Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Baseline Security Requirements for Network Security Zones

(Version 2.0)

PRACTITIONER

ITSP.80.022

Canada

FOREWORD

ITSP.80.022 Baseline Security Requirements for Network Security Zones is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). For more information or suggested amendments, contact the Canadian Centre for Cyber Security (Cyber Centre) Contact Centre:

CCCS Contact Centre
contact@cyber.gc.ca
Local: (613)-949-7048
Toll Free: 1-833-CYBER-88

This version of ITSP.80.022 supersedes previous versions of the document.

EFFECTIVE DATE

This publication takes effect on January 12, 2021.

REVISION HISTORY

Revision	Amendments	Date
1	Released version 2.0	January 12, 2021

OVERVIEW

This document outlines network security zone models and architectures and provides technical guidance on implementing network security zones.

The guidance in this document is intended for information technology (IT) solutions operating at UNCLASSIFIED, PROTECTED A, and PROTECTED B levels[1] (i.e. low sensitivity or partial sensitivity). Systems operating in PROTECTED C[2] or classified domains[3] (i.e. highly sensitive) require additional design considerations that are not within the scope of this document. You can email or phone our Contact Centre for guidance on cryptographic solutions for PROTECTED C or classified domains.

Your organization is responsible for determining the security objectives that you require to protect information and services. Following only the guidance in this document does not adequately secure an IT environment.

This document is written for IT practitioners who are familiar with the principles, standards, and terminology of network engineering. For further guidance on network security, contact our Contact Centre:

Contact Centre
contact@cyber.gc.ca
(613)-949-7048
Toll Free: 1-833-CYBER-88

[1] Protected A and Protected B are Government of Canada protection terms for information (e.g. business or personal information) that is of low sensitivity and partial sensitivity. If Protected A information is compromised, it could cause injury or embarrassment to a business or person. If Protected B information is compromised, it could cause injury to serious injury to a business or person (e.g. competitive advantage, loss of reputation).

[2] Protected C is a protection term for highly sensitive business or personal information. If Protected C information is compromised, it could cause grave injury to a business or a person (e.g. serious financial harm or loss of life).

[3] Classified systems or information (e.g. confidential, secret, top secret) are those that are of national interest (e.g. economic, political, military) to Canada. If classified systems and information are compromised, they could endanger national security, cause injury to relationships with other nations, or give substantial advantage to a foreign country.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXES

1 INTRODUCTION

This document explains zoning and the use of network security zones to take a layered approach to security. This document also outlines the functional model of these zones. This model covers the principles and the design philosophy for using different security zones to separate IT infrastructure.

To help you implement network security zones, this document includes the internal configuration and management issues for each zone and zone interface point (ZIP). The security objectives and requirements included in this document define how to connect one zone to another. They also define how to determine whether a direct connection between certain zones is recommended or permissible to maintain the required security level.

Network security zones are the foundations of a balanced and layered security architecture that can support a range of security solutions for your organization's business needs. These zones also provide a common network infrastructure to support electronic service delivery, interconnectivity, and interoperability. If your organization shares a common infrastructure for online service delivery or other purposes, you must conform to all the security standards established for that infrastructure.

If you're implementing IT solutions in a Government of Canada (GC) department or agency, you must follow all relevant Treasury Board of Canada Secretariat (TBS) policies, including the following:

- *Policy on Service and Digital* [1][4];
- *Policy on Government Security* [2]; and
- *Directive on Security Management* [3].

If your organization is not a GC department or agency, you can still refer to these policies for additional information.

1.1 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

Like any IT project or solution, when implementing network security zones, you should consider the IT security risk management activities described in *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [4]. Figure 1 outlines these activities.

ITSG-33 [4] describes two levels of IT security risk management activities: organizational-level activities (also referred to as departmental-level activities) and information system-level activities. You should include organizational-level activities, which are described in Annex 1 of ITSG-33 [4], in your organization's security programs. This level of activities helps you plan, manage, and assess IT security risks. You should include information system-level activities, which are described in Annex 2 of ITSG-33 [4], in an information system's lifecycle through the information system security implementation process (ISSIP).

[4] Numbers in square brackets indicate a reference from the Supporting Content section of this document.

Your organization's implementation of network security zones should align with your current IT security risk management activities, specifically the following: defining organizational IT security needs and security controls, deploying security controls, and monitoring and assessing the performance of security controls. Your implementation should also align with your information system-level activities to ensure the solution is dependable. Specifically, you should consider the following phases of the ISSIP: initiation, development and acquisition, integration and installation, and operations and maintenance.

