Government of Canada Managed Security Service (GCMSS)

Attachment 2.2: Service Model

Date: June 8, 2012

TABLE OF CONTENTS

INDEX OF FIGURES

1 FOREWORD

(1) The following service model is provided for information purposes only and should not be construed as a commitment from the Government of Canada (GC) to favour, or to limit itself to, any of the deployment models.

2 CONCEPTUAL MODEL

(2) The conceptual model of the GCMSS shown in Figure 1 proposes a distribution of the Threat Management Services that is somewhat similar to the existing MSS. The Threat Management Services are represented into two categories:

a) Centrally hosted services - on shared or common high-availability appliances at a Canada-owned Internet control point; and

b) Distributed services - on dedicated standard or high-availability appliances located on Client Organization premises.

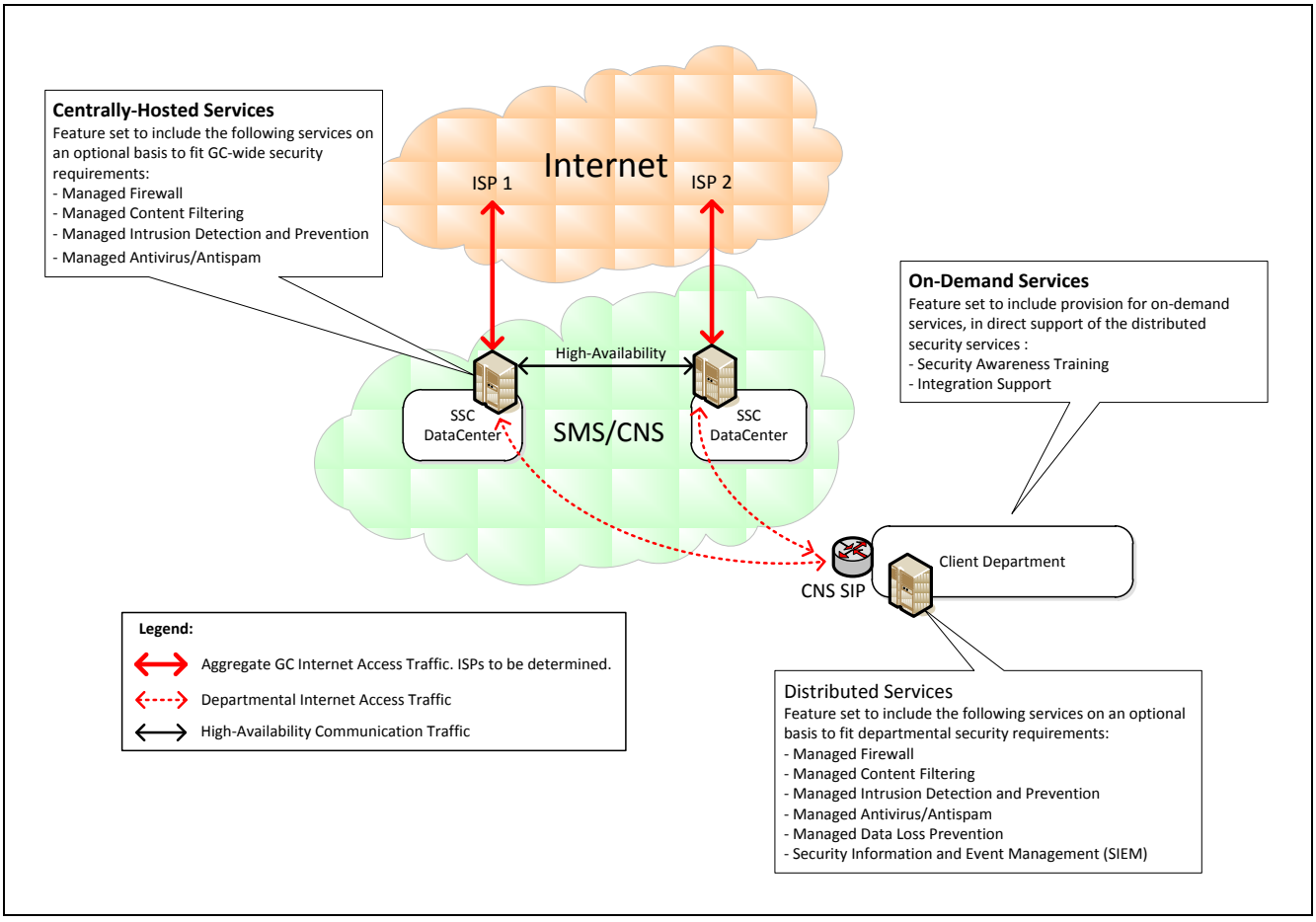


Figure 1 - GCMSS Conceptual Model

(3) All Threat Management Services must be able to work in conjunction with each other as well as pre-existing Client Organization owned and/or Shared Services Canada-owned security services to facilitate transition.

(4) Capacity at each centralized SDP must be sufficient to handle all Internet traffic in the event of the loss of an ISP (i.e. must support the Internet access high availability architecture);

3 POTENTIAL DEPLOYMENT SCENARIOS

(5) The actual deployment of GCMSS could be accomplished using multiple deployment scenarios. Canada identified 3 potential deployment scenarios that could be viable for the implementation of GCMSS recognizing that some Client Organizations will be more suited to a distributed approach, while others will be better suited to a centralized approach.

(6) The key elements of the distributed deployment model include:

a) GC security policy for Internet inbound traffic is applied at the Central SDP while departmental security policy is applied at a Client Organization SDP.

b) Each Client Organization needs to deploy GCMSS in its own SDP.

c) Capacity at each centralized SDP must be sufficient to handle all Internet traffic in the event of the loss of an ISP (i.e. must support the Internet access high availability architecture).

