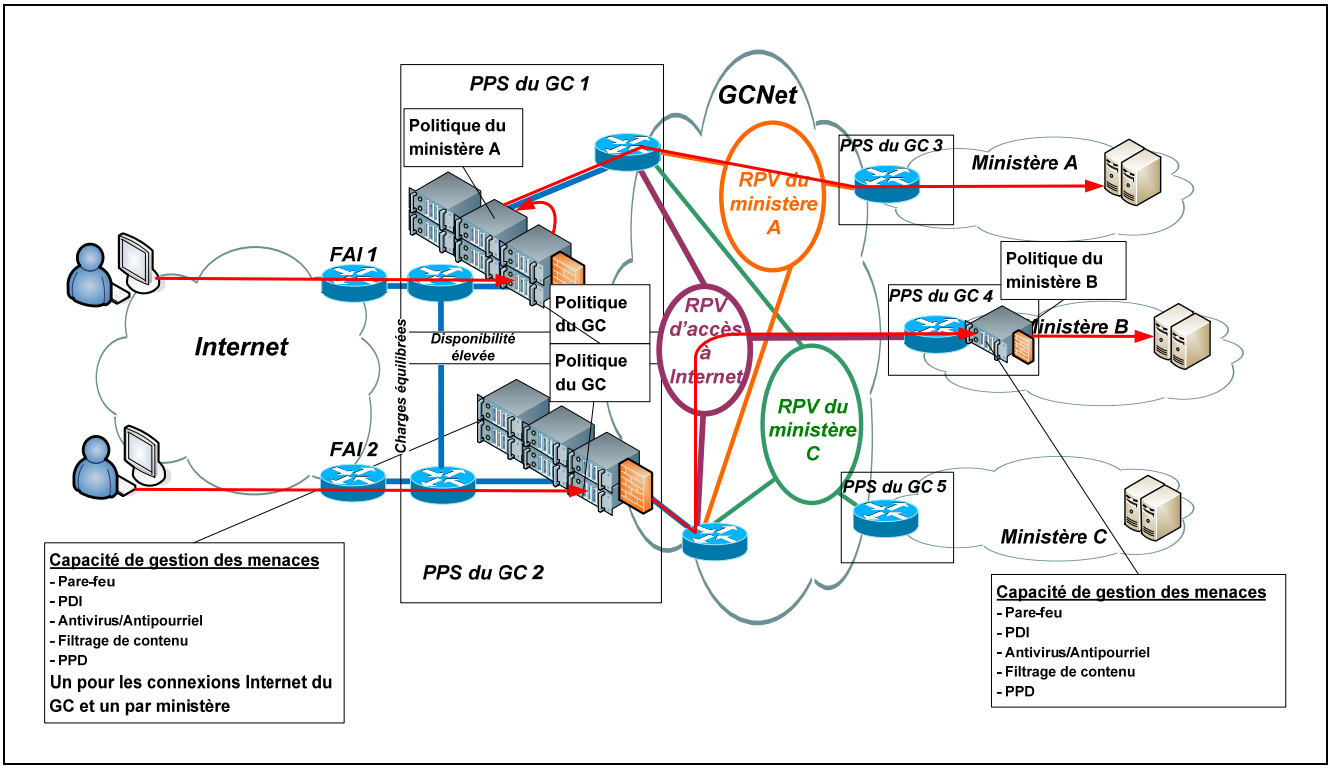

Figure 5 – Modèle de déploiement mixte du SSGGC

(12) La figure 5 illustre l'application de la politique de sécurité du GC, puis l'application de la politique de sécurité de l'organisation cliente, pour le trafic entrant, lorsqu'une politique de sécurité de l'organisation cliente est appliquée au PPS centralisé (c.-à-d. ministère A) et une autre politique de sécurité de l'organisation cliente est appliquée au PPS d'une organisation cliente (c.-à-d. ministère B).

4 MODÈLE DE CAPACITÉ ET D'ÉTABLISSEMENT DES PRIX

(13) La présente section porte uniquement sur les services de gestion des menaces et de GIES.

4.1 Modèle de capacité

(14) Le modèle de capacité du SSGGC repose sur une capacité d'hébergement, désignée « capacité de gestion des menaces », capable de maintenir une vitesse filaire donnée, peu importe le nombre de services de gestion des menaces en fonctionnement.

(15) Les services de sécurité particuliers, désignés « services de gestion des menaces » sont censés traiter les configurations de multiples clients, lorsque la politique de sécurité de l'organisation cliente A diffère de celle de l'organisation cliente B.

(16) La capacité de gestion des menaces est située dans un PPS qui est en fait un centre de données ou un local technique situé dans un immeuble.

(17) La figure 6 illustre le modèle de capacité décrit dans la présente section.

(18) Les mêmes caractéristiques s'appliquent dans le cas de la capacité de GIES, à l'exception que cette capacité est dédiée à un seul client et que la performance est mesurée en TPS.

(19) La capacité de gestion des menaces et la capacité de GIES peuvent regrouper toutes les composantes matérielles et logicielles nécessaires pour la livraison du service visé.

(20) Dans le cas où deux zones de sécurité de réseau différentes auraient besoin d'être protégées, deux capacités de gestion des menaces, accompagnées des services de gestion des menaces nécessaires, seraient achetées.

(21) Dans le cas où un dispositif de basculement serait nécessaire, deux capacités de gestion des menaces seraient achetées pour deux PPS différents, et l'entrepreneur aurait la tâche de les configurer pour qu'elles prennent en charge le basculement automatique.

