Digital Policy Office

INFORMATION SECURITY

Practice Guide

for

Internet Gateway Security

Version 2.1

July 2024

COPYRIGHT NOTICE

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	G50 Internet Gateway Security Guidelines version 5.0 was converted to Practice Guide for Internet Gateway Security. Please refer to the document with revisions marked at the government intranet portal ITG InfoStation: (http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	Whole document	1.0	December 2016
2	Updates were made based on the latest updates to IT Security Guidelines (G3) v9.0	5.1, 16, 22, 29-31, 33, A-2	1.1	June 2021
3	Updates were made based on the latest updates to IT Security Guidelines (G3) v10.0	2, 8-9, 11,12, 29-31	2.0	April 2024
4	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”)		2.1	July 2024

Table of Contents

1. Introduction

Any B/D that supports Internet facilities shall protect its information systems and data assets from unauthorised access or public break-ins. All Internet access from departmental network shall be made through centrally arranged Internet gateways or B/D's own Internet gateway.

This document provides technical guidelines on Internet gateway for secure Internet access and services. These guidelines represent what are regarded as best practices to maintain security risks at an acceptable level under the Internet open platform. It is intended for staff who are involved in the operational and technical functions of Internet gateway services.

As the materials included in this document are general in nature and are prepared irrespective of computer platforms, readers should consider and select those that are applicable to their own environment.

1.1 Purpose

This document addresses security considerations in the following major areas:

- Internet Gateway Overview
- Firewalls
- Routers
- Mail Gateway Security
- Web Security
- Remote Access
- Domain Name System (DNS) Servers
- Intrusion Detection and Monitoring
- Other Security Considerations

The purpose of this document is to provide information on some best practices on Internet gateways. It should be used in conjunction with established IT security policy, guidelines and procedures.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- "Security Regulations", the Government of the Hong Kong Special Administrative Region
- Baseline IT Security Policy (S17), the Government of Hong Kong Special Administrative Region
- IT Security Guidelines (G3), the Government of Hong Kong Special Administrative Region
- "Code on Access to Information", the Government of the Hong Kong Special Administrative Region. http://www.access.gov.hk/filemanager/content/codeonacctoinfo/code.pdf
- "Site Security Handbook", RFC2196, Internet Engineering Task Force (IETF). https://www.ietf.org/rfc/rfc2196.txt
- "The World Wide Web Security FAQ", the World Wide Web Consortium (W3C). https://www.w3.org/Security/faq/wwwsf1.html
- "Guidelines on Firewalls and Firewall Policy", SP 800-41, NIST. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
- "Email Bombing and Spamming", Software Engineering Institute. http://www.cert.org/tech_tips/email_bombing_spamming.html
- "Good Practices Guide for Deploying DNSSEC", ENISA. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec/at_download/fullReport
- "Guide to Intrusion Detection and Prevention Systems", SP 800-94, NIST. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
- "Zero Trust Architecture", SP 800-207, NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- "Selecting a Protective DNS Service", May 2021 Ver. 1.2, National Security Agency, Cybersecurity and Infrastructure Security Agency https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting-Protective-DNS_UOO11765221.PDF
- "Secure Domain Name System (DNS) Deployment Guide", SP 800-81-2, NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
- "Election Security Spotlight – Domain Name System (DNS), Center for Internet Security (CIS) https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-domain-name-system-dns

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3, and the following apply.

Abbreviation and Terms	
NA	NA

1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to :

Email: it_security@digitalpolicy.gov.hk

Lotus Notes mail: IT Security Team/DPO/HKSARG@DPO

CMMP mail: IT Security Team/DPO

2. Internet Gateway Overview

Internet gateway is an interface with dedicated Internet connection. It provides a point of connection with the Internet, no matter whether the interface has any connection with the internal departmental or government network. A secure Internet gateway can tighten the control and establish a more cost-effective and secure operation environment.

Because of the openness of the Internet and the rapid growth of complex network services and applications, the lack of security protection on the gateway may leave the internal network vulnerable to attacks. Hence, an Internet gateway should be properly configured with appropriate security measures to protect it from attacks.

B/Ds may leverage central Internet gateway hosted by DPO, but B/Ds remain ultimately responsible for ensuring that adequate security measures have been implemented.

In today's evolving cybersecurity landscape, it is important to consider emerging trends such as zero trust architecture when configuring an Internet gateway.

Zero trust architecture incorporates principles such as network segmentation, micro-segmentation, strong authentication, least privilege, continuous monitoring, and strong encryption to ensure a more granular, robust and dynamic security posture. It emphasises the importance of authentication, authorisation, and continuous evaluation of trust throughout the network.

Rather than solely relying on perimeter defences, zero trust architecture places equal importance on protecting data, applications, and users wherever they are located. This approach aligns with the evolving nature of modern networks, where resources are distributed across multiple environments, including cloud services, on-premises systems, and remote devices.

B/Ds need to recognise the limitations of perimeter-based architecture and consider adopting more advanced security frameworks, such aszero trust, to improve the security posture, detect and respond to threats more effectively, and adapt to the changing nature of today's interconnected and dynamic networks.

2.1 Interconnection of Networks

Setting up an Internet gateway often interconnects with internal networks in order to allow them to gain access to the service. However, considerable care should be exercised to ensure that interconnecting the network will not degrade or weaken the existing security level to an unacceptable level, or compromise the security of information processed. Hence, the connecting parties have to:

- Maintain their own specific security defences on their networks, hosts and systems.
- Maintain their own security policies and guidelines, and these policies and guidelines should be aligned with those on the Internet gateway.
- Set up stringent logical access controls to the Internet gateway.
- Establish security incidents handling and reporting procedures for the Internet access and services.
- Advise and train users to observe and follow the related security policy, guidelines and procedures.

2.2 Recommended Security Protection

It is recommended that a secure Internet gateway, merely offering Internet access services, should be equipped with the following security functions:

- Firewall (for access control).
- Packet-filtering router (for routing traffic and filtering packet).
- Intrusion Detection and Prevention System (IDPS) (for logging, monitoring, detecting and stopping attacks).
- Protection against malware (for monitoring network traffic, detecting malware, and preventing information systems from infection).

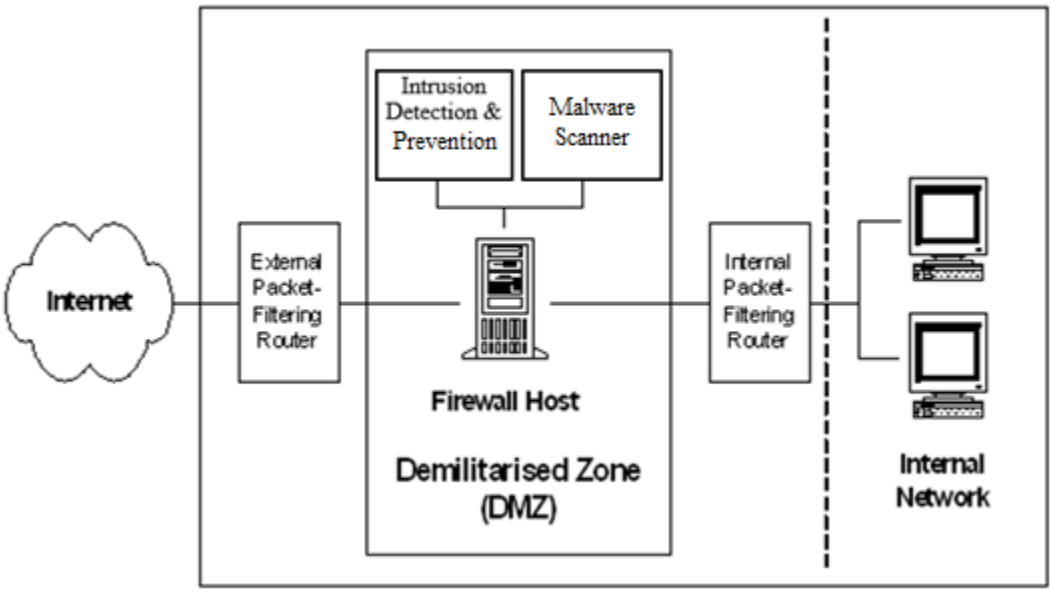

Figure 1 An Internet Gateway with Recommended Security Protection

Illustrated above is the recommended security protection required for an Internet gateway, which provides a channel for access from internet network to the Internet

without hosting any web servers or mail servers. The de-militarised zone (DMZ) is the area where security measures are placed.