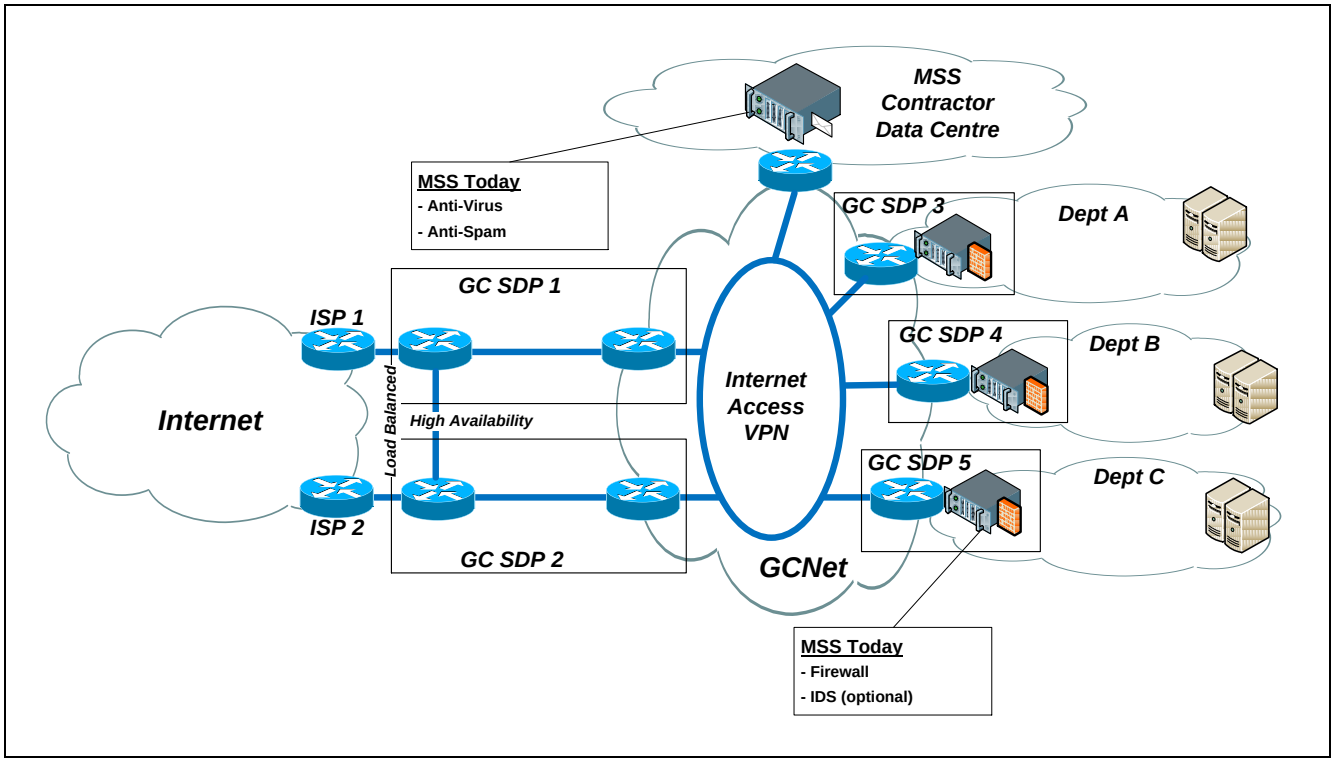


Figure 2 - GCMSS Distributed Deployment Model

(7) Figure 2 shows the application of GC security policy at the central SDP for inbound traffic, and then the application of departmental security policy at a Client Organization SDP (i.e. Department B).

(8) The key elements of the centralized approach include:

a) GC Policy and Client Organization policies applied at a Threat Management Capacity at a central SDP.

b) Possible virtualization or multi-tenant capability of the Threat Management Capacity at the central SDP such that UTM appliances can be shared thereby reducing power and space requirements at the central SDP.

c) Capacity at each centralized SDP must be sufficient to handle all Internet traffic in the event of the loss of an ISP (i.e. must support the Internet access high availability architecture).

