Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Baseline Security Requirements for Network Security Zones in the Government of Canada

(ITSG-22)

June 2007

Canada

This page intentionally left blank.

Foreword

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 (CSEC).

This publication is effective upon receipt and supersedes *IT Security Zones Baseline Security Requirements* (ITSD-02, May 2003) and *Directives for the Application of Baseline Security Requirements for Network Security Zones in the Government of Canada* (ITSD-02) (Draft-only revision of ITSD-02, June 2006).

This publication is distributed as a Guidance document. The guidance provided herein is intended to help departments and agencies satisfy the requirements of the *Government Security Policy* (GSP, February 2004) and the *Operational Security Standard: Management of Information Technology Security* (MITS, April 2004).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at mailto:itsclientservices@cse-cst.gc.ca or call (613) 991-7654.

This publication takes effect on June 2007.

Originally signed by

Gwen Beauchemin
Director, IT Security Information Management

This page intentionally left blank.

Executive Summary

This Guidance document is intended to outline the baseline security requirements for achieving Network Security within the Government of Canada, in accordance with the Government Security Policy (February, 2004) and the Operational Security Standard: Management of Information Technology Security (April, 2004).

This is a technical document, intended for readers familiar with the principles and terminology of network engineering.

The network security Objectives and Requirements defined in this document are based on the implementation of a Network Security Zones model, where security policies between and within Zones are defined and enforced.

There are 7 Network Security Zones defined within the model:

1. *Public Zone*
2. *Public Access Zone*
3. *Operations Zone*
4. *Restricted Zone*
5. *Highly Restricted Zone*
6. *Restricted Extranet Zone*
7. *Special Access Zone*

The Zones are defined to minimize network complexity, to ensure effective and efficient delivery of network services, to promote interoperability and to provide a consistent level of security for services provided within and across Zones. Zones boundaries are well-defined and respect assigned accountabilities for network security.

The security Objectives and Requirements detailed herein define the internal configuration and management issues for each Zone, to a level that is granular enough to be implemented. The Objectives and Requirements also define how to connect one Zone to another, or whether a direct connection between certain Zones is advisable.

This document is a companion to Network Security Zoning Design - Considerations for Placement of Services within Zones in the Government of Canada (ITSG-38) which is intended to assist network architects and security practitioners with the appropriate placement of services into network security zones. [3]

This document is not intended to provide advice or guidance on how to secure a host platform or an application. Compliance with the contents of this Guidance document is not sufficient to adequately secure an entire IT environment, but will provide a baseline security level for the network itself.

This page intentionally left blank.

Revision History

Document No.	Title	Release Date
ITSG-22	Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)	April 2013 *Revisions made to references only.
ITSG-22	Added references to ITSG-38	October 2013

This page intentionally left blank.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Acronyms

ANR	Address and Name Resolution (appears only in figures)
AP	Access Point (wireless)
App	Application (appears only in figures)
Auth.	Authentication (appears only in figures)
CAVP	Cryptographic Algorithm Validation Program
CDRL	Contract Data Requirements List
CEP	Cryptographic Endorsement Program
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment Canada
DDoS	Distributed Denial-of-Service
Dept.	Department (appears only in figures)
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial-of-Service
DP	Data Protection (requirement)
DSA	Directory Service Agent
EAN	External Access Network
EIA	Electronic Industries Alliance
FAA	Financial Administration Act
FIPS	Federal Information Processing Standard
FOLDOC	Free On-Line Dictionary of Computing
FTP	File Transfer Protocol
GC	Government of Canada
GSP	Government Security Policy
HC	Host Configuration (requirement)
HRZ	Highly Restricted Zone
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification and Authentication
IAN	Internal Access Network
IBS	Internal Boundary System
ICMP	Internet Control Message Protocol

IDS	Intrusion Detection System (appears only in figures)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Security (IT Security)
ITSG	Information Technology Security Guidance
LAN	Local Area Network
MAC	Media Access Control
MITS	Management of Information Technology Security
NAT	Network Address Translation
NC	Network Configuration (requirement)
NI	Network Interface (requirement)
NTP	Network Time Protocol
OBJ	Objective
OGD	Other Government Department
OSI	Open Systems Interconnection
OZ	Operations Zone
PAT	Port Address Translation
PAZ	Public Access Zone
PKI	Public Key Infrastructure
PoP	Point of Presence
PSTN	Public Switched Telephone Network
PWGSC	Public Works and Government Services Canada
PZ	Public Access Zone (in a security objective or requirement)
REZ	Restricted Extranet Zone
RF	Radio Frequency
RFC	Request for Comments
RZ	Restricted Zone
SAZ	Special Access Zone
SCNet	Secure Channel Network
SPAN	Switched Port Analyzer

SVPN	Secure Virtual Private Network
SYN	Synchronization packet
TBS	Treasury Board of Canada Secretariat
TC	Traffic Control (requirement)
TCP	Transmission Control Protocol
TRA	Threat and Risk Assessment
U.S.	United States
UTM	Unified Threat Management
VA	Vulnerability Assessment
VPN	Virtual Private Network
ZIP	Zone Interface Point

This page intentionally left blank.

1 Introduction

1.1 Purpose and Application

This Guideline describes the concepts and philosophy of network security and Network Security Zones and gives models for applying Network Security Zones. It also specifies baseline security requirements for the Public Access Zone (PAZ), the Operations Zone (OZ), the Restricted Zone (RZ), and the Highly Restricted Zone (HRZ). Requirements for the Special Access Zone (SAZ) and the Restricted Extranet Zone (REZ) will vary on a case-by-case basis, so this Guideline addresses them in general terms only.

This Guideline will help departments and agencies satisfy requirements of the *Government Security Policy* (*GSP*; reference [19]) and the *Operational Security Standard: Management of Information Technology Security* (*MITS*; reference [27]) that relate to network security. Implementation of these baseline security requirements will promote a consistent level of network security across the Government of Canada (GC) to support secure network interconnectivity and interoperability.

The scope of this Guideline is the network security provided by Network Security Zones. Network security includes more than Zones, and information technology (IT) security includes other disciplines besides network security, such as management controls and technical and operational safeguards for the prevention of, detection of, and recovery from security incidents (see the *MITS* standard and Section 3.2 of this Guideline for more details). Complying with the content of this Guideline is not, by itself, sufficient to adequately secure an IT environment. For further guidance on network security and on other matters of IT security (ITS), departments should contact IT Security Client Services at the Communications Security Establishment Canada (CSEC).

1.2 Related Work

The implementation suggestions presented in this Guideline satisfy requirements of the *GSP* and the *MITS* as they relate to network security. In accordance with the *GSP* and the *MITS*:

“Assets must be safeguarded according to baseline security requirements and continuous risk management; and continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous risk management [Section 4 of the *GSP*].”

“Departments must comply with the baseline requirements of this policy and its associated operational standards and technical documentation. These requirements are based on integrated assessments of threats and risks to the national interest and to GC employees and assets. Departments must conduct their own Threat and Risk Assessments (TRAs) to determine the necessity of safeguards above baseline levels [Section 10 of the *GSP*].”

“Departments must apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery requirements and threats to confidentiality, availability or integrity increase [Section 13 of the *MITS*].”

“Departments must segregate networks into IT security zones and implement perimeter defence and network security safeguards [Section 16.4.6 of the *MITS*].”

Network Security Zones create a foundation for a balanced and layered security architecture that can support a range of security solutions for GC business needs. Network Security Zones also provide a foundation for implementing a common network infrastructure to support Electronic Service Delivery, interconnectivity, and interoperability across the GC. Departments that share in the common infrastructure for on-line service delivery and other purposes must conform to all security standards established for that infrastructure.

1.3 Document Overview

The main body of this Guideline consists of five main sections. Following that is a set of Annexes that give proposed baseline security requirements for the Network Security Zones.

Section 1 (this section) is an introduction to the Guideline. Section 2 describes the basic concepts and philosophy of Network Security Zones. Section 3 explains how Network Security Zones fit into the larger ITS context. Section 4 introduces and explains the seven Network Security Zones. This section also describes a generic Network Security Zone and the components of such a Zone. Finally, Section 5 contains a glossary that defines terms used in this Guideline.

Annexes A through D contain models and baseline security requirements for the most common Network Security Zones: the Public Access Zone (Annex A), the Operations Zone (Annex B), the Restricted Zone (Annex C), and the Highly Restricted Zone (Annex D). The remaining Zones either are outside the scope of the GC (the Public Zone) or must be specified on a case-by-case basis to suit local circumstances and business needs. The security objectives and requirements in this Guideline are uniquely numbered. The numbering scheme was originally defined in the previous version of this document (ITSD-02 [39]) and has been maintained and expanded upon. Annex E gives guidance on implementing Zones. Annex F gives a mapping of requirement numbers from ITSD-02 to ITSG-22, and indicates where changes have occurred. Future versions of this Guideline should not change the sequence number of any objective or requirement; new objectives or requirements should extend the existing number sequence; rescinded objectives or requirements should be so marked.

1.4 How to Read this Guideline

This is a technical document and is not intended for non-technical readers. Readers should be familiar with the principles, standards (e.g., reference [21]), and terminology of network engineering.

The core content of this Guideline is in the defined requirements contained in Annexes A through D. The requirements are identified by structured sequence numbers contained in square brackets. All other text in the Annexes and in the main body of this Guideline is explanatory and supports the requirements.

The numbered statements in Annexes A through D are divided into two main types: objectives and requirements. Objectives identify what departments will achieve by meeting the stated requirements. Finally, objectives provide a way to analyze the validity of the requirements. The requirements are the detailed criteria that govern how a “zoned” network could be implemented and how it should function.

Each Annex addresses a single type of Network Security Zone and is intended to stand alone in defining the requirements for instances of that type of Zone. Certain core text that supports the requirements appears in each Annex to ensure that readers understand the context and intent of the requirements.

When reading the requirements, readers seeking further clarification should read the associated Zone-specific reference model in the appropriate Annex. For further clarification on the reference model, readers should read Section 4 of this Guideline.

The requirements in this Guideline are functional and serve to outline baseline, or minimum, security requirements. Departments selecting and deploying technology products that implement the defined functionality should reasonably expect to achieve the baseline security requirements. They may also deploy products that implement features and functions beyond those that this Guideline specifies. Departments should not read this Guideline as constraining the types of network security products they may use.

1.5 Terminology

The term *security*, where not otherwise qualified, refers to network security.

The term *Zone* (capitalized), where not otherwise qualified, refers to a *Network Security Zone*.

The layer notation (e.g., “network layer”) is that used in the International Organization for Standardization (ISO) standard 7498-1:1994, *Open Systems Interconnection – Basic Reference Model* (reference [22]).

The term *Internetwork* has the meaning given in the Glossary (Section 5).

The terms *department* and *departmental* refer to all GC departments and agencies listed in Schedule I, Schedule I.1, and Schedule II of the *FAA* (reference [13]).

Words or phrases appearing in blue, underlined text (except in Section 6 References) are defined in the Glossary (Section 5). In electronic versions of this Guideline, they are also hyperlinks that link to the Glossary definitions. Such formatting is used the first time a defined word appears in any section or Annex of this Guideline.

2 Basic Concepts and Philosophy

2.1 Information Technology (IT) Security

According to the *GSP* (reference [19]), ITS is "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information." ITS is a broad field that contains many specialities, one of which is network security.

2.2 Network Security

Today's pervasive interconnectivity between networks, and in particular connectivity to the public Internet, exposes non-public networks to a hostile environment of rapidly evolving threats. Connections to other networks (such as to public data carriers or the public Internet) provide convenient channels through which external entities can imperil internal End-Systems. In addition, internal network users can deliberately or inadvertently threaten the network and its End-Systems through their actions. If an internal node on the network is compromised, it can become a threat to the rest of the network.

Network security is the measures taken to reduce the susceptibility of a network to these sorts of threats. Broadly speaking, network security has three fundamental objectives:

a. to protect the network service;

b. to reduce the susceptibility of End-Systems and applications to threats originating from the network; and

c. to protect data during transmission across the network.

Network security counters both external and internal threats with a full suite of security safeguards to address risks to the network. These safeguards include the following:

a. physical and environmental safeguards to protect network equipment and media;

b. technical controls within the network infrastructure to reduce its susceptibility to security threats;

c. controls applied within lifecycle processes to limit the vulnerability of the network infrastructure to security threats; and

d. information security operations to detect, contain, respond to, and recover from security incidents.

Network security controls threats from external networks primarily through safeguards deployed at external network interfaces. Inside the network security perimeter, safeguards that are designed to detect, contain, respond to, and recover from attacks control threats from insiders and provide in-depth defence against external threats.

Network security protects data in transit by controlling access to network media, by deploying cryptographic security measures within the network, and by facilitating the deployment of cryptographic security measures within application systems and the distributed computing environment.

Network security can reduce the susceptibility of End-Systems to threats from external and internal entities by filtering malware and invalid network traffic, detecting suspicious traffic patterns, raising alarms, and blocking or terminating threatening connections. However, valid data streams often carry threats to the information infrastructure. In these cases, there is a limit to the ability of network security controls to mitigate risks to End-Systems because those controls can address threats only if they can detect threats in the network traffic. Platform safeguards, distributed computing safeguards, and application security safeguards should be deployed to address the additional threats. These other types of safeguards are outside the scope of network security and of this Guideline.

The baseline security requirements and guidance specified in this Guideline respond to network-related threats and vulnerabilities. They do not constitute a complete security solution; they are one part of a complete ITS solution. See Section 3 for more on this issue. In addition, contact IT Security Client Services at the CSEC for information and guidance on other aspects of ITS.

2.3 The Concept of Network Security Zones

2.3.1 Introduction to the Concept

A *Network Security Zone*, as defined and used in this Guideline, is a construct to implement security consistently across an interconnected network environment. 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. This is achieved by:

a. defining the entities which populate Network Security Zones;

b. identifying discrete entry points;

c. filtering network traffic at entry points;

d. monitoring the state of the network;

e. authenticating the identity of network entities; and

f. monitoring network traffic at the entry points.

The concept of Network Security Zones is limited to the network environment. The use of the Zones is intended to reduce the threat to End-Systems and applications. A Zone is not intended to meet all of the information management and IT requirements to safeguard End-Systems, applications, or data. To achieve a sound overall security posture, Zones must be used in conjunction with additional safeguards such as platform, application, and administrative security controls. Within a Zone, these additional safeguards can be implemented based on assumptions about the network security environment, including:

a. the level of trust in entities present in the network environment;

b. the nature of network traffic entering and exiting the environment;

c. the nature of traffic within the environment;

d. the security services available to protect communications; and

e. the robustness of the network environment.

2.3.2 Inspiration – Physical Security Zones

The Network Security Zone is analogous to the well-established concept of a physical security zone as defined in the GC's *Operational Security Standard on Physical Security* (reference [26]). A physical security zone is an area within a well-defined perimeter and assumptions can be made concerning the threat present within the zone. The *Operational Security Standard on Physical Security* identifies five types of physical security zones (Public Zone, Reception Zone, Operations Zone, Security Zone, and High Security Zone). The small number of zone types limits the complexity of the standard and simplifies the choices available to facility providers, yet meets the vast majority of security needs.

Physical security zones are distinguished by the strength of perimeter defence, the degree of control over the entities (individuals and equipment) allowed in the zone, the degree to which movement within the zone is monitored, and the trust assigned to individuals allowed in the zone. Physical security zones are nested, in the sense that people cannot enter a more protected zone without first passing through the more open zones and the security controls at the boundaries between zones. Generally, as one progresses through the physical security zones from most open to most protected, the number of people permitted to enter the next zone decreases and those people should submit to increased scrutiny of their persons and their actions.

An important concept in physical security zones relates to the handling and storage of sensitive information within the zones. A physical security zone provides a certain level of inherent security. For less sensitive information, that inherent security may be sufficient for handling and storing that information. For information that is more sensitive, that same inherent security may not be sufficient. This does not mean that sensitive information may not be handled in such a zone. It means that *additional* security measures, beyond those provided by the physical security zone itself, are required. However, if that same information were moved to a more protected physical security zone, then those additional security measures might not be needed. The additional requirements depend on the combination of the information's sensitivity and the inherent security level of the physical security zone.

2.3.3 Details of the Concept

The concepts involved in physical security zones were used as a starting point to develop the Network Security Zone Implementation Model (Section 4.2). For example, just as the number of physical security zones is limited, so too is the number of Network Security Zones. This limits the complexity of available choices, while meeting the majority of security needs. Therefore, this Guideline identifies the following Zones:

a. Public Zone;

b. Public Access Zone (PAZ);

c. Operations Zone (OZ);

d. Restricted Zone (RZ);

e. Highly Restricted Zone (HRZ);

f. Restricted Extranet Zone (REZ); and

g. Special Access Zone (SAZ).

Annexes A through D, respectively, describe the PAZ, OZ, RZ, and HRZ.

The Zones were chosen in an effort to minimize network complexity and ensure effective and efficient delivery of network services. Using a small number of network security environments, networks can be built to accommodate the computing needs of the GC independent of the intricacies of specific applications or business processes. In a manner similar to the physical security context, a department or agency can choose to use a Zone with more security to ease the security burden on attached hosts and supported applications. Alternatively, it can choose a Zone with less security and apply additional controls to the hosts and applications supported by the Zone.

The Network Security Zone model differs from the physical security zone model in one important respect. Unlike physical security zones, Network Security Zones are not nested; rather Network Security Zones are organized in a network model. Figure 1 below illustrates this difference.

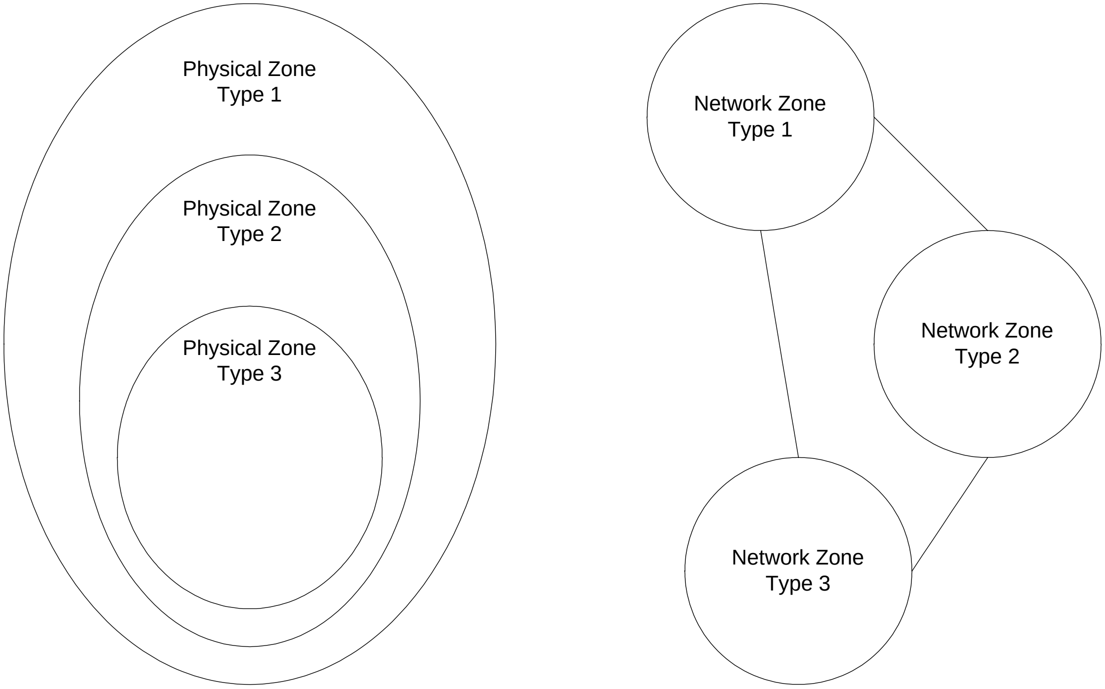


Figure 1 – Physical vs. Network Security Zones

On the left of Figure 1 is a set of nested physical security zones. The only way to reach a Type 3 physical security zone is by going through the Type 1 and Type 2 zones in sequence. On the right side of Figure 1 is a set of Network Security Zones. These Zones are networked, not nested. Thus, it is possible to reach a Type 3 Zone directly from a Type 1 Zone, without going through a Type 2 Zone (although this may be possible as well). The specific connectivity between different types of Zones will depend on the needs of the implementing department.

It is important to understand that a Zone does not inherently provide security for multiple sensitivity levels[1] of information and other assets. An IT environment that handles multiple levels of sensitive information requires controls that are beyond the scope of Network Security Zones, so this Guideline does not address them. This Guideline does detail, however, certain requirements for a Zone that sends Protected C or classified information to another Zone.

2.4 Objective for Network Security Zones

The objective of Network Security Zones is to develop a consistent, GC-wide, network security environment that:

[1] "Sensitivity" in this context means sensitivity in terms of confidentiality, availability, and integrity. This is broader in meaning than the term "classification", which refers specifically and only to sensitivity in terms of confidentiality. See also the definition of sensitive in Section 5.

a. establishes baseline requirements while providing departments flexibility to meet their specific security obligations;

b. promotes interoperability and network interconnectivity; and

c. provides a consistent level of security for platforms and applications within a given Zone.

2.5 Principles for the Network Security Zones Model

The objective for Zones (Section 2.4) is met by applying the following principles to the development of the architecture and baseline requirements.

2.5.1 Consistent Level of Susceptibility to Network Threats

Zones support a variety of security solutions to reflect differences in the criticality of assets and levels of risk involved in meeting a range of business requirements. Each type of Zone has a specific security target in terms of susceptibility to network threats. The level of susceptibility depends on the frequency, types, and severity of network threats to which an End-System within the Zone would be exposed. Similarly, when two Zones are connected, controls are established at the interface to maintain the consistent level of susceptibility within each connected Zone.

Threats, vulnerabilities and assets should be periodically reviewed, and the Threat and Risk Assessment (TRA) updated accordingly, within the Continuous Risk Management framework implemented within each Zone.

2.5.2 Respect for Accountabilities

Zone boundaries respect assigned accountabilities for network security. Network boundaries are determined primarily by the allocation of accountabilities. A Network Security Zone Authority is accountable for security within the Zone. The Network Security Zone Authority should be responsible for ensuring regular TRAs are performed, and that the results are incorporated into the Zone implementation and/or modifications. There should be a process in place for the sharing of threat and vulnerability information with other GC infrastructure owners, to ensure that a consistent level of security within each Zone is maintained (and that security across Zone boundaries is not compromised). The process for sharing this information should include a definition of the responsibilities of those authorized to send and/or receive the information and a plan for responding to the data received (e.g. how to respond to a heightened security level). Considering this, each Network Security Zone Authority should have sufficient control over interfaces with other Zones to be able to react to security incidents and to ensure due diligence to prevent security incidents. Control over interfaces with other Zones must be balanced against the need for interoperability.

If a department authorizes the use of an outsourced commercial provider to manage any portion of a Zone (services, interfaces, etc), the commercial provider’s site, personnel and processes should not compromise the security objectives of that Zone. The Network Zone Authority is responsible for ensuring the security objectives (as dictated by business requirements and TRA results) are maintained, within the terms of the contract. Contracts should be written to explicitly promote the Principles of Separation of Duties, Need-to-Know and Least Privilege at the commercial provider's site.

2.5.3 Interoperability

Zones support a "whole-of-government approach" that recognizes the interdependencies between federal departments and agencies, businesses, and citizens. Currently, each department establishes its own front-line defences against network threats. Departments have implemented a variety of perimeter defence solutions and this variety has created barriers to network interconnectivity and interoperability. Moreover, because individual departmental defences are often based on conflicting assumptions about topics such as internal network security, application technology, and host configuration, it is extremely difficult to overcome these barriers without the risk of compromising the security of all parties. This Guideline should help overcome these problems by providing a consistent approach for network interconnectivity. Departments that share in the common infrastructure for Electronic Service Delivery and other purposes should conform to the requirements of this Guideline.

An important aspect of maintaining a secure infrastructure is the sharing of relevant information among all interested parties, to the extent possible. The exchange of Lessons Learned, Best Practices, Threat and Vulnerability information and Security Awareness bulletins are some of the items that, if shared appropriately, should lead to a more secure infrastructure overall.

When two Zones of the same type are connected, the resulting network threat environment remains unchanged. This does not mean that End-Systems may freely interact with other End-Systems across Zone boundaries without additional risks. For example, safeguards within an End-System may have been selected on an assumption that all users within the Zone are authorized to access the End-System. In this case, interaction of this End-System with End-Systems outside the Zone needs to be controlled.

To support interoperability, Zones must support requirements for certain traffic types to flow between Zones. Traffic must flow from the Public Zone to internal Zones (e.g., OZ, RZ) and between the internal Zones themselves. The types of traffic permitted to flow between Zones must be determined by balancing the need for carrying particular traffic types to support particular applications against the risks posed by the traffic. Application developers must be able to plan for certain types of traffic being available across interfaces to minimize the complexity of applications and to avoid the risk of impairing security and reliability. However, individual Network Security Zone Authorities responsible for determining the types of traffic that are permitted within their Zones, should remain vigilant to ensure that particular traffic types do not pose unacceptable risks.

2.5.4 Flexibility

Zones apply baseline security requirements that define a mandatory minimum level of protection under the *GSP* and the *MITS*. Zones provide the flexibility for departments and agencies to select the types of Zones that best meet their specific business and security needs. In other words, this Guideline does not constrain departments to use specific types of Zones in specific situations. However, as noted earlier, handling sensitive information or assets in a more open Zone may require the use of additional platform or application security measures to supplement the security provided by the Zone.

Departments and agencies must also have the ability to refine requirements to meet needs specific to the organization. Enhancements beyond baseline security requirements, however, should be limited to organization-specific requirements and should not impair common infrastructure interoperability.

2.5.5 Traffic Control

Zones control traffic flowing between them to ensure that:

a. required traffic is allowed to pass between Zones;

b. malicious traffic is identified and filtered wherever possible;

c. traffic is directed to specified resources; and

d. outgoing traffic does not expose the Zone to additional risks.

2.5.6 Network Boundary Protection

To manage risks associated with backdoors to the network, Zones ensure that:

a. all devices attached to a Zone are authorized;

b. all interfaces with other Zones are authorized;

c. all boundary subsystems are hardened against attack; and

d. host configuration at the perimeter is strictly controlled and appropriate assurance levels are enforced.

2.5.7 Privacy

Zones provide the network-level security controls necessary to protect personal information in accordance with the Privacy Act (reference [31]). Network-level controls may be necessary depending on the IT environment; however, network-level controls are rarely sufficient to protect personal information. Additional privacy requirements related to specific GC programs must be addressed as part of the associated applications.

To comply with Article 10.12.2 of the GSP, and in accordance with Article 17 of the MITS standard, departments must continually monitor system performance to rapidly detect the following:

a. attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms;

b. unauthorized probes or scans to identify system vulnerabilities;

c. unplanned disruption of systems or services;

d. denial-of-service attacks;

e. unauthorized changes to system hardware, firmware, or software;

f. system performance anomalies; and

g. known attack signatures.

Subsection 184(1)(e) of the Criminal Code (reference [11]) permits the interception of private communications for the purposes of managing the quality of service of a computer system and protecting the system against defined illegal acts. These measures must be undertaken in compliance with sections 4 to 9 of the Privacy Act (on the collection and protection of personal information). See also the section on “Monitoring of electronic networks” in Policy on the Use of Electronic Networks (reference [30]) for requirements related to the collection, analysis, and protection of information gathered during monitoring.

Network audit and monitoring solutions in a Network Security Zone must respect both individuals’ reasonable expectations of privacy and the GC’s duties to protect sensitive information, to protect GC assets (including computers and networks), and to ensure that the GC conducts its activities efficiently and in conformity with the law. All solutions must comply with legal requirements including the Charter of Rights and Freedoms (reference [10]), the Privacy Act, and the Criminal Code, as well as policy requirements, such as the GSP and the Policy on the Use of Electronic Networks, and any additional guidance that the Treasury Board of Canada Secretariat may provide relating to network monitoring.

2.5.8 Data Protection

All Zones support the use of security protocols that implement data confidentiality and data integrity services. To ensure reliable, open, and interoperable networks, however, data protection services might be required in a Zone only in certain situations, such as using a particularly vulnerable transmission technology (e.g., wireless), frequent transmission of large amounts of sensitive data, or otherwise facing additional risks (as determined by a TRA).

2.5.9 Layers of Defence

Perimeter defences are applied at Zone boundaries to ensure that sensitive assets (e.g., in the internal Zone) are maintained behind multiple layers of defences and to limit the damage associated with the failure of a perimeter defence mechanism.

2.5.10 Continuity of Service

Although network availability is achieved largely through design measures that are outside the scope of this document (e.g., fault tolerance, redundancy, and reliability engineering), Zones provide protective measures to contain failures and to reduce threats to availability of critical services. If threat and vulnerability information is routinely shared amongst the GC infrastructure owners, then Zone Authorities/Administrators may be able to predict (and prevent) imminent attacks on their own systems, thereby averting a disruption in service. In addition, where appropriate, Zones provide network capabilities to support efficient recovery if a failure occurs, including capabilities to permit reconfiguration in response to changing conditions, and, in some instances, dynamic reconfiguration in response to any increase or decrease in the level of security threat. See the Operational Security Standard – Readiness Levels for Federal Government Facilities (reference [25]) for further information.

2.5.11 Encapsulation of Network Services

Zones encapsulate network services offered by one Zone to other Zones. Only those services available at the interface of a Zone should be visible to other Zones. There should be no exposure of any other network services to entities outside a Zone.

3 Network Security Zones and IT Security

3.1 General

This section provides a general description of the relationship between Zones and other ITS safeguards. The objective is to provide context for the Zones. Zones do not provide a complete security solution: they provide a basis for the consistent application of network security. Additional security requirements are and will be provided in current and future ITS standards and directives, including the *MITS* standard (reference [27]).

Significant investments in network management and technical security are required to protect GC networks and ensure that publicly accessible servers meet the continuous service delivery objectives of the GC.

3.2 The MITS Framework for IT Security

The MITS document outlines a comprehensive ITS framework that consists of management, technical, and operational security controls. The technical and operational controls are further subdivided into security-supporting processes, and controls for prevention, detection, and response and recovery (see Figure 2 below). Some prevention controls are detailed in other standards, such as physical security (see the Operational Security Standard on Physical Security; reference [26]) and personnel security (see the Personnel Security Standard, reference [28]). The MITS framework places network security and Zones in the technical safeguards category, a subgroup of prevention controls.

3.2.1 Management Controls

As described in the MITS, management controls include, but are not limited to, security in the system development life cycle; asset identification and categorization; risk management (which includes TRA and certification and accreditation); incident and vulnerability management; security assessment and audit; and security awareness and training.

Although this publication is primarily for technical guidance, it does include some management controls directly related to network security. This Guideline supports TRAs by providing a standardized level of susceptibility or exposure to network threats. It also includes some requirements for incident and vulnerability management necessary to maintain network security. These areas are outlined in light blue in Figure 2.

This Guideline does not address requirements for the system development life cycle, asset identification and categorization, certification and accreditation, security assessments and audits, or security awareness and training. However, it must be noted that these activities are all necessary and important aspects of an overall security strategy. Specifically, Security Awareness and Training are fundamental to all security implementations; without properly trained and aware users, the best technology may be rendered useless.

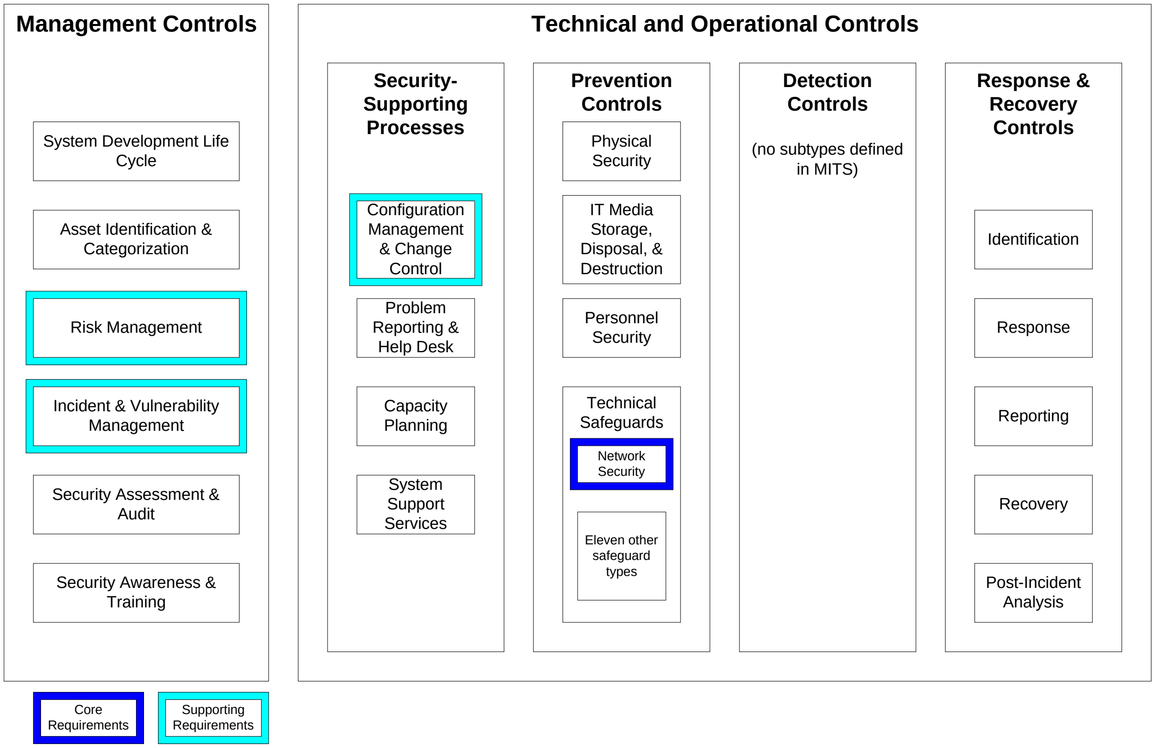

Management Controls
System Development Life Cycle
Asset Identification & Categorization
Risk Management
Incident & Vulnerability Management
Security Assessment & Audit
Security Awareness & Training
Technical and Operational Controls
Security-Supporting Processes
Configuration Management & Change Control
Problem Reporting & Help Desk
Capacity Planning
System Support Services
Prevention Controls
Physical Security
IT Media Storage, Disposal, & Destruction
Personnel Security
Technical Safeguards
Network Security
Eleven other safeguard types
Detection Controls
(no subtypes defined in MITS)
Response & Recovery Controls
Identification
Response
Reporting
Recovery
Post-Incident Analysis
Core Requirements
Supporting Requirements

Figure 2 – MITS Framework

3.2.2 Processes that Support IT Security

The MITS standard identifies four key processes that support ITS:

a. configuration management and change control;

b. problem reporting and help desk;

c. capacity planning; and

d. system support services.

This Guideline includes requirements for configuration management of networks and End-Systems (outlined in light blue in Figure 2); however, the configuration management requirements for End-Systems are limited in scope and include only requirements to prevent End-Systems from introducing threats to the network. Aside from this, this Guideline does not address other security-supporting processes.

3.2.3 Prevention Controls

Prevention controls are deployed within the application systems and the computing infrastructure to protect the confidentiality, integrity, and availability of information and IT assets. They are the first line of defence and aim to keep security incidents from happening.

In the MITS framework, prevention controls are grouped into four main types: physical security controls; controls for the storage, disposal, and destruction of IT media; personnel security controls[2]; and technical safeguards. The MITS standard describes twelve types of technical safeguards, including identification and authentication (I&A), authorization and access control, cryptography, emanations security, and security configuration. Network security is also identified as a technical safeguard; that is where Zones fit into the MITS framework (outlined in dark blue in Figure 2).

This Guideline addresses technical safeguards for network security (and thus focuses on prevention). While it establishes requirements in certain situations for other safeguards such as I&A or cryptography in support of network security, it does not specify how those other safeguards should operate.

Although this Guideline does not specifically address personnel security, it must be noted that even authorized Users and Administrators of systems pose a tremendous threat to the security of any given system. By ensuring that authorized personnel possess an adequate clearance level and are properly trained for a given system, and the Principles of Least Privilege, Separation of Duties and Need-to-Know are honoured in the implementation of access control, the risk to that system from ‘inside’ threat agents can be significantly reduced.

3.2.4 Detection Controls

Detection is the second line of defence. Detection is necessary because prevention controls sometimes fail or are unable to stop some security incidents. When that happens, it is essential to be able to detect whether a security incident has occurred. The MITS standard gives a brief overview of the means and objectives of detection.

This Guideline does not contain any requirements for detection as such, although it does include requirements to ensure that Zones can support detection capabilities where necessary.

3.2.5 Response and Recovery Controls

Response and recovery controls provide the ability to handle security incidents after they have been detected and to bring the IT systems back to a stable state. Lessons learned from the response and recovery activities feed back into improving the prevention and detection controls to counter similar security incidents in the future.

[2] Section 16.3 of the *MITS* requires “all personnel with privileged access to critical systems” to have a Level II security clearance.

The MITS standard identifies five stages in the incident handling process: identification, response, reporting, recovery, and post-incident analysis.

Although this Guideline does not include requirements for response and recovery controls, it does stipulate capabilities to support them.

3.3 The Federated Architecture Framework

The MITS framework is not the only framework in the GC that addresses ITS. The Federated Architecture model (reference [14]) provides another perspective on the division of ITS safeguards. This model identifies eight technology domains:

a. application;

b. information management;

c. network;

d. platform;

e. presentation;

f. security;

g. services; and

h. systems management.

The domains divide the GC's IT infrastructure into manageable parts that will each be the focus of a domain team to further develop the architecture and associated requirements. Figure 3 below, taken from reference [14], shows how the domains relate to each other.

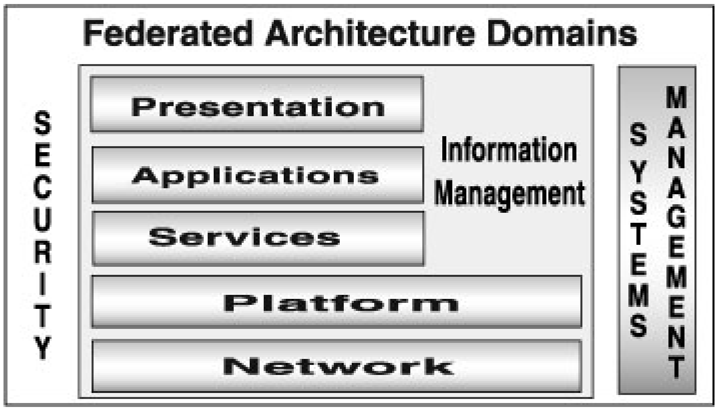


Figure 3 – Federated Architecture Domains

In this framework, security applies across several other domains, including: network, platform, services, and application. This Guideline only addresses security controls to protect the network domain. A complete ITS architecture must address the stacked set of domains in the centre of Figure 3.

Platform security includes operating system controls within each platform such as mobile devices, desktops, and servers. Platform security protects the integrity and availability of the local computing platform and the data stored on the platform. Safeguards are also included within the various software systems that make up the distributed computing environment such as Common Object Request Broker Architecture, Enterprise JavaBeans, .Net, and middleware.

Services security includes processes such as I&A, access or privilege management, and key management.

Applications security includes safeguards within application components to provide controls specific to a business process.

Security controls are required at all layers to provide complete protection for a business process. Since the controls at each layer are interdependent, security service profiles are required to provide a total set of safeguards for common business patterns. For example, a business application may span several different Zones and different platforms in a distributed environment. Service profiles simplify implementation of technical safeguards across the GC IT infrastructure.

3.4 Network Security, Information Security, and Cryptography

As Section 2.2 stated, network security is the measures taken to reduce the susceptibility of a network to various threats. Information security, by comparison, is the measures taken to reduce the susceptibility of information to various threats. This covers information in various forms (e.g., paper, electronic) and states (e.g., at rest, in transit). Each type of security covers issues that the other does not, but there is also some overlap between them. Specifically, both information security and network security address the protection of electronic information transmitted across computer networks. Thus, some security controls that provide information security should also be effective network security controls.

Cryptography is a very effective information security control. It provides confidentiality and integrity, and supports other security services such as non-repudiation (preventing an information sender from successfully claiming that he or she did not send the information in question). Cryptography is also a useful network security measure; it prevents certain network-based attacks such as eavesdropping and replaying messages. The types of benefits that cryptography delivers depend on the layer of the network stack in which it is implemented.

Some cryptographic solutions, such as Public Key Infrastructure services, are implemented at the application layer. Others, such as Type I encryption for classified information, are mandated because of information security considerations, not because of network security considerations. These types of solutions protect the information, not the network. Considering that the focus of network security is the transport layer and below, some cryptographic solutions are beyond the scope of network security.

This Guideline contains suggestions for the use of cryptography where such cryptography contributes to providing a low-threat environment. Aside from this, however, this Guideline does not contain broad requirements for cryptography. Departments should conduct TRAs to determine if measures such as cryptography are warranted to provide information security in their IT environments.

Note that where cryptographic products are warranted, departments should seek further guidance from CSEC.

4 Conceptual Models

4.1 Overview

This section presents the architecture for Zones. This architecture is presented in three models: an implementation model, a general reference model, and a functional model.

The implementation model (Section 4.2) identifies and describes the different types of Zones and how they would be applied in the GC environment. It explains the purpose of each specific Zone and how the different types of Zones relate to each other.

The general reference model (Section 4.3) establishes the technical concepts and terminology needed to support the requirements specifications in Annexes A through D. It defines and describes the components within a single, generic Zone. The safeguards and capabilities associated with a Zone exist within a specific network technology environment as defined in the reference model. Each of Annexes A through D contains a detailed reference model for the Zone specified in that Annex.

The functional model (Section 4.4) identifies five main security functions that Zones perform. These five functions are the basis for structuring the detailed Zone requirements in Annexes A through D.

A Zone is a networking environment with a well-defined boundary delineated by its network interface requirements. It has an assigned Network Security Zone Authority, which is an entity accountable for the development, implementation, and maintenance of the Zone security requirements and practices. Zone safeguards provide an environment with a standardized level of susceptibility to network threats.

A Network Security Zone Authority's control arises through either direct ownership of the network or binding relationships with service providers (e.g., contract, Memorandum of Understanding) with defined service levels that ensure the Zone’s baseline security requirements are met. Each Zone should have its own Network Security Zone Authority. A single Zone Authority may be responsible for multiple Zones.

In most cases, a single department operates a Zone, but it is permissible to share Zones between departments. Departments may implement multiple instances of each Zone type.

4.2 Network Security Zones Implementation Model

4.2.1 General

Section 2.3 earlier in this Guideline identified the different types of Zones:

a. Public Zone;

b. Public Access Zone (PAZ);

c. Operations Zone (OZ);

d. Restricted Zone (RZ);

e. Highly Restricted Zone (HRZ);

f. Restricted Extranet Zone (REZ); and

g. Special Access Zone (SAZ).

Figure 4 illustrates the Network Security Zone implementation model. It shows how the seven Zones relate to each other. The acronym "ZIP" in Figure 4 stands for "Zone Interface Point." See Section 4.3.5 for more information on ZIPs.

