Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guideline

Network Security Zoning

Design Considerations for Placement of Services within Zones

ITSG-38

May 2009

This page intentionally left blank.

Foreword

The *Network Security Zoning* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

For further information or suggestions for amendments, please contact CSEC's IT Security Client Services by e-mail at itsclientservices@cse-cst.gc.ca or call (613) 991-7654 or (613) 991-8495.

Effective Date

This publication takes effect on (01/03/2009).

Originally signed by

Gwen E. Beachemin
Director, IT Security Mission Management

© 2009 Government of Canada, Communications Security Establishment Canada

This page intentionally left blank.

Executive Summary

This guideline is intended to assist network architects and security practitioners with the appropriate placement of services (for example, domain name service, email service, and web proxy service) into network security zones.

A service is a logical construct that represent a set of functional requirements in an information technology architecture. These functional requirements can be simple such as providing resolution of domain names, or complex such as processing and transmitting email. Services can be physically implemented in many ways, for example, a single process on server, multiple processes on a virtual machine, or distributed processes among pool of servers.

Concepts used in this document are based on the Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22), which describes the concepts of network security zones and specifies baseline security requirements for zone.

The network security zones in ITSG-22 covered in this guideline are:

- *Public Zone*
- *Public Access Zone*
- *Operations Zone*
- *Restricted Zone*

To assist in determining the appropriate placement of services, two typical logical zone architectures are illustrated: Internet Service network zone architecture and Departmental network zone architecture.

The primary purpose of the Internet Services network is to provide Unclassified (Protected B and below) business application delivery via the Internet to the public.

The primary purpose of the Departmental network is to deliver Unclassified (Protected B and below) business applications to public servants.

This document is a companion to Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22). This document is an input into the design process not a prescriptive design for all GC networks. The examples described in this guideline are examples only and should not be copied verbatim in any network design.

This page intentionally left blank.

Revision History

Document No.	Title	Release Date
ITSG-38	*Network Security Zoning*	*May 2009*

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

List of Tables

List of Figures

This page intentionally left blank.

List of Abbreviations

CSEC	Communications Security Establishment Canada
DNS	Domain Name Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
ITS	Information Technology Security
ITSG	Information Technology Security Guidance
OZ	Operations Zone
PAZ	Public Access Zone
PSTN	Public Switched Telephone Network
RZ	Restricted Zone
SCNet	Secure Channel Network
SFTP	Secure File Transfer Protocol
SSH	Secure Shell Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Data Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
ZIP	Zone Interface Point

This page intentionally left blank.

1 Introduction

1.1 Background

An element of the design for an IT security infrastructure is the zoning, which segments similar information technology assets (hardware, software, and data) into logical groupings that have the same security policies and security requirements.

A zone, as defined and used in this guideline, is a construct to define standard baseline security requirements that if adopted by GC departments will lead to consistency in their implementation of network security. It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defence requirements by:

- defining the entities which populate zones;
- identifying discrete entry points;
- monitoring and filtering network traffic at entry points;
- monitoring the state of the network; and
- authenticating the identity of network entities.

This document is a companion to the CSEC publication, *Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*, which describes the concepts of network security zones and specifies baseline security requirements for zones.

1.2 Purpose

The purpose of this document is to assist network architects and security practitioners with the appropriate placement of infrastructure services (for example, domain name service, email service, and web proxy service) into zones. To assist in the understanding of appropriate placement of infrastructure services, two typical logical zone architectures are illustrated:

- Internet Service network zone architecture;
- Departmental network zone architecture.

The primary purpose of the Internet services network is to provide Unclassified (Protected B and below) business application delivery via the Internet to the public.

The primary purpose of the Departmental network delivers Unclassified (Protected B and below) business applications to public servants.

1.3 Scope

The scope of this document is limited to network security zones, zone interface points (ZIPs), perimeters, and infrastructure services required for the design of zoning architecture (logical) that does not constrain the physical design.

This document addresses the following zones as specified in ITSG-22 [1]:

- Public Zone (PZ);
- Public Access Zone (PAZ);
- Operations Zone (OZ); and
- Restricted Zone (RZ).

1.4 Audience

This document is written for network architects and security practitioners within the Canadian federal government.

2 Zoning

Zoning is used to mitigate the risk of an open network by segmenting infrastructure services into logical groupings that have the same communication security policies and security requirements. The zones are separated by perimeters (Zone Interface Points) implemented through security and network devices.

Zoning is a logical design approach used to control and restrict access and data communication flows only to those components and users as per security policy. A new zone is defined by a logical grouping of services under the same policy constraints, driven by business requirements. When a new set of policy constraints are established, then a new zone is required.

Baseline Security Architecture Requirements for Network Security Zones in the Government of Canada (ITSG-22) identifies seven zones, however this guideline only covers the four most common zones shown in **Figure 1**:

- Public Zone (PZ);
- Public Access Zone (PAZ);
- Operations Zone (OZ); and
- Restricted Zone (RZ).