A firewall host is deployed to filter out unauthorised or malicious traffic. It should be noted that a firewall is not the totality of security solutions. There are a number of things that a firewall cannot protect against, including but not limited to:

- Denial of service attacks and assure data integrity.
- Attacks from unwitting users.
- Attacks from malware.

That is why other security functions (such as intrusion detection and prevention, and malware scanning) should be used together. However, it is observed that the boundary between firewall and other security measures is becoming blurred as firewall manufacturers continuously incorporate additional features, e.g. Virtual Private Network (VPN), encryption, etc. to firewall.

Two packet-filtering routers (one external and one internal) are used to filter and route the selected traffic to the firewall from either external side or internal network. In order to connect to the Internet, the external packet-filtering router should be set up. The internal packet-filtering router is used to separate the DMZ segment (which will be explained in later sub-section) from the internal network. Unlike firewalls, these routers are normally considered as network devices with value-added security features rather than as security products.

The intrusion detection and prevention stated above refers to any means, such as tools or procedures, that can provide such functions, but may not be necessary a physical device. However, procedure-based mechanism to detect and monitor intrusions is a slow and manual way, and is considered not adequate to protect against rapidly changing intrusion attempts. The use of IDPS tools can help to automate, speed up and facilitate the intrusion detection and prevention process. As such, B/Ds are recommended to deploy such tools to detect and stop intrusions.

Apart from that, a set of security policy and procedures should be developed for controlling and monitoring the Internet gateway. There is a need to perform security audit regularly, after major changes or prior to implementation to ensure that the Internet gateway is set up properly in accordance with the security policy. Even if there is no internal network connection, it would still be better to have the above recommended security protection.

Annex A shows a checklist for some of the recommended protections.

2.3 Internet Gateway Architecture Sample

B/Ds should implement multi-level defense for their systems.Illustrated below is a sample logical network diagram for an Internet gateway. B/Ds may revise the

network architecture according to their own requirements, services offered and existing network structure. The relative position of network components may need to be altered.

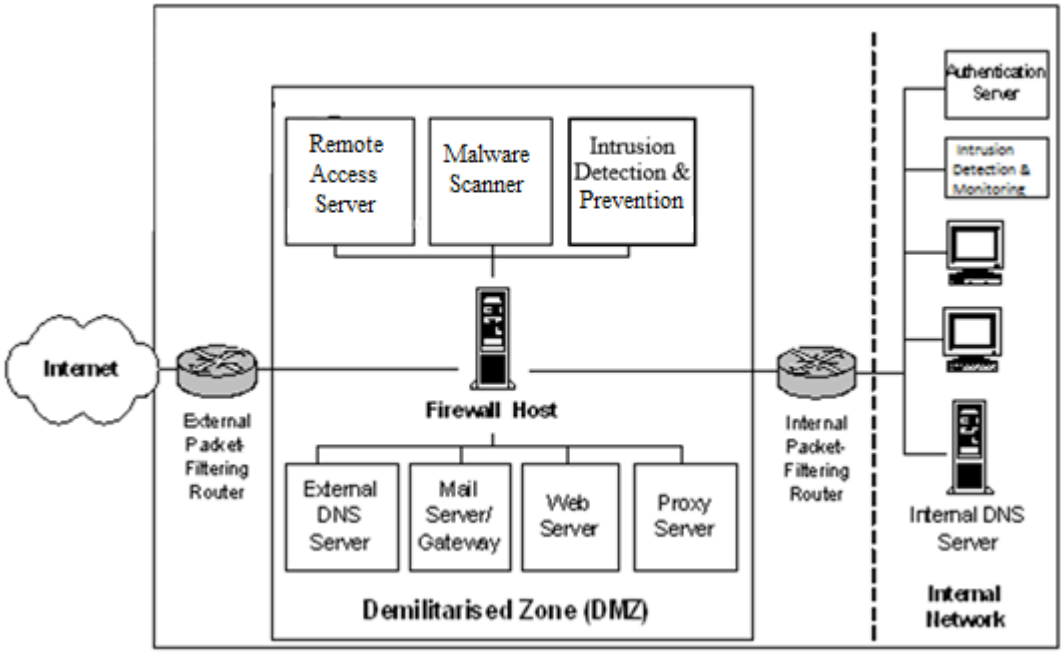

Figure 2 A Sample Internet Gateway with a DMZ

A firewall system, intrusion detection mechanism and malware scanning tools should be maintained to provide security protection for Internet access service. Depending on the services to be provided, the following network devices may be deployed with:

- Authentication servers (for user identification and access control)
- Remote Access Server (RAS) (for remote access)
- Domain Name System (DNS) servers (for host name and address mapping)
- Simple Mail Transfer Protocol (SMTP) gateway and mail servers (for Internet email)
- Web servers (for information publishing)
- Proxy servers (for caching, network address hiding, access control)

Nonetheless, some security guidelines on the above components will be explained in later sections with focus on their security measures.

This architecture can separate the internal network from the external one, and can hide the information about the internal network. Separate segments may be assigned within the DMZ for better access control and protection. Network segmentation/

isolation should be adopted. Moreover, cross-network connectivity should be provided only when necessary.

In fact, Internet gateway architecture for different services may require specific tailoring depending on many factors such as network infrastructure, services provided, performance, mode of operations, cost and so on.

2.3.1 Web Servers

- Separate web servers should be used to restrict access when providing different information to internal and external users.
- Web servers can be placed inside or outside the internal network. Web servers used for providing information to internal users shall be placed inside the internal network and any connection from public or external users is prohibited. For web servers used for disseminating information to the public or external users, they shall be placed in the DMZ and protected by the firewall. All outside web servers need to be connected to the firewall in the DMZ with a separate network interface.
- A dedicated host should be assigned for running a web server, a mail server or any critical service separately. Individual host should have protective measures to guard against attack from other compromised hosts. In case of being compromised, this can reduce the impact to other services.

2.3.2 Domain Name System (DNS) Servers

- All host names and addresses stored in an external DNS server are supposed to be exposed to public. Hence, the external DNS server shall not hold information about the internal network. If the external DNS server is hosted at the Internet Service Provider (ISP), resilience should be considered to ensure system availability.
- A separate internal DNS server could be set up and placed in the internal network if internal domain information is needed, but the information shall not be disclosed to the Internet.

2.3.3 Intrusion Detection and Prevention

As mentioned above, procedure-based mechanism to detect and monitor intrusions is considered not adequate to protect against rapidly changing intrusion attempts. IDPS is recommended as it can provide an effective way of identifying, responding to and containing intrusions and suspicious network activities. In addition, system and application logs should be properly kept, reviewed and analysed for all critical components. Reviewing, monitoring and response procedures should be properly established and followed.

An Intrusion Detection System (IDS) passively monitors traffic by listening to and examining the packets within a network. Signatures of known attack attempts will be compared against traffic pattern to trigger an alert.