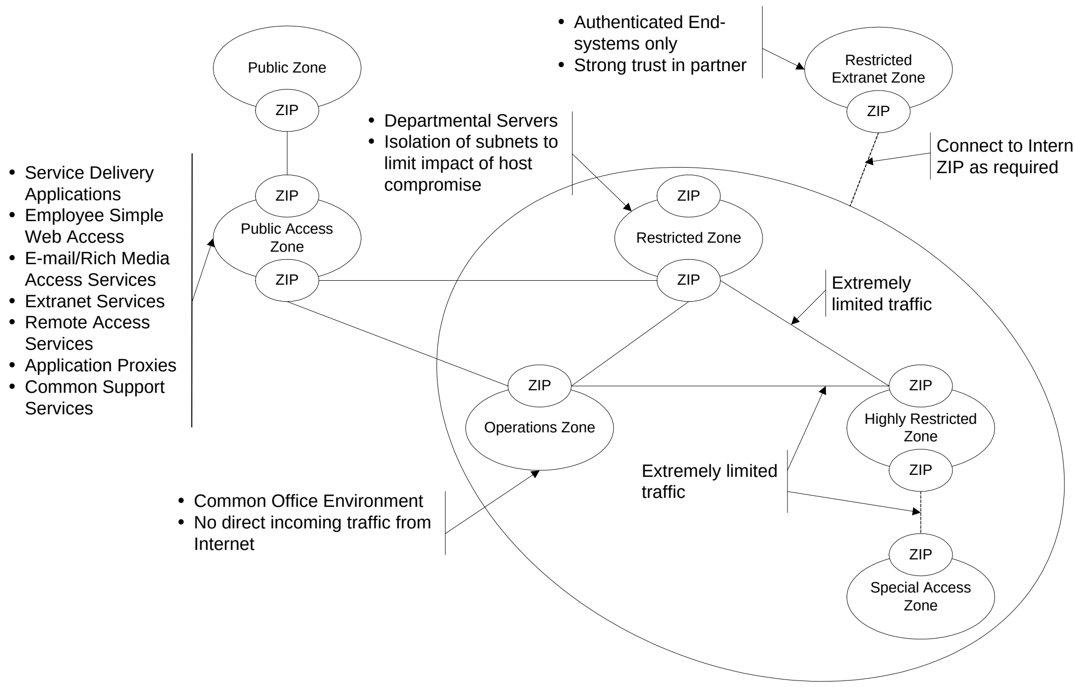

• Authenticated End-systems only
• Strong trust in partner
Public Zone
ZIP
Restricted Extranet Zone
ZIP
• Departmental Servers
• Isolation of subnets to limit impact of host compromise
Connect to Internal ZIP as required
• Service Delivery Applications
• Employee Simple Web Access
• E-mail/Rich Media Access Services
• Extranet Services
• Remote Access Services
• Application Proxies
• Common Support Services
ZIP
Public Access Zone
ZIP
ZIP
Restricted Zone
ZIP
Extremely limited traffic
ZIP
Operations Zone
ZIP
Highly Restricted Zone
ZIP
Extremely limited traffic
• Common Office Environment
• No direct incoming traffic from Internet
ZIP
Special Access Zone

Figure 4 – Network Security Zone Implementation Model

Every Zone contains one or more separate, routable networks. Every separate, routable network should be entirely within a single Zone (i.e., two nodes with the same network address cannot be in different Zones). In certain circumstances, a single End-System may participate in more than one Zone through separate interfaces.

Every Zone connects to other Zones through ZIPs. All the Zones except the Public Zone and the REZ are within or under the control of the GC. The only Zone that may connect to the Public Zone is the PAZ. OZs and RZs may connect to a PAZ, to an HRZ, and to each other. REZs may connect to any of the Zones within the large oval in Figure 4 (via an appropriate ZIP). PAZs, OZs, and RZs may not connect to a SAZ; only HRZs and REZs may do that. Each type of Zone may also connect to another Zone of the same type (not shown in Figure 4). For example, an OZ may connect to other OZs.

This Guideline provides a set of baseline security requirements for the PAZ, OZ, RZ, and HRZ. Other baseline security requirements may be added as the need arises. Network Security Zone Authorities may modify these requirements and practices to strengthen the baseline, to meet particular business issues, or to address a peculiar threat environment. However, certain aspects of the requirements are fixed to ensure that interoperability is achieved throughout.

Note that a Zone does not necessarily correspond to a department. A department could implement many Zones just as it implements many physical security zones. Departments may also share Zones between them. For example, a shared PAZ (e.g., in the Secure Channel Network) may provide Internet access to employees across the GC. Also note that controlled interfaces exist between similar Zones with different Network Security Zone Authorities (e.g., from an OZ in one department to an OZ in another department). Traffic entering and leaving a Zone should conform to the traffic control requirements set by the Network Security Zone Authority.

4.2.2 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 as a system owner. The Public Zone environment is assumed extremely hostile. Any systems delivered in, or interfacing with, the Public Zone should be hardened against attack.

The fact that the Public Zone 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 extremely unwise to discount the magnitude of the threat presented by a Public Zone when developing baseline security requirements.

4.2.3 Public Access Zone (PAZ)

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[3].

A PAZ is a tightly controlled environment that protects internal GC networks and applications from the hostile Public Zone. The PAZ also acts as a screen to hide internal resources from the Public Zone 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 Model (see reference [14]).

4.2.4 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 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 (e.g., compromised host, unauthorized wireless attachment to the Zone).

4.2.5 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 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 Public Zone 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

[3] Extranets connecting via a PAZ are different from those connecting via a Restricted Extranet Zone (see Section 4.2.8). They differ mainly in the trust placed in the extranet partner. Restricted Extranet Zone partners are highly trusted, and connect directly to an internal, GC-controlled Zone.

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.

4.2.6 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 Public Zone). 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.

4.2.7 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.

4.2.8 Restricted Extranet Zone (REZ)

A REZ supports directly connected (i.e., not connected via a PAZ; see Figure 4) 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:

a. integration with financial institutions;

b. outsourced IT environments;

c. federal-provincial interfaces; and

d. 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).

4.3 Network Security Zones Reference Model

4.3.1 General

A generic Network Security Zone consists of four component types (see Figure 5 below):

a. End-System;

b. Internetwork;

c. Internal Boundary System (IBS); and

d. Zone Interface Point (ZIP).

The Internetwork component is further subdivided into an Internetwork Access Subsystem, an Internetwork Core, and an Edge Interface (see Section 4.3.3 below). The ZIP component is further subdivided into a Boundary Subsystem and a Boundary Interface (see Section 4.3.5 below)

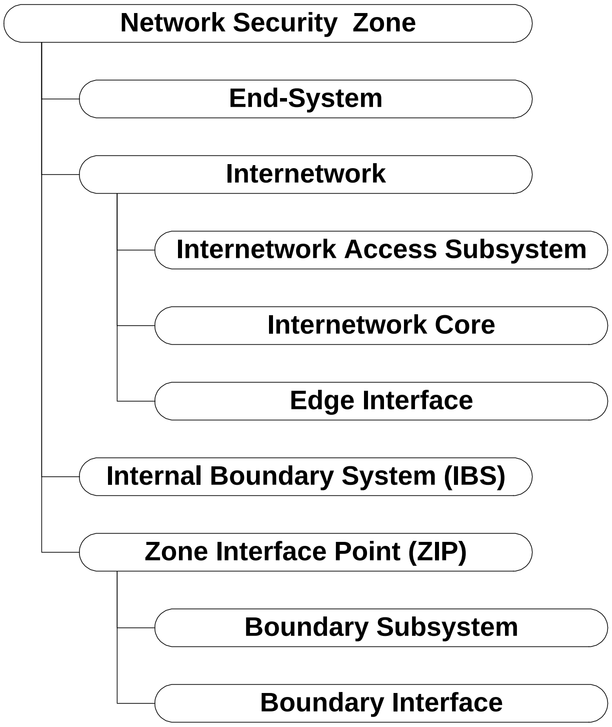


Figure 5 – Network Security Zone Components

Figure 6 illustrates a logical topology of a generic Zone using the four main components. Components are connected to each other via two different types of interface. ZIPs, End-Systems, and IBSs connect to Internetworks via Edge Interfaces (shown as small circles in Figure 6). ZIPs connect to ZIPs in other Zones via Boundary Interfaces (shown as small squares in Figure 6).

An instance of a Zone generally consists of one or more Internetworks with End-Systems, IBSs, and ZIPs connected to them. ZIPs also provide network interfaces to other Zones. If connectivity is required between Internetworks, the connection should go through an IBS (the requirement for such interconnection depends on business needs). Figure 6 also shows that a single ZIP may support interfaces to more than one other Zone and that an End-System may be shared (i.e., connected to Internetworks in two different Zones).

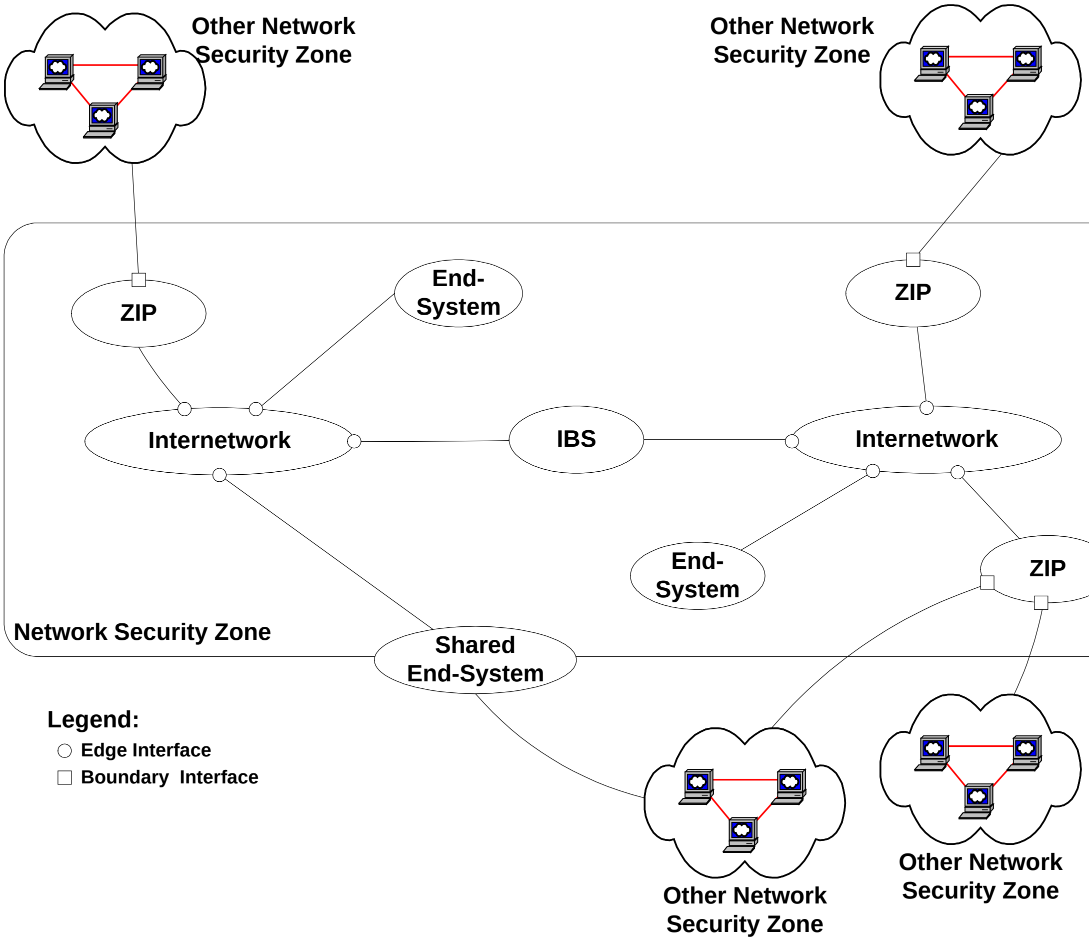


Figure 6 – Network Security Zone Logical Topology

Each of these Zone components and subsystems is a logical construct encompassing specific features and functionality. Readers should not interpret these components as necessarily corresponding to physical devices. It is possible that a single physical device could incorporate the functionality of multiple Zone components (e.g., a ZIP and aspects of an Internetwork). It is also possible that a single Zone component could require multiple physical devices to implement all its features and functions.

4.3.2 End-System

A Zone End-System consists of all localized components that connect to an Edge Interface of an Internetwork. An End-System belongs to the Zone but usually an End-System administrator is responsible for security within the End-System, not the Network Security Zone Authority. The End-System typically consists of a single host. An End-System may also consist of a network of hosts (e.g., storage area network, load-balanced server cluster) connected to the Internetwork's Edge Interface. Such an internal, private network is not part of the Zone and is beyond the recommendations of this Guideline.

End-Systems fall into one of the following four categories:

a. Simple Host – An End-System consisting of a single host;

b. Mobile End-System – An End-System (e.g., laptop, Personal Digital Assistant) that sometimes connects to the Zone and sometimes to another Zone (e.g., Public Zone);

c. Wireless End-System – An End-System that connects to the Internetwork by way of a wireless Internetwork Access Subsystem (if an End-System has multiple interfaces with the Internetwork, it is considered a wireless End-System if any of these connects over a wireless Internetwork Access Subsystem); and

d. Complex End-System – An End-System that consists of a logical group of hosts and an internal private network between hosts (e.g., storage area network).

Note: End-Systems using internal wireless communications need to apply additional security measures to limit exploitation as a backdoor to the Zone.

Any type of End-System may be shared (see Figure 6), which means the End-System is connected to two or more Zones simultaneously, does not route traffic between the Zones[4], and meets the configuration requirements of all Zones that it participates in (e.g., system management workstation, single employee workstation hosted by a second department).

A "remote" End-System (i.e., an End-System that belongs to a Public Zone and logically communicates with a GC-controlled Zone only through a ZIP) is not part of the Zone. However, when a Zone permits remote network access from Public Zones, host configuration requirements for the remote End-Systems are specified.

[4] This means the shared End-System can communicate with both Zones, but the Zones cannot exchange traffic with each other through the shared End-System.

4.3.3 Internetwork

Internetworks provide the network services to connect End-Systems, IBSs, and ZIPs. Internetworks may consist of any combination of local area networks (LANs), metropolitan area networks, or wide area networks. They may run over multiple physical-layer media, including copper wire, optical fibre, or wireless links (e.g., wireless LANs, fixed wireless metropolitan or long-haul links, satellite uplinks). Internetworks provide a network distribution service (e.g., routing) between Edge Interfaces within a Zone.

An Internetwork includes the following subsystems:

a. Internetwork Access Subsystem – provides the physical-layer and data-link-layer services that connect an Edge Interface to the Internetwork Core. Physical implementations of these services include hubs, bridges, the Ethernet protocol, data-link-layer switches (including multiplexers), and gateways. The Internetwork Access Subsystem may also provide network-layer and upper-layer layer services. In particular, Virtual Private Network (VPN) access would be implemented in this subsystem. An Internetwork may have more than one Internetwork Access Subsystem;

b. Internetwork Core – provides the core network services for the Internetwork, such as backbone routing and address resolution; and

c. Edge Interface – is the logical boundary between the Internetwork and a ZIP, End-System, or IBS. An example of a physical implementation of an Edge Interface would be a network interface card in an End-System, an interface port on a switch, and the connecting medium between them. An Internetwork may have more than one Edge Interface.

The Internetwork Access Subsystem includes those Internetwork entities that are always fully under the control of the Network Security Zone Authority. By contrast, the Internetwork Core may include entities that are operated for or on behalf of the Zone Authority, but are not under its direct control.

A Zone should include at least one instance of an Internetwork. If a Zone includes more than one Internetwork, then IBSs provide any required connectivity between the Internetworks. A Zone may use multiple Internetworks to segregate traffic and provide defence in depth. Multiple Internetworks may also exist within a Zone when existing network infrastructures are combined to create a Zone.

4.3.4 Internal Boundary System (IBS)

An IBS provides a network interface between Internetworks. An IBS also acts as a buffer implementing traffic control and network configuration safeguards. An IBS connects to the Internetworks through Edge Interfaces.

An IBS is required in a Zone only if that Zone has more than one Internetwork and if those Internetworks must be connected.

Examples of IBSs include perimeter protection systems such as screening routers, firewalls, intrusion prevention systems (IPSs), and Unified Threat Management (UTM) products. Other examples include bridges between different protocols (e.g., Internetwork Packet Exchange (IPX) to Internet Protocol (IP), or IP version 4 to IP version 6) and connections between two enclaves over another network using a VPN.

An IBS could itself be a network. Such a network is not a distinct Zone.

4.3.5 Zone Interface Point (ZIP)

A ZIP provides a network interface between its Zone and other Zones. The ZIP also acts as a buffer implementing perimeter security measures. It is composed of the following subsystems:

a. Boundary Interface – is the boundary between the ZIP and a ZIP in another Zone. The physical implementation of a Boundary Interface may be a cable between two screening routers. It may also be a small, switched network connecting multiple ZIPs. A ZIP may have more than one Boundary Interface; and

b. Boundary Subsystem – implements the perimeter protection services of the ZIP. Examples of physical implementations of Boundary Subsystems include screening routers, firewalls, guards, IPSs, and UTM products. A ZIP may have more than one Boundary Subsystem.

Two or more Zones may share a ZIP (instead of each Zone having its own ZIP). Note that in the case where two Zones share a ZIP to connect to each other, the Boundary Interfaces are purely logical. Whenever a ZIP is shared, the respective Network Security Zone Authorities should demonstrate clear accountability for control and management of the ZIP. A shared ZIP may require connections to discrete Edge Interfaces on different Internetworks.

The focus of a ZIP is traffic entering that ZIP’s Zone. If a ZIP connects to a Zone that provides similar or more security (e.g., a ZIP in an OZ that connects to an RZ), then the ZIP would not filter (i.e., block) incoming traffic. However, it would monitor that traffic to ensure that the sending Zone is behaving and to encourage the sending Zone to continue to live up to its commitments. If a ZIP connects to a Zone that provides less security (e.g., a ZIP in an RZ that connects to an OZ), then the ZIP would filter incoming traffic for malware and other forms of malicious traffic. The ZIP may also monitor this traffic at the discretion of the receiving Zone’s Network Security Zone Authority. Monitoring is optional in this case because the ZIP already implements the more stringent security measure of traffic filtering.

In this Guideline, ZIPs are named according to the other Zones to which they connect. For example, a ZIP in one Zone that connects that Zone to a PAZ is referred to as a PAZ ZIP. A ZIP that connects its Zone to an OZ is an OZ ZIP, and so on. If a ZIP provides connectivity to multiple Zones, it should meet the requirements for each type of ZIP. For example, if a single ZIP in an OZ connects to both an RZ and an HRZ, it should meet the OZ requirements for an RZ ZIP and an HRZ ZIP. If there is a conflict between requirements, the more restrictive requirements take precedence.

4.4 Network Security Zones Functional Model

The Network Security Zone Functional Model describes how the requirements for Network Security Zones are structured. It identifies and defines the different types of requirements. This structure is the basis for Annexes A to D in this Guideline.

The Functional Model encompasses the following security requirements components:

a. *Network Interface requirements:* the set of security requirements governing the types of interfaces permitted with other Zones. Network interface requirements are intended to clearly delineate the boundary of a Zone. These requirements address issues such as permitted interfaces to other Zones, use of common infrastructure, and sharing of End-Systems with other Zones;

b. *Traffic Control requirements:* the set of security requirements governing the flow of network traffic within the Zone and between the Zone and other Zones. These requirements address issues such as the types of traffic, network access control requirements, non-interference rules, quality of service, traffic content rules, and resource consumption constraints;

c. *Network Configuration requirements:* the set of security requirements governing the connection of devices to the Zone. These requirements address the management of associations between network entities, data link entities, and physical interfaces and nodes, plus the management and control of physical transmission media;

d. *Host Configuration requirements:* the set of security requirements governing the configuration management of the hardware and software load on each host with the goal of ensuring that each host operates within a known security state and does not pose a threat to other hosts in the network. These requirements do not address what software may be on a host. Rather, they address the actions necessary to ensure that the software load is in a secure state (e.g., properly patched and configured); and

e. *Data Protection requirements:* the set of security requirements governing the assignment and use of Open Systems Interconnection (OSI) security services to provide Data Protection services.

Network Security Zones isolate the security aspects of the network infrastructure from the business processes. A Zone offers applications a predictable level of security while ensuring that the security functionality is relatively transparent. Different Zones deliver different levels of security service to the business processes within the Zone.

Zones provide a foundation for secure interoperability. The technical requirements for a Zone and the practices used to implement these requirements provide an objective measure for a partner to assess the network security posture of another partner.

4.4.1 Network Interface Requirements

Network interface requirements define constraints on the boundary of a Zone. Network interface requirements may be thought of as a set of connection rules for a Zone. They fall into one of the following categories:

a. requirements for ZIPs (see Section 4.3.5) that define the controls at network-layer interfaces with other Zones;

b. requirements for interfaces to underlying communications infrastructure (e.g., interfaces to data communications carriers); and

c. requirements for End-System interfaces that define the types of End-Systems that may be attached to the Network Security Zone and that identify constraints on these interfaces.

Network interface requirements address the following security issues:

a. network interface requirements clearly delineate the boundary of the Zone ensuring that the scope of the Network Security Zone Authority's accountability is clear; and

b. network interface requirements place limits on the types of interface supported by a Zone, thereby controlling the threat environment to which the Zone is exposed.

4.4.2 Traffic Control Requirements

Traffic control requirements specify safeguards that control the flow of traffic within the Zone and between the Zone and other Zones. Traffic control requirements also specify network capabilities that should be present to support the implementation of measures for platform, application, and system management security.

Traffic control safeguards include the following:

a. Access Control – controls traffic based on source and destination address, and type of service. Access Controls are used to limit access to sensitive resources, to limit the data communication protocols used within the Zone, to ensure non-interference between communities of interest, or to localize the impact of security failures;

b. Entity Authentication – validates the authenticity of entities and establishes a security association between them. The primary purpose of entity authentication is support for access controls;[5]

[5] Throughout this Guideline, the baseline security requirement for authentication of remote access attempts is strong authentication. Two-factor authentication is sometimes recommended in environments with greater threats. Note that strong authentication may be applied to users, devices, and peer entities. Two-factor authentication only applies to users.

c. Data Origin Authentication – validates the authenticity of entities participating in a security association throughout the life of the security association. Within traffic control, data origin authentication is primarily used to support access controls;

d. Data Integrity Verification – verifies that network traffic has not been modified or replayed. It protects assets attached to the Zone by ensuring that content from a source arrives at its destination without modification;

e. Traffic Filters – filter or block traffic based on properties of the data communications stream including Traffic Control Protocol (TCP) state, source and destination, conformance with authorized communications protocols, data types embedded within the data communications stream, and contents of the data communications stream. For example, filters may be used to block traffic to or from prohibited IP or MAC addresses or TCP ports. Filters can block prohibited protocols (e.g., firewall products) and stop malicious traffic containing exploits or potential exploits (e.g., IPS products). They may also be used to filter traffic containing malware (e.g., anti-virus products, anti-spyware products) or to filter traffic containing dangerous or illicit content (e.g., web and e-mail filtering products);

f. Intrusion Detection and Audit Support – provide the services and attributes that support the implementation of security functions such as intrusion detection, audit, and incident response[6]. This support may come in the form of traffic logs or attachment points for traffic monitoring sensors (e.g., a mirror port on a switch);

g. Address and Name Resolution Security – refers to a collection of safeguards aimed at ensuring the integrity of the association between resources and their identifiers; and

h. Resource Encapsulation – refers to the mechanisms that allow the Zone to hide its internal structure. This includes network address translation, port address translation, and service mapping. Resource encapsulation supports access control and survivability.

Each traffic control safeguard is typically associated with certain layers within the network stack. Figure 7 illustrates the primary traffic control functions associated with the various layers of the network stack.

Traffic control requirements also specify network capabilities needed to support platform, application, and operational security safeguards. For example, an RZ should be able to support Internet Protocol Security (IPSec) between any two Edge Interfaces and any Zone should support attachment of intrusion detection sensors at certain points in the Zone.

[6] Intrusion detection and response are an important part of computer and network security. However, these baseline security requirements do not address operational security processes such as intrusion detection except to ensure that mechanisms are in place to ensure that information needed by these processes is available from the network.

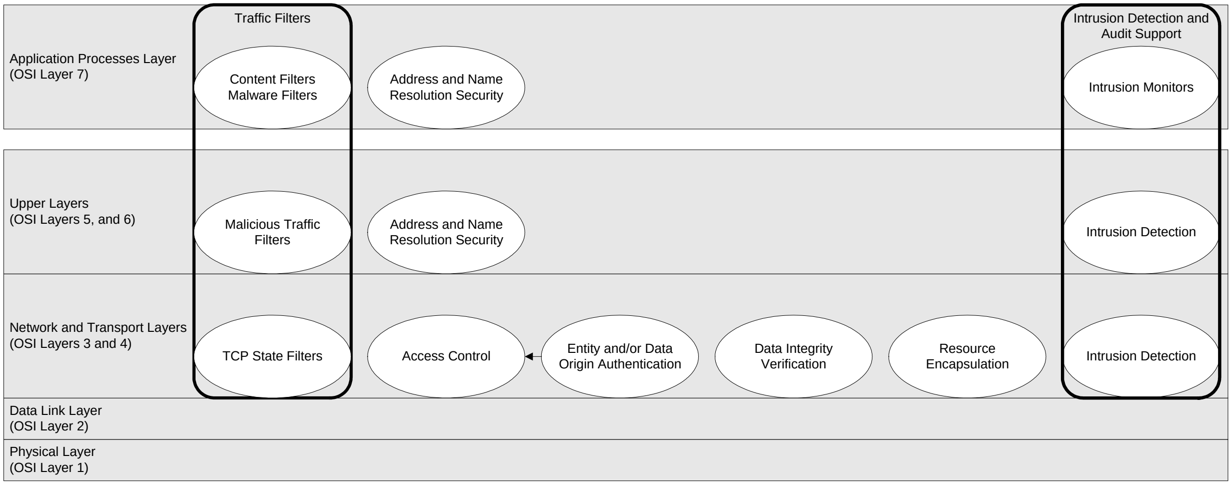

Traffic Filters
Intrusion Detection and Audit Support
Application Processes Layer (OSI Layer 7)
Content Filters Malware Filters
Address and Name Resolution Security
Intrusion Monitors
Upper Layers (OSI Layers 5, and 6)
Malicious Traffic Filters
Address and Name Resolution Security
Intrusion Detection
Network and Transport Layers (OSI Layers 3 and 4)
TCP State Filters
Access Control
Entity and/or Data Origin Authentication
Data Integrity Verification
Resource Encapsulation
Intrusion Detection
Data Link Layer (OSI Layer 2)
Physical Layer (OSI Layer 1)

Figure 7 – Allocation of Traffic Control Functions

4.4.3 Network Configuration Requirements

Network configuration requirements specify the safeguards and capabilities necessary to control the attachment and removal of End-Systems from a Zone. A Zone offering a very high level of network security would implement mechanisms to authenticate all End-System interfaces before permitting the interface to participate in communications. A Zone providing a minimal level of security would implement safeguards to deter the attachment of unauthorized devices.

Network configuration safeguards include:

a. administrative controls (configuration identification, change control, configuration status reporting, and configuration audit);

b. physical security;

c. authentication; and

d. event logging.

Access to a network interface is a prerequisite to any network attack. Access to a network interface may be gained by attaching an unauthorized device to the network, exploiting an established host, or through an external interface. Network configuration controls either limit the ability of an attacker to attach an unauthorized device to the network or limit the ability of an attacker to do so without detection.

4.4.4 Host Configuration Requirements

Host configuration requirements govern the configuration of hosts attached directly and indirectly to a Zone. Host configuration requirements do not specify safeguards to protect assets managed by the host; rather host configuration requirements specify the minimum requirements to ensure that hosts attached to the Zone do not compromise the security of the network or End-Systems by providing an access point for an attacker.

Host configuration safeguards include:

a. administrative controls (e.g., configuration management, vulnerability management, and security audit);

b. access controls (including entity authentication)

c. physical security;

d. platform security measures; and

e. event logging.

Access to a network interface is a prerequisite to any network attack. Access to a network interface may be gained by attaching an unauthorized device to the network, exploiting an established host, or through an external interface. Host configuration controls limit the ability of an attacker to exploit an established host or, at least, to exploit an established host without detection.

4.4.5 Data Protection Requirements

Data protection requirements specify the safeguards and capabilities necessary to protect the confidentiality, integrity, and availability of data during transmission. Data protection requirements also specify network capabilities necessary to support protection of confidentiality, integrity, and availability of data communications by applications, processes, and network overlays.

5 Glossary

For the purpose of this Guideline, the following definitions apply. Wherever possible, existing definitions have been adopted from stable documents from recognized sources. In these cases, the source of the definition is noted.

Authentication: The process of verifying an identity claimed by or for a system entity. (Reference [33])

Authorization: Access privileges granted to a user, program or process. (Reference [37])

Baseline Security Requirements: Minimum security functionality required to meet the requirements of the *GSP* and its associated operational standards and technical documentation

Boundary Interface: A network-layer interface between two ZIPs.

Demilitarized Zone (DMZ): A part of the network that is located between any two policy-enforcing components of the network (typically between the Internet and internal networks) and that enables an organization to host its own Internet services without risking unauthorized access to its private network.

Denial-of-Service (DoS) Attack: The prevention of authorized access to a system resource or the delaying of system operations and functions. (Reference [33])

Distributed Denial-of-Service (DDoS) Attack: An attack in which multiple compromised systems (which are usually infected with a Trojan) are used to target a single system causing a Denial-of-Service (DoS) attack. Victims of a DDoS attack consist of both the end-targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. (Reference [9])

Edge Interface: A network-layer service interface point through which an End-System, Internal Boundary System, or ZIP attaches to a Zone Internetwork.

Electronic Service Delivery: The provision of GC on-line information and transaction services to citizens, businesses, other governments, nongovernmental organizations, and employees.

Encapsulation: The ability to provide users with a well-defined interface to a set of functions in a way that hides their internal workings. (Reference

[1])

Enclave: A distinct subset of a Network Security Zone that may be geographically separate from other Zone entities but that remains part of the Zone and is under the control of the Network Security Zone Authority at all times.

End-System: A system that, for a particular instance of communication, is the ultimate source or destination of the communication.

Note: If the End-System consists of multiple hosts connected by a network, this network is under the management of the End-System administrator and is outside the direct management of the Network Security Zone Authority.

End-to-end encryption: Confidentiality service provided by encrypting data within or at the source End-System, with corresponding decryption occurring only within or at the destination End-System. (Reference [21])

Entity: An active element of a system – e.g., an automated process, a subsystem, a person or group of persons – that incorporates a specific set of capabilities. (Reference [33])

Extranet: A constrained extension of a private GC network used to share information and resources for specific business needs with specific partners, including other governments (international, domestic), industry, and non-governmental organizations.

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.

Gateway: An intermediate system that is the interface between two computer networks. (Reference [33])

Guard: A gateway that is interposed between two networks (or computers, or other information systems) operating at different security levels (one level is usually higher than the other) and is trusted to mediate all information transfers between the two levels, either to ensure that no sensitive information from the first (higher) level is disclosed to the second (lower) level, or to protect the integrity of data on the first (higher) level. (Reference [33])

Host: A computer that is attached to a communication subnetwork or inter-network and that can use network services to exchange data with other attached systems. (Reference [33])

Interface: A boundary across which two systems communicate. An interface might be a hardware connector used to link to other devices, or it might be a convention used to allow communication between two software systems. Often there is some intermediate component between the two systems that connects their interfaces together. For example, two EIA-232 interfaces connected via a serial cable. (Reference [2])

Internal Boundary System (IBS): A gateway that connects two or more Internetworks within a Network Security Zone.

Internal Zone: A Network Security Zone that is farther away (in terms of number of Zones traversed) from the Public Zone than the Zone currently being discussed.

Internet: The single, interconnected, worldwide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the Internet Architecture Board and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers. (Adapted from reference [33])

Internetwork: Any combination of local, metropolitan, or wide area networks providing some or all network services to a Network Security Zone.

Intrusion detection: A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access network or system resources in an unauthorized manner. (Adapted from reference [33])

Least Privilege: Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error or unauthorized use of an IS. (Reference [37])

Malware: Short for “malicious software.” Software that is intentionally included or inserted in a system for a harmful purpose; includes such specific sub-types as logic bomb, Trojan horse, virus, and worm. (Adapted from reference [33])

Mobile code: Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient. (Reference [12])

Need-to-Know: Access to (including knowledge of) sensitive information, is restricted to those whose duties require such access.

Network Security Zone Authority: The person or persons responsible and accountable for the security of the Network Security Zone.

Network Security Zone: A networking environment with a well-defined boundary, a Network Security Zone Authority, and a standard level of susceptibility to network threats. Types of Zones are distinguished by security requirements for interfaces, traffic control, data protection, host configuration control, and network configuration control

Node: An addressable device attached to a computer network. If the node is a computer, it is more often called a “host.” The term node includes devices such as routers and printers that would not normally be called “hosts.” (Reference [4])

Peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. (Reference [33])

Platform: Specific computer hardware, as in the phrase “platform-independent”. It may also refer to a specific combination of hardware and operating system and/or compiler, as in “this program has been ported to several platforms”. It is also used to refer to support software for a particular activity, as in “This program provides a platform for research into routing protocols”. (Reference [5])

Point of presence (PoP): An artificial demarcation point or interface point between communications entities. (Reference [6])

Protocol: A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. In particular, a series of ordered steps involving computing and communication that are performed by two or more system entities to achieve a joint objective. (Reference [33])

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*.)

Restricted Extranet: A highly constrained extension of a private GC network, used to share information and resources with highly trusted, non-GC partners. The Restricted Extranet may terminate in any GC-controlled Zone (unlike the ‘generic’ extranet, which must terminate in the Public Access Zone). Management and control of the interface should be mutually agreed upon by the two trusted parties involved.

Secure Virtual Private Network (SVPN): A Virtual Private Network (VPN) that uses cryptography (e.g., Internet Protocol Security (IPSec)) (in contrast to a VPN based simply on logical isolation (e.g., multi-protocol label switching or Ethernet Virtual Local Area Networking)).

Security audit: An independent review and examination of the system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security and to recommend any indicated changes in control, policy and procedures. (Reference [21])

Security domain: An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources. (Reference [33])

Security perimeter: The boundary of the domain in which a security policy or security architecture applies; i.e., the boundary of the space in which security services protect system resources. (Reference [33])

Sensitive (information): Information is sensitive if disclosure, alteration, destruction, or loss of the information would adversely affect the interests or business of its owner or user. (Reference [33])

Separation of Duties: "Separation of Duties" is a Security Principle, which requires that the responsibilities for an activity of a sensitive or critical nature be distributed among multiple entities (staff, processes, etc), to help prevent a breach of security by a lone entity with control over the entire activity.

Shared End-System: An End-System that is connected to two or more Network Security Zones, does not route traffic between the Zones, and meets the configuration requirements of all Zones in which it participates.

Smurf: Software that mounts a DoS attack ("smurfing") by exploiting Internet Protocol (IP) broadcast addressing and Internet Control Message Protocol (ICMP) ping packets to cause flooding. (Reference [33])

Stateful inspection: With Stateful Inspection, packets are intercepted at the network layer for best performance (as in packet filters), but then data derived from all communication layers is accessed and analyzed for improved security (compared to layers 4–7 in application-layer gateways). Stateful Inspection then introduces a higher level of security by incorporating communication- and application-derived state and context information which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. (Reference [34])

Strong Authentication: An authentication process that uses cryptography – particularly public-key certificates – to verify the identity claimed for an entity. (Reference [33])

Subnet: Short for "subnetwork." Portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an inter-network. (Reference [7])

SYN flood: A DoS attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle. (Reference [33])

TEMPEST: A nickname for specifications and standards for limiting the strength of electromagnetic emanations from electrical and electronic equipment and thus reducing vulnerability to eavesdropping. This term originated in the U.S. Department of Defense. (Reference [33])

Threat: Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental. (Reference [38])

Two-factor authentication: A form of user authentication that requires two different ways (factors) of verifying a claimed identity. The three most commonly recognized factors are: (1) something you know (e.g., a password), (2) something you have (e.g., a physical authentication token), and (3) something you are (e.g., a biometric). Note that two-factor authentication can be applied only to users; it cannot be applied to devices or peer entities.

Unified Threat Management (UTM): A network firewall that has many features in one product, including e-mail filtering, anti-malware capability, intrusion detection or prevention, and World Wide Web content filtering, along with the traditional activities of a firewall. (Based on reference [8])

Virtual private network (VPN): A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network. (Reference [33]) In general terms, it often refers to a network that emulates a private network, although it runs over public network lines and infrastructure.

Vulnerability: A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs. (Reference [38])

Zone Interface Point (ZIP): An interface between two Network Security Zones through which traffic may be routed.

Note the definitions of *End-System*, *host*, *node*, and *platform*. *Node* is the most generic term, and applies to any addressable device on a network. A *host* is a node that is a computer (as opposed to being, for example, a printer). Every host is a node, but not every node is a host. An *End-System* is one or more nodes, some of which may be hosts, that are the source or destination of a communication. A *platform* is a generic computing system consisting of hardware, an operating system, and applications. Platforms in a network are also hosts.

This page intentionally left blank.

6 References

[1] "encapsulation" [online]. In *FOLDOC* (Free On-Line Dictionary of Computing) web site. [London]: Imperial College Department of Computing, 7 September 1998 [cited 25 January 2006]. Available from World Wide Web: <http://foldoc.org/?query=encapsulation>.

[2] "interface" [online]. In *FOLDOC* web site. [London]: Imperial College Department of Computing, 22 May 1996 [cited 28 March 2006]. Available from World Wide Web: <http://foldoc.org/?query=interface>.

[3] ITSG-38 Network Security Zoning Design - Considerations for Placement of Services within Zones in the Government of Canada

[4] "node" [online]. In *FOLDOC* web site. [London]: Imperial College Department of Computing, 25 August 2004 [cited 25 January 2006]. Available from World Wide Web: <http://foldoc.org/foldoc.cgi?network+node>.

[5] "platform" [online]. In *FOLDOC* web site. [London]: Imperial College Department of Computing, 7 December 1994 [cited 10 April 2006]. Available from World Wide Web: <http://foldoc.org/foldoc.cgi?query=platform>.

[6] "Point of presence" [online]. In *Wikipedia, The Free Encyclopedia* web site. 9 March 2006 [cited 28 March 2006]. Available from World Wide Web: <http://en.wikipedia.org/wiki/Point_of_presence>.

[7] "subnet" [online]. In *FOLDOC* web site. [London]: Imperial College Department of Computing, undated [cited 28 March 2006]. Available from World Wide Web: <http://foldoc.org/?query=subnet>.

[8] "Unified threat management" [online]. In *Wikipedia, The Free Encyclopedia* web site. 27 April 2006 [cited 19 May 2006]. Available from World Wide Web: <http://en.wikipedia.org/wiki/Unified_threat_management>.

[9] "What is DDoS attack?" [online]. In *Webopedia, the Online Computer Dictionary for Computer and Internet terms and definitions* web site. Jupitermedia Corporation, 2006 [cited 6 March 2006]. Available from World Wide Web: <http://www.pcwebopedia.com/TERM/D/DDoS_attack.html>.

[10] *Canadian Charter of Rights and Freedoms* [online]. [Ottawa]: Department of Justice, 17 April 1982 [cited 27 January 2006]. Available from World Wide Web: < http://laws-lois.justice.gc.ca/eng/const/page-15.html>.

[11] *Criminal Code* [online]. [Ottawa]: Department of Justice, 31 August 2004 [cited 27 January 2006]. Available from World Wide Web: < http://laws-lois.justice.gc.ca/eng/acts/c-46/>.

[12] *Department of Defense Directive 8500.1: Information Assurance* [online]. [Washington, District of Columbia]: Department of Defense, 24 October 2002 [cited 25 January 2006]. Available from World Wide Web: < http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>.

[13] *Financial Administration Act* [online]. [Ottawa]: Department of Justice, 31 August 2004 [cited 24 January 2006]. Available from World Wide Web: <http://laws-lois.justice.gc.ca/eng/acts/f-11/>.

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

[15] *Government of Canada – Information Infrastructure Protection: Vulnerability Assessment – Concept of Operations*. Final version 3.0. [Ottawa]: Communications Security Establishment, 7 December 2005. CSE requisition W2213-6-0051, Contract Data Requirements List (CDRL) EN-01. Available from Treasury Board of Canada Secretariat (TBS) SiteScape Forum: <https://tbs-sct.scc.ca/tbs-sct/dispatch.cgi/f.gocpkitfnew/AVFLoginForm>.

[16] *Government of Canada – Information Infrastructure Protection: Vulnerability Assessment – Methodology and Best Practices*. Final version 3.0. [Ottawa]: Communications Security Establishment, 7 December 2005. CSE requisition W2213-6-0051, CDRL EN-02. Available from TBS SiteScape Forum: <https://tbs-sct.scc.ca/tbs-sct/dispatch.cgi/f.gocpkitfnew/AVFLoginForm>.

[17] *Government of Canada – PKI Network Architecture with Automated Certificate Issuance, Roaming Profiles, and Trusted Time Clocks*. Version 4.2. [Ottawa]: Communications Security Establishment, 26 March 2001. CSE requisition W2213-1-2494, CDRL EN03-02. Available from TBS SiteScape Forum: <https://tbs-sct.scc.ca/tbs-sct/dispatch.cgi/f.gocpkitfnew/AVFLoginForm>.

[18] *Government of Canada – PKI-Enabled Virtual Private Network Detailed Architecture*. Final version 1.0. [Ottawa]: Communications Security Establishment, 12 December 2002. CSE requisition W2213-2-6111, CDRL: EN01-02.

[19] *Policy on Government Security [online]. [Ottawa] Treasury Board of Canada Secretariat, 1 July 2009. Available at: <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578>..*

[20] *Information Technology Security Alert ITSA-11C: CSE Approved Cryptographic Algorithms for the Protection of Protected Information and for Electronic Authentication and Authorization Applications within the Government of Canada* [online]. [Ottawa]: Communications Security Establishment, 18 April 2006 [cited 20 May 2006]. Available

from World Wide Web: <http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsa/itsa11c-e.pdf>.

[21] *ISO 7498-2:1989 – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*. International Organization for Standardization.

[22] *ISO/IEC 7498-1:1994 – Open Systems Interconnection – Basic Reference Model: The Basic Model*. International Organization for Standardization.

[23] MELL, Peter; BERGERON, Tiffany; and HENNING, David. *Special Publication 800-40: Creating a Patch and Vulnerability Management Program* [online]. Version 2.0. Gaithersburg, Maryland: National Institute of Standards and Technology, November 2005 [cited 24 January 2006]. Portable Document Format. Available from World Wide Web: <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>.

[24] MILLS, David L. *Request for Comments: 1305 – Network Time Protocol* [online]. The Internet Society, March 1992 [cited 23 April 2006]. Available from World Wide Web: <http://www.ietf.org/rfc/rfc1305.txt>.

[25] *Operational Security Standard – Readiness Levels for Federal Government Facilities* [online]. [Ottawa]: Treasury Board of Canada Secretariat, 1 November 2002 [cited 11 April 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/oss-nos_e.asp>.

[26] *Operational Security Standard on Physical Security* [online]. [Ottawa]: Treasury Board of Canada Secretariat, November 2004 [cited 27 January 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/osps-nosm_e.asp>.

[27] *Operational Security Standard: Management of Information Technology Security (MITS)* [online]. [Ottawa]: Treasury Board of Canada Secretariat, 31 May 2004 [cited 24 January 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp>.

[28] *Personnel Security Standard* [online]. [Ottawa]: Treasury Board of Canada Secretariat, 17 October 2002 [cited 1 April 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp>.

[29] *Policy for Public Key Infrastructure Management in the Government of Canada* [online]. [Ottawa]: Treasury Board of Canada Secretariat, 26 April 2004 [cited 24 January 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/PKI/pki1_e.asp>.

[30] *Policy on the Use of Electronic Networks* [online]. [Ottawa]: Treasury Board of Canada Secretariat, 12 February 1998 [cited 24 January 2006]. Available from World Wide Web: <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_CP/uen1-2_e.asp>.

[31] *Privacy Act* [online]. [Ottawa]: Department of Justice, 31 August 2004 [cited 27 January 2006]. Available from World Wide Web: <http://lois.justice.gc.ca/en/P-21/index.html>.

[32] REKHTER, Y.; MOSKOWITZ, B.; KARRENBERG, D.; DE GROOT, G.J.; and LEAR, E. *Request for Comments: 1918 – Address Allocation for Private Internets* [online]. The Internet Society, February 1996 [cited 22 April 2006]. Available from World Wide Web: <http://www.ietf.org/rfc/rfc1918.txt>.

[33] 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>.

[34] *Stateful Inspection Technology* [online]. Ramat Gan, Israel: Check Point Software Technologies, 2 August 2005 [cited 21 April 2006]. Portable Document Format. Available from World Wide Web: <http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf>.