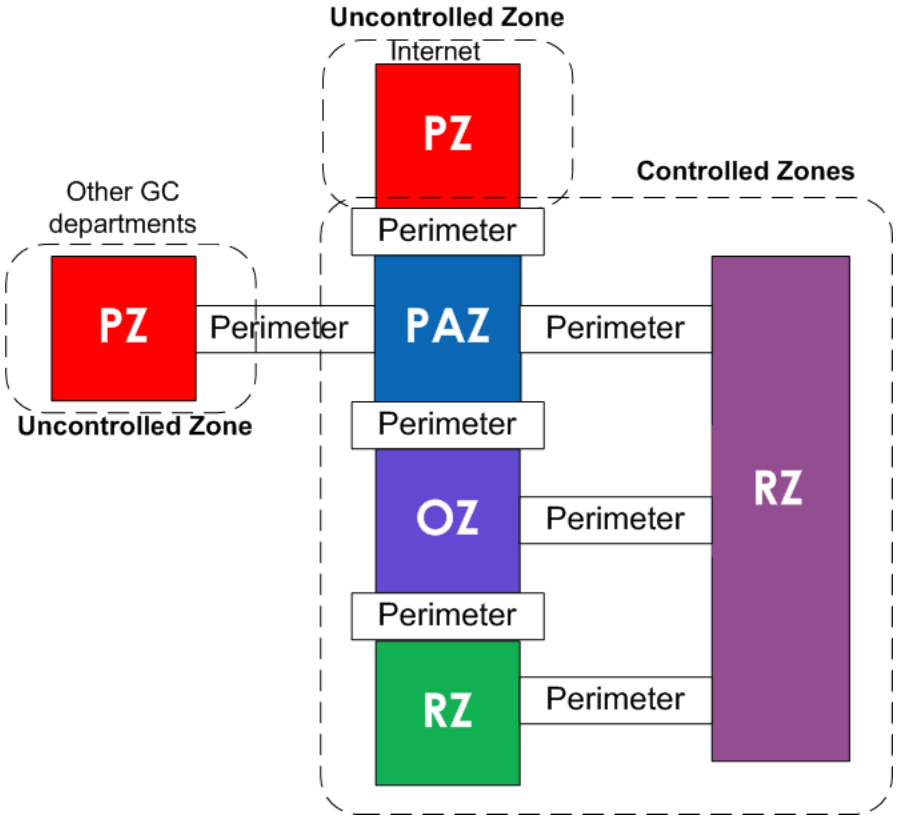

Figure 1: Sample Architecture using ITSG-22 Zones

Each zone has the following fundamental characteristics:

- Every zone contains one or more separate, routable networks;
- Every separate, routable network is contained within a single zone;
- Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs); and
- The only zone that may connect to the public zone is the PAZ.

Zones where all components are entirely within or under the control of the GC department are considered controlled zones. In the case where the GC does not control all zone components, the zone is considered uncontrolled.

Data communications entering and leaving a zone must conform to the data communication control requirements set by the policy for that zone.

2.1 Zone

A zone is a construct to define standard baseline security requirements that if adopted by GC departments will lead to consistency in their implementation of network security. It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defence requirements. As described in ITSG-22, zones achieved these network boundaries by:

- defining the entities which populate zones;
- identifying discrete entry points;
- monitoring and filtering network traffic at entry points;
- monitoring the state of the network; and
- Authenticating the identity of network entities.

2.1.1 Public Zone

The public zone is entirely open and includes public networks such as the public 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. The public zone environment is assumed extremely hostile. [4]

2.1.2 Public Access Zone

A PAZ mediates access between operational GC systems and the public zone. 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. [4]

A demilitarized zone (DMZ) is a component within a PAZ and is not discussed in this guideline.

2.1.3 Operation Zone

An OZ is the standard environment for routine GC operations and is where 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 guideline.

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 also originate from hostile insiders, from hostile code imported from the public zone, or from undetected malicious nodes on the network (for example, compromised host, or unauthorized wireless attachment to the Zone). [4]

2.1.4 Restricted Zone

An RZ provides a controlled network environment generally suitable for business-critical IT services (that is, those having medium reliability requirements, where compromise of the IT services would cause a business disruption) or large repositories of sensitive information (for example, a data centre). It supports access from systems in the public zone via a PAZ. [4]

2.2 Zone Interface Point (ZIP)

A ZIP provides a network interface between a zone and another zone. ZIPs are the logical construct used to describe the controlled interfaces connecting the zones. ZIPs enforce zone data communication policy through perimeter security measures. ZIPs are only discussed in this guideline to bridge the understanding from ITSG-22 ZIPs to perimeters.

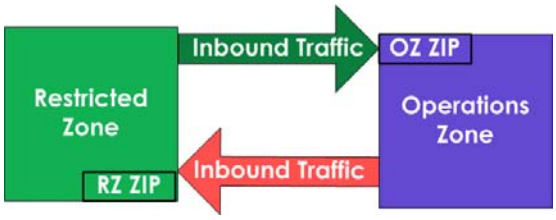

Figure 2: Zone Interface Points

ZIPs have the following fundamental characteristics:

- Every ZIP controls inbound data communication;
- ZIPs implement the security policy of their respective zones; and
- All data communication must be through a ZIP[1].

