Office of the Chief Information Officer

ENTERPRISE IT SECURITY ARCHITECTURE SECURITY ZONES: NETWORK SECURITY ZONE STANDARDS

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC

People ● Collaboration ● Innovation

Version 2.0

July 20, 2012

Table of Contents

Date	Author	Version	Change Reference
10/25/2011	Christopher Lyons	3.0	Draft for ASRB review
11/08/2011	Christopher Lyons	3.1	Changes proposed by Ronald Warden
12/15/2011	Christopher Lyons	3.1	Removal of vendor references as per Malcolm McGregor.
12/23/2011	Christopher Lyons	3.1	Changes proposed by ISB
1/9/2012	Christopher Lyons	3.1	Changes proposed by David Steffy
1/12/2012	Christopher Lyons	3.1	Formatting
2/6/2012	Christopher Lyons	3.2	Replaced figure 2 diagram
2/15/2012	Christopher Lyons	3.2	Updated IP or port from zone B to Internet
4/25/2012	Christopher Lyons	3.3	Removed access from Zone B to Internet and B to SPAN
4/27/2012	Christopher Lyons	3.3	Updated Introduction
7/17/2012	Christopher Lyons	4.0	Minor updates throughout
9/25/2012	Christopher Lyons	4.1	Updated to include cases for zone B to Internet and update terms.
10/02/2012	Christopher Lyons	4.1	Modified Zone C to be only trusted device & trusted user

1 Foreword

Between 2005 and 2007 considerable work was conducted to develop an Enterprise IT Security Architecture (EITSA) as part of the Security Enhancement Project (SEP). The architectures described in the draft documentation were not considered mandatory for core government, and the EITSA was not formally published. The broad architectures described in the EITSA serve as the foundation of this standard, and also served as the mandatory security architecture for the SSBC Managed Services Environment with the STMS datacenter design. The EITSA was not published and therefore is not a publicly available document.

The Government of BC has traditionally invested heavily in perimeter security where firewalls and Intrusion Prevention Systems have been intended to provide the bulk of Government's data protection. Government collaboration with external partners has been carefully funnelled through 3rd Party Gateways with extensive security controls. The EITSA was written with the goal of moving Government towards a Defense In Depth posture where many layers of defense from the perimeter right down to the data encryption all play a role in protecting the enterprise Information Assets.

2 Introduction

This standard recommends dividing or segmenting the enterprise network into secure network segments or "Security Zones" as an important step in creating a secure layered network infrastructure that is consistent with moving security controls closer to the data that they are intended to protect.

The boundary controls employed to create and secure these zones and other associated network security services are included in this standard. The Zone model is consistent with the best practises of Defense in Depth.

In addition to the Network Security Zones standard, host-based firewalls, encryption, secure data protocols, data loss prevention, and data-level authentication are also considered critical to a long term successful information security strategy.

The main body of this document contains informative descriptions that support the implementation of this standard.

2.1 Classification

The proposed standard is classified as follows:

Table 1

Standard	Type	Nature	Review	Scope
Network Security Zones	Technical	Tactical	Annual	Enterprise IP networks, including those provided by ASD partners.

3 Scope

This document applies to government. It:

1. Specifies standard for the Network Security Zones; and

2. To the entire Government of BC enterprise network, including services delivered by ASD partners.

This document does not apply to:

1. Private and public entities which are not directly under the control or governance of the Government of BC; and

2. Existing legacy mainframe; and

3. Services that are provided by third parties and delivered across the Internet (public cloud services).

4 Normative references

International Standards

- ISO 27002:2005

OCIO IM/IT Standards Manual
http://www.cio.gov.bc.ca/local/cio/standards/documents/standards/standards_manual.pdf

- Cryptographic Standards for Information Protection (section 6.10)
- Interim Standards for Information Systems Security and Network Connectivity (section 6.4)
- Standard for Information STRA Methodology, Process and Assessment tool (section 6.11)
- Physical Security Technical Standards
- Web Content Filtering (sections 1.1, 6.2 and 6.3)

Information Security Policy **http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/isp.pdf**

- Information Security Classification Framework

Information Management Standards
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

- Ministries must ensure all government technology and information is managed in line with Government Core Policy Manual Chapter 12 Information Management and Information Technology Management,.