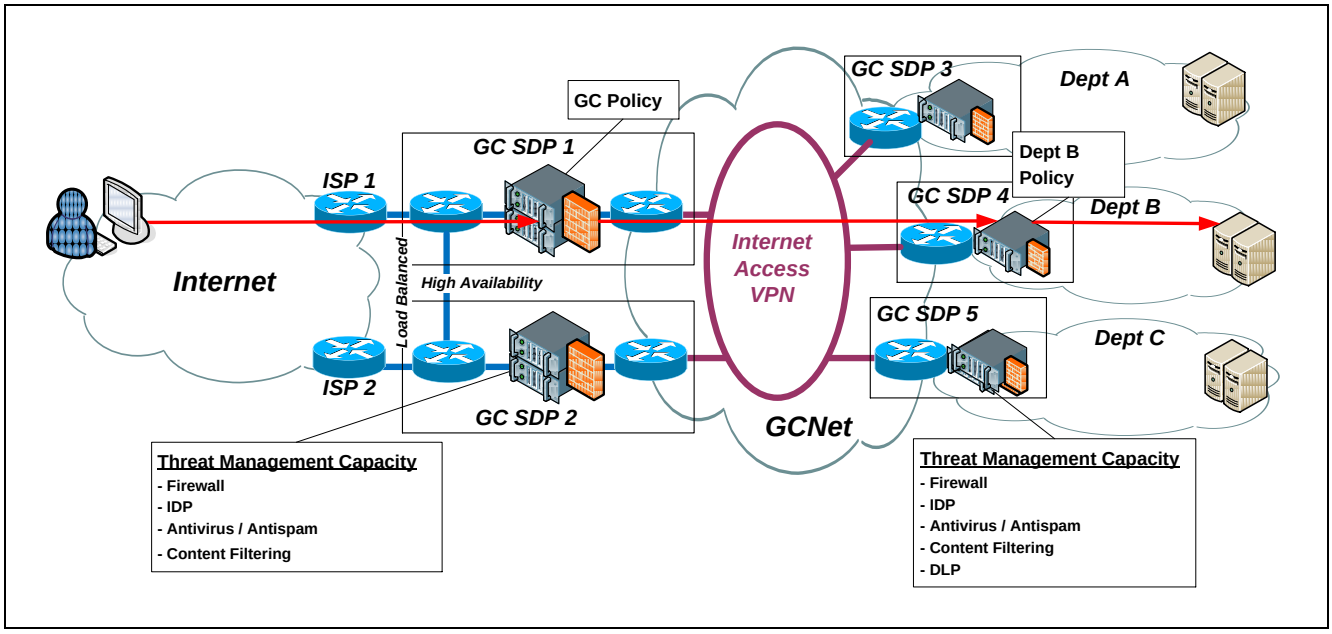


Figure 3 - GCMSS Centralized Deployment Model

(9) Figure 3 shows the stages in the application of security policy (i.e. first the GC policy and then the Client Organization specific policy) for a typical inbound data flow from the Internet.