The exception to these characteristics is the ZIP required between the PZ and PAZ. The PAZ ZIP must enforce the zone policy requirements for both inbound and outbound traffic because

1 Data communication that passes through a zone without being terminated within the zone may need additional security controls

the GC has no control over the PZ and there is no PZ ZIP. This key point is illustrated in **Figure 3** below.

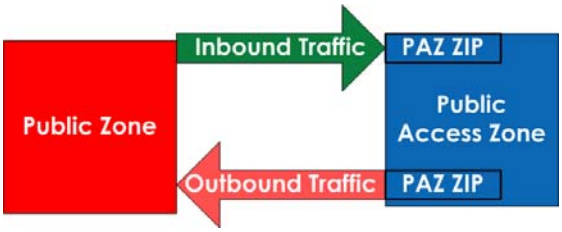

Figure 3: How a PAZ ZIP Works

In this guidance, a logical construct called a perimeter contains the ZIPs.

As shown in **Figure 4**, the perimeter contains both ZIPs (OZ and RZ ZIPs) and controls the data communication in both directions.

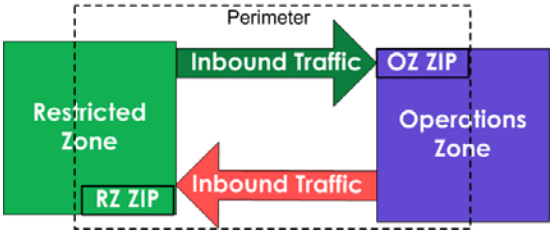

Figure 4: ZIPs Create a Perimeter

A perimeter is composed of security devices and network devices and represents the ZIPs of each adjacent zone as shown in **Figure 5.**

Figure 5: Perimeter

Using the concept of a perimeter that contains the two ZIPs simplifies the architecture diagrams, but does not change the requirements of *ITSG-22* to control data communication in both directions (inbound and outbound) for each zone**.**

2.2.1 Physical Implementation of Perimeters (or ZIPs)

Physical implementations of perimeters (or ZIPs) can be accomplished using a single component or a combination of components as shown in **Figure 6**. **Figure 6** also shows the perimeter is equivalent to the two ZIPs (for example, RZ connecting to the OZ) and the sample physical

implementation (for example, firewall, IPS, IDS, and Routers). For example, a router (a network device) may implement part of the perimeter, but it must be used in conjunction with an intrusion prevention system (a security device) and other security devices, which together provide appropriate security safeguards.

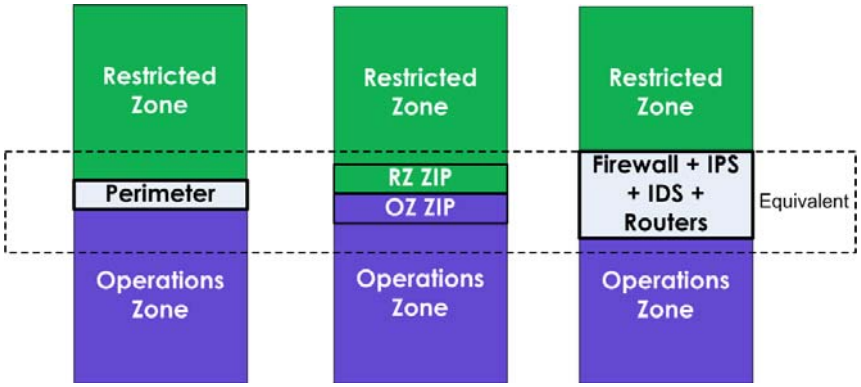

Figure 6: Perimeters, ZIPs, and Sample Physical Implementation Equivalency

Physical representations provided in **Figure 6** are examples only and do not indicate a preference of design or approach.

3 Services

A service is a logical construct that represent a set of functional requirements in an information technology architecture. These functional requirements can be simple such as providing resolution of domain names, or complex such as processing and transmitting email. Services can be physically implemented in many ways, for example, a single process on server, multiple processes on a virtual machine, or distributed processes among pool of servers.

A service can be accessed from other adjacent zones and not just the zone in which it resides.

The following list of services represents the most typical required for an IT infrastructure. The list is not exhaustive.