5 Terms and Definitions

For the purposes of this document, following acronyms apply.

Table 2

Acronym		Comments
ACL	Access Control List	
DLP	Data Loss Prevention	
DMZ	Demilitarized Zone	
EITSA	Enterprise Information Technology Security Architecture	
FQDN	Fully Qualified Domain Name	
IPS	Intrusion Prevention System	
ISCF	Information Security Classification Framework	
MPLS	Multi-protocol Label Switching	
NAT	Network Address Translation	
SAG	Secure Access Gateway	
SPI	Stateful Packet Inspection	
STRA	Security Threat Risk Assessment	
VLAN	Virtual Local Area Network	
VPN	Virtual Private Network	
VRF	Virtual Routing and Forwarding	
	Firewall Rules	A system of security rules that control by blocking or allowing communication between trusted and untrusted network segments or hosts.
	Information Asset	Any data created, processed and used by the Government of BC.
	Network Security Zone	A physically or logically isolated network consisting of network interfaces with similar security requirements or profiles.

6 Requirements

1. Information Assets classified in accordance with ISCF will determine the appropriate level of security measures needed to protect the asset.

2. Information Assets are periodically monitored to determine the effectiveness of the measures and controls in place with particular focus on those assets deemed High Security.

3. The Security Threat Risk Assessment (STRA) must be used by the Information Asset owner to evaluate the risk associated with a given service, or the information associated with a service. This standard is to be used in conjunction with the information security classification and security threat risk assessment.

4. Staff accessing the information through the network must complete all steps required in Core Policy and regulations required to have access to Government data.

5. All documentation to support the above four points have been completed, authorized and stored according to Core Policy and regulations.

7 General characteristics

7.1 Enterprise Security Model

The security controls employed by the BC Government have been divided into four logical groupings:

1. Boundary Layers (network segmentation, security zones, network firewalls, network IPS, anomaly detection, proxy/reverse proxy, network encryption, network access control, content filtering)

2. Trust Levels (device and user validation, user authorization, data level authentication)

3. Platform Hardening (host/application firewall, patch management, malware protection, data encryption, host IPS), and

4. Security Management (vulnerability management, asset management, security information management, review controls).

7.1.1 Overview of Network Security Zones

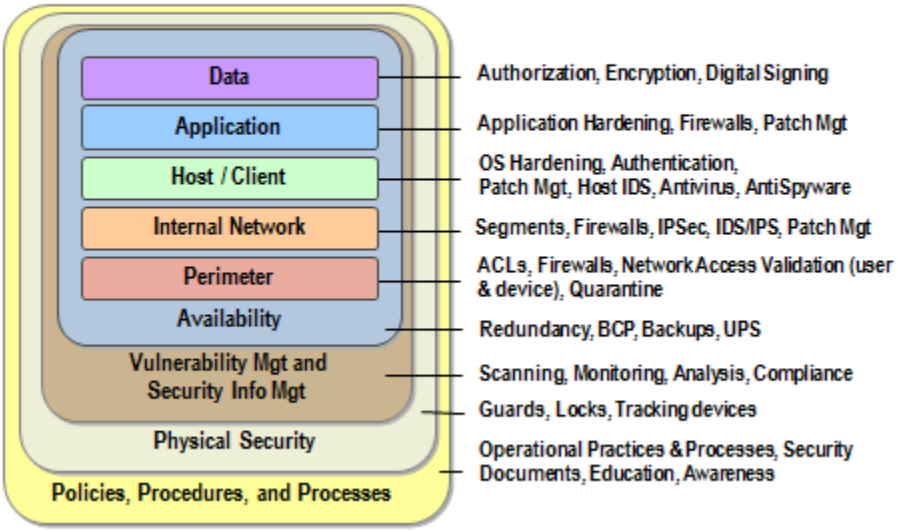

Figure 1

This Network Security Zone standard applies to the Perimeter and Internal Network controls as reflected in Figure 1 and utilizes network segmentation to create clearly defined Security Zones. The concept of Security Zones is an IT industry, widely accepted best practice for establishing security boundaries, control points and accountabilities. A Security Zone is a logical entity containing one or more types of services or entities. Security Zones group together those entities with similar security requirements and levels of risk. Further segmentation within the Zones is supported to allow each service and businesses program the level of security isolation they require.