[35] TRACY, Miles; JANSEN, Wayne; and McLARNON, Mark. *Special Publication 800-44, Guidelines on Securing Public Web Servers* [online]. Gaithersburg, Maryland: National Institute of Standards and Technology, September 2002 [cited 24 January 2006]. Portable Document Format. Available from World Wide Web: <http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>.

[36] WACK, John; CUTLER, Ken; and POLE, Jamie. *Special Publication 800-41: Guidelines on Firewalls and Firewall Policy* [online]. Gaithersburg, Maryland: National Institute of Standards and Technology, January 2002 [cited 24 January 2006]. Portable Document Format. Available from World Wide Web: < http://csrc.nist.gov/publications/nistpubs/800-41-rev1.pdf>.

[37] *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, Committee on National Security Systems, National Security Agency, June 2006 [cited 6 November 2006]. Portable Document Format. Available from World Wide Web: <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>.

[38] *Threat and Risk Assessment Working Guide*, ITSG-04, Communications Security Establishment, October 1999 [cited 6 November 2006]. Portable Document Format available from World Wide Web: < http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg04.pdf >.

[39] *IT Security Zones Baseline Security Requirements*, ITSD-02 (Version 1), Communications Security Establishment, May 2003. Portable Document Format available [as of 9 January 2007] from World Wide Web: < http://www.cse-cst.gc.ca/publications/gov-pubs/itsd/itsd02-e.html >.

[40] *Directives for the Application of Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSD-02)*, Draft-only revision of ITSD-02, Communications Security Establishment, June 2006.

This page intentionally left blank.

Annex A Public Access Zone (PAZ) Baseline Security Requirements

A.1 Introduction

This Annex provides a set of baseline security requirements for the Public Access Zone (PAZ). A PAZ mediates access between internal Zones and the Public Zone. The interfaces to all Government On-Line services should be implemented in a PAZ. Proxy services, which allow Government of Canada (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 domain that protects internal GC networks and applications from a hostile Public Zone environment (e.g., the public Internet). The PAZ also acts as a screen that hides internal resources from the Public Zone and limits the exposure of internal resources. In short, a PAZ is meant to:

a. mediate access between operational systems and the Public Zone;

b. hide internal resources from the Public Zone; and

c. limit the exposure of internal resources.

A PAZ mediates access between GC internal networks and the Public Zone (e.g., Internet). Interfaces to all external services are implemented through a PAZ. Services that the PAZ could provide include proxy services to allow GC staff to access external services in the Public Zone, e-mail and other message gateways, service delivery applications, remote access, extranet access, and common support services.

In general, sensitive information should not be stored in a PAZ. Sensitive information may transit or be collected in a PAZ, but it should be transferred to databases in either a Restricted Zone (RZ) or Operations Zone (OZ) and accessed by applications in the PAZ. This approach limits the amount of sensitive information exposed should a compromise occur.

A.2 Reference Model

Section 4.3 describes the general reference model for a Network Security Zone and its components. This section of Annex A describes a reference model for the PAZ that is based on the general reference model.

A PAZ consists of:

a. End-Systems, which typically connect to the Demilitarized Zone (DMZ) Internetwork component (see Section A.2.1);

b. three types of Internetworks: an External Access Network (EAN), an Internal Access Network (IAN), and a DMZ (see Sections A.2.2, A.2.3, and A.2.4 respectively);

c. two types of Internal Boundary Systems (IBS): the EAN/DMZ Boundary System, and the IAN/DMZ Boundary System (see Section A.2.5); and

d. two types of Zone Interface Points (ZIP): Public Zone ZIP, and Internal Zone ZIP (see Sections A.2.6 and A.2.7 respectively).

A PAZ may have more than one of each component listed above. In addition, a PAZ may support part of a department, an entire department, or multiple departments.

Figure 8 below illustrates the logical topology for a PAZ. A Public Zone ZIP connects an EAN to a Public Zone (e.g., Internet, Public Switched Telephone Network (PSTN), or other external network). An EAN connects to a DMZ through an EAN/DMZ Boundary System that provides the Public-Zone-facing firewall function. An IAN connects to the DMZ through the IAN/DMZ Boundary System, which provides the internal firewall function. Internal GC Zones are accessed through an Internal Zone ZIP that connects the internal Zones to the IAN.

The outer box in Figure 8 defines the region that is considered to be under the control of a GC entity. More specifically, the point of demarcation between the PAZ and the Public Zone (e.g., Internet) is that point behind which all systems, networks, and assets are required to undergo certification and accreditation as mandated in the *Government Security Policy* (reference [19]).

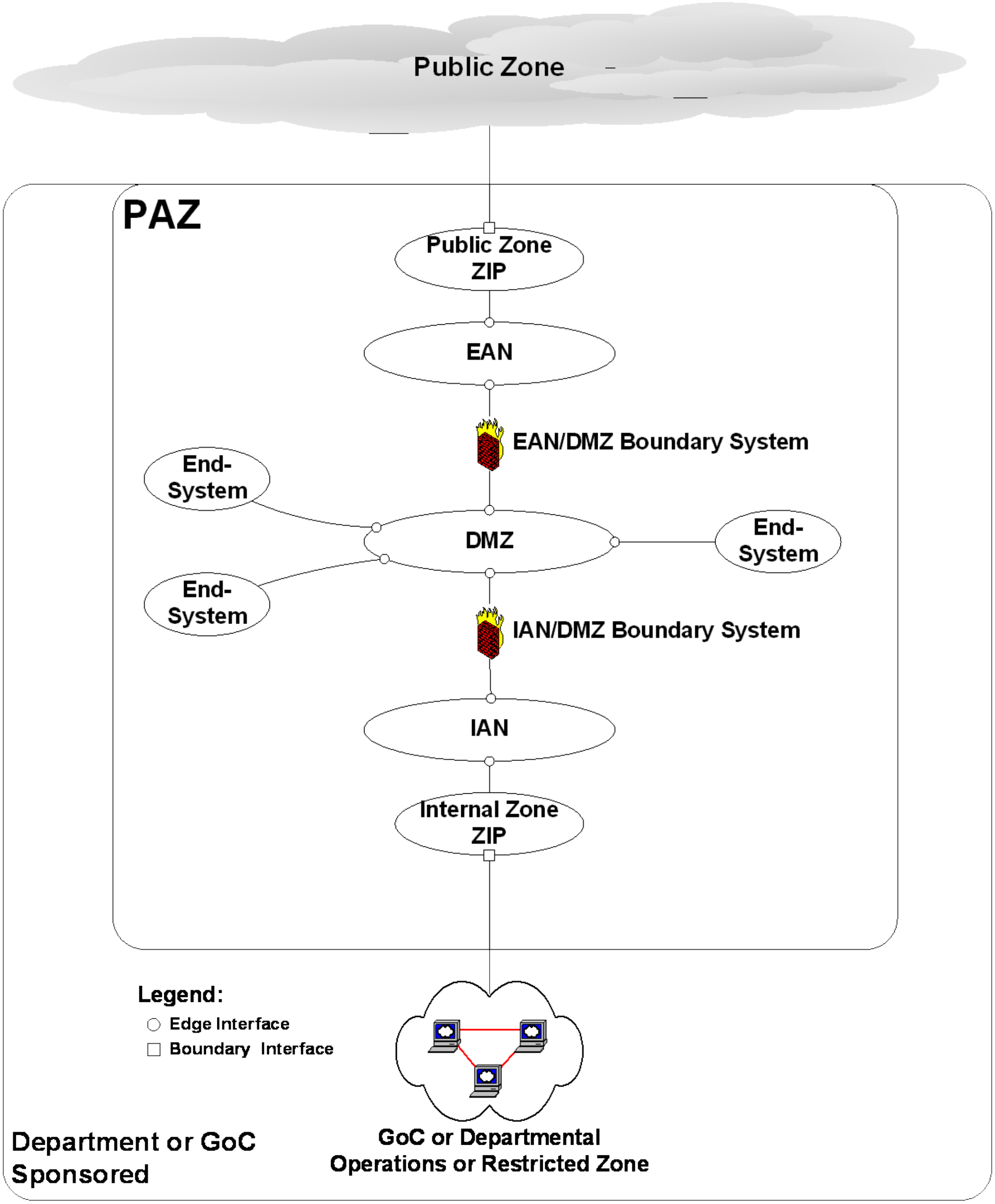


Figure 8 – Typical Public Access Zone (PAZ) Logical Topology

Figure 9 illustrates the PAZ logical architecture. It identifies the entities that make up the PAZ, the relations between entities, and the allocation of security services[7]. This figure provides an end-to-end mapping of the logical connection between the Public Zone, the PAZ, and internal GC Zones (i.e., OZs, RZs), including the security services that are provided at each Open Systems Interconnection (OSI) layer. The vertical lines depict the interfaces through which communications flow both up and down the protocol stack during a communications session. Note that when implementing a Secure Virtual Private Network (SVPN) gateway the traffic will be null (i.e., encrypted) across the EAN/DMZ boundary system. Additionally, if the DMZ were implemented using a single device (e.g., an appliance device) then the DMZ traffic in this instance would also be null.

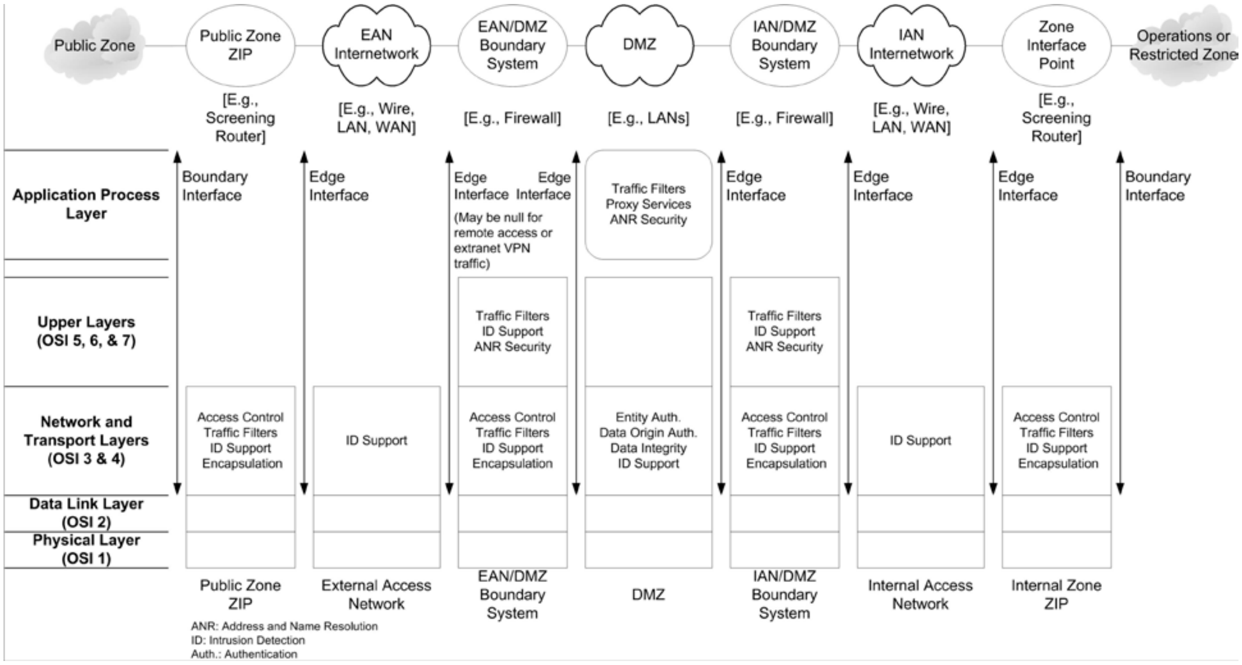


Figure 9 – PAZ Logical Architecture

A.2.1 End-Systems

End-Systems in the PAZ attach to the DMZ (see Section A.2.4 for more on the DMZ). They host application resources to which Public Zone systems (e.g., Internet systems) have direct access. An End-System in the DMZ may support the following functions, each of which has specific security objectives and requirements:

[7] The allocation of security services is based on the model of Section 4.4.2 and the requirements of Section A.4.2. See Section 4.4.2 for an explanation of the security services. In the PAZ, not every service is required in every component or OSI layer.

a. employee simple web access – provides access for GC employees to public Internet sites, rich media web and streaming media;

b. e-mail access – provides common communication tools such as e-mail for GC employees;

c. employee remote/mobile access[8] (includes mobile and wireless remote access and SVPN) – provides access to business resources for GC employees;

d. extranet services – provide a secure method of interfacing with partner organizations external to the GC;

e. service delivery applications – provide a web based interface to the public for GC services and departments; and

f. common support services – provide the common services required to run a modern, secure network, e.g., Domain Name Service (DNS), Border Directory Service Agent (DSA), Network Time Protocol (NTP).

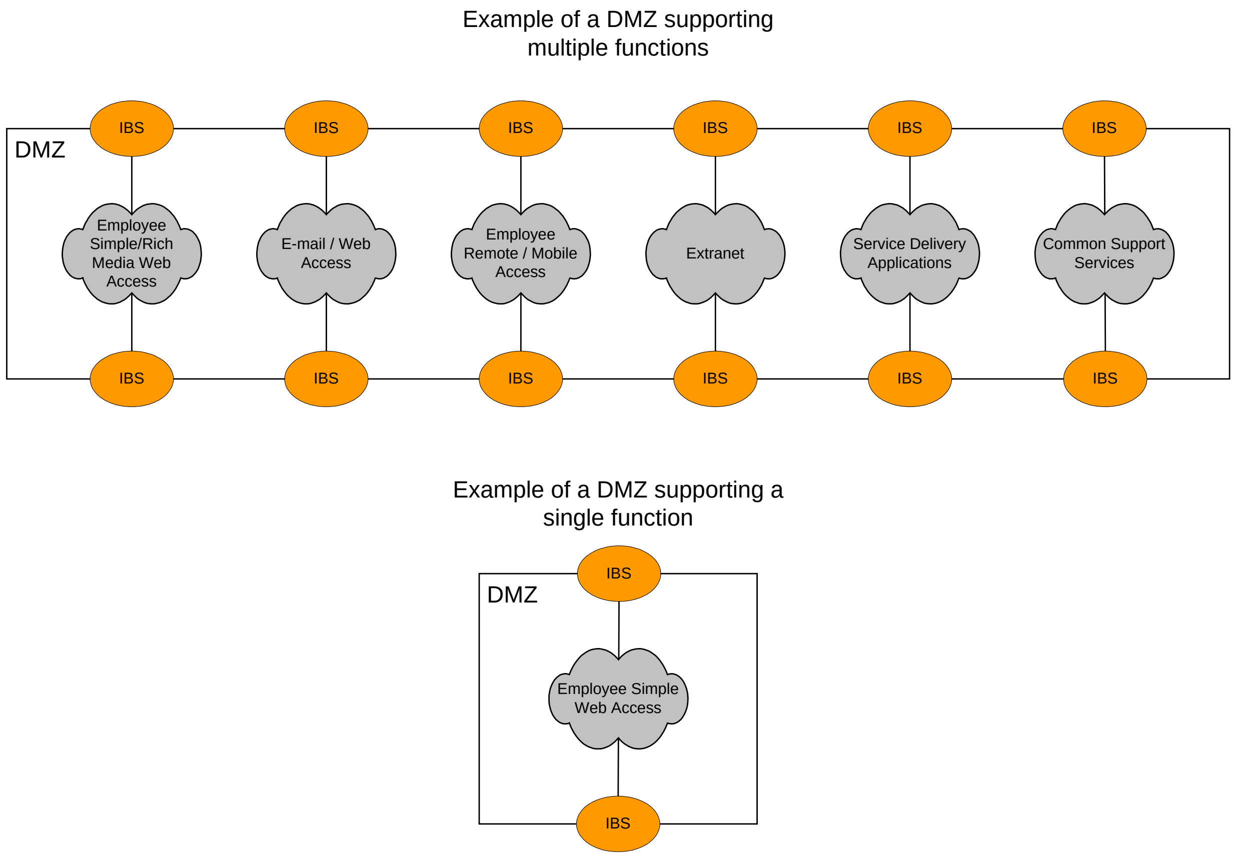
As Figure 10 shows, an individual PAZ need not implement all these functions. In fact, an individual PAZ will likely implement only a small subset of these services. For example, employee access services (e-mail, outgoing proxies, Voice Over Internet Protocol-to-PSTN, and remote access) are a valid grouping. On-line service delivery to the public may form another valid grouping of services. It is therefore expected that the size and the complexity of the DMZ and of the entire PAZ will vary considerably depending on departmental business requirements.

Common support services provide infrastructure functions that are necessary for the operation of the network. Common support services may be a public service (e.g., Public Key Infrastructure (PKI) user interface, Privilege Management Infrastructure user interface), a private service (e.g., intrusion detection, management protocol, network time), or a border service (e.g., border DNS, border DSA). Border services provide only a minimum subset of information to the public network that is necessary to inter-operate with the GC network.

An extranet provides a constrained extension of a private GC network to share information and resources for specific business needs with specific partners including other governments, industry, and non-governmental organizations. An extranet should terminate in a PAZ and be governed by standardized agreements with limited GC control over its external configuration. Note that this "general" extranet differs from the Restricted Extranet Zone (REZ) described in Section 4.2.8. A Restricted Extranet with highly trusted partners may terminate in any GC-

[8] Remote/mobile access in this publication includes only implementations that provide full network access for employees to resources on internal government networks. This use of remote/mobile access explicitly excludes access by IT personnel for remote management of network nodes. Some remote access solutions 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 considered Service Delivery Applications and the security requirements for Service Delivery Applications apply as discussed in the Federated Architecture Model (see reference [14]).

controlled Zone and would be governed by an agreement specific to the instance of the extranet with mutually agreed controls.


Example of a DMZ supporting multiple functions

Example of a DMZ supporting a single function
DMZ
IBS
Employee Simple/Rich Media Web Access
E-mail / Web Access
Employee Remote / Mobile Access
Extranet
Service Delivery Applications
Common Support Services
DMZ
IBS
Employee Simple Web Access

Figure 10 – Examples of PAZ DMZ

A.2.2 External Access Network (EAN)

The EAN is an Internetwork component that provides network services to connect the Public Zone to the DMZ. The GC controls the EAN (i.e., the EAN is owned by the GC or operated under agreement on behalf of a GC department or agency). It connects to a Public Zone (e.g., Internet) through a Public Zone ZIP. It connects to a DMZ though an EAN/DMZ Boundary System (e.g., firewall). An EAN allows a PAZ to support multiple points of presence to public networks and allows access to multiple DMZs through these points of presence. This supports survivable distributed designs.

The EAN is an Internetwork component within the Zones general reference model and thus includes the following subsystems:

a. Edge Interfaces to Public Zone ZIPs (present in all EANs);

b. Edge Interfaces to EAN/DMZ Boundary Systems (present in all EANs);

c. EAN Access Subsystem (may be trivial); and

d. EAN Core (may be trivial).

An EAN could be a substantial network infrastructure (e.g., Secure Channel Network) supporting access to the Internet and other Public Zones through multiple Public Zone ZIPs and access to multiple DMZ instances. At the other extreme, an EAN could be a cable connecting the Public Zone ZIP to an EAN/DMZ Boundary System. A generalized model is used to describe a comprehensive set of security requirements that apply either to a small scale PAZ or to a GC-wide PAZ.

A.2.3 Internal Access Network (IAN)

The IAN is an Internetwork component that provides network services to connect the DMZ to one or more OZs or RZs. The GC controls the IAN (i.e., the IAN is owned by the GC or operated under agreement on behalf of a GC department or agency). It connects to an OZ or RZ through an Internal Zone ZIP. It connects to a DMZ through an IAN/DMZ Boundary System (e.g., firewall).

The IAN is an Internetwork component within the Zones general reference model and thus includes the following subsystems:

a. Edge Interfaces to Internal Zone ZIPs (present in all IANs);

b. Edge Interfaces to IAN/DMZ Boundary Systems (present in all IANs);

c. IAN Access Subsystem (may be trivial); and

d. IAN Core (may be trivial).

As with the EAN, an IAN could be a substantial network infrastructure supporting access to multiple OZs and RZs through multiple Internal Zone ZIPs and supporting access to multiple DMZ instances. At the other extreme, an IAN could be a cable connecting an Internal Zone ZIP to an IAN/DMZ Boundary System. A generalized model is used to describe a comprehensive set of security requirements that apply either to a small scale PAZ or to a GC-wide PAZ.

A.2.4 Demilitarized Zone (DMZ)

A DMZ is an Internetwork component that provides a buffer between the EAN and the IAN. Traffic originating from a Public Zone is distributed by the EAN to a DMZ instance where the network traffic is processed by End-Systems attached to the DMZ before being forwarded through the IAN to an OZ or RZ. Traffic originating from an OZ or RZ is distributed by the IAN to a DMZ instance, where the network traffic is processed by End-Systems attached to the DMZ before being forwarded through the EAN to a Public Zone. The DMZ is protected from both the EAN and the IAN by IBSs.

A.2.5 Internal Boundary Systems (IBSs)

The EAN/DMZ and IAN/DMZ Boundary Systems are IBS components. Both implement traffic control functions to protect the DMZ from attack.

EAN/DMZ Boundary Systems are hardened against attacks from the Internet and other Public Zones and implement traffic control functions to protect the DMZ from network-based attacks. The EAN/DMZ Boundary Systems filter all traffic except for traffic destined for remote access or extranet gateways because these traffic types are encrypted (which is why Figure 9 shows that the EAN/DMZ Boundary System may be null with respect to remote access or extranet traffic).

IAN/DMZ Boundary Systems protect the DMZ from network-based attacks originating from OZs or RZs connected to the PAZ. IAN/DMZ Boundary Systems also implement traffic controls to protect OZs and RZs from attacks originating from compromised or improperly configured PAZ End-Systems.

The EAN/DMZ and IAN/DMZ Boundary Systems are logically distinct entities. However, in some implementations these components may be implemented on the same node. When the EAN/DMZ and IAN/DMZ are implemented on the same node, care must be exercised to ensure that the traffic control functions are isolated, traffic rules do not conflict, and that traffic is not able to flow directly between the EAN and IAN.

A.2.6 Public Zone ZIP

A Public Zone ZIP is used to control all types of traffic between the Public Zone and the PAZ. The Public Zone ZIP should be capable of filtering packets based on defined characteristics. The Public Zone ZIP hides the details of the network services from the Public Zone and presents only those services necessary for communications with the Public Zone.

A.2.7 Internal Zone ZIP

An Internal Zone ZIP is used to control and filter all traffic between the PAZ and internal Zones. The Internal Zone ZIP should be capable of filtering packets based on defined characteristics. It should support the implementation of proxy services. The Internal Zone ZIP should be capable of rejecting all malformed service requests. It hides the details of the PAZ network services from the Internal Zones and presents only those services necessary for communications with Internal Zones.

A.3 Security Objectives

In general, the PAZ provides a security service to other GC-controlled Zones, protecting these internal Zones from many of the threats that originate from the Public Zones. In particular, the PAZ aims to prevent (i.e., remove susceptibility to) network-based attacks from unsophisticated external attackers (i.e., external adversaries with minimal resources and limited skill) against internal Zones. It also aims to significantly reduce other sources and forms of attacks against internal Zones. The PAZ should also protect itself against attacks from public zones.

Each objective and requirement specified in this Annex is labelled according to the following notation:

a. the first set of letters (PZ) refers to the Zone;

b. the second set of letters designates either an objective (i.e., OBJ) or a requirement. Requirements are grouped into the following categories as applicable: network interface (NI), traffic control (TC), network configuration (NC), host configuration (HC) and data protection (DP); and

c. each objective or requirement is sequentially numbered within its group[9].

A.3.1 Traffic Control Objectives

[PZ-OBJ-100] The PAZ should mediate the flow of all traffic types between GC internal networks and the Public Zone. The PAZ should:

a. restrict data flows to a well-defined set of services and network protocols;

b. control access based on source and destination;

c. ensure that traffic conforms to the protocol definition;

d. ensure direct network connections between Public Zone ZIPs and Internal Zone ZIPs are restricted to traffic originating from strongly authenticated hosts; and

e. either block or raise an alert for traffic associated with known attacks.

[PZ-OBJ-101] All traffic types to and from the Public Zone should be controlled through Public Zone ZIPs and IBSs.

[PZ-OBJ-102] The PAZ should protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with PAZ security functions.

[PZ-OBJ-103] The PAZ should protect itself against unauthorized changes to the network configuration.

[PZ-OBJ-104] The PAZ should provide the first line of protection against malicious traffic and mobile code.

[PZ-OBJ-105] The PAZ should help reduce illegal or illicit usage of network resources by authorized users.

[9] These numbers may differ from defined in the previous version of this document (ITSD-02). Annex F to this Guideline maps the old objective and requirement numbers to the new ones. Future versions of this Guideline should maintain objective and requirement numbers across versions and indicate whether an objective or requirement has been rescinded or added.

A.3.2 Network Availability and Reliability Objectives

[PZ-OBJ-106] The PAZ should be designed and implemented to support departmental and GC service delivery and business objectives.

[PZ-OBJ-107] The PAZ should effectively protect itself and GC internal resources against sustained and non-sustained cyber attacks originating from the Public Zone.

[PZ-OBJ-108] The PAZ should employ segregation to isolate and minimize the impact of security failures such that a security failure in a node or subnet should not trigger security failures in other nodes or subnets. In particular, critical services should be segregated to ensure continued service delivery.

[PZ-OBJ-109] The PAZ should provide the capability to dynamically alter its configuration when required to ensure continuity in the delivery of essential services. Dynamic configuration changes may be automated or require operator intervention.

[PZ-OBJ-110] The PAZ common support services should meet or exceed the minimum availability requirements of any dependent e-government services.

A.3.3 Data Protection Objectives

[PZ-OBJ-111] The PAZ should be capable of supporting network-layer security services as required for extranets and remote/mobile access.

[PZ-OBJ-112] The PAZ should be capable of supporting the use of application-layer security services to protect against the unauthorized or inadvertent disclosure and modification of data communicated through the PAZ.

[PA-OBJ-113] The PAZ should provide a Security Audit[10] service to assist in the investigation, detection, response, and recovery from incidents.

[PA-OBJ-114] All Security Audit information should be protected against inadvertent or unauthorized disclosure, modification, or destruction.

A.3.4 Security Objectives for the Demilitarized Zone (DMZ) Functional Services

Each of the six functions provided through the DMZ has a distinct set of security objectives. This section describes the high-level security objectives that are achieved through the security applied to each service.

[10] The Security Audit service and the governing Security Audit policy are outside the scope of this Guideline. A Security Audit policy defines auditable events (such as configuration changes and potential security incidents) and identifies rules to be applied for the collection and recording (in an audit trail) of the various security-related information and events, and the analysis of the audit trail information. The Security Audit service implements the applicable Security Audit policy. At this point, the security audit service and security audit policy will be defined by departments to meet local requirements in accordance with the *GSP* requirement for continuous monitoring, though audit service and policy requirements may be addressed in a future standard.

[PZ-OBJ-115] The security objectives for Employee Simple Web Access/Rich Media Access are to:

a. separate internal networks from Public Zone through proxy services;

b. permit outgoing web access through tightly controlled interfaces;

c. terminate established connections within the DMZ;

d. protect external networks from malware; and

e. protect the internal network from malware.

[PZ-OBJ-116] The security objectives for E-mail Access are to:

a. separate internal networks from Public Zone through e-mail gateways;

b. permit incoming and outgoing mail traffic through tightly controlled interfaces;

c. protect the internal network from malware;

d. protect external recipients from malicious e-mail traffic originating from the GC; and

e. protect internal and external networks from spamming and other e-mail attacks.

[PZ-OBJ-117] The security objectives for Employee Remote/Mobile Access are to:

a. provide strong authentication of remote/mobile users;

b. permit access to internal GC Zones for authorized users; and

c. secure all remote/mobile access traffic with an SVPN.

[PZ-OBJ-118] The security objectives for Extranet Services are to:

a. provide mutual authentication of extranet interfaces;

b. provide access controls to restrict access to internal GC resources;

c. protect against malicious traffic originating from partners;

d. ensure accountability of extranet partners;

e. protect partner network from malicious traffic originating from the GC; and

f. protect data exchanged with extranet users during transmission.

[PZ-OBJ-119] The security objectives for Service Delivery Applications are to:

a. provide entity authentication of peer services and individuals as needed;

b. provide confidentiality and privacy commensurate with sensitivity of delivered information and the GC service;

c. protect against malicious traffic originating from service delivery peers/users;

d. protect the GC information repositories by providing separation from public-facing service delivery applications;

e. provide availability of infrastructure services in accordance with availability agreements (e.g., high availability);

f. ensure horizontal interoperability with shared common infrastructure is not impaired by security mechanisms; and

g. support service delivery accountability.

Note: Security services specific to the Service Delivery Applications, such as access control and non-repudiation services should be provided by application specific components deployed in DMZ.

[PZ-OBJ-120] The security objectives for Common Support Services are to:

a. provide continuous availability of infrastructure services such as naming and directory services to support dependency of higher-level services and applications;

b. ensure integrity of common support services provided to higher-level services and applications;

c. protect private information used by and transported through common support services; and

d. ensure authentication of peer services.

A.4 Security Requirements

This section describes the baseline security requirements for the PAZ. These are categorized by operational requirement (i.e., network interface, traffic control, network configuration, host configuration, and data protection). Within each operational requirement category are sub-categories consisting of common requirements that apply across the entire PAZ, followed by requirements specific to each of the different Internetworks (DMZ, EAN, and IAN). Note that in some cases, a sub-category may not exist or have a heading because perimeter defence requirements are not applicable for that sub-category within that operational requirement category, or are common to the entire category.

To achieve all of the Security Objectives for this Zone, as detailed above, the complete set of Security Requirements which follows must be implemented.

A.4.1 Network Interface Requirements

A.4.1.1 Common Network Interface Requirements

[PZ-NI-100] Except as noted below, PAZ nodes should not be connected, either simultaneously or periodically, to another Zone. (PAZ nodes include devices such as, but not limited to, laptops, printers, gateways, switches, multiplexers, routers, and computers.) The only types of nodes that may participate in a PAZ and another Zone are:

a. nodes within an Internal Zone ZIP;

b. nodes within a Public Zone ZIP;

c. nodes within the EAN core; and

d. nodes within the IAN core.

[PZ-NI-101] All PAZ components should support the attachment of network-based intrusion detection sensors. The attachment points should enable a complete view of all traffic.

A.4.1.2 Demilitarized Zone (DMZ) Network Interface Requirements

[PZ-NI-102] To protect the DMZ from interference and tampering by untrusted subjects, the DMZ should isolate its internal network from any other network infrastructure including the PAZ, EAN, and IAN. That is, the DMZ should not share:

a. any network-layer infrastructure with any other Zone or Internetwork component;

b. any data link-layer infrastructure with any other Zone or Internetwork component; or

c. any physical-layer infrastructure with any Public Zone.

Note: A DMZ may share physical-layer infrastructure with GC-controlled Zones.

A.4.1.3 External Access Network (EAN) Interface Requirements

[PZ-NI-103] The EAN should be a logically separate network. It should maintain traffic interfaces only with:

a. a Public Zone through a Public Zone ZIP; and

b. the DMZ through an EAN/DMZ Boundary System (for extranet and remote access traffic, the EAN/DMZ Boundary System may be a null device. See PZ-TC-135 and PZ-TC-147.).

Note: The EAN may share physical-layer, data link-layer, and network-layer infrastructure with any Zone (including a Public Zone).

Rationale: A public commercial carrier may provide this network, in which case, the Crown usually has little or no control over whether the leased network is shared.

A.4.1.4 Internal Access Network (IAN) Interface Requirements

[PZ-NI-104] The IAN should be a logically separate network. It should maintain traffic interfaces only with:

a. an OZ through an OZ ZIP;

b. an RZ through an RZ ZIP; and

c. the DMZ through an IAN/DMZ Boundary System.

Note: The IAN may share physical-layer, data link-layer, and network-layer infrastructure with any Zone (including a Public Zone).

[PZ-NI-105] If the IAN shares physical-layer, data link-layer, or network-layer infrastructure with another Zone such sharing should occur only in the IAN Core.

Note: Additional requirements concerning the logical separation between PAZ components and other network infrastructure are found in Section A.4.3 – Network Configuration Requirements.

Rationale: In some cases, a public commercial carrier may provide the IAN infrastructure. This implementation is acceptable provided there are security mechanisms in place to ensure logical isolation. A commercially provided implementation requires significant trust in the network equipment (e.g., routers) to avoid intrusions from the public network. Consequently, sharing of DMZ access and internal boundary devices is not permitted (i.e., sharing should occur only within the IAN core).

A.4.2 Traffic Control Requirements

A.4.2.1 Common Traffic Control Requirements

[PZ-TC-100] All data flows between the Public Zone and the GC should be made through a PAZ. That is, there should be no direct connections between the Public Zone and GC networks located in Zones other than a PAZ.

[PZ-TC-101] The PAZ should limit available network paths for vulnerable or sensitive End-Systems (e.g., test and development sub-networks).

[PZ-TC-102] The PAZ should implement traffic control functions within IBSs at the boundaries of the DMZ and the IANs and EANs.

[PZ-TC-103] IBSs should implement network-layer and upper-layer controls to protect DMZ hosts from traffic originating from other Zones and to protect other Zones in the event that malicious traffic originates from within the DMZ.

[PZ-TC-104] PAZ management traffic, other than traffic related solely to device status, should be segregated from operational traffic.

Note: Segregation may be either virtual or physical. That is, segregation may be achieved through cryptography, network access controls, or physical separation.

[PZ-TC-105] Hosts in a Public Zone should not be able to direct management traffic at hosts located in the PAZ.

[PZ-TC-106] The PAZ should be capable of responding quickly to heightened security levels in case of emergency and increased threat, when and how authorized to do so. (Personnel should be aware, trained and authorized to initiate such a response.) For example, the PAZ should possess the capability to improve the network security posture by increasing the level of security measures such as:

a. filtering at each PAZ interface;

b. active and/or passive monitoring;

c. protection to ensure the continuous delivery of critical services, including the capability to reconfigure or block non-essential services if required; and

d. auditing.

Note: Implementation of such measures should be carefully tested to reduce the likelihood of exploitation via a denial-of-service (DoS) attack.

[PZ-TC-107] No continuous logical path at any OSI layer should be established between a host located in a Public Zone and a host located in an internal GC Zone unless explicitly permitted by requirements contained in this Guideline. That is, all network paths between hosts in a Public Zone and hosts in an internal GC Zone should be subject to mediation by an application process located within the PAZ.

[PZ-TC-108] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

A.4.2.2 Demilitarized Zone (DMZ) Traffic Control Requirements

These DMZ requirements can be read in conjunction with Figure 9.

[PZ-TC-109] All connections originating from the IANs or EANs should terminate in the DMZ.

[PZ-TC-110] Within the DMZ, traffic should be segregated so that traffic may flow only between related nodes.

Rationale: Segregation within the DMZ limits the impact of compromise of a DMZ host. For example, a compromised web server should not be able to be used to attack other hosts within the DMZ.

[PZ-TC-111] Traffic associated with different service classes should be strictly segregated and any requested communication between the service classes should flow through well-defined interfaces.

[PZ-TC-112] A DMZ that supports more than one function (as defined in Section A.2.1) or more than one security domain should provide separation between the functions and security domains to:

a. prevent interference between security domains;

b. support specific access policies;

c. protect sensitive or critical functions on dedicated hosts;

d. ensure continued delivery of critical services; and

e. ensure that any compromises of the DMZ end systems are contained within the DMZ.

[PZ-TC-113] Care should be taken to ensure that traffic rules do not conflict. Where a potential conflict exists, it may be necessary to physically separate functions or security domains and the associated IBSs into dedicated DMZ clusters.

[PZ-TC-114] In the case where the EAN provides access to multiple DMZs, the EAN registered address space should be partitioned into multiple subnets to provide a unique address space per DMZ interface.

Rationale: To support segregation of traffic types and facilitate audit and identification.

A.4.2.3 Employee Web Access Traffic Control Requirements

[PZ-TC-115] To provide Employee Web Access, functionality should permit Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), and File Transfer Protocol (FTP) originating from GC employees to be processed within the PAZ network.

Rationale: While employees may require access to the Web to perform their job functions, the normal limits on available protocols have to be employed. Departments may implement additional access controls based on job duties and functions, but to support common implementation requirements, the PAZ should support the above protocols.

[PZ-TC-116] All Employee Web Access Traffic should be processed by a proxy service. Proxy services should be capable of supporting the following functions:

a. content filtering and scanning;

b. web access management (i.e., Uniform Resource Locator filtering);

c. quarantine or removal of illicit traffic;

d. notification; and

e. logging.

[PZ-TC-117] Inbound FTP, HTTP, and HTTPS traffic for established connections from the Public Zone should be mediated in the DMZ.

[PZ-TC-118] The DMZ should support the detection and blocking of malware and mobile code.

[PZ-TC-119] The PAZ Network Security Zone Authority should administer malware detection and content filtering.

[PZ-TC-120] Monitoring and content filtering should be consistent with the *Policy on the Use of Electronic Networks* (reference [30]).

[PZ-TC-121] The address translation policy for simple web access should map outgoing traffic to external addresses so that external websites can associate traffic with individual departments.

A.4.2.4 E-mail Traffic Control Requirements

[PZ-TC-122] For GC employees to send/respond to e-mails received from Public Zone, outbound e-mail (e.g., Simple Mail Transfer Protocol) traffic should be permitted.

[PZ-TC-123] Similarly, for GC employees to receive e-mails originating from the Public Zone, inbound e-mail traffic should be permitted.

[PZ-TC-124] All inbound and outbound e-mail traffic should terminate in the DMZ.

[PZ-TC-125] All e-mail traffic (except in those instances where end-to-end encryption is used) should be mediated and processed by an e-mail gateway that is capable of providing content filtering and protection against mobile code and/or malware[11].

[PZ-TC-126] Content filtering should be consistent with the *Policy on the Use of Electronic Networks* (reference [30])[12].

[PZ-TC-127] Inbound e-mail traffic should only be relayed to a restricted list of peer GC e-mail servers.

[PZ-TC-128] Except in those instances where end-to-end encryption is used, all inbound e-mail traffic and attachments should be scanned for malware before being relayed to a specific GC e-mail server located in a GC RZ or OZ.

[PZ-TC-129] Except in those instances where end-to-end encryption is used, all outbound e-mail traffic and attachments should be scanned for malware before being relayed to a Public Zone Message Transfer Agent.

Rationale: If departments do not do this and they spread malware, they could be held liable through neglect.

[PZ-TC-130] The PAZ Network Security Zone Authority, guided by the *Policy on the Use of Electronic Networks*, should determine if:

a. a content scanner should be used in the PAZ to detect and quarantine/delete e-mails that may contain sensitive data, offensive content, or illicit language;

b. attachments that may, for example, contain audio, video, or executable code are to be blocked;

c. extra-large e-mails are to be stored for delivery at off peak hours; and/or

d. spam is to be blocked.

[11] Where scanning and content filtering cannot be performed at the DMZ, for example, where end-to-end encryption is used, equivalent protection must be provided at the end systems.

[12] Scanning for malware in the DMZ does not remove the requirement for a department to install and maintain GC-mandated malware scanning software on GC internal e-mail server(s) and clients.

[PZ-TC-131] Incoming (from another Zone) e-mail traffic with a “From:” address belonging to an entity within the Zone should be blocked. Outgoing (to another Zone) e-mail traffic with a “From:” address belonging to an entity outside the Zone should be blocked. Measures should be taken to ensure the legitimacy of e-mail source and destination addresses (e.g., digital signature).

Rationale: These measures will block spoofed e-mail addresses.

A.4.2.5 Remote/Mobile Access Traffic Control Requirements

[PZ-TC-132] For GC employees to access GC internal resources in an OZ or an RZ, remote access should be permitted from the Public Zone through tightly controlled interfaces in the PAZ.

[PZ-TC-133] Remote access should be restricted to traffic originating from authorized and authenticated network entities. The following security services should be used at the network layer:

a. peer-entity authentication, using strong authentication (as defined in Section 5), should be enforced at the PAZ. This includes support for both host and user mobility; and

b. data origin authentication.

[PZ-TC-134] The GC PKI should be employed to provide strong authentication for peer-entity authentication. In addition, two-factor authentication for users is recommended.

[PZ-TC-135] Access controls to another GC Zone should be enforced based on the authenticated identity of the remote access client.

[PZ-TC-136] All mobile access SVPN traffic originating from the Public Zone should terminate at an SVPN gateway. The SVPN gateway should be located within the EAN/DMZ Boundary System. It is recommended that this traffic be completely decrypted at the SVPN gateway.

Rationale: Remote/mobile access traffic supports employee access to internal Zones. In most cases, this traffic would not need to be encrypted inside the destination Zone. As such, it is recommended that this traffic be completely decrypted at the SVPN gate to permit traffic controls to be applied within the DMZ and at the EAN/DMZ Boundary System. However, in some cases requirements exist to provide end-to-end encryption. This should be done using nested tunnels so that authentication can be performed in the PAZ. The next requirement addresses remote/mobile access points to support nested tunnels.

Note: See reference [18] for a detailed discussion of SVPN design.

[PZ-TC-137] Subject to the above requirements, remote/mobile access points should support secure end-to-end communications using nested tunnels from the client to the destination host within another GC Zone.

[PZ-TC-138] GC-sponsored dial-in services such as Remote Access Service servers should be located in the DMZ.

A.4.2.6 Service Delivery Applications Traffic Control Requirements

[PZ-TC-139] All inbound and outbound Service Delivery traffic should terminate in the DMZ.

[PZ-TC-140] Security associations between Service Delivery End-Systems and application components installed in the DMZ and back-end servers or databases should be tightly controlled. These security associations should be established using strong peer-entity authentication.

[PZ-TC-141] All Service Delivery traffic should be mediated and processed by application processes in the DMZ.

[PZ-TC-142] The DMZ should support the detection and blocking of malware and mobile code.

A.4.2.7 Extranet Services Traffic Control Requirements

[PZ-TC-143] Extranet traffic should be restricted to traffic originating from authorized and authenticated network entities.

[PZ-TC-144] At a minimum, strong peer-entity authentication at the network layer should be used between the external party's extranet Point of Presence (PoP) and the PAZ.

[PZ-TC-145] Data Origin Authentication should be used at the network layer.

[PZ-TC-146] The GC PKI should be employed to provide strong authentication for peer-entity authentication.

[PZ-TC-147] Access controls to another GC Zone should be enforced based on the authenticated identity of the extranet PoP.

Note: The extranet agreement should require the partner to restrict access to authorized hosts within its own network.

[PZ-TC-148] All extranet SVPN traffic originating from the Public Zone should terminate at an SVPN gate. The SVPN gate should be located within the DMZ (i.e., behind an EAN/DMZ Boundary System) or the SVPN gate should act as an EAN/DMZ Boundary System.

Rationale: To protect an unauthorized connection to an OZ or RZ, the SVPN device should be located in the DMZ.

[PZ-TC-149] Subject to the above requirements, extranet points of presence should support secure end-to-end communications using nested tunnels from the client to the destination host within another GC Zone.

Note: The above requirements limit the ability of the PAZ to identify malware and malicious traffic. GC hosts participating in an extranet need additional intrusion detection and malware detection.

A.4.2.8 Common Support Services Traffic Control Requirements

[PZ-TC-150] The PAZ naming service instance should logically separate internal GC naming information from Public Zone naming information.

[PZ-TC-151] All naming service traffic from the Public Zone should be directed to the border naming service instance located in the PAZ.

[PZ-TC-152] Transfer of internal GC naming service configurations should not be permitted to the Public Zone.

[PZ-TC-153] Transfers of GC naming configurations to the PAZ Border naming service instance should only be permitted from GC naming service peers.

[PZ-TC-154] Transfers of Public Zone naming configurations should only be permitted from the Public Zone Service Provider naming service.

[PZ-TC-155] The PAZ time service instance should logically separate internal GC time service from Public Zone time service.