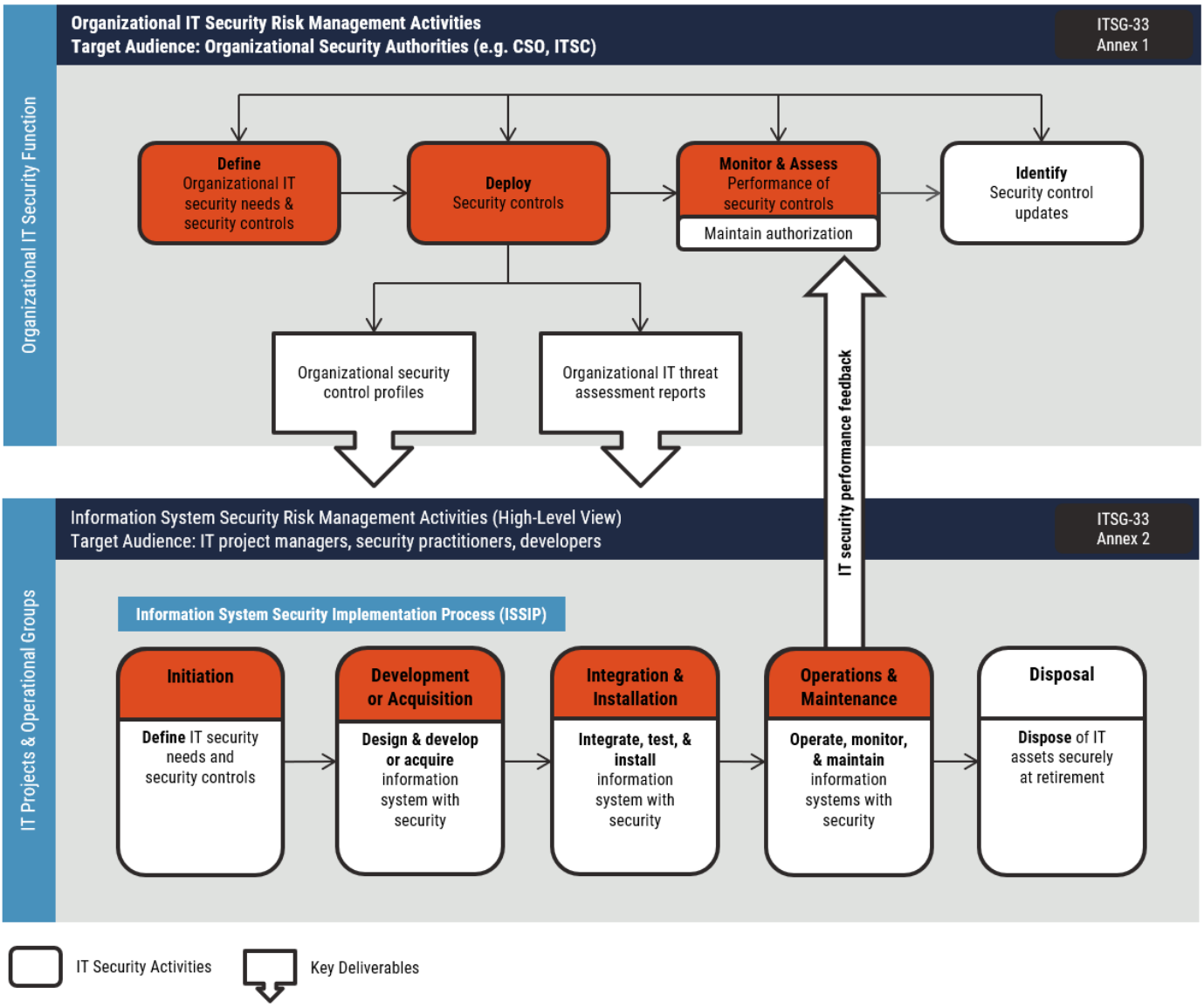

Figure 1: IT Security Risk Management Activities

2 NETWORK SECURITY ZONES

2.1 NETWORK SECURITY ZONE TYPES

A zone is a networking environment with a well-defined perimeter and connection points. This document defines the following types of zones:

- Public zone;
- Public access zone;
- Operations zone;
- Restricted zone;
- Highly restricted zone;
- Restricted extranet zone; and
- Management zone.

The relationship between these zones is demonstrated in the zone implementation model, which is illustrated in Figure 5 of this document (see subsection 3.2.2).

2.1.1 PUBLIC ZONE

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

Although the PZ is assumed to be extremely hostile, a network security zone authority (see subsection 2.3 for more information) is permitted to use security services from public providers. In fact, the use of security services from public providers is encouraged because it enhances the defence-in-depth posture. However, you should not discount a PZ's threat level when developing baseline security requirements.

2.1.2 PUBLIC ACCESS ZONE

A public access zone (PAZ) mediates access between operational systems and the PZ. A PAZ is a tightly controlled environment that protects the internal network and applications from the hostile PZ. A PAZ also acts as a screen, hiding internal resources from the PZ and limiting the exposure of internal resources.

The interfaces to all online organizational services should be implemented in a PAZ. Proxy services that allow personnel to access Internet-based applications should also be implemented in a PAZ, as should external email, remote access, and extranet gateways.

Extranets connecting via a PAZ are different than those connecting via a restricted extranet zone (REZ) (see subsection 2.1.6). Extranets connecting via a REZ differ mainly in the trust placed in the extranet partner. REZ partners are highly trusted and may connect directly to an internal, organization-controlled zone.

2.1.3 OPERATIONS ZONE

An operations zone (OZ) is the standard environment for an organization's routine operations. An OZ is where most end-user systems, application servers, and file and print servers are installed. With the appropriate security controls on the end systems, this zone may be suitable for processing sensitive information. However, in general, this zone is not suitable for large repositories of sensitive data or critical applications.

Within an OZ, traffic is generally unrestricted and can originate internally (i.e. from other zones within an organization) or from authorized external sources (e.g. remote access, mobile access, extranets) via the PAZ and the REZ.

However, in the OZ, malicious traffic may originate from hostile insiders, hostile code imported from the PZ, or undetected malicious nodes on the network (e.g. a compromised host or unauthorized wireless attachment to the zone).

2.1.4 RESTRICTED ZONE

A restricted zone (RZ) provides a controlled network environment, generally suitable for business-critical IT services (i.e. services with medium integrity and availability requirements and that, if compromised, would cause disruption to a business). An RZ is also suitable for large repositories of sensitive information (e.g. in a data centre).

An RZ supports access from systems in the PZ via the OZ and the PAZ. All network-layer entities in an RZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and configuration control. The RZ reduces threats from system insiders by limiting access. Threats are also reduced through administrative monitoring. Data confidentiality services are implemented in an RZ to protect zone traffic from being eavesdropped by unauthorized nodes.

2.1.5 HIGHLY RESTRICTED ZONE

A highly restricted zone (HRZ) provides a tightly controlled network environment that, in general, is suitable for safety-critical applications (i.e. applications with high availability and integrity requirements that would endanger human health or safety if compromised). An HRZ is also suitable for extensive repositories of sensitive information.

Only other organization-controlled zones may access an HRZ (i.e. there is no access by systems in the PZ). All network-layer entities in an HRZ are authenticated, either explicitly through the implementation of a peer-entity authentication service or implicitly through a combination of physical security and rigorous configuration control. In general, the HRZ has stricter requirements for end systems than the RZ. The HRZ also imposes stricter controls on system insiders, addressing threats from that source.

Data confidentiality services, which are suitable for protecting sensitive information, are also implemented in an HRZ. Data confidentiality services protect zone traffic against being eavesdropped by unauthorized nodes. These services can be implemented at either the network or the physical layer.

2.1.6 RESTRICTED EXTRANET ZONE

The restricted extranet zone (REZ) may support directly connected extranet services with highly trusted partners. The REZ is not necessarily connected via a PAZ (see Figure 3 in subsection 3.2.1.3).

When implementing a REZ, you need to follow the ISSIP (see Annex 2 of ITSG-33 [4]). Extra controls may be necessary to properly protect the zone connected to the REZ. The requirements and practices for this zone should be developed on a case-by-case basis and enforced through agreements with partners.

> **Note:** In the context of the GC, connections between GC departments or agencies do not use a REZ; the REZ is only used for connections to organizations outside of the GC (e.g. outsourced IT environments, federal-provincial interfaces, integrated services with financial institutions).

2.1.7 MANAGEMENT ZONE

The management zone (MZ) is an isolated zone, which is similar in build robustness to an RZ. With the MZ, network administrators have a dedicated and isolated administration network for configuring and monitoring network infrastructures. From a security perspective, this zone provides administrators with the capability to perform command and control operations while minimizing the risk of interception or compromise.

GC departments can manage zones remotely if GC-approved means are used. In the GC context, zones should only be managed remotely if a department has GC-approved, dedicated, and hardened management hosts that are authenticated to an MZ from GC-approved locations. Remote management hosts should connect and authenticate through a remote management access zone (RMAZ). The RMAZ has the same networking components and characteristics as a PAZ, but the RMAZ operates on a physically isolated infrastructure.

2.2 ZONE INTERFACE POINTS

The demarcation area between zones is called the boundary (see Figure 2 below). The boundary contains zone interface points (ZIPs), which are the connecting points between zones. A ZIP is the logical construct used to describe the controlled interface connecting two zones, and it is the network interface between these zones.

ZIPs enforce zone communication policies between two zones. All data communication between zones must be through a ZIP, which exclusively connects these two zones through a unique communication path.

