



Network Security Zoning Reference Architecture

Enterprise Architecture, CTO Branch

Status: **In Progress**

Document Version: **10**

Publish Date: TBD

Security Classification: **UNCLASSIFIED**



Shared Services
Canada

Services partagés
Canada

Canada

Document Approval

The signing authorities below concur with the conditions and responsibilities specified within this document.

Victor Ulitsky	Director General, Enterprise Architecture Chief Technology Officer Branch Shared Services Canada	_____ Date	_____ Signature
Mathieu Fortin	Director, Partner Enterprise Architecture Liaison Chief Technology Officer Branch Shared Services Canada	_____ Date	_____ Signature

Document History

This Reference Architecture Document (RAD) artifact is subject to formal architectural governance. Upon completion of the development of this artefact, clearly identify participants and committees that this document has been circulated to and have provided endorsement of the document.

Ver. #	Date	Consulted/ Reviewers (name of individual & working group consulted)	Brief description of Change	Author of Change
0.1	2019-03-31	See Appendix B.	Initial draft	Andrew Wykurz
0.2	2019-05-24	See Appendix B.	Updated Section 4 Architectural Patterns with enhanced descriptions and clearer models. Also removed document content instructions.	Andrew Wykurz
0.3	2019-06-18	See Appendix B.	Updated section 4, added missing security artefacts	Yacin Abdallah
0.4	2019-07-18	See Appendix B.	Updated Section 4, added GC Cloud To Ground And Internet	Yacin Abdallah
0.5	2020-07-15	See Appendix B.	Updated based on EA review	Yacin Abdallah
0.6	2020-07-27	See Appendix B.	Updated Section 4.6.5, changed CG-TIP connection to cloud. Also removed AWS from the section title as the model supports both AWS and Azure.	Yacin Abdallah
0.7	2020-08-19	Walter Sokyko	Incorporated feedback received at AC presentation (2020-07-27). Removed DRAFT watermark.	Claude Vallée
08	2020-09-03	See Appendix B.	Updated section 1.1.1 based on Security Management Group (SMG) recommendation	Yacin Abdallah
09	2020-09-22	SARB Recommendation	Updated based on SARB recommendation	Yacin Abdallah
10	2020-11-08	PRWG Recommendation	Updated based on PRWG recommendation	Yacin Abdallah

Table of Contents

1	Introduction	1
1.1	Authoritative Body	1
1.1.1	Roles & Responsibilities (RACI)	2
1.2	Purpose	2
1.3	Background	2
1.4	Scope	3
1.4.1	Exceptions.....	3
1.5	Vision, Goals and Objectives	4
1.5.1	Business and Motivation views.....	4
1.6	High-Level Operational Concept.....	5
1.6.1	Business Architecture	5
1.6.2	Business View	5
1.6.3	Government of Canada High Level Business Patterns.....	6
1.6.4	GC Departments Interoperability Pattern.....	7
1.6.5	Definitions.....	8
1.6.5.1	Public Zone (PZ)	8
1.6.5.2	Public Access Zone (PAZ).....	9
1.6.5.3	Operations Zone (OZ)	9
1.6.5.4	Restricted Zone (RZ)	9
1.6.5.5	Highly Restricted Zone (HRZ)	10
1.6.5.6	Restricted Extranet Zone (REZ).....	10
1.6.5.7	Management Restricted Zone (MRZ)	11
1.6.5.8	Special Access Zone (SAZ).....	11
1.7	Linkages to Other Architectures, Programs and Initiatives	11
2	High Level Guidance.....	13
2.1	Principles.....	13
2.2	Drivers	13
3	Standards & Policies	14
3.1	Standards	14
3.2	Policies.....	14
4	Architecture Patterns.....	15
4.1	Departmental B2B Zones Interaction View	15
4.2	Security Zone Concepts.....	15
4.2.1	Zone Interface Points (ZIPs) and Their Security Functions.....	15

4.2.2 Operations Zone and ZIP 16

4.2.3 Public Access Zone and ZIP 17

4.2.4 Internet Application Restricted Zone and ZIP 18

4.2.5 Restricted Zone and RZ ZIP 19

4.2.6 Data RZ and ZIP 19

4.2.7 Management RZ and ZIP 20

4.3 High Level Network Zoning 21

4.4 Management Restricted Zones 23

4.5 Application, Information and Data Views 24

 4.5.1 Application Views 24

4.6 Cloud Zoning Scenarios 25

 4.6.1 SSC EDC & Cloud Service Integration 25

 4.6.2 Department Cloud Hybrid Zoning View 26

 4.6.3 Department Shift to Full Cloud Hosting 28

 4.6.4 Cloud Zones 28

 4.6.5 GC Cloud To Ground And Internet 30

4.7 Internet of Things 31

4.8 OGD-PGA Interoperability 32

5 Glossary of Terms & Acronyms 34

 5.1 Glossary of Terms 34

 5.2 Acronyms 34

6 References 36

Appendix A. ArchiMate® Notation 38

Appendix B. Contributors and Reviewers 41

List of Figures

Figure 1. Network Zoning Motivation Model	4
Figure 2. GC Service Delivery Context	5
Figure 3. SSC Business View	6
Figure 4. Department B2B View	7
Figure 5. GC Departments Interoperability Pattern	7
Figure 6. Current State Network Security Zone Implementation Model	8
Figure 7. Department B2B Zones Interaction View	15
Figure 8. ZIPs & Security Functions	16
Figure 9. Operations Zone & ZIP Services View	17
Figure 10. PAZ & PAZ ZIP Services View	18
Figure 11. Internet Application Restricted Zone & ZIP Services View	18
Figure 12. Restricted Zone & RZ ZIP Services View	19
Figure 13. Data RZ & ZIP Services View	20
Figure 14. Management RZ & ZIP Services View	21
Figure 15. EDC to SaaS Cloud	22
Figure 16. Virtual Data Center (VDC) to SaaS Cloud	23
Figure 17. GC Network Zones	24
Figure 18. Application Objects Network Zoning Dependency	25
Figure 19. Cloud Hosted Services Integration View	26
Figure 20. Department Cloud Hybrid Zoning View	27
Figure 21. Full Cloud Hosting View	28
Figure 22. Cloud Network Zones	29
Figure 23. GC Cloud to Ground and Internet for AWS	30
Figure 24. Internet of Things	32
Figure 25. OGD-PGA Interoperability View	33
Figure 26. Top Level Concepts of ArchiMate®	38
Figure 27. ArchiMate® Core Concepts	39
Figure 28. ArchiMate® Extensions	39
Figure 29. ArchiMate® Relationships	40

List of Tables

Table 1. Roles & Responsibilities (RACI)	2
Table 2. Reviewed and Endorsed By	41

1 Introduction

A Reference Architecture (RAs) is a description that provides a blueprint or template description of the solution to a problem. Reference Architectures assist in the management of complexity and are essential tools for SSC and its partners to direct, guide and constrain Solution Architectures (SAs) by providing common information, guidance, standards and direction that enables the development of effective and efficient solutions. To be most effective, RAs need to be developed based on sound architectural principles and meet common standards in terms of form and content. This Reference Architecture Document (RAD) is the first step in establishing this process for creating consistent and complete RAs.

An RA is an existing proven architecture template that represents the IT current state as defined by current architecture for a subject area. In this document the ITSG-22 security guidance is the current state reference. It will assist in reducing the time and effort required for the design and development of solutions.

The ArchiMate enterprise architecture modeling language is used throughout this document to illustrate concepts and examples. ArchiMate is a technical standard from The Open Group and is based on the concepts of the IEEE 1471 standard. It is supported by various tool vendors and consulting firms. A brief introduction to the ArchiMate modelling notation is provided in Appendix A with additional information regarding the ArchiMate Specification available at the [Open Group website](https://www.opengroup.org/archimate-forum/archimate-overview)¹.

1.1 Authoritative Body

This document contains contributions from, and was reviewed by many subject matter experts, including the principle SME's listed in Appendix B.

Please direct any enquiries about this document to your department's assigned liaison with Shared Services Canada. Exact point of contact To Be Determined.

¹ <https://www.opengroup.org/archimate-forum/archimate-overview>.

1.1.1 Roles & Responsibilities (RACI)

In this section we are identifying roles and responsibility RACI matrix (Accountable, Responsible, Contributor/ Consultant, Informed)

Network Zoning Reference Architecture Process	SSC	TBS Cyber	CSE/CCCS	Partners
Designing/Implementing Service	A/R	C	C	I
Advice And Guidance	A/R	R	R	I
Compliance (i.e. GC EARB, ITSG-22)	R	A	R	R
Maintenance (updates)	A/R	C	C	C

Table 1. Roles & Responsibilities (RACI)

Responsible: Have the obligation to complete a process

Accountable: Decision-making authority expected to ensure the successful completion of a process

Consulted: Consulted for details and additional info on a process

Informed: Made aware of the status of the conditions

Design: The primary focus of designers/engineers is the overall technical design and engineering of specific elements of service, project and enterprise architectures. They provides subject matter expertise to the Service Architect and Solution Architect to produce a technical specification for development and systems integration requirements.

Maintenance: Ensuring the requirements of this network zoning reference architecture is in alignment with ITSG-22 whenever a change occurs.

1.2 Purpose

The purpose of this reference architecture document (RAD) is to describe network zoning so that departments and agencies in the Government of Canada (GC) can use network zoning to enhance their security posture.

1.3 Background

In the context of service excellence, innovation and value for money, Shared Services Canada (SSC) is mandated to maintain and improve the delivery of IT infrastructure services while simultaneously renewing the Government of Canada's IT infrastructure.

SSC is bringing a true enterprise perspective to GC IT infrastructure, not just to improve service but also to eliminate duplication and cut costs. An important aspect of that work is the development of enterprise-wide service standards, formerly established and maintained by each of the 43 partner organizations for their own environment, and now being collaboratively developed for the Government of Canada.

In collaboration with its partners, and through the counsel provided by industry, SSC is identifying the IT infrastructure requirements of the government as an enterprise and applying best practices to address its operational challenges and meet the government's modernization targets. Building a more secure and robust foundation for modern government operations is also strengthening our ability to protect the information of Canadians.

Zoning is part of GC security guidelines but generally not followed for various reasons. Given the rise of EDC and Cloud, it is an opportunity and necessary to implement the requirement.

1.4 Scope

This reference architecture applies to the consolidated GC IT domain operated by Shared Services Canada (SSC) for hosting SSC, SSC Partners and SSC clients in the Protected domain. The Protected domain is limited to confidentialities of Protected B and lower (medium and lessor non-national injury).

This document defines the zones and high-level communication flows which are permitted between zones. It is to be used in conjunction with a more detailed companion document which defines security requirements within the defined security zones.

1.4.1 Exceptions

Legacy SSC services (i.e. services which were not transformed by an SSC program such as the Data Centre Consolidation Program, the Telecom Transformation Program, etc.) might not be compliant with this reference architecture. It is anticipated that noncompliant infrastructure in the Protected GC IT domain would be transformed over time; and, during such transformation, compliance to this architecture is required.

This document does not apply to departments which are not SSC Partners, as they are permitted to operate their own IT domain and should have their own security zoning standard.

1.5 Vision, Goals and Objectives

This reference architecture is not a design document in and of itself. Rather, it is an anchor document which can be used:

- During the high-level design of SSC IT infrastructure
- As a guide during service and Partner network design.

The Zoning Reference Architecture document should be used in conjunction with a more detailed companion document which defines security requirements within the defined security zones.

1.5.1 Business and Motivation views

The motivation model for network zoning is one of the most important models because it represents the linkages between business processes/solutions and the key stakeholders of an architecture.

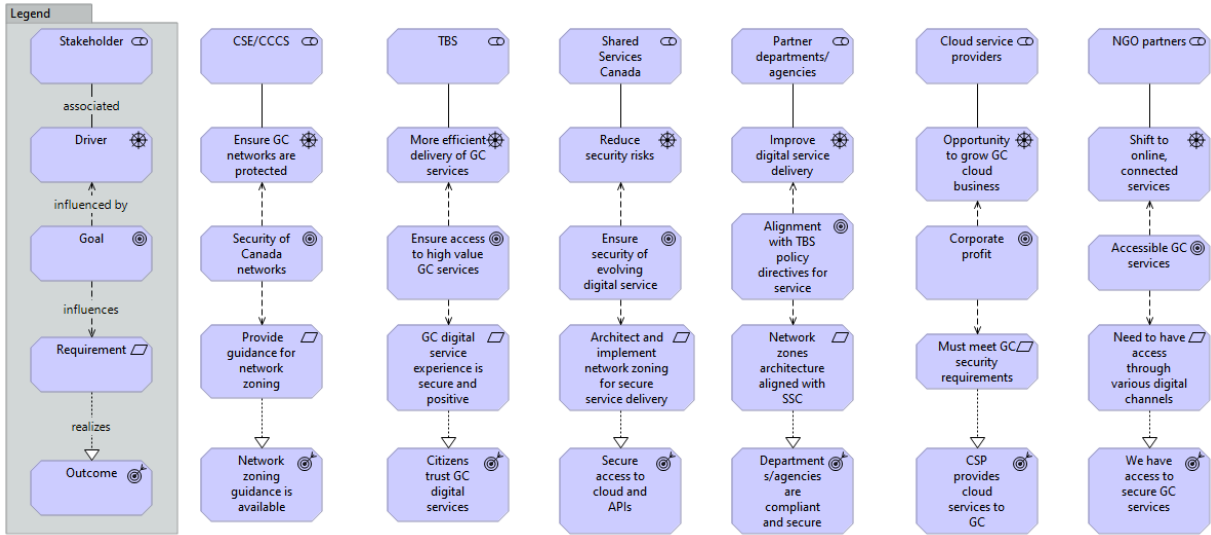


Figure 1. Network Zoning Motivation Model

Figure 1 above utilizes The Open Group ArchiMate 3.0.1 Specification Enterprise Architecture (EA) modeling language, that is a visual language with a set of default iconography for describing, analyzing, and communicating many concerns of EA. An overview of the ArchiMate concepts is contained in Appendix A or a link to the detailed specification is available at Ref E.