Rationale: A time service based on the NTP, which runs over the Internet Protocol (IP) and is documented in Request for Comments (RFC) 1305 (reference [24]), synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur. See also the section on a trusted time source in Government of Canada – PKI Network Architecture with Automated Certificate Issuance, Roaming Profiles, and Trusted Time Clocks (reference [17]).

[PZ-TC-156] Transfer of NTP from the Public Zone should be directed to the time service instance located in the PAZ.

A.4.2.9 External Traffic Control Requirements

External Traffic Control requirements can be read in conjunction with Figure 9. Unless a specific allocation is indicated, External Traffic Control Requirements may be allocated to Public Zone ZIPs, EANs, or the EAN/DMZ Boundary Systems, or may be distributed across a combination of these components.

[PZ-TC-157] By default, all traffic types (i.e., associated ports and services) originating from the Public Zone should be blocked by Public Zone ZIPs and the EAN/DMZ Boundary Systems unless there are specific departmental and GC business requirements to allow a particular traffic type.

[PZ-TC-158] The PAZ Network Security Zone Authority should be responsible for ensuring that only traffic types (i.e., associated ports and services) that are essential to the department and GC business activities are permitted.

[PZ-TC-159] A packet-filtering device should be utilized at each Public Zone ZIP to control the access to the PAZ EAN.

[PZ-TC-160] The Public Zone ZIP should be capable of filtering packets based on the following characteristics:

a. protocols;

b. source and destination address (e.g. IP, MAC);

c. source and destination ports; and

d. address from which the packets originate.

[PZ-TC-161] Filtering of all IP packets originating from a Public Zone should be performed at both Public Zone ZIPs and EAN/DMZ Boundary Systems to ensure that only appropriate packet types, and packets with appropriate service access points and source and destination addresses, are permitted to enter the PAZ. At a minimum, filtering of traffic originating from the Public Zone should:

a. block any traffic containing directed broadcast addresses;

b. block any traffic containing a network loop-back address;

c. block traffic destined to *RFC 1918* (reference [32]) reserved addresses;

d. block network traffic containing a source or destination address of 0.0.0.0;

e. block inbound traffic with an internal source IP address;

f. block any traffic containing IP source routing information;

g. block any management traffic (e.g., Simple Network Management Protocol);

h. block Internet Control Message Protocol (ICMP) broadcasts; and

i. block any traffic determined to have malicious intent against the EAN.

Rationale: Protection against DoS attacks and spoofing.

[PZ-TC-162] Once filtered, traffic originating from a Public Zone should be routed to the specific DMZ interface based on a specific destination and service.

[PZ-TC-163] Filtering of IP packets destined for a Public Zone should be performed to prevent any packets with invalid or incorrect addresses from leaving the EAN.

Rationale: Prevent Distributed Denial-of-Service attacks and use of illegal addresses.

[PZ-TC-164] Filtering of IP packets destined for a Public Zone should be performed to block packets containing a GC private IP address as their source IP address.

Rationale: Ensuring that GC private addresses are not leaked.

[PZ-TC-165] Unless specifically required by an application, the external network systems (i.e., Public Zone ZIPs, EAN, and EAN/DMZ Boundary Systems) should only allow protocols that can be examined with a proxy service.

[PZ-TC-166] EAN/DMZ Boundary Systems should be capable of mediating and examining inbound and outbound packets up through the Application Layer (i.e., up to Layer 7) of the OSI model.

[PZ-TC-167] The external network components (i.e., Public Zone ZIPs, EAN, and the EAN/DMZ Boundary Systems) should provide encapsulation for PAZ resources.

Rationale: Encapsulating PAZ resources serve a number of security functions. It limits access to any non-public interface; facilitates the detection of malicious activity, supports fault-tolerant implementations, and facilitates incident response and recovery. Encapsulation of network resources within Traffic Control Protocol (TCP)/IP networks is typically implemented using port and address translation.

[PZ-TC-168] The EAN should be capable of rejecting all malformed service requests.

[PZ-TC-169] The design of the Public Zone ZIPs, EAN, and EAN/DMZ Boundary Systems should not hinder or adversely affect the following functions:

a. encryption of communications;

b. Internet Protocol Security (IPSec); and

c. integration with the GC PKI.

[PZ-TC-170] In a case where the EAN provides access to multiple services, the EAN registered address space should be partitioned into multiple subnets to provide a unique address space for each service interface.

Rationale: To support segregation of traffic types and facilitate audit and identification.

A.4.2.10 Internal Traffic Control Requirements

These Internal Traffic Control Requirements can be read in conjunction with Figure 9. Unless a specific allocation is indicated, Internal Traffic Control Requirements may be allocated to Internal Zone ZIPs, IAN, or the IAN/DMZ Boundary Systems, or may be distributed across a combination of these components.

[PZ-TC-171] By default, all traffic types should be blocked by the Internal Zone ZIPs and the IAN/DMZ Boundary Systems unless there are specific departmental and GC business requirements to allow a particular traffic type.

[PZ-TC-172] The PAZ Network Security Zone Authority should be responsible for ensuring that only traffic types (i.e., associated ports and services), which are essential to the department and to GC activities, are permitted.

[PZ-TC-173] The Internal Zone ZIP should be capable of filtering packets based on the following characteristics:

a. protocols;

b. source and destination address (e.g. IP, MAC);

c. source and destination ports; and

d. address from which the packets originate.

[PZ-TC-174] IAN/DMZ Boundary Systems should be capable of mediating and examining inbound and outbound packets up through the Application Layer (i.e., up to Layer 7) of the OSI model.

[PZ-TC-175] Filtering of IP packets originating from an internal GC Zone should be distributed between the IAN/DMZ Boundary Systems and Internal Zone ZIPs to ensure that only appropriate packet types, and packets with appropriate service access points and source and destination addresses, are permitted to enter the PAZ. At a minimum, filtering of traffic should:

a. block any traffic containing directed broadcast addresses;

b. block any traffic containing a network loop-back address;

c. block traffic destined to *RFC 1918* (reference [32]) reserved addresses;

d. block network traffic containing a source or destination address of 0.0.0.0;

e. block any traffic containing IP source routing information;

f. block ICMP broadcasts; and

g. block any traffic determined to have malicious intent against the IAN.

[PZ-TC-176] Unless specifically required by an application, the internal network systems (i.e., Internal Zone ZIPs, IAN, and IAN/DMZ Boundary Systems) should only allow protocols that can be examined with an application proxy. That is, all outbound traffic (i.e., traffic originating from an RZ or OZ) should be mediated and processed by application proxies.

[PZ-TC-177] The internal network components (i.e., Internal Zone ZIPs, IANs, and the IAN/DMZ Boundary Systems) should provide encapsulation for PAZ resources.

[PZ-TC-178] Traffic originating from an internal GC Zone should be routed to the appropriate DMZ interface based on destination and service.

[PZ-TC-179] Traffic destined to an internal GC Zone should be routed to the appropriate Internal Zone ZIP interface based on destination and service.

[PZ-TC-180] The internal network systems (i.e., Internal Zone ZIPs, IANs, and IAN/DMZ Boundary Systems) should be capable of rejecting all malformed service requests.

[PZ-TC-181] The design of the Internal Zone ZIPs, IAN, and IAN/DMZ Boundary Systems should not hinder or adversely affect the following functions:

a. encryption of communications;

b. IPSec; and

c. integration with the GC PKI.

[PZ-TC-182] In the case where the IAN provides access to multiple services, the IAN address space should be partitioned into multiple subnets to provide a unique address space for each service interface.

Rationale: To support segregation of traffic types and facilitate audit and identification.

A.4.3 Network Configuration Requirements

[PZ-NC-100] The PAZ should be continually monitored for changes to its network configuration. All identified changes should be validated and categorized as authorized, network fault, or potential intrusion. Potential intrusions should be handled as security incidents. Where required by the Security Audit service, changes to the network configuration should be recorded in the Security Audit log.

[PZ-NC-101] If remote management is allowed, a PAZ should allow only authorized administrator(s) to remotely manage PAZ nodes from a GC-controlled Zone or from a REZ. The access should be controlled and protected by using the following methods:

a. strong authentication[13]; and

b. restricting access by address (e.g. IP, MAC) , port, and protocol.

Note: If a department authorizes the use of an outsourced commercial provider to manage the department's PAZ, the commercial provider's site would have to satisfy the requirements for a Restricted Extranet Zone (as determined on a case-by-case basis). Significant care is required in establishing this outsourcing agreement to ensure that this arrangement does not compromise the PAZ security objectives. Such agreements should include some flexibility for changing the security parameters, based on new requirements resulting from TRAs or other threat/vulnerability information received through authoritative channels. Personnel security plays a key role in the security implications of contracted services, and the Principles of Separation of Duties, Need-to-Know and Least Privilege should be addressed within outsourcing agreements.

[PZ-NC-102] All Boundary and Edge Interfaces should be registered with and approved by the PAZ Network Security Zone Authority before attachment to the Zone.

[PZ-NC-103] Each interface should act in exactly one role: Boundary Interface or Edge Interface.

[PZ-NC-104] The PAZ should implement the following constraints on address space for interfaces:

a. EAN Edge Interface addresses should be distinct and dedicated, but not necessarily private;

[13] Two-factor authentication is also recommended in high-threat environments.

b. DMZ interface addresses should be distinct and assigned from a private non-routable address space;

c. IAN Edge Interface addresses should be distinct; and

d. IAN Edge Interface addresses should be private.

[PZ-NC-105] Boundary Interfaces should be assigned addresses upon attachment to the network.

[PZ-NC-106] A change to a Boundary Interface address assignment should constitute a configuration change requiring approval. Approval may be given in advance to permit dynamic reconfiguration; however, the conditions under which such a change may be effected should be clearly delineated.

[PZ-NC-107] Edge Interfaces should establish security associations with other Edge Interfaces and all communications should be authenticated (either explicitly or implicitly) within the context of these security associations. The security associations permitted should be determined by traffic control requirements.

Note: The type and strength of authentication are implementation dependent. The goal is to prevent an intruder attaching a Network-layer entity in the core and masquerading as an Edge Interface.

[PZ-NC-108] IAN Edge Interfaces should be authenticated to each other. (Because the IAN is behind the DMZ access devices (e.g., firewalls), it is extremely important that hostile entities be excluded from masquerading as an Edge Interface.) This authentication may be achieved through one of the following methods:

a. strong authentication applied at the network layer;

b. physical controls over the Edge Interfaces and over all media connecting these interfaces; or

c. physical controls over the Edge Interfaces and approved network- and lower-layer controls implemented within the core network connecting these interfaces.

[PZ-NC-109] If a Network Service Provider is responsible for providing security controls within the core network to maintain the security association between Edge Interfaces, the service level agreement should include provisions to ensure that these security controls are effective.

[PZ-NC-110] The service level agreement should require the Network Service Provider to control changes to core interfaces and to report to the Network Security Zone Authority any changes that affect the security association between edge devices.

[PZ-NC-111] The service level agreement should require the Network Service Provider to provide evidence that the security controls used to enforce the security within the core network are effective and to report to the Network Security Zone Authority all security incidents that could impact the PAZ. The Network Service Provider should also provide the Network Security Zone Authority with the capability to verify the effectiveness of the controls on at least a quarterly basis.

[PZ-NC-112] All interfaces in the DMZ should be registered with the Network Security Zone Authority before attachment to the PAZ.

[PZ-NC-113] A change to a DMZ interface address assignment should constitute a configuration change requiring approval. Approval may be given in advance to permit dynamic reconfiguration; however, the conditions under which such a change may be effected should be clearly delineated.

A.4.4 Host Configuration Requirements

[PZ-HC-100] All nodes in the PAZ should configure features to ensure the maximum protection against intrusion. This includes, but is not limited to:

a. strictly limiting the number of operating system accounts and ensuring that the security Principle of "*least privilege*" is strictly applied to each account;

b. ensuring that the most appropriate authentication is used for all accounts depending on departmental business requirements and risk assessment;

c. disabling all unnecessary services (i.e., the software load configuration is the minimum necessary to provide required functions); and

d. ensuring only authorized administrators are given user accounts for perimeter/boundary nodes (e.g., for DMZ access devices, routers, intrusion detection systems, etc.), in accordance with the Principle of Need-to-Know.

[PZ-HC-101] Operating systems for all nodes should be hardened based on documented best practices.

[PZ-HC-102] rescinded.

[PZ-HC-103] PAZ EAN/DMZ Boundary Systems should be documented and approved by the accreditation Authority for the PAZ.

Rationale: DMZ access devices perform security-critical services that require a high degree of assurance to resist attack and prevent intrusions into GC networks.

[PZ-HC-104] SVPN products, if used, should be validated to Federal Information Processing Standard (FIPS) 140-1 or FIPS 140-2 at a minimum of Security Level 2 through the Cryptographic Module Validation Program (CMVP).

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and Cryptographic Endorsement Program (CEP), each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the Cryptographic Algorithm Validation Program (CAVP).

[PZ-HC-105] Each node should be subject to strict configuration change controls. Independent verification of configuration changes is recommended.

[PZ-HC-106] Each PAZ node should be subject to regular configuration audits. The frequency of such audits should be determined by the Zone Authority and documented in configuration management procedures for the PAZ. The frequency of configuration audits should be sufficient to identify configuration errors. The configuration audit includes but is not limited to:

a. verification of node configuration against network topology design;

b. verification of hardware devices and physical interfaces;

c. verification of traffic control configuration, including permissions and access controls; and

d. verification of permitted software load and permitted functions.

Rationale: Configuration errors are a significant source of exploitable vulnerabilities. Regular configuration audits ensure that the window of exposure from configuration errors is limited.

[PZ-HC-107] System and network management processes and technology should be implemented within a PAZ to detect changes in node configurations.

[PZ-HC-108] All nodes should be subject to regular vulnerability assessments (VAs). The frequency of VAs should be determined by the Zone Authority and documented in VA procedures for the Zone. The VA procedures for a PAZ should be appropriate for critical hosts with a high level of exposure[14]. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: PAZ nodes are exposed to significant threats from the Internet. Regular VAs are aimed at reducing the window of exposure from configuration errors and new exploits.

[PZ-HC-109] Individual nodes should be subject to VAs following configuration changes.

[PZ-HC-110] A comprehensive process for managing software updates[15] should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software that exists on nodes.

[PZ-HC-111] An intrusion detection capability should be implemented on all critical hosts.

[PZ-HC-112] PAZ nodes should be capable of generating and maintaining audit log records as required by the Security Audit service.

[PZ-HC-113] Audit log files should not be allowed to be overwritten (thereby overwriting potential evidence) before they have been backed up to secured storage.

[PZ-HC-114] PAZ nodes should ensure that locally stored Security Audit log records are accessible to authorized Security Audit administrators, as required by the Security Audit service.

[PZ-HC-115] PAZ nodes should be capable of using a common time source.

[14] Guidance on vulnerability assessment is provided by the CSEC in References [15] and [16].

[15] See, for example, reference [23].

[PZ-HC-116] Regular backups of system files and system configuration parameters should be performed for every node contained in the PAZ. Frequency and retention period of backups should be consistent with business needs.

[PZ-HC-117] The failure of a PAZ node should not result in the compromise of its resources or those of any connected network.

[PZ-HC-118] All PAZ nodes should be within an area that meets as a minimum the physical security requirements of a physical Security Zone (see reference [26]). Exceptions may be permitted for core devices owned by public Network Service Providers.

[PZ-HC-119] Each common support services host should perform only a single service.

Note: This requirement does not preclude using a single node to provide multiple virtual hosts, with each virtual host providing a single service.

[PZ-HC-120] Service Delivery hosts should be restricted to the minimum necessary software load with only essential services enabled.

A.4.5 Data Protection Requirements

A.4.5.1 Common Data Protection Requirements

[PZ-DP-100] Although traffic at all sensitivity levels may be transmitted through a PAZ, data that is processed in the clear by the PAZ nodes should be restricted to Unclassified, Protected A, and Protected B only. Additional data protection mechanisms may need to be implemented based on the Statement of Sensitivity and the results of a Threat and Risk Assessment. Protected C and classified information require additional controls and data protection mechanisms that are not specified in this publication. The distribution of data protection services within a PAZ will depend on the implementation requirements.

Note: The use of end-to-end encryption for protection of sensitive information would place additional security responsibilities on End-Systems in internal Zones (e.g., OZ, RZ) to perform traffic control functions such as malware defence.

[PZ-DP-101] The PAZ should implement controls that protect against reuse and replay of user authentication data.

[PZ-DP-102] Where encryption is mandatory, applications must use a CSEC-approved algorithm. Implementations of approved algorithms for use in protecting information at or below Protected B must be validated by CSEC through programs such as the CMVP (FIPS 140-1 or 140-2) or CEP.

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and the CEP, each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e., product) must be (or must have been) validated or certified under a recognized program such as the CAVP. See Information Technology Security Alert ITSA-11C (reference [20]) for a list of CSEC-approved algorithms.

A.4.5.2 Demilitarized Zone (DMZ) Data Protection Requirements

A.4.5.2.1 E-mail Data Protection Requirements

[PZ-DP-103] To protect against inadvertent disclosure and modification, upper-layer security protocols should be used to protect the integrity, authenticity, and confidentiality of sensitive data exchanged with entities in the Public Zone.

A.4.5.2.2 Employee Web Access Data Protection Requirements

[PZ-DP-104] The DMZ should not preclude upper-layer security mechanisms (e.g., Transport Layer Security/Secure Sockets Layer) from being used for employee web access.

A.4.5.2.3 Remote/Mobile Access Data Protection Requirements

[PZ-DP-105] Network-layer encryption between a remote/mobile access client and the PAZ should be used for remote/mobile access via the Public Zone.

[PZ-DP-106] Remote clients should be authenticated to the SVPN devices before the establishment of a connection to an internal Zone (e.g., OZ or RZ).

Rationale: The SVPN device authenticates the identity of the remote access client and terminates the connection if authentication is unsuccessful.

[PZ-DP-107] For remote access via the Public Zone, strong user authentication supported by the GC PKI should be used. Two-factor authentication is also recommended.

Rationale: Strong authentication and two-factor authentication provide higher assurance about the identity of the user.

[PZ-DP-108] Data flowing in the SVPN tunnel between the remote user’s computer and the SVPN device should be encrypted.

Rationale: Connections over the Public Zone can be intercepted and exploited by external entities. Therefore, the data passing through the communication tunnel should be encrypted to prevent the exploitation of GC information. While most SVPNs are established with encryption enabled, it is not necessary to do so. SVPNs can be established using only the Authentication Header to provide strongly authenticated connections. In this case, such a configuration would not be acceptable.

[PZ-DP-109] User and SVPN device PKI certificates should meet GC Medium-Assurance PKI policy and practices (see reference [29] for the GC’s PKI policy).

Rationale: A standard level of assurance provides consistent security and facilitates interoperability.

[PZ-DP-110] Security access privileges of remote/mobile users to another GC Zone (i.e., OZs or RZs) should be agreed upon by the Network Security Zone Authorities of each Zone.

Rationale: Decision on who can access department operational services/assets and data are the responsibility of the department.

[PZ-DP-111] Dial-in users should be authenticated to the dial-in device/service.

[PZ-DP-112] Data flowing between a remote client's host and the dial-in service device should be encrypted.

[PZ-DP-113] Dial-in or SVPN remote clients should be configured in accordance with applicable GC standards and have appropriate security safeguards to mitigate risk from malware.

Note: For employees to access their mailboxes remotely, additional application-layer security mechanisms may need to be implemented to protect against inadvertent disclosure and modification of GC data.

A.4.5.2.4 Service Delivery Applications Data Protection Requirements

[PZ-DP-114] To protect against disclosure and modification of sensitive data:

a. data encryption should be employed between End-Systems in a Public Zone and End-Systems in the DMZ when Protected or classified data is being transmitted;

b. data encryption should be employed for transmission of Protected or classified information when wireless media are used;

c. encryption services should be employed between public End-Systems and the DMZ and also between the DMZ and back-end servers whenever Protected C or classified information is being transmitted; and

d. the use of data encryption for transmission of Protected B information in cases not governed by a and b (above) should be based on a continuous risk management approach. Additional protection may be required for data exchanged with End-Systems in other Zones or where portions of the Internetwork have been outsourced to a Network Service Provider.

A.4.5.2.5 Extranet Services Data Protection Requirements

[PZ-DP-115] The following network-layer security services to support Extranet Services should be employed:

a. peer-entity authentication;

b. data origin authentication;

c. data confidentiality; and

d. data integrity.

[PZ-DP-116] Data confidentiality services should provide isolation between partners using an extranet.

A.4.5.2.6 Common Support Services Data Protection Requirements

[PZ-DP-117] If remote management is allowed, strong authentication and integrity protection mechanisms should be used and all network traffic dealing with remote management of PAZ hosts, including identification and authentication traffic, should be encrypted.

Rationale: Some management protocols currently have only limited support for security, therefore implementers must select protocols that offer support for security (e.g., Secure Shell is preferred to telnet).

[PZ-DP-118] Transfers of naming service configurations between naming services should use strong peer-entity authentication.

Rationale: Transfers of DNS zone configurations between a root name server and a local name server can be replaced with false information by a DNS zone transfer from a spoofed IP address.

[PZ-DP-119] Access to management agents on PAZ devices should only be permitted from authenticated GC hosts

This page intentionally left blank.

Annex B Operations Zone (OZ) Baseline Security Requirements

B.1 Introduction

This Annex provides a set of baseline security requirements for the Operations Zone (OZ). An OZ is the standard environment for routine Government of Canada (GC) operations. It is the primary environment in which end-user systems are installed[16]. With appropriate security controls at the End-Systems, this Zone may be suitable for processing sensitive information; however, it is generally not suitable for large repositories of sensitive data or critical applications.

Within an OZ, traffic is generally unrestricted and can originate internally or from authorized external sources via the Public Access Zone (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 (e.g., compromised host, unauthorized wireless attachment to the Zone). If warranted by a Threat and Risk Assessment (TRA), emanation security measures may be required to protect against unauthorized access to electronic emissions.

B.2 Reference Model

Section 4.3 describes the general reference model for a Network Security Zone and its components. This section of Annex B describes a reference model for the OZ that is based on the general reference model.

An OZ provides a general-purpose, private, network environment under the control of a GC entity (i.e., under the single or shared control of departments and agencies). For many departments and agencies, the OZ should be the Zone where most information technology resources are placed.

Typically, an OZ provides attachment points for workstations used by GC employees and contractors to access private departmental services in internal GC Zones and public services in the Public Zone. The OZ may also provide attachment points for servers that provide back-end services to the PAZ and private services to the GC. An OZ allows GC employees to access private departmental or agency services such as e-mail, file storage, printing, databases, directories, and vertical line of business applications for workflow, inventory, finance, logistics, shipping, personnel management, and others that are required to support GC operations. An OZ may support the following functions, which have specific security objectives and requirements:

a. internal departmental applications – provides access to internal departmental services and business applications;

[16] Smaller departments or organizations within departments may choose to put their servers in an OZ.

b. employee file and print services – provides access for GC employees and contractors to private GC file and print resources;

c. employee simple/rich media web access – provides access for GC employees and contractors to private GC and public websites and streaming media through the PAZ;

d. e-mail access – provides common communication tools such as e-mail for GC employees;

e. inter-departmental applications – provides services to other GC departments for GC employees to access inter-departmental information;

f. employee remote /mobile access (includes mobile and wireless remote access and Secure Virtual Private Network (SVPN)) – provides access to selected OZ resources for GC employees through the PAZ;

g. extranet services – provides a secure method of communicating with partner organizations external to the GC;

h. service delivery applications – provides back-end services to the publicly-accessible, PAZ-hosted web interface for GC services; and

i. common support services – provides the common services required to run a modern, secure network (e.g., Domain Name Service, Directory Service Agent, Network Time Protocol, etc.).

The OZ is intended for routine, low-sensitivity, departmental information services. However, with additional security measures, an OZ is capable of processing and distributing sensitive departmental information using appropriately configured hosts, upper-layer security protocols, and application security controls.

In general, sensitive information repositories (e.g., large enterprise databases or databases containing sensitive information) should not be maintained in the OZ[17].

High-availability applications on critical End-Systems are most appropriately located in a Restricted Zone (RZ) or Highly Restricted Zone (HRZ) to limit susceptibility to denial-of-service (DoS) attacks. In addition, OZ network services would typically not be designed to provide high or ultra-high reliability and should not be used as the only communication channel supporting high-availability applications. However, this does not preclude the use of an OZ as a primary communications path in support of high-availability applications, provided the overall system availability requirements are met, perhaps through the provision of secondary communications channels.

Interfaces to all public services are implemented through a PAZ. External access from the OZ to the Internet is provided through an interface from the OZ to the PAZ. Access to other GC

[17] "Sensitivity" in this context means sensitivity in terms of confidentiality, availability, and integrity. This is broader in meaning than the term "classification", which refers specifically and only to sensitivity in terms of confidentiality. See also the definition of sensitive in Section 5.

departments is provided by interfaces to peer OZs or RZs. Interfaces to sensitive services or repositories are implemented through tightly controlled interfaces provided by other Zones.

An OZ has the structure of a generic Zone (see Figure 5). Theoretically, it is composed of four classes of components: Zone Interface Points (ZIPs), Internetwork components, Internal Boundary Systems (IBSs) and End-Systems. Typically, an OZ has a single Internetwork component and no IBSs and, unlike the PAZ, IBSs play no role in the specification of security requirements. Figure 11 below gives a high-level view of an OZ and its interconnection to other Zones. The ZIPs provide ingress and egress controls on traffic flows at the points where the OZ interconnects with other Zones. Where a node is shared between two Zones (like the Shared End-System in Figure 11), both Zone Authorities should agree on management and oversight of the node. Note that multiple ZIPs can be implemented through a single boundary device as long as the requirements for all other Zones are being met and as long as it is mutually acceptable to all affected Network Security Zone Authorities. For example, a single appliance firewall with two separate physical interfaces may support an OZ ZIP and an RZ ZIP.

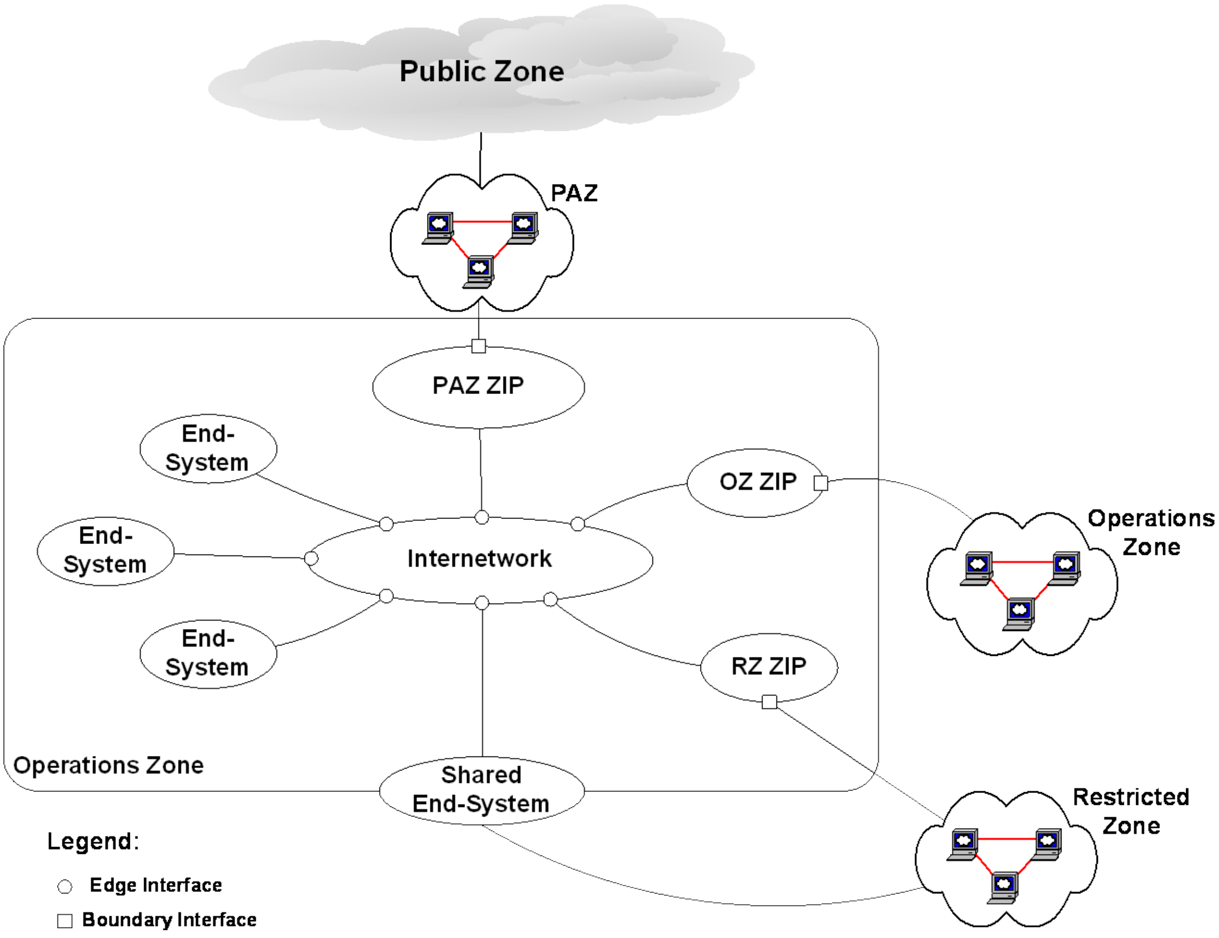
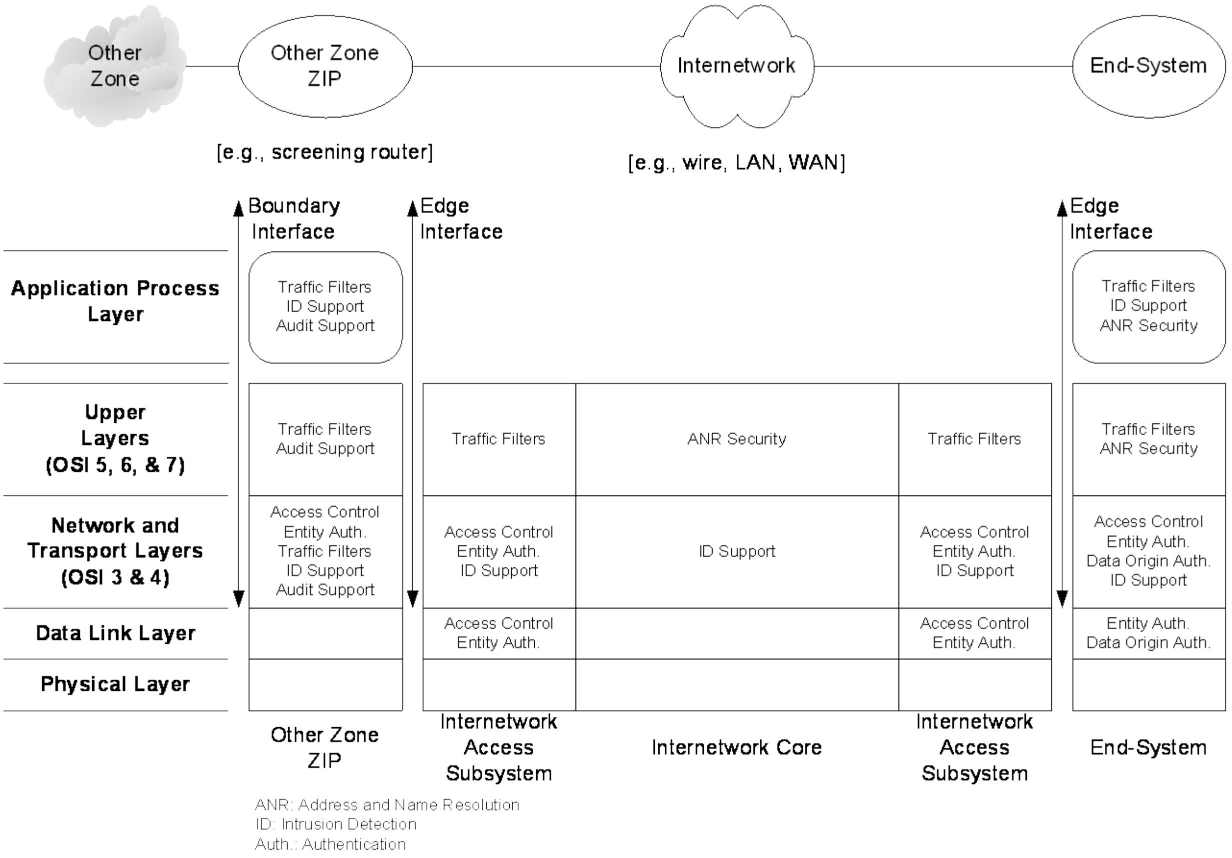


Figure 11 – Typical Operations Zone (OZ) Logical Topology

Figure 11 also provides a logical view of the interconnection relationships between components in an OZ. A ZIP provides the interface between internal OZ entities and other Zones[18]. The Internetwork provides the internal network for the OZ to aggregate and distribute traffic between End-Systems and ZIPs. End-Systems provide localized processing and storage of departmental information.

Figure 12 shows the OZ logical architecture. It identifies the entities that make up the OZ, the relations between entities, and the allocation of security services[19]. This figure provides an end-to-end mapping of the logical connection between the OZ and other GC Zones (i.e., PAZ, other OZs, and RZs), including the security services that are provided at different Open Systems Interconnection (OSI) layers.



	Other Zone ZIP	Internetwork Access Subsystem	Internetwork Core	Internetwork Access Subsystem	End-System
Application Process Layer	Traffic Filters ID Support Audit Support				Traffic Filters ID Support ANR Security
Upper Layers (OSI 5, 6, & 7)	Traffic Filters Audit Support	Traffic Filters	ANR Security	Traffic Filters	Traffic Filters ANR Security
Network and Transport Layers (OSI 3 & 4)	Access Control Entity Auth. Traffic Filters ID Support Audit Support	Access Control Entity Auth. ID Support	ID Support	Access Control Entity Auth. ID Support	Access Control Entity Auth. Data Origin Auth. ID Support
Data Link Layer		Access Control Entity Auth.		Access Control Entity Auth.	Entity Auth. Data Origin Auth.
Physical Layer					

ANR: Address and Name Resolution
ID: Intrusion Detection
Auth.: Authentication

Figure 12 – OZ Logical Architecture

[18] A node that provides logical separation of ZIPs may implement separate physical interfaces to more than one type of Zone (i.e., other OZ, PAZ, RZ).

[19] The allocation of security services is based on the model of Section 4.4.2 and the requirements of Section B.4.2. See Section 4.4.2 for an explanation of the security services. In the OZ, not every service is required in every component or OSI layer.

B.3 Security Objectives

In general, the target security state of the OZ is a network environment that prevents (i.e., removes susceptibility to) network-based attacks from unsophisticated external attackers (i.e., external adversaries with minimal resources and limited skill). The OZ target security state also aims to significantly reduce susceptibility to other sources and forms of attacks. It should be assumed that a sophisticated attacker could defeat security controls within an OZ. Therefore, additional security measures would be required to protect sensitive assets within an OZ.

Each objective and requirement specified in this Annex is labelled according to the following notation:

a. the first set of letters (OZ) refers to the Zone;

b. the second set of letters designates either an objective (i.e., OBJ) or a requirement. Requirements are grouped into the following categories as applicable: network interface (NI), traffic control (TC), network configuration (NC), host configuration (HC) and data protection (DP); and

c. each objective or requirement is sequentially numbered within its group, beginning at 100[20].

B.3.1 Traffic Control Objectives

[OZ-OBJ-100] An OZ should protect the integrity and availability of End-Systems attached to the Zone by reducing the prevalence of malicious traffic. In particular, an OZ aims to:

a. prevent network-based DoS attacks (e.g., SYN flood, smurf attack) on End-Systems from unsophisticated attackers;

b. significantly reduce network-based DoS attacks on End-Systems from all other sources;

c. prevent access to End-Systems as a result of network intrusions (i.e., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface) by unsophisticated attackers;

d. significantly reduce susceptibility to network intrusions from all other sources;

e. prevent the ability to exploit OZ End-Systems as staging points for attacks on other End-Systems by unsophisticated attackers ;

f. significantly reduce the ability to exploit OZ End-Systems as staging points for attacks on End-Systems from all other sources;

[20] These numbers may differ from those in the original version (ITSD-02) of this Guideline. Annex F to this Guideline maps the old objective and requirement numbers to the new ones. Future versions of this document should maintain objective and requirement numbers across versions and indicate whether an objective or requirement has been rescinded or added.

g. limit the propagation of malicious traffic from other Zones in support of sub-objectives (a), (b), and (c) above; and

h. greatly reduce the propagation of malware.

Note: Network security measures are limited in their ability to protect End-Systems from compromises through valid application interfaces. The risks associated with threats of this type should be addressed through platform, application, and operational security measures.

[OZ-OBJ-101] An OZ should provide the ability to continuously assess traffic at its interfaces to other Zones to continuously validate assumptions concerning the security environment provided by neighbouring Zones.

[OZ-OBJ-102] An OZ should permit changes to enhance security measures in response to increased threat levels (e.g., time of crisis), including:

a. flexible, dynamic traffic controls based on Community of Interest;

b. increased status monitoring of ZIPs; and

c. ensuring that Network Service Providers increase surveillance of outsourced network infrastructure.

[OZ-OBJ-103] The PAZ implements safeguards that provide effective protection against malicious network traffic originating from public networks; however, there are residual risks from the PAZ that should be addressed by the OZ. The objective of the OZ is to:

a. significantly reduce susceptibility to attacks originating from compromised remote-access and extranet End-Systems;

b. significantly reduce susceptibility to malicious traffic from compromised service delivery application servers in the PAZ through safeguards that include restricting access by these servers to designated resources and protocols; and

c. greatly reduce susceptibility to attacks originating from a compromised host in the PAZ other than a service delivery application server and against failures in PAZ traffic control measures including intrusions through the PAZ Internal Access Network.

Rationale: The PAZ Authority has limited control over the configuration of applications residing on front-end servers. Thus, there is potential for compromise and thus the specification of explicit safeguards aimed at containing these interfaces. All other hosts within the PAZ are completely within the control of the PAZ Authority and a more general statement of objective is sufficient.

B.3.2 Network Availability and Reliability Objectives

[OZ-OBJ-104] An OZ should protect the integrity and availability of network services by reducing the susceptibility to a variety of attacks. In particular, an OZ should:

a. prevent susceptibility of network services to DoS attacks from external adversaries having minimal resources and limited skill;

b. significantly reduce the susceptibility of network services to DoS attacks from other sources (e.g., dedicated adversaries, infrastructure insiders, and network users);

c. prevent susceptibility to network intrusions (i.e., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface, or the compromise of an attached End-System) from external adversaries having minimal resources and limited skill;

d. significantly reduce susceptibility to network intrusions from all other sources;

e. prevent the ability to exploit End-Systems as staging points for attacks on other network services by external adversaries with minimal resources and limited skill;

f. significantly reduce the ability to exploit End-Systems as staging points for attacks on network services from all other sources;

g. limit the propagation of malicious traffic from other Zones in support of sub-objectives (a), (b), and (c) above; and

h. greatly reduce the propagation of malware.

B.3.3 Data Protection Objectives

[OZ-OBJ-105] An OZ should significantly reduce susceptibility of Zone traffic to interception by external adversaries with minimal resources and limited skill and reduce the susceptibility to undetected interception from all other sources.

[OZ-OBJ-106] An OZ should support data protection measures to protect the confidentiality and integrity of data. These measures include:

a. support for SVPN within the Internetwork and across all ZIPs;

b. support for upper-layer security protocols; and

c. providing SVPN as an optional data service.

Rationale: The OZ infrastructure may employ a variety of physical media including wireless. It should be assumed that a sophisticated attacker could intercept traffic.

Note: There are many situations across the GC in which employees from another department must access network services and be able to securely access their home networks. These situations may include temporary access through an access point located in a boardroom, or permanent access for employees assigned to the host department (e.g., Justice employees at other departments).

B.4 Security Requirements

This section describes the baseline security requirements for the OZ. These are categorized by operational requirement (i.e., network interface, traffic control, network configuration, host configuration, and data protection). Within each operational requirement category are sub-categories consisting of common requirements that apply across the entire OZ, followed by requirements specific to the Internetwork, the various types of ZIPs, and certain types of End-Systems. Note that in some cases, a sub-category may not exist or have a heading because requirements for perimeter defence security are not applicable for that sub-category within that operational requirement category, or are common to the entire category.

The Zone Implementation Model (Section 4.2) allows a Restricted Extranet Zone (REZ) to connect to an OZ. This would require a REZ ZIP in the OZ. The security requirements for a REZ ZIP in an OZ should be established on a case-by-case basis, so this Guideline does not contain requirements for a REZ ZIP.

To achieve all of the Security Objectives for this Zone, as detailed above, the complete set of Security Requirements which follows must be implemented.

B.4.1 Network Interface Requirements

[OZ-NI-100] All network paths between the OZ and other Zones should pass through a ZIP.

Rationale: ZIPs implement traffic controls to reduce the volume and type of malicious traffic flowing between Zones.

[OZ-NI-101] The number of ZIPs between any two Zones should be limited.

Rationale: Limiting the number of ZIPs reduces the management burden and limits the introduction of security vulnerabilities due to operating and configuration errors. The number of ZIPs should be determined by the geographic distribution of the network, network traffic patterns, and the availability needs of supported applications.

[OZ-NI-102] All network paths destined for, or originating from a Public Zone (e.g., Internet), should pass through a PAZ. That is, the OZ should not have direct network connections to a Public Zone.

[OZ-NI-103] An OZ Internetwork should be a logically separate network. It should maintain traffic interfaces only with:

a. ZIP(s) in the OZ; and

b. OZ End-Systems.

[OZ-NI-104] The Internetwork may share physical-layer, data link-layer, and network-layer infrastructure with any Zone (including a Public Zone). If the OZ Internetwork shares physical-layer, data link-layer, and network-layer infrastructure with a Public Zone, such sharing should occur only in the Internetwork Core.

Note: Additional requirements concerning the logical separation between OZ components and other network infrastructure are found in section B.4.3, Network Configuration Requirements.

Rationale: In some cases, a public commercial carrier may provide the Internetwork infrastructure. This implementation is acceptable provided there are security mechanisms in place to ensure logical isolation. A commercial implementation requires significant trust in the network equipment (e.g., routers) to avoid intrusions from the public network. Consequently, sharing of Internetwork Edge Interfaces and Access Subsystems is not permitted (i.e., sharing should occur only within the Internetwork core).

[OZ-NI-105] The ZIP, IBS (if present), and Internetwork components should support the attachment of network-based intrusion detection sensors (e.g., monitors). ZIP, IBS (if present), and Internetwork components should provide interfaces to support the collection of data from these sensors.

B.4.2 Traffic Control Requirements

B.4.2.1 Common Traffic Control Requirements

[OZ-TC-100] If an OZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the OZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement.

[OZ-TC-101] OZ management traffic, other than traffic related solely to device status, should be segregated from operational traffic.

Note: Segregation may be either virtual or physical. That is, segregation may be achieved through cryptography, network, access controls, or physical separation.

[OZ-TC-102] The OZ should be capable of responding quickly to heightened security levels in case of emergency and increased threat, when and how authorized to do so. (Personnel should be aware, trained and authorized to initiate such a response.) For example, the OZ should possess the capability to improve the network security posture by increasing the level of security measures such as:

a. filtering at each ZIP;

b. active and/or passive monitoring;

c. protection to ensure the continuous delivery of critical services, including the capability to reconfigure or block non-essential services if required; and

d. auditing.

Note: Implementation of such measures should be carefully tested to ensure that these capabilities could not be exploited to cause a denial of service.

[OZ-TC-103] Each ZIP should authenticate the Boundary Interfaces of the ZIPs (in other Zones) to which it connects. This authentication may be achieved through physical control over the media between the Boundary Interfaces.