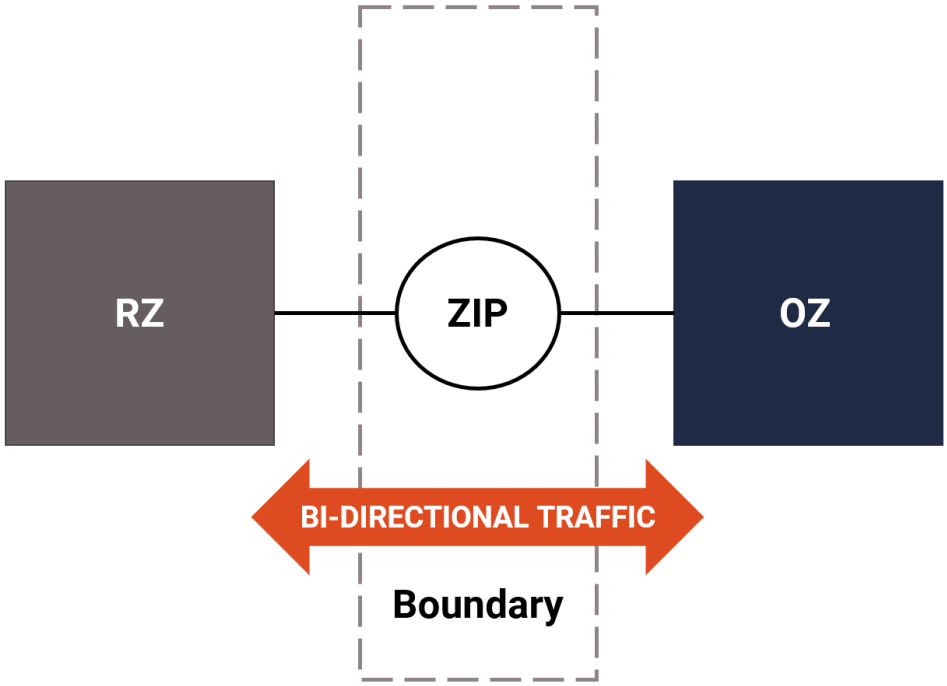

Figure 2: Example of a Zone Boundary

2.3 NETWORK SECURITY ZONE AUTHORITY

Each zone has an assigned network security zone authority, which is an entity accountable for developing, implementing, and maintaining zone security requirements and practices. As defined in ITSG-33 [4], a network security zone authority is one of the functions assigned to an IT security coordinator. The network security zone authority is responsible for the following tasks:

- Reviewing zone security policies and standards;
- Recommending zone security policies and standards for approval by the chief security officer;
- Reviewing requests for proposals and other contracting documentation, including security requirements checklists, that affect their assigned zone(s);
- Working with program and service delivery managers to ensure their IT security needs are met;
- Providing advice on zone security controls and the implementation of these controls; and
- Advising program and service delivery managers of the potential impact to the security posture due to changes to the network.

Detailed network security zone authority tasks, responsibilities, and roles are identified in Annexes A to F of this document.

A network security zone authority's control comes from direct ownership of the network or binding relationships with service providers (e.g. contracts, memorandums 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 network security zone authority may be responsible for multiple zones.

3 HIGH-LEVEL SECURITY ZONE MODELS

3.1 OVERVIEW

This section outlines a zone implementation model (see Figure 5 in subsection 3.2.2) to help you apply network security zones in your department or organization. You can apply the guidance in this section in either single- or multi-tenant environments. In multi-tenant environments, you should consider additional design and security requirements to meet individual confidentiality, integrity, and availability requirements; these additional design and security requirements are not within the scope of this document.

3.2 ZONE IMPLEMENTATION MODEL

3.2.1 PRINCIPLES OF NETWORK SECURITY ZONES

Zoning is a logical design approach used to control and restrict access and data communication flows to certain components and users. Zones establish the network perimeters and their associated boundary defence requirements through the following functions:

- Defining the entities that populate zones;
- Identifying discrete entry and exit points;
- Filtering network traffic at entry and exit points;
- Monitoring the state of the network;
- Authenticating the identity of network entities; and
- Monitoring network traffic at the entry and exit points.

A zone has an assigned network security zone authority. The network security zone authority is an entity that is accountable for developing, implementing, and maintaining the zone security requirements and practices.
The zone security requirements and practices complement common network infrastructures in electronic service delivery, interconnectivity, and interoperability.

You can use zones to implement a network infrastructure that reduces security risks related to business processes and information. The zones are separated by ZIPs, which are implemented through security and network devices. Zones can be used to create a defence-in-depth architecture. In this architecture approach, layers of protection are added to a network so that sensitive data (whether being stored or processed) can be accessed only by a small group of users and applications.

Using a defence-in-depth architecture, the functions performed on selected data are organized into zones based on the users' needs, the data sensitivity, and the expected threat environment. Different zones deliver different levels of security to the business processes within each zone. A new zone is needed when new policy requirements are established. For example, Internet-accessible zones, which focus on user access to the Internet, require a greater number of controls because these zones have more users and a variety of data types and applications. As you progress through each connected zone, there is a decrease in the variety of applications, the users who can use the applications, and the functions that can be performed. Because there is a decrease in the

variety of applications and data, the number of controls will appear to decrease as well. However, the assurance levels of the implemented controls will rise as the data sensitivity rises.

Zones in which all components are entirely within the control of your department are considered to be controlled zones. If your department does not control all zone components, the zone is considered to be uncontrolled. You should evaluate uncontrolled zones as part of your departmental or organizational risk management process.

3.2.1.1 NETWORK SECURITY AND INFORMATION SECURITY

Network security consists of the measures taken to reduce a network's vulnerability to threats. Information security consists of the measures taken to reduce the vulnerability of information in its various forms (e.g. paper, electronic) and states (e.g. at rest, in transit).

While network security and information security address different issues, there is some overlap. For example, both network security and information security address the protection of electronic information transmitted across computer networks. With this overlap in mind, some security controls provide both types of security.

3.2.1.2 INFORMATION SECURITY AND CRYPTOGRAPHY

We recommend using cryptography in a low-threat environment; however, we do not include broad requirements for cryptography in this document. You should conduct a threat and risk assessment (TRA) to determine if your IT environment needs information security measures, such as cryptography.

Cryptography is an effective information security control. Cryptography protects confidentiality and integrity and supports other security services, such as non-repudiation (i.e. preventing an information sender from successfully claiming to not have sent the information in question). Cryptography is also an effective network security control because it prevents certain network-based attacks (e.g. eavesdropping and replaying messages). The benefits delivered by cryptography will vary, depending on the layer of the network stack in which it is implemented. Some cryptographic solutions, such as public key infrastructure (PKI) services, are implemented at the application layer.

Other cryptographic solutions (e.g. Type 1 encryption) are mandated because of information security considerations rather than network security considerations. These types of solutions protect the information, not the network. Because network security focuses on the transport layer and below, some cryptographic solutions are out of the scope of network security.

For more guidance on cryptographic solutions, contact our Contact Centre (see subsection 5.1 for contact information).

3.2.1.3 NETWORK IMPLEMENTATION OPTIONS

You can physically or logically implement the separation and the security functions of a ZIP or a zone. You can also use a mix of physical and logical implementation methods. You should use the results of the ISSIP to decide whether to use physical or logical separation for zone boundaries. Using the ISSIP, security engineering artefacts (e.g. applicable domain security control profile, threat assessment, and information system security categorization) are developed to help determine security requirements. These security requirements specify the assurance level required by the physical and virtual network security mechanisms.

Physical Separation

Physical separation is recommended for all boundaries around the demilitarized zone (DMZ), which is the zone within the PAZ and around the MZs.