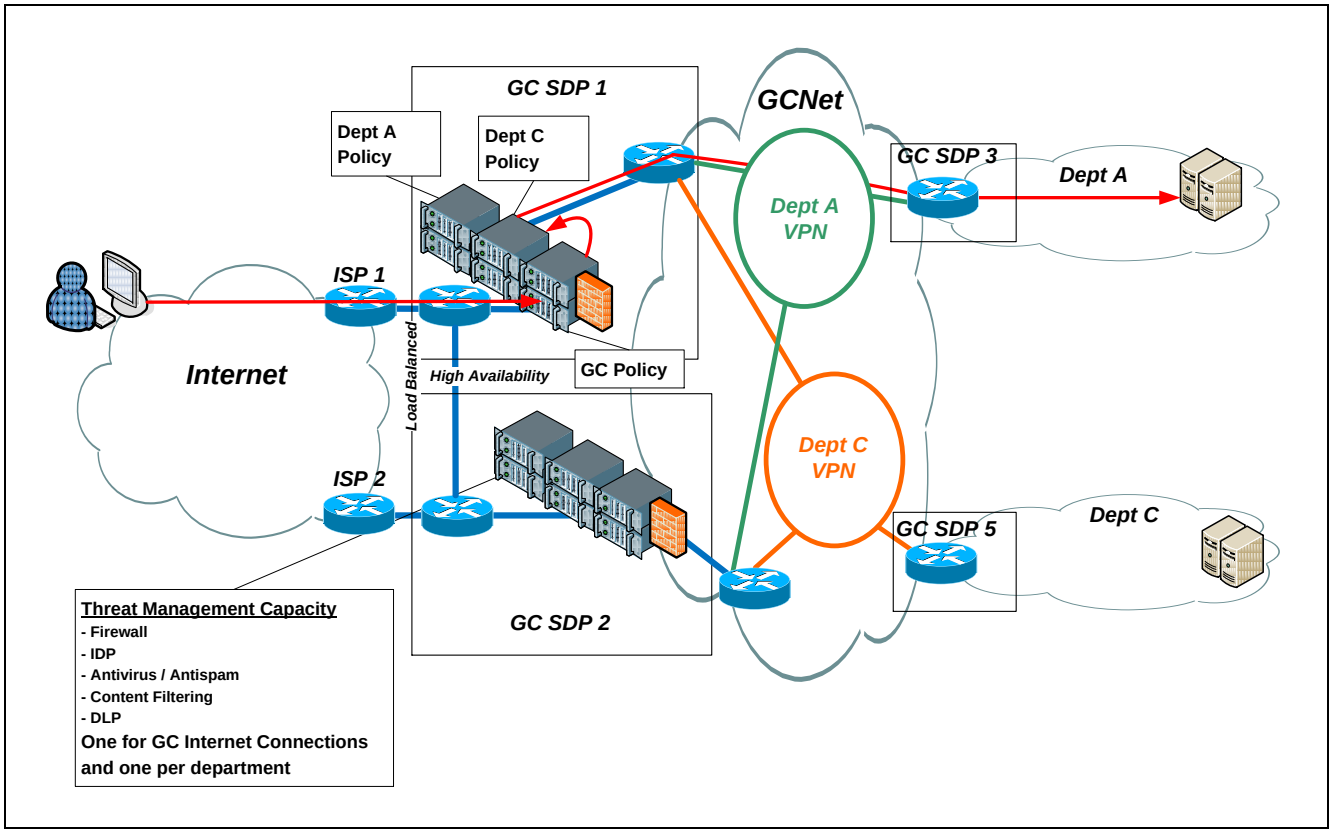


Figure 4 - GCMSS Centralized Deployment Model

(10) Figure 4 shows the application of Client Organization security policy for communications between two Client Organizations (i.e. interdepartmental rather than inbound Internet traffic).

(11) The key elements of the hybrid deployment model include:

a) GC Policy and some Client Organization policies applied at a Threat Management Capacity at a central SDP.

b) Some Client Organization policies applied at a Threat Management Capacity at a Client Organization SDP.

c) Possible virtualization or multi-tenant capability of the Threat Management Capacity at the central SDP such that UTM appliances can be shared thereby reducing power and space requirements at the central SDP.

d) Capacity at each centralized SDP must be sufficient to handle all Internet traffic in the event of the loss of an ISP (i.e. must support the Internet access high availability architecture).