Table 1 List of Services

Service Name	Description
Application Tier Internet Service	The application tier (sometimes called the business layer) implements business functionality by performing calculations and making logical decisions. It also moves and process data between the data layer and presentation layer[2].
Auditing Service	The auditing service receives logs from all computer platforms (for example, hosts and servers) within the network. The auditing service generates alerts and reports related to log events for follow-up by an administrator.
Authentication Service	This service is the primary authentication service for all applications and end-users.
Backup Service	The backup service provides backup and restore capabilities for files and settings to computer platforms. Virtualization-related backup services and high availability services may be considered backup services.
Critical Data Service	Critical Data service provides file storage, and database services for large repositories of sensitive information. (See also Data Tier Internet Service)
Data Service	Data service provides file storage, and database services for large repositories of non-sensitive information.
Data Tier Internet Service	This data service stores information to be retrieved by the Application Tier Internet Service. Data Tier service provides file storage, and database services for large repositories of sensitive

[2] http://msdn.microsoft.com/en-us/library/ms978689.aspx

	information. Data Tier Service is considered the Internet Services network equivalent of the critical data service used in the Departmental network.
Desktop Service	The desktop service provides a graphical user interface (GUI) or terminal session to an end-user to access the network.
Email Proxy Service	The email proxy service provides an email proxy to the Internet for the email service and is used for all external email communications.
Email Service	The email service provides an internal email service and allows external email communication by communicating with the email proxy service.
External Domain Name Service	The external domain name service (DNS) provides a restricted set of departmental domain addresses for resolution to the internet and controls how departmental systems access the Internet DNS securely.
Extranet Service	The extranet service enables sharing of information and resources for specific business needs with authorized partners, such as other government (international and domestic), industry, and non-government organizations.
Forward Proxy (web proxy)	The forward proxy service (web proxy) supports content-based filtering of websites. Forward proxy service can allow or block websites or web content based on departmental policy.
Internal Domain Name Service	The internal DNS service provides domain names to the controlled zones (PAZ, OZ, and RZ). Internal DNS names are not published on the external DNS.
Internal Intranet Service	This service provides departmental intranets to internal users (for example, public servants).
IT Administration Service	The IT administration service encompasses the administration of all IT services.
Presentation Tier Internet Service	Presentation tier internet service provides a portal for external clients (for example, Canadian citizens) to request government services. The presentation layer provides information related to services such as web browsing, e-payment, and electronic data interchange. It communicates requests from the user/computer to the application layer.
Remote Access Service	The remote access service provides an end-user with a secure connection to the network. Remote Access services require the use of the authentication service to authenticate the end-user.

Reverse Proxy Service	The reverse proxy service routes and filters all data communication from the Internet to public facing web servers. It may provide load balancing, encryption acceleration, and protocol filtering functionality.
Security Administration Service	This service provides a central point for administration of network devices and security devices.
Time Service	Time service provides accurate time and time synchronization to computer platforms within the IT infrastructure.
Voice over IP (VoIP) Service	VoIP-enabled devices are connected to an IP network for VoIP services such as telephony.

4 Placement of Services

This section presents the Internet services network zone architecture and the Departmental network zone architecture to illustrate the placement of services.

The example architectures describe the purpose of the network, placement of services, context of the zones within the network zone architecture, and communication policies implemented in the perimeters.

4.1 Internet Services Network Example

The primary purpose of the internet services network is to provide Unclassified (Protected B and below) business application delivery via the Internet to the public. The Internet services network, illustrated in **Figure 7,** is built with four controlled zones consisting of the following:

- Data tier services RZ;
- Application tier internet services RZ;
- Management RZ; and
- the PAZ that connects to the PZ (Internet, SCNet)**.**

In this architecture, business applications are hosted within GC departments and accessed by the public through the Internet and the SCNet.

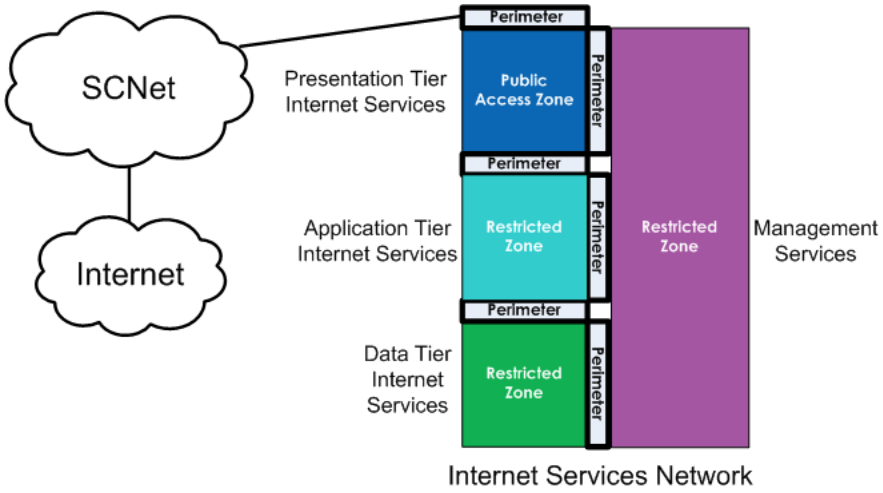

Figure 7: Context for Internet Services Network Zone Architecture

In **section 3**, a list of services was defined. For the Internet services network zone architecture, the following service are typically required:

- External Domain Name Service

- Email Proxy Service
- Reverse Proxy Service
- Presentation Tier Internet Service
- Internal Domain Name Service
- Time Service
- Authentication Service
- Email Service
- Application Tier Internet Service
- Data Tier Internet Service
- Auditing Service
- Backup Service
- IT Administration Service
- Security Administration Service

In **Table 2**, the placements of services in the four zones of Internet Services Network are listed.