Segmenting networks into well-defined Security Zones involves a number of different security controls working in concert. On a local switch, VLANs are used to isolate user groups with Virtual Routing Forwarding (VRF) instances providing policy enforcement. All routing between zones is done with firewalls and security is enhanced through the additional use of intrusion prevention systems (IPS) and anomaly detection for stronger policy enforcement. Over the wide area network, technologies like multi-protocol label switching (MPLS), and virtual private networks (VPN) are used to isolate traffic and provide geographic extension of different security zones. Datacenter to datacenter zone extensions must be encrypted when required by the data classification except in situations where dedicated private network facilities are used. Inter-zone security controls are discussed in subsequent sections of this document.

This standard defines several Zones and an associated operations management layer or plane. (See Figure 2, Security Zones: Connectivity) The architecture supports the classic network Zones such as the Demilitarized Zone (DMZ) and the Internet Zone. It also supports Zones internal to the government

network such as its shared ISP-like service called SPAN/BC, an Extranet Zone for connectivity with business partners of IT services. In addition, the Zone model provides internal Zones at its core; the Restricted High Security Zone (Zone A), the High Security Zone (Zone B), and the Trusted Client Zone (Zone C). Other Zones that are not reflected in figure 2 include Trusted User (BYOD) Zone, PCI Zone, Guest Zone (Internet only), Building Utility Services Zone, PLNet Zone, Pharmanet Zone, BPS Zone and a Collaboration Zone for edge servers and infrastructure associated with unified communications and collaboration. Lastly, the zone model supports a highly restricted and segmented operations management layer to provide the administrator access required to service the core infrastructure as well as the business applications.