The Legend column of the figure identifies the element (object) type for each row of this 5x6 matrix diagram and the columns are the specific Stakeholder perspectives. ArchiMate models are used throughout this RA document to illustrate concepts and specific use case information. Readers are encouraged to familiarize themselves with

the ArchiMate EA modelling language to fully understand the information provided in the figures.

1.6 High-Level Operational Concept

1.6.1 Business Architecture

Government departments' primary function is to deliver government business services to Canadian citizens and businesses. Consumer service expectations are higher than ever with companies continually raising the bar for digital service delivery. Government departments are under pressure to securely deliver high value services. The following model shows how government departments and agencies deliver GC services to private sector organisations, other government departments/partner government agencies, non-government organisations, and most importantly citizens/individuals.

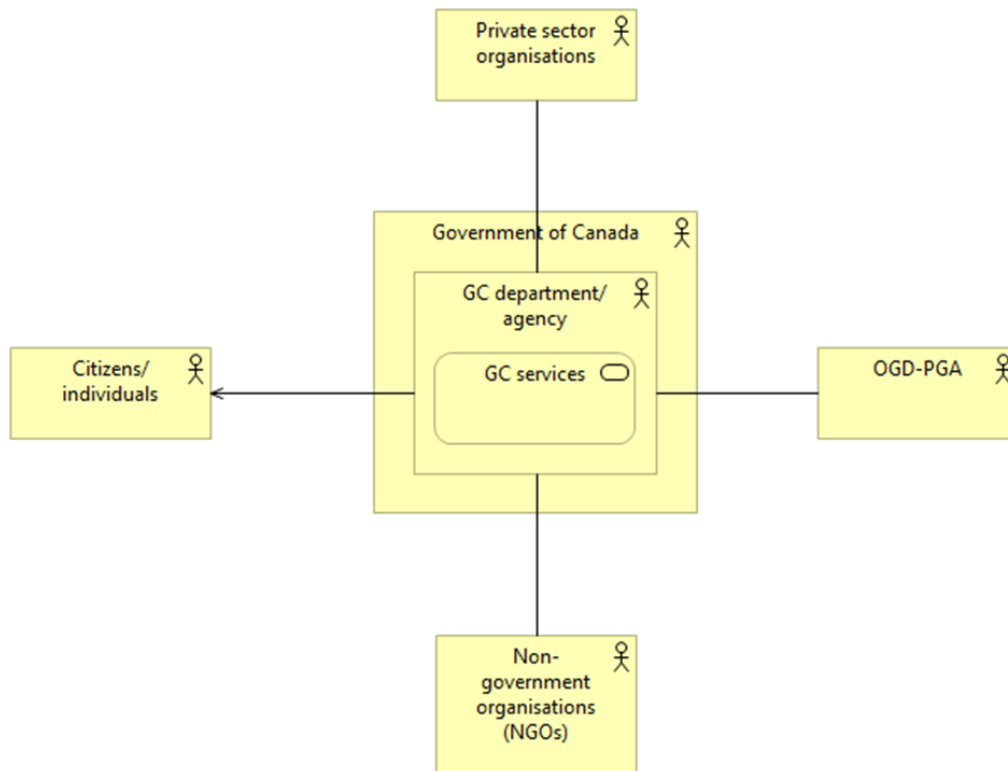


Figure 2. GC Service Delivery Context

1.6.2 Business View

The following model focuses on the SSC business view where SSC provides partners infrastructure, network and security services.

This view supports the GC "Cloud First" based on GC Architectural Standards for Digital Alignment that all departments must aligned with.

SSC is associated to its 'Mandate' represented here as a driver (ArchiMate Driver element), to consolidate and provide information technology and network infrastructure services. The model depicts this relationship between the SSC party and the high-level services as an assignment. The relevant GC Technology services (to network zoning) and is composed of data centre operations and network and telecom services that serve GC partners. On the right side, the GC Vendor management services as associated to a brokering function that is associated to GC Cloud services, which in turn serve SSC's GC partners.

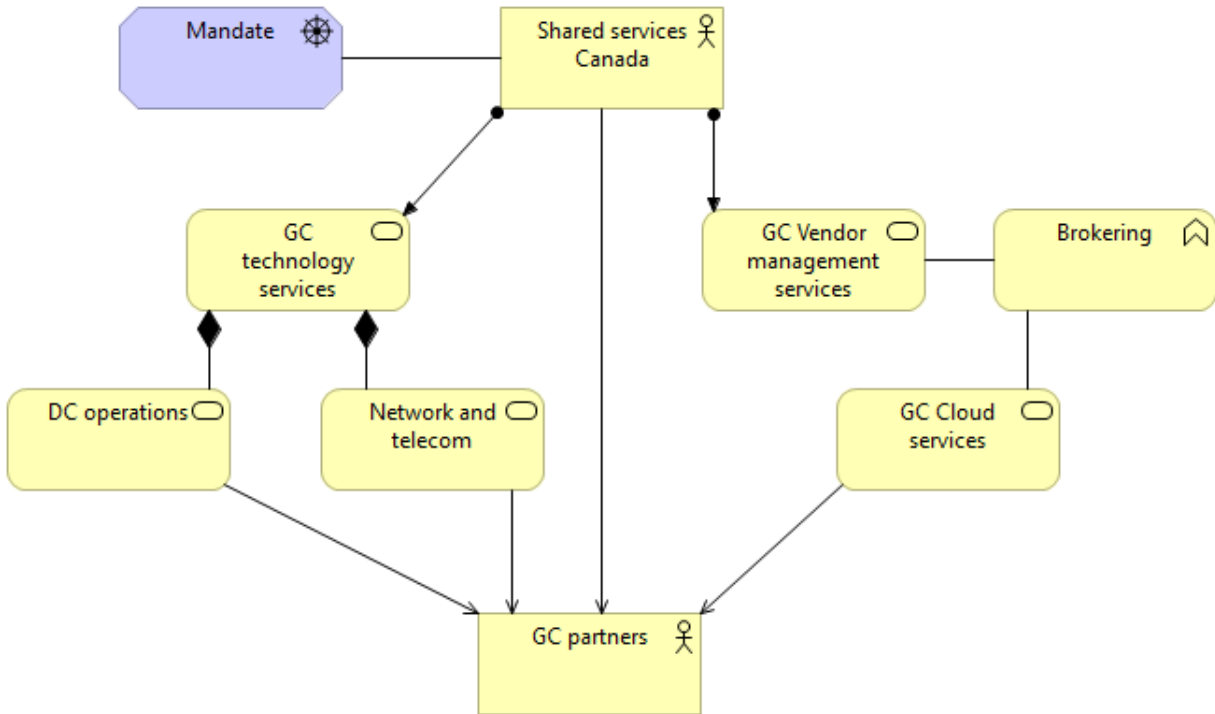


Figure 3. SSC Business View

1.6.3 Government of Canada High Level Business Patterns

The following model illustrates a generic business to business (B2B) integration between a GC department/agency and private sector organizations and/or non-government organizations. There is a bidirectional information flow between the external entities and GC applications and GC data that is mediated by both security services and B2B technology services.

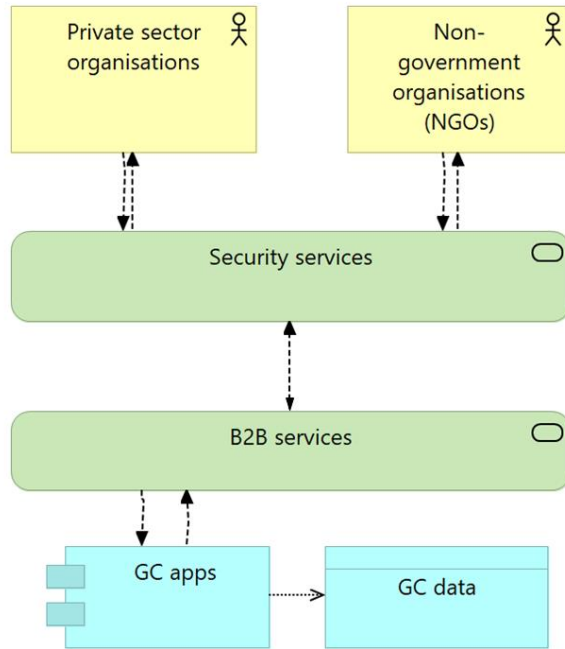


Figure 4. Department B2B View

1.6.4 GC Departments Interoperability Pattern

Figure 5 provides a high-level view of GC departments current interoperability pattern. GC departments work and collaborate with external partners or non-government organizations (NGOs) and government partners as well as citizens. The Internet of Things (IoT) is growing rapidly with more smart devices connected to people and networks across the globe.

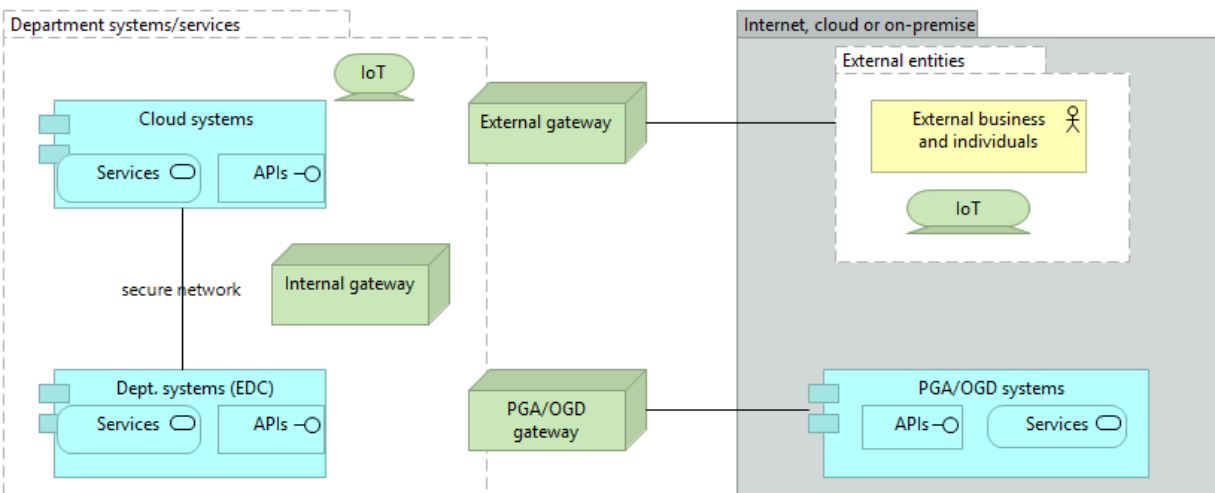


Figure 5. GC Departments Interoperability Pattern

1.6.5 Definitions

The definitions of types of security zones and their elements come from ITSG-22 [Ref B] which is the current state reference for this document. They are copied here for convenience. Additional definitions are contained in Section 5 Glossary of Terms & Acronyms.

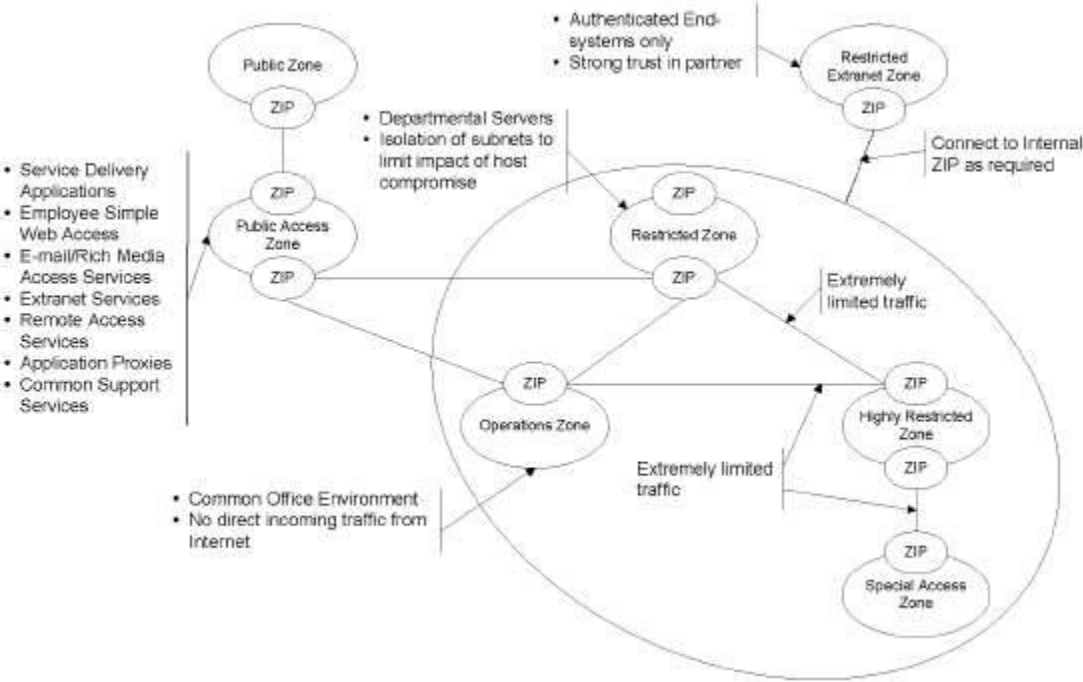


Figure 6. Current State Network Security Zone Implementation Model²

1.6.5.1 Public Zone (PZ)

The PZ is entirely open and includes public networks such as the Internet, the public switched telephone network, and other public carrier backbone networks and services. Restrictions and requirements are difficult or impossible to place or enforce on this Zone because it is normally outside the control of the GC as a system owner. The PZ environment is assumed extremely hostile. Any systems delivered in, or interfacing with, the PZ should be hardened against attack.