B.4.2.2 Internetwork

[OZ-TC-104] The Internetwork should provide an access control service capable of enforcing access control policies between Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[OZ-TC-105] The OZ Authority should define requirements for an OZ Internetwork access control service based on the following principles:

a. the access control policy should be constructed to permit all traffic unless explicitly denied;

b. the access control policy should support Community of Interest separation (i.e., where network traffic is divided into natural communities of interests, the access control policy should enforce these natural traffic flows);

c. the access control policy should restrict available network paths to vulnerable or sensitive End-Systems (e.g., test and development sub-networks and application servers supporting public applications);

d. the access control policy should be configured to limit available network paths for End-Systems accessible by extranets;

e. if the OZ Authority permits connection to the OZ by remote access hosts with operating systems that do not provide separation of user and administrator roles, then the access control policy should be configured to limit access to other End-Systems by remote access hosts; and

f. if the Internetwork provides more than one class of service, the access control policy should support isolation between classes of service.

Rationale: Internal access controls contain intrusions and the spread of malware. Internal access controls also support the detection of malicious behaviour (e.g., router logs will often show an increase in access failures). However, the OZ is intended to be an open network environment and access controls should be designed to allow all natural traffic flows.

[OZ-TC-106] If the OZ supports more than one class of service, the Internetwork should implement mechanisms to ensure non-interference between classes of service.

Rationale: If classes of service other than "best effort" are required by End-Systems, simple bandwidth consumption within one class of service can result in denial of service within another class of service unless controls are put in place to limit interference. Such controls are often available within mechanisms that implement class of service and quality of service.

[OZ-TC-107] The Internetwork should employ an addressing model that facilitates detection and diagnosis of malicious traffic.

Rationale: The choice of address model can have a significant impact on the ability to detect and isolate network problems in general and security problems in particular. It is good network design practice to facilitate access controls to isolate shared resources, and to segregate by location (e.g., remote access and extranet clients) and organization.

[OZ-TC-108] The OZ should support Internet Protocol Security (IPSec) traffic between any pair of Edge Interfaces.

Rationale: The OZ should permit End-System managers the option of implementing network-layer data protection. IPSec traversal of network address translation and firewall implementations may affect interoperability of some networks and applications.

B.4.2.3 Public Access Zone (PAZ) Zone Interface Point (ZIP)

[OZ-TC-109] The PAZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[OZ-TC-110] The Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. the access control policy should be constructed to deny all traffic unless it is explicitly permitted;

b. all outgoing traffic should be restricted to destination addresses corresponding to designated proxy servers in the PAZ;

c. traffic to and from application servers should be restricted to addresses corresponding to front-end servers in the PAZ and to those protocols necessary to support communication with the front-end servers;

d. extranet hosts should be restricted to a defined set of internal addresses which contain the resources required by the extranet;

e. if the Zone Authority permits remote access hosts with open configurations (see host configuration at paragraph [OZ-HC-105]), then remote access clients should be restricted to a defined set of internal addresses.

[OZ-TC-111] If justified by a TRA, a stateful filter should be applied at the ZIP to ensure that incoming traffic is restricted to authorized protocols.

Rationale: The PAZ can normally be trusted to filter out most malicious traffic originating from the Internet, provided all outgoing access is routed through a designated proxy server and incoming traffic (remote access, extranet, and applications) is limited to specified resources. Additional protection using stateful inspection at the ZIP may be justified if the protection provided by the PAZ is in doubt.

[OZ-TC-112] An intrusion detection capability should be implemented at the ZIP.

Rationale: Access controls, together with the controls applied in the PAZ, should eliminate most attacks via the ZIP. However, these safeguards will not provide complete protection. The resources required to manage this capability should be modest since the frequency of alarms at this interface should be low.

[OZ-TC-113] If warranted by a TRA or if required by the Network Security Zone Authority to enforce Internet Use Policy, a content filter should be implemented at the PAZ ZIP.

B.4.2.4 Operation Zone (OZ) Zone Interface Point (ZIP)

[OZ-TC-114] The OZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[OZ-TC-115] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this OZ ZIP;

b. for outgoing traffic, access controls should be configured to permit all traffic that is not explicitly denied;

c. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses; and

d. the access controls should support interdepartmental applications.

Rationale (for sub-paragraph b above): In communications between two internal Zones, each Zone depends on the other to apply controls on ingress. Consequently, few controls are required on egress.

[OZ-TC-116] An intrusion detection capability should be implemented at the ZIP. The intrusion detection capability should be configured to provide an alarm if traffic contains malware or malicious behaviour.

Rationale: Please see [OZ-TC-112] Rationale.

[OZ-TC-117] If justified by a TRA, a stateful filter should be applied at the ZIP to ensure that incoming traffic is restricted to authorized protocols.

[OZ-TC-118] An e-mail gateway should be employed at the OZ ZIP and this gateway should implement malware filters on all incoming and outgoing e-mail.[21]

Rationale: E-mail is the primary vector for the spread of malware.

[OZ-TC-119] If warranted by a TRA or if required by the Network Security Zone Authority to enforce Internet Use Policy, a content filter should be implemented at the ZIP.

[OZ-TC-120] The OZ ZIP interface to common infrastructure may share traffic control functionality with the common infrastructure provider. A service level agreement should include the baseline requirements for both sides of the interface.

B.4.2.5 Restricted Zone (RZ) Zone Interface Point (ZIP)

[OZ-TC-121] If justified by a TRA, the RZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[OZ-TC-122] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this ZIP;

b. for outgoing traffic, access controls should be configured to permit all traffic that is not explicitly denied; and

c. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses.

[OZ-TC-123] An intrusion detection capability should be implemented at the ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

Rationale: Please see [OZ-TC-112] Rationale.

[21] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

Note: If an intrusion detection capability is implemented at the OZ ZIP within the RZ (see [RZ-TC-117]), it may not be necessary to implement intrusion detection here as well.

[OZ-TC-124] If justified by a TRA, an e-mail gateway should be employed at the ZIP and this gateway should implement malware filters on all incoming and outgoing e-mail[22].

Rationale: In most cases the RZ will provide a network environment with a significantly more secure security posture than the OZ. While additional controls add protection, the risk of malware remains. In many cases an RZ will be a server-farm serving clients in the OZ.

B.4.2.6 Highly Restricted Zone (HRZ) Zone Interface Point (ZIP)

[OZ-TC-125] An intrusion detection capability should be implemented at the HRZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

Note: The HRZ should have intrusion detection at its OZ ZIP (see [HRZ-TC-112]). Implementing intrusion detection here as well should only be necessary in high-risk environments.

[OZ-TC-126] If justified by a TRA, the HRZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[OZ-TC-127] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this ZIP;

b. for outgoing traffic, access controls should be configured to permit all traffic that is not explicitly denied; and

c. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses.

[OZ-TC-128] If justified by a TRA, an e-mail gateway should be employed at the ZIP and this gateway should implement malware filters on all incoming and outgoing e-mail[23].

Rationale: In most cases the HRZ will provide a network environment with a significantly more secure security posture than the OZ. While additional controls add protection, the risk of malware remains. In some cases, an HRZ will be a server-farm serving clients in the OZ.

[22] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.
[23] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[OZ-TC-129] HRZ ZIPs should implement network-layer and upper-layer controls to protect OZ hosts from traffic originating from an HRZ and to protect the HRZ in the event that malicious traffic originates from within the OZ.

[OZ-TC-130] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

B.4.3 Network Configuration Requirements

B.4.3.1 Common Network Configuration Requirements

[OZ-NC-100] The OZ network configuration should be monitored to detect additions, deletions, or changes to Edge Interfaces. Unauthorized changes should be reported to the OZ Authority.

Rationale: Continuous status monitoring is necessary to detect unauthorized changes to the network configuration in a timely manner. Timely detection allows Zone Authorities of impacted Zones to respond to prevent or limit damage from an attack or failure.

[OZ-NC-101] The OZ Boundary and Edge Interfaces should be registered with the OZ Network Security Zone Authority.

[OZ-NC-102] Each OZ interface should act in exactly one role: Boundary or Edge Interface.

[OZ-NC-103] The OZ Network Security Zone Authority should periodically verify the network topology. The Network Security Zone Authority should determine the frequency of such verifications and document the frequency in configuration management procedures for the OZ.

[OZ-NC-104] The OZ Network Security Zone Authority should periodically assess the network configuration for unauthorized external interfaces (e.g., modems and wireless access points (APs)). The Network Security Zone Authority should determine the frequency of assessments and document the frequency in configuration management procedures for the OZ.

Rationale: The presence of unauthorized modems can create vulnerabilities in a well-configured network. These unauthorized modems provide a means to bypass most or all of the security measures in place to stop unauthorized users from accessing a network.

[OZ-NC-105] If remote management is allowed, an OZ should allow only authorized administrators to remotely manage OZ nodes from a GC-controlled Zone or from a Restricted Extranet Zone. The access should be controlled and protected by using the following methods:

a. strong authentication; and

b. restricting access by Internet Protocol address, port, and protocol.

B.4.3.2 Zone Interface Point (ZIP) Network Configuration Requirements

[OZ-NC-106] OZ Boundary Interface addresses should be distinct and dedicated. OZ Boundary Interface addresses should be visible to other GC Zones but should not be visible to the Public Zone.

[OZ-NC-107] OZ Boundary Interfaces should be assigned addresses upon attachment to the network.

[OZ-NC-108] A change to an OZ Boundary Interface address assignment should constitute a configuration change requiring approval by the OZ Network Security Zone Authority. Approval may be given in advance to permit dynamic reconfiguration; however, the conditions under which such a change may be effected should be delineated clearly.

B.4.3.3 Internetwork Configuration Requirements

[OZ-NC-109] The OZ Network Security Zone Authority should maintain current configuration information for all Edge Interfaces. The configuration information should include:

a. a unique identifier;

b. the status of the Edge Interface (active/non-active);

c. the address assignment rules;

d. the current network address;

e. the list of all names/aliases associated with the Edge Interface;

f. the current physical-layer interface to which the Edge Interface is assigned;

g. the communications security parameters for the Edge Interface; and

h. security constraints on the instantiation of each Edge Interface.

[OZ-NC-110] The following changes to an OZ should be approved by the OZ Network Security Zone Authority before implementation:

a. addition or deletion of an Edge Interface;

b. a change to the address assignment rules for any Edge Interface;

c. a change to the communications security parameters of any Edge Interface; and

d. a change to the security constraints on the instantiation of any Edge Interface.

Rationale: These changes may affect the implementation of security measures or the configuration of intrusion detection capabilities.

[OZ-NC-111] Edge Interfaces should establish security associations with other Edge Interfaces and all communications should be authenticated (either explicitly or implicitly) within the context of these security associations. The security associations permitted should be determined by traffic control requirements.

Note: The type and strength of authentication are implementation dependent. The goal is to prevent an intruder attaching a network-layer entity in the core and masquerading as an Edge Interface.

[OZ-NC-112] Internetwork Edge Interfaces should be authenticated to each other through one of the following methods:

a. cryptographic authentication mechanisms applied at the network layer;

b. physical controls over the Edge Interfaces and over all media connecting these interfaces; or

c. physical controls over the Edge Interfaces and approved network- and lower-layer controls implemented within the Internetwork Core connecting these interfaces.

Rationale: Because the Internetwork is a significant component of an internal GC Zone, it is extremely important that hostile entities be excluded from masquerading as Edge Interfaces.

[OZ-NC-113] If a Network Service Provider is responsible for providing security controls within the Core of the Internetwork to maintain the security association between Edge Interfaces, the service level agreement should include provisions to ensure that these security controls are effective.

[OZ-NC-114] The service level agreement should require the Network Service Provider to control changes to Core interfaces and to report to the OZ Network Security Zone Authority any changes that affect the security association between Edge Interfaces.

[OZ-NC-115] The service level agreement should require the Network Service Provider to provide evidence that the security controls used to enforce the security within the Internetwork Core are effective and to report all security incidents that could impact the OZ to the OZ Network Security Zone Authority. The Network Service Provider should also provide the OZ Network Security Zone Authority with the capability to verify the effectiveness of the controls on at least a quarterly basis.

B.4.3.4 Wireless Network Configuration Requirements

[OZ-NC-116] Addresses provided to End-Systems that use wireless/radio frequency (RF) data link layers should be assigned dynamically from a segregated address pool.

Rationale: Address assignment from a distinct pool of addresses permits access control by Community of Interest.

[OZ-NC-117] Wireless End-Systems should be authenticated to the OZ using strong peer-entity and data origin authentication before the establishment of a connection to the OZ.

Rationale: Authentication of the End-System provides confirmation that the connection being processed is coming from a valid source. Persistent authentication would be necessary to permit roaming between APs.

[OZ-NC-118] Peer-entity and data origin authentication at the data link layer should be used to establish connections between wireless APs and wireless End-Systems.

Rationale: Authentication of the End-System provides confirmation that the connection being processed is coming from a valid End-System.

[OZ-NC-119] The OZ Network Security Zone Authority should conduct a mapping of the signal strength, in the horizontal and vertical planes, for all wireless APs in the OZ. Such mappings should be updated periodically. The Network Security Zone Authority should determine the frequency of mapping updates.

Rationale: A map of signal strength defines the physical space into which RF energy is transmitted. This mapping is particularly relevant in multi-level buildings and in built-up areas where the wireless signal extends beyond the perimeter of physical security zones. RF-based wireless networks are subject to all the security issues normally faced with conventional wired networks but additionally, they suffer from vulnerabilities directly associated with the use of wireless connectivity. The nature of the wireless medium makes it practically impossible to confine the radio signals to a controlled location. Unless TEMPEST shielding is used or adequate physical zoning is established, the radiated signals are subject to clandestine interception and exploitation. Finally, eavesdroppers may use high-gain antennas, which permit interception of wireless signals beyond the limit of a manufacturer's specification of signal distance.

[OZ-NC-120] The wireless intrusion detection policy should be integrated with facility access policies.

Rationale: The source of a wireless network intrusion may be within an organization's controlled physical space. If so, a suitable response may be a physical response to locate the source and remove it from the facility.

[OZ-NC-121] The OZ Network Security Zone Authority should monitor[24] the wireless local area network to:

a. understand the nature of traffic (e.g. data/protocols);

b. discover traffic generated by unauthorized users (e.g. outsiders);

c. find irregular traffic generated by legitimate users;

d. make an inventory of APs; and

[24] WLAN monitoring may involve the interception of private communications, which may constitute a violation of Canadian law, including the Criminal Code. Before using monitoring tools on any WLAN, it is recommended to consult with legal services to ensure that the monitoring does not violate Canadian law.

e. solve problems.

[OZ-NC-122] The OZ Network Security Zone Authority should perform network discovery inside his or her facilities and evaluate the list of discovered APs and communication channels with the inventory of authorized APs and communication channels.

B.4.3.5 End-System Network Configuration Requirements

[OZ-NC-123] End-Systems should maintain the integrity of Edge Interfaces with other GC Zones while connected to an OZ. Dual-homing, split-tunnelling[25], or other shared network paths with the Public Zone by OZ End-Systems should not be permitted.

Rationale: Simultaneous connection of an Ethernet interface to an OZ and an active modem connection to the Internet would permit intrusion to the OZ. Similarly, having an SVPN tunnel split between an OZ and the Internet or having a wireless interface available for incoming connections while maintaining a wired interface to an OZ could permit intrusion (i.e., port forwarding should be turned off).

[OZ-NC-124] Wireless devices should be configured to limit or suppress broadcasting of their device identifiers (such as IEEE 802.11 Service Set Identifiers).

B.4.4 Host Configuration Requirements

B.4.4.1 Common Host Configuration Requirements

[OZ-HC-100] The OZ Network Security Zone Authority should maintain a host configuration policy consistent with applicable baseline security requirements, standards, and guidance. This policy should apply to all hosts attached to the Zone.

Note: From a Zone perspective, the host configuration policy should be limited to specifying the constraints on the software load and the maintenance procedures required to prevent a sophisticated attacker from compromising a host and using that host to attack network assets. The policy should also reduce susceptibility to compromise from all other sources. The primary focus should be the control of malware as this is the easiest and most prevalent method of attack. Note that hosts may be subject to additional platform security requirements to protect applications and data; however, these are outside the scope of Zone requirements. These additional platform security requirements will depend on the type of host (e.g., workstation, application server).

[OZ-HC-101] The host configuration policy should contain:

[25] Split-tunnelling: Simultaneous direct access to a non-corporate (or public/private) network from a remote device while connected to a corporate network through a VPN tunnel.

a. a specification of prohibited and mandated software and hardware configurations such as not allowing active modems, “sniffer” software, or remote access software permitting control of an OZ host, but requiring the installation of current anti-virus software;

b. minimum maintenance procedures for all software components (e.g., configuration management procedures for hardware and software, emergency patch procedures, technician training, etc.); and

c. specific maintenance procedures for software that provides client access to Internet-based resources, and for software that provides back-end services to public clients (e.g., mail service).

Rationale: The PAZ and the Internetwork infrastructure should limit direct intrusions (i.e., those not using malware) to sophisticated attackers. Host configuration controls are aimed at further reducing the susceptibility to such intrusions. In most cases, an OZ will be a large network installation with diverse business needs and distributed authority over End-Systems. Although it is impractical to expect rigid controls over all End-System configurations in such diverse environment, a minimum practical level of discipline over the End-System configuration is necessary to reduce the susceptibility to intrusion via End-Systems. The greatest attention should be placed on any software that has the potential to interact with public networks.

[OZ-HC-102] The OZ Network Security Zone Authority should ensure that End-System managers are aware of this host configuration policy and that they ensure the policy is enforced.

[OZ-HC-103] Regular network vulnerability assessments (VAs) of a representative subset of hosts should be conducted to assess trends in the effectiveness of the host configuration policy. The frequency of such VAs should be sufficient to support trend analysis. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: Network VAs involve port scans and possibly some software fingerprinting. The goal is to provide the Zone Authority with a statistical picture of the vulnerability of End-Systems and compliance to the host configuration policy. This approach has been chosen to balance a liberal approach to host configuration control. A significant change in the results may indicate a widespread problem or may be evidence that other measures are required.

[OZ-HC-104] All hosts should invoke controls that implement continuous protection against malware at start-up. The Network Security Zone Authority should approve any exceptions to this requirement.

Rationale: Malware is the easiest and most likely vehicle for an external attacker to gain control of an End-System to attack OZ assets. Controls are placed in the PAZ to reduce the amount of malware that reaches the End-System. However, no network filter is completely effective and malware protection is required on the hosts within the End-Systems. Exceptions may be required for those few hosts for which it may be prohibitively expensive or impossible to meet the requirement (e.g., mainframes, super computers).

[OZ-HC-105] All hosts that provide applications to permit client access to public resources (e.g., Internet web browsers and e-mail clients) should:

a. employ an operating system that provides separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege); and

b. be configured to operate any applications that provide access to public resources in user mode.

Rationale: If the platform is able to enforce configuration controls by restricting changes to administrators, then many intrusion scenarios can be thwarted. Most new commercial operating systems (e.g., Windows 2000, Windows NT, Windows XP, Apple OS X, and all UNIX/Linux variants) provide this capability.

[OZ-HC-106] If an OZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the OZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement.

B.4.4.2 Shared End-System Configuration Requirements

[OZ-HC-107] A shared End-System, whether shared permanently or periodically, should comply with the following:

a. it should employ an operating system that supports the separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege);

b. changes to network configuration should require administrative privileges;

c. the End-System configuration and procedures for maintaining that configuration should be approved by the OZ Network Security Zone Authority;

d. the End-System should be subject to regular VAs (results to be provided to the TRA process), the frequency of which should be determined by the Network Security Zone Authority and documented in VA procedures for the Zone; and

e. requirements [OZ-TC-100] and [OZ-HC-106] (if applicable).

Rationale: Shared End-Systems have the potential to create back doors between Zones. Shared End-Systems are also likely to be relatively few in number, making greater control possible. This vulnerability scan focuses on vulnerabilities associated with routing.

[OZ-HC-108] If an End-System is shared periodically (e.g., laptop) with a Public Zone, then:

a. the End-System should include a personal firewall; and

b. the End-System should include a configuration integrity mechanism capable of identifying changes to the configuration and notifying the End-System administrator.

B.4.4.3 Wireless End-System Configuration Requirements

[OZ-HC-109] A shared, wireless End-System, whether shared permanently or periodically, should comply with the following:

a. it should employ an operating system that enforces the separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege);

b. changes to network configuration should require administrative privileges;

c. the End-System configuration and procedures for maintaining that configuration should be approved by the OZ Network Security Zone Authority; and

d. the End-System should be subject to regular VAs, the frequency of which should be determined by the Network Security Zone Authority and documented in VA procedures for the Zone. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: Wireless End-Systems have the potential to create back doors between Zones.

[OZ-HC-110] A shared, wireless End-System that is shared periodically with a Public Zone, is subject to the following:

a. the End-System should include a personal firewall; and

b. the End-System should include a configuration integrity mechanism.

B.4.4.4 Network Node Configuration Requirements

[OZ-HC-111] Operating systems for all nodes (i.e., ZIP boundary devices and for Internetwork edge/core devices) should be hardened based on documented best practices.

[OZ-HC-112] SVPN products, if used, should be validated to Federal Information Processing Standard (FIPS) 140-1 or FIPS 140-2 at a minimum of Security Level 2 through the Cryptographic Module Validation Program (CMVP).

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and Cryptographic Endorsement Program (CEP), each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the Cryptographic Algorithm Validation Program (CAVP).

[OZ-HC-113] Internetwork devices and ZIPs should be physically secured to limit access to only those authorized personnel with an ongoing need to access the equipment, in accordance with the Principles of Least Privilege and Need-to-Know.

Rationale: Restricted access to devices with Edge Interfaces reduces the opportunity for network reconfiguration or introduction of unauthorized Edge Interfaces. A Network Service Provider can restrict access with physical barriers such as cages. Devices located at GC premises can be located in physical security zones.

B.4.4.5 Complex End-System Configuration Requirements

[OZ-HC-114] A complex End-System should have a certification and accreditation review before attachment to an Edge Interface is permitted.

Rationale: A complex End-System may use a private network between its components, may have traffic controls, and may have unique network configurations that could compromise the infrastructure of the OZ.

B.4.5 Data Protection Requirements

[OZ-DP-100] The Internetwork should be capable of supporting SVPN data traffic connections between Edge Interfaces.

Rationale: This provides the capability to protect sensitive data transported through the Internetwork between sites or enclaves.

[OZ-DP-101] The OZ should be capable of supporting SVPN data traffic connections between ZIPs.

[OZ-DP-102] The OZ should be capable of supporting upper-layer security protocols (e.g., Secure Sockets Layer/Transport Layer Security, Simple Public-Key Mechanism, Secure Multimedia Internet Mail Extensions) used by applications.

Rationale: This provides the capability to protect sensitive data for session traffic that is being transported between OZ End-Systems and End-Systems in other Zones.

[OZ-DP-103] Although traffic at all sensitivity levels may be handled by the OZ, data protection measures may be required depending on the Statement of Sensitivity and the results of a TRA. In addition, data protection services may be applied at either the network layer or higher layers depending on the implementation requirements. Protected C and classified information will require additional controls and data protection mechanisms that are not specified in this Guideline.

[OZ-DP-104] Where encryption or digital signature is required, products (whether software, firmware, or hardware) must incorporate a CSEC-approved algorithm and CSEC-approved key management processes, such as those products validated to FIPS 140-1 and FIPS 140-2 by the CSEC through the CMVP and/or evaluated under the CSEC's CEP.

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and the CEP, each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e., product) must be (or must have been) validated or certified under a recognized program such as the CAVP. See *Information Technology Security Alert ITSA-11C* (reference [20]) for a list of CSEC-approved algorithms.

Note: CMVP solutions in general may be suitable for Protected B information. Consult the CSEC for solutions for Protected C and Classified information.

[OZ-DP-105] To protect against disclosure and modification of sensitive data:

a. data encryption should be employed when Protected C or classified data is being exchanged with End-Systems in other Zones or where portions of the Internetwork have been outsourced to a Network Service Provider;

b. data encryption should be employed when wireless media are used; and

c. the use of data encryption for transmission of Protected B information within the OZ and between the OZ and other GC-controlled Zones should be based on a continuous risk management approach. Additional protection may be required for data exchanged with End-Systems in other Zones or where portions of the Internetwork have been outsourced to a Network Service Provider.

Note: The processing of Protected C or classified data requires additional controls that are not specified in this Guideline.

[OZ-DP-106] If an OZ has End-Systems that process Protected C or classified information, then it is subject to Traffic Control requirement [OZ-TC-100] and Host Configuration requirement [OZ-HC-106].

Annex C Restricted Zone (RZ) Baseline Security Requirements

C.1 Introduction

This Annex provides a set of baseline security requirements for the Restricted Zone (RZ). An RZ is the standard environment for concentrations of End-Systems such as those found in data centres. It is the primary environment in which server farms, storage networks, and management servers are installed. It may also contain enclaves of end-user systems requiring higher levels of protection. The RZ is suitable for processing sensitive information, large repositories of sensitive data, and critical applications.

Traffic is restricted within an RZ. An RZ supports interfaces to Government of Canada (GC)-controlled Zones (Public Access Zone (PAZ), Operations Zone (OZ), and Highly Restricted Zone (HRZ)) and End-Systems within an RZ may serve public applications (mediated by a PAZ). Within an RZ, traffic should be constrained to limit the potential for interference between platform or application security domains. If warranted by a Threat and Risk Assessment (TRA), emanation security measures may be required to protect against unauthorized access to electronic emissions.

C.2 Reference Model

An RZ provides a general-purpose, private network environment under the control of a GC entity (i.e., under the single or shared control of departments and agencies). For many departments and agencies, the RZ will be the Zone where the bulk of sensitive information technology resources are placed.

The network threat environment provided by an RZ provides sufficient protection from denial-of-service (DoS) attacks to support deployment of high-availability applications. However, this Guideline does not require an RZ to be designed for high availability or high reliability.

Interfaces to all public services are implemented through a PAZ. External access from the RZ to the Internet is provided through an interface from the RZ to the PAZ. Access to an RZ from another department or agency is provided by interfaces to peer Zones (i.e., OZ, RZ, HRZ) in the other departments. Interfaces to sensitive services or repositories are implemented through tightly controlled interfaces provided by Zones.

An RZ has the structure of a generic Zone, (see Section 4.3). It is composed of four classes of components: Zone Interface Points (ZIPs), Internetwork components, Internal Boundary Systems (IBSs) and End-Systems. Typically, an RZ has a single Internetwork component and no IBSs and, unlike in the PAZ, IBSs play no role in the specification of security requirements. Figure 13 gives a high-level view of an RZ and its interconnection to other Zones. The ZIPs provide ingress and egress controls on traffic flows at the points where the RZ interconnects with other Zones. Where a node is shared between two Zones (like the Shared End-System in Figure 13), both Zone Authorities should agree on management and oversight of the node. Note that multiple ZIPs can be implemented through a single boundary device as long as the requirements for both Zones are being met and as long as it is mutually acceptable to both Network Security Zone Authorities. For example, a single appliance firewall with two separate physical interfaces may support an OZ and an RZ ZIP.

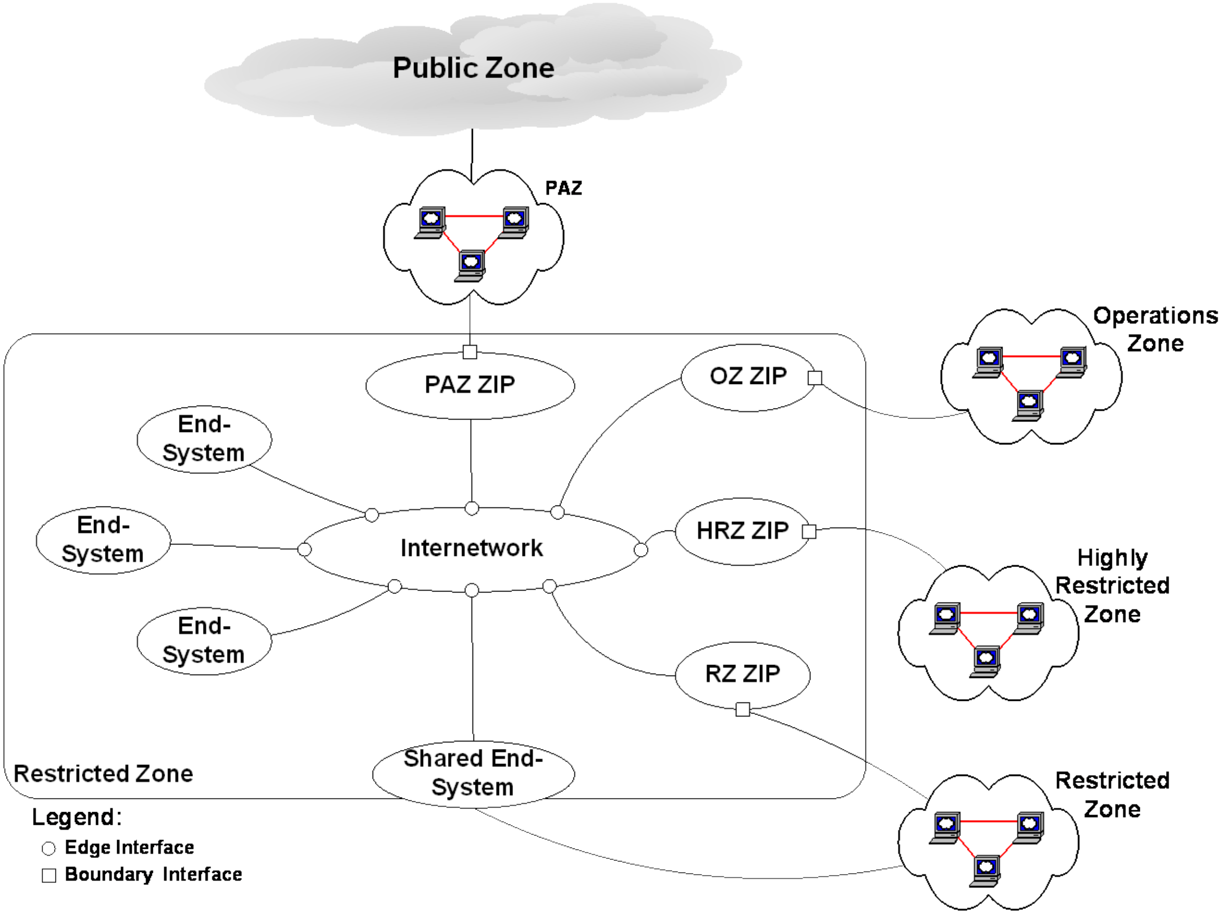
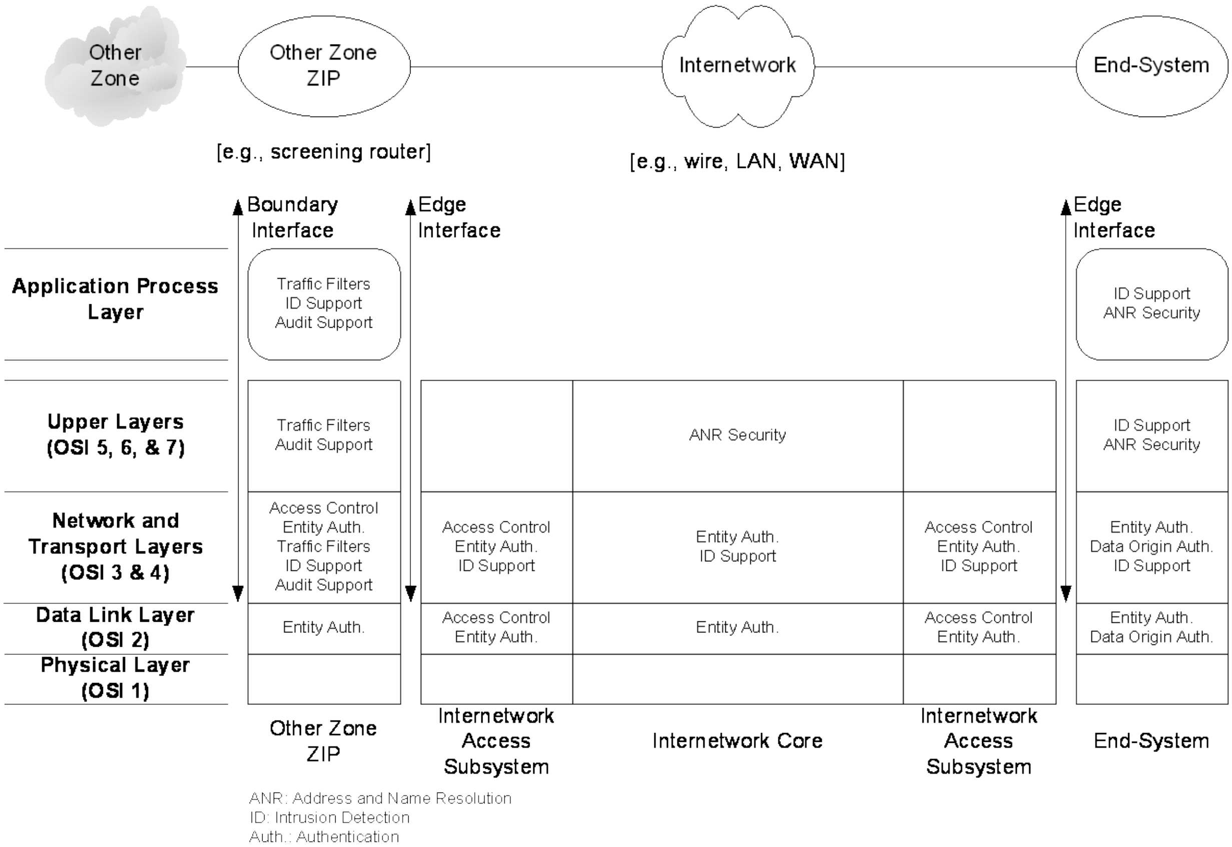


Figure 13 – Typical Restricted Zone (RZ) Logical Topology

Figure 13 also provides a logical view of the RZ and the interconnection relationships between components in an RZ. A ZIP provides the interface between internal RZ entities and other Zones[26]. The Internetwork provides the internal network for the RZ to aggregate and distribute traffic between End-Systems and ZIPs. End-Systems provide localized processing and storage of departmental information.

26A platform that provides logical separation of ZIPs may implement separate physical interfaces to more than one type of zone (i.e., other RZ, PAZ, OZ).

Figure 14 shows the RZ logical architecture. It identifies the entities that make up the RZ, the relations between entities, and the allocation of security services[27]. This figure provides an end-to-end mapping of the logical connection between the RZ and other GC Zones (i.e., OZ, other RZs, and HRZs), including the security services that are provided at various Open Systems Interconnection (OSI) Layers.



	Other Zone ZIP	Internetwork Access Subsystem	Internetwork Core	Internetwork Access Subsystem	End-System
Application Process Layer	Traffic Filters ID Support Audit Support				ID Support ANR Security
Upper Layers (OSI 5, 6, & 7)	Traffic Filters Audit Support		ANR Security		ID Support ANR Security
Network and Transport Layers (OSI 3 & 4)	Access Control Entity Auth. Traffic Filters ID Support Audit Support	Access Control Entity Auth. ID Support	Entity Auth. ID Support	Access Control Entity Auth. ID Support	Entity Auth. Data Origin Auth. ID Support
Data Link Layer (OSI 2)	Entity Auth.	Access Control Entity Auth.	Entity Auth.	Access Control Entity Auth.	Entity Auth. Data Origin Auth.
Physical Layer (OSI 1)					

ANR: Address and Name Resolution
ID: Intrusion Detection
Auth.: Authentication

Figure 14 – RZ Logical Architecture

C.3 Security Objectives

In general, the target security state of an RZ is a controlled network environment suitable for enterprise platform and application services and for client enclaves requiring higher levels of protection. An RZ is characterized by rigorous network configuration controls and carefully controlled traffic flow. Traffic control measures in an RZ are designed to contain security failures.

[27] The allocation of security services is based on the model of Section 4.4.2 and the requirements of Section C.4.2. See Section 4.4.2 for an explanation of the security services. In the RZ, not every service is required in every component or network layer.

Each objective and requirement specified in this Annex is labelled according to the following notation:

a. the first set of letters (RZ) refers to the Zone;

b. the second set of letters designates either an objective (i.e., OBJ) or a requirement. Requirements are grouped into the following categories as applicable: network interface (NI), traffic control (TC), network configuration (NC), host configuration (HC), and data protection (DP); and

c. each objective or requirement is sequentially numbered within its group[28].

C.3.1 Traffic Control Objectives

[RZ-OBJ-100] An RZ should protect the integrity and availability of End-Systems attached to the Zone. In particular, an RZ aims to:

a. prevent network-based DoS attacks within the Zone (e.g., SYN flood, smurf attack) from all attackers;

b. significantly reduce the impact of network-based DoS attacks originating from outside the Zone by concentrating the impact on the ZIPs;

c. prevent access to End-Systems as a result of network intrusions (e.g., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface) from sophisticated attackers or from the public telecommunication infrastructure;

d. contain the impact of a compromised End-System;

e. significantly reduce the ability to exploit End-Systems as staging points for attacks on End-Systems from all other sources;

f. limit the propagation of malicious traffic from other Zones in support of a) and b) and c); and

g. greatly reduce the propagation of malware.

Note: Network security measures are limited in their ability to protect End-Systems from compromises through valid application interfaces. The risks associated with threats of this type should be addressed through platform, application, and operational security measures. Malicious network traffic inside the RZ should only originate from the system staff or from compromised applications.

[RZ-OBJ-101] An RZ should provide the ability to continuously assess traffic at the interface to other Zones to continuously validate assumptions concerning the security environment provided by neighbouring Zones.

[28] These numbers are in addition to those defined in the previous version of this document (ITSD-02). Future versions of this document should maintain objective and requirement numbers across versions and indicate whether an objective or requirement has been rescinded or added.

[RZ-OBJ-102] An RZ should permit changes to enhance security measures in response to increased threat levels (e.g., time of crisis), including:

a. flexible, dynamic traffic controls based on Community of Interest;

b. increased status monitoring of ZIPs; and

c. ensuring that Network Service Providers increase surveillance of outsourced network infrastructure.

[RZ-OBJ-103] The PAZ implements safeguards that provide effective protection against malicious network traffic originating from public networks; however, there are residual risks from the other Zones that should be addressed by the RZ. The objective of the RZ is to:

a. significantly reduce susceptibility to attacks originating from compromised remote access and extranet End-Systems;

b. significantly reduce susceptibility to malicious traffic from compromised service delivery application servers in the PAZ by safeguards that include limiting access from these servers to designated resources and protocols; and

c. greatly reduce susceptibility to attacks originating from a compromised host in the PAZ other than a service delivery application server and against failures in PAZ traffic control measures including intrusions through the PAZ Internal Access Network.

Rationale: The PAZ Network Security Zone Authority has limited control over the configuration of applications residing on front-end servers. Thus, there is potential for compromise and thus the specification of explicit safeguards aimed at containing these interfaces.

C.3.2 Network Availability and Reliability Objectives

[RZ-OBJ-104] An RZ should protect the integrity and availability of network services by reducing the susceptibility to a variety of attacks. In particular, an RZ should:

a. significantly reduce the susceptibility of network services to DoS attacks from all sources (e.g. dedicated adversaries, infrastructure insiders, and network users) by filtering all other malicious attacks from outside the RZ;

b. prevent susceptibility to network intrusions (e.g., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface, or the compromise of an attached End-System) from sophisticated attackers or from the public telecommunication infrastructure;

c. prevent the ability to exploit End-Systems as staging points for attacks on other network services by external adversaries;

d. significantly reduce the ability to exploit End-Systems as staging points for attacks on network services from all other sources;

e. limit the propagation of malicious traffic from other Zones in support of sub-objectives (a), (b), and (c) above; and

f. greatly reduce the propagation of malware.

C.3.3 Data Protection Objectives

[RZ-OBJ-105] An RZ should significantly reduce susceptibility of traffic to interception by all adversaries.

[RZ-OBJ-106] An RZ should support data protection measures to protect the confidentiality and integrity of data. These measures include:

a. support for Secure Virtual Private Networks (SVPNs) within the Internetwork and across all ZIPs;

b. support for upper-layer security protocols; and

c. providing SVPN as an optional data service.

Rationale: RZ infrastructure may support a variety of physical media including wireless. It should be assumed that a sophisticated attacker could intercept traffic.

Note: Security services specific to the Service Delivery applications, such as access control and non-repudiation services, should be provided by application-specific components deployed in the Demilitarized Zone of a connected Public Access Zone.

C.4 RZ Security Requirements

This section describes the baseline security requirements for the RZ. These are categorized by operational requirement (i.e., network interface, traffic control, network configuration, host configuration, and data protection). Within each operational requirement category are sub-categories consisting of common requirements that apply across the entire RZ, followed by requirements specific to the Internetwork, the various types of ZIP, and certain types of End-System. Note that in some cases, a sub-category may not exist or have a heading because requirements for perimeter defence security are not applicable for that sub-category within that operational requirement category, or are common to the entire category.

The Zone Implementation Model (Section 4.2) allows a Restricted Extranet Zone (REZ) to connect to an RZ. This would require a REZ ZIP in the RZ. The security requirements for a REZ ZIP in an RZ should be established on a case-by-case basis, so this Guideline does not contain requirements for a REZ ZIP.

To achieve all of the Security Objectives for this Zone, as detailed above, the complete set of Security Requirements which follows must be implemented.

C.4.1 Network Interface Requirements

[RZ-NI-100] All network paths between the RZ and other Zones should pass through a ZIP.

Rationale: ZIPs implement traffic controls to reduce the volume and type of malicious traffic flowing between Zones.

[RZ-NI-101] The number of ZIPs between any two Zones should be limited.

Rationale: Limiting the number of ZIPs reduces the management burden and limits the introduction of security vulnerabilities due to operating and configuration errors. The number of ZIPs should be determined by the geographic distribution of the network, network traffic patterns, and the availability needs of supported applications.

[RZ-NI-102] All network paths destined for, or originating from a Public Zone (e.g., Internet), should pass through the PAZ. That is, the RZ should not have direct network connections to a Public Zone.

[RZ-NI-103] The ZIP and Internetwork components should support the attachment of network-based intrusion detection sensors (e.g., monitors). The attachment points should enable a complete view of all traffic. ZIP and Internetwork components should provide interfaces to support the collection of data from these sensors.

[RZ-NI-104] To protect the RZ from interference and tampering by untrusted subjects, the RZ should isolate its internal network from any other network infrastructure. That is, the RZ should not share:

a. any network-layer infrastructure with any other Zone;

b. any data link-layer infrastructure with any Public Zone; or

c. any physical-layer infrastructure with any Public Zone.

[RZ-NI-105] The Internetwork should be a logically separate network. It should maintain traffic interfaces only with:

a. ZIPs in the RZ; and

b. RZ End-Systems.

Exception: Traffic interfaces are permitted for approved appliances for outgoing Web access and the two remote access modes (extranet, SVPN).

C.4.2 Traffic Control Requirements

C.4.2.1 Common Traffic Control Requirements

[RZ-TC-100] If an RZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the RZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement.

[RZ-TC-101] RZ management traffic, other than traffic related solely to device status, should be segregated from operational traffic.

Note: Segregation may be either virtual or physical. That is, segregation may be achieved through encryption, network access controls, or physical separation.

[RZ-TC-102] The RZ should be capable of responding quickly to heightened security levels in case of emergency and increased threat, when and how authorized to do so. (Personnel should be aware, trained and authorized to initiate such a response.) For example, the RZ should possess the capability to improve the network security posture by increasing the level of security measures such as:

a. filtering at each ZIP;

b. active and/or passive monitoring;

c. protection to ensure the continuous delivery of critical services, including the capability to reconfigure or block non-essential services if required; and

d. auditing.

Note: Implementation of such measures should be carefully tested to ensure that these capabilities could not be exploited to cause a denial of service.

[RZ-TC-103] Each ZIP should authenticate the Boundary Interfaces of the ZIPs to which it connects. This authentication may be achieved through physical control over the media between the Boundary Interfaces.

