数字政策办公室

信息安全

互联网网关安全

实务指南

第 2.1 版

2024 年 7 月

版权公告

修改记录

修改次数	修改详情	经修改页数	版本编号	日期
1	G50 互联网网关安全指南第 5.0 版已转换成互联网网关安全实务指南。有关文件修订可于政府资讯科技情报网查阅：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	基于最新的《资讯科技保安指引》（G3）v9.0 而作出的修改	5.1, 16, 22, 29-31, 33, A-2	1.1	2021 年 6 月
3	基于最新的《资讯科技保安指引》（G3）v10.0 而作出的修改	2, 8-9, 11, 12, 29-31	2.0	2024 年 4 月
4	将「政府资讯科技总监办公室」更改为「数字政策办公室」		2.1	2024 年 7 月

目录

1. 简介

任何支持互联网设施的决策局 / 部门都需要保护本身的信息系统及数据资产，防范非法访问或公共入侵。应令所有源自部门网络的互联网访问都统经中央安排的互联网网关或决策局 / 部门本身的互联网网关。

本文件为互联网网关提供技术指南，以安全地使用互联网访问及服务。这些指南针对互联网公开平台，是维持安全风险于可接受水平的良好作业模式。这份文件专为参与互联网网关操作及技术工作的人员而制订。

由于本文件所载为一般性数据，不是为任何特定的计算机平台而编制，读者应衡量个别环境考虑以选择适用的资料。

1.1 目的

本文件就下列主要安全范畴提出指南：

- 互联网网关概览
- 防火墙
- 路由器
- 邮件网关安全
- 网站安全
- 远程访问
- 域名系统服务器
- 入侵侦测及监察
- 其它安全考虑事项

本文件旨在提供有关互联网网关良好作业模式的资料，并应与既定的《保安规例》、信息技术安全政策、指南及程序一并使用。

1.2 参考标准

以下的参考文件为本文件在应用上的参考：

- 香港特别行政区政府《保安规例》
- 香港特别行政区政府《基准信息技术安全政策》（S17）

- 香港特别行政区政府《信息技术安全指南》（G3）
- 香港特别行政区政府——《公开资料守则》
  http://ref.ccgo.hksarg/csogc/tc/c201002c.pdf
- “Site Security Handbook”, RFC196, Internet Engineering Task Force.
  https//www.ietf.org/rfc/rfc2196.txt
- “The World Wide Web Security FAQ”，the World Wide Web Consortium (W3C).
  http://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 术语及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用，以及以下的术语及惯用词。

缩写及术语	
无	无

1.4 联络方法

本文件由数字政策办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@digitalpolicy.gov.hk

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

CMMP 电邮： IT Security Team/DPO

2. 互联网网关概览

互联网网关是互联网专用连接的界面。不论界面与部门或政府内部网络是否有连接，互联网网关提供了与互联网的连接点。安全的互联网网关可收紧控制，并建立更具成本效益和安全的操作环境。

由于互联网属于开放性平台，加上复杂的网络服务和应用系统发展迅速，网关缺乏安全措施可能令内部网络容易遭受攻击。因此，互联网网关的配置必须恰当，并应采取适当的安全措施以保护网关免被攻击。

决策局 / 部门可利用数字政策办公室托管的中央互联网网关，但决策局 / 部门最终仍需要负责确保实施足够的安全措施。

在当今不断转变的网络安全角势中，当配置互联网网关时，考虑到新兴趋势（例如零信任架构）是非常重要的。

零信任架构融合了网络分段、微分段、强认证、最小权限、持续监察和强加密等原则，以确保更精细、稳健和动态的安全态势。它强调了整个网络中身份认证、授权和持续评估信任的重要性。

零信任架构并不完全依赖边界防御，而是同样重视保护在任何位置的数据、应用系统和用户的安全性。这种方法符合现代网络不断转变的特性，在现代网络中，资源分布在多个环境中，包括云端服务、本地系统和远程装置。

决策局 / 部门需要辨识到基于边界的架构的局限性，并考虑采用更先进的安全框架，例如零信任，以改善安全态势，更有效地侦测和应对威胁，并适应当今互联和动态网络不断变化的性质。

2.1 网络互连

互联网网关往往与内部网络互连，使内部网络能够访问网关服务。然而，在互连网络时必须加倍小心，以确保网络互连不会降低或削弱现有安全水平至无法接受的程度，也不会损害所处理资料的安全性。因此，互连各方必须：

- 维持在自有网络、主机和系统所实施的特定安全防卫措施
- 维持本身的安全政策和指南，但这些政策和指南应配合互联网网关的有关政策和指南
- 建立严格的互联网网关逻辑访问控制
- 为互联网访问和服务制订安全事故处理和报告程序