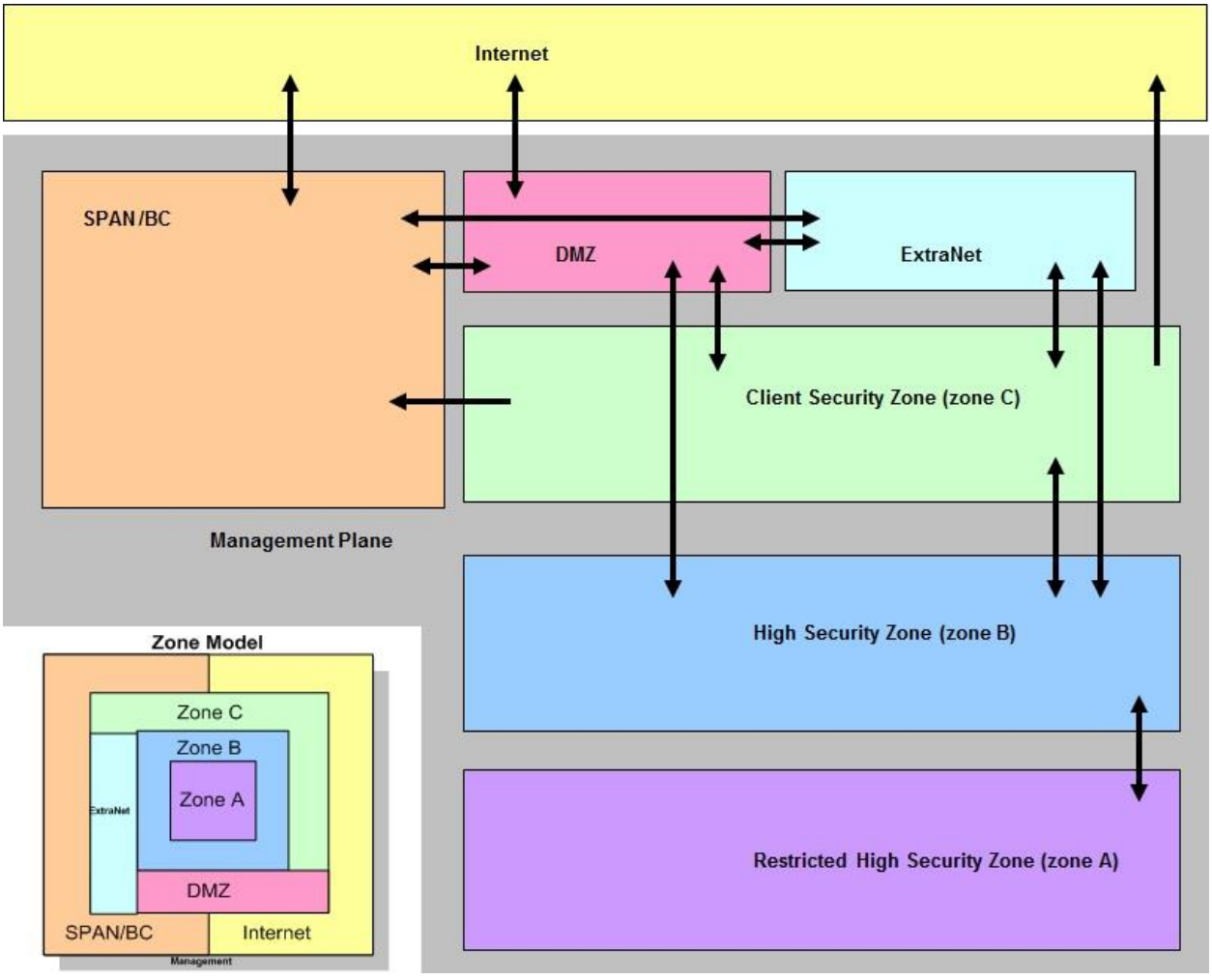

Figure 2 - Security Zones: Connectivity

The objective of the internal zones A, B and C are to provide increasing levels of security by limiting their visibility and connectivity to other zones and their associated devices.

7.1.2 Summary

The fundamental zone connectivity concepts for the security zones model are:

- Not all Zones are visible to all other Zones; only Security Zones adjacent to one another may initiate or service communication requests and as a result, there is no Security Zone "hopping". E.g., desktops in the Trusted Client Zone cannot directly initiate a session with the application data stored in a server in the Restricted High Security Zone as they are not adjacent.
- Zone extensions (eg. Zone B in the Calgary datacentre to Zone B in the Kamloops datacentre) must be encrypted when required by the data classification framework except in situations where dedicated private network facilities are used.
- The session initiation between the security zones may or may not be bi-directional with an adjacent security zone. E.g., a desktop in the Trusted Client Zone can initiate a session with the Internet, but devices on the Internet cannot initiate a session with the Trusted Client Zone desktop.
- The datacenter **Management Plane** is physically separate from other Zones, and it is internally segmented. Each server's dedicated network interface is on its own segmented network and interfaces on the Management Plane networks do not have visibility to each other.
- All traffic that transits a Security Zone boundary must pass firewall rules, IPS and anomaly detection.
- All Internet bound traffic sourced from Zone C, Trusted User Zone, Guest Zone or the PLNet Zone must pass through content filtering in accordance with the BC Government standard on Web Content Filtering.

7.2 Detailed Characteristics and Standard

7.2.1 Zone Constructs

7.2.1.1 Management Plane

There are multiple Management Planes used by the Government of BC and its ASD partners. This document is specifically concerned with the Management Plane in the datacenter.

In the datacenters the Management Plane:

- Is a construct that is used for performing backups and patch management.
- Is used for all server administration within datacenters.
- There is no direct access to the Management Plane.
- All access to the Management Plane is achieved through a dedicated Secure Access Gateway (SAG) service.
- IP addresses used in the Management Plane do not have Internet routing.

7.2.1.2 SPAN/BC

The Shared Public Access Network is an ISP-like service where public entities connect to government resources. SPAN is a network that hosts both trusted and un-trusted end-points.

7.2.1.3 DMZ

The DMZ is populated with proxies, web gateways, and other citizen facing interfaces.

Servers and application residing within the DMZ may be Internet accessible and require tighter host and application controls than Zone A and Zone B servers.