4.2 Modèle d'établissement des prix

(22) Le premier aspect dont tient compte le modèle d'établissement des prix est la gestion des capacités de gestion des menaces et de GIES pouvant être situées dans plusieurs PPS. Ainsi, le soumissionnaire peut facturer des frais mensuels à l'égard de chaque PPS où est mis en œuvre le SSGGC, peu importe le nombre de capacités de gestion des menaces ou de GIES installées à un PPS donné. Ces frais mensuels sont indiqués dans le tableau de prix A et ils peuvent différer en fonction de l'emplacement du PPS et du NS-DMRS obligatoire rattaché au PPS en question.

(23) Le deuxième aspect a trait aux frais uniques facturés pour la mise en œuvre et la maintenance d'une capacité ou d'un service de gestion des menaces ou d'une capacité de GIES. Le NS-TIMS lié au service de gestion des menaces doit correspondre à celui associé à la capacité de gestion des menaces qui l'héberge. Le modèle d'établissement des prix autorise le soumissionnaire à facturer des frais uniques pour la mise en œuvre des éléments suivants :

a) Une capacité de gestion des menaces dans un PPS (tableau de prix B);

b) Une capacité de GIES dans un PPS (tableau de prix C);

c) Un service de gestion des menaces de l'organisation cliente hébergé sur une capacité de gestion des menaces (tableau de prix D).

(24) La figure 6 illustre le niveau auquel les tableaux de prix sont déterminés dans le modèle de capacité.

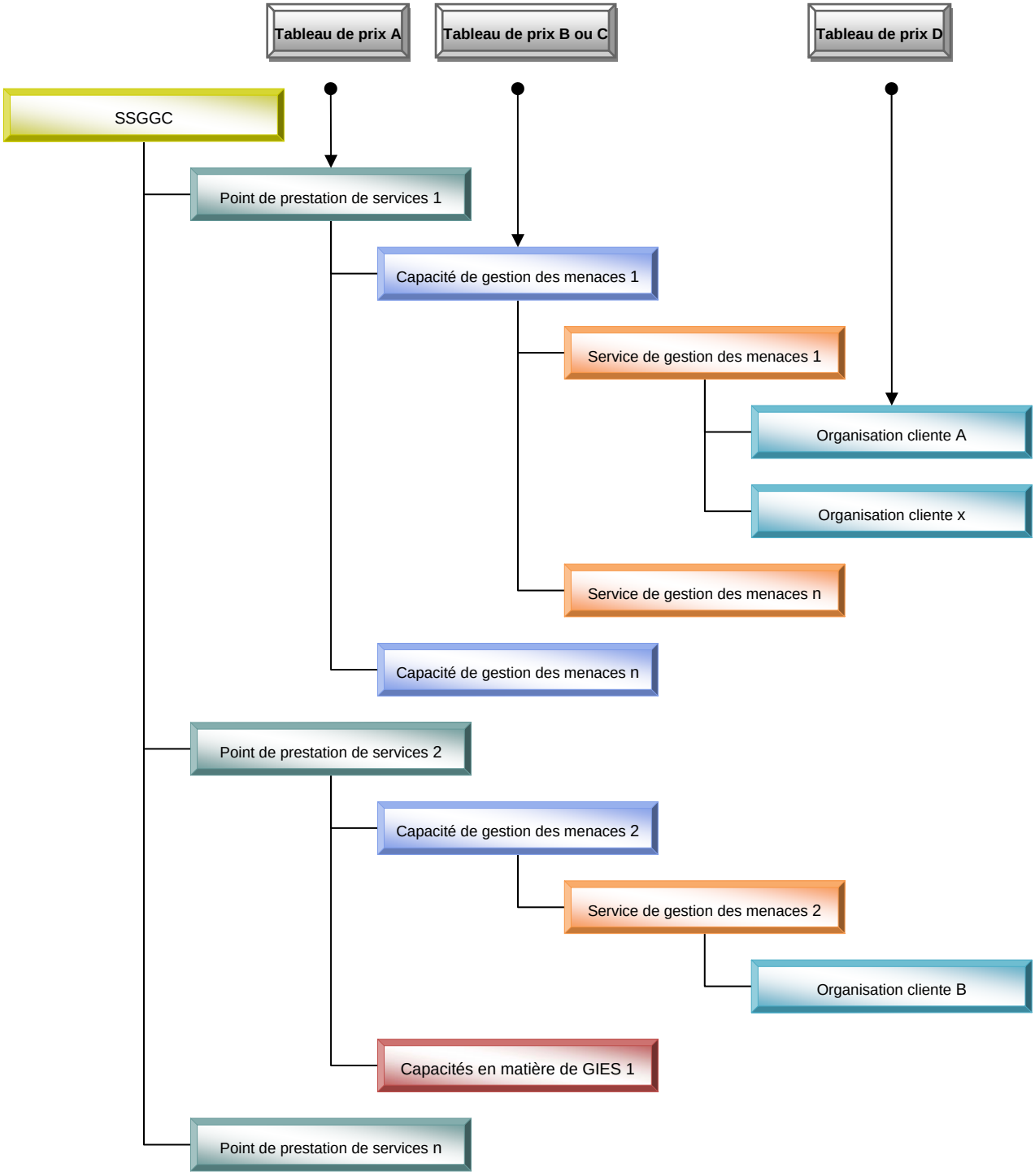

Figure 6 - Modèle de capacité et d'établissement des prix du SSGGC