Table 2: Services Locations in the Internet Services Network

PAZ	Application Tier Internet Services RZ	Data Tier RZ	Management RZ
External Domain Name Service Email Proxy Service Reverse Proxy Service Presentation Tier Internet Service	Internal Domain Name Service Time Service Authentication Service Email Service Application Tier Internet Service	Data Tier Internet Service	Auditing Service Backup Service IT Administration Service Security Administration Service

4.2 Departmental Network Zone Architecture Example

The departmental network delivers Unclassified (including Protected A or Protected B) business applications to public servants. The departmental network is built with the following zones:

- OZ;
- RZ;
- Management RZ; and
- the PAZ that connects to the public zone.

The network zone architecture for the departmental network is illustrated in **Figure 8**, where business applications are hosted within GC departmental networks and accessed by public servants. The public servants typically access their business applications from within their departmental network, or over the Secure Channel Network (SCNet) Virtual Private Network (VPN).

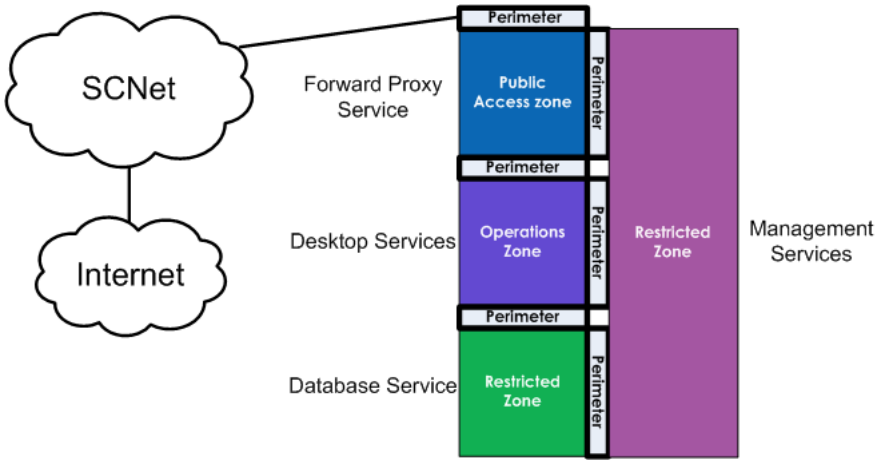

Figure 8: Context for Departmental Network Architecture

In **section 3**, a list of services was defined. For the departmental network zone architecture, the following services are required:

- Application Authentication Service
- Auditing Service
- Backup Service
- Critical Data Service
- Data Service
- Desktop Service
- Email Proxy Service

- Email Service
- External Domain Name Service
- Extranet Service
- Forward (Web) Proxy Service
- Internal Intranet Service
- IT Administration Service
- Reverse Proxy Service
- Security Administration Service
- Time Service
- Voice over IP Service

In **Table 3**, the placement of service in the four zones is shown for the departmental network:

Table 3: Services Locations in the Departmental Networks

PAZ	OZ	RZ	Management RZ
Email Proxy Service External Domain Name Service Extranet Service Forward (Web) Proxy Presentation Tier Internet Service Remote Access Service Reverse Proxy Service	Authentication Service Data Services Desktop Service Email Service Internal Domain Name Service Internal Intranet Service Time Service Voice Over IP Service	Critical Data Services	Auditing Service Backup Service IT Administration Service Security Administration Service

4.3 Context for Departmental and Internet Services Networks

For the zone architecture for Departmental and Internet services networks, each zone has a specific purpose and defined set of characteristics. In the following sub-section, the four types of zones will be described in the context of the Departmental network zone architecture and Internet services network zone architecture. These architectures are illustrated in **Figure 9** and **Figure 10** respectively.