- 提醒并培训用户遵守及遵从相关的安全政策、指南和程序。

2.2 建议采用的安全措施

仅提供互联网访问服务的安全互联网网关应配备以下安全功能：

- 防火墙（访问控制）
- 小包过滤路由器（通讯路由和小包过滤）
- 入侵侦测及防御系统（记录、监察、侦测及制止攻击）
- 防范恶意软件（监察网络通讯，侦测恶意软件，和防止系统受感染）

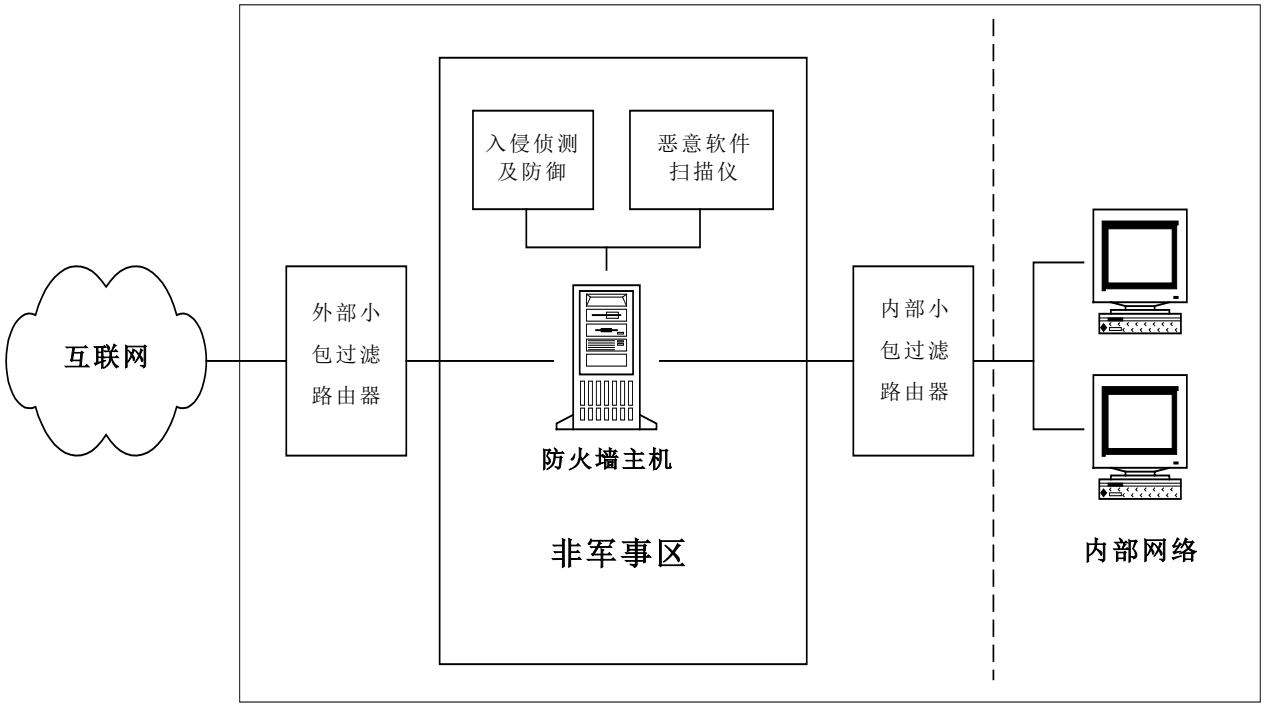

图 1　具备建议安全保护措施的互联网网关

上图所示是建议采用的互联网网关安全保护措施，互联网网关在毋须托管任何网站服务器或邮件服务器的情况下，提供了内部访问互联网的途径。非军事区是安全措施所在的区域。

设立防火墙主机的目的是要过滤未获授权或恶意的网络通讯。值得注意的是架设防火墙并非解决所有安全问题的方案。防火墙无法抵御的攻击，包括但不限于：

- 拒绝服务攻击，也无法保证数据的完整性
- 恶意用户的攻击
- 恶意软件的攻击

这些都是防火墙应与其它安全功能（例如入侵侦测及防范与恶意软件扫描）一并使用的原因。然而，防火墙制造商不断加强防火墙的功能（例如虚拟私有网络、加密等），使防火墙与其它安全措施的分别日趋模糊。