The fact that the PZ is assumed extremely hostile does not prohibit a Network Security Zone Authority from using security services from public providers. In fact, this is encouraged because it enhances the defence-in-depth posture. However, it would be

² Figure sourced from Ref B ITSG – 22 - Baseline Security Requirements for Network Security Zones in the Government of Canada, June 2007.

extremely unwise to discount the magnitude of the threat presented by a PZ when developing baseline security requirements.

1.6.5.2 Public Access Zone (PAZ)

A PAZ mediates access between operational GC systems and the PZ. The interfaces to all Government On-Line services should be implemented in a PAZ. Proxy services that allow GC personnel to access Internet-based applications should be implemented in a PAZ, as should external e-mail, remote access, and extranet gateways.

A PAZ is a tightly controlled environment that protects internal GC networks and applications from the hostile PZ. The PAZ also acts as a screen to hide internal resources from the PZ and limit the exposure of internal resources.

Note that remote access, mentioned above, includes only implementations that provide full network access to resources on internal GC networks. Some remote access solutions, including access over the public switched telephone network, provide remote control of specific hosts on internal networks (e.g. terminal servers). These host-based implementations are more restrictive and provide only a terminal window on the internal network. These solutions are Service Delivery Applications and the security requirements for Service Delivery Applications apply as discussed in the federated Architecture Model³.

1.6.5.3 Operations Zone (OZ)

An OZ is the standard environment for routine GC operations. It is the environment in which most end-user systems and workgroup servers are installed. With appropriate security controls at the End-Systems, this Zone may be suitable for processing sensitive information; however, it is generally unsuitable for large repositories of sensitive data or critical applications without additional strong, trustworthy security controls that are beyond the scope of this Guideline⁴.

Within an OZ, traffic is generally unrestricted and can originate internally or from authorized external sources via the PAZ. Examples of external traffic sources include remote access, mobile access, and extranets. Malicious traffic may originate from hostile insiders, from hostile code imported from the PZ, or from undetected malicious nodes on the network (e.g. compromised host, unauthorized wireless attachment to the Zone).

1.6.5.4 Restricted Zone (RZ)

An RZ provides a controlled network environment generally suitable for business-critical IT services (i.e., those having medium reliability requirements, where compromise of the

³ *Government of Canada - Federated Architecture - Iteration One* [online]. [Ottawa]: Treasury Board of Canada Secretariat, June 2000 [cited 1 April 2006]. Available from http://www.tbs.sct.gc.ca/fap-paf/documents/iteration/iteration_e.asp.

⁴ Refers to ITSG-22.

IT services would cause a business disruption) or large repositories of sensitive information (e.g. in a data centre). It supports access from systems in the PZ via a PAZ. All network-layer entities in an RZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and configuration control. The RZ reduces the threats from system insiders by limiting access and through administrative monitoring. Data confidentiality services are implemented in an RZ to protect Zone traffic from eavesdropping by unauthorized nodes. These services may be implemented in the network or through media security.

1.6.5.5 Highly Restricted Zone (HRZ)

An HRZ provides a tightly controlled network environment generally suitable for safety-critical applications (i.e., those with high reliability requirements, where compromise of the IT systems would endanger human health or safety) or extensive repositories of sensitive information. Only other Zones controlled by the GC may access an HRZ (i.e., there is no access by systems in the PZ). All network-layer entities in an HRZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and rigorous configuration control. In general, the HRZ has more stringent requirements for End-Systems than the RZ does. It also imposes stricter controls on system insiders to address threats from that source. Data confidentiality services, suitable for protecting sensitive information, are also implemented in an HRZ to protect Zone traffic against eavesdropping by unauthorized nodes. These services may be implemented at either the network or physical layer. Measures may be required to protect against unauthorized access to electronic emissions.

1.6.5.6 Restricted Extranet Zone (REZ)

A REZ supports directly connected (i.e. not connected via a PAZ, see Figure 6) extranet services with highly trusted partners. This Zone can be viewed as a logical extension of internal Zones to organizations external to the GC. The requirements and practices for this Zone would be developed on a case-by-case basis and enforced through agreements with partners.

Possible examples of REZs include:

- Integration with financial institutions;
- Outsourced IT environments;
- Federal-provincial interfaces; and
- Interfaces with other governments.

Connections between departments of the GC do not use a REZ. A REZ is only for connections to organizations outside the GC. Connections between departments would be via direct Zone-to-Zone connections (e.g. OZ to OZ, OZ to PAZ to OZ, RZ to RZ, RZ to PAZ to RZ, HRZ to HRZ).

1.6.5.7 Management Restricted Zone (MRZ)

Departmental and Internet services network architectures have a restricted zone designed specifically for management called the management RZ. This zone contains IT administration related services for the departmental and Internet services network operations.

Services located in the management RZ only communicate with the public zone via the PAZ for updates from a vendor network sites using appropriate security safeguards that protect integrity and confidentiality of the communication and authenticate the vendor network address.

1.6.5.8 Special Access Zone (SAZ)

A SAZ is a tightly controlled network environment suitable for special processing needs. Requirements for a SAZ would be developed on a case-by-case basis to meet the special processing needs of the environment. Measures may be required to protect against unauthorized access to electronic emissions. Limitations in security technology may prohibit network connections to other Zones.

1.7 Linkages to Other Architectures, Programs and Initiatives

Reference architectures that could be informative are:

- GCCOF - GC Cloud Onboarding Framework - SSC EA
- GC E2E Net - GC End to End Network RAD - SSC EA
- EDC RAD - SSC EA
- SCED - Secure Cloud Enablement and Defence - SSC SM&G
- SRAD - Security Reference Architecture Document - SSC SM&G

Additional sources of information used in the preparation of this RA are:

- GC Enterprise architecture strategies and services, including:
 - OneGC,
 - Sign-in Canada,
 - Pan-Canadian Trust Framework [Ref L],
 - GC Internal Central Authentication Services (GCpass - the GC Internal Centralized Authentication Service (ICAS)) [Ref K],
 - Digital Exchange Platform, and
 - Open Data.
- GC Digital Standards and GC EA Architectural Principles
- GC Data Strategy
- Government of Canada Policy Instruments
- GC Architectural Standards for Digital Alignment [Ref H]
- GC Enterprise Architecture Framework [Ref I]
- GC Existing Architectural Standards [Ref J]

- GC Enterprise Security and Privacy Architecture [Ref M]
- GC Enterprise Security Architecture (ESA) [Ref N]
- Government of Canada - Federated Architecture - Iteration One [Ref O]

2 High Level Guidance

2.1 Principles

Principles are high-level definitions of fundamental values that guide decisions made concerning the management of business, information, application, technology, security, and privacy.

SSC's Enterprise Architecture principles that are intended to be used as guidance when considering service solution introductions or changes that are enabled by processes, systems, or technology.

The nine prioritized Principles leverage & align with the guiding principles from the other strategic GC & SSC sources.

1. Become Business Driven
2. Enterprise First
3. Understand Client Needs
4. Security and Privacy
5. Reliability and Availability
6. Scalability and Sustainability
7. Loose Coupling and Modularity
8. Automate
9. Metering and Monitoring

Detailed principle descriptions, rationale and implication details are in the SSC [EA Principles](#).

2.2 Drivers

Figure 1 from Section 1.5.1 above provides an example of various drivers associated with specific stakeholders.

3 Standards & Policies

General Shared Services Canada's policies, directives, standards, and guidelines can be viewed via http://service.ssc.gc.ca/en/policies_processes/policies.

3.1 Standards

The following SSC Security related standards should be reviewed for adherence when using this RA:

- [SSC Security Standards](#)
- [Security zone definition security standard](#)

3.2 Policies

[SSC Security policy instruments](#)

[Government of Canada Security Policy](#)

4 Architecture Patterns

4.1 Departmental B2B Zones Interaction View

Figure 7 describes a traditional business to business patterns between a GC department and non-government entities. The Public Zone hosts private sector organizations and non-government organizations, each having bi-directional information flows with GC services. The PAZ hosts enterprise security services to reduce the risks associated with the Public zone. PAZ services mediate the continued bi-directional flow through B2B services and eventually GC applications and GC data hosted in department RZs.

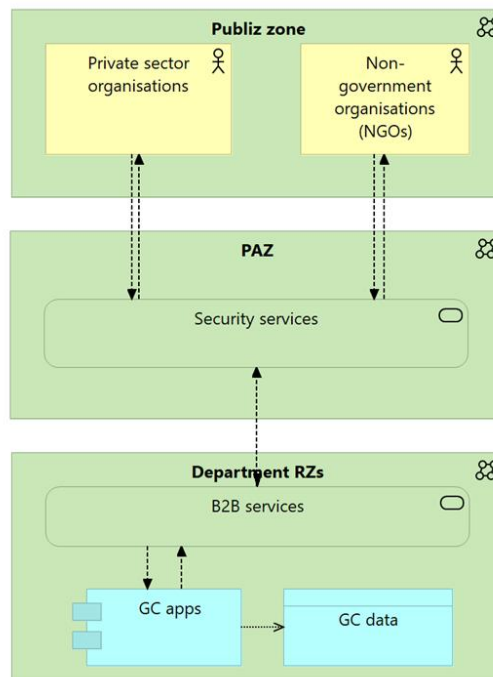


Figure 7. Department B2B Zones Interaction View

4.2 Security Zone Concepts

4.2.1 Zone Interface Points (ZIPs) and Their Security Functions

The model below provides a high-level look at the zone interface points (ZIPs) and the security functions that the ZIPs host. The three primary ZIPs are:

1. Public Access Zone ZIP
2. Operations Zone ZIP
3. Restricted Zone ZIP

The PAZ is the only zone that provides security controls for bi-directional network traffic.

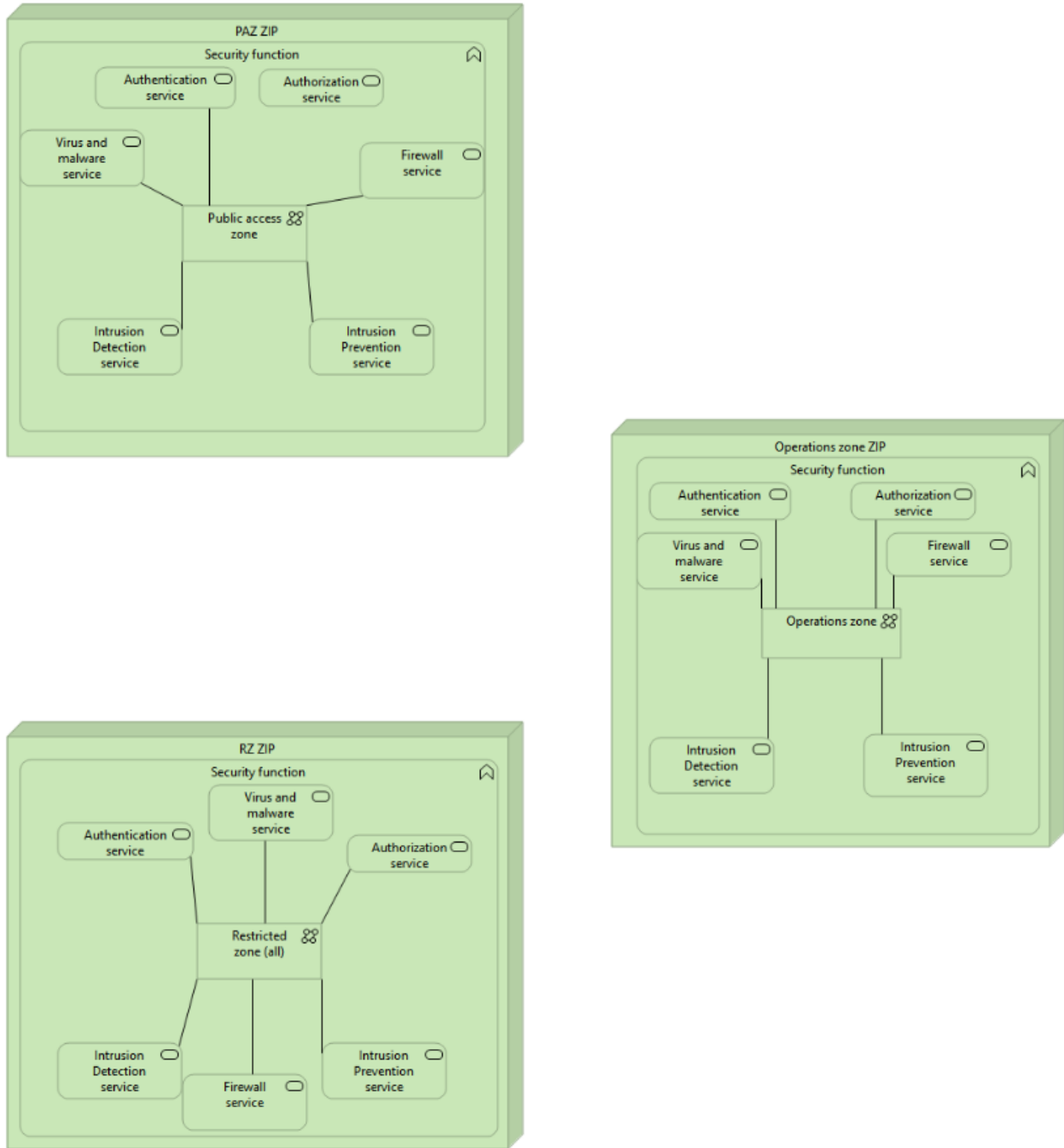


Figure 8. ZIPs & Security Functions

4.2.2 Operations Zone and ZIP

The model below describes the technology services that are most commonly associated to the operations zone (OZ) and the OZ ZIP.