In the context of zones and ZIPs, physical separation is demonstrated in the following two situations:

- A device is connected to another device through only a physical (wired or wireless) communication medium; and
- A device is not connected to other systems.

The mechanisms within a device may perform multiple security operations or have multiple security appliances and functions on the same connected platform. Figure 3 depicts the physical separation model.

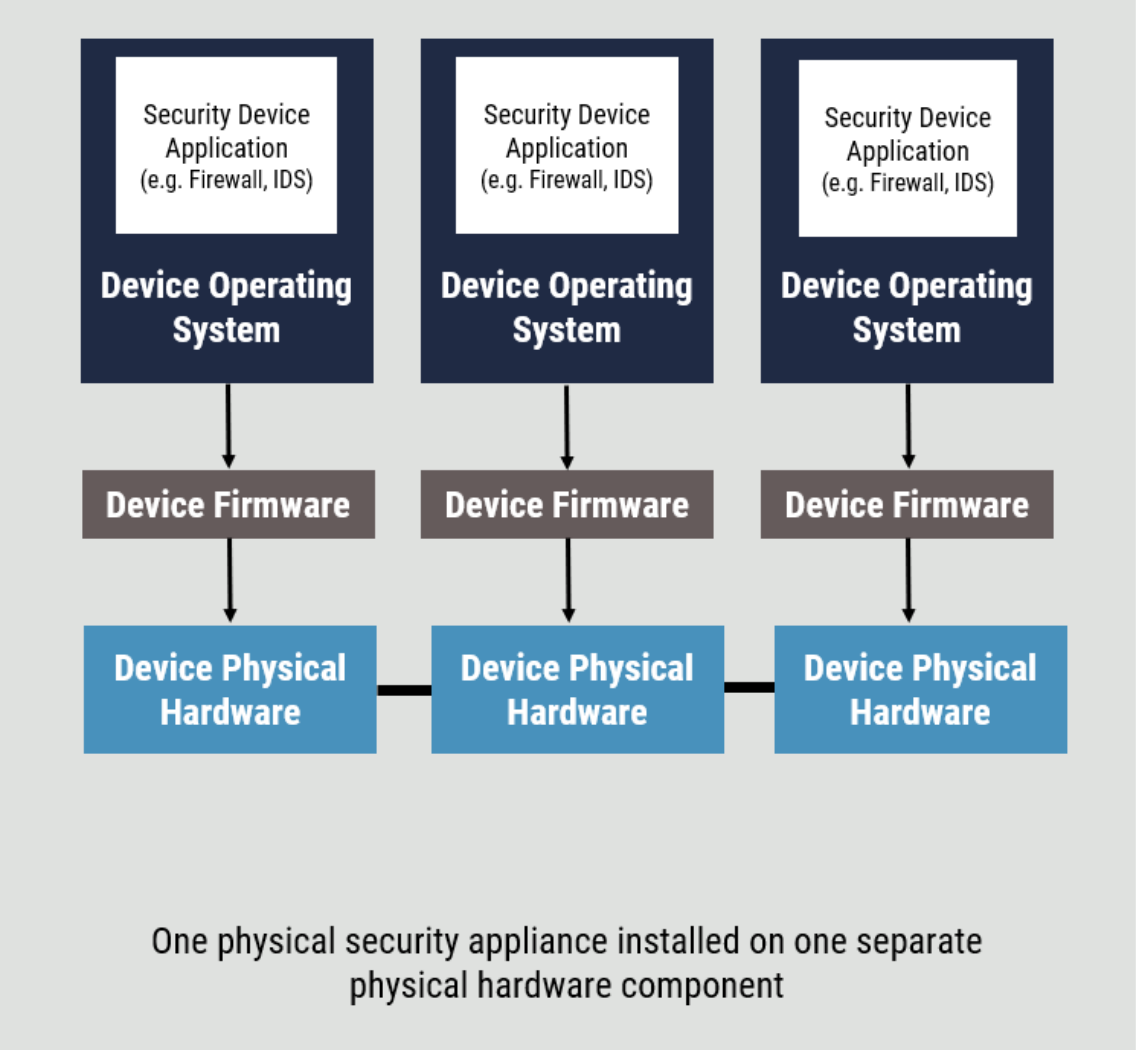

Figure 3: Physical Separation Model

Logical Separation

Virtualization can be used for logical separation within a boundary or a zone perimeter. Virtualization is a technology that allows one physical device (e.g. machines, networks, security devices, and other physical components) to behave as if it were two or more devices, virtualizing and consolidating these devices onto a single physical system. Network virtualization combines hardware and software network resources and functionality into a single software-based administrative entity. Figure 4 depicts the logical separation model.

Logically implemented security mechanisms may not have the same assurance levels as comparable physical systems. The vulnerabilities of the host operating system and hypervisors must also be considered when choosing logically implemented security mechanisms.