C.4.2.2 Internetwork Traffic Control Requirements

[RZ-TC-104] The Internetwork should provide an access control service capable of enforcing access control requirements between Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[RZ-TC-105] The RZ Network Security Zone Authority should define requirements for an RZ Internetwork access control service based on the following principles:

a. the access control policy should be constructed to deny all traffic that is not explicitly permitted;

b. the access control policy should support Community of Interest separation (i.e., where network traffic is divided into natural communities of interests, the access control policy should enforce these natural traffic flows);

c. the access control policy should limit available network paths to vulnerable or sensitive End-Systems (e.g., test and development sub-networks and application servers supporting public applications);

d. the access control policy should be configured to limit available network paths for End-Systems accessible by extranets;

e. if the RZ Network Security Zone Authority permits connection to the RZ by remote access hosts with operating systems that do not provide separation of user and administrator roles, then the access control policy should be configured to limit access to other End-Systems by remote access hosts; and

f. if the Internetwork provides more than one class of service, the access control policy should support isolation between classes of service.

Rationale: Internal access controls contain intrusions and the spread of malware. Internal access controls also support the detection of malicious behaviour (e.g., router logs will often show an increase in access failures.). However, the RZ is intended to be a controlled network environment and access controls should be designed to allow all natural traffic flows.

[RZ-TC-106] If the RZ supports more than one class of service, the Internetwork should implement mechanisms to ensure non-interference between classes of service.

Rationale: If classes of service other than “best effort” are required by End-Systems, simple bandwidth consumption within one class of service can result in denial of service within another class of service unless controls are put in place to limit interference. Such controls are often available within mechanisms that implement class of service and quality of service.

[RZ-TC-107] The Internetwork should employ an addressing model that facilitates detection and diagnosis of malicious traffic.

Rationale: The choice of address model can have a significant impact on the ability to detect and isolate network problems in general and security problems in particular. It is good network design practice to facilitate access controls to isolate shared resources, and to segregate by location (e.g., remote access and extranet clients) and organization.

[RZ-TC-108] The RZ should support Internet Protocol (IPSec) traffic between any pair of Edge Interfaces.

Rationale: The RZ should permit End-System managers the option of implementing network-layer data protection. IPSec traversal of network address translation and firewall implementations may affect interoperability of some networks and applications.

C.4.2.3 Public Access Zone (PAZ) Zone Interface Point (ZIP)

[RZ-TC-109] The PAZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[RZ-TC-110] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. the access control policy should be constructed to deny all traffic that is not explicitly permitted;

b. all outgoing traffic should be restricted to destination addresses corresponding to designated proxy servers in the PAZ;

c. traffic to and from application servers should be restricted to addresses corresponding to front-end servers in the PAZ and to those protocols necessary to support communication with the front-end server;

d. extranet hosts should be restricted to a defined set of internal addresses which contain the resources required by the extranet; and

e. if the Network Security Zone Authority permits remote access hosts with open configurations (see host configuration at paragraph [RZ-HC-105]), then remote access clients should be restricted to a defined set of internal addresses.

[RZ-TC-111] If justified by a TRA, a stateful filter should be applied at the ZIP to ensure that incoming traffic is restricted to authorized protocols.

Rationale: The PAZ can normally be trusted to filter out most malicious traffic originating from the Internet provided all outgoing access is routed through a designated proxy server and incoming traffic (remote access, extranet, and applications) is limited to specified resources. Additional protection using stateful inspection at the ZIP may be justified if the protection provided by the PAZ is in doubt.

[RZ-TC-112] An intrusion detection capability should be implemented at the ZIP.

Rationale: Access controls, together with the controls applied in the PAZ, should eliminate most attacks via the ZIP. However, these safeguards will not provide complete protection. The resources required to manage these sensors should be modest since the frequency of alarms at this interface should be low.

[RZ-TC-113] If warranted by a TRA or if required by the Network Security Zone Authority to enforce Internet Use Policy, a content filter should be implemented at the PAZ ZIP.

C.4.2.4 Operations Zone (OZ) Zone Interface Point (ZIP)

[RZ-TC-114] The OZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[RZ-TC-115] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this ZIP;

b. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses; and

c. the access controls should support interdepartmental applications.

Rationale: In communications between two internal Zones, each Zone depends on the other to apply controls on ingress. Consequently, few controls are required on egress.

[RZ-TC-116] OZ ZIPs should implement network-layer and upper-layer controls to protect RZ hosts from traffic originating from OZs and to protect OZs in the event that malicious traffic originates from within the RZ.

[RZ-TC-117] The OZ ZIP should support the implementation of an intrusion detection capability.

[RZ-TC-118] If justified by a TRA, a stateful filter should be applied at the ZIP to ensure that incoming traffic is restricted to authorized protocols.

[RZ-TC-119] If client e-mail functionality is deployed within the RZ, an e-mail gateway should be employed at the OZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[29].

Note: The e-mail gateway is not needed if the RZ is simply used to provide an e-mail server.

Rationale: E-mail is the primary vector for the spread of malware.

[RZ-TC-120] If justified by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the OZ ZIP.

[RZ-TC-121] If the OZ ZIP interface to common infrastructure shares traffic control functionality with the common infrastructure provider, then the service level agreement should include the baseline requirements for both sides of the interface.

C.4.2.5 Restricted Zone (RZ) Zone Interface Point (ZIP)

[RZ-TC-122] If justified by a TRA, the RZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces.

[29] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[RZ-TC-123] The Network Security Zone Authority should define an access control policy that reflects the access-control-related risks identified by the TRA.

[RZ-TC-124] If client e-mail functionality is deployed within the RZ, an e-mail gateway should be employed at the RZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[30].

Rationale: E-mail is the primary vector for the spread of malware.

[RZ-TC-125] An intrusion detection capability should be implemented at the RZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

[RZ-TC-126] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

[RZ-TC-127] If warranted by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the RZ ZIP.

C.4.2.6 Highly Restricted Zone (HRZ) Zone Interface Point (ZIP)

[RZ-TC-128] If justified by a TRA, the HRZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces.

[RZ-TC-129] The Network Security Zone Authority should define an access control policy that reflects the access-control-related risks identified by the TRA.

[RZ-TC-130] If client e-mail functionality is deployed within the RZ, an e-mail gateway should be employed at the HRZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[31].

Rationale: E-mail is the primary vector for the spread of malware.

[RZ-TC-131] An intrusion detection capability should be implemented at the HRZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

[RZ-TC-132] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

[RZ-TC-133] If warranted by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the HRZ ZIP.

[30] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[31] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

C.4.3 Network Configuration Requirements

C.4.3.1 Common Network Configuration Requirements

[RZ-NC-100] The RZ network configuration should be monitored to detect changes. Unauthorized changes should be reported to the Network Security Zone Authority.

Rationale: Continuous status monitoring is necessary to detect unauthorized changes to the network configuration in a timely manner. Timely detection allows Zone Authorities of impacted Zones to respond to prevent or limit damage from an attack or failure.

[RZ-NC-101] The RZ boundary and Edge Interfaces should be registered with the RZ Network Security Zone Authority.

[RZ-NC-102] Each RZ interface should act in exactly one role: Boundary or Edge Interface.

[RZ-NC-103] The RZ Network Security Zone Authority should periodically verify the network topology. The frequency of such verifications should be determined by the Network Security Zone Authority and documented in configuration management procedures for the RZ.

[RZ-NC-104] The RZ Network Security Zone Authority should periodically assess the network configuration for unauthorized external interfaces (e.g., modems and wireless access points (APs)). The frequency of assessments should be determined by the Network Security Zone Authority and documented in configuration management procedures for the RZ.

Rationale: The presence of unauthorized modems can create vulnerabilities in a well-configured network. These unauthorized modems provide a means to bypass most or all of the security measures in place to stop unauthorized users from accessing a network.

C.4.3.2 Zone Interface Point (ZIP) Network Configuration Requirements

a. [RZ-NC-105] RZ Boundary Interface addresses should be distinct and dedicated. RZ Boundary Interface addresses should be visible to other GC Zones but should not be visible to the Public Zone.

b. [RZ-NC-106] RZ Boundary Interfaces should be assigned addresses upon attachment to the network.

c. [RZ-NC-107] A change to an RZ Boundary Interface address assignment should constitute a configuration change requiring approval by the RZ Network Security Zone Authority. Approval may be given in advance to permit dynamic reconfiguration; however, the conditions under which such a change may be effected should be delineated clearly.

C.4.3.3 Internetwork Configuration Requirements

[RZ-NC-108] The RZ Network Security Zone Authority should maintain current configuration information for all interfaces within the Internetwork. The configuration information should include:

a. a unique identifier;

b. the status of the interface (active/non-active);

c. the address assignment rules;

d. the current network address;

e. the list of all names/aliases associated with all interfaces within the Internetwork;

f. the current physical-layer interface to which all interfaces within the Internetwork are assigned;

g. the communications security parameters for all interfaces within the Internetwork; and

h. security constraints on the instantiation of each interface within the Internetwork.

[RZ-NC-109] The following changes to an RZ should be approved by the RZ Network Security Zone Authority before implementation:

a. addition or deletion of an interface within the Internetwork;

b. a change to the address assignment rules for any interface within the Internetwork;

c. a change to the communications security parameters of any interface within the Internetwork; and

d. a change to the security constraints on the instantiation of any interface within the Internetwork.

Rationale: These changes may affect the implementation of security measures or the configuration of intrusion detection capabilities.

[RZ-NC-110] Edge Interfaces should establish security associations with external Edge Interfaces and all communications should be authenticated (either explicitly or implicitly) within the context of these security associations. The security associations permitted should be determined by traffic control requirements.

Note: The type and strength of authentication are implementation dependent. The goal is to prevent an intruder attaching a network-layer entity in the core and masquerading as an Edge Interface.

[RZ-NC-111] Internetwork Edge Interfaces should be authenticated to each other through one of the following methods:

a. cryptographic authentication mechanisms applied at the network layer; or

b. physical controls over the Edge Interfaces and over all media connecting these interfaces.

Rationale: Because the Internetwork is a significant component of an internal GC Zone, it is extremely important that hostile entities be excluded from masquerading as an Edge Interface.

[RZ-NC-112] The service level agreement should require the Network Service Provider to control changes to all Internetwork interfaces under Provider's control and to report to the RZ Network Security Zone Authority any changes that impact the security association between Edge Interfaces.

[RZ-NC-113] The service level agreement should require the Network Service Provider to provide evidence that the security controls used to enforce the security within the Internetwork Core are effective and to report all security incidents that could impact the RZ to the RZ Network Security Zone Authority. The Network Service Provider should also provide the RZ Network Security Zone Authority with the capability to verify the effectiveness of the controls on at least a quarterly basis.

C.4.3.4 Wireless Network Configuration Requirements

[RZ-NC-114] Addresses provided to End-Systems that use wireless/radio frequency (RF) data link layers should be assigned dynamically from a segregated address pool (i.e., an assigned range of addresses).

Rationale: Address assignment from a distinct pool of addresses permits access control by Community of Interest. Dynamic address assignment permits address reuse.

[RZ-NC-115] Wireless hosts should be authenticated to the RZ using strong peer-entity and data origin authentication before the establishment of a connection to the RZ.

Rationale: Authentication of the host provides confirmation that the connection being processed is coming from a valid source. Persistent authentication would be necessary to permit roaming between APs.

[RZ-NC-116] Peer-entity and data origin authentication at the data link layer should be used to establish connections between wireless APs and wireless hosts.

Rationale: Authentication of the host provides confirmation that the connection being processed is coming from a valid End-System.

[RZ-NC-117] Wireless APs should be placed in locations that optimize coverage and minimize exposure to eavesdropping.

[RZ-NC-118] The RZ Network Security Zone Authority should conduct a mapping of the signal strength, in the horizontal and vertical planes, for all wireless APs in the RZ. Such mappings should be updated periodically. The frequency of mapping updates should be determined by the Network Security Zone Authority.

Rationale: A map of signal strength defines the physical space into which RF energy is transmitted. This mapping is particularly relevant in multi-level buildings and in built-up areas where the wireless signal extends beyond the perimeter of physical security zones. RF-based wireless networks are subject to all the security issues normally faced with conventional wired networks but additionally, they suffer from vulnerabilities directly associated with the use of wireless connectivity. The nature of the wireless medium makes it practically impossible to confine the radio signals to a controlled location. Unless TEMPEST shielding is used or adequate physical zoning is established, the radiated signals are subject to clandestine interception and exploitation. Finally, eavesdroppers may use high-gain antennas, which permit interception of wireless signals beyond the limit of a manufacturer's specification of signal distance.

[RZ-NC-119] The RZ Network Security Zone Authority should monitor[32] the wireless local area network to:

a. understand the nature of traffic (e.g. data/protocols)

b. discover traffic generated by unauthorized users (e.g. outsiders);

c. find irregular traffic generated by legitimate users;

d. make an inventory of APs; and

e. solve problems.

[RZ-NC-120] The RZ Network Security Zone Authority should perform network discovery inside his or her facilities and evaluate the list of discovered APs and communication channels with the inventory of authorized APs and communication channels.

[RZ-NC-121] The wireless intrusion detection policy should be integrated with facility access policies.

Rationale: The source of a wireless network intrusion may be within an organization's controlled physical space. If so, a suitable response may be a physical response to locate the source and remove it from the facility.

C.4.3.5 End-System Network Configuration Requirements

[RZ-NC-122] End-Systems should maintain the integrity of network interfaces with GC Zones while connected to an RZ. Dual-homing, tunnel-splitting, or other shared network paths with the Public Zone by RZ End-Systems should not be permitted.

Rationale: Simultaneous connection of an Ethernet interface to an RZ and an active modem connection to the Internet would permit intrusion to the RZ. Similarly, having an SVPN tunnel split between an RZ and the Internet would permit intrusion. Similarly, having a wireless interface available for incoming connections while maintaining a wired interface to an RZ can permit intrusion (i.e., port forwarding should be turned off).

[RZ-NC-123] Wireless devices should be configured to limit or suppress broadcasting of their device identifiers (such as IEEE 802.11 Service Set Identifiers).

[32] WLAN monitoring may involve the interception of private communications, which may constitute a violation of Canadian law, including the Criminal Code. Before using monitoring tools on any WLAN, it is recommended to consult with legal services to ensure that the monitoring does not violate Canadian law.

[RZ-NC-124] If remote management is allowed, an RZ should allow only authorized administrators to remotely manage RZ nodes from a GC-controlled Zone or from a Restricted Extranet Zone. The access should be controlled and protected by using the following methods:

a. strong authentication; and

b. restricting access by Internet Protocol address, port, and protocol.

C.4.4 Host Configuration Requirements

C.4.4.1 Common Host Configuration Requirements

[RZ-HC-100] The RZ Network Security Zone Authority should maintain a host configuration policy consistent with applicable baseline security requirements, standards, and guidance. This policy should apply to all hosts attached to the Zone.

Note: From a Zone perspective, the host configuration policy should be limited to specifying the constraints on the software load and the maintenance procedures required to prevent a sophisticated attacker from compromising a host and using that host to attack network assets. The policy should also reduce susceptibility to compromise from all other sources. The primary focus should be the control of malware as this is the easiest and most prevalent method of attack. Note that hosts may be subject to additional platform security requirements to protect applications and data; however, these are outside the scope of Zone requirements. These additional platform security requirements will depend on the type of host (e.g., workstation, application server).

[RZ-HC-101] The host configuration policy should contain:

a. a specification of prohibited and mandated software and hardware configurations such as not allowing active modems, “sniffer” software, and remote access software permitting control of an RZ host, but requiring the installation of current anti-virus software;

b. minimum maintenance procedures for all software components (e.g., configuration management procedures for hardware and software, emergency patch procedures, technician training, etc.); and

c. specific maintenance procedures for software that provides client access to Internet-based resources and for software that provides back-end services to public clients (e.g., mail service).

Rationale: The RZ and the Internetwork infrastructure should limit direct intrusions (i.e., those not using malware) to sophisticated attackers. Host configuration controls are aimed at further reducing the susceptibility to such intrusions. In most cases, an RZ will be a large network installation with diverse business needs and distributed authority over End-Systems. Although it is impractical to expect rigid controls over all End-System configurations in such diverse environment, a minimum practical level of discipline over the End-System configuration is necessary to reduce the susceptibility to intrusion via End-Systems. The greatest attention should be placed on any software that has the potential to interact with public networks.

[RZ-HC-102] The RZ Network Security Zone Authority should ensure that End-System managers are aware of this host configuration policy and that they ensure the policy is enforced.

[RZ-HC-103] Regular network vulnerability assessments (VAs) of all hosts should be conducted to assess trends in the effectiveness of the host configuration policy. The frequency of such VAs should be sufficient to support trend analysis. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: Network VAs involve port scans and possibly some software fingerprinting. The goal is to provide the Network Security Zone Authority with a picture of the vulnerability of end systems and compliance to the host configuration policy. This approach has been chosen to balance a liberal approach to host configuration control. A significant change in the results may indicate a widespread problem or may be evidence that other measures are required.

[RZ-HC-104] All hosts should invoke controls that implement continuous protection against malware at start-up. The Network Security Zone Authority should approve any exceptions to this requirement.

Rationale: Malware is the easiest and most likely vehicle for an external attacker to gain control of an End-System to attack GC systems. Controls are placed in the RZ to reduce the amount of malware that reaches the End-System. However, no network filter is completely effective and malware protection is required on the hosts within the End-Systems. Exceptions may be required for those few hosts for which it may be prohibitively expensive or impossible to meet the requirement (e.g., mainframes, super computers).

[RZ-HC-105] All hosts that provide applications to permit client access to public resources (e.g., Internet web browser and e-mail clients) should:

a. employ an operating system that provides separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege); and

b. be configured to operate any applications that provide access to public resources in user mode.

Rationale: If the platform is able to enforce configuration controls by restricting changes to administrators, then many intrusion scenarios can be thwarted. Most new commercial operating systems (e.g., Windows 2000, Windows NT, Windows XP, Apple OS X, and all UNIX/Linux variants) provide this capability.

[RZ-HC-106] If an RZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the RZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement (see traffic control at paragraph [RZ-TC-100]).

[RZ-HC-107] Operating systems for all nodes should be hardened based on documented best practices.

[RZ-HC-108] System and network management processes and technology should be implemented within an RZ to detect changes in node configurations.

[RZ-HC-109] Regular backups of system files and system configuration parameters should be performed for every node contained in the RZ. Frequency and retention period of backups should be consistent with business needs.

[RZ-HC-110] The failure of an RZ node should not result in the compromise of its resources or those of any connected network.

[RZ-HC-111] All RZ nodes should be within an area that meets as a minimum the physical security requirements of a physical Security Zone (see reference [26]).

C.4.4.2 Shared End-System Configuration Requirements

[RZ-HC-112] A shared End-System, whether shared permanently or periodically, should comply with the following:

a. it should employ an operating system which supports the separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege);

b. changes to network configuration should require administrative privileges;

c. the End-System configuration and procedures for maintaining that configuration should be approved by the RZ Network Security Zone Authority;

d. the End-System should be subject to regular VAs, the frequency of which should be determined by the Network Security Zone Authority and documented in VA procedures for the Zone. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.; and

e. requirements [RZ-TC-100] and [RZ-HC-106] (if applicable).

Rationale: Shared End-Systems have the potential to create back doors between Zones. Shared End-Systems are also likely to be relatively few in number, making greater control possible. This vulnerability scan focuses on vulnerabilities associated with routing.

[RZ-HC-113] If an End-System (e.g., laptop) is shared periodically with a Public Zone, then the End-System should include a personal firewall; it should also include a configuration integrity mechanism capable of identifying changes to the configuration and notifying the End-System administrator.

C.4.4.3 Wireless End-System Configuration Requirements

[RZ-HC-114] A shared End-System that uses wireless interfaces, whether it is shared permanently or periodically, is subject to the following:

a. it should employ an operating system that enforces the separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege);

b. changes to network configuration should require administrative privileges;

c. the End-System configuration and procedures for maintaining that configuration should be approved by the RZ Network Security Zone Authority; and

d. the End-System should be subject to regular VAs, the frequency of which should be determined by the Network Security Zone Authority and documented in VA procedures for the Zone. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: Wireless End-Systems have the potential to create back doors between Zones.

[RZ-HC-115] If an End-System using wireless interface(s) is shared periodically with a Public Zone, then:

a. the End-System should include a personal firewall; and

b. the End-System should include a configuration integrity mechanism.

C.4.4.4 Network Node Configuration Requirements

[RZ-HC-116] SVPN products, if used, should be validated to Federal Information Processing Standard (FIPS) 140-1 and FIPS 140-2 at a minimum of Security Level 2 through the Cryptographic Module Validation Program (CMVP).

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and Cryptographic Endorsement Program (CEP), each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the Cryptographic Algorithm Validation Program (CAVP).

[RZ-HC-117] Internetwork devices and ZIP devices should be physically secured to limit access to only those authorized personnel with an ongoing need to access the equipment, in accordance with the Principles of Least Privilege and Need-to-Know.

Rationale: Restricted access to devices with Edge Interfaces reduces the opportunity for network reconfiguration or introduction of unauthorized Edge Interfaces. A Network Service Provider can restrict access with physical barriers such as cages. Devices located at GC premises can be located in physical security zones (see reference [26]).

C.4.4.5 Complex End-System Configuration Requirements

[RZ-HC-118] A complex End-System should have a certification and accreditation review before attachment to an Edge Interface is permitted.

Rationale: Complex End-Systems may contain private networks between their components, may have traffic controls, and may have unique network configurations that could compromise the infrastructure of the RZ.

C.4.5 Data Protection Requirements

[RZ-DP-100] The Internetwork should be capable of supporting SVPN data traffic connections between Edge Interfaces.

Rationale: This provides the capability to protect sensitive data transported through the Internetwork between sites or enclaves.

[RZ-DP-101] The RZ should be capable of supporting SVPN data traffic connections between ZIPs.

[RZ-DP-102] The RZ should be capable of supporting upper-layer security protocols (e.g., Secure Sockets Layer/Transport Layer Security, Simple Public-Key Mechanism, and Secure Multimedia Internet Mail Extensions) used by applications.

Rationale: This provides the capability to protect sensitive data for session traffic that is being transported between RZ hosts and servers or hosts and servers in other Zones.

[RZ-DP-103] Although traffic at all sensitivity levels may be handled by the RZ, data protection measures are required depending on the Statement of Sensitivity and the results of a TRA. In addition, data protection services may be applied at either the network layer or higher layers depending on the implementation requirements. Protected C and classified information will require additional controls and data protection mechanisms that are not specified in this Guideline.

[RZ-DP-104] Where encryption or digital signature is required, products (whether software, firmware or hardware) must incorporate a CSEC-approved algorithm and CSEC-approved key management processes, such as those products validated to FIPS 140-1 and FIPS 140-2 by CSEC through the CMVP and/or evaluated under CSEC's CEP.

Note 1: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and CEP, each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the CAVP. See *Information Technology Security Alert ITSA-11C* (reference [20]) for a list of CSEC-approved algorithms.

Note 2: CMVP solutions in general may be suitable for Protected B information. Consult the CSEC for solutions for Protected C and classified information.

[RZ-DP-105] To protect against disclosure and modification of sensitive data:

a. data encryption should be employed when Protected C or classified data is being exchanged with End-Systems in other Zones or where portions of the Internetwork have been outsourced to a Network Service Provider;

b. data encryption should be employed for transmission of designated or classified information over wireless media; and

c. the use of data encryption for transmission of Protected B information within the RZ and between the RZ and other internal Zones should be based on a continuous risk management approach. Additional protection may be required for data exchanged with End-Systems in other Zones or where portions of the Internetwork have been outsourced to a Network Service Provider.

Note: The processing of Protected C or classified data requires additional controls that are not specified in this Guideline.

[RZ-DP-106] If an RZ has End-Systems that process Protected C or classified information, then it is subject to Traffic Control requirement [RZ-TC-100] and Host Configuration requirement [RZ-HC-106].

Annex D Highly Restricted Zone (HRZ) Baseline Security Requirements

D.1 Introduction

This Annex provides a set of baseline security requirements for the Highly Restricted Zone (HRZ). An HRZ is a tightly controlled network environment for highly sensitive Government of Canada (GC) operations. It is designed for enterprise platform and application services and for client enclaves requiring the highest levels of protection. The HRZ is suitable for processing sensitive information and for safety-critical applications (i.e., those with high reliability requirements, where compromise of the information technology (IT) systems would endanger human health or safety).

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. Data confidentiality services, suitable for protecting classified 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. If warranted by a Threat and Risk Assessment (TRA), emanation security measures may be required to protect against unauthorized access to electronic emissions.

D.2 Reference Model

An HRZ provides a purpose-specific private network environment under the control of a GC entity (i.e., under the single or shared control of departments and agencies). For many departments, the HRZ will be the Network Security Zone where the bulk of highly sensitive IT resources are placed.

The HRZ is intended for routine high sensitivity departmental or agency information services. However, with additional security measures, an HRZ should be capable of processing and distributing sensitive departmental information using appropriately configured hosts, upper-layer security protocols, and application security controls.

In general, sensitive information repositories (e.g., large enterprise databases or databases containing sensitive information) could be maintained in the HRZ[33].

The network threat environment provided by an HRZ provides sufficient protection from network denial-of-service (DoS) attacks to support the deployment of high-availability applications on critical End-Systems. However, this Guideline does not require an HRZ to be designed for high availability or high reliability.

[33] “Sensitivity” in this context means sensitivity in terms of confidentiality, availability, and integrity. This is broader in meaning than the term “classification”, which refers specifically and only to sensitivity in terms of confidentiality. See also the definition of sensitive in Section 5.

Interfaces to all public services should be justified by a TRA and should be implemented through an Operations Zone (OZ) or Restricted Zone (RZ) and from there to a Public Access Zone (PAZ). Access to other GC departments is provided by interfaces to peer HRZs, OZs, or RZs. Interfaces to sensitive services or repositories are implemented through tightly controlled interfaces provided by Zones.

An HRZ has the structure of a generic Zone (see Figure 5). It is composed of four classes of components: Zone Interface Points (ZIPs), Internetwork components, Internal Boundary Systems (IBSs) and End-Systems. Typically, an HRZ has a single Internetwork component and no IBSs and, unlike the PAZ, IBSs play no role in the specification of security requirements. A high-level view of an HRZ and its interconnection to other Zones is provided at Figure 15. The ZIP provides ingress and egress controls on traffic flows at the points where the HRZ interconnects with other Zones. Where a node is shared between two Zones (like the Shared End-System in Figure 15), both Zone Authorities should agree on management and oversight of the node. Note that multiple ZIPs can be implemented through a single boundary device as long as the requirements for Zones are being met and as long as it is mutually acceptable to both Network Security Zone Authorities. For example, a single appliance firewall with two separate physical interfaces may support an RZ and an HRZ ZIP.

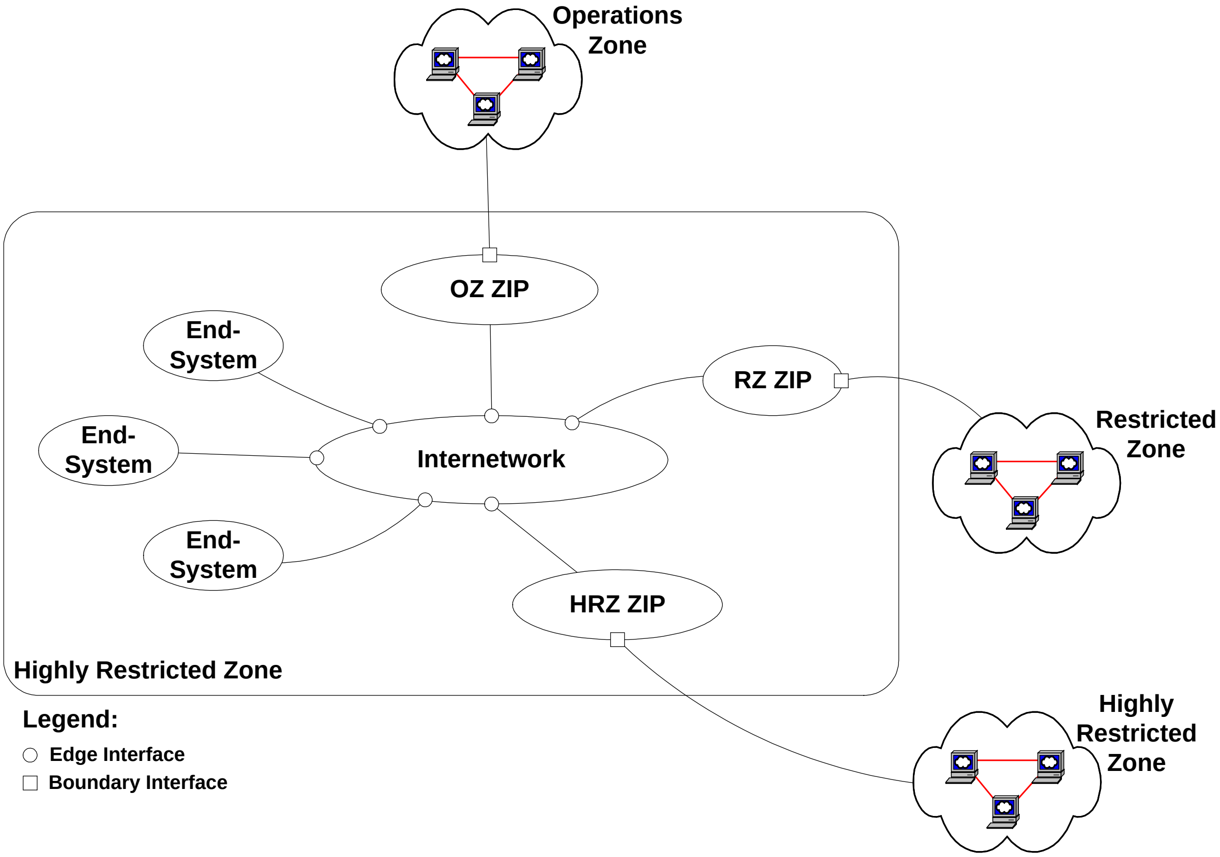
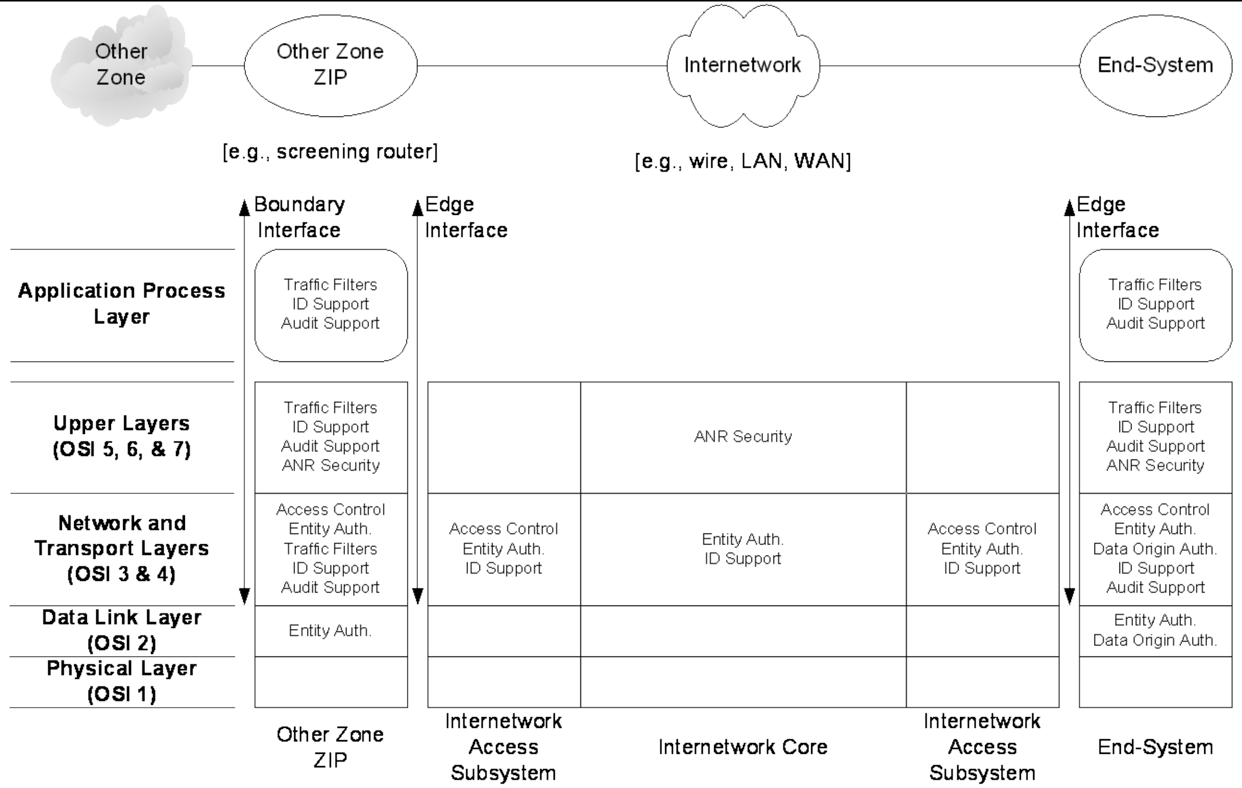


Figure 15 – Typical Highly Restricted Zone (HRZ) Logical Topology

Figure 15 also provides a logical view of the HRZ and the interconnection relationships between components in an HRZ. A ZIP provides the interface between internal HRZ entities and other Zones[34]. The Internetwork provides the internal network for the HRZ to aggregate and distribute traffic between End-Systems and ZIPs. End-Systems provide localized processing and storage of departmental information.

Figure 16 shows the HRZ logical architecture. It identifies the entities that make up the HRZ, the relations between entities, and the allocation of security services[35]. This figure provides an end-to-end mapping of the logical connection between the HRZ and other GC Zones (i.e., OZ, other RZs, and HRZs), including the security services that are provided at various Open System Interconnection (OSI) Layers.

[34]A platform that provides logical separation of ZIPs may implement separate physical interfaces to more than one type of zone (i.e., other HRZ, OZ, RZ). For example, a separate physical interface connection to another zone.
[35] The allocation of security services is based on the model of Section 4.4.2 and the requirements of Section D.4.2. See Section 4.4.2 for an explanation of the security services. In the HRZ, not every service is required in every component or OSI layer.



	Other Zone ZIP	Internetwork Access Subsystem	Internetwork Core	Internetwork Access Subsystem	End-System
Application Process Layer	Traffic Filters ID Support Audit Support				Traffic Filters ID Support Audit Support
Upper Layers (OSI 5, 6, & 7)	Traffic Filters ID Support Audit Support ANR Security		ANR Security		Traffic Filters ID Support Audit Support ANR Security
Network and Transport Layers (OSI 3 & 4)	Access Control Entity Auth. Traffic Filters ID Support Audit Support	Access Control Entity Auth. ID Support	Entity Auth. ID Support	Access Control Entity Auth. ID Support	Access Control Entity Auth. Data Origin Auth. ID Support Audit Support
Data Link Layer (OSI 2)	Entity Auth.				Entity Auth. Data Origin Auth.
Physical Layer (OSI 1)					

ANR: Address and Name Resolution
ID: Intrusion Detection
Auth.: Authentication

Figure 16 – HRZ Logical Architecture

D.3 Security Objectives

In general, the target security state of an HRZ is a network environment that provides a tightly controlled network environment suitable for sensitive enterprise platform and application services and for client enclaves requiring higher levels of protection. An HRZ is characterized by rigorous network and host configuration controls and carefully controlled traffic flow. Traffic control measures in an HRZ are designed to contain security failures.

Each objective and requirement specified in this Annex is labelled according to the following notation:

a. the first set of letters (HRZ) refers to the Zone;

b. the second set of letters designates either an objective (i.e., OBJ) or a requirement. Requirements are group ed into the following categories as applicable: network interface (NI), traffic control (TC), network configuration (NC), host configuration (HC) and data protection (DP); and

c. each objective or requirement is sequentially numbered within its group[36].

D.3.1 Traffic Control Objectives

[HRZ-OBJ-100] An HRZ should protect the integrity and availability of End-Systems attached to the Zone by preventing the prevalence of malicious network traffic including network traffic originating from a small population of system staff or from compromised applications. In particular, an HRZ aims to:

a. prevent network-based DoS attacks within the Zone (e.g., SYN flood, smurf attack);

b. significantly reduce the impact of network-based DoS attacks originating from outside the Zone by concentrating the impact on the ZIPs;

c. prevent access to End-Systems as a result of network intrusions (e.g., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface);

d. contain the impact of a compromised End-System;

e. prevent the ability to exploit End-Systems as staging points for attacks on End-Systems from all other sources;

f. prevent the propagation of malicious traffic from other Zones in support of (a), (b), and (c); and

g. stop the propagation of malware.

Note: Network security measures are limited in their ability to protect End-Systems from compromises through valid application interfaces. The risks associated with threats of this type should be addressed through platform, application, and operational security measures. The only malicious network traffic that should occur inside the HRZ is expected to originate from the system staff or from compromised applications.

[HRZ-OBJ-101] An HRZ should provide the ability to continuously assess traffic at the interfaces to other Zones to continuously validate assumptions concerning the security environment provided by neighbouring Zones.

[HRZ-OBJ-102] An HRZ should permit changes to enhance security measures in response to increased threat levels (e.g., time of crisis), including:

a. flexible, dynamic traffic controls based on Community of Interest;

b. increased status monitoring of ZIPs; and

c. ensuring that Network Service Providers increase surveillance of outsourced network infrastructure.

[36] These numbers are in addition to those defined in the previous version of this document (ITSD-02). Future versions of this document should maintain objective and requirement numbers across versions and indicate whether an objective or requirement has been rescinded or added.

[HRZ-OBJ-103] The RZ and OZ implement safeguards that provide effective protection against malicious network traffic originating from public networks; however, there are residual risks from the other Zones that should be addressed by the HRZ. The objective of the HRZ is to:

a. significantly reduce susceptibility to attacks originating from compromised remote access and extranet End-Systems;

b. significantly reduce susceptibility to malicious traffic from compromised service delivery application servers in the other Zones by safeguards that include limiting access from these servers to designated resources and protocols; and

c. greatly reduce susceptibility to attacks originating from compromised hosts in other Zones (other than a service delivery application server, which is addressed in sub-paragraph b, above) and against failures in other Zones' traffic control measures including intrusions through other Zones' Internetworks.

Rationale: Other Network Security Zone Authorities have limited control over the configuration of applications residing on front-end servers. Thus, there is potential for compromise and thus the specification of explicit safeguards aimed at containing these interfaces. All other hosts within the other Zones are completely within the control of the other Network Security Zone Authorities and a more general statement of objective is sufficient.

D.3.2 Network Availability and Reliability Objectives

[HRZ-OBJ-104] An HRZ should protect the integrity and availability of network services by reducing the susceptibility to a variety of attacks. In particular, an HRZ should:

a. significantly reduce the susceptibility of network services to DoS attacks from all sources (e.g. dedicated adversaries, infrastructure insiders, and network users), by filtering all external malicious attacks from outside the HRZ;

b. prevent susceptibility to network intrusions (e.g., the attachment of an unauthorized device to an existing interface, the addition of an unauthorized Edge Interface, or the compromise of an attached End-System) from all sources;

c. prevent the ability to exploit End-Systems as staging points for attacks on other network services by external adversaries;

d. significantly reduce the ability to exploit End-Systems as staging points for attacks on network services from all other sources;

e. limit the propagation of malicious traffic from other Zones in support of (a), (b), and (c) above; and

f. greatly reduce the propagation of malware.

D.3.3 Data Protection Objectives

[HRZ-OBJ-105] An HRZ should significantly reduce susceptibility to interception by external adversaries.

[HRZ-OBJ-106] An HRZ should support data protection measures to protect the confidentiality and integrity of data. These measures include:

a. support for Secure Virtual Private Networks (SVPNs) within the Internetwork and across all ZIPs;

b. support for upper-layer security protocols; and

c. providing SVPN as an optional data service.

Rationale: The HRZ infrastructure may support a variety of physical media. It should be assumed that a sophisticated attacker could intercept traffic.

Note 1: There are many situations across the GC in which employees from another department must gain access to network services and be able to securely access their home network. These situations may include temporary access through a wireless AP located in a boardroom, or permanent access for employees assigned to the host department (e.g. Justice employees at other departments).

Note 2: Security services specific to the Service Delivery applications, such as access control and non-repudiation services should be provided by application-specific components deployed in a Demilitarized Zone (DMZ) in the department's PAZ.

D.4 Security Requirements

This section describes the baseline security requirements for the HRZ. These are categorized by operational requirement (i.e., network interface, traffic control, network configuration, host configuration, and data protection). Within each operational requirement category are sub-categories consisting of common requirements that apply across the entire HRZ, followed by requirements specific to the Internetwork, the various types of ZIP, and certain types of End-System. Note that in some cases, a sub-category may not exist or have a heading because requirements for perimeter defence security are not applicable for that sub-category within that operational requirement category, or are common to the entire category.

The Zone Implementation Model (Section 4.2) allows a Restricted Extranet Zone (REZ) to connect to an HRZ. This would require a REZ ZIP in the HRZ. The security requirements for a REZ ZIP in an HRZ should be established on a case-by-case basis, so this Guideline does not contain requirements for a REZ ZIP.

To achieve all of the Security Objectives for this Zone, as detailed above, the complete set of Security Requirements which follows must be implemented.

D.4.1 Network Interface Requirements

[HRZ-NI-100] All network paths between the HRZ and other Zones should pass through a ZIP.

Rationale: ZIPs implement traffic controls to reduce the volume and type of malicious traffic flowing between Zones.

[HRZ-NI-101] The number of ZIPs between any two Zones should be limited.

Rationale: Limiting the number of ZIPs reduces the management burden and limits the introduction of security vulnerabilities due to operating and configuration errors. The number of ZIPs should be determined by the geographic distribution of the network, network traffic patterns, and the availability needs of supported applications.

[HRZ-NI-102] All network paths destined for, or originating from a Public Zone (e.g., Internet), should pass through a PAZ and an RZ or an OZ. That is, the HRZ should not have direct network connections to a Public Zone or to a PAZ.

[HRZ-NI-103] All HRZ components should support the attachment of network-based intrusion sensors (e.g., monitors). The attachment points should enable a complete view of all traffic.

[HRZ-NI-104] HRZ nodes should not be connected, either simultaneously or periodically, to another Zone. (HRZ nodes include, but are not limited to, laptops, printers, gateways, switches, routers, and computers.) Any exceptions to this requirement should be approved by the Network Security Zone Authority.

Note: It is recognized that departments may not have dedicated test equipment for each Zone, therefore exceptions may be required to allow test equipment to connect periodically to multiple Zones.

[HRZ-NI-105] To protect the HRZ from interference and tampering by untrusted subjects, the HRZ should isolate its internal network from any other network infrastructure. That is, the HRZ should not share its infrastructure, at any layer, with any other Zone or Internetwork component.

[HRZ-NI-106] The Internetwork should be a logically separate network. It should maintain traffic interfaces only with the:

a. ZIPs in the HRZ; and

b. HRZ End-Systems.

[HRZ-NI-107] Wireless access to an HRZ should be permitted only with securely configured and closely monitored wireless devices, where the risk is deemed acceptable. It should be assumed that a sophisticated attacker could intercept wireless traffic.

D.4.2 Traffic Control Requirements

D.4.2.1 Common Traffic Control Requirements

[HRZ-TC-100] If an HRZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the HRZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement.

[HRZ-TC-101] HRZ management traffic, other than traffic related solely to device status, should be segregated from operational traffic.

Note: Segregation may be either virtual or physical. That is, segregation may be achieved through encryption, network access controls, or physical separation.

[HRZ-TC-102] The HRZ should be capable of responding quickly to heightened security levels in case of emergency and increased threat, when and how authorized to do so. (Personnel should be aware, trained and authorized to initiate such a response.) For example, the HRZ should possess the capability to improve the network security posture by increasing the level of security measures such as:

a. filtering at each ZIP;

b. active and/or passive monitoring;

c. protection to ensure the continuous delivery of critical services, including the capability to reconfigure or block non-essential services if required; and

d. auditing.