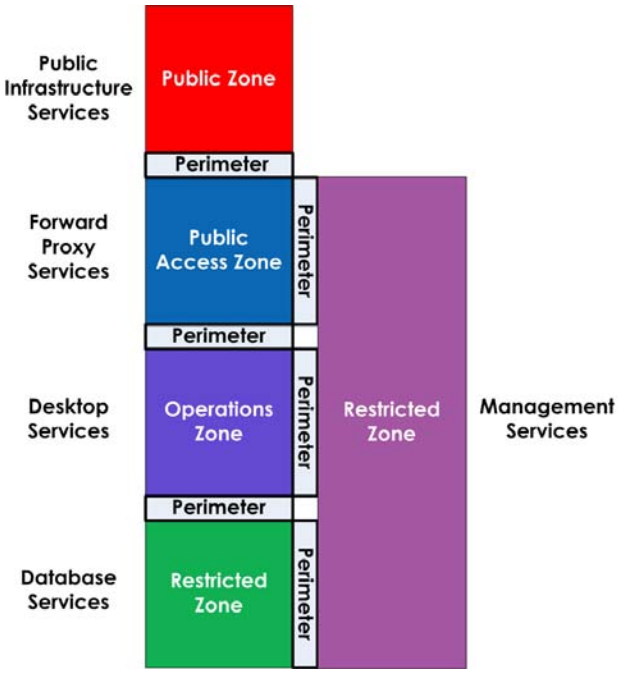

Figure 9: Departmental Network Zone Architecture

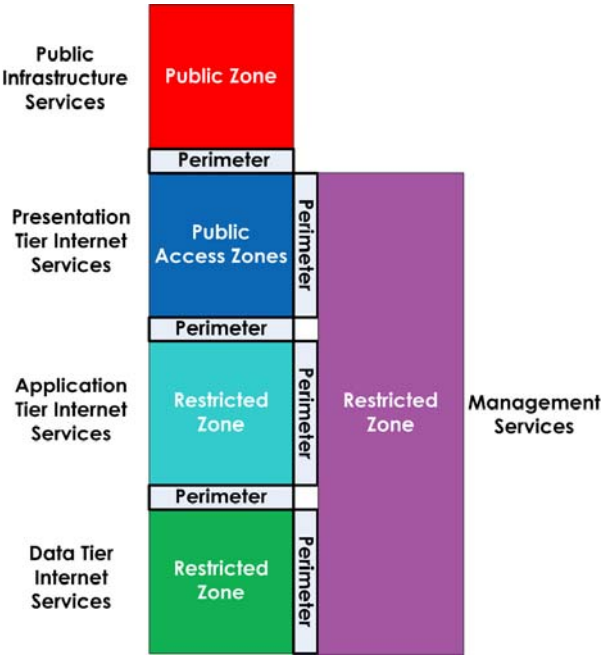

Figure 10: Internet Services Network Zone Architecture

4.3.1 Public Zone

Public zones are part of the global information infrastructure (Internet). Public carrier backbone networks like the Secure Channel Network and private lines are considered uncontrolled and are therefore treated as public zones because these networks are not owned, managed, and physically controlled by the GC.

4.3.2 Public Access Zone

4.3.2.1 Usage

The public access zone (PAZ) contains internet related services for external clients. It does not retain any sensitive information, but passes it across the network to other zones. Sensitive information is stored in other zones that are not directly connected to the public zone. The PAZ perimeter to the public zone implements security safeguards that protect PAZ services in the controlled zones (PAZ, OZ, and RZ).

4.3.2.2 Communication Policy to/from the Public Zone

All inbound communication terminates at a service such as a proxy service or email service within the PAZ after being processed at the perimeter.

All other inbound communication that does not terminate at an IT service within the PAZ is blocked.

In some circumstances there may be no proxy service available to terminate specific protocols in the PAZ. This circumstance applies primarily, but not exclusively, to encrypted protocols such as TLS (Transport Layer Security) and SFTP (Secure File Transfer Protocol). A risk assessment should be performed to determine the risks associated with terminating such traffic in the OZ, and the requirement for additional security controls.

All inbound and outbound communication to the public zones should be restricted by blocking network addresses using a black list. Black lists contain a list of public zone network addresses which are unallocated, or are a well-known source of malicious data and/or communication. Black lists are provided through commercial vendors, carriers, and government agencies.

All outbound communications must be filtered so that only valid internal department address ranges are allowed to communicate to the PZ.

4.3.2.3 Communication Policy to/from the Operations Zone and Restricted Zone

All communication between the PAZ and the other controlled zones (OZ and RZ) should be processed by the perimeter and white listed. In case of a departmental network, the OZ email service can only communicate with the PAZ email proxy service. The OZ desktop service must use the PAZ web proxy service, which in turn communicates with the PZ web services. **Figure 11** illustrates the communications paths from the PZ to the RZ.

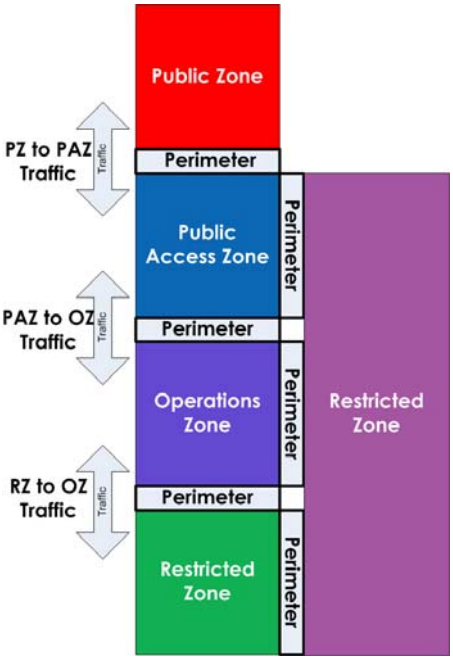

Figure 11: Departmental Network Communications Flows

4.3.2.4 Communication Policy to/from the OZ, PAZ, RZ to Management RZ

All communication between the RZ management zone and the other controlled zones (PAZ, OZ, and RZ) should be processed by the perimeter and white listed. **Figure 11** illustrates the communications paths from the PZ to the RZ.