An IDPS provides a more proactive approach beyond an IDS because it can be configured to stop the attack from damaging or retrieving data from the target victim upon detection of an attack pattern. Similar to a firewall, an IPS can intercept and forward packets and can thus block attacks in real-time.

These tools reside in the networks or hosts to detect any suspicious activities, and monitor the network traffic or system activities. In general, IDPS should be installed at critical nodes of network. Critical nodes are referring to strategic connection points in front of critical IT assets or junctions of different security perimeters, e.g. mission critical systems, servers with sensitive data, Internet gateway, remote access gateway, floor of senior staff, etc. Some suggestions are listed as follows:

- IDPS should be kept update with latest signatures and recognition patterns for security threats. Latest patches should also be applied.
- IDPS should be placed at critical nodes of network, such as DMZ to detect external attacks or places in the internal network to detect internal attacks if required.
- The operation of the IDPS should be as stealth as possible. It should be hidden and protected by the firewall system to protect it from attacks.
- Do not solely rely on IDPS to protect the network. IDPS are only real-time detection tools to alert users on abnormal or suspicious activities. More importantly, the network should be properly configured with all necessary security protection mechanisms. The whole network should be closely monitored and regularly reviewed so that security loopholes or misconfiguration can be identified promptly.

2.3.4 Firewalls

Depending on the security requirements, the use of two or more firewalls or routers in serial helps to provide an additional level of defence. For example, two firewalls in serial (one internally connected with the internal router and one externally connected with the external router) may be required to provide different protections. If there is one RAS, such as VPN gateway, connected to the DMZ and placed between the internal and external firewall, the external firewall may aim at blocking malicious traffic from the Internet while the internal one may aim at blocking malicious traffic from the internal network users and the remote access users connected to the RAS.

If multiple firewalls are used in parallel for load balancing or performance reasons, the configuration of each firewall should be aligned.

2.3.5 Protection against Malware

- A separate host machine may be set up together with the firewall to check for malware in all incoming traffic when going through the firewall. This can centralise the control in updating signatures for malware, and prevent the malware from entering into the web or mail servers.
- Malware detection measure may also be installed in other positions, such as incorporated with the mail server or the web server to specifically protect individual servers.
- The decision of where to apply malware detection measure depends on many factors such as network architecture, performance, system or data to be protected and the required protection level. In most cases, mail server should be accommodated with malware detection measure as usually malware come in as email attachments.

2.3.6 Remote Access Servers (RAS)

A RAS is a special-purpose networking device designed to support remote or mobile computing. A VPN gateway is a specific type of RAS that allows remote connection to internal network securely over an un-trusted network. A RAS can also work with a modem pool to provide dial-up access service.

- Authorised users may like to have a remote access capability, i.e. to access internal network from remote locations. This capability may introduce vulnerabilities, and thus it should be implemented and managed properly. Request for remote access should be authorised with adequate justification.
- Authentication mechanism shall be used to control remote or dial-in access.

2.3.7 Proxy Servers

A proxy server is a server running simple programs or processes examining packets passed through. It is normally treated as performance enhancing devices for internal network users with value-added security service. It is used as a middleman in which the communications between two sides (e.g. a client and a server) are mediated and destined. That is, each side is communicating with the proxy server instead of directly connecting with the other side. Proxy servers should be configured to provide authorised proxy services and restrict user access to unauthorised destinations. Proxy servers can provide additional support such as caching of recently accessed web pages, access control, logging, content filtering or even address hiding.

Figure 2 above shows a proxy server, which serves to control internal users' access to the Internet. Proxy server can be configured to block unauthorised access to personal webmail, public cloud storage and web-version of instant messaging

services. Any IP addresses or websites known or suspected to be malicious shall be blocked.

Some firewalls can enforce proxy servers for typical services such as TELNET, File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP) and SMTP, so that no communication can go through the firewall without application level mediation.

2.3.8 Authentication Servers

Firewall and proxy servers can perform some kinds of user authentication functions. It can also consider the use of a central database, known as "authentication server" to centrally store all the necessary information for authenticating and authorising users such as user passwords and access privileges. In addition, these authentication servers can support stronger authentication schemes such as the use of tokens and smart cards, which may not be able to be supported by proxies.

For example, Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are common schemes used for remote authentication. Referring to Figure 2, an authentication server can be used to authenticate remote dial-in users before they are granted access rights to the network.

- The communication between user devices and the authentication server should be encrypted and be protected from security threats, such as eavesdropping and replay attacks.
- The information stored in the authentication database should be encrypted and be well protected from unauthorised access or modification.
- A single dedicated machine, which is securely protected, should be used.
- The server should be properly configured to log administrative transactions, usage accounting information and authentication transactions such as failed login attempts.
- If more than one authentication servers are used for resilience, make sure that the information stored in the authentication databases is propagated to all other replicas.
- System log files should be reviewed periodically to detect any unauthorised account creation or privilege modification.

A Risk Assessment Reference Framework for Electronic Authentication has been promulgated, which aims to introduce a consistent approach for B/Ds' reference in deciding the appropriate authentication method for their e-government services. The framework is to provide citizens/staff with a consistent experience and interface when transacting electronically with the Government for services of similar authentication requirements. B/Ds should follow the framework as far as possible in determining and implementing the electronic authentication requirements of their e-

government services. For details of the framework, please refer to the 'e-Authentication Framework' theme page at ITG InfoStation (https://itginfo.ccgo.hksarg/content/eauth)

3. Firewalls

A firewall can be considered as a security measure for protecting an organisation's resources against intruders. It is an important component of a security infrastructure. It should be reminded that the design and setup of a firewall requires thorough understanding about the firewall features, functions, capabilities and limitations as well as the threats and vulnerabilities associated with the Internet.

A firewall should be installed at all network junctions between internal network (e.g. department's network), external networks (e.g. Internet), and any network points that the flow of data is required to be examined, restricted, filtered or redirected.

There are different types of firewall available in the market. Upon selection of a firewall product, the following core criteria should be considered:

- Product features.
- Performance / throughput.
- Interoperability with existing network.
- Reliability.
- Resilience.
- Ease of management.
- Vendor support.
- Product certification (e.g. Common Criteria Evaluation Assurance Level).
- Support to authentication services (e.g. RADIUS).
- System capacity and scalability.
- Logging.
- Price.
- Customer reference.
- Skill sets availability.
- Security requirements.

Most importantly, the firewall should be properly configured and administered.

3.1 Firewall Configuration

Firewall should be properly configured to filter traffic, control access and perform content filtering. Poor or incorrect configuration of a firewall may result in a false sense of security, which is more dangerous than without a firewall. B/Ds should assess the security risks and determine the appropriate configurations based on their business needs.

Listed below are some considerations in firewall configuration for reference:

- All incoming and outgoing Internet traffic should be forced to go through the firewall, which is the sole means of entry from and exit to the Internet.
- Do start with a conservative firewall security policy, i.e. "Deny all services except those explicitly permitted." It is recommended not to blindly follow the default settings in the firewall.
- All services allowed to go through the firewall should be carefully planned and evaluated.
- The firewall can be configured to use network address translation (NAT) to hide internal network information such as IP addresses. In an IPv6 environment, B/Ds may allow end-to-end connectivity to the Internet if there are operational necessities. In doing so, proper security measures, such as using temporary IP addresses to inhibit user activities profiling, should be considered.
- The firewall should be configured to enable content filtering, and malware scanning capabilities.
- The firewall should be configured to block unauthorised access to personal webmail, public cloud storage and web-version of instant messaging services.
- The firewall should be properly configured for IP level filtering. Any IP addresses or websites known or suspected to be malicious shall be blocked.
- The firewall should be configured to block unused ports and filter unnecessary traffic, e.g. unnecessary incoming or outgoing Internet Control Message Protocol (ICMP) traffic.
- The firewall itself should be physically secured.
- The firewall policy established should be flexible for future growth and adaptable to changes on security requirements.
- Correctly set and assign file permissions on firewall. Permissions on system files should be as restrictive as possible.
- A firewall should be thoroughly tested, and its configuration should be properly verified before going production.
- A firewall test is necessary after major change or upgrade to the firewall.
- All software and OS installed on the firewall should be maintained with proper version by periodically revisiting the vendor sources and upgrading with patches and bug fixes.
- Real-time alerts should be set up for emergency incidents.