Note: Implementation of such measures should be carefully tested to ensure that these capabilities could not be exploited to cause a denial of service.

[HRZ-TC-103] Each ZIP should authenticate the Boundary Interfaces of the ZIPs to which it connects. This authentication may be achieved through physical control over the media between the Boundary Interfaces.

D.4.2.2 Internetwork Traffic Control Requirements

[HRZ-TC-104] The Internetwork should provide an access control service capable of enforcing access control requirements between Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[HRZ-TC-105] The HRZ Network Security Zone Authority should define requirements for an HRZ Internetwork access control service based on the following principles:

a. the access control policy should be constructed to deny all traffic that is not explicitly permitted;

b. the access control policy should support Community of Interest separation (i.e., where network traffic is divided into natural communities of interests, the access control policy should enforce these natural traffic flows);

c. the access control policy should limit available network paths to vulnerable or sensitive End-Systems (e.g., test and development sub-networks and application servers supporting public applications);

d. the access control policy should be configured to limit available network paths for End-Systems accessible by extranets;

e. if the HRZ Network Security Zone Authority permits connection to the HRZ by remote access hosts with operating systems that do not provide separation of user and administrator roles, then the access control policy should be configured to limit access to other End-Systems by remote access hosts; and

f. if the Internetwork provides more than one class of service, the access control policy should support isolation between classes of service.

Rationale: Internal access controls contain intrusions and the spread of malware. Internal access controls also support the detection of malicious behaviour (e.g., router logs will often show an increase in access failures.). However, the HRZ is intended to be a controlled network environment and access controls should be designed to allow all natural (within the HRZ) traffic flows.

[HRZ-TC-106] If the HRZ supports more than one class of service, the Internetwork should implement mechanisms to ensure non-interference between classes of service.

Rationale: If classes of service other than "best effort" are required by End-Systems, simple bandwidth consumption within one class of service could result in denial of service within another class of service unless controls are put in place to limit interference. Such controls are often available within mechanisms that implement class of service and quality of service.

[HRZ-TC-107] The Internetwork should employ an addressing model that facilitates detection and diagnosis of malicious traffic.

Rationale: The choice of address model can have a significant impact on the ability to detect and isolate network problems in general and security problems in particular. It is good network design practice to facilitate access controls to isolate shared resources, and to segregate by location (e.g., remote access and extranet clients) and organization.

[HRZ-TC-108] The HRZ should support Internet Protocol Security (IPSec) traffic between any pair of Edge Interfaces.

Rationale: The HRZ should permit End-System managers the option of implementing network-layer data protection. IPSec traversal of network address translation and firewall implementations may affect interoperability of some networks and applications.

D.4.2.3 Operations Zone (OZ) Zone Interface Point (ZIP)

[HRZ-TC-109] The OZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[HRZ-TC-110] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this ZIP;

b. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses; and

c. the access controls should support interdepartmental applications.

Rationale: In communications between two internal Zones, each Zone depends on the other to apply controls on ingress. Consequently, few controls are required on egress.

[HRZ-TC-111] OZ ZIPs should implement network-layer and upper-layer controls to protect HRZ hosts from traffic originating from OZs and to protect OZs in the event that malicious traffic originates from within the HRZ.

[HRZ-TC-112] An intrusion detection capability should be implemented at the OZ ZIP. The capability should be configured to provide an alarm if traffic contains malware or malicious behaviour.

Rationale: Access controls, together with the controls applied in the OZ, should eliminate most attacks via the ZIP. However, these safeguards will not provide complete protection. The resources required to manage this capability should be modest since the frequency of alarms at this interface should be low.

[HRZ-TC-113] If justified by a TRA, a stateful filter should be applied at the ZIP to ensure that incoming traffic is restricted to authorized protocols.

[HRZ-TC-114] If client e-mail functionality is deployed within the HRZ, an e-mail gateway should be employed at the OZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[37].

[37] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

Note: The e-mail gateway is not needed if the HRZ is simply used to provide an e-mail server.

Rationale: E-mail is the primary vector for the spread of malware.

[HRZ-TC-115] If justified by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the OZ ZIP.

[HRZ-TC-116] If the OZ ZIP interface to common infrastructure shares traffic control functionality with the common infrastructure provider, then the service level agreement should include the baseline requirements for both sides of the interface.

D.4.2.4 Restricted Zone (RZ) Zone Interface Point (ZIP)

[HRZ-TC-117] The RZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces based on network-layer source, network-layer destination, transport protocol, and transport-layer service interface.

[HRZ-TC-118] The Network Security Zone Authority should define an access control policy to be enforced by the access control service based on the following principles:

a. for incoming traffic (i.e., traffic with an external source address), the access controls should be configured to deny all traffic that is not explicitly permitted. Incoming traffic should be limited to accessing network resources that provide service to other Zones connected to this ZIP;

b. the access controls should permit outgoing IPSec traffic and should permit incoming IPSec traffic to designated addresses; and

c. the access controls should support interdepartmental applications.

Rationale: In communications between two internal Zones, each Zone depends on the other to apply controls on ingress. Consequently, few controls are required on egress.

[HRZ-TC-119] RZ ZIPs should implement network-layer and upper-layer controls to protect HRZ hosts from traffic originating from RZs and to protect RZs in the event that malicious traffic originates from within the HRZ.

[HRZ-TC-120] If client e-mail functionality is deployed within the HRZ, an e-mail gateway should be employed at the RZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[38].

[HRZ-TC-121] An intrusion detection capability should be implemented at the RZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

Rationale: Please see [HRZ-TC-112] Rationale.

[38] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[HRZ-TC-122] If warranted by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the RZ ZIP.

D.4.2.5 Highly Restricted Zone (HRZ) Zone Interface Point (ZIP)

[HRZ-TC-123] If justified by a TRA, the HRZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces.

[HRZ-TC-124] The Network Security Zone Authority should define an access control policy that reflects the access-control-related risks identified by the TRA.

[HRZ-TC-125] If client e-mail functionality is deployed within the HRZ, an e-mail gateway should be employed at the HRZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[39].

[HRZ-TC-126] An intrusion detection capability should be implemented at the HRZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

Rationale: Please see [HRZ-TC-112] Rationale.

[HRZ-TC-127] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

[HRZ-TC-128] If warranted by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the HRZ ZIP.

D.4.2.6 Special Access Zone (SAZ) Zone Interface Point (ZIP)

Note: Only an HRZ may connect to a Special Access Zone (SAZ)

[HRZ-TC-129] If justified by a TRA, the SAZ ZIP should provide an access control service capable of enforcing an arbitrary access control policy between external interfaces and internal Edge Interfaces.

[HRZ-TC-130] The Network Security Zone Authority should define an access control policy that reflects the access-control-related risks identified by the threat and risk assessment.

[HRZ-TC-131] If client e-mail functionality is deployed within the HRZ, an e-mail gateway should be employed at the SAZ ZIP. This gateway should implement malware filters on all incoming and outgoing e-mail[40].

Note: The e-mail gateway is not needed if the HRZ is simply used to provide an e-mail server.

[HRZ-TC-132] An intrusion detection capability should be implemented at the SAZ ZIP and configured to provide an alarm if traffic contains malware or malicious behaviour.

[39] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[40] Where end-to-end encryption is used, scanning and filtering must be done at the End-Systems.

[HRZ-TC-133] Audit-relevant traffic control and data flow information should be recorded in the Security Audit log in accordance with the requirements of the Security Audit service.

[HRZ-TC-134] If justified by a TRA or if required by the Network Security Zone Authority to enforce an Internet Use Policy, a content filter should be implemented at the SAZ ZIP.

D.4.3 Network Configuration Requirements

D.4.3.1 Common Network Configuration Requirements

[HRZ-NC-100] The HRZ network configuration should be monitored to detect additions, deletions, or changes to all interfaces within the Internetwork. Unauthorized changes should be reported to the Network Security Zone Authority.

Rationale: Continuous status monitoring is necessary to detect unauthorized changes to the network configuration in a timely manner. Timely detection allows Zone Authorities of impacted Zones to respond to prevent or limit damage from an attack or failure.

[HRZ-NC-101] The HRZ Boundary and Edge Interfaces should be registered with the HRZ Network Security Zone Authority.

[HRZ-NC-102] Each HRZ interface should act in exactly one role: Boundary or Edge Interface.

[HRZ-NC-103] The HRZ Network Security Zone Authority should periodically verify the network topology. The frequency of such verifications should be determined by the Network Security Zone Authority and documented in configuration management procedures for the HRZ.

[HRZ-NC-104] The HRZ Network Security Zone Authority should periodically assess the network configuration for unauthorized external interfaces (e.g., modems and wireless access points (APs)). The frequency of assessments should be determined by the Network Security Zone Authority and documented in configuration management procedures for the HRZ.

Rationale: The presence of unauthorized modems can create vulnerabilities in a well-configured network. These unauthorized modems provide a means to bypass most or all of the security measures in place to stop unauthorized users from accessing a network.

D.4.3.2 Zone Interface Point (ZIP) Network Configuration Requirements

[HRZ-NC-105] HRZ Boundary Interface addresses should be distinct and dedicated. HRZ Boundary Interface addresses should be visible to other GC Zones. HRZ Boundary Interface addresses should not be visible to the Public Zone.

[HRZ-NC-106] HRZ Boundary Interfaces should be assigned addresses upon attachment to the network.

[HRZ-NC-107] A change to an HRZ Boundary Interface address assignment should constitute a configuration change requiring approval by the HRZ Network Security Zone Authority.

Approval may be given in advance to permit dynamic reconfiguration; however, the conditions under which such a change may be effected should be delineated clearly.

D.4.3.3 Internetwork Configuration Requirements

[HRZ-NC-108] The HRZ Network Security Zone Authority should maintain current configuration information for all interfaces within the Internetwork. The configuration information should include:

a. a unique identifier;

b. the status of the interface (active/non-active);

c. the address assignment rules;

d. the current network address;

e. the list of all names/aliases associated with all interfaces within the Internetwork;

f. the current physical-layer interface to which all interfaces within the Internetwork are assigned;

g. the communications security parameters for all interfaces within the Internetwork; and

h. security constraints on the instantiation of each interface within the Internetwork.

[HRZ-NC-109] The following changes to an HRZ should be approved by the HRZ Network Security Zone Authority before implementation:

a. addition or deletion of an interface within the Internetwork;

b. a change to the address assignment rules for any interface within the Internetwork;

c. a change to the communications security parameters of any interface within the Internetwork; and

d. a change to the security constraints on the instantiation of any interface within the Internetwork.

Rationale: These changes may affect the implementation of security measures or the configuration of intrusion detection capabilities.

[HRZ-NC-110] Edge Interfaces should establish security associations with other Edge Interfaces and all communications should be authenticated (either explicitly or implicitly) within the context of these security associations. The security associations permitted should be determined by traffic control requirements.

Note: The type and strength of authentication are implementation dependent. The goal is to prevent an intruder attaching a Network-layer entity in the core and masquerading as an Edge Interface.

[HRZ-NC-111] Internetwork Edge Interfaces should be authenticated to each other through one of the following methods:

a. cryptographic authentication mechanisms applied at the network layer; or

b. physical controls over the Edge Interfaces and over all media connecting these interfaces.

Rationale: Because the Internetwork is a significant component of an internal GC Zone, it is extremely important that hostile entities be excluded from masquerading as an Edge Interface.

[HRZ-NC-112] The service level agreement should require the Network Service Provider to control changes to all Internetwork interfaces under Provider's control and to report to the HRZ Network Security Zone Authority any changes that impact the security association between Edge Interfaces.

[HRZ-NC-113] The service level agreement should require the Network Service Provider to provide evidence that the security controls used to enforce the security within the Internetwork Core are effective and to report all security incidents that could impact the HRZ to the HRZ Network Security Zone Authority. The Network Service Provider should also provide the HRZ Network Security Zone Authority with the capability to verify the effectiveness of the controls on at least a quarterly basis.

D.4.3.4 Wireless Network Configuration Requirements

Note: While the HRZ infrastructure may support a variety of physical media including wireless APs, it should be assumed that a sophisticated attacker could intercept wireless traffic.

[HRZ-NC-114] Addresses provided to End-Systems that use wireless/radio frequency data link layers should be assigned dynamically from a segregated address pool (i.e., an assigned range of addresses).

Rationale: Address assignment from a distinct pool of addresses permits access control by Community of Interest. Dynamic address assignment permits address reuse. Please also see [HRZ-OBJ-106] Rationale.

[HRZ-NC-115] Wireless hosts should be authenticated to the HRZ using strong peer-entity and data origin authentication before the establishment of a connection to the HRZ.

Rationale: Authentication of the host provides confirmation that the connection being processed is coming from a valid source. Persistent authentication would be necessary to permit roaming between APs.

[HRZ-NC-116] Peer-entity and data origin authentication at the data link layer should be used to establish connections between wireless APs and wireless hosts.

Rationale: Authentication of the host provides confirmation that the connection being processed is coming from a valid End-System.

[HRZ-NC-117] The Wireless APs should be placed in locations that optimize coverage and minimize exposure to eavesdropping.

Rationale: The nature of the wireless medium makes it practically impossible to confine the radio signals to a controlled location. Unless TEMPEST shielding is used or adequate physical zoning is established, the radiated signals are subject to clandestine interception and exploitation. Finally, eavesdroppers may use high-gain antennas, which permit interception of wireless signals beyond the limit of a manufacturer's specification of signal distance.

[HRZ-NC-118] The wireless intrusion detection policy should be integrated with facility access policies.

Rationale: The source of a wireless network intrusion may be within an organization's controlled physical space. If so, a suitable response may be a physical response to locate the source and remove it from the facility.

D.4.3.5 End-System Network Configuration Requirements

[HRZ-NC-119] End-Systems should maintain the integrity of network interfaces with GC Zones while connected to an HRZ; therefore, dual-homing, tunnel-splitting, or other shared network paths with the Public Zone by HRZ End-Systems should not be permitted.

Rationale: Simultaneous connection of an Ethernet interface to an HRZ and an active modem connection to the Internet would permit intrusion to the HRZ. Similarly, having an SVPN tunnel split between an HRZ and the Internet would permit intrusion.

[HRZ-NC-120] If remote management is allowed, an HRZ should allow only authorized administrators to remotely manage HRZ nodes from a GC-controlled Zone or from a Restricted Extranet Zone (see Section 4.2.8). The access should be controlled and protected by using the following methods:

a. strong authentication; and

b. restricting access by Internet Protocol address, port, and protocol.

[HRZ-NC-121] Wireless devices should be configured to limit or suppress broadcasting of their device identifiers (such as IEEE 802.11 Service Set Identifiers).

D.4.4 Host Configuration Requirements

D.4.4.1 Common Host Configuration Requirements

[HRZ-HC-100] All nodes in the HRZ should ensure the maximum protection against intrusion. This includes, but is not limited to:

a. strictly limiting the number of operating system accounts and ensuring that the security principle of "*least privilege*" is strictly applied to each account;

b. ensuring that the most appropriate authentication is used for all accounts depending on departmental business requirements and risk assessment;

c. disabling all unnecessary services (i.e., the software load configuration is the minimum necessary to provide required functions); and

d. ensuring only authorized administrators are given user accounts for perimeter/boundary nodes (e.g. for DMZ access devices, routers, network intrusion systems).

[HRZ-HC-101] The HRZ Network Security Zone Authority should maintain a host configuration policy consistent with applicable baseline security requirements, standards, and guidance. This policy should apply to all hosts attached to the Zone.

Note: From a Zone perspective, the host configuration policy should be limited to specifying the constraints on the software load and the maintenance procedures required to prevent a sophisticated attacker from compromising a host and using that host to attack network assets. The policy should also reduce susceptibility to compromise from all other sources. The primary focus should be the control of malware as this is the easiest and most prevalent method of attack. Note that hosts may be subject to additional platform security requirements to protect applications and data; however, these are outside the scope of Zone requirements. These additional platform security requirements will depend on the type of host (e.g., workstation, application server).

[HRZ-HC-102] The host configuration policy should contain:

a. a specification of prohibited and mandated software and hardware configurations such as not allowing active modems, “sniffer” software, and remote access software permitting control of an HRZ host, but requiring the installation of current anti-virus software;

b. minimum maintenance procedures for all software components (e.g., configuration management procedures for hardware and software, emergency patch procedures, technician training, etc.); and

c. specific maintenance procedures for software that provides client access to Internet-based resources and for software that provides back-end services to public clients (e.g., mail service).

Rationale: The HRZ and the Internetwork infrastructure should limit direct intrusions (i.e., those not using malware) to sophisticated attackers. Host configuration controls are aimed at further reducing the susceptibility to such intrusions. In most cases, an HRZ will be a small network installation with specific business needs and narrowly distributed authority over End-Systems. A minimum practical level of discipline over the End-System configuration is necessary to reduce susceptibility to intrusion via End-Systems. The greatest attention should be placed on any software that has the potential to interact with public networks.

[HRZ-HC-103] The HRZ Network Security Zone Authority should ensure that End-System managers are aware of this host configuration policy and that they ensure the policy is enforced.

[HRZ-HC-104] Regular network vulnerability assessments (VAs) of all hosts should be conducted to assess trends in the effectiveness of the host configuration policy. The frequency of such VAs must be sufficient to support trend analysis. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.

Rationale: Network VAs involve port scans possibly with some software fingerprinting. The goal is to provide the Network Security Zone Authority with a complete picture of the vulnerability of end systems and compliance to the host configuration policy. This approach has been chosen to balance a liberal approach to host configuration control. A significant change in the results may indicate a widespread problem or may be evidence that other measures are required.

[HRZ-HC-105] All hosts should invoke controls that implement continuous protection against malware at start-up. The Network Security Zone Authority should approve any exceptions to this requirement.

Rationale: Malware is the easiest and most likely vehicle for an external attacker to gain control of an End-System to attack HRZ assets. Controls are placed in the HRZ to reduce the amount of malware that reaches the End-System. However, no network filter is completely effective and malware protection is required on the hosts within the End-Systems. Exceptions may be required for those few hosts for which it may be prohibitively expensive or impossible to meet the requirement (e.g., mainframes, super computers).

[HRZ-HC-106] All hosts that provide applications to permit client access to public resources (e.g., Internet web browser and e-mail clients) should:

a. employ an operating system that provides separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege); and

b. be configured to operate any applications that provide access to public resources in user mode.

Rationale: If the platform is able to enforce configuration controls by restricting changes to administrators, then many intrusion scenarios can be thwarted. Most new commercial operating systems (e.g., Windows 2000, Windows NT, Windows XP, Apple OS X, and all UNIX/Linux variants) provide this capability.

[HRZ-HC-107] If an HRZ has End-Systems that process Protected C or classified information, then all ZIPs and any shared End-Systems in the HRZ should not illicitly route traffic between Zones.

Note: Firewalls are not generally approved as ZIPs for this requirement; only guards or data diodes meet the requirement.

[HRZ-HC-108] A comprehensive process for managing software updates[41] should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software that exists on HRZ nodes.

[HRZ-HC-109] Host-based intrusion detection sensors should be placed on all critical hosts.

[HRZ-HC-110] HRZ nodes should be capable of generating and maintaining audit log records as required by the Security Audit service.

[HRZ-HC-111] HRZ nodes should ensure that locally stored Security Audit log records are accessible to authorized Security Audit administrators, as required by the Security Audit service.

[HRZ-HC-112] HRZ nodes should be capable of using a common time source.

[HRZ-HC-113] Regular backups of system files and system configuration parameters should be performed for every node contained in the HRZ. Frequency and retention period of backups should be consistent with business needs.

[HRZ-HC-114] The failure of an HRZ node should not result in the compromise of its resources or those of any connected network.

[HRZ-HC-115] All HRZ nodes should be within an area that meets as a minimum the physical security requirements of a physical High Security Zone (see reference [26]).

[HRZ-HC-116] HRZ nodes should enforce the separation of roles between node configuration management and node operation management.

[HRZ-HC-117] Audit log files should not be overwritten before they have been backed up to secured storage.

[HRZ-HC-118] HRZ extranet connectivity should be only for remote management and should be provided only under highly controlled circumstances.

[HRZ-HC-119] Any End-System should have a certification and accreditation review before attachment to an Edge Interface is permitted.

Rationale: End-Systems may contain private networks between their components, may have traffic controls, and may have unique network configurations that could compromise the infrastructure of the HRZ.

[HRZ-HC-120] Operating systems for all nodes should be hardened based on documented best practices.

[HRZ-HC-121] Wireless access within an HRZ should only be permitted with a securely configured and closely monitored wireless device, where the risk is deemed acceptable. It should be assumed that a sophisticated attacker could intercept traffic.

[41] Refer to NIST Special Publication 800-40 for an example process.

D.4.4.2 Shared End-System Configuration Requirements

[HRZ-HC-122] A shared End-System, whether shared permanently or periodically, is subject to the following:

a. it should employ an operating system which supports the separation of users and administrators (i.e. enforces Principles of Separation of Duties and Least Privilege);

b. changes to network configuration should require administrative privileges;

c. the End-System configuration and procedures for maintaining that configuration should be approved by the HRZ Network Security Zone Authority;

d. the End-System should be subject to regular VAs, the frequency of which should be determined by the Network Security Zone Authority and documented in VA procedures for the Zone. Results of all VAs should be managed within the framework of Continuous Risk Management, and as such should provide feedback to the TRA process.; and

e. requirements [HRZ-TC-100] and [HRZ-HC-107] (if applicable).

Rationale: Shared End-Systems have the potential to create back doors between Zones. Shared End-Systems are also likely to be relatively few in number, making greater control possible. This vulnerability scan focuses on vulnerabilities associated with routing.

[HRZ-HC-123] If an End-System is shared periodically (e.g., laptop) with a Public Zone, then:

a. the End-System should include a personal firewall; and

b. the End-System should include a configuration integrity mechanism capable of identifying changes to the configuration and notifying the End-System administrator.

[HRZ-HC-124] rescinded.

[HRZ-HC-125] Each HRZ node should be subject to regular configuration audits. The frequency of such audits should be determined by the Network Security Zone Authority and documented in configuration management procedures for the HRZ. The frequency of configuration audits should be sufficient to identify configuration errors. The configuration audit includes but is not limited to:

a. verification of node configuration against network topology design;

b. verification of hardware devices and physical interfaces;

c. verification of traffic control configuration, including permissions and access controls; and

d. verification of permitted software load and permitted functions.

Rationale: Configuration errors are a significant source of exploitable vulnerabilities. Regular configuration audits ensure that the window of exposure from configuration errors is limited.

D.4.4.3 Network Node Configuration Requirements

[HRZ-HC-126] Operating systems for all nodes (i.e., ZIP boundary devices and for Internetwork edge/core devices) should be hardened based on documented best practices.

[HRZ-HC-127] SVPN products, if used, should be validated to Federal Information Processing Standard (FIPS) 140-1 or FIPS 140-2 at a minimum of Security Level 2 through the Cryptographic Module Validation Program (CMVP).

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and the Cryptographic Endorsement Program (CEP), each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the Cryptographic Algorithm Validation Program (CAVP).

[HRZ-HC-128] Internetwork devices and ZIP devices should be physically secured to limit access to only those authorized personnel with an ongoing need to access the equipment, in accordance with the Principles of Least Privilege and Need-to-Know.

Rationale: Restricted access to devices with Edge Interfaces reduces the opportunity for network reconfiguration or introduction of unauthorized Edge Interfaces. A Network Service Provider can restrict access with lockable cages. Devices located at GC premises can be located in physical security zones.

D.4.4.4 Complex End-System Configuration Requirements

[HRZ-HC-129] A complex End-System should have a certification and accreditation review before attachment to an Edge Interface is permitted.

Rationale: Complex End-Systems may contain private networks between their components, may have traffic controls, and may have unique network configurations that could compromise the infrastructure of the HRZ.

D.4.5 Data Protection Requirements

[HRZ-DP-100] The Internetwork should be capable of supporting SVPN data traffic connections between Edge Interfaces.

Rationale: this provides the capability to protect sensitive data transported through the Internetwork between sites or enclaves.

[HRZ-DP-101] The HRZ should be capable of supporting SVPN data traffic connections between ZIPs.

[HRZ-DP-102] The HRZ should be capable of supporting upper-layer security protocols (e.g., Secure Sockets Layer/Transport Layer Security, Simple Public-Key Mechanism, Secure Multimedia Internet Mail Extensions) used by applications.

Rationale: This provides the capability to protect sensitive data for session traffic that is being transported between HRZ End-Systems or to End-Systems in other Zones.

[HRZ-DP-103] Although traffic at all sensitivity levels may be handled by the HRZ, data protection measures are required depending on the Statement of Sensitivity and the results of a TRA. In addition, data protection services may be applied at either the network layer or higher layers depending on the implementation requirements. Protected C and classified information will require additional controls and data protection mechanisms that are not specified in this Guideline.

[HRZ-DP-104] Where encryption or digital signature is required, products (whether software, firmware or hardware) must incorporate a CSEC-approved algorithm and CSEC-approved key management processes, such as those products validated to FIPS 140-1 and FIPS 140-2 by the CSEC through the CMVP and/or evaluated under the CSEC's CEP. In addition, Protected C and Classified data will require additional controls and data protection mechanisms not specified in this Guideline.

Note: Cryptographic algorithm validation is a prerequisite to the CMVP. Under both the CMVP and CEP, each implementation of a CSEC-approved algorithm used in a cryptographic module (i.e. product) must be (or must have been) validated or certified under a recognized program such as the CAVP which may be suitable in general for up to and including Protected B data. Contact CSEC IT Security Client Services for solutions for Protected C and Classified data. See Information Technology Security Alert ITSA-11C (reference [20]) for a list of CSEC-approved algorithms.

[HRZ-DP-105] To protect against disclosure and modification of sensitive data:

a. data encryption should be employed between HRZ End-Systems and End-Systems in other Zones when highly sensitive data is being transmitted; and

b. data encryption should be employed between GC-owned Edge Interfaces when particularly sensitive or highly sensitive data is being transmitted over portions of the Internetwork that have been outsourced to a Network Service Provider.

[HRZ-DP-106] If an HRZ has End-Systems that process Protected C or classified information, then it is subject to Traffic Control requirement [HRZ-TC-100] and Host Configuration requirement [HRZ-HC-107].

Annex E Implementation Guidance and Examples

E.1 Target Enterprise Architecture

The target Enterprise Architecture is under consideration. This Annex describes how Zones may be implemented to provide a secure Government of Canada (GC)-wide network infrastructure. At issue is whether the GC must use the Secure Channel Network (SCNet) and whether to implement the Public Access Zone (PAZ) as a common service, shared service, or unique service as described below:

a. Common Service – functionality is provided centrally for all GC departments, and departments requiring the functionality are mandated to use the common facilities;

b. Unique Service – each department is responsible for implementing its own infrastructure and creating its own support structure to provide the functionality. The GC-wide baseline security requirements would exist and the departments would be responsible for meeting those standards; and

c. Shared Service – a hybrid of the *Common* and *Unique* options where some departments opt to receive functionality provided in common to all departments while other departments are responsible for providing the functionality themselves. In practice, this would be the same as the unique option but some departments would outsource the functionality to a common service provider. This option is a candidate for further consideration if there are apparent economies of scale. However, there is concern that the *Common Service* option would not be accepted GC-wide.

It is possible that some PAZ functionality (e.g., service delivery applications and some common support functions) may be implemented as a common service, while other PAZ functionality (e.g., Employee Web Access and e-mail) is implemented as a shared service, and the remainder (e.g., Remote Access and Extranet Access) implemented exclusively by a department.

Figure 17 illustrates a possible future state for the GC network infrastructure. Boxes with the magnifying glass icon represent systems that function as filters such as firewalls.

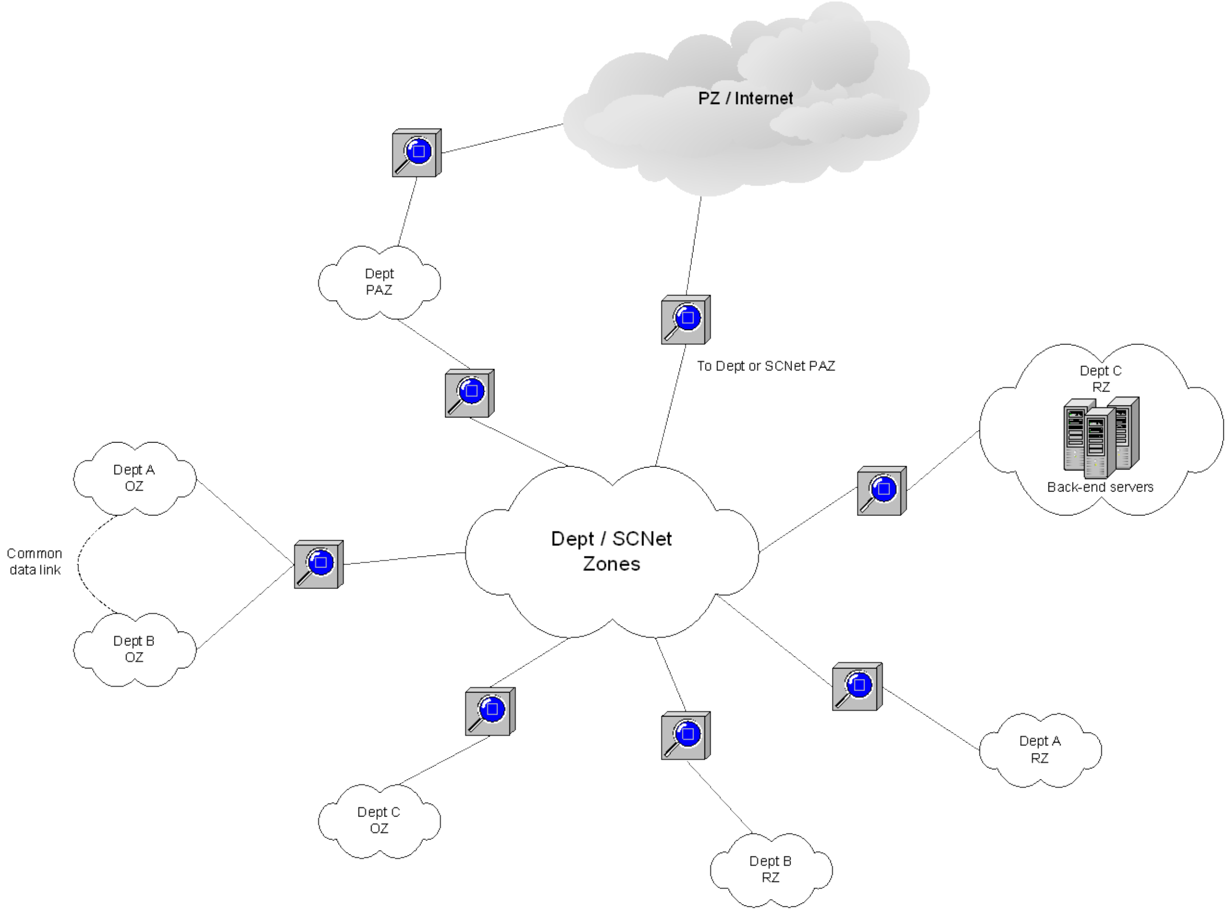


Figure 17 – Realizing Network Security Zones

In this diagram, the GC common backbone is the SCNet and has been implemented as one of three Zones: the PAZ, Operations Zone (OZ), or Restricted Zone (RZ). All departments access the Public Zone (e.g., Internet) through the SCNet PAZ or using their own departmental PAZs.

Department A implements two Zones: an OZ and an RZ. Each of these Zones has a single Point of Presence (PoP) on the SCNet Internetwork as a filtered connection to the backbone. This may be comprised of devices such as screening routers, firewalls, or anything capable of filtering communications between Zones.

Department B also implements an OZ and an RZ. Departments A and B share data link- and physical-layer infrastructure between OZs installed in a building.

Department C implements an OZ. Department C also implements an RZ with back-end servers.

Figure 18 illustrates the possible connectivity of public and mobile users. Boxes with the magnifying glass icon represent systems that function as filters such as firewalls. Dotted lines represent the logical path between users and Zones.

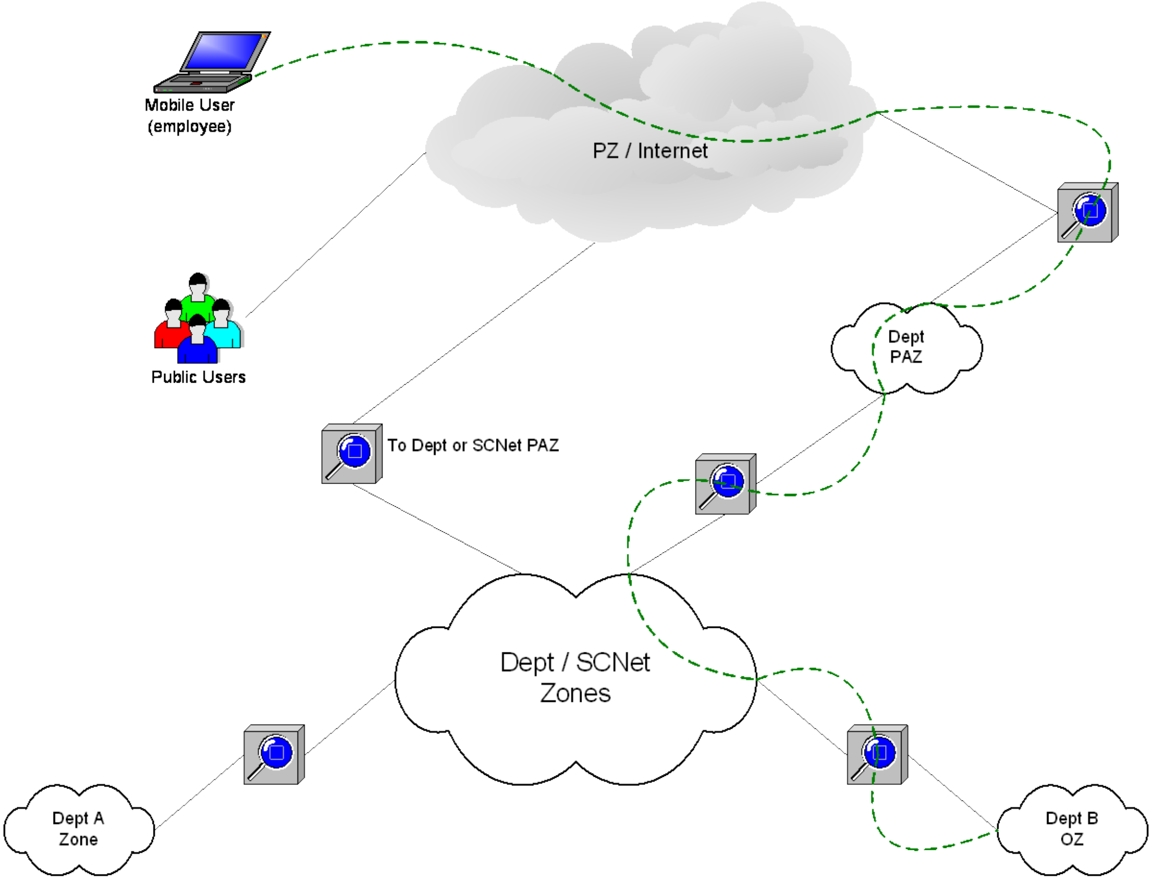


Figure 18 – Public and Mobile Users

In this diagram, public users have limited connectivity to a department via the Internet / PZ. In comparison, authorized mobile users and employees are capable of accessing departmental Zones from the PZ to internal departmental Zones.

Figure 19 illustrates the possible connectivity of extranets and trusted partner extranets. Boxes with the magnifying glass icon represent systems that function as filters such as firewalls. Dotted lines represent the logical path between extranet users and Zones.

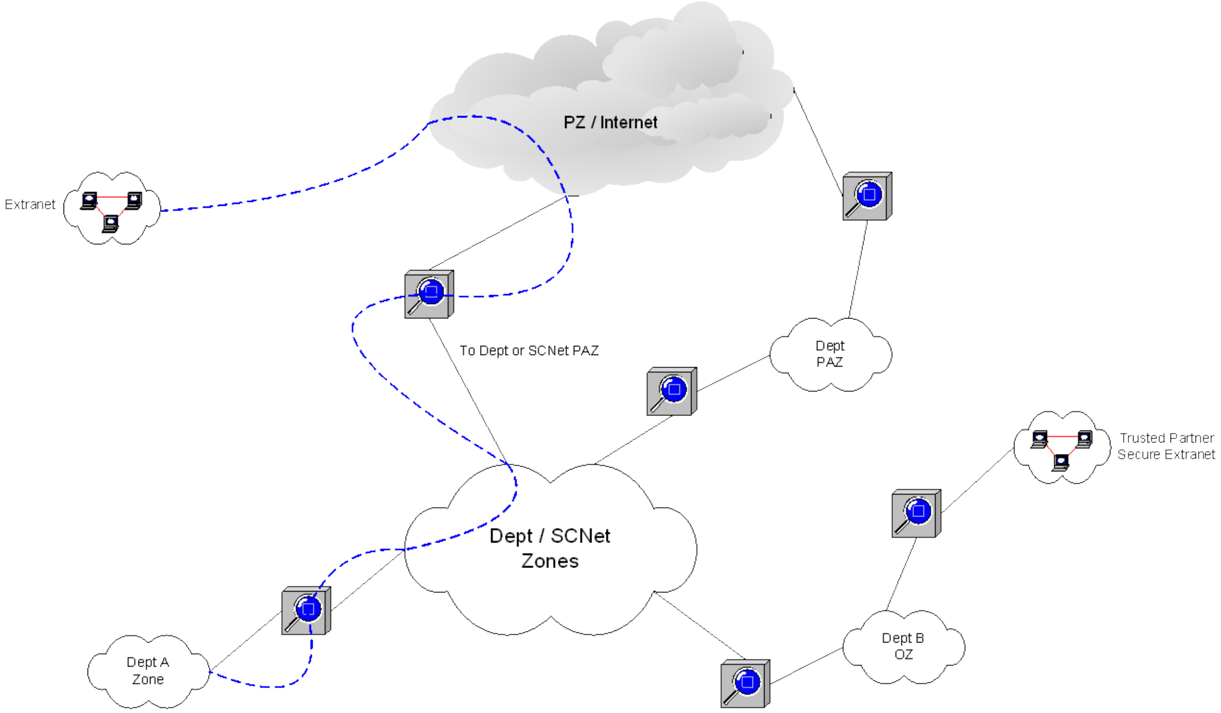


Figure 19 – Extranets

In this diagram, non-trusted extranets are granted connectivity to a department via the Internet / PZ and PAZ. In comparison, trusted partner extranets do not necessarily connect through a PAZ when accessing a departmental Zone.

The following sections describe examples of options a department may consider to use. While these examples do adhere to the principles presented in ITSG-22 and the preceding Annexes, they DO NOT represent mandatory implementation recommendations. The purpose of these examples is to provide implementation guidance only.

E.2 Implementation Options for a Public Access Zone (PAZ) Instance

There are various options for the implementation of a PAZ. In this Annex, an example is presented to illustrate how a PAZ could be implemented in various configurations and combinations. The particular choice of implementation will depend on factors such as the size of a department and whether or not the PAZ is department-specific or shared with one or more other departments and whether there are common services offered on behalf of all departments. Please note that this annex is illustrative only and the examples should not be taken as definitive statements of PAZ implementations.

E.2.1 Example 1: Enterprise-scale Public Access Zone (PAZ)

In this example, there is a Public Zone separated from the departmental network by a Demilitarized Zone (DMZ) located between screening routers (Figure 20). The screening routers constitute the Public and Internal Zone Interface Points (ZIPs) as described in Sections A.2.6 and A.2.7. The EANs and IANs consist of the systems connecting the screening routers to the filtering devices. Separate External Access Network (EAN)/DMZ and Internal Access Network (IAN)/DMZ Boundary systems (i.e., firewalls or Intrusion Prevention Systems) are recommended in an enterprise-scale architecture, however, these functions could be provided by a single boundary system or platform, such as those performing Unified Threat Management (UTM). A UTM system is designed to protect systems and users from blended threats while reducing complexity. Although a UTM system can diminish the complexity and cost of managing multiple security systems, the functionality and capability provided by such dedicated systems (routers, firewalls, content filters) may also be reduced in a UTM product. The cost for UTMs capable of the same level of functionality of those dedicated systems may remain competitive. All factors should be considered through a cost-benefit analysis before the procurement of any product type.

Figure 20 illustrates an example of a PAZ implementation interfacing with a Public Zone and an OZ infrastructure. In this diagram, boxes represent End-Systems and service functions. Those pale green boxes represent optional items as to their presence and location. Such items may be substantiated by a TRA.

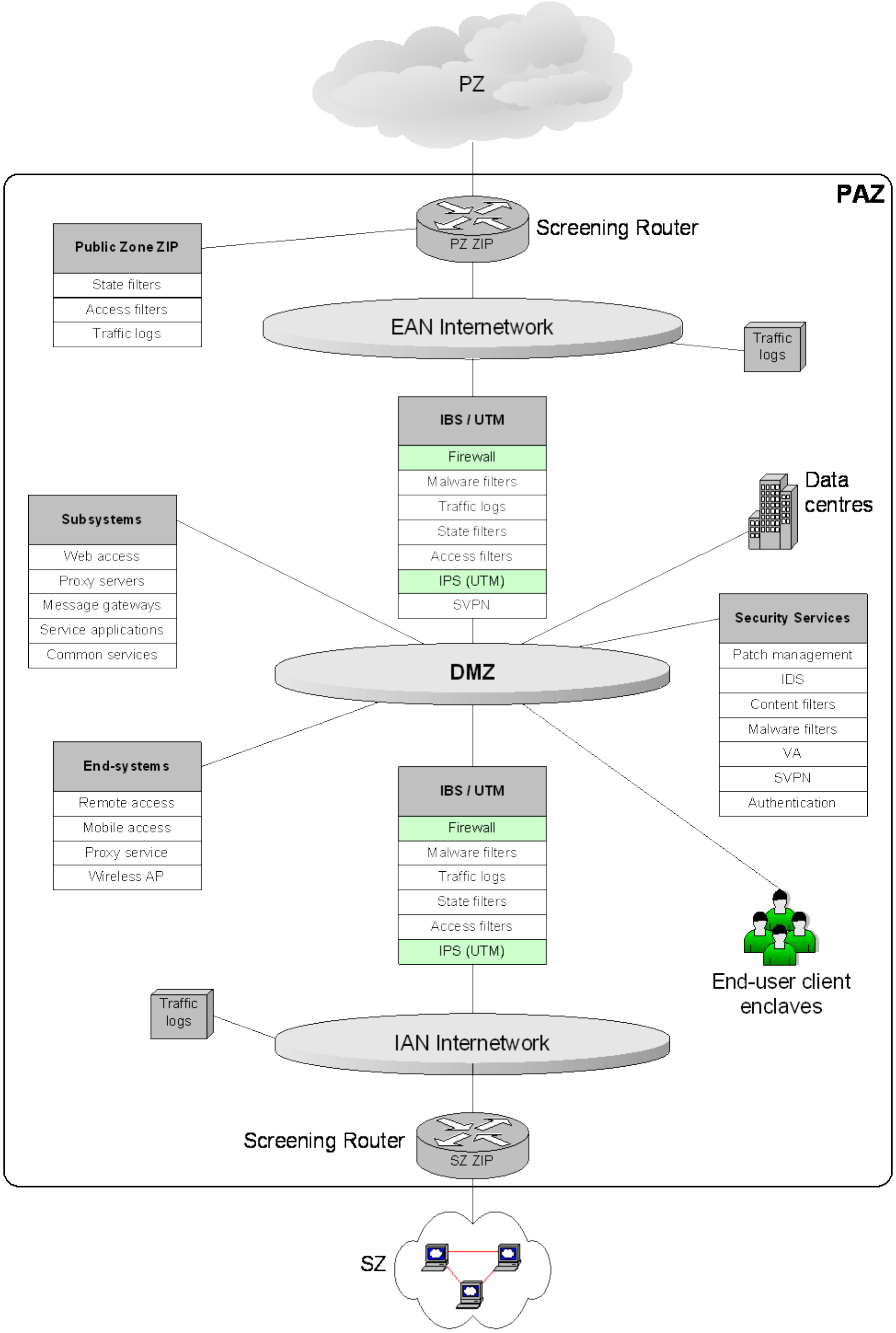


Figure 20 – Implementation of an Enterprise-scale PAZ

The Public Zone ZIP can consist of multiple screening routers for redundancy and filtering access from the Public Zone or Internet service providers. The Internal Zone ZIP is (in this example) a screening router that provides the interface to the internal departmental network infrastructure. All the screening (access) routers perform state filtering, access filtering, network address translation (NAT), and port address translation (PAT).