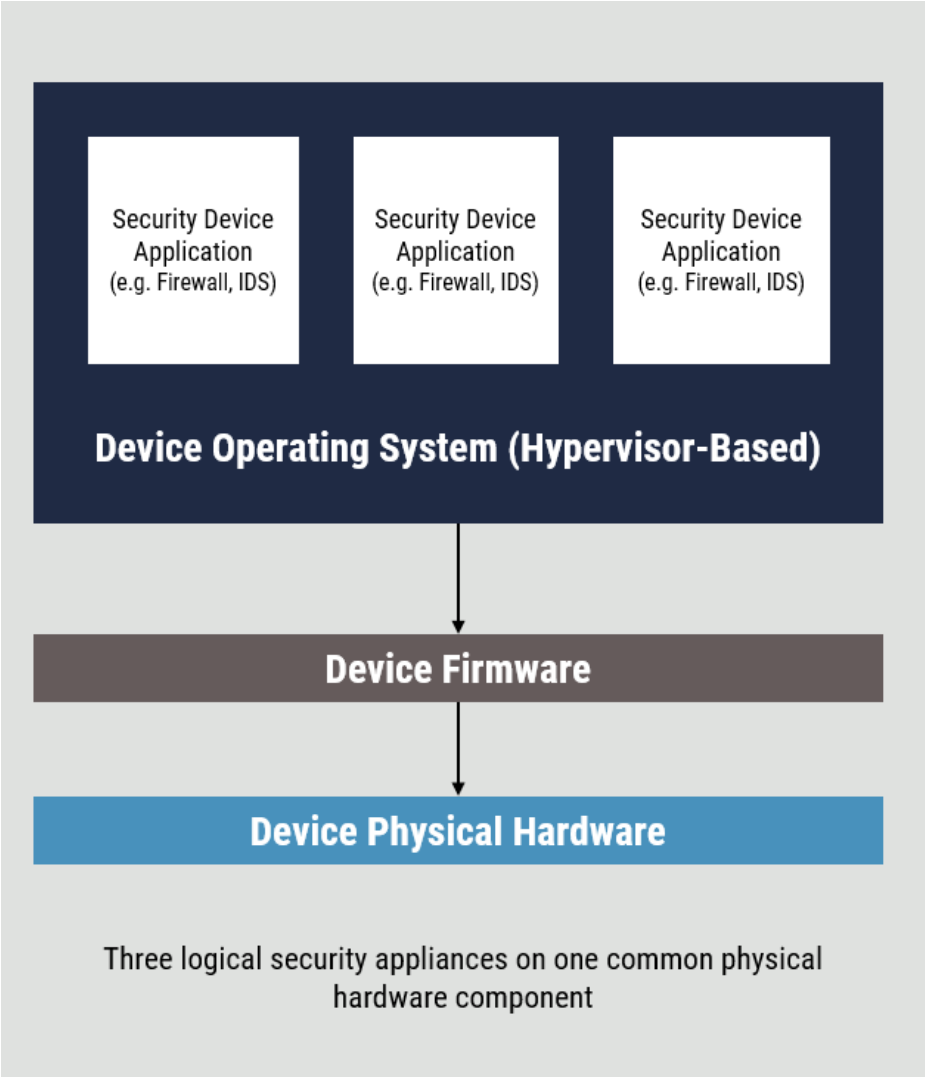

Figure 4: Logical Separation Model

3.2.2 IMPLEMENTATION MODEL

The network security zone implementation model is illustrated in Figure 5. Departments or organizations may implement multiple instances of each zone type based on their business requirements. Every zone contains one (or more) separate, routable network within its perimeter. Every separate, routable network should be entirely within a single zone. In certain circumstances, a single end system may participate in more than one zone through separate interfaces. See subsection 4.2.1 for an explanation of the end system.

This document provides a set of baseline security requirements for the following network security zones: PAZ, OZ, RZ, HRZ, MZ, and ZIPs. Other baseline security requirements may be added as needed. A network security zone authority may modify these requirements and practices to strengthen the baseline, meet particular business issues, or address a particular threat environment. However, some requirements will need to be standardized to ensure network interoperability.

A zone does not necessarily correspond to an organization's branches or business and IT functions. Your organization could implement many zones like how it implements many physical security zones. Zones may also be shared between branches or business and IT functions.

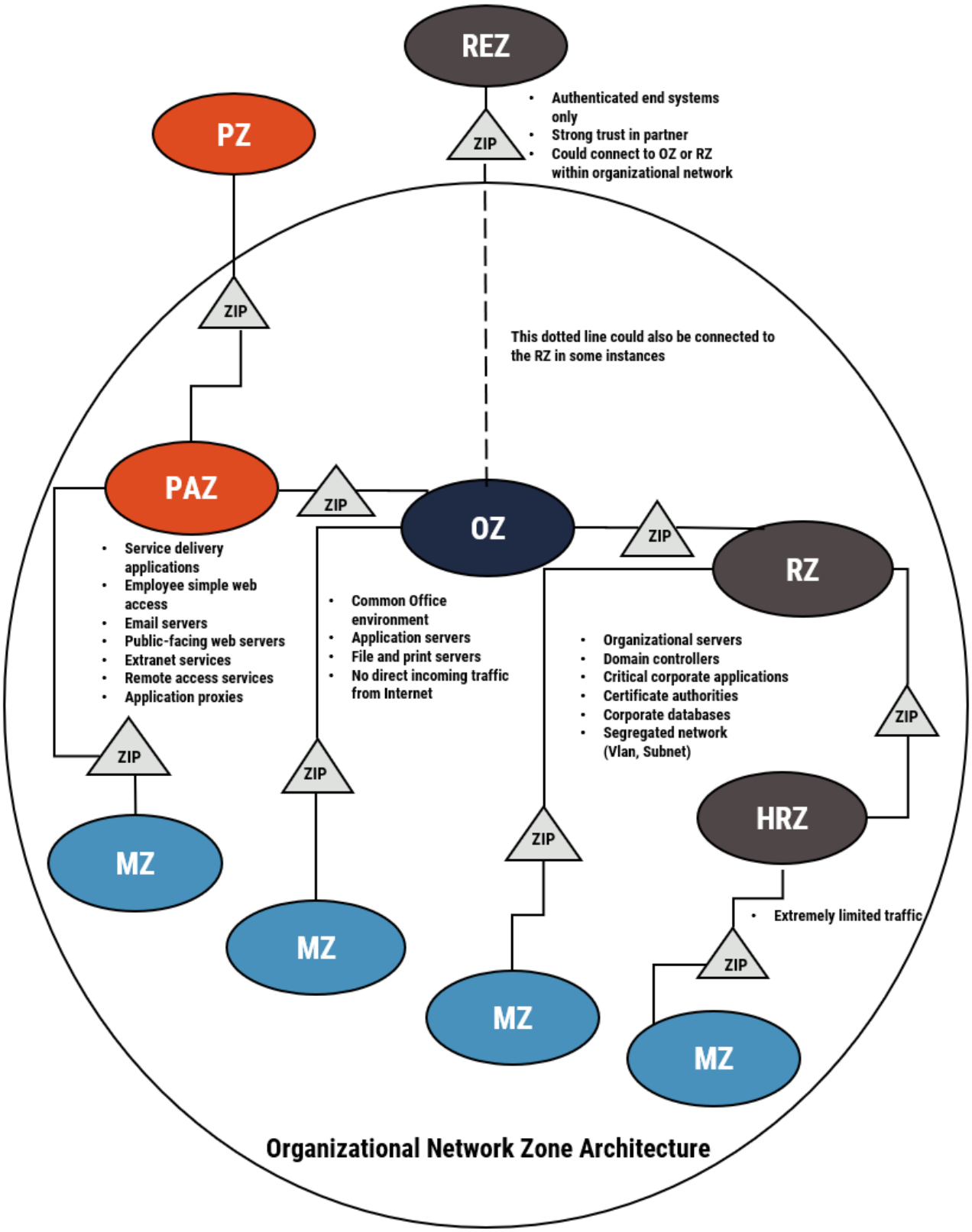

Figure 5: Network Security Zone Implementation Model

4 NETWORK SECURITY ZONE REFERENCE MODELS

4.1 OVERVIEW

This section includes two reference models:

- General reference model; and
- Functional reference model.

The general reference model establishes the technical concepts and terminology needed to support the requirements specified in annexes A to F of this document. The general reference model describes the components within a single, generic zone. The detailed reference models and the zones' required safeguards and capabilities are included in annexes A to E.

The functional model identifies five main security functions that the zones perform. These five functions are the basis for structuring the detailed zone requirements, which are detailed in annexes A to E.

4.2 GENERAL REFERENCE MODEL

A generic zone has three component types:

- End system;
- Internetwork; and
- Internal boundary system (IBS).

The internetwork component is divided into an internetwork access sub-system, an internetwork core, and an edge interface.

Figure 6 below illustrates a logical topology of a generic zone, using the three main components and the ZIPs to other zones. ZIPs, end systems, and IBSs connect to internetworks via edge interfaces (shown as small circles in Figure 6 below). In general, an instance of a zone consists of one or more internetworks with end systems and IBSs. If connectivity is required between internetworks, the connections should go through an IBS (the requirement for such interconnection depends on your business needs). ZIPs provide network interfaces to other zones. Figure 6 also shows that an end system may be shared (i.e. connected to internetworks in two different zones). Shared end systems must not allow any traffic to pass between zones.