两部小包过滤路由器（外部及内部路由器各一部）从外部或内部网络，过滤和引入经挑选的通讯至防火墙。为连接互联网，外部小包过滤路由器是必需的设施。内部路由器则用来将非军事区部分（下文将作详细说明）与内部网络隔开。与防火墙不同，这些路由器一般被视为具增值安全功能的网络设备，而不是安全产品。

上文所述泛指可提供入侵侦测及防范功能的任何方法，可以是工具或程序，而不一定是实体装置。可是，以基于程序机制去侦测及监察入侵是一个缓慢的手动方法，被认为不适合用于防御急促转变的入侵尝试。使用入侵侦测及防御系统工具有助将入侵侦测及防御程序自动化、加快和促进入侵侦测及防御程序。就此，决策局 / 部门应部署这些工具以侦测及制止入侵。

此外，为控制和监察互联网网关，还应制订一系列安全政策和程序。在重大变更后或推行互联网网关前，须定期进行安全审计，可确保互联网网关是按照安全政策适当地设置。即使在没有内部网络的情况下，亦宜采取上述建议的安全保护措施。

附件 A 列表所载为建议就互联网网关安全采取的一些安全措施。

2.3 互联网网关架构示例

决策局 / 部门应为其系统实施多重防御措施。下图所示是互联网网关的逻辑网络图标例。各决策局 / 部门可根据个别需要、所提供的服务和现行的网络结构，按下图所示调整网络架构。网络构件的相对位置可能需要作出调整。

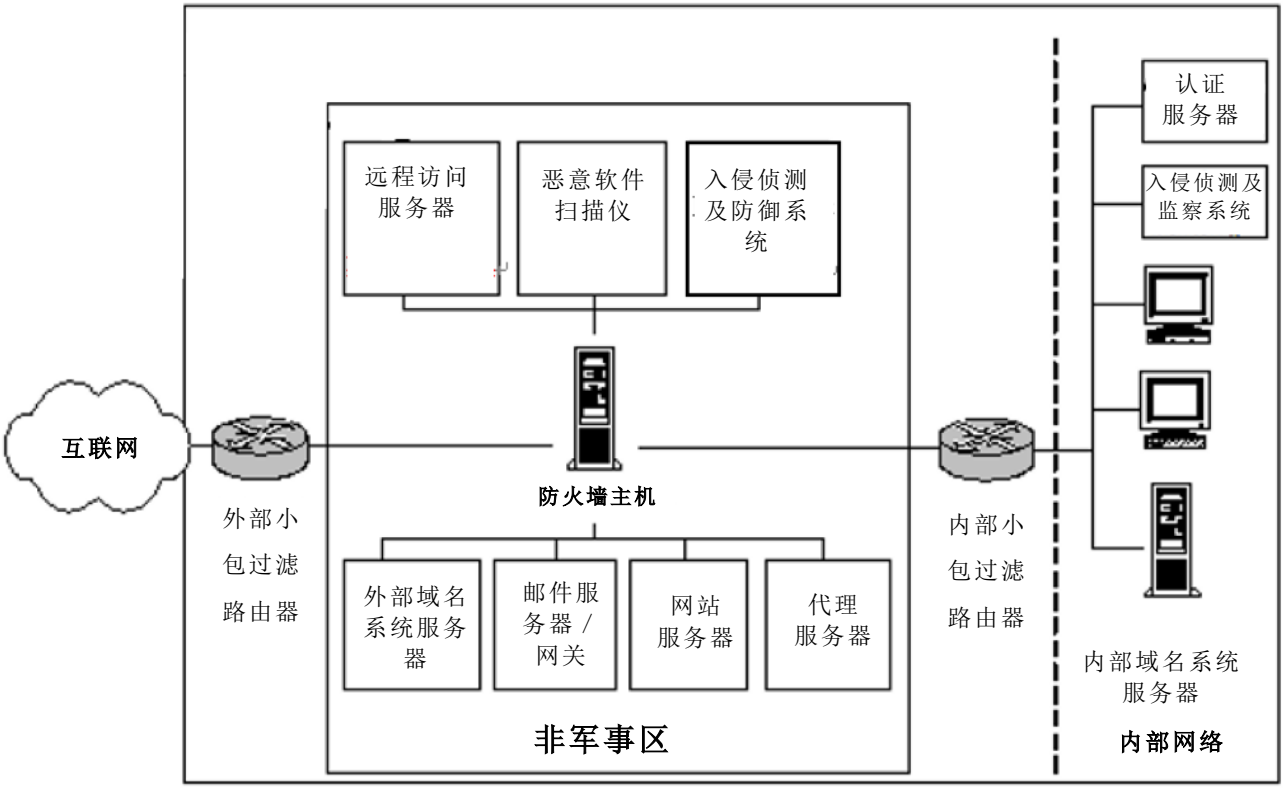

图 2　具备非军事区的互联网网关示例

网络架构应保留防火墙系统、入侵侦测机制和恶意软件扫描工具，为互联网访问服务提供安全保护措施。因应所提供的服务，可考虑纳入下列网络设备：

- 认证服务器（用户识别及访问控制）
- 远程访问服务器（供远程访问）
- 域名系统服务器（供主机名称及地址配对）
- 简单邮递传送规约网关及邮件服务器（供互联网电邮）
- 网站服务器（供发布信息）
- 代理服务器（供快取记忆、隐藏网址、访问控制）