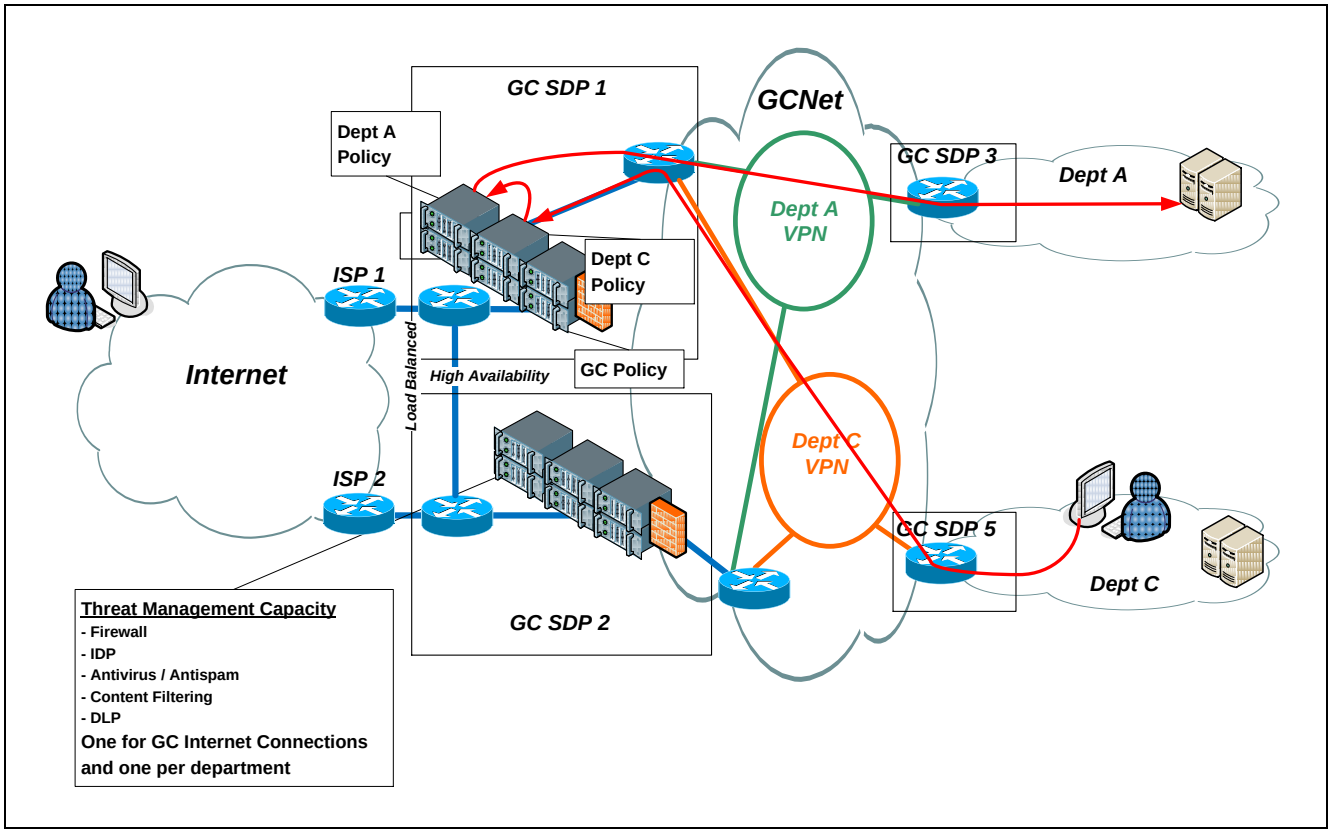