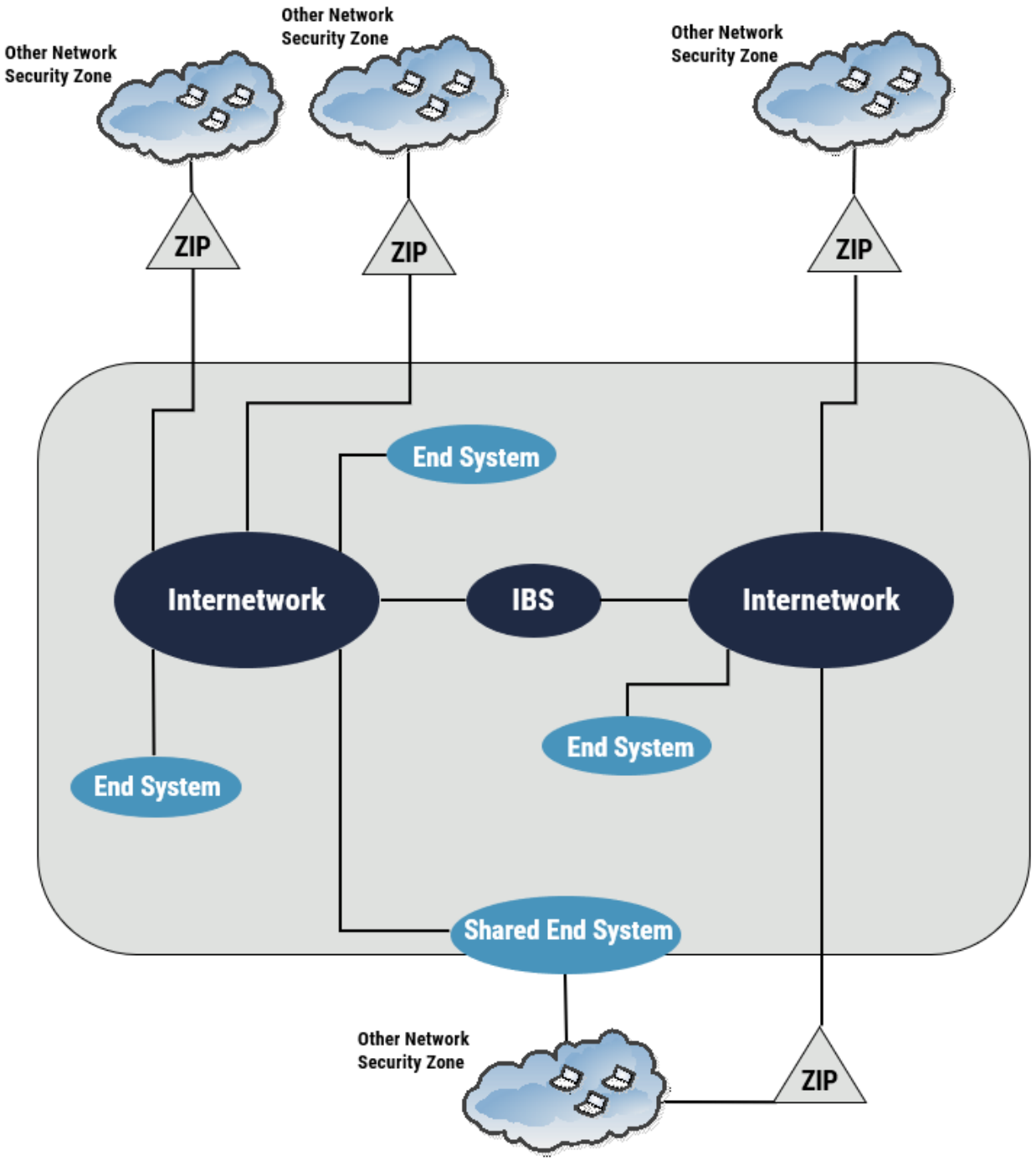

Figure 6: Network Security Zone Logical Topology

Each zone component and sub-system is a logical construct that includes specific features and functions. These components do not necessarily correspond to physical devices. For example, a single physical device could incorporate the functionality of multiple zone components, or a single zone component could require multiple physical devices to implement all its features and functions.

4.2.1 END SYSTEM

A zone end system is a computing platform that connects to an internetwork and either initiates or terminates a communication path. While an end system belongs to the zone, an end system administrator (rather than a network security zone authority) is usually responsible for the security of the end system. Although an end system typically consists of a single host, it may also consist of a network of hosts (e.g. storage area network, load-balanced server cluster) connected to the internetwork. The internal networks of these complex end systems are beyond the recommendations of this document.

End systems fall into one of the following four categories listed in Table 1.

Table 1: End System Categories

End System Category	Description
Simple host	An end system consisting of a single host.
Mobile end system	An end system (e.g. laptop) that sometimes connects to the zone and another zone (e.g. PZ).
Wireless end system	An end system connecting to the internetwork by way of a wireless internetwork access sub-system (an end system that has multiple interfaces with the internetwork is considered a wireless end system if any of these interfaces connect over a wireless internetwork access sub-system).
Complex end system	An end system consisting of a logical group of hosts and an internal private network between hosts (e.g. storage area network).

If end systems use internal wireless communications, you need to apply additional security measures to limit their exploitation as a backdoor to the zone.

When there is a business requirement to connect an end system to two or more zones simultaneously, this end system will be designated as a shared end system (see Figure 6 above). An example of a shared end system is a logically partitioned storage area network. Shared end systems must be configured and secured so they cannot route traffic between the zones. They can communicate with the zones to which they are connected, but those zones cannot exchange traffic with each other through the shard end system. Shared end systems must also meet the configuration requirements of all the zones to which they are connected. Due to the logical separation of shared end systems, the zone authorities for each zone need to understand and consider this additional risk to each connected zone.

A remote end system is an end system that belongs to a PZ and communicates logically with a GC-controlled or an organization-controlled zone through or to a PAZ. A remote end system is not considered part of the GC-controlled or organization-controlled zone. However, when a GC-controlled or an organization-controlled zone permits remote network access from PZs, the host configuration requirements for the remote end systems must comply with the GC-controlled or the organization-controlled zone's security requirements.

4.2.2 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 physical-layer media (i.e. copper wire or optical fibre) or wireless links (e.g. wireless LANs, fixed wireless links, satellite uplinks). Internetworks provide a network distribution service (e.g. routing) between edge interfaces within a zone. An internetwork includes the sub-systems listed in Table 2.

Table 2: Internetwork Sub-Systems

Sub-System	Description
Internetwork access sub-system	Provides the physical-layer and data-link-layer services that connect an edge interface to the internetwork core. Implementations of these services include bridges, Ethernet protocol, data-link-layer switches (including multiplexers), and gateways. The internetwork access sub-system may also provide network-layer and upper-layer services. Virtual private network (VPN) access would be implemented in this sub-system. An internetwork may have more than one internetwork access sub-system.
Internetwork core	Provides the core network services (e.g. backbone routing, address resolution) for the internetwork.
Edge interface	The logical boundary between the internetwork and a ZIP, an end system, or an IBS. Examples of physical implementations of an edge interface include a network interface card in an end system, an interface port on a switch, and the connecting between them. An internetwork may have more than one edge interface.

The internetwork access sub-system includes those internetwork entities that are always under the full 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 that are not under its direct control.