Internet facing applications must undergo an Application Vulnerability Scan prior to be placed in the DMZ.

Servers cannot be in IDIR domain if they are in the DMZ. Servers in the DMZ are in the .DMZ domain. A trust relationship exists between IDIR and the DMZ domains.

7.2.1.4 ExtraNet

The ExtraNet zone serves as a landing point for business partners who require connectivity to internal government services.

All ingress and egress traffic from the ExtraNet Zone must pass through a third party gateway equivalent infrastructure.

7.2.1.5 Trusted Client Zone (zone C)

Zone C is the Trusted Client Zone. All Zone C end-points are managed by Government and used by trusted users (IDIR).

7.2.1.6 Trusted User (BYOD) Zone

The Trusted User (BYOD) Zone is for end-user devices that are authenticated to the network with IDIR credentials.

7.2.1.7 High Security Zone (zone B)

Zone B is populated with applications, or databases with data that has a security classification of Low or Medium. High security data may reside in the High Security Zone upon completion of a Security Threat Risk Assessment and following risk acceptance by the information owner.

7.2.1.8 Restricted High Security Zone (zone A)

Zone A is populated with information, applications or databases with data that are classified as High security according to the Information Security Classification Framework (ISCF).

7.2.2 Standard Elements

7.2.2.1 Secure Access Gateway (SAG)

The Secure Access Gateway is a hardened Virtual Desktop or Terminal Services based service that is used to administer applications or data in the datacenter. The Secure Access Gateway should be used to administer applications or databases that reside on servers in the Restricted High Security zone and may be used to administer databases or applications in any datacenter zone.

The SAG service design requirements include:

Connections to the SAG must be made from Zone C or via a VPN that terminates in Zone C.

The SAG service is the best practice for administering applications and databases in Zone A.

The SAG service may be used to administer applications or databases in any zone that is adjacent to Zone B as show above in Figure 2.

SAG users must authenticate against IDIR.

Authentication must not pass through from the end-user localhost session to the SAG session.

The SAG service must have the capability to support multi-factor authentication.

The SAG service must log all connections and session details including failed connection attempts with accurate time stamps.

The desktop delivered by the SAG service must reside in Zone B and will be subject to all Zone B rules as defined in this standard.

The SAG must provide a mechanism to restrict user inter-zone and intra-zone access based on static IP address or VLAN assignment.

The desktop delivered by the BC SAG must follow a regular patching schedule, maintain up to date anti-virus protection, host-based firewall, and support session timeout.

Controls must be in place between the end-user localhost and the SAG desktop to restrict the ability to cut-and-paste or transfer files between the two environments. There must be no direct file transfer access from the user desktop to the SAG. Any file transfer must be in a secure and auditable manner.

The SAG must allow for client specific builds based on user requirements for specific management software.

Modifications to the SAG must not persist across sessions. Changes to the SAG client specific builds must be facilitated by the administrator of the SAG service.

7.2.2.2 Servers

Servers, both dedicated and virtual, can reside in only one non-management zone. A server may not exist in both the High Security Zone and the DMZ at the same time. Virtual Servers sharing a common Hardware or Virtual Operating System must reside on the same Zone.

7.2.2.3 Switches

Access and virtual access switches can reside in only one non-management zone.

A switch may not exist in both the High Security Zone and the DMZ at the same time.

Virtual Switches sharing a common Hardware or Virtual Operating System must reside on the same Zone.

Core and aggregation switches may reside in more than one zone.

7.2.2.4 Network Firewalls

Within the Government of B.C.'s security zone model, network firewalls are a key tool used to control the flow of communication between security zones. Additionally, firewalls may be employed to provide or support other functions such as network address translation (NAT), stateful packet inspection (SPI), device validation, and virtual private network (VPN) services.

7.2.2.5 Host Firewalls

Host firewalls must be configured on all servers that operate outside the SSBC datacenter and should optionally be configured on servers within the datacenter based on the sensitivity of applications and the particular threats presented to that server.

The host firewall on servers should be centrally managed, with the ability to monitor and report security events.

Firewall rules must support configuration based on source and destination IP address and port number for incoming and outbound traffic.