下文将阐述适用于上述各构件的安全指南，以强调这些构件所需要的安全措施。

互联网网关架构可将内部网络与外部网络隔开，并可隐藏有关内部网络的资料。非军事区内可划分个别的区段，以实施更有效的访问控制和保护。应采用网络分段／隔离。此外，跨网络连接应仅按需要而提供。

事实上，提供不同服务的互联网网关架构都须要因应网络基建、所提供的服务、性能、操作模式和成本等多种因素作出特定的调整。

2.3.1 网站服务器

- 如须向内部和外部用户提供不同资料，便应使用不同的网站服务器以限制访问。
- 网站服务器可置于内部网络内面或外面。一般用来向内部用户提供数据的网站服务器须放置在内部网络内面，并禁止任何从公众或外部用户的连接。用来向公众或外部用户发布数据的网站服务器则应放置于非军事区内，并由防火墙保护 。所有放置在内部网络外面的网站服务器须与非军事区内的防火墙连接，以隔开网络界面。
- 网站服务器、邮件服务器或任何关键服务均应使用专用主机。个别主机应有保护措施防范来自其他受袭主机的攻击。一旦遭受攻击，可借此减轻对其它服务的影响。

2.3.2 域名系统服务器

- 储存在外部域名系统服务器中的所有主机名称和网址，原则上是可公开的。因此，外部域名系统服务器不可储存与内部网络相关的任何资料。若外部域名系统服务器由互联网服务供货商托管，则应考虑其复原能力以确保系统的可用性。
- 如需要内部领域数据，应另设一个域名系统服务器，并将该服务器置于内部网络内，而有关资料不可在互联网上披露。

2.3.3 入侵侦测及监察

如上文所述，以基于程序的机制去侦测及监察入侵并不适合防范急促转变的入侵尝试。建议使用入侵侦测及防御系统，因为它能提供有效方法辨认、回应及遏制入侵和可疑的网络活动。此外，必须妥善备存、覆检和分析所有关键构件的系统及应用系统记录，并应适当地制订及遵从覆检、监察和回应程序。

入侵侦测系统监听及检查网络内部的小包，以被动的方式监察网络通讯，并将已知的攻击活动识别码与通讯模式作比对，在吻合时发出警报。

入侵侦测及防御系统采取比入侵侦测系统更积极的方式阻截外来入侵，因为此系统可予以配置，在发现攻击模式后阻止攻击，使目标受害者免受损毁或被盗取资料。与防火墙类似，入侵防御系统可阻截及传送小包，从而实时阻止攻击。

这些基于网络或主机的工具可侦测任何可疑的活动，并监察网络通讯或系统活动。通常应当在网络关键节点安装入侵侦测及防御系统。关键节点是指在关键信息技术资产或者不同安全区域节点之前的策略性的连接点，例如关键信息系统、具有敏感资料的服务器、互联网通讯闸、远程访问通讯闸、高层人员楼层等。下文列出设置入侵侦测系统的一些建议：

- 入侵侦测及防御系统应保持更新安全威胁的最新标识符和识别模式，亦应安装最新的修补程序。
- 入侵侦测及防御系统应置于网络关键节点，例如非军事区内，以侦测外来攻击或者设置于内部网络内，以在有需要时侦测内部攻击。
- 应尽可能隐蔽入侵侦测及防御系统的运作。防火墙系统应掩护和保护入侵侦测及防御系统，以防止该系统受到攻击。
- 不应只依赖入侵侦测及防御系统保护网络。入侵侦测及防御系统只是在发生异常或可疑活动时向用户发出警报的实时侦测工具。最重要的措施仍是适当地配置网络，并确保已采取所需的安全机制。此外，亦应密切监察及定期覆检整个网络，以尽早发现安全漏洞或配置不当之处。