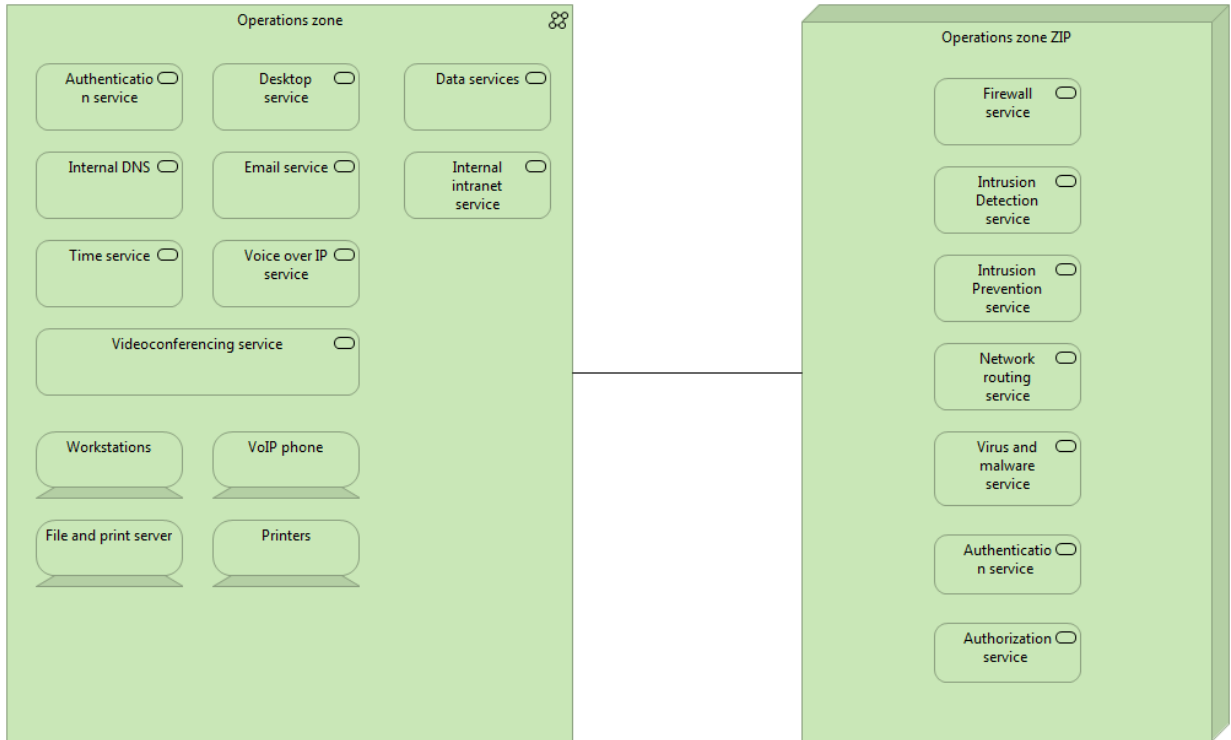


Figure 9. Operations Zone & ZIP Services View

4.2.3 Public Access Zone and ZIP

The model below describes the technology services that are most commonly associated to the public access zone (PAZ) and the PAZ ZIP.

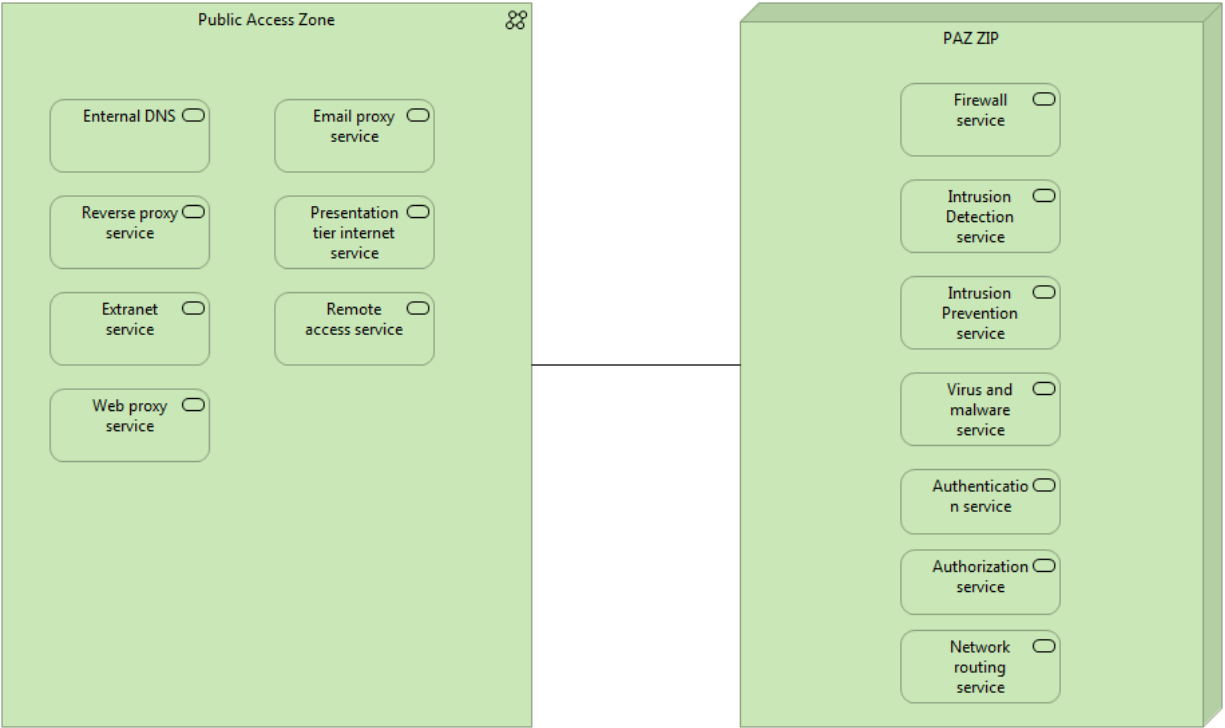


Figure 10. PAZ & PAZ ZIP Services View

4.2.4 Internet Application Restricted Zone and ZIP

The model below describes the technology services that are most commonly associated to the internet application restricted zone (IARZ) and the RZ ZIP.

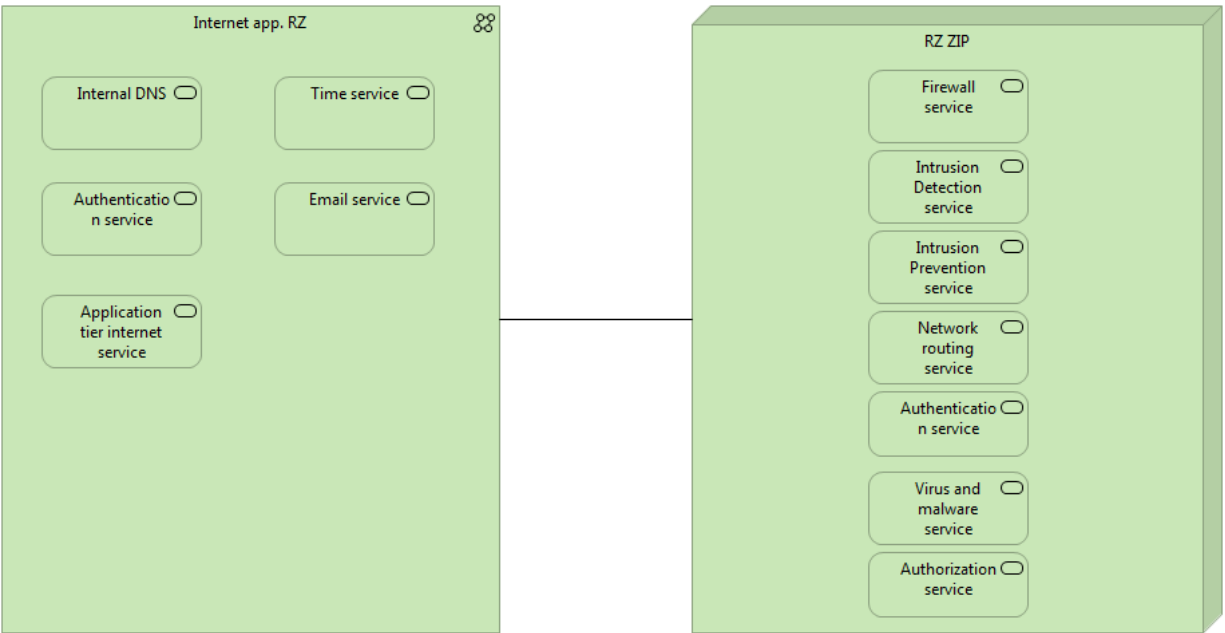


Figure 11. Internet Application Restricted Zone & ZIP Services View

4.2.5 Restricted Zone and RZ ZIP

The model below describes the technology services that are most commonly associated to the restricted zone (RZ) and the RZ ZIP.

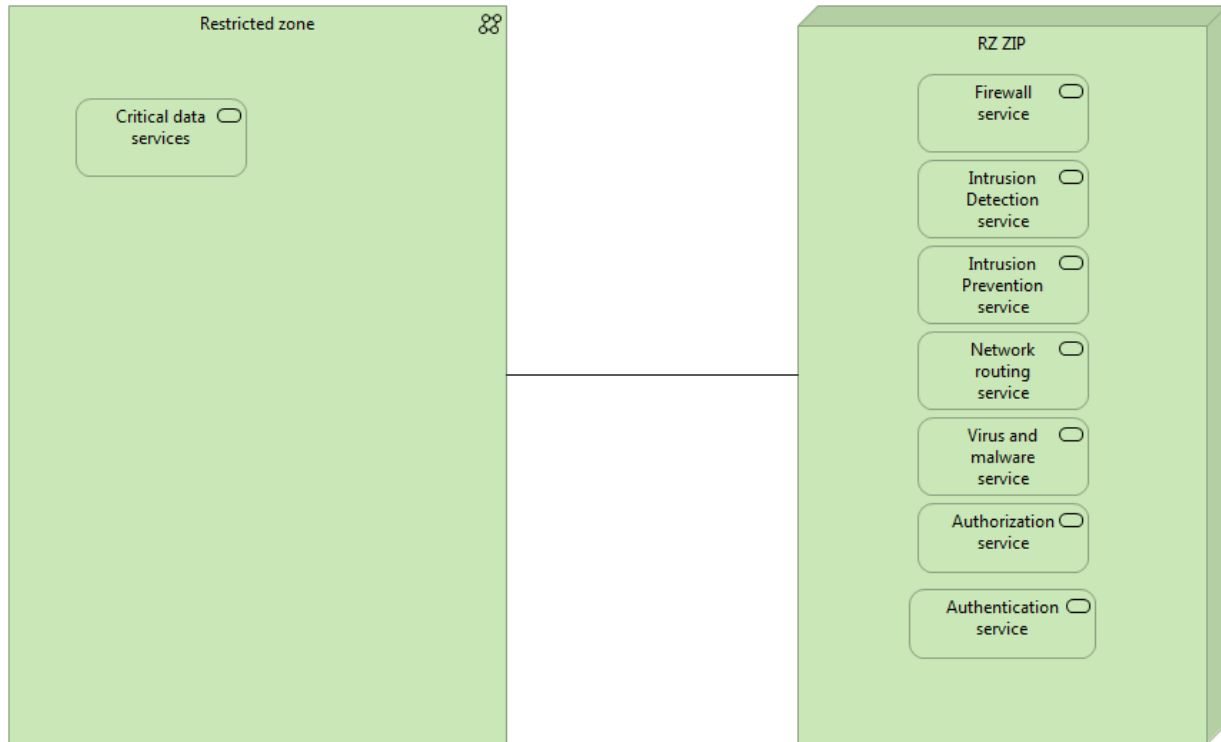


Figure 12. Restricted Zone & RZ ZIP Services View

4.2.6 Data RZ and ZIP

The model below describes the technology services that are most commonly associated to the data restricted zone (DRZ) and the RZ ZIP.