A zone will include at least one instance or an internetwork. If a zone includes more than one internetwork, then IBSs provide the required connectivity between the internetworks. A zone may use multiple internetworks to segregate traffic and provide additional defence in depth. Multiple internetworks may also exist within a zone when existing network infrastructures are combined to create a zone.

4.2.3 INTERNAL BOUNDARY SYSTEM

An IBS provides a network interface between internetworks and 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 the zone has more than one internetwork; those interworks must be connected. Examples of IBSs include protection systems, such as screening routers, firewalls, intrusion prevention systems (IPS), and unified threat management (UTM) products.

An IBS could be a network, but such a network is not a distinct zone.

4.3 FUNCTIONAL REFERENCE MODEL

The functional reference model describes how the requirements for zones are structured. The model identifies and defines the different types of requirements. The requirements structure is the basis for annexes A to E of this document.

The functional reference model includes the security requirement components listed in Table 3.

Table 3: Functional Reference Model: Security Requirement Components

Security Requirement Component	Description
Network interface requirements	The set of security requirements governing the types of interfaces permitted with other zones. Network interface requirements delineate the perimeter of a zone. These requirements address issues such as the permitted interfaces to other zones, the use of common infrastructure, and the sharing of end systems with other zones.
Traffic control requirements	The set of security requirements governing the flow of network traffic within a zone and between a zone and other zones. These requirements address issues such as types of traffic, network access control requirements, non-interference rules, quality of service, traffic content rules, and resource consumption constraints.
Network configuration requirements	The set of security requirements governing the connection of devices to a zone. These requirements address the management of associations between network entities, data-link entities, and physical interfaces and nodes. The management and control of physical transmission media are also included in these requirements.
Host configuration requirements	The set of security requirements governing the configuration management of the hardware and software load on each host. These requirements ensure that each host operates within a known security state and does not pose a threat to the other hosts in the network. These requirements do not address which software may be on a host. However, they do address the actions necessary to ensure the software load is in a secure state (e.g. properly patched and configured).
Data protection requirements	The set of security requirements governing the assignment and use of security services to provide data protection services.

4.3.1 NETWORK INTERFACE REQUIREMENTS

Network interface requirements define constraints on the perimeter of a zone. You can think of network interface requirements as a set of connection rules for a zone. The following requirements are the basis for Annex F of this document. These requirements fall into one of the following categories:

- Requirements for ZIPs (see section 3.2.1) that define the controls on network-layer interfaces with other zones;
- Requirements for interfaces to underlying communications infrastructure (e.g. interfaces to data communications carriers); or
- Requirements for end-system interfaces that define the types of end systems that may be attached to the zone and the constraints on these interfaces.

Network interface requirements address the following needs:

- Delineate the zone perimeter to ensure that the scope of the network security zone authority's accountability is clear; and
- Limit the types of interfaces supported by a zone to reduce the threat environment to which the zone is exposed.

4.3.2 TRAFFIC CONTROL REQUIREMENTS

Traffic control requirements specify safeguards that control the flow of traffic within a zone and between zones. Traffic control requirements also specify network capabilities that should be present to support the implementation of measures for platform, application, and system management. Table 4 includes the traffic control safeguards.

Traffic control requirements also specify the 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. Any zone should support the attachment of intrusion detection sensors within the zone.

Table 4: Traffic Control Safeguards

Traffic Control Safeguard	Description
Access control	Controls traffic based on source and destination addresses and types of service. Access controls are used to limit access to sensitive resources, limit the data communication protocols used within the zone, ensure non-interference between communities of interest, and localize the impact of security failures.
Entity authentication	Validates the authenticity of entities and establishes a security association between them. The primary purpose of entity authentication is to support access controls.
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.
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.
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 can block traffic to or from prohibited Internet protocol (IP) or media access control (MAC) addresses or TCP ports. Filters can block prohibited protocols (e.g. firewall products) and stop malicious traffic that contains exploits or potential exploits (e.g. IPS products). They may also be used to filter traffic containing malware (e.g. anti-malware products) or dangerous or illicit content (e.g. web and email filtering products).
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[5]. This support may include traffic logs or attachment points for traffic monitoring sensors (e.g. a mirror port on a switch).
Address and name resolution security	Refers to a collection of safeguards to protect the integrity of the association between resources and their identifiers.
Resource encapsulation	Refers to the mechanisms that allow the zone to hide its internal structure. These mechanisms include network and port address translation and service mapping. Resource encapsulation supports access control and survivability.

[5] 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.

4.3.3 NETWORK CONFIGURATION REQUIREMENTS

Network configuration requirements specify the safeguards and the capabilities necessary to control the attachment and the removal of devices, such as end systems and networking equipment, from a zone. A zone offering a very high level of network security should implement mechanisms to authenticate all network and end-system interfaces before permitting the interface to participate in communications. A zone with a minimal level of security should implement safeguards to deter the attachment of unauthorized devices.

Network configuration safeguards include the following:

- Administrative controls (e.g. configuration identification, change control, configuration status reporting, and configuration audit);
- Physical security;
- Authentication; and
- Event logging.

To attack a network, a threat actor needs access to the network interface. A threat actor can access a network interface by attaching an unauthorized device to the network, exploiting an established host, or using an external interface. Network configuration controls either limit an attacker's ability to attach an unauthorized device to the network and to do so without detection.

4.3.4 HOST CONFIGURATION REQUIREMENTS

Host configuration requirements govern the configuration of the hosts that are attached directly and indirectly to a zone. Host configuration requirements do not specify measures 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 the end systems.

Host configuration requirements include the following safeguards:

- Administrative controls (e.g. configuration management, vulnerability management, and security audit);
- Access controls (including entity authentication);
- Physical security;
- Platform security measures; and
- Event logging.

4.3.5 DATA PROTECTION REQUIREMENTS

Within the context of this document, data protection requirements specify the safeguards and capabilities needed to protect the confidentiality, integrity, and availability of data during its transmission within and between zones.

5 SUMMARY

This document outlines the security objectives, along with the inherent configuration and management issues, related to applying a network security zone architecture to departmental or organizational networks.

The functional reference model included in this document describes how the requirements for the zones are structured and identifies and defines the different types of requirements. This reference model is the basis for a defence-in-depth architecture approach, which, when implemented rigorously, provide secures data and processes against cyber threats.

Your organization can use the guidance in this document to implement a network security zoning model that offers a structured approach, which you can tailor to meet your security needs.