7.2.2.6 Network IDS/IPS

Within the architecture, network IDS/IPS are used to provide general network awareness, detection, notification, and blocking of attacks.

At a minimum, IDS/IPS must be used at the perimeter edges and key boundaries within the enterprise network.

A key boundary may be a physical location where all traffic is inspected, regardless of zone such as in the case of the SSBC datacentre, or the key boundaries may be based on network zones.

7.2.2.7 Proxy/Reverse Proxy

Within the architecture, proxy services are employed primarily in the DMZ to allow applications located within security zones to isolate themselves from untrusted clients or devices requesting their services.

A proxy service can be used to facilitate software updates and license validation for applications in zones A and B.

To prevent compromise of the security zone connectivity rules, proxies may also be employed to support single or two-tiered application that wish to leverage the High Security and Restricted High Security zones.

7.2.2.8 Network Encryption

As a minimum, encryption and its use must comply with the Cryptographic Standards for Information Protection.

7.2.2.9 Access (Wired, Wireless, and Remote)

All devices requesting access to the network require validation. The minimum level of validation is dependent on the device and entry point or zone used to gain network access. Each Security Zone's "access" policy relates to the Zone's base security requirements and is strictly enforced.

The architecture provides support for network access via wired, wireless and remote services. Restrictions apply to some configurations of network access, as is required to support the enterprise Security Zones model. For example, access to the "High Security Zone (zone B)" from the Internet via remote services will not be supported. Those business solutions requiring such connectivity will need to leverage an alternative access solution like; web based proxy or Secure Access Gateway services.

7.2.3 Inter-zone Connectivity

Connectivity between zones is subject to principles of adjacency (no zone hopping), rules may be asymmetric, and intra-zone communications will in some cases be restricted. The following table contains the standard for access controls and the description of the minimum connectivity rules:

Table 3

To / From	Restricted High Security (A)	High Security Zone (B)	Clients (C)	DMZ	ExtraNet	SPAN/BC	Internet
Restricted High Security (A)	Destination IP address **AND** Port #	Destination IP address **AND** Port #	No Access	No Access	No Access	No Access	No Access
High Security Zone (B)	Destination IP address **AND** Port #	Destination IP address **OR** Port #	Destination IP address **OR** Port #	Destination IP address **AND** Port #	Destination IP address **AND** Port #	No Access	No Access
Clients (C)	No Access	Destination IP address **OR** Port #	No Restrictions	Destination IP address **OR** Port #	Destination IP address **OR** Port #	No Restrictions	No Restrictions (except Internet Policies)
DMZ	No Access	Destination IP address **AND** Port #	Destination IP address **OR** Port #	Destination IP address **AND** Port #	Destination IP address **OR** Port #	No Restrictions (except Internet Policies)	No Restrictions (except Internet Policies)
ExtraNet	No Access	Destination IP address **AND** Port #	Destination IP address **OR** Port #	Destination IP address **AND** Port #	No Restrictions	Destination IP address **OR** Port #	No Access
SPAN/BC	No Access	No Access	No Access	Destination IP address **OR** Port #	Destination IP address **OR** Port #	No Restrictions	No Restrictions
Internet	No Access	No Access	No Access	Destination IP address **OR** Port #	No Access	No Restrictions	n/a
Mgmt	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Restrictions - Management functions only	No Access	No Access

Note that the table references port numbers, but some protocols do not use ports. In some cases a protocol may be defined if that protocol does not use ports. This table describes minimum rules for a specific source IP address (ie. server) within a Zone. Additional restrictions may be applied across and within Zone boundaries based on a business requirements and threat risk assessment.