- Audit trail function should be enabled such that any configuration modifications made by administrators or intruders can be traced.

3.2 Firewall Administration

- Firewall configuration, administration and operational procedures should always be well documented.
- Configuration of multiple firewalls used in parallel should be identical.
- Integrity checking of the configuration files of firewall by checksums should be performed whenever applicable.
- Log recording and reviewing for firewall should be done regularly.
- Backups of system and configuration files for firewall should be taken regularly.
- Proper maintenance of user accounts is important. Only the firewall administrator and backup administrators will be given user accounts on the firewall. Tight access control should be enforced for authorised users to perform necessary functions only.
- Ongoing training of firewall administrators is essential for firewall maintenance and management.
- At least two firewall administrators (one primary and one secondary) should be designated for administrating the firewall.
- Establish an effective communication channel between LAN administrators and firewall administrators.
- Security audit has to be conducted on a regular basis. Perform periodic scans and checks of host systems to detect common vulnerabilities and faults in configuration.

4. Routers

Routers are used to connect two or more networks. They can filter traffic and restrict access to servers or network components, similar to the application proxies.

The following guidelines should be observed and followed when configuring and managing routers in the network:

- Similar to firewall, routers should be properly configured to deny all traffic by default, and to allow only permitted traffic to go through. Source routing should be disabled unless for troubleshooting.
- Logging, backup and other administrative tasks should be properly performed, similar to those for firewall.
- Testing should be done thoroughly before live implementation.
- If routers are used with firewalls, they should be consistent with the firewall policy.

5. Mail Gateway Security

To set up a secure mail gateway, the following guidelines should be observed and followed.

5.1 Mail Server Design and Configuration

- A mail server should be run behind a firewall system, which helps to restrict the access to the mail server and provide various security protections.
- Properly configure firewalls or routers to block unwanted traffic such as traffic from particular IP addresses of known spammers, into the mail server or gateway.
- Anti-malware protection should be adopted for filtering inbound and outbound email including any attachments that contain malware.
- The email system should not disclose names or IP addresses of internal network or systems.
- The email system should be properly configured to avoid disclosing internal systems or configurations information in email headers.
- Directories of internal email addresses should not be made publicly accessible.
- Mail gateway should be capable for logging all email headers for auditing. It should provide information such as how, when and where an email is entered or left.
- If there are email bombs or spam emails, identify the source or origin of emails and configure the router or firewall to block or drop the emails.
- Mail relay functions for unauthorised users or IP addresses should be disabled.
- Internet mail exchange should enable Sender Policy Framework (SPF) and should stamp outgoing mails with DomainKeys Identified Mail (DKIM) signature to facilitate the receiving side to verify such mails as sent by the Government.
- Internet mails shall be protected by Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol, which is an email authentication protocol to give email domain owners the ability to protect their domain from unauthorised use, such as email spoofing.

5.2 Email Bombing, Spamming and Spoofing

Email bombing refers to repeatedly sending emails to fill up a mail gateway or a mailbox. Email spamming refers to the sending of unwanted email to users. Both email bombing or spamming resulted in flooding the Internet with unwanted junk emails. Email bombing/spamming attackers usually hijack other mail servers, and use them to send the emails.

Email spoofing refers to emails in which the sender or other parts of the email header are manipulated to appear as from a different user or source with impersonated identity. Email bombing/spamming may be combined with email spoofing, making it more difficult to determine who actually sent the email.

If mail servers are not properly configured, they may suffer from these kind of email attacks. The mail system may crash, overload or even lose internal data because all available resources are plundered by the spammers. The cost of recovery to normal service may also be high.

Examples of symptoms of email attacks are:

- Denial of service such as disk full or system shut down.
- Large number of incoming/outgoing emails from same originator in a very short period of time.
- Large number of incoming/outgoing emails from invalid source address or to non deliverable address.
- Incoming/outgoing emails from an unknown source.
- Emails claiming to be from the administrator requesting users to send a copy of their passwords or other sensitive information.
- Emails requesting users to change their passwords to a specified value or string.
- Emails redirecting users to fraudulent website that appears to be a legitimate organisation, for the purpose of gaining personal identity and private information, such as credit card information.

Listed below are some points for protecting from email bombing, spamming and spoofing:

- Remove unused mail daemons such as Sendmail if not used.
- Keep mail gateway software up-to-date.
- Enable logging to record origin or header information of the spoofed email. Use IDPS to detect any suspicious activities such as sudden increase of incoming/outgoing emails from the same originator to assist the detection/prevention of mail bombing.
- Properly configure the firewall and router to allow incoming SMTP connections to a dedicated email gateway or server only to centralise the logging and traffic control.
- Mail relaying to and from unauthorised users or non-existence addresses should be blocked. For example, a mail server should only allow mail relay for some specified internal IP addresses or authorised internal users, but not external ones.
- Mail daemons or mail gateway software, which can filter out invalid messages, should be properly set up to remove junk mails or invalid messages such as from unauthorised domains or with invalid email headers.

- Set a limit on the maximum file size of an email, or on the maximum number of email messages that can be transmitted within a certain period of time. This can avoid flooding to eat up all available network resources or disk space.
- Update spammer list regularly.
- Set up spam blocking system before mail server to block out unwanted emails. Such spam blocking system acts as an email gateway to filter out spam emails before entering the mail server based on various criteria, such as email header, content, spam blacklist, spam whitelist, reverse DNS lookup, SPF and DKIM information.

5.3 Access Control

- Only authorised users should be allowed to use the mailing service.
- Use authentication schemes such as passwords or digital signatures to authenticate the emails, and ensure their origin and integrity during transmission.
- The number of users allowed to access the email server should be limited.
- Store emails in secure repository with proper access controls. Care should be taken to maintain the privacy of emails.

6. Web Security

Web security is a set of procedures, practices and technologies to protect web servers, users and internal network. The web server including its components such as the web server's operating system (OS), the network, application programs/software, and all resided information are subject to attacks from the Internet.

Since the web server is facing the Internet, strong host and network security protection should be employed. The security guidelines on web security described in this section should be observed and followed. For best practices on defending websites and web applications against cyber threats, please refer to the Practice Guide for Website and Web Application Security.

6.1 Web Server Configuration and Administration

Web server software is an application running on a host system, often facing the Internet, to provide information or web services to users. The below security best practices are important for deploying and maintaining a secure web server.

- Critical websites, websites of high workload, or websites more vulnerable to cyber attack should be hosted in separate web servers in order to reduce or avoid potential collateral damage if the web servers must be exposed to the Internet. To further enhance security, a dedicated host for running each websites separately should also be considered.
- The web server should be configured not to start up any SMTP service allowing external users to relay mails through the web server.
- All server software and application should be running with the least privilege, especially it should not be running with 'administrator', 'superuser' or 'root' privilege.
- Proper access permissions should be set for directories, files and web pages in the web server.
- All unnecessary network services, applications, or internet protocols should not be running on the web server by default. In particular, server administration and content update channels (e.g. FTP, SFTP, SSH) should not be open to the Internet.
- Remove or restrict any unnecessary server-side executable codes such as Common Gateway Interface (CGI) programs and server plug-ins as far as possible.
- If applicable, dedicate a single working directory for processes of web server to create/manage working files during execution. Ensure to have the working files removed after the processes finished.