5.1 CONTACT INFORMATION

Contact us for more information on network security zones:

Contact Centre
contact@cyber.gc.ca
Local: (613)-949-7048
Toll Free: 1-833-CYBER-88

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
CMVP	Cryptographic Module Validation Program
COMSEC	Communications Security
CSE	Communications Security Establishment
CSO	Chief security officer
DDoS	Distributed denial of service
Dept.	Department (appears only in figures)
DMZ	Demilitarized zone
DNS	Domain name service
DoS	Denial of service
DSA	Director service agent
EAN	External access network
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GC	Government of Canada
HRZ	Highly restricted zone
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
IAN	Internet area network
IBS	Internal boundary system
ICMP	Internet control message protocol
IDS	Intrusion detection system (appears only in figures)
IP	Internet protocol
IPS	Intrusion prevention system
IPSec	Internet protocol security
ISO	International Organization for Standardization
ISSIP	Information system security implementation process
IT	Information technology
ITS	Information technology security
KVM	Key-video-mouse
LAN	Local area network

MAC	Media access control
MITS	Management of information technology security
MZ	Management zone
NTP	Network time protocol
OSI	Open systems interconnection (model)
OZ	Operations zone
PAZ	Public access zone
PKI	Public key infrastructure
PoP	Point of presence
PZ	Public zone
RCMP	Royal Canadian Mounted Police
REZ	Restricted extranet zone
RMAZ	Restricted management access zone
RZ	Restricted zone
SA&A	Security assessment and authorization
SNMP	Simple network management protocol
SSL	Secure sockets layer
SVPN	Secure virtual private network
TBS	Treasury Board of Canada Secretariat
TCP	Transmission control protocol
TLS	Transport layer security
TRA	Threat risk assessment
URL	Uniform resource locator
UTM	Unified threat management
VA	Vulnerability assessment
VLAN	Virtual local area network (appears only in figures)
VPN	Virtual private network
ZIP	Zone interface point

6.2 GLOSSARY

Some of the definitions used in this glossary have been adopted from recognized sources, which are referenced.

Term	Definition
Authentication	The process of verifying an identity claimed by or for a system entity [14].
Authorization	Access privileges granted to a user, program, or process [15].
Baseline security requirements	Minimum security functionality required to meet the requirements of the TBS *Policy on Government Security* [2] and its associated operational standards and technical documentation.
Boundary	A portion of the perimeter of a zone or network that is the point of connection between two zones or networks.
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 [14].
Distributed denial-of-service (DDoS) Attack	An attack in which multiple systems, usually compromised, are used to target a single system, causing a denial of service. Victims of a DDoS attack consist of both the end-targeted system and any systems maliciously used in the distributed attack [7].
Edge interface	A network-layer service interface point through which an end system, IBS, or ZIP attaches to a zone internetwork.
Electronic service delivery	The provision of GC information and transaction services online to citizens, businesses, other governments, non-governmental 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.
End system	A system that, for an instance of communication, is the ultimate source or destination of the communication.
End-to-end encryption	Confidentiality service provided by encrypting data within, or at the source of, an end system with corresponding decryption occurring only within or at the destination end system [9].
Entity	An active element of a system (e.g. an automated process, a sub-system, a person, or a group of persons) that incorporates a specific set of capabilities [14].
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 or 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 the kinds of traffic that may pass between the two.
Gateway	An intermediate system that is the interface between two computer networks [14].
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

Term	Definition
	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 [14].
Host	A computer that is attached to a communication subnetwork or internetwork and that can use network services to exchange data with other attached systems [14].
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.
Internal boundary system	A gateway that connects two or more internetworks within a network security zone.
Internet	The single, interconnected, worldwide system of commercial, governmental, 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. (Definition adapted from [14]).
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. (Definition adapted from [14]).
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 accidental, erroneous, or unauthorized use of an information system [15].
Malware	Short for malicious software. Software (e.g. logic bomb, trojan, virus, worm) that is intentionally included or inserted in a system for a harmful purpose. (Definition adapted from [14]).
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 [14].
Need to know	Access to (including knowledge of) sensitive information, which is restricted to those whose duties require such access.
Network security zone authority	The person(s) 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 normally not be called hosts.
Peer-entity authentication	The corroboration that a peer entity in an association is the one claimed [14].
Platform	Specific computer hardware, as in the term, *platform-independent*. It may also refer to a specific combination of hardware and operating system or compiler (e.g. this program has been ported to several platforms). It is also used to refer to support software for an activity (e.g. this program provides a platform for research into routing protocols).

Term	Definition
Perimeter	An imaginary connecting line around a set of network components that defines the components contained in the zone.
Point of presence	An artificial demarcation point or interface point between communications entities [5].
Protocol	A set of rules (i.e. formats and procedures) to implement and control some type of association (e.g. communication) between systems. A series of ordered steps involving computing and communication that are performed by two or more system entities to achieve a joint objective [14].
Proxy service	An application-service internetworking 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, and 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 PAZ). 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]) rather than a VPN based 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, ensure compliance with established policy and operational procedures, detect breaches in security, and recommend any indicated changes in control, policy and procedures [9].
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 a set of system entities that have the right to access the resources [14].
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) [14].
Sensitive (information)	Information is sensitive if disclosure, alteration, destruction, or loss of the information would adversely affect the interests or business of its owner(s) or user(s) [14].
Separation of duties	A security principle requiring that the responsibilities for an activity of a sensitive or critical nature be distributed among multiple entities (e.g. staff, processes) to 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 the zones in which it participates.
Strong authentication	An authentication process that uses cryptography (particularly public key certificates) to verify the identity claimed for an entity [14].
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 introduces a higher level of security by incorporating communication- and application-derived state and

Term	Definition
	context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated.
Subnet	Short for subnetwork. A portion of a network, which may be a physically independent network segment, that 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 internetwork.
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 [4].
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	A network firewall that has many features in one product, including email filtering, anti-malware capability, intrusion detection or prevention, and World Wide Web content filtering, along with the traditional activities of a firewall. (Definition adapted from [6]).
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 (e.g. the Internet), often by using encryption (located at hosts or gateways), and tunnelling links of the virtual network across the real network [14]. In general terms, a VPN often refers to a network that emulates a private network, although it runs over public network lines and infrastructure.
Vulnerability	A weakness or gap in protection efforts of a network, a system, or an IT asset [4].
Zone interface point	An interface between two network security zones through which traffic may be routed.

6.3 REFERENCES

Number	Reference
[1]	Treasury Board of Canada Secretariat. *Policy on Service and Digital*. 1 April 2020.
[2]	Treasury Board of Canada Secretariat. *Policy on Government Security.* 1 April 2012.
[3]	Treasury Board of Canada Secretariat. *Directive on Security Management.* 1 July 2019.
[4]	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. 30 June 2015.
[5]	Canadian Centre for Cyber Security. *TRA-1 Harmonized Threat and Risk Assessment Methodology*. 23 October 2007.
[6]	Wikipedia. "Unified threat management".
[7]	Webopedia. *IT Business Edge*. "DDoS attack – Distributed Denial of Service". 2015.
[8]	Department of Defense (U.S.). *Department of Defense Instruction 8500.01: Cybersecurity*. 14 March 2014.
[9]	International Organization for Standardization. *ISO 7498-2:1989 Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*. February 1989.
[10]	SHIREY, Robert W. *The Internet Society*. "Request for Comments: 4949 – Internet Security Glossary, Version 2". Aug 2007.
[11]	Committee on National Security Systems. National Counterintelligence and Security Center. *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009*. 26 April 2010.
[12]	Canadian Centre for Cyber Security. *ITSG-31 User Authentication Guidance for IT Security.*
[13]	Rekhter, Y., Moskowitz, B., Karrenberg, D. et al. *The Internet Society.* "Request for Comments: 1918 – Address Allocation for Private Internets". February 1996.
[14]	Royal Canadian Mounted Police. *G1-026 Guide to the Application of Physical Security Zones.* September 2005.
[15]	Treasury Board of Canada Secretariat. *Guidelines on the Management of Public Key Infrastructure in the Government of Canada.* January 2011.
[16]	Treasury Board of Canada Secretariat. *Operational Security Standard on Physical Security.* 18 February 2013.