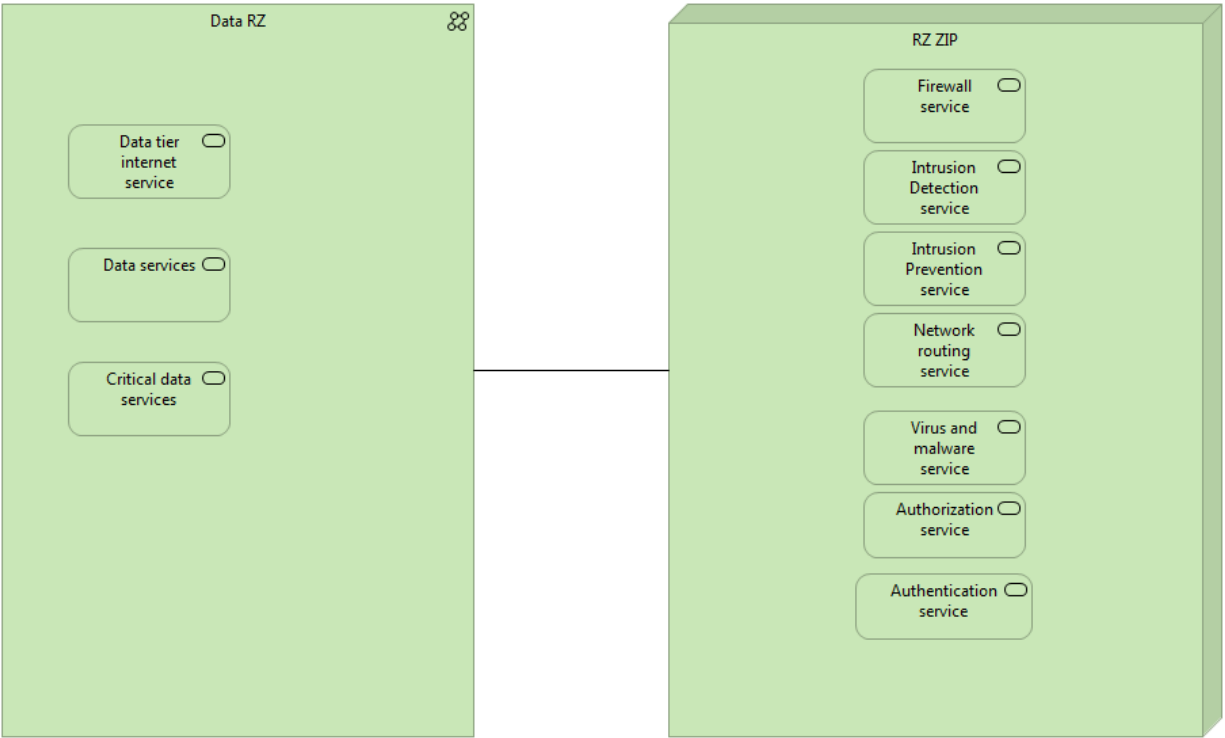


Figure 13. Data RZ & ZIP Services View

4.2.7 Management RZ and ZIP

The model below describes the technology services that are most commonly associated to the internet application management restricted zone (MRZ) and the RZ ZIP.



Figure 14. Management RZ & ZIP Services View

4.3 High Level Network Zoning

Two models are provided for implementing SaaS cloud service delivery. The first option, Figure 15, is integration between a traditional EDC hosted department and the second, Figure 16, is for connectivity from a department cloud infrastructure to a SaaS application. Departments using SaaS services should implement network zoning to mediate the risks associated with using an IT environment that is fully controlled by a 3rd party.

Figure 15 describes a department using traditional SSC Enterprise Data Centre (EDC) for primary IT and IM application service hosting. This department is also using a cloud-based SaaS solution that is accessible by department users and interoperates with other department systems.

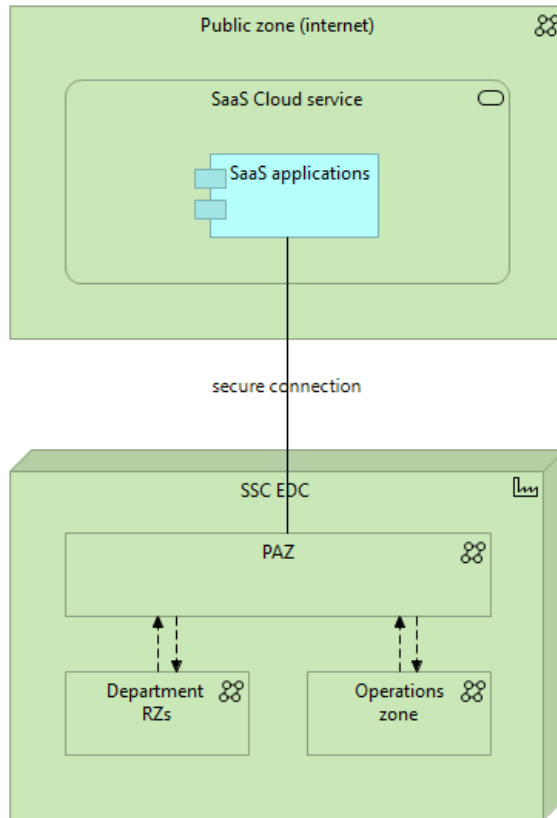


Figure 15. EDC to SaaS Cloud

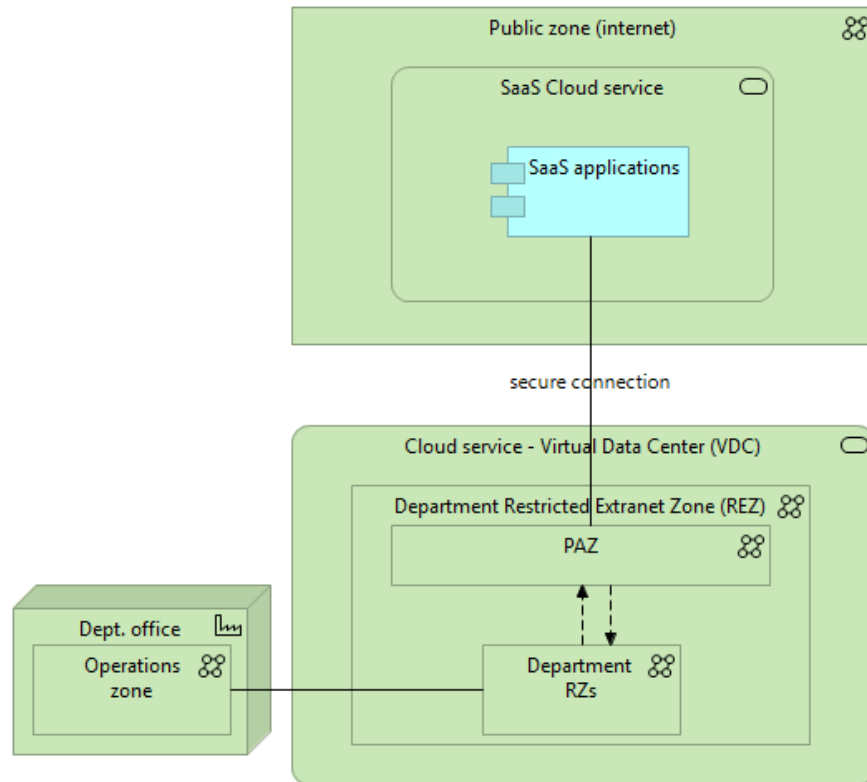


Figure 16. Virtual Data Center (VDC) to SaaS Cloud

4.4 Management Restricted Zones

The next model provides a high-level look at all the network zones available to government of Canada departments/agencies. The management zone is a logical representation of the zone where administrative access to other zones and their configurations initiates.

Each zone has a corresponding MRZ. This doesn't mean that privileged users have a number of physical workstations. Virtual desktops can be configured to support privileged access to specific network zones.

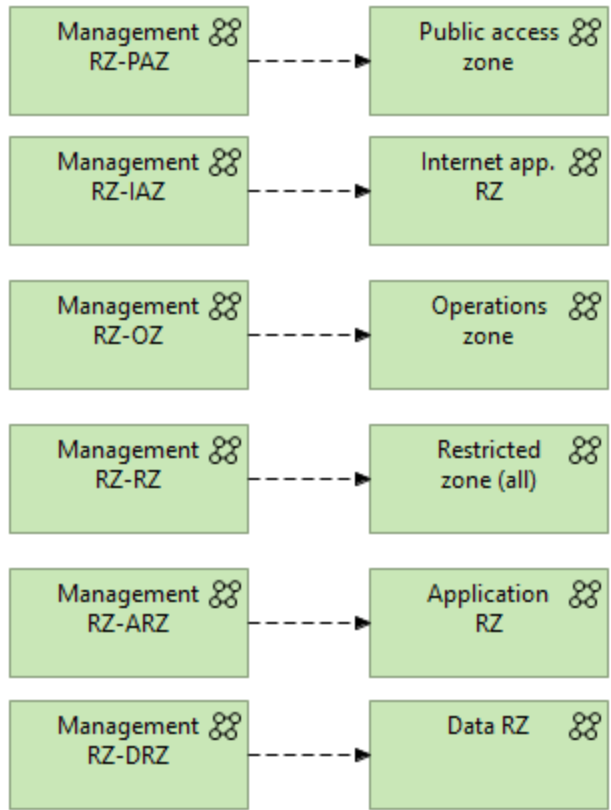


Figure 17. GC Network Zones

4.5 Application, Information and Data Views

4.5.1 Application Views

GC Application Programming Interfaces (APIs) trigger small services that access GC information/data. These application objects are dependent on network zoning.

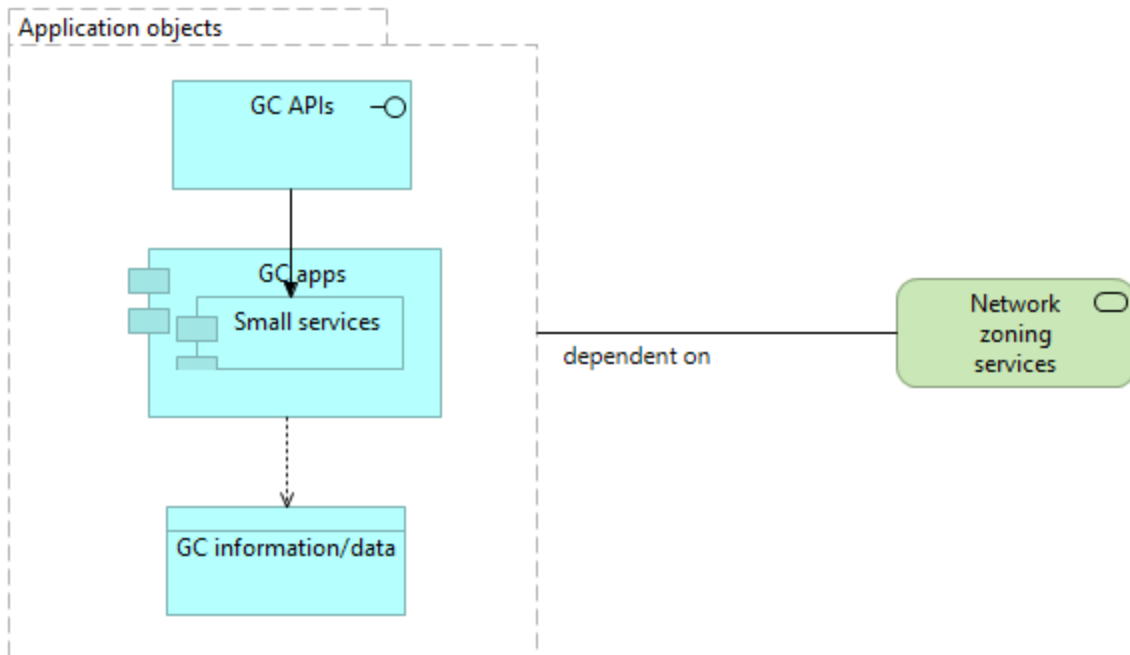


Figure 18. Application Objects Network Zoning Dependency

4.6 Cloud Zoning Scenarios

4.6.1 SSC EDC & Cloud Service Integration

The following model represents a partner department that has limited integration with outside technologies but that does want to leverage cloud computing services. From the bottom up this model represents an SSC Enterprise Data Centre facility where common department zones (PAZ, RZs and MRZ) are configured. Note that the departmental OZ is located in a department facility. This model also represents an association between the department PAZ and a trusted service provider.

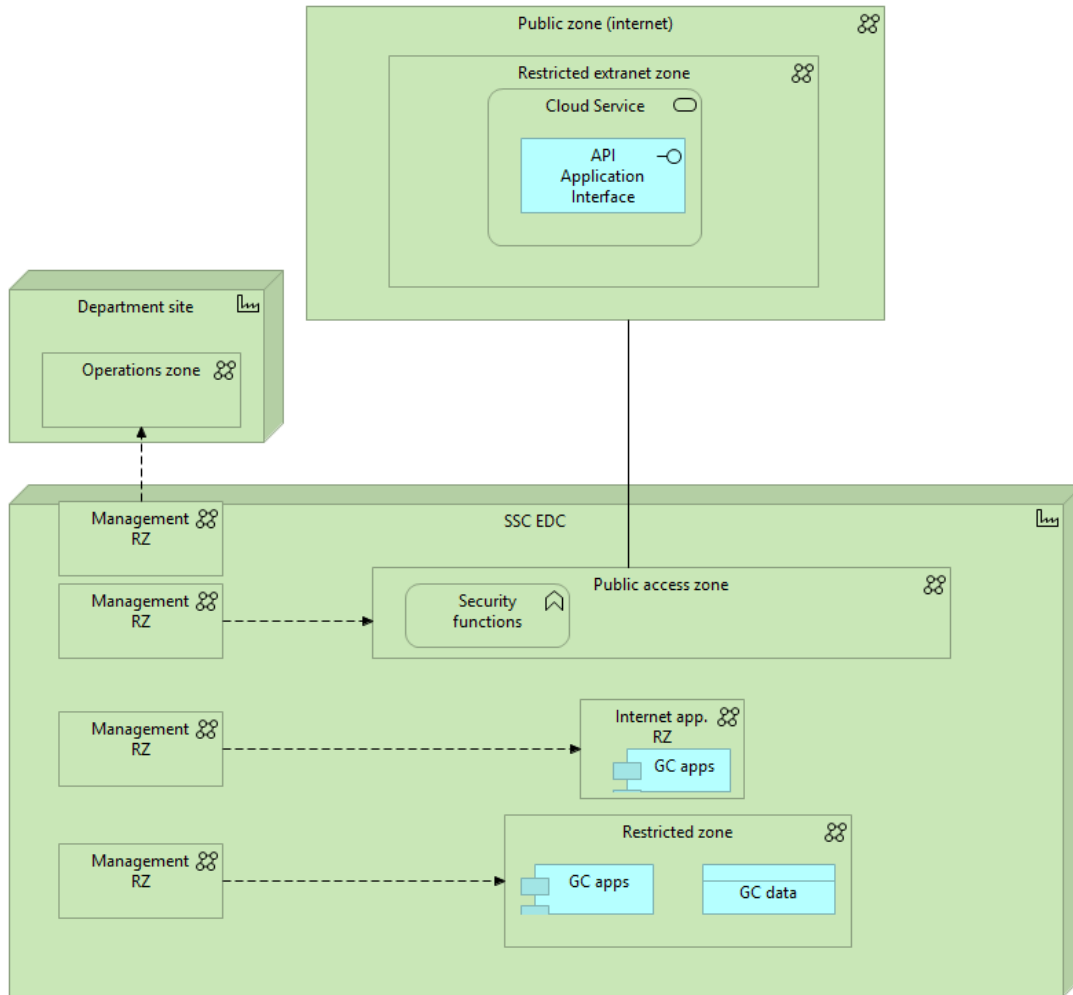


Figure 19. Cloud Hosted Services Integration View

4.6.2 Department Cloud Hybrid Zoning View

This model describes a GC partner with a significant investment in legacy systems that is ready for a shift to modern IT technologies such as AI and cloud offerings hosted in a virtual data centre.