- The web server administration tools should only be accessed by authorised administrators through authentication systems with log records. Vital configuration files should only be updated by the administrators.
- The integrity and availability of the websites should be closely monitored daily. IDPS should be used to detect suspicious activities, notify administrators and stop any unauthorised modifications or access.
- Disable all unused accounts, including user, service and default accounts.
- Remove all default or sample files from the web server.
- Restrict web crawling for the contents which are not supposed to be searched or archived by public search engines.
- The passwords of administrative tools should be changed periodically and should not be repeated. Never use the default passwords for these administration tools.

6.2 Access Control

- Strong authentication should be used for user authentication. IP address restriction should not be solely used for user authentication because source IP address can be forged.
- No directories or data files should be accessed or updated by anonymous or unauthorised users.
- Access should be granted only to registered users. Limit the numbers of login accounts available in the server machine. Review and delete inactive users periodically.
- All unnecessary accounts should be disabled, especially those guest accounts.
- Only appropriate administration processes / accounts should be allowed to access the logs.
- Sensitive information stored on an external web server should be protected with strong encryption and should require authentication for access.

6.3 Web Content Management

- All websites and pages should be thoroughly tested and checked before production or after major changes.
- Control should be made such that only delegated and authorised persons could have rights for posting and updating web pages to the production environment.
- If a web server has to be shared among different sections or even departments, different web content directories or resources should be granted with access control to restrict the access, execution and storage of these web applications.
- No links to internal files, which are stored outside the assigned web directories, should be set in the web applications.

- Adequate access control should be applied to the folders and files to ensure users cannot access any files that stored in the web server but not intended for user access.
- User access logs such as unauthorised access attempts to system files should be kept so that any abnormal or suspicious activities can be traced.
- No administration privileges on the OS and web server should be granted to web content developers.
- Establish web content management procedures for posting or updating web pages and applications to the web server.
- For web forms or applications that accept user input, all input data should be properly checked, validated and sanitised before passing to the backend application. Any unexpected input, e.g. overly long input, incorrect data type, unexpected negative values or date range, unexpected characters, should be handled properly and would not become a means for attacking the application.
- Unnecessary contents such as platform information in server banners, help database, online software manuals, and default or sample files should be removed from production servers to avoid disclosure of internal system information.

6.4 Common Gateway Interface (CGI) Programs and Application Programming Interface (API)

Usually web servers can be extended using Common Gateway Interface (CGI) programs and Application Programming Interfaces (APIs) to improve their capabilities. Default CGI programs supplied with web servers may provide unintentional "back door" access to web content. Such programs may leak internal information about the host system and may be vulnerable to attacks. Moreover, CGI programs often accept user input data.

The following items should be observed and followed:

- CGI programs and programs built on APIs should be properly designed, tested and examined to ensure that they only perform the desired function. No default or custom CGI programs and APIs should be remained on the server unless they are thoroughly tested and verified.
- These programs should be run and stored in a restricted environment such as in a designated directory, to limit the access and facilitate the maintenance.
- These programs should be given executable permissions only, but not readable or writable permissions. Use of system resources should be limited including the CPU time, timeout period and disk utilisation. Access to other data files or information should be properly restricted.
- Programs should not be resided in the default directories of program files such as compilers, interpreters, shells and scripting engines. They should be located safely in appropriate directories and should be removed completely from the web server when not required.

- User data input to these programs should be properly checked, validated and sanitised before passing to the server software or the underlying OS to prevent them from triggering command-line function.

6.5 Authentication

- Wherever applicable, use strong authentication schemes such as digital certificates, smart cards and tokens for remote administration control and authentication of critical applications, servers and clients.
- Use encrypted connection such as Hypertext Transfer Protocol Secure (HTTPS) for transmission of sensitive information. HTTPS shall be implemented for all Internet services, including informational websites, so as to strengthen the authenticity of Internet services and also the content integrity.

6.6 Web Browser

Web browsers should be properly configured. Some suggestions are listed below for reference.

- Access to the Internet should be made through an authorised communication channel e.g. the Central Internet Gateway.
- Turn off any active content enabling options, e.g. Java, JavaScript and ActiveX, in the email application or browser, except when communicating with a trusted source.
- Scan any downloaded files for malware before opening or executing them.
- Use up-to-date browsers and apply latest security patches.
- Disable password auto-complete / remembering feature.
- Enable pop-up blocking feature, except when communicating with trusted sites.
- Regularly remove cache files or temporary files of browsers to protect data privacy.
- Plug-ins, add-ons or software should be checked and tested before installation and such installation should be done by authorised persons only.

6.7 Active Content and Cookies

Active content enables information servers to tailor their presentation script which is to be executed in the client side browser. Examples are Java applet and ActiveX. It is important to note that plug-in based technology is migrating to plug-in free technology, due to the rise of web usage on mobile device browsers which typically do not support plug-ins. B/Ds should check the end of support date for plug-ins at the official websites of software vendors and prepare a viable migration plan beforehand.

Cookies are mechanisms used by the server side to maintain the state information of a client's browser when using stateless connection protocol such as HTTP.

6.7.1 Java Applet

Java applet is a program that is usually embedded in a web page. Client browsers may automatically download Java applets for execution. Nevertheless, Java system restricts its applets to a set of safe actions known as "sandboxing" making them difficult to damage the file system or the boot sector of a client computer. When developing Java applets, developers should design and restrict access of Java applets to designated directories, files and OS properties.

The following areas should also be considered at the client side where Java applets will be running:

- Tighten the security controls on Java's compilers, interpreters and generators. Remove these compilers, interpreters and generators whenever not required in the production environment.
- Keep up-to-date information about security vulnerabilities of Java system and Java applets, and apply latest patches.
- Java applet may only be enabled in the browser when it is required.

6.7.2 ActiveX

ActiveX is a software control which can be used to create distributed applications working over the Internet through web browsers. ActiveX controls are designed to allow web browsers to download and execute them. ActiveX controls are composed and embedded in web pages, but there are no restrictions on what they can do. For example, ActiveX is allowed to reside on a system, or even wipe out the data or write to the local hard disk without users' discretion. Moreover, the browser is not capable of recording down what actions the ActiveX controls have been performed on the client machine.

ActiveX should be prohibited by default. If running of ActiveX is necessary, the ActiveX control should be carefully verified and evaluated. Such installation should be done by authorised persons only. A software author can apply digital signature technology, which is certified by a certification authority, onto an ActiveX control. In this way, the client can verify the signature before deciding to either accept or reject the control based on the author's identity. Bearing in mind that digital signatures only tell who wrote the ActiveX controls but could not help to decide whether they are trusted or not. One should always carefully consider and accept only those controls from trusted sources, or one should evaluate and disable "ActiveX controls and plug-ins" in the browser settings to prohibit running of unnecessary ActiveX on the system.

6.7.3 Cookies

Cookies are mechanisms used by server side to store and retrieve information from client side. They are objects, which provide state information of the client to the server such as descriptions of accessed URLs, client user's email addresses and sensitive information. An attacker can masquerade as the server to retrieve cookies from the client.

System developers should be aware that it is inappropriate for cookies to keep too much private information. Plaintext user name and passwords should never be kept in cookies. Apply encryption to the entire cookies if authentication information is needed to be stored in the cookies. System designers can also include some control information such as an expiration date and time to restrict the valid period of the cookies and hence, reduce its potential damage.