4.3.3 Operations Zone

4.3.3.1 Usage

Most government activities take place in the controlled zone. OZ systems are allowed filtered access to the PZ for legitimate government activities. OZ computer platforms accessing the PZ will be filtered by Internet proxy services and perimeters in the PAZ.

For example, workstations, printers, and VoIP terminals would be located in the OZ.

4.3.3.2 Communication Policy to/from the Public Zone

OZ services do not communicate directly with the public zone. Encrypted IT service examples such as SSH and HTTPS cannot be properly proxied through the PAZ and should either be denied or white listed using access controls.

White listing is enforcing a set of approved addresses and protocols. A risk assessment should be performed to assess the risk to the network if a protocol cannot be terminated within the PAZ through a proxy.

If the risk assessment results are acceptable to the department, then communications may go through the PAZ and terminate within the OZ.

4.3.3.3 Communication Policy Inbound from the Public Access Zone and Restricted Zone

All communication between the OZ and other controlled zones (RZ and PAZ) should be processed by the perimeter and white listed. The desktop service (web browsing for example) should only communicate with the PAZ web proxy service.

4.3.4 Restricted Zone

4.3.4.1 Usage

Restricted zones (RZs) contain services for the Departmental and Internet services network operations that require additional safeguards from threats originating from the controlled zones.

For the departmental network, critical data services that need to be protected from the OZ are located in the restricted zone.

The data tier internet services are located in the restricted zone (3rd layer)[3]. This configuration was illustrated in **Figure 10** on page 27. In certain commercial-off-the-shelf applications, the application and data tier services may be bundled in a single product. This restriction would necessitate that the application and data service be deployed in the RZ (2nd tier) instead of an RZ (3rd Tier). The three layer approach is the preferred security architecture because a perimeter can be placed between the application and the database services.

3 A common *three-tier* architecture based on a presentation, application (logic), and data layers can be zoned using a PAZ, a 2nd tier restricted zone, and a 3rd tier restricted zone.

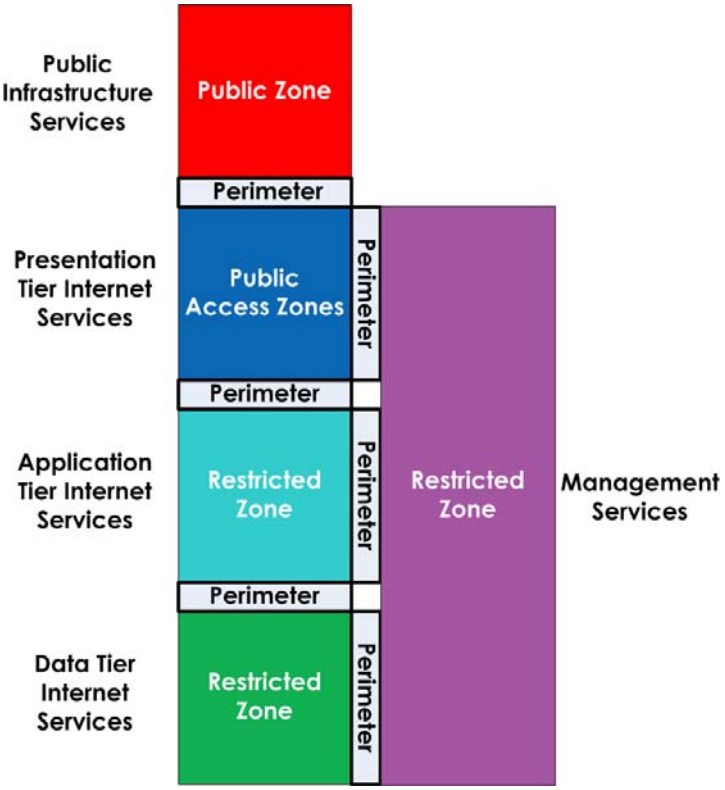

Figure 12: Internet Services Network Architecture

4.3.4.2 Communication Policy Inbound from the Public Zone

RZ services do not communicate with the public zone directly.

4.3.4.3 Communications Policy Inbound from the Operations Zone and Public Access Zone

All communication between the RZ and other controlled zones should be processed by the perimeter and white listed. RZs only communicate directly with the OZ and the other RZs. The exception is if the RZ is the management RZ which also communicates with the PAZ.

4.3.5 Management Restricted Zone

4.3.5.1 Usage

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.

4.3.5.2 Communication Policy to/from the Public Zone

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.

4.3.5.3 Communication Policy to/from the OZ, PAZ, and RZ

All communication between the RZ and other controlled zones should be processed by the perimeter and white listed. The management RZ communicates with all controlled zones (OZ, RZ, and PAZ).

4.3.6 Application Tier Internet Services Restricted Zone

4.3.6.1 Usage

Departmental and Internet services network architectures have a restricted zone designed specifically for the application tier internet services called the application tier internet services RZ. This zone contains application tier internet services.