7.2.4 Intra-Zone Connectivity

Within a given security zone, there are additional segments or partitions. The segmentation of networks within a zone may be accomplished through the use of VLANs. These segments are used, for example, to isolate different classes of hosts that have no requirement to interact with each other. This principle of least privilege helps to contain the damage in the event that any given system is compromised. Instead of VLANs, host based firewalls may be used to protect hosts within a common Zone. The following diagram provides a conceptual view of how the High Security and Restricted High Security zones could be partitioned:

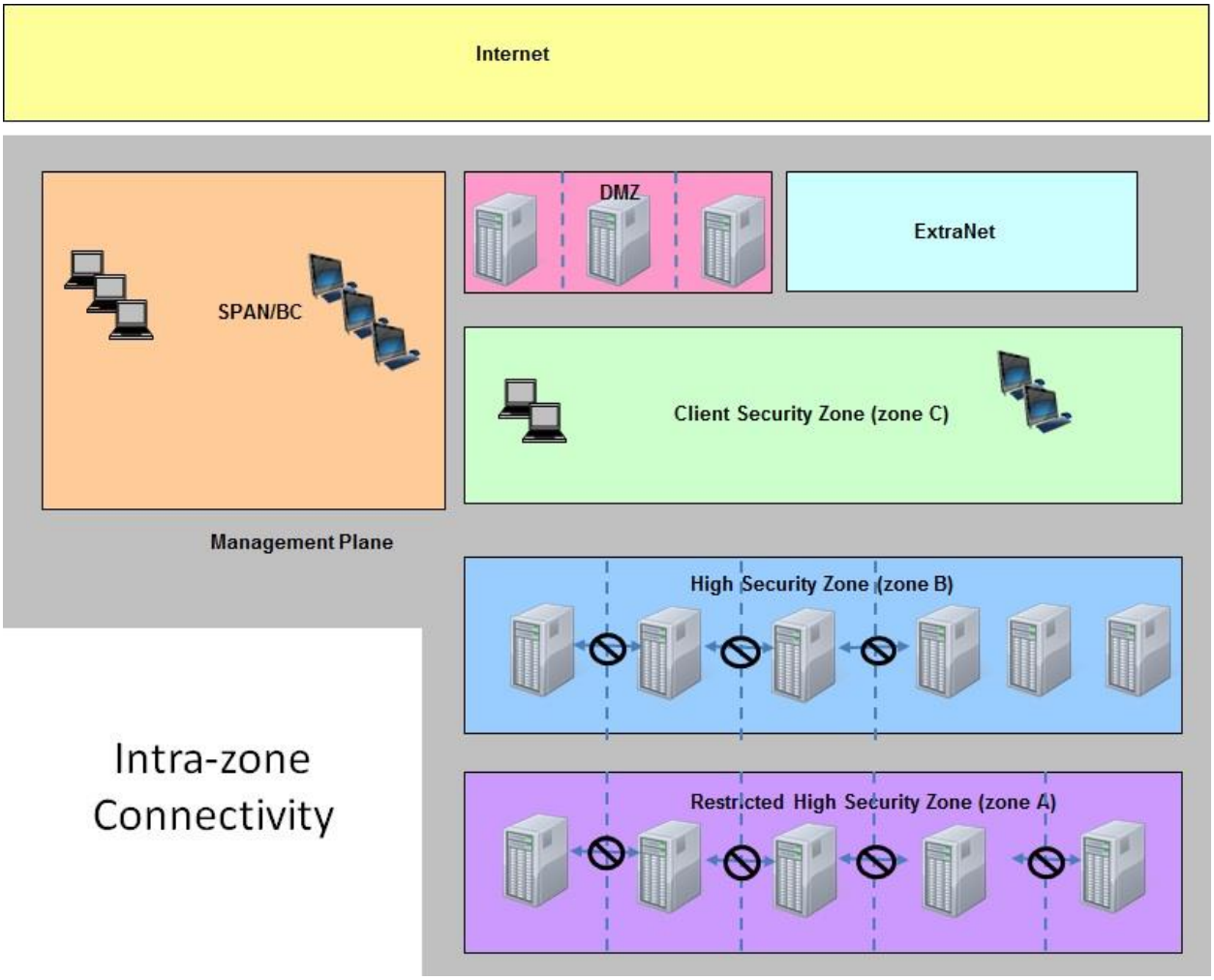

Figure 3

For simplicity, figure 3 does not attempt to show supporting security elements such as firewalls, intrusion detection systems or content filters. Intra-zone communication between sub-zones is denied by default, and subject to the minimum security configuration outlined in Table 3.