7. Remote Access

Remote access refers to the use of network resources from a remote location, which is not directly attached to the network. There are different ways of remote access, such as dial-up access and Virtual Private Network.

7.1 Dial-up access

Dial-up access is one form of remote access over a public telephone network. Only authorised persons should be allowed with dial-up access. B/Ds should keep an updated inventory of their dial-up access points and modem lines. Dial-up access is advised to be safeguarded by user authentication, and dial-up passwords should be changed regularly. In some cases, two-factor authentication may need to be implemented.

B/Ds should also consider using call-back security feature. With call-back security, the answering modem accepts the incoming call and authenticates the user. Once the user is authenticated, the modem disconnects the call and then places a call-back to the user using a telephone number in a predefined database. The implementation assists in preventing unauthorised access or use of stolen credential. Although call-back improves security, it is susceptible to compromise by call forwarding and should be used together with other security controls such as two-factor authentication for dial-up connection to sensitive environment.

Access logs should be kept for every dial-up request. At least the following information should be recorded: date, time and duration of access, username, and the connected communication port. The access log should be made available for the inspection when necessary.

In addition, the following best practices should be followed regarding dial-up access:

- Clearly identify users who would be granted with remote access privileges and what types of services could be provided to them.
- Only authorised users should be allowed to gain remote access to the network with proper authentication and logging.
- Properly configure firewall system to restrict remote access.
- RAS and modem pool should be physically secured.
- A central modem pool is recommended to be used for ease and effectiveness of management and control.
- Connection to RAS should be logged to record the login session initiation and termination, the connection starting and ending time, the addition, updates or deletion of user accounts on the RAS and etc.

- Encryption should be used to protect user credentials or data during transmission over these links.
- Dial-in services can also be flooded by repeatedly dialling. The setting of time-outs counters or dial-in time limitations can be used to reduce the chance of being flooded.

7.2 Virtual Private Network (VPN)

Virtual Private Network (VPN) establishes a secure connection over un-trusted network by using a technique called tunnelling. Operating on layer 2 or layer 3's networking protocols, tunnelling encapsulates a message packet within an IP (Internet Protocol) packet for transmission across a network. There are different tunnelling protocols such as Internet Protocol Security (IPSEC) and Layer 2 Tunnelling Protocol (L2TP).

In addition to traditional layer 2 and layer 3 VPN, SSL-VPN (Secure Sockets Layer Virtual Private Network) is another VPN technology providing the tunnelling protection. In SSL-VPN, the tunnel rides on TLS (Transport Layer Security) communication sessions. SSL-VPN differs from traditional VPN because it can operate without the need of VPN client software while the traditional VPN usually requires client software.

Setup of VPN is considered to be a viable solution to establish secure communication channel for users to work outside office. Before implementing VPN, B/Ds should evaluate compatibility with the existing network and consider implementing the following VPN security guidelines:

- Authenticate with either one-time password authentication such as a token device or public/private key system with a strong passphrase as the second factor of authentication for remote access.
- Disconnect automatically from government internal network after a predefined period of inactivity. The user must then logon again to reconnect to the network.
- Disallow dual (split) tunnelling. Only one network connection is allowed.
- Protect all computers or devices connected to government internal networks via VPN with personal firewall, latest security patches, anti-malware and malware detection and recovery software. All these security measures should be activated all the time and with the latest malware signatures and definitions.
- Set up whitelist for registered users and endpoints.
- The use of remote access computers or devices shall comply with the government IT security requirements. Privately-owned IT equipment shall not be connected to the government internal network. If there is an operational necessity, approval from the Departmental IT Security Officer shall be sought.

- Provide logging and auditing functions to record network connection, especially for failed access attempt. The log should be reviewed regularly to identify any suspicious activities.
- Remind users with VPN privileges that they are accountable for the proper use of the account, ensuring that unauthorised users cannot use the account to access government internal networks.
- Educate LAN/system administrator, supporting staff as well as remote users to ensure that they follow the security best practices and policies during the implementation and usage of VPN.
- Install gateway-level firewalls to control network traffic from VPN clients to authorised information systems or servers.

8. Domain Name System (DNS) Servers

A Domain Name System (DNS) server provides support for mapping and translation between domain names and IP addresses. The DNS server can provide information such as the IP addresses lists of hosts in a given domain, IP address-to-hostname mapping, and email address.

To protect the DNS servers, the following guidelines should be observed and followed:

- Use the latest DNS server software or service pack.
- Apply security protection mechanisms on the DNS server such as access control on DNS database files and use of strong encryption system.
- Maintain a record of IP addresses assignment information such as host location and host information. This record acts as an inventory list for backup, verification and audit in case the DNS server is compromised.
- For DNS servers providing DNS resolution service to internal users, the baseline of DNS query traffic pattern should be maintained so that any anomaly of the current traffic against the baseline may trigger an investigation of suspected malicious activities or unauthorised tunnel from the internal network.
- For DNS servers providing DNS resolution service to the public, the recursive lookup feature should be disabled and the rate of DNS response should be limited in order to prevent the DNS servers from taking part in DNS amplification Distributed Denial of Service (DDoS) attacks. Response to well-known sites or addresses not going to generate DNS query should be blocked as well to avoid taking part in attacks against important infrastructure, such as the 13 root DNS servers and the country code Top-Level Domain (ccTLD) DNS servers.

8.1 Domain Name System Security Extensions (DNSSEC)

DNS is often subject to man-in-the-middle, spoofing, and cache-poisoning attacks that are hard to defend against. Domain Name System Security Extensions (DNSSEC) adds an additional layer of protection to the network by providing validation of DNS responses. It uses public key cryptography to verify the authenticity of a DNS record. By checking the digital signature, the client computers can trust that information they receive has not been modified or tampered. It protects users from being redirected to malicious sites.

To enforce the authenticity of Internet resources, the resources records of Internet domains shall be protected by DNSSEC. For DNSSEC implementation, B/D should consider:

- Designing a signing system – how to integrate the system with the existing DNS architecture and the changes to the existing procedures of DNS management have to be considered.
- Signing in a testing environment – before releasing the system to the external world, test the complete system, including all the defined procedures, under a testing environment.
- Checking DNS servers – verify the external authoritative name servers supporting DNSSEC.
- Key generating and management – the procedures to generate, publish and manage keys, as well as the size and lifespan of the keys should be planned.
- Establishing emergency procedure – the procedures to re-generate keys and re-sign the zone for should be established for case of key compromise.

Content Delivery Network (CDN) service provides faster content delivery such that the content is replicated and stored in a distributed way. However, CDN may have limitation in the extent of their DNSSEC support. In such scenario, the domain name records owned by B/Ds shall be protected by DNSSEC while the lower layers of the domain name should be protected by DNSSEC as far as practicable if CDN service is deployed.

8.2 DNS Blocking

DNS blocking is an essential feature for B/Ds to safeguard its network against online threats. It involves preventing access to specific websites or online resources by blocking their domain names using the DNS. B/Ds should assess the security risks and determine the appropriate blocking mechanism based on their business needs.

DNS blocking works by intercepting user requests and checking the domain name against a predefined blacklist. If the domain name is found on the blacklist, the DNS server responds with a blocked message instead of the IP address, hence preventing the user from accessing the website.

Listed below are considerations that can be used in building and maintaining the blacklist:

- Malicious Domains
- Suspicious Domains
- Command-and-Control Servers
- Phishing and Scam Domains
- Known Malicious IP Addresses

- Emerging Threats

By implementing DNS blocking, B/Ds can enforce content filtering policies, prevent access to malicious websites, protect against phishing attacks, and reduce the risk of malware infections or data breaches. It serves as an additional layer of defence, complementing other security measures and enhancing B/Ds' overall security strategy.