Information flows between the cloud and ground are mediated by the security functions in the respective PAZs. The extra “data RZ” found in the cloud is only used to show that zoning requirements could be different across department/agency clouds VDCs and GC enterprise data centres. A data RZ in the cloud could be required to facilitate data analytics in the cloud.

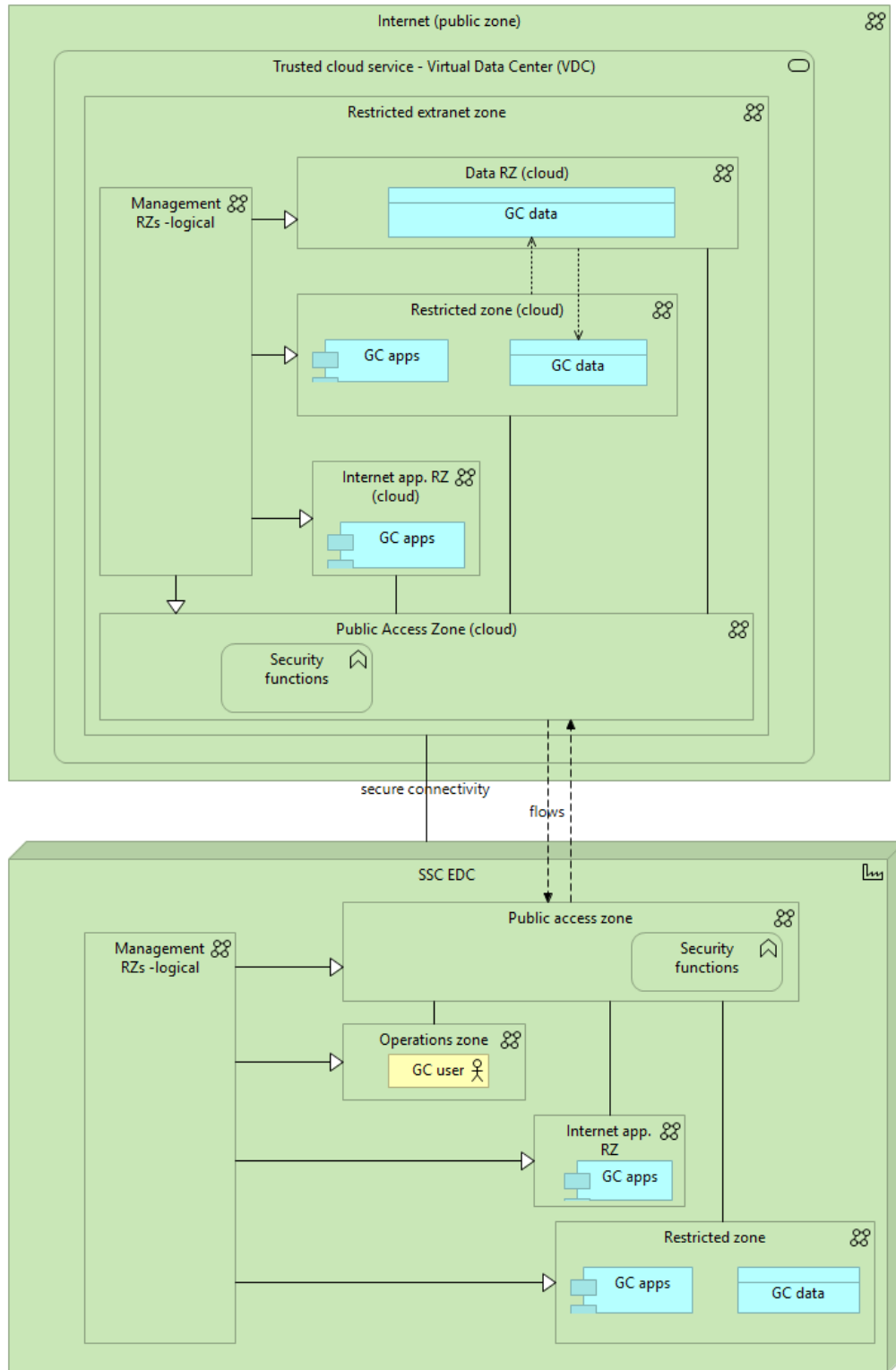


Figure 20. Department Cloud Hybrid Zoning View

4.6.3 Department Shift to Full Cloud Hosting

Some partner departments and agencies may seek to shift most of their IT/IM to the cloud. This may be a good model for partner departments and agencies without user interactive digital services. Note that the OZ, MRZ and PAZ are still required. From left to right GC users work using end point devices in the OZ which is managed (specialized) from the MRZ. The MRZ also manages (specializes) PAZs and department RZs hosted in the cloud.

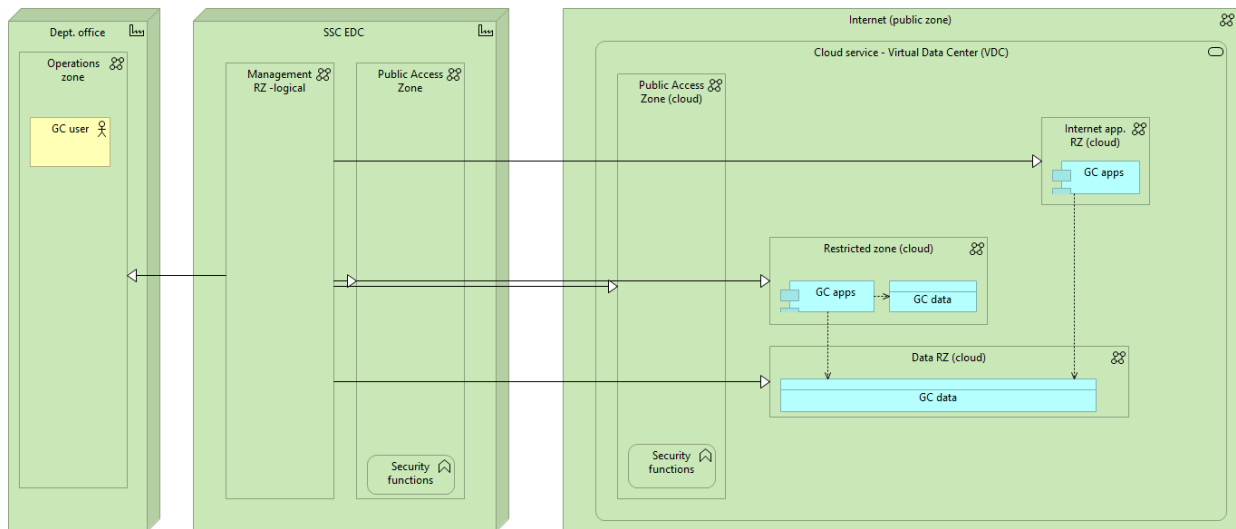


Figure 21. Full Cloud Hosting View

4.6.4 Cloud Zones

The CSE guidance for network zoning was developed well before cloud computing became mainstream and truly accessible. The government of Canada has a “cloud first” approach to selecting computer platforms and IT-IM services. As such GC network zones shall (also) exist in the cloud. Historically the ITSG-22 (published version) focuses on security zones for a single organization. As such the PAZ applies security policy that apply to the entire organization. Department virtual data centers (VDCs) in the cloud require the same network zoning as they would in a traditional EDC.

Figure 22 shows how traditional zones and cloud zones are deployed to support bi-directional information flows. One difference that stands out is that the OZ is not in the cloud.

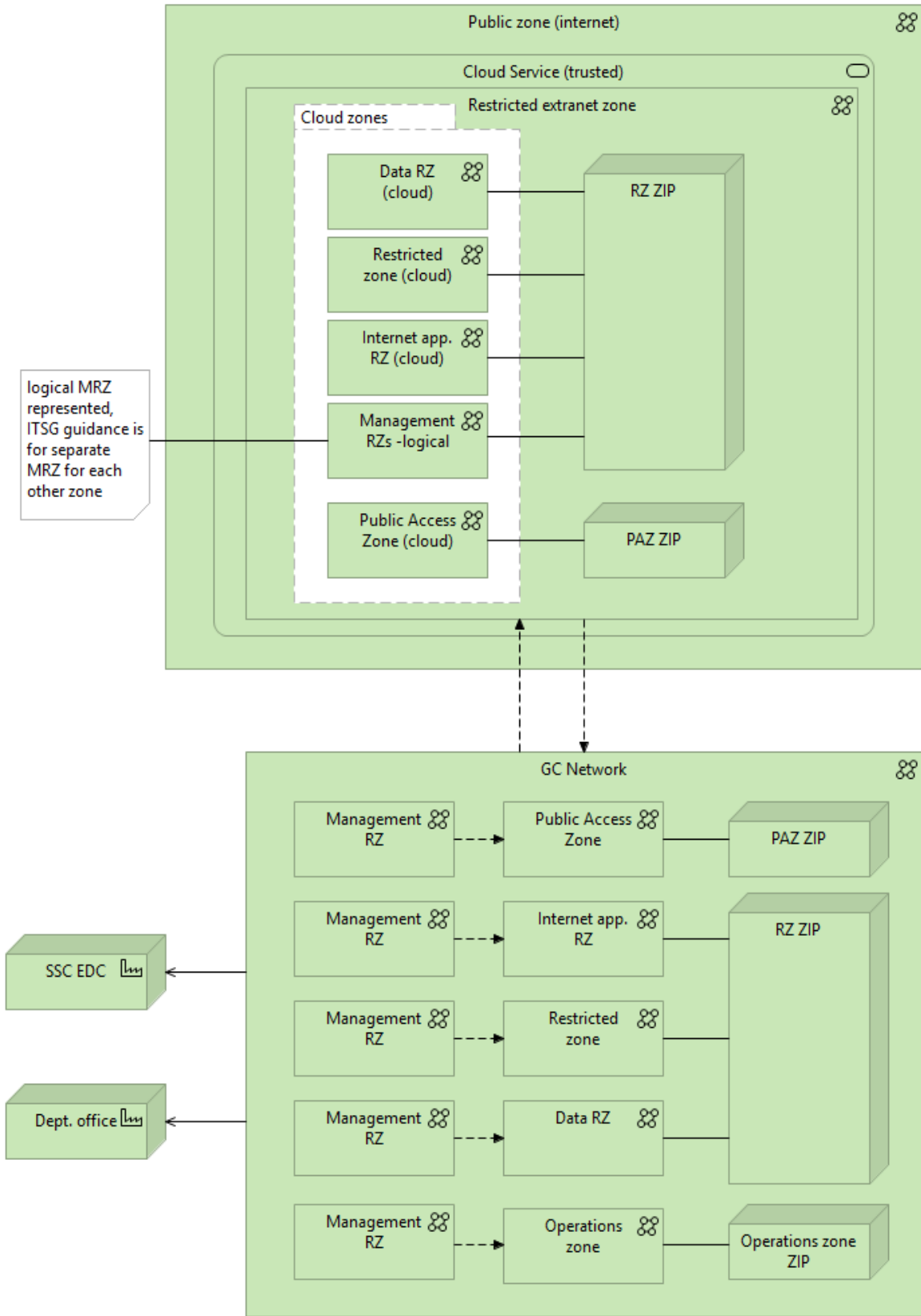


Figure 22. Cloud Network Zones

4.6.5 GC Cloud To Ground And Internet

Figure 23 shows how a GC department with digital services available in the cloud interoperates with its ground systems and the internet. At bottom left the model shows department apps and data hosted in traditional SSC data centres, connected to GCNet. From the SCED TIP GC users connect to the department PAZ then to department RZs. From the top left we see that Internet traffic travels to the SSC PAZ (in the cloud) where the GC CAP mediates internet based traffic before allowing interoperability with the department PAZ and then the department RZs. The yellow “account” objects represent different cost centres that use cloud resources (used for billing ...).