Each partition within a zone is a separate VLAN or MPLS-VPN.

7.2.5 Enforcement

Information owners define the information security classification of the assets that they are responsible for. The information owner in conjunction with the application or database administrator determines the appropriate zone placement. HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard. The Information Asset owner is responsible to ensure that a periodic validation of the configured firewall rule set is compared against the rules that have been requested for the application or database.

Zone B Access to the Internet

Some applications will require access to resources on the Internet. License validation and downloading application updates are examples where applications may require access to the Internet. Due to the dynamic nature of content distribution networks it may be difficult to identify specific IP addresses or even network ranges that need to be accessed by a specific application, therefore it is desirable to filter Internet traffic outbound from zone B based on URL. This may be accomplished by using the SSBC provided forward proxy service. In the event that an application requires Internet access and cannot be configured to use the forward proxy service, then the public IP address must be obscured using NAT.

- The default for zone B applications is No Access to the Internet.
- Applications that require access to the Internet from zone B should be deployed in such a way that the application owner leverages a proxy server in the DMZ.
- Access to the Internet for applications from zone B for applications that use HTTP or HTTPS may use the SSBC forward proxy service.
- In the event that an application is unable to use the SSBC proxy service and the application owner deems that it is impractical to host their own proxy service in the DMZ, then the application owner may request that SSBC grant an exception to allow the specified zone B application access to the Internet. The exception process differs from the exemption process.
- The exception request must include the name and IP address of the application. The name, telephone and email address of the application owner. Confirmation that the application requires Internet access and that the proxy service has been ruled out as an option and the reason for ruling out the proxy service as an option. Additionally the application owner must specify a destination port and IP address range that are required for their application.
- There will be no Zone B firewall rules that have a destination of any.
- In the event that an exception is made for a Zone B application the server's IP address will be NAT'd.

8 Evaluation criteria

8.1 Enquiry Scope

OCIO Information Security Branch, OCIO Architecture and Standards Branch, SSBC Network Services, SSBC Security Operations, SSBC Technology Solutions Division.

Annex A. Standard for Network Security Zones

IM/IT Architecture & Standards Manual STANDARD **Office of the Chief Information Officer** **Province of British Columbia**	**Effective Date:** 2012-10-18 **Scheduled Review: Biannual** **Last Updated:** 2012-10-18 **Last Reviewed:** 2012-10-11 **Type: Technical**
X.0 Information Technology Security (CPPM 12.3.6)	
X.Y Network Security Zone standard	
Keywords: Network, datacenter	

Description of Standard

The strategic aim of this standard is to support the Government's goals through improvements to IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support Province's business needs of the future.

This standard governs the separation and protection of government data networks according to zones that are based on the classification of the information assets that the zones and associated security controls are intended to protect.

Where to Apply This Standard

This standard applies where there is a need to isolate and segment the government's networks and and/or for the graduated protection of government applications and the data that those applications process. The zone required in any given network application is determined by business requirements, Security Threat Risk Assessment and Privacy Impact Assessment.

Authority and Exemptions

This standard has been issued by the Office of the CIO in accordance with the Core Policy and Procedures Manual Chapter 12.3.6, Information Technology Security and the Information Security Policy.

If there are compelling business reasons why an organization is unable to comply with this architecture or standard, the organization's CIO may authorize a submission for exemption through the ASB.

Metrics and Enforcement

Information owners define the information security classification of the assets that they are responsible for. The information owner in conjunction with the application or database administrator determines the appropriate zone placement. HP-AS defines firewall rules as requested by administrators. The information asset owner for the destination of firewall rule request is the approver and also responsible for ensure that firewall requests comply with this standard. The Information Asset owner is

responsible to ensure that a periodic validation of the configured firewall rule set is compared against the rules that have been requested for the application or database.

Terms and Definitions

See section 5 of the full standard for Terms and Definitions.

References

The full Network Security Zones standard is available on the intranet at:

<insert link to standard>

Additional Information

The OCIO is the owner of this standard. Its website is located at www.cio.gov.bc.ca

Contact

Architecture and Standards Branch, Office of the CIO

email: ASB.CIO@gov.bc.ca