IM/IT Architecture & Standards Manual STANDARD	Effective Date: 2008-11-10 Scheduled Review: Annual Last Updated: Last Reviewed: 2009-01
Office of the Chief Information Officer **Province of British Columbia**	**Type:** Technical, Product and Reference

5.0 Information Technology Management (CPPM 12.3.5)

5.8 Network to Network Connectivity

Keywords:

Description of Standard

This standard, which is composed of three sections, defines the connectivity requirements that must be addressed with respect to the connection between disparate networks. This includes connectivity to the SPAN/BC network and external service provider to external service provider networks.

1) Technical Standard:

a) Standard Components:

- **Connection Routers:** Each network to network connection must ensure appropriate logical, and if necessary physical, separation is achieved. A virtualized router may also be used, but logical separation needs to be guaranteed at all times (even in the event of device failure) through the use of appropriate controls.
- **Managed Router Access Control List (ACL):** The connection routers will be configured with a 'basic' ACL to deny/permit using the principle of least privilege, for access from the 3rd party network to the Provinces network or from 3-rd party network to another 3-rd party network. Separate ACL's, designed based on least privilege and using the "Deny All" as the default fall back rule, need to be configured and maintained on each interface in each direction (i.e. external vs. internal interfaces; inbound vs. outbound traffic directions) This access control list will be the first line of defense in a multi-layered protection strategy.
- **Firewall(s):** The firewall used must perform stateful packet inspection. Stateful Inspection Firewalls will be installed with the managed security rules permitting and denying access based on the principle of least access/privilege. **NOTE:** Devices that combine the Stateful Inspection Firewall and Routing functionality on one device are acceptable as long as the above requirements are met fully.
- **Intrusion Detection /Prevention System(s) (IDS/IPS):** IDS/IPS will be in place to monitor network traffic for security threats.
- **Content Filtering and Malware Protection:** Correction system(s) including content filters will be in place to screen for malicious code (viruses, etc.).

- **Data Leakage Protection**: Appropriate controls will be in place to ensure that data is prevented from being lost/leaked.
- **Proxies: (optional)** HTTP Proxy server(s) can provide user authentication and DNS name translation for HTTP traffic if required.

b) Security: The principles of least privilege will apply.

- All ports will be closed by default and all IP addresses will be hidden by default. Opening of ports and IP addresses are requested by the Contract manager and must be approved by the data owner and the Ministry owning the contract.
- Internal addresses will not be accessible by default. Requirements to connect to internal IP addresses will be addressed through the implementation of a Split DNS Service.
- Minimum AES 128 encryption will be used for encryption. Encryption using keys of less than 128 bits are not acceptable. DES is not an acceptable encryption standard. If using 3DES encryption standard, the minimum key required is 168bit. Acceptable encryption standards include: 128bit AES, 168 bit 3DES.

2) **Product Standard:**
When one end of the connection is the SPAN network, then the Third Party Gateway (3PG) service must be used.

3) **Reference Standard:**
ISO/IEC 18028-3:2005 - Securing communications between networks using security gateways – will serve as the reference standard for network to network connectivity, specifically, the ISO Screened Subnet model.

Where to Apply This Standard

The standard is meant for SSBC, any ministry, other public agency or external service provider that is considering interconnecting networks that carries public sector information.

Authority and Exemptions

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.

Special note: For the time being a pre-existing policy directive issued in 2004 (see item 2 under References) still requires anyone connecting external networks to SPAN/BC to seek an exemption from the OCIO (whether this connectivity standard has been met or not). It is the intent that at the completion of the Network BC Project (JSRFP) this 2004 directive will be retired.

Metrics and Enforcement

SSBC offers secure network to network connectivity through the 3rd Party Gateway Service. Details of this Shared Services BC service offering can be found on the SSBC client website (see Reference #1 below).

The intention of the OCIO is to advertise and promote this standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other provincial agencies are expected to adopt and monitor compliance to this standard. The OCIO Information Security Branch will also monitor for compliance.

Terms and Definitions

Any IM/IT security and network terminology found in this standard will be included in a consolidated Glossary which is currently under development by the OCIO.

References

1. A copy of the Submission for Network to Network Connectivity Technical and Product Standards can be found at www.cio.gov.bc.ca/local/cio/standards/documents/standards/n2n_connectivity.pdf
2. A memo from the Government Chief Information Officer (dated August 12, 2004) defined the Interim Standards for Information Systems Security and Network Connectivity. A copy of this document can be found at www.cio.gov.bc.ca/local/cio/standards/documents/standards/interim_n2n_standards.pdf
3. Security Schedule G: www.gov.bc.ca (TBD)

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, OCIO

email: ASB.CIO@gov.bc.ca