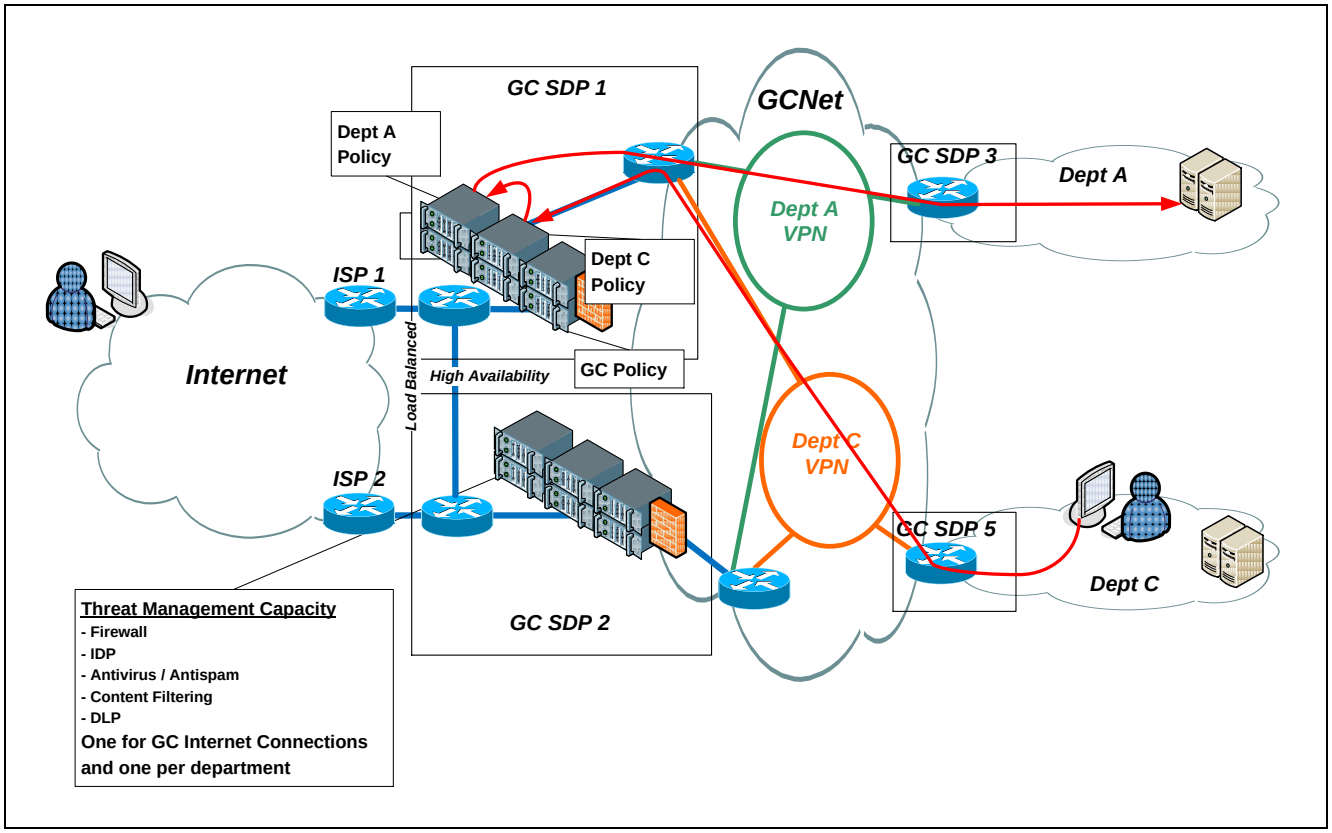