4.3.6.2 Communication Policy to/from the Public Zone

Management RZ services only communicate with the public zone via the PAZ for updates from controlled vendor network sites using appropriate security controls that protect integrity and confidentiality of the communication and authenticate the controlled vendor network address.

4.3.6.3 Communication Policy to/from the OZ, PAZ, and RZ

All communication between the RZ and other controlled zones should be processed by the perimeter and white listed. The management RZ communicates with all controlled zones (RZs and PAZ).

This page intentionally left blank.

Glossary

Black list	An access control list that is based on the premise to deny only what is known to be harmful and allow everything else.
Computer network	A collection of [IT] systems together with the sub network or Internetwork through which [IT] systems can exchange data. [2]
Computer Platform	A combination of computer hardware and an operating system (which may consist of software, firmware, or both) for that hardware. [2]
Detection	Sensing and analyzing system events for the purpose of noticing (that is becoming aware of) attempts to access system resources in an unauthorized manner.
End-System	A system [computer platform] that, for a particular instance of communication, is the ultimate source or destination of the communication. [4]
End-user Systems	End-systems for human operations. For example, a desktop consisting of a personnel computer (display, keyboard, mouse, and an operating system). This is equivalent to computer platform.
Firewall	A gateway that enforces a boundary between two networks and that is used to isolate, filter, and protect local system resources from external connectivity by controlling the amount and kinds of traffic that may pass between the two. [4]
Gateway	An intermediate system that is the interface between two computer networks. (Reference [2])
Government of Canada IT Infrastructure	All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, control or support IT services for the Government of Canada. The term IT infrastructure includes all of the information technology but not the associated people, processes and documentation. [5]
Host	A networked computer that does not forward IP packets that are not addressed to the computer itself. [2]
Internet	The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers. [2]
IT system	A group of independent but interrelated elements comprising a unified whole, working together to perform certain tasks that process, store or transmit information. The IT system can be small (for example, embedded system, computer platforms, and network devices) or large (for example, an IT infrastructure, and an intranet).
IT infrastructure	All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, control or support IT services. The term IT infrastructure includes all of the information technology but not the associated people, processes and documentation. [5]

Service	A service is a logical construct that represent a set of functional requirements in an information technology architecture. These functional requirements can be simple such as providing resolution of domain names, or complex such as processing and transmitting email. Services can be physically implemented in many ways, for example, a single process on server, multiple processes on a virtual machine, or distributed processes among pool of servers.
Malicious traffic	Any data transmitted over a network that can do harm to the availability, integrity or confidentiality to systems or the systems' data.
Network device	A device whose primary purpose is to provide network functionality such as a router or switch.
Network Security Zone	It demarcates a logical area within a networking environment with a defined level of network security. Zones define the network boundaries and their associated perimeter defence requirements.
Network Security Zoning	Zoning is a logical design approach used to control and restrict access and data communication flows only to those components and users as per security policy.
Perimeter	The boundary between two Network Security Zones through which traffic may be routed.
Protocol	A set of rules (formats and procedures) to implement and control some type of association (for example, communication) between systems. An example of a protocol is the Internet protocol. [2]
Proxy Service	An application-service inter-networking function, which may be incorporated in a firewall, and which provides, to the client, replication of services available on other servers. To the client, the proxy appears to be the server, while to the server it appears to be the client. When incorporated in a firewall, a proxy service is often referred to as an application gateway firewall. [4]
Security controls	Security controls are safeguards that are designed and implemented to meet security requirements. They are a logical abstraction of security requirements, specified independently of the physical mechanism used to deliver them.
Security device	A device whose primary purpose is to provide security functionality.
Server	Any computer platform whose primary purpose is to provide services to other computer platforms. Servers and workstations are defined as computer platforms in this guidance.
Virtual Private Network	A virtual private network (VPN) is a computer network that may share physical communication links with other computer networks, but are separated logically.
White List	An access control list that is based on the premise that only what is explicitly defined is allowed and everything else is denied.
Zone	See Network Security Zone.
Zone Interface Point	An interface between two Network Security Zones through which traffic may be routed. [4]

Bibliography

[1] National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Committee on National Security Systems, National Security Agency, June 2006 [cited 6 November 2006]. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[2] Internet Security Glossary, Version 2 http://tools.ietf.org/rfc/rfc4949.txt

[3] Baseline Security Architecture for GC IT Infrastructures, Communication Security Establishment Canada. 2009.

[4] ITSG-22, Baseline Security Requirements for Network Security Zones in the Government of Canada, Communications Security Establishment. Canada. 2007

[5] ITIL® V3 Glossary v01, 30 May 2007,

http://www.best-management-practice.com/gempdf/ITILV3_Glossary_English_v1_2007.pdf

[6] NIST SP 800-53 rev 3 - Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technologies. February 2009.

[7] SHIREY, Robert W. Request for Comments: 2828 – Internet Security Glossary [online]. The Internet Society, May 2000 [cited 25 January 2006]. Available from World Wide Web: <http://www.ietf.org/rfc/rfc2828.txt>.

This page intentionally left blank.