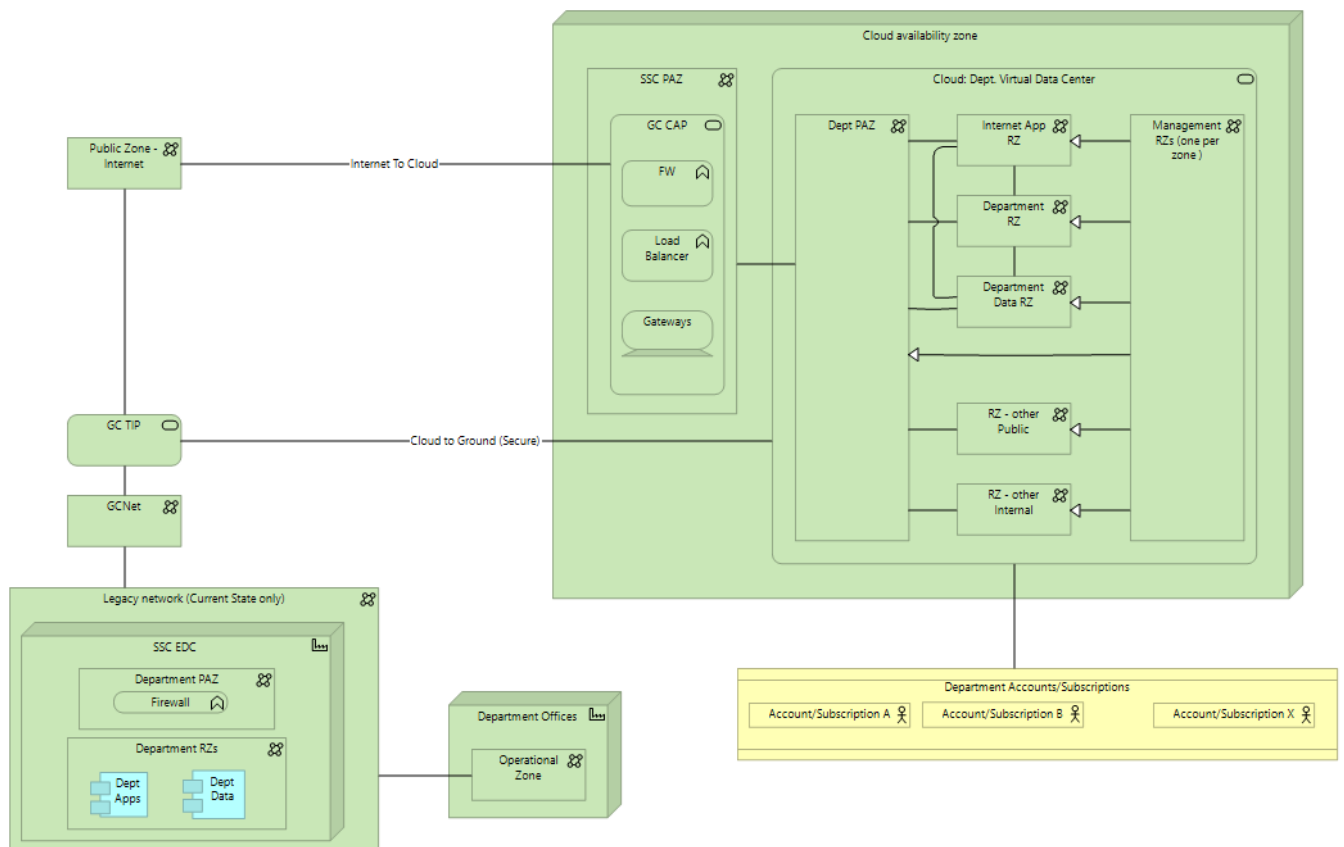


Figure 23. GC Cloud to Ground and Internet for AWS

4.7 Internet of Things

The Internet of Things brings all kinds of connected devices to the table. Many citizens have IoT wearables and the reality of autonomous/connected vehicles is expected to become available over the next few years, already most new vehicles sold throughout the world are connected. Provinces and municipalities are investing in smart devices that help them deliver better government services like snow and ice removal from roadways for example. Some government departments use connected devices such as scientific instruments to gather data for all manner of metrics ranging from images, temperature to nuclear isotopes.

Unlike traditional endpoint devices, many of the IoT devices are not under GC control and therefore cannot be trusted. In general devices that are connected to the internet (public zone) are not trusted, other GC owned and controlled IoT devices are found in department/agency OZs, and these are trusted. The general guidance is that untrusted IoT devices must be mediated through departmental PAZs. Trusted IoT devices will be part of department/agency OZs and will follow traditional endpoint patterns much like a laptop or smartphone does today.

Figure 23 shows the connectivity to public IoT devices (left side) and network zoning for GC IoT devices (right side and center).

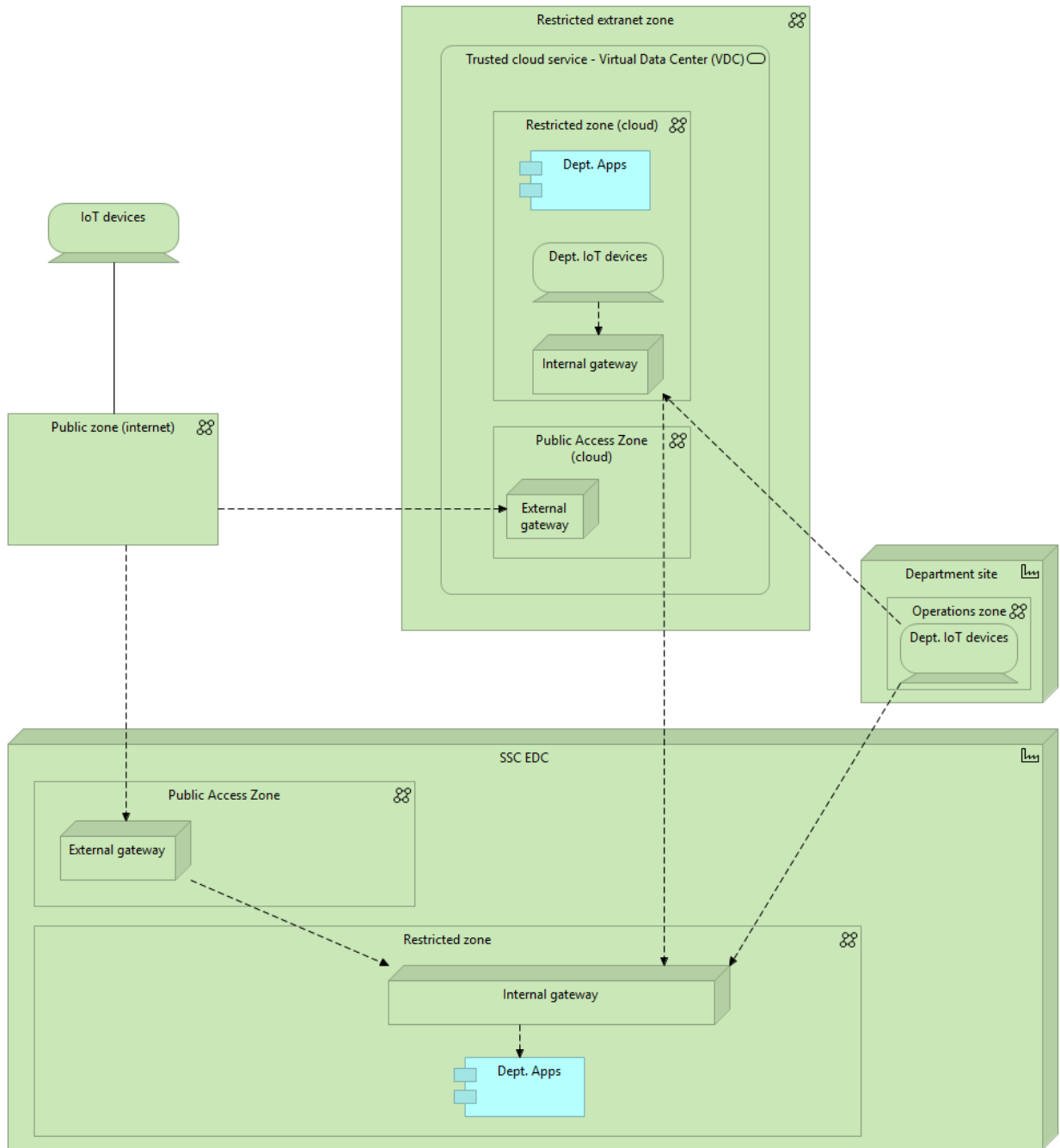


Figure 24. Internet of Things.

4.8 OGD-PGA Interoperability

Figure 25 describes three fundamental integration patterns: Internet facing cloud services, department cloud services, and government to government (G2G) integration (G2G). We're using two visual groupings to separate the patterns between G2G and the rest.

In the G2G grouping element we have 2 GC departments (departments A and B) network zoning in SSC enterprise data centers (EDC) using GC common Canada's Digital eXchange Platform (CDXP) services also hosted in an SSC EDC to enable integration between GC applications (GC apps). CDXP services connect to each department's PGA/OGD gateway to reach GC apps. Province and Territory (PT) also use CDXP services to provide identity services used by GC departments.

In the Internet and cloud GC services grouping we describe from left to right: Department A's trusted computing services located in the cloud where Dept. A GC apps are hosted. An internal gateway mediates integration and messaging with other trusted services in Restricted Extranet Zones (REZs).

The next REZ represents the CDXP services hosted in the public cloud, note a public access zone (PAZ) is included in this REZ because it has internet facing connectivity using a secure external gateway. The dashed lines in the model represent data or information flows.

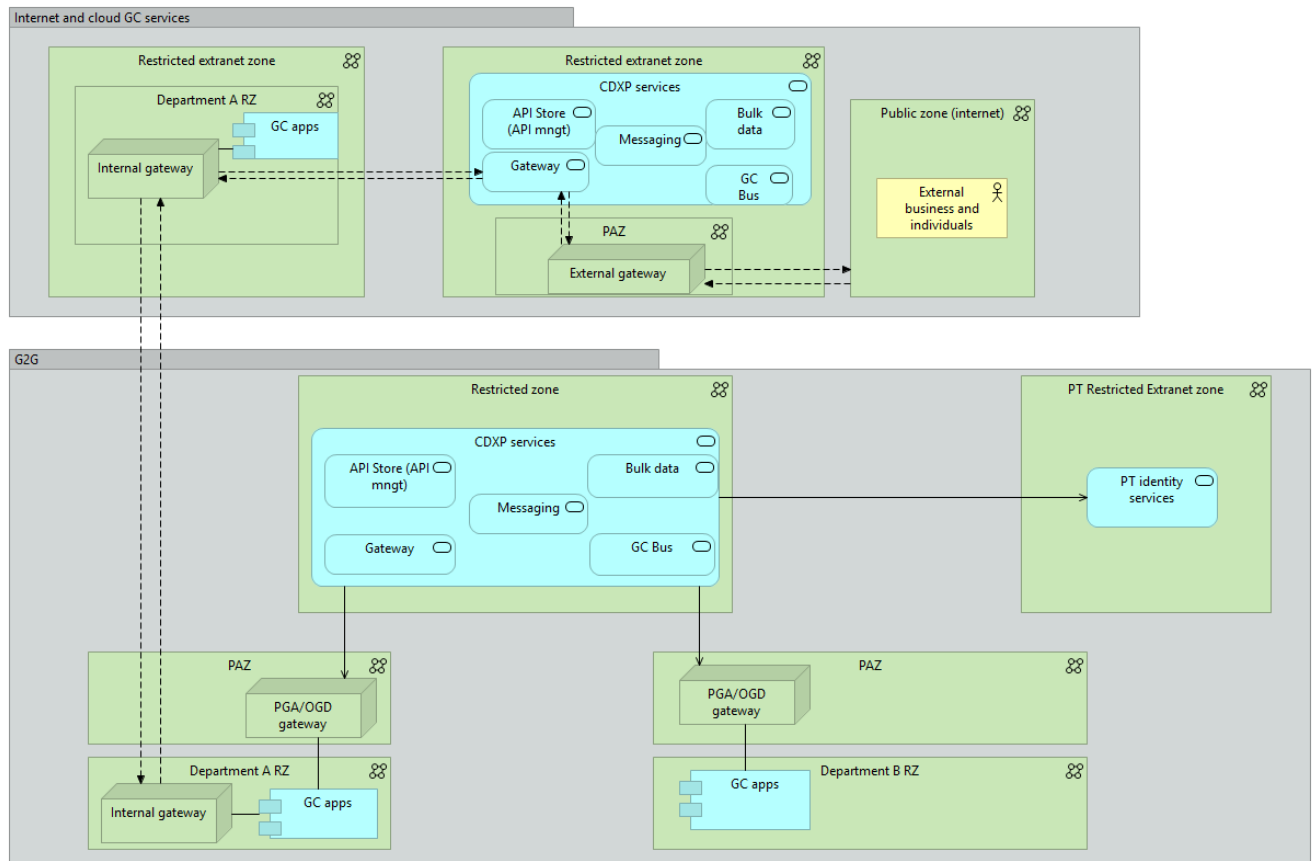


Figure 25. OGD-PGA Interoperability View

5 Glossary of Terms & Acronyms

5.1 Glossary of Terms

Term	Description
CSE	Communications Security Establishment (CSE) Canada: An agency of the Department of National Defence, that is responsible for the development of security standards and guidance related to computer networks.
End System	A system that, for a particular instance of communication, is the ultimate source or destination of the communication. (Source: ITSG-22)
External Service	A service that a client department can order from SSC (i.e. in the SSC Service Catalogue).
Highly Restricted Zone (HRZ)	See Section 1.6.5.5. (Source: ITSG-22)
Management Zone (MZ)	See Section 1.6.5.7. (Source: ITSG-22)
Operations Zone (OZ)	See Section 1.6.5.3. (Source: ITSG-22)
Public Access Zone (PAZ)	See Section 1.6.5.2. (Source: ITSG-22)
Public Zone (PZ)	See Section 1.6.5.1. (Source: ITSG-22)
Restricted Extranet Zone (REZ)	See Section 1.6.5.6. (Source: ITSG-22)
Restricted Zone (RZ)	See Section 1.6.5.4. (Source: ITSG-22)
Special Access Zone (SAZ)	See Section 1.6.5.8. (Source: ITSG-22)
Zone Interface Point (ZIP)	An interface between two Network Security Zones through which traffic may be routed. (Source: ITSG-22)