Figure 5 - GCMSS Hybrid Deployment Model



(12) Figure 5 shows the application of GC security policy and then Client Organization security policy for inbound traffic where a Client Organization security policy is applied at the central SDP (i.e. for Department A), and another Client Organization security policy is applied at a Client Organization SDP (i.e. for Department B).

4 CAPACITY AND PRICING MODEL

(13) This section focuses only on the threat management and SIEM services.

4.1 Capacity Model

(14) The GCMSS capacity model is based on a hosting capacity, named Threat Management Capacity, which is capable of sustaining a given wire speed with any number of Threat Management Services running on it.

(15) The specific security services, named Threat Management Services, are expected to handle multi-clients configuration where the security policy of Client Organization “A” is different from the security policy of Client Organization “B”.

(16) The Threat Management Capacity is located in a SDP which is a data centre or equipment room located in a building.

(17) Figure 6 provides a visual representation of the Capacity Model presented in this section.

(18) The same characteristics apply to the SIEM Capacity, excepted that the SIEM Capacity is dedicated to a single client and the measure of performance is the TPS.

(19) The Threat Management Capacity and the SIEM Capacity can be comprised of any combination of hardware and software required to deliver the target service.

(20) In a scenario where two different network security zones need to be protected, two Threat Management Capacities would be purchased along with the required Threat Management Services.

(21) In a scenario where failover is required, two Threat Management Capacities would be purchased for two different SDP and the Contractor would have to configure them to support automatic failover.

4.2 Pricing Model

(22) The first aspect of the pricing model is the management of the Threat Management Capacities and the SIEM Capacities that can be located in multiple SDP. The pricing model allows the bidder to charge a monthly price for each SDP where GCMSS is implemented regardless of the number of Threat Management Capacities or SIEM Capacities installed at that given SDP. This monthly price is covered by the Pricing Table A and it can be different based on the location of the SDP and the mandatory SL-MTRS associated to the SDP location.

(23) The second aspect of the pricing model is the one-time price to cover the implementation and the maintenance of a Threat Management Capacity, Threat Management Service and SIEM Capacity. The SL-MSOT of the Threat Management Service must match the SL-MSOT of the hosting Threat Management Capacity. The pricing model allows the bidder to charge a one-time price to implement:

a) a Threat Management Capacity in a SDP (Pricing Table B);

b) a SIEM Capacity in a SDP (Pricing Table C); and

c) a Client Organization's Threat Management Service on a Threat Management Capacity (Pricing Table D).

(24) Figure 6 provides a visual indication of where the individual pricing tables fit in the Capacity Model.