8.3 Protective Domain Name System (PDNS)

PDNS hampers the use of DNS for malware distribution and operation. A core capability of PDNS is the ability to categorise domain names based on threat intelligence. PDNS services typically leverage open source, commercial, and governmental information feeds of known malicious domains. These feeds enable coverage of domain names found at numerous points of the network exploitation lifecycle.

Protecting users' DNS queries is a key defence because cyber threat actors use domain names across the network exploitation lifecycle: users frequently mistype domain names while attempting to navigate to a known-good website and unintentionally go to a malicious one instead; threat actors lace phishing emails with malicious links; a compromised device may seek commands from a remote command and control server; a threat actor may exfiltrate data from a compromised device to a remote host. The domain names associated with malicious content are often known or knowable, and preventing their resolution protects individual users and the enterprise.

PDNS prevents access to malware, ransomware, phishing attacks, viruses, malicious sites and spyware at source. PDNS block data can be ingested into SIEM tools as a source of threat intelligence to help identify and remediate threats. By ingesting such data into a SIEM, B/Ds can consolidate various security logs into a single view, providing further context for blocks by PDNS.

When selecting a PDNS service provider, B/Ds should consider the following capabilities:

- Blocks malware domains
- Blocks phishing domains
- Malware Domain Generation Algorithm (DGA) protection
- Leverages machine learning or other heuristics to augment threat feeds
- Content filtering
- Supports API access for SIEM integration or custom analytics
- Web interface dashboard
- Validates DNSSEC

- DoH/DoT capable
- Enables customisable policies by group, device, or network
- Deploys across hybrid architectures

9. Intrusion Detection and Prevention

Maintaining Internet gateway security requires ongoing and comprehensive system operation, support and surveillance to oversee the prevention, detection, response and escalation of any irregular, abnormal or suspicious activities or incidents. This can be achieved by proper manual procedures such as reviewing and analysing log or statistics, and testing and drilling the incident handling procedures.

If possible, IDPS tools should be installed and used at strategic locations to collect and examine information continuously for suspicious activity. Both network based and host based IDPS tools could be used. The former type examines network packets in the network while the latter one monitors the system configuration and application activities on a single host system.

Improper configuration and use of these tools may disclose information to attackers and result in a false sense of security.

- IDPS tools should be used to identify suspicious activities on both the network and the host machines, in particular the web server and the mail server.
- Automatic generation of notifications or alerts by electronic messages or mobile paging should be set up to warn system administrators when symptoms of attacks are detected.
- If applicable, systems or functions capable of reacting to suspicious network activity should be implemented to disconnect or block these connections in the first place and record them for subsequent analysis.
- These tools should be properly tested and verified before going operation.
- The use, administration and management of these tools should be properly controlled and restricted.
- Firewall system should be properly configured to protect and hide such tools as far as possible.
- The attack signature files should be kept up-to-date.
- New update of signature file and blocking rules should be tested thoroughly and verified before putting into production. The new update should be tested to determine whether its new / modified signature and blocking rules perform as expected, and whether it conflicts with the original signature and blocking rules.
- Proper operating, administrative and monitoring procedures should be established for using these tools. The procedures should be reviewed periodically to ensure the network configuration is up-to-date.

The strategic places for IDPS deployment could be on firewall, hosts or any information assets that are important. A secure Internet gateway could be introduced in the Internet Gateway infrastructure as a first line of defence deployed between the Internet and the existing Internet Gateway to fight against threats on the Internet. The secure Internet gateway could be configured by allowing intrusion detection and prevention in web filtering, https traffic inspection, malicious IP address and domain detection or blocking and monitoring of network traffic, detecting malware, and preventing information systems from infection.

10. Other Security Considerations

Apart from the above specific network components, there are also some security issues that should be concerned. Some related issues are discussed in the following sections.

10.1 Physical Security

- All gateway components should be physically secured and be placed in a restricted area.
- The computer room with these equipment placed should be well equipped to protect against physical or natural disasters.
- Lockable racks should be used to store these components.
- Regular monitor and review on the current physical protection e.g. examine site entrance or access logs, check cables for unauthorised taps, check door locks of racks and any sticking labels.
- Remove and erase all storage media before disposal, especially those containing system configuration.

10.2 Logging

- Enable logging functions wherever applicable in firewall, router, OS, web server and mail server.
- Keep logs such as the error logs, system logs, access logs, web server and mail server logs with adequate storage capacity available.
- Endeavor to log information such as invalid account login attempts, account misuse in websites, illegal or unauthorised attempts to websites, administrative and configuration updates, or specific information of requests, including requestor's IP address, host name, URL and names of files accessed.
- Logs should be reviewed regularly and kept for at least a week in a secure place. Write-once device such as optical disk may be used to record those log files.
- Logs showing intrusions and attacks should be kept properly for investigation and record.
- Consideration on privacy should be made when designing the types and details of information to be logged.

10.3 Backup and Recovery

- Formal backup and recovery procedures should be established and well documented.
- All gateway components' configuration, log files, system files, programs, data and other system information should be backed up regularly and whenever there is configuration change. Encryption may be applied to the backup if necessary.
- Backup copies should be kept in a secure place. Two backup copies for system configuration are preferably to be kept with one on-site and one off-site.

10.4 Protection against Malware

- Enable anti-malware protection or malware detection to check all incoming Internet traffic, and automatically clean for malware.
- The gateway should be configured to stop traffic with malicious content, quarantine / drop them, and create audit logs for future investigation.
- Malware signature and definition should be updated regularly. The update should be configured as automatic and update frequency should be at least on daily basis.
- If automatic update is not possible (e.g. mobile devices which are often not attached to networks), update should be done manually at least once a week.
- Users should also note that from time to time, there could be ad-hoc and serious malware outbreaks. If so, users should follow the instructions and immediately update with the latest malware signature and definition in order to protect against malware outbreak. After signature/definition update, users should conduct full-system scan on the machines to detect any potential existence of the concerned malware.
- Regularly perform malware scanning for the host machine where the information servers are installed.

10.5 Operating System Security

Operating system (OS), where the network application software are running on, should be carefully selected with respect to the security requirements. The vulnerabilities or security holes of the OS may affect the security of the application software.

A secure OS platform should be chosen especially for the firewall and critical servers. It is preferable to select those OSs which can provide the following features:

- Multiple simultaneous processes
- Secure file access permissions and controls

- Accountability and auditability of users and system actions such as detailed event logs
- Identification and authentication of all users on the system
- Resources isolations such as controlling reuse of system objects e.g. deleted files, allocated memory

Different OSs have different ways to secure their configuration. Listed below are some examples for general reference.

- Remove or disable all unnecessary services or processes, especially those unused but default running services and processes.
- Remove unnecessary default accounts if possible, otherwise change all default accounts with strong passwords.
- The number of privileged processes running should be reduced to the minimum. The assignment of privileges should be carefully handled.
- Default file permissions and privileges should be reviewed periodically, and set to restrictive values.
- Use a strong password for the system administrator account. The password should be regularly changed.
- Standardise and minimise the number of OS versions and software to make installation and maintenance more manageable.
- Install OS upgrades regularly and apply latest OS patches, especially those related to security issues.

10.6 Peer-to-Peer (P2P) Network

Peer-to-peer (P2P) file-sharing systems are commonly characterised as network-based applications in which the peers (i.e. the participating computers) use the Internet to exchange files with each other directly. P2P network is a network model used by the P2P file-sharing systems, such that every peer plays the roles of a client and a server at the same time. This opens a channel for files stored in an user computer in internal network to be uploaded to other peers in the Internet.