5.2 Acronyms

Acronym	Description
API	Application Programming Interface
CSE	Communications Security Establishment Canada
CDXP	Digital eXchange Platform
EA	Enterprise Architecture
EDC	Enterprise Data Centres

Acronym	Description
G2G	Government to Government
PGA	Partner Government Agencies
OGD	Other Government Departments
GC	Government of Canada
HRZ	Highly Restricted Zone
ITSG	Information Technology Security Guideline
ITSP	Information Technology Security Practitioner
MAZ	Management Access Zone
MZ	Management Zone
OZ	Operations Zone
PAZ	Public Access Zone
PT	Province and Territory
PZ	Public Zone
RA	Reference Architecture
REZ	Restricted Extranet Zone
RZ	Restricted Zone
SAZ	Special Access Zone
SMG	Security Management and Governance
NSDS	Network Security and Digital Service
CCCS	Canadian Center for Cyber Security
SSC	Shared Services Canada
TOGAF	The Open Group Architecture Framework
ZIP	Zone Interface Point

6 References

The following documentation was used to develop this Reference Architecture Description.:

Reference	Title	Notes
Ref A	Terms of Reference	SSC Network Security – Zoning architecture Working Group Terms of Reference https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=33397799
Ref B	ITSG – 22 - Baseline Security Requirements for Network Security Zones in the Government of Canada	Information Technology Security Guideline (ITSG) – 22 - Baseline Security Requirements for Network Security Zones in the Government of Canada, (ITSG-22), June 2007. https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22 <i>Baseline Security Requirements for Network Security Zones in the Government of Canada is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSE).</i>
Ref C	ITSG 38 - Network Security Zoning	Information Technology Security Guideline (ITSG) – 38 – Network Security Zoning - Design Considerations for Placement of Services within Zones, May 2009. https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38 <i>The Network Security Zoning is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSE).</i>
Ref D	ITSG 33 – IT Security Risk Management: A Lifecycle Approach	Information Technology Security Guideline (ITSG) – 33 - IT Security Risk Management: A Lifecycle Approach – Overview, Nov 2012. https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33 <i>The IT Security Risk Management: A Lifecycle Approach is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSE).</i>
Ref E	ArchiMate 3.0.1	The Open Group ArchiMate 3.0.1 Specification http://pubs.opengroup.org/architecture/archimate3-doc/toc.html
Ref F	The Open Group Architecture Framework (TOGAF)	The Open Group Architecture Framework “TOGAF Version 9.1,” 2011. TOGAF

Reference	Title	Notes
Ref G	Security Zone Definition Security Standard	https://gcdocs.gc.ca/ssc-spc/llisapi.dll?func=ll&objaction=overview&objid=10649608
Ref H	GC Architectural Standards for Digital Alignment	http://www.gcpedia.gc.ca/wiki/GC_Architectural_Standards_for_Digital_Alignment
Ref I	GC Enterprise Architecture Framework	http://www.gcpedia.gc.ca/wiki/GC_Enterprise_Architecture_Framework
Ref J	GC Existing Architectural Standards	http://www.gcpedia.gc.ca/wiki/GC_Existing_Architectural_Standards
Ref K	GCpass - the GC Internal Centralized Authentication Service (ICAS)	http://www.gcpedia.gc.ca/gcwiki/index.php?title=GCpass_-_the_GC_Internal_Centralized_Authentication_Service_(ICAS)&redirect=no
Ref L	Pan- Canadian Trust Framework	https://diacc.ca/pan-canadian-trust-framework/
Ref M	GC Enterprise Security and Privacy Architecture	https://wiki.gccollab.ca/GC_Enterprise_Security_and_Privacy_Architecture
Ref N	GC ESA	http://www.gcpedia.gc.ca/wiki/Category:Government_of_Canada_Enterprise_Security_Architecture_(ESA)_Program
Ref O	Government of Canada - Federated Architecture - Iteration One	<i>Government of Canada - Federated Architecture - Iteration One</i> [online]. [Ottawa]: Treasury Board of Canada Secretariat, June 2000 [cited 1 April 2006]. Available from http://www.tbs.sct.gc.ca/fap-paf/documents/iteration/iteration_e.asp .
Ref P	Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)	https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html

Appendix A. ArchiMate® Notation

Details regarding the ArchiMate® 3.0.1 notation used in the figures of this reference architecture document are from Chapter 4 of The Open Group™ website [Ref F].

1.1 Quick Reference

Provided below is a graphical representation of the key modelling notation used throughout this document.

1.1.1 Top Level Language Structure

Figure 26 outlines the top-level hierarchical structure of the language:

- A model is a collection of concepts. A concept is either an element or a relationship.
- An element is either a behavior element, a structure element, a motivation element, or a composite element.
-

© 2017 The Open Group

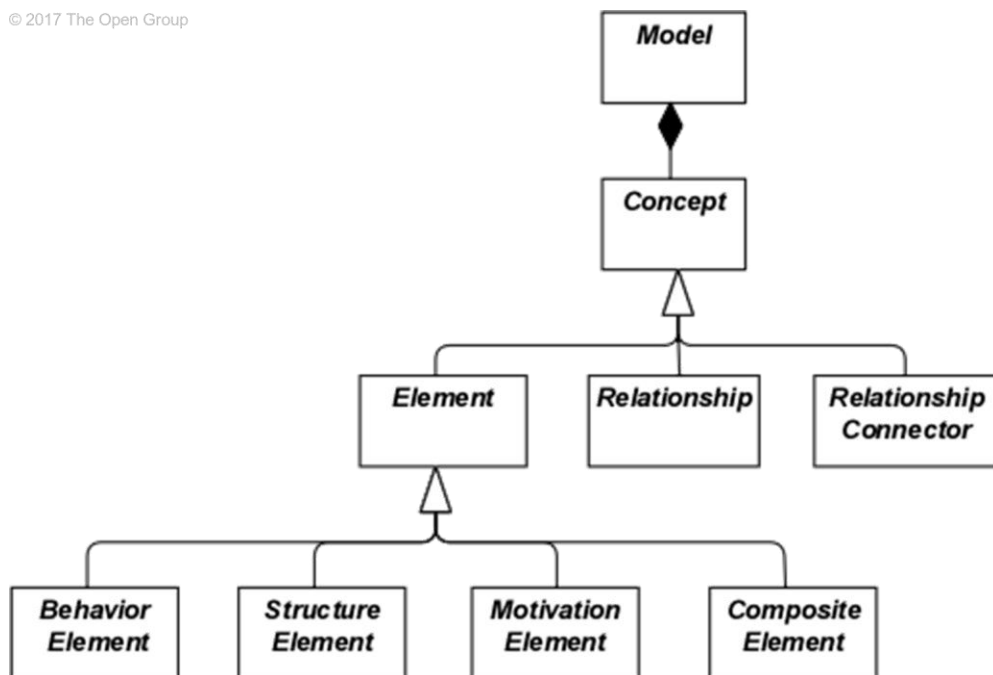


Figure 26. Top Level Concepts of ArchiMate®

1.1.2 Core Concepts

	Active Structure Concepts				Behavioral Concepts				Passive Structure Concepts	
Business	Business actor		Business role		Business process		Business service		Business object	Representation
	Business collaboration		Business interface		Business function		Business event		Product	Meaning
	Location				Business interaction				Contract	Value
Application	Application component		Application collaboration		Application function		Application interaction		Data object	
	Application interface				Application service					
Technology	Node		Device		Infrastructure function		Infrastructure service		Artifact	
	Network		System software							
	Communication path		Infrastructure interface							

Figure 27. ArchiMate® Core Concepts

1.1.3 Extensions

Stakeholder	Assessment
Driver	Goal
Requirement	Constraint
Principle	

Figure 28. ArchiMate® Extensions

1.1.4 Relationships













Structural Relationships		Notation
Association	Association models a relationship between objects that is not covered by another, more specific relationship.	Weakest Relation 
Access	The access relationship models the access of behavioral concepts to business or data objects.	
Used by	The used by relationship models the use of services by processes, functions, or interactions and the access to interfaces by roles, components, or collaborations.	
Realization	The realization relationship links a logical entity with a more concrete entity that realizes it.	
Assignment	The assignment relationship links units of behavior with active elements (e.g., roles, components) that perform them, or roles with actors that fulfill them.	
Aggregation	The aggregation relationship indicates that an object groups a number of other objects.	
Composition	The composition relationship indicates that an object is composed of one or more other objects.	Strongest relation 
Dynamic Relationships		Notation
Flow	The flow relationship describes the exchange or transfer of, for example, information or value between processes, function, interactions, and events.	
Triggering	The triggering relationship describes the temporal or causal relationships between processes, functions, interactions, and events.	
Other Relationships		Notation
Grouping	The grouping relationship indicates that objects, of the same type or different types, belong together based on some common characteristic.	
Junction	A junction is used to connect relationships of the same type.	
Specialization	The specialization relationship indicates that an object is a specialization of another object.	

Figure 29. ArchiMate® Relationships

Appendix B. Contributors and Reviewers

The following individuals reviewed and contributed to this GC Network Zoning reference architecture document.

Table 2. Reviewed and Endorsed By

Participant Full Name - Title	Participant Department - Division	Role / Contribution
Vanessa Clowe, PMP Vanessa.Clowe@cyber.gc.ca Telephone: 613-998-2837	CSE Partnership and Risk Mitigation Standards Architecture and Risk Management	Contributor/Reviewer
Mike Albert Michael.Albert@cyber.gc.ca	CSE	Contributor/Reviewer
Peter Benisson Peter.Bennison@cyber.gc.ca	CSE	Reviewer
Jim Palmer James.Palmer@cyber.gc.ca	CSE	Reviewer
David Alton David.Alton@cyber.gc.ca	CSE	Reviewer
Po Tea-Duncan 613-404-2924 Po.Tea-Duncan@tbs-sct.gc.ca	TBS/Cyber Security	Contributor/Reviewer
Rahim Charania Rahim.Charania@tbs-sct.gc.ca	TBS/Cyber Security	Reviewer

Participant Full Name - Title	Participant Department - Division	Role / Contribution
John Biro – Enterprise Architect office: 343-291-7390 mobile: 613-612-4624 john.biro@cbsa-asfc.gc.ca	CBSA/ Enterprise Architect, Technology and Security Enterprise Architecture Information Science and Technology Branch	Contributor/Reviewer
Jianmin Gao, Senior Advisor, Enterprise Architecture, CBSA Jianmin.Gao@cbsa-asfc.gc.ca	CBSA	Contributor/Reviewer
Yacin Abdallah Technical Advisor, yacin.abdallah2@canada.ca Tel.: 343-548-0839	SSC/ Chief Technology Officer Branch	Contributor/Reviewer
Oliveira, Fabien fabien.deoliveira@canada.ca	SSC/SISD (Solution Integration Services)	Reviewer
Brian McKittrick brian.mckittrick@canada.ca	Software Defined Services and Security / Digital Enablement	Reviewer
James MacLeod james.macleod@canada.ca	Security Management Group	Reviewer
LLOYD LOW lloyd.low@canada.ca	DCSB (Data Centre Services Branch)	Reviewer
Brad Matthews Senior Advisor brad.matthews@canada.ca Tel: 506-449-2536	SSC/ Engineering and Integration Networks, Security and Digital Services Branch	Contributor/Reviewer

Participant Full Name - Title	Participant Department - Division	Role / Contribution
Brent Lahaise, CISSP, CCSP Security Advisor brent.lahaise2@canada.ca Tel: 613-884-3257	SSC/ Enterprise Security Architecture Security Management & Governance, Chief Technology Officer Branch	Contributor/Reviewer
Andrew Martin Director andrew.martin@canada.ca	SSC	
Jason Boutilier Tel: 613-219-6227 jason.boutilier@canada.ca	SSC	Contributor/Reviewer
Mark McLean mark.mclean3@canada.ca	SSC-CSD (Cloud Services Directorate)	Contributor/Reviewer
Ali, Tarek tarek.ali@canada.ca	SSC- Cloud Research and Development	Reviewer
Hill, Gerald Gerald.Hill@canada.ca ,	SSC- Cloud Research and Development	Reviewer
Sylvain Bluteau sylvain.bluteau@canada.ca	SSC/CSD	Reviewer
Rob Bryce (SSC) rob.bryce2@canada.ca	SSC	
David Zinni (SSC) david.zinni@canada.ca	SSC	
Rick Cairns rick.cairns@tbs-sct.gc.ca	TBS	

Participant Full Name - Title	Participant Department - Division	Role / Contribution
Centurione, Marcello marcello.centurione@canada.ca	SSC/EA	Contributor/Reviewer
Claude Vallee	SSC/EA	Contributor/Reviewer
Walter Sokyko	SSC/NSDS	Contributor/Reviewer
Earle, Simon (Consultant assigned to Cloud Research and Development)	SSC/CSD	Contributor/Reviewer
Nguyen, Tho Tho.Nguyen@ssc-spc.gc.ca	SSC/NSDS	Reviewer
Andre Hiotis (Consultant assigned to SCED) andre.hiotis@canada.ca	SSC	Contributor/Reviewer