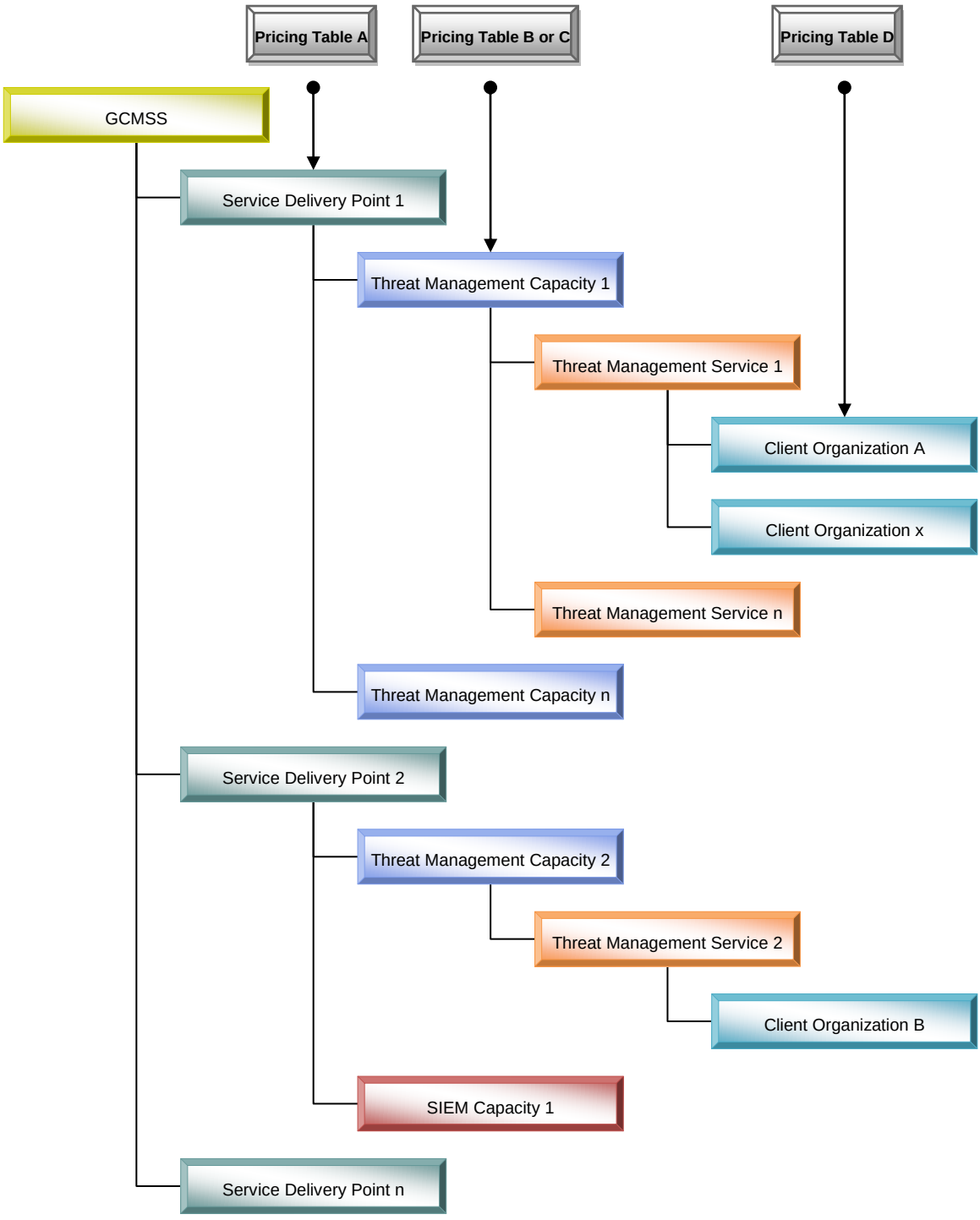


Figure 6 – GCMSS Capacity and Pricing Model