The potential security risks with P2P technology include:

- Improper configuration may lead to information leakage when using a P2P application. Other files apart from the ones being shared can be exposed unknowingly if they are stored in the same workstation or storage media. Once a file is uploaded to the peers, this information is hard to be removed from the P2P network totally.
- P2P applications need the firewall to open a number of ports in order to function properly. Each open port in the firewall is a potential avenue that attackers might use to exploit the network.

- As P2P networks facilitate file sharing among peers, malware can exploit this channel to propagate themselves to other peers.
- The P2P application may contain vulnerability that attacker may use for spreading malware, hacking or launching a denial of service attack.
- When a file is downloaded using a P2P software, it is not possible to know who created the file or whether it is trustworthy. The person downloading the file might be exposed to criminal and/or civil litigation if any illegal content is involved.
- Use of P2P applications in B/Ds' networks could generate large amount of network traffic, monopolising network bandwidth that impacts other important business applications.
- As P2P technology relies on user workstations, it is unmanageable from the server side aspect and all the security measures implemented at server side has no effect to such P2P sharing.

The best practices for mitigating the risks of P2P technology are listed below.

- B/Ds should take very serious consideration in employing P2P technology in their business environment. Use of P2P technology is not encouraged unless there is a strong and exceptional business case to justify its use for file-sharing. In any case, classified or personal information should not be shared in a P2P network.
- If a P2P network is not required, security policies should be established to block all unnecessary ports. Staff should be regularly reminded not to install P2P applications on the workstation.
- Traffics in critical networks should be monitored by an IDPS. Any unauthorised P2P traffic detected should be investigated and blocked. A clear firewall policy should be defined to allow the minimum necessary network ports.
- If use of P2P technology is deemed necessary, the software should be installed to an isolated workstation with dedicated Internet connection and configured with due care, default settings must be examined before use. All unnecessary user privileges and file / directory sharing on the workstation should be removed to prevent exposure of files not intended for sharing inadvertently.

10.7 Security Risk Assessment and Audit

Security risk assessment should be performed periodically, after major changes and prior to implementation. It is required to be performed at least once every two years. It targets at reviewing the existing security measures and identifying for any potential security vulnerabilities.

A security audit can be a general review on existing security policies or a technical review by the use of various security assessment tools that should be used with considerable care to scan the host systems and the networks for security vulnerabilities. It targets at ensuring that the current protection mechanism complies with the existing security policy.

- Audit scope and objectives should be clearly defined to ensure that all target network components are included.
- Technical audit review should be performed prior to implementation. Host based scanning is necessary for each host in the gateway, especially for the running services and file permissions.
- Firewall policy should be thoroughly audited for its rules and allowed services.
- Password mechanisms should be checked and assured for effectiveness.
- After audit, testing results and data should be removed from the network components and stored securely.
- Access should be controlled to prevent unauthorised persons from accessing the scanning tools.
- Audit recommendations should be followed up as soon as possible.

10.8 System Management and Operations

- User accounts should be properly managed and maintained.
- No users or staff are allowed to install or run web servers or mail servers for Internet access, without obtaining formal approval from the Head of B/Ds.
- All roles and responsibilities of staff performing system administration and management should be clearly defined, assigned and documented.
- Procedures should be well established and followed for the Internet gateway such as change and configuration management control procedures especially for firewalls, backup and recovery procedure, web content management procedure and other related ones.
- Programs or software installed and run on the hosts should be of secured modes to prevent unintended alteration, and be applied with latest patches or updates.
- Administration for critical components should be performed directly from a locally attached terminal, otherwise, strong authentication such as tokens, smart cards, challenge-and-response or one-time passwords etc. should be employed.
- Regularly check online security news or archives, for latest technical advice on security incidents or vulnerabilities.
- Configuration should be reviewed and modified with respect to the latest environmental changes such as changing requirements, emerging security threats or vulnerabilities.
- System welcome, greeting or error messages may disclose internal system information. Disable these messages whenever appropriate.

- If possible, install and use management tools or services to centralise system administration and installation, e.g. using software for site-wide installation of patches.

ENDS

11. Annex A

Sample Protection Checklist For Internet Gateway Security

ITEM	RECOMMENDED PROTECTION
Firewall	*Firewall Configuration*
	All incoming/outgoing traffic should go through the firewall
	Start with 'Deny all services except those explicitly permitted' firewall policy
	Carefully plan and evaluate services allowed
	Enable Network Address Translation (NAT) if available
	Enable content filtering and malware scanning features
	Block unauthorised access to personal webmail, public cloud storage and web-version of instant messaging services
	Properly configure IP level filtering and block malicious IPs.
	Establish flexible firewall policy for future enhancements
	Correctly set and assign file/port permissions on the firewall
	Thoroughly tested before implementation or after major changes
	Keep proper version of all software installed on the firewall
	Set up real-time alerts
	Disable FTP or TELNET traffic originated from external to internal network unless it is necessary
	Secure OS where firewall is installed
	Firewall Administration
	Well document firewall configuration, administration and operational procedures
	Make identical configuration for multiple firewalls when used in parallel
	Perform integrity checking of the configuration files periodically, e.g. using checksums
	Regularly record and review firewall logs
	Make regular backups of the system and configuration files
	Properly maintain administrative and user accounts, and change their passwords periodically
	Provide ongoing training to firewall administrators
	Designate at least 2 firewall administrators
	Incorporate firewall administration with security incident handling
	Establish an effective communication channel between LAN and firewall administrators
	Conduct regular security risk assessment and audit
Intrusion Detection and Prevention	*Operational Control*

ITEM	RECOMMENDED PROTECTION
	Establish manual procedures for operational control
	Regularly review and analyse logs
	Monitor and analyse user and system activity
	IDPS Tools (if used)
	Use for both network and host machines particularly web or mail servers
	Set up automatic generation of notifications or alerts
	Implement functions to react to suspicious activities e.g. disconnect or block those connections
	Properly test and verify before going into operation
	Properly control and restrict the use of these tools
	Properly protect and hide these tools behind firewall
	Keep up-to-date attack signature files
	Establish and review operating, administrative and monitoring procedures for using these tools
Protection Against Malware	*Malware Detection and Prevention*
	Enable malware protection to scan all incoming traffic from Internet. The gateway should be configured to stop traffic with malicious content, quarantine / drop them, and create audit logs for future investigation.
	Keep malware signature and definition up-to-date
	Perform regular malware scanning
	Apply comparable security measures and procedures to computer equipment and software under development or being used for testing purposes
	Perform full system scans before the machines are connected to the government networks
	Request external vendor to perform a malware scan (with the latest malware signature) after new machine installation, service maintenance, or installation of software
Security Policy, Guidelines and Standards	*Establishment and Enforcement of Security Policies, Guidelines and Standards*
	Establish own Internet gateway security policy
	Establish related operating procedures e.g. change and configuration management control procedures, backup and recovery procedures, web content management procedures
	Establish and regularly test security incident handling and reporting procedures
	Assign and define roles and responsibilities of staff performing administration and maintenance
	Advise and train users to observe and follow policies

ITEM	RECOMMENDED PROTECTION
Security Risk Assessment and Audit	*Conduct of Security Risk Assessment and Audit*
	Perform security risk assessment at least once every two years and security audit periodically
	Perform security risk assessment before production or prior to major changes
	Clearly define security risk assessment and audit scope and objectives
	Conduct security audit by third parties
	Audit firewall policy
	Assure effectiveness of password management
	Secure auditing results and data
	Control access to assessment and auditing tools, if any
	Follow up assessment and audit recommendations as soon as possible