The EAN/DMZ and IAN/DMZ Boundary Systems may consist of firewall clusters (for larger departments) at both the internal and external borders of the DMZ to provide redundancy and ensure segregation of traffic.

Employee access to web resources is through dedicated application proxies in the DMZ. The IAN/DMZ Boundary Systems (e.g., firewalls, UTM products) provide ingress filtering to protect the departmental network from a compromised application proxy.

The application servers in the DMZ communicate with back-end servers (depicted in Figure 22) on the departmental network in an OZ.

Traffic is strictly segregated. Functional traffic is segregated to ensure failures are isolated and management traffic is segregated from operational traffic. External applications (e.g. for e-government services) are protected from other network traffic. Management interfaces are not accessible from the EAN.

In the case of a large-scale PAZ for multiple departments, support for common applications via data centres may be located between the EAN and IAN. Each data centre implements one or more common services (web access, e-mail, remote/mobile access, extranets, common applications and collaborative services). The PAZ can contain a number of these data centres to ensure redundancy and appropriate load balancing. Traffic between the Public Zone and departments is mediated by the data centres, which also act as the DMZ.

On the EAN side, there may be multiple Public Zone ZIPs in the form of packet-filtering routers. Similarly, packet-filtering routers may be used for the IAN to provide the DMZ Access Device function at the IAN/DMZ boundary. NAT and PAT are performed at the external and internal PoP routers along with access control based on source, destination, protocol, service, and transport-layer header attributes.

Traffic from the external PoP routers (providing the external Boundary Device function) is distributed via a private EAN to the data centres. Similarly, a private IAN distributes traffic between internal interface points and the data centres.

The internal network interface points (i.e., the internal PoP routers providing the Boundary Device function for internal GC Zones) provide connections to departmental OZs and/or RZs.

In the larger departments, the data centres would typically be implemented with redundant routers and interior and exterior DMZ Access Devices (e.g., firewalls, UTM) that support multiple DMZ segments. The DMZ Access Devices (e.g., firewalls) perform address translation and stateful inspection[42], with policy specific to a given set of services. Dedicated application

[42] Stateful inspection can also refer to state filters and TCP state filtering.

proxy and gateway services are attached to the DMZs. It is recommended that management traffic be separated from operational traffic.

E.2.2 Example 2: Small-scale PAZ

This example is a variation of Example 1, such that it simplifies the depiction of a PAZ that reflects the use of a single boundary system (vice the two boundary/DMZ approach). A department may choose this single boundary system to be a UTM system.

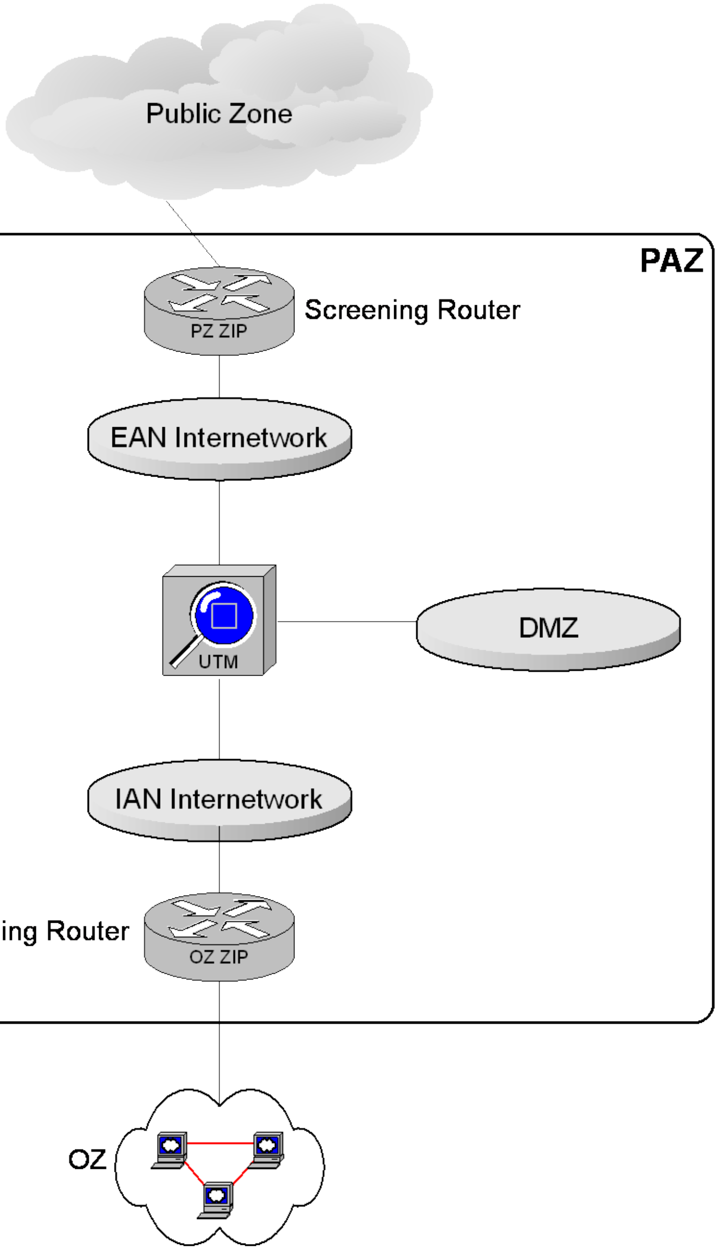


Figure 21 – Implementation of a Small-scale PAZ

Figure 21 illustrates an example of a PAZ implementation interfacing with a Public Zone and an OZ infrastructure. In this diagram, the PAZ is interfacing with an OZ; however, the PAZ can also interface with an RZ.

E.3 Implementation Options for an Operations Zone Instance

As one moves from the PAZ to an OZ, the environment changes from one suited to host proxy services and Internet-based applications (such as e-mail, remote access, and extranet gateways) to one that accommodates end-user systems and workgroup servers suitable for processing sensitive information.

E.3.1 Example 1: Enterprise-scale Operations Zone

The OZ example illustrated in Figure 22 applies for departments that support internally hosted services and a range of on-line services, indirectly.

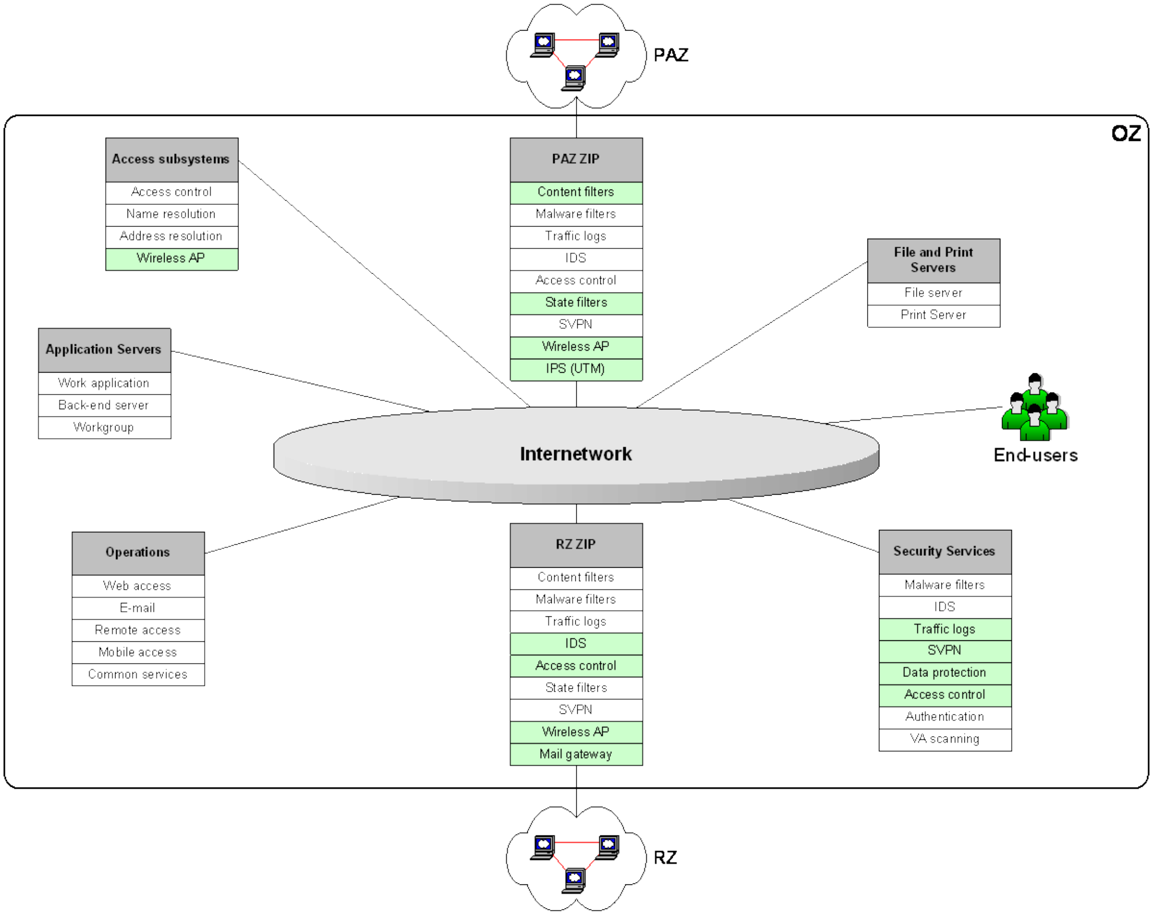


Figure 22 – Implementation of an Enterprise-scale OZ

In this example, there is access to the OZ from the PAZ and an RZ. Each ZIP has an edge router for filtering access to the target OZ. The Internal Zone ZIP (in this case, the RZ ZIP) can be a screening router (combined with a logical switch) that provides the interface to the internal departmental network infrastructure. The External Zone ZIP (in this case, the PAZ ZIP) can be a screening router combined with a UTM that provides the interface to the external departmental network infrastructure. All the access routers perform or provide connectivity to boundary systems capable of packet filtering, NAT, and PAT. A wireless access point (AP) provides End-Systems access from a dynamically assigned distinct address pool. Wireless End-Systems undergo strong authentication (see B.4.3.4) before the establishment of a connection to the OZ.

The Internal Zone ZIP is connected to a departmental switch, from which an intrusion detection sensor taps the switch's switched port analyzer (SPAN) port. This switch can also host a series of services including filtering of malware, filtering of Internet content, SVPN, intrusion detection, intrusion prevention, UTM, and wireless connectivity[43].

The ZIPs may also consist of stateful filters or firewalls (optional, based on Threat and Risk Assessment (TRA) results) at the Edge Interface to provide redundancy and ensure segregation of traffic. The ZIPs (e.g., stateful inspection) provide ingress filtering to protect the departmental network from a compromised service.

Security services such as malware filtering, vulnerability scanning, access control, IPSec, traffic logging, and proxies are used to facilitate the secure use of network resources by departmental end-users.

The application servers in the PAZ DMZ can communicate with back-end servers on the departmental network in an OZ. Business application servers, file/print servers, and network servers provide for the workgroup services.

Traffic is strictly segregated. Functional traffic is segregated to ensure failures are isolated and management traffic is segregated from operational traffic. External applications (e.g. for e-government services) are protected from other network traffic.

E.3.2 Example 2: Small-scale OZ

This example is a variation of Example 1, such that it simplifies the depiction of an OZ that reflects the use of a single boundary system. A department may choose this single boundary system to be a UTM system.

[43] Please note that the inclusion and location of wireless access is optional and its location under consideration. Wireless could be considered to be located on the Internetwork with the other Access Subsystems.

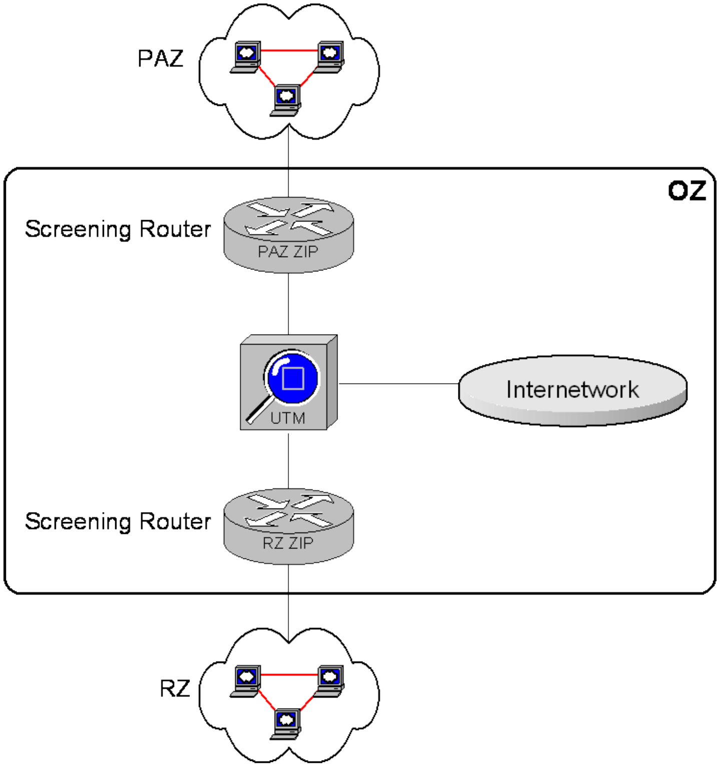


Figure 23 – Implementation of a Small-scale OZ

Figure 21 illustrates an example of an OZ implementation interfacing with a PAZ and an RZ infrastructure. In this diagram, the OZ is interfacing with an RZ; however, the OZ can also interface with another OZ or a Highly Restricted Zone (HRZ). Based on a department's requirements, a single UTM system can also provide the functionality of the interfacing ZIPs as long as it fulfills the security requirements of those connecting Zones.

E.3.3 Example: Other Government Departments

The SCNet and Network Security Zones facilitates the connectivity of other Government departments (OGD) to the OZ. OGD connectivity is achieved via the SCNet or a dedicated network service provider. The SCNet router provides one interface for the GC and Internet access, thus both the PAZ and OZ ZIPs can be used for OZ connectivity between OGDs.

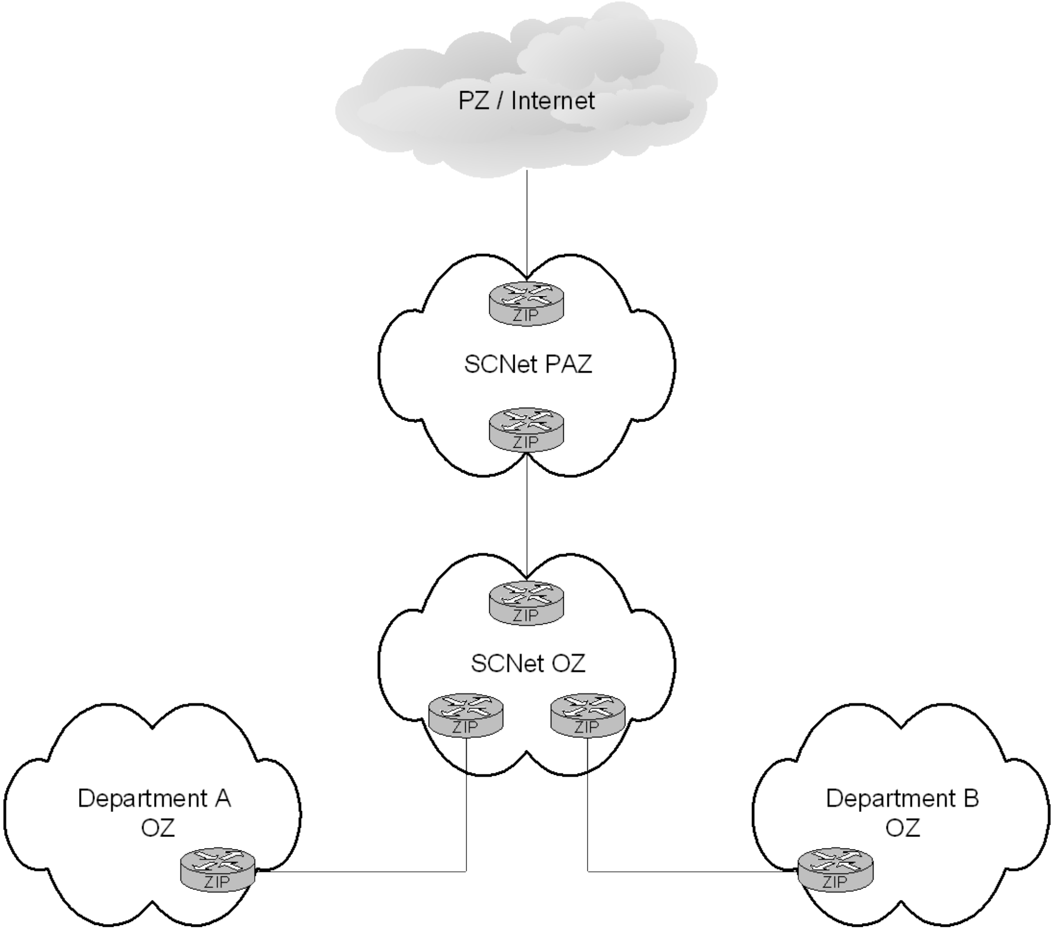


Figure 24 – Connectivity to Other Government Departments

E.4 Implementation Options for a Restricted Zone (RZ) Instance

As one moves from the OZ to an RZ, the environment changes from one that accommodates end-user systems and workgroup servers to an environment of End-Systems such as those found in data centres. The RZ is the primary environment hosting server farms, storage networks, and network management servers. It may also contain enclaves of end-user systems requiring higher levels of protection. The RZ is suitable for processing sensitive information, large repositories of sensitive data and critical applications.

The RZ example illustrated in Figure 25 applies for departments that support internally hosted services and a range of on-line services, indirectly.

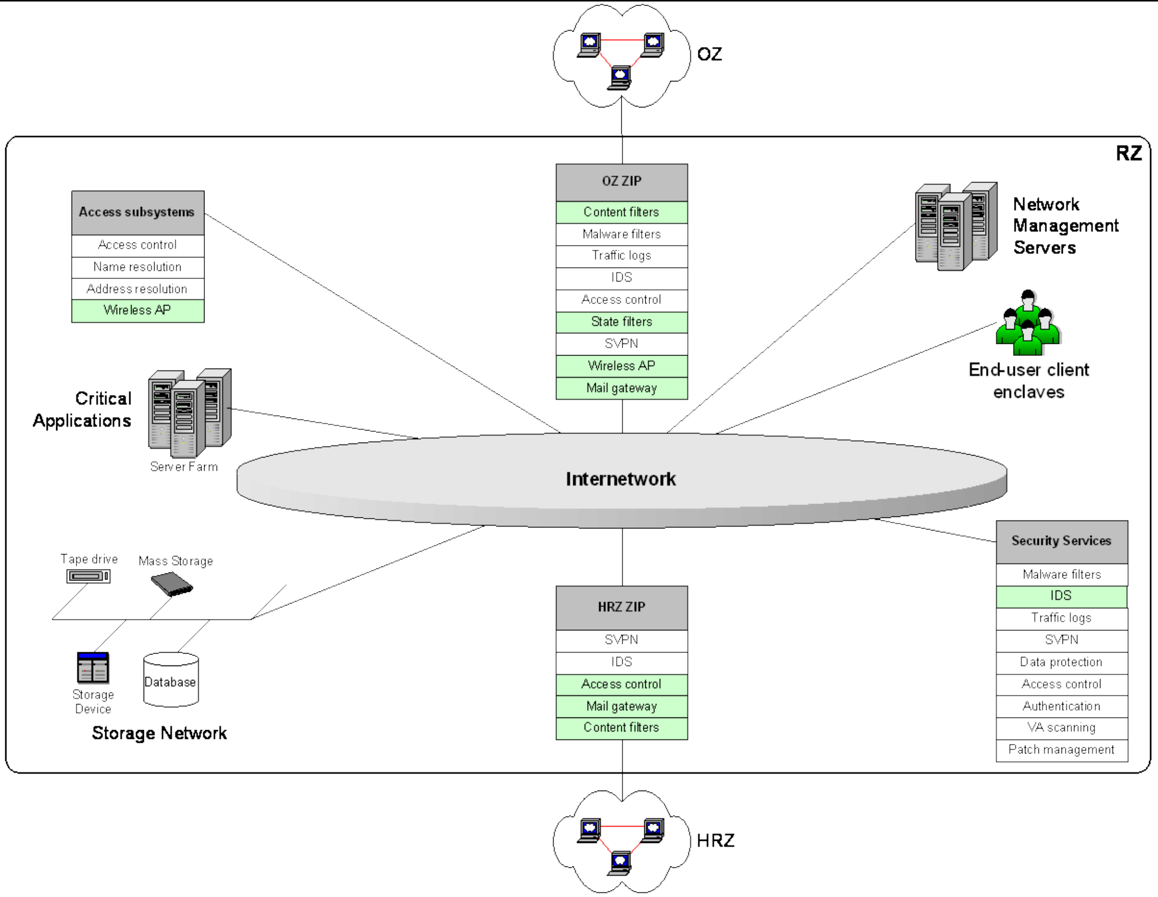


Figure 25 – Implementation of an RZ

In this example, there is access to the RZ from the OZ or an HRZ. Each ZIP has an edge router for filtering access to the target RZ. The internal ZIP can be a router that provides the interface to the internal departmental network infrastructure. All the access routers perform or provide connectivity to boundary systems capable of packet filtering, NAT, and PAT. A wireless AP[44] provides End-Systems access from a dynamically assigned distinct address pool. Wireless End-Systems undergo strong authentication (see B.4.3.4) before the establishment of a connection to the RZ.

The internal ZIP is connected to a departmental switch, from which an intrusion detection sensor taps the switch's SPAN port. This switch can also host a series of services including filtering of malware, filtering of Internet content, Virtual Private Network (VPN) connectivity, intrusion detection, intrusion prevention, UTM, and wireless connectivity.

[44] Please note that the inclusion and location of wireless access is optional and its location under consideration. Wireless could be considered to be located on the Internetwork with the other Access Subsystems.

The ZIPs may also consist of stateful filters or firewalls (based on TRA results) at the Edge Interface to provide redundancy and ensure segregation of traffic. The ZIPs (e.g., stateful inspection) provide ingress filtering to protect the departmental network from a compromised service.

Security services such as malware filtering, vulnerability scanning, access control, IPSec, and traffic logging are used to facilitate secure use of network resources by departmental end-users.

E.5 Implementation Options for a Highly Restricted Zone (HRZ) Instance

As one moves from the RZ to an HRZ, the environment changes from an environment of End-Systems such as those found in data centres to a tightly controlled network environment for highly secure GC operations. The HRZ is designed for enterprise platform and application services and for client enclaves requiring the highest levels of protection. The HRZ is suitable for processing classified information and safety-critical applications.

The HRZ example illustrated in Figure 26 applies for departments that support internally hosted services and a range of on-line services, indirectly.

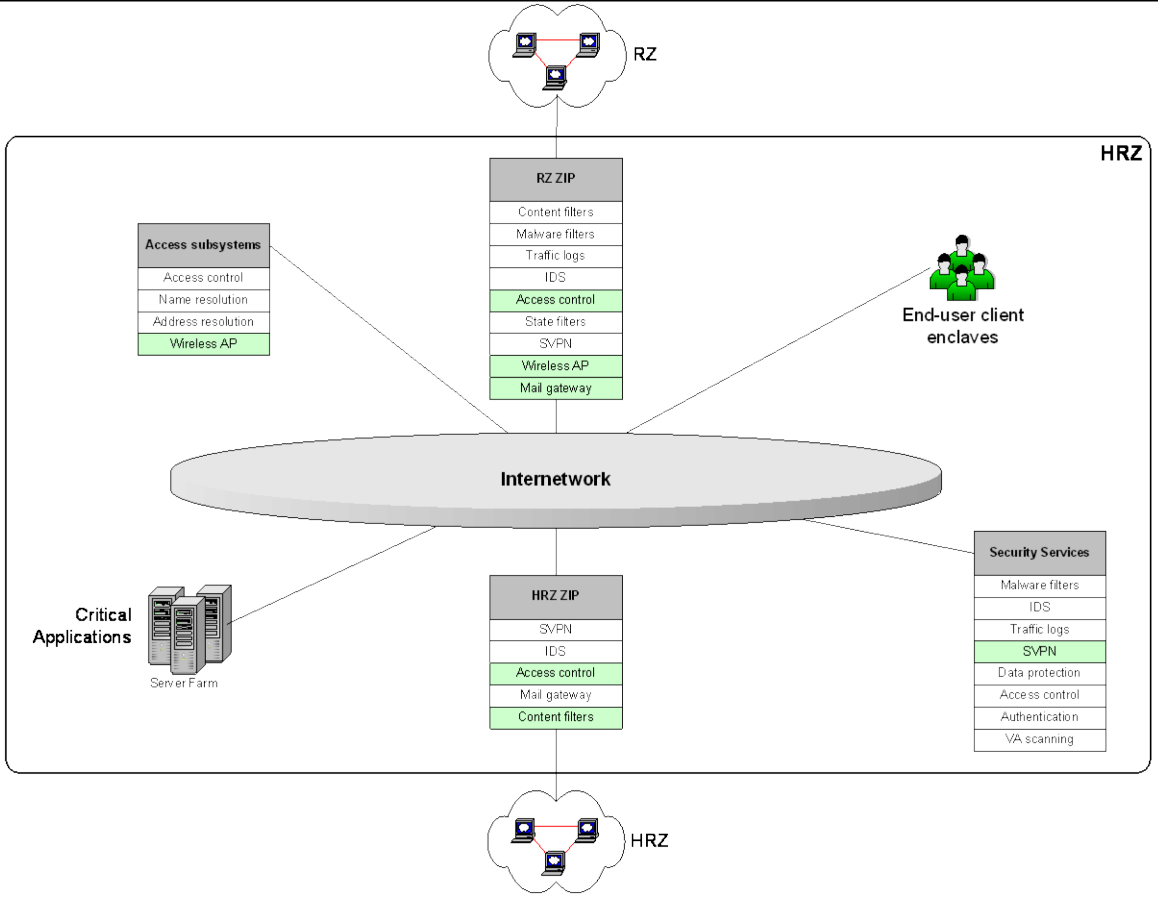


Figure 26 – Implementation of an HRZ

In this example, there is access to the HRZ from the RZ or another HRZ. Each ZIP has an edge router for filtering access to the target HRZ. The internal ZIP can be a router that provides the interface to the internal departmental network infrastructure. All the access routers perform or provide connectivity to boundary systems capable of packet filtering, NAT, and PAT. A wireless AP[45] provides End-Systems access from a dynamically assigned distinct address pool. Wireless End-Systems undergo strong authentication (see B.4.3.4) before the establishment of a connection to the HRZ.

The internal ZIP is connected to a departmental switch, from which an intrusion detection sensor taps the switch's SPAN port. This switch can also host a series of services including filtering of malware, filtering of Internet content, VPN connectivity, IPSec traffic, intrusion detection, intrusion prevention, UTM, and wireless connectivity.

[45] Please note that the inclusion of wireless access is optional and its location under consideration. Wireless could be considered to be located on the Internetwork with the other Access Subsystems.

The ZIPs may also consist of stateful filters or firewalls (based on TRA results) at the Edge Interface to provide redundancy and ensure segregation of traffic. The ZIPs (e.g., stateful inspection) provide ingress filtering to protect the departmental network from a compromised service.

Security services such as malware filtering, vulnerability scanning, access control, IPSec, and traffic logging are used to facilitate secure use of network resources by departmental end-users.

This page intentionally left blank.

Annex F ITSD-02 to ITSG-22 Requirements Traceability Matrix

This Annex provides traceability of the requirements between the previously-published CSEC Directive document *IT Security Zones Baseline Security Requirements* (ITSD-02, dated May 2003) and this Guideline. The purpose of this section is to aid Government of Canada (GC) users of the (now rescinded) Directive in determining if requirements that have been implemented previously or are being planned for implementation, are still valid.

In the tables below, requirements from ITSD-02 are listed in the first data column and requirements detailed in this Guideline are listed in the second. The third data column indicates if the requirements are the *same* (i.e., no change) as the previous document, if it is a *new* requirement, or if the requirement has been *revised* (i.e., certain criteria and/or wording has been changed or updated).

Table 1 – ITSD-02 to ITSG-22 Traceability Matrix for the Public Access Zone (PAZ)

Topic	ITSD-02	ITSG-22	Status
Security Objectives			
Traffic Control Objectives	PZ-OBJ-100	PZ-OBJ-100	Same
	PZ-OBJ-101	PZ-OBJ-101	Same
	PZ-OBJ-102	PZ-OBJ-102	Same
	PZ-OBJ-103	PZ-OBJ-103	Same
	PZ-OBJ-104	PZ-OBJ-104	Same
	PZ-OBJ-105	PZ-OBJ-105	Same
Network Availability and Reliability Objectives	PZ-OBJ-106	PZ-OBJ-106	Same
	PZ-OBJ-107	PZ-OBJ-107	Same
	PZ-OBJ-108	PZ-OBJ-108	Same
	PZ-OBJ-109	PZ-OBJ-109	Same
	PZ-OBJ-110	PZ-OBJ-110	Same
Data Protection Objectives	PZ-OBJ-111	PZ-OBJ-111	Revised
	PZ-OBJ-112	PZ-OBJ-112	Same
	PZ-OBJ-113	PZ-OBJ-113	Same
	PZ-OBJ-114	PZ-OBJ-114	Same
Security Objectives for the DMZ	PZ-OBJ-115	PZ-OBJ-115	Same
	PZ-OBJ-116	PZ-OBJ-116	Same

Topic	ITSD-02	ITSG-22	Status
Functional Services	PZ-OBJ-117	PZ-OBJ-117	Same
	PZ-OBJ-118	PZ-OBJ-118	Same
	PZ-OBJ-119	PZ-OBJ-119	Same
	PZ-OBJ-120	PZ-OBJ-120	Same
Security Requirements			
Network Interface Requirements	PZ-NI-100	PZ-NI-100	Same
	PZ-NI-101	PZ-NI-101	Same
	PZ-NI-102	PZ-NI-102	Same
	PZ-NI-103	PZ-NI-103	Revised
	PZ-NI-104	PZ-NI-104	Revised
	PZ-NI-105	PZ-NI-105	Same
Traffic Control Requirements	PZ-TC-100	PZ-TC-100	Same
	PZ-TC-101	PZ-TC-101	Same
	PZ-TC-102	PZ-TC-102	Same
	PZ-TC-103	PZ-TC-103	Same
	PZ-TC-104	PZ-TC-104	Same
	PZ-TC-105	PZ-TC-105	Same
	PZ-TC-106	PZ-TC-106	Revised
	PZ-TC-107	PZ-TC-107	Same
	PZ-TC-108	PZ-TC-108	Same
	PZ-TC-109	PZ-TC-109	Same
	PZ-TC-110	PZ-TC-110	Same
	PZ-TC-111	PZ-TC-111	Same
	PZ-TC-112	PZ-TC-112	Same
	PZ-TC-113	PZ-TC-113	Same
	PZ-TC-114	PZ-TC-114	Same
	PZ-TC-115	PZ-TC-115	Same
	PZ-TC-116	PZ-TC-116	Same
	PZ-TC-117	PZ-TC-117	Same

Topic	ITSD-02	ITSG-22	Status
	PZ-TC-118	PZ-TC-118	Revised
	PZ-TC-119	PZ-TC-119	Same
	PZ-TC-120	PZ-TC-120	Same
	PZ-TC-121	PZ-TC-121	Same
	PZ-TC-122	PZ-TC-122	Same
	PZ-TC-123	PZ-TC-123	Same
	PZ-TC-124	PZ-TC-124	Same
	PZ-TC-125	PZ-TC-125	Same
	PZ-TC-126	PZ-TC-126	Revised
	PZ-TC-127	PZ-TC-127	Same
	PZ-TC-128	PZ-TC-128	Revised
	PZ-TC-129	PZ-TC-129	Same
	PZ-TC-130	PZ-TC-130	Same
	–	PZ-TC-131	New
	PZ-TC-131	PZ-TC-132	Same
	PZ-TC-132	PZ-TC-133	Same
	PZ-TC-133	PZ-TC-134	Same
	PZ-TC-134	PZ-TC-135	Same
	PZ-TC-135	PZ-TC-136	Revised
	PZ-TC-136	PZ-TC-137	Same
	PZ-TC-137	PZ-TC-138	Same
	PZ-TC-138	PZ-TC-139	Same
	PZ-TC-139	PZ-TC-140	Same
	PZ-TC-140	PZ-TC-141	Same
	PZ-TC-141	PZ-TC-142	Same
	PZ-TC-142	PZ-TC-143	Same
	PZ-TC-143	PZ-TC-144	Same
	PZ-TC-144	PZ-TC-145	Same
	PZ-TC-145	PZ-TC-146	Same
	PZ-TC-146	PZ-TC-147	Same

Topic	ITSD-02	ITSG-22	Status
	PZ-TC-147	PZ-TC-148	Same
	PZ-TC-148	PZ-TC-149	Revised
	PZ-TC-149	PZ-TC-150	Same
	PZ-TC-150	PZ-TC-151	Same
	PZ-TC-151	PZ-TC-152	Same
	PZ-TC-152	PZ-TC-153	Same
	PZ-TC-153	PZ-TC-154	New
	Not assigned	PZ-TC-155	New
	Not assigned	PZ-TC-156	New
	PZ-TC-154	PZ-TC-157	Same
	PZ-TC-155	PZ-TC-158	Same
	PZ-TC-156	PZ-TC-159	Same
	PZ-TC-157	PZ-TC-160	Same
	PZ-TC-158	PZ-TC-161	Revised (list item e)
	PZ-TC-159	PZ-TC-162	Same
	PZ-TC-160	PZ-TC-163	Revised
	PZ-TC-161	PZ-TC-164	Revised
	PZ-TC-162	PZ-TC-165	Same
	PZ-TC-163	PZ-TC-166	Same
	PZ-TC-164	PZ-TC-167	Same
	PZ-TC-165	PZ-TC-168	Same
	PZ-TC-166	PZ-TC-169	Same
	PZ-TC-167	PZ-TC-170	Same
	PZ-TC-168	PZ-TC-171	Same
	PZ-TC-169	PZ-TC-172	Same
	PZ-TC-170	PZ-TC-173	Same
	PZ-TC-171	PZ-TC-174	Same
	PZ-TC-172	PZ-TC-175	Same
	PZ-TC-173	PZ-TC-176	Revised
	PZ-TC-174	PZ-TC-177	Same

Topic	ITSD-02	ITSG-22	Status
	PZ-TC-175	PZ-TC-178	Revised
	PZ-TC-176	PZ-TC-179	Same
	PZ-TC-177	PZ-TC-180	Same
	PZ-TC-178	PZ-TC-181	Same
	PZ-TC-179	PZ-TC-182	Same
Network Configuration Requirements	PZ-NC-100	PZ-NC-100	Same
	PZ-NC-101	PZ-NC-101	Revised
	PZ-NC-102	PZ-NC-102	Same
	PZ-NC-103	PZ-NC-103	Same
	PZ-NC-104	PZ-NC-104	Same
	PZ-NC-105	PZ-NC-105	Same
	PZ-NC-106	PZ-NC-106	Same
	PZ-NC-107	PZ-NC-107	Revised
	PZ-NC-108	PZ-NC-108	Revised
	PZ-NC-109	PZ-NC-109	Same
	PZ-NC-110	PZ-NC-110	Same
	PZ-NC-111	PZ-NC-111	Same
	PZ-NC-112	PZ-NC-112	Same
	PZ-NC-113	PZ-NC-113	Same

Host Configuration Requirements	PZ-HC-100	PZ-HC-100	Revised
	PZ-HC-101	PZ-HC-101	Same
	PZ-HC-102	PZ-HC-102	deleted
	PZ-HC-103	PZ-HC-103	Revised
	PZ-HC-104	PZ-HC-104	Revised
	PZ-HC-105	PZ-HC-105	Same
	PZ-HC-106	PZ-HC-106	Same
	PZ-HC-107	PZ-HC-107	Same
	PZ-HC-108	PZ-HC-108	Revised
	PZ-HC-109	PZ-HC-109	Same
	PZ-HC-110	PZ-HC-110	Same
	PZ-HC-111	PZ-HC-111	Revised
	PZ-HC-112	PZ-HC-112	Same
	PZ-HC-113	PZ-HC-113	Same
	PZ-HC-114	PZ-HC-114	Same
	PZ-HC-115	PZ-HC-115	Same
	PZ-HC-116	PZ-HC-116	Same
	PZ-HC-117	PZ-HC-117	Same
	PZ-HC-118	PZ-HC-118	Same
	PZ-HC-119	PZ-HC-119	Revised
	PZ-HC-120	PZ-HC-120	Same
Data Protection Requirements	PZ-DP-100	PZ-DP-100	Revised
	PZ-DP-101	PZ-DP-101	Same
	PZ-DP-102	PZ-DP-102	Same
	PZ-DP-103	PZ-DP-103	Same
	PZ-DP-104	PZ-DP-104	Same
	PZ-DP-105	PZ-DP-105	Same
	PZ-DP-106	PZ-DP-106	Revised
	PZ-DP-107	PZ-DP-107	Same
	PZ-DP-108	PZ-DP-108	Same
	PZ-DP-109	PZ-DP-109	Same

	PZ-DP-110	PZ-DP-110	Revised
	PZ-DP-111	PZ-DP-111	Revised
	PZ-DP-112	PZ-DP-112	Same
	PZ-DP-113	PZ-DP-113	Same
	PZ-DP-114	PZ-DP-114	Revised
	PZ-DP-115	PZ-DP-115	Same
	PZ-DP-116	PZ-DP-116	Same
	PZ-DP-117	PZ-DP-117	Revised
	PZ-DP-118	PZ-DP-118	Same
	PZ-DP-119	PZ-DP-119	Same

Table 2 – ITSD-02 to ITSG-22 Traceability Matrix for the Operations Zone (OZ)

Topic	ITSD-02	ITSG-22	Status
Security Objectives			
Traffic Control Objectives	OZ-OBJ-100	OZ-OBJ-100	Same
	OZ-OBJ-101	OZ-OBJ-101	Same
	OZ-OBJ-102	OZ-OBJ-102	Same
	OZ-OBJ-103	OZ-OBJ-103	Same
Network Availability and Reliability Objectives	OZ-OBJ-104	OZ-OBJ-104	Same
Data Protection Objectives	OZ-OBJ-105	OZ-OBJ-105	Same
	OZ-OBJ-106	OZ-OBJ-106	Same
Other Objectives	OZ-OBJ-107	*Requirement Deleted*	–

Security Requirements			
Network Interface Requirements	OZ-NI-100	OZ-NI-100	Same
	OZ-NI-101	OZ-NI-101	Same
	OZ-NI-102	OZ-NI-102	Same
	OZ-NI-103	OZ-NI-103	Same
	OZ-NI-104	OZ-NI-104	Same
	OZ-NI-105	OZ-NI-105	Revised
Traffic Control Requirements	–	OZ-TC-100	New
	_	OZ-TC-101	New
	_	OZ-TC-102	New
	OZ-TC-100	OZ-TC-104	Revised
	OZ-TC-101	OZ-TC-105	Same
	OZ-TC-102	OZ-TC-106	Revised
	OZ-TC-103	OZ-TC-107	Same
	OZ-TC-104	OZ-TC-108	Same
	OZ-TC-105	OZ-TC-103	Same
	OZ-TC-106	OZ-TC-109	Same
	OZ-TC-107	OZ-TC-110	Same
	OZ-TC-108	OZ-TC-111	Same
	OZ-TC-109	OZ-TC-112	Same
	OZ-TC-110	OZ-TC-113	Same
	OZ-TC-111	OZ-TC-114	Same
	OZ-TC-112	OZ-TC-115	Revised
	OZ-TC-113	OZ-TC-116	Revised
	OZ-TC-114	OZ-TC-117	Same
	OZ-TC-115	OZ-TC-118	Same
	OZ-TC-116	OZ-TC-119	Same
	OZ-TC-117	OZ-TC-120	Same
	OZ-TC-118	OZ-TC-123	Same
	OZ-TC-119	OZ-TC-121	Revised

	OZ-TC-120	OZ-TC-122	Same
	OZ-TC-121	OZ-TC-124	Same
	Not assigned	OZ-TC-125	New
	Not assigned	OZ-TC-126	New
	Not assigned	OZ-TC-127	New
	Not assigned	OZ-TC-128	New
	Not assigned	OZ-TC-129	New
	Not assigned	OZ-TC-130	New
Network Configuration Requirements	OZ-NC-100	OZ-NC-100	Revised
	OZ-NC-101	OZ-NC-101	Same
	OZ-NC-102	OZ-NC-102	Same
	OZ-NC-103	OZ-NC-103	Same
	OZ-NC-104	OZ-NC-104	Same
	–	OZ-NC-105	New
	OZ-NC-105	OZ-NC-106	Same
	OZ-NC-106	OZ-NC-107	Same
	OZ-NC-107	OZ-NC-108	Same
	OZ-NC-108	OZ-NC-109	Same
	OZ-NC-109	OZ-NC-110	Same
	OZ-NC-110	*Requirement Deleted*	–
	OZ-NC-111	OZ-NC-111	Same
	OZ-NC-112	OZ-NC-112	Same
	OZ-NC-113	OZ-NC-113	Same
	OZ-NC-114	OZ-NC-114	Same
	OZ-NC-115	OZ-NC-115	Same
	OZ-NC-116	OZ-NC-116	Same
	OZ-NC-117	OZ-NC-117	Revised
	OZ-NC-118	OZ-NC-118	Revised
	OZ-NC-119	OZ-NC-119	Same
	OZ-NC-120	OZ-NC-120	Revised

	–	OZ-NC-121	New
	OZ-NC-121	OZ-NC-123	Revised
	Not assigned	OZ-NC-122	New
	Not assigned	OZ-NC-124	New
Host Configuration Requirements	OZ-HC-100	OZ-HC-100	Revised
	OZ-HC-101	OZ-HC-101	Same
	OZ-HC-102	OZ-HC-102	Same
	OZ-HC-103	OZ-HC-103	Revised
	OZ-HC-104	OZ-HC-104	Revised
	OZ-HC-105	OZ-HC-105	Revised
	–	OZ-HC-106	New
	OZ-HC-106	OZ-HC-107	Revised
	OZ-HC-107	OZ-HC-108	Revised
	OZ-HC-108	OZ-HC-109	Revised
	OZ-HC-109	OZ-HC-110	Revised
	OZ-HC-110	OZ-HC-111	Same
	OZ-HC-111	OZ-HC-112	Revised
	OZ-HC-112	OZ-HC-113	Revised
	OZ-HC-113	OZ-HC-114	Revised
Data Protection Requirements	OZ-DP-100	OZ-DP-100	Same
	OZ-DP-101	OZ-DP-101	Same
	OZ-DP-102	OZ-DP-102	Same
	OZ-DP-103	OZ-DP-103	Same
	OZ-DP-104	OZ-DP-104	Revised
	OZ-DP-105	OZ-DP-105	Revised
	Not assigned	OZ-DP-106	New

Table 3 – ITSD-02 to ITSG-22 Traceability Matrix for the Restricted Zone (RZ)

Topic	ITSD-02	ITSG-22	Status
All Topics	N/A	All requirements and objectives are new	All requirements and objectives are new

Table 4 – ITSD-02 to ITSG-22 Traceability Matrix for the Highly Restricted Zone (HRZ)

Topic	ITSD-02	ITSG-22	Status
All Topics	N/A	All requirements and objectives are new	All requirements and objectives are new