2.3.4 防火墙

根据用户的安全要求，串行使用两部或以上的防火墙或路由器有助加强防卫水平。举例来说，两部串行的防火墙（一部经内部路由器连接至内部网络，另一部则经外部路由器连接至外部网络）可提供不同的保护措施。如果有一部远程访问服务器（例如虚拟专用网络网关）与非军事区连接，并设置于内部及外部防火墙之间，外部防火墙可用来堵截来自互联网的恶意网络通讯，而内部防火墙则可堵截来自内部网络用户及连接远程访问服务器的恶意网络通讯。

如果是出于平衡负荷或性能的理由而平行使用多部防火墙，各部防火墙的配置应互相配合。

2.3.5 防范恶意软件

- 应一并设置独立主机与防火墙，以便在数据经过防火墙时，检验其中是否存有任何恶意软件。此配置可由中央控制个别恶意软件的识别码的更新，以防止恶意软件进入网站或邮件服务器。
- 宜在不同的位置（如邮件服务器或网站服务器等）采用可侦测恶意软件的措施，以保护特定的服务器。
- 在哪个位置采用侦测恶意软件的措施，取决于网络性能、需要保护的系统或数据及须达到的防范水平等多个因素。在通常情况下，因许多恶意软件都是以电邮附件的形式入侵系统，因此邮件服务器应采用侦测恶意软件的措施。

2.3.6 远程访问服务器

远程访问服务器是支持远程或流动信息处理的网络互连设备。虚拟专用网络网关是其中一种远程访问服务器。它容许透过不可靠网络上安全地以远程连接接驳到内部网络。远程访问服务器亦可以与调解器群一起提供拨号访问服务。

- 获授权用户可在没有互联网的情况下，透过使用远程访问功能进行远距离访问至内部网络。由于这种功能可能存有安全漏洞，因此应妥当地推行和管理。远程访问的要求应在有合适的理据下审批。
- 须以一套验证机制控制远程或拨号访问。

2.3.7 代理服务器

代理服务器是指运行简单程序或程序检验通过的小包的服务器。代理服务器一般被视为加强性能的设备，为内部网络用户提供增值安全服务。代理服务器担当了在通讯两方（例如客户和服务器）之间调解通讯及确定通讯方向的中介角色。换言之，各方均与代理服务器通讯，而不是直接与另一方连接。至于代理服务器的配置，除应提供已获授权的服务外，亦应限制用户访问未经授权之目的地。代理服务器还提供其它支持服务，例如快取记忆最近登入的网页、访问控制、记录、内容过滤，甚至隐藏网址。

图 2 所示的代理服务器协助控制内部用户访问互联网。代理服务器可以配置为堵截对个人网络电邮、公共云端存储和网络版即时通讯服务的未获授权访问。任何已知或疑似恶意的互联网规约地址或网站均须被堵截。

部分防火墙可加强代理服务器最常提供的服务，例如远程登录、档案传送规约、超文本传输规约及简单邮递传送规约，以防止未经过应用系统层调解的通讯穿过防火墙。

2.3.8 认证服务器

防火墙和代理服务器在某程度上具备用户身分鉴定功能。用户还可考虑使用被称为「认证服务器」的中央数据库，以作中央储存所有鉴定用户身分及授权用户所需的数据，例如用户密码和访问权限。此外，这些认证服务器还支持更有效的认证模式，例如运用权标和智能卡，而代理服务器不一定支持这些认证模式。

举例来说，远程认证拨号用户服务和终端机访问控制器控制系统是常见的远程认证模式。图2所示的认证服务器可在远程拨号用户获授权访问网络前，用来鉴定远程拨号用户的身分。

- 应为用户装置及认证服务器间的通讯加密，以及保护有关通讯，防范安全威胁，例如窃听及重放攻击。
- 储存在认证数据库内的数据应经过加密，而且应受到严密保护，以免被未获授权访问或窜改。
- 应使用独立及专用的计算机，并将此机放置在安全的地方保管。
- 应适当配置服务器，以记录管理事项、账户使用数据及认证事项，例如错误的登入。
- 如果使用一部或以上的认证服务器作复原用途，应确保储存在认证数据库内的数据已传送到所有其它备用服务器。
- 应定期审阅系统记录档案以发现任何未获授权建立账户或权限修改。

在制订电子政府服务的电子认证要求时，决策局／部门亦应遵从《电子认证风险评估参考架构》的指南。该参考架构旨在提供一个统一的方法给决策局／部门在制订其电子政府服务的认证方法时作为参考，务求令市民／人员于使用有类似认证要求的电子政府服务时会有一致的经验及接口。决策局／部门应在决定及推行其电子政府服务时，尽量跟从该架构。有关该架构的详细资料，可于政府资讯科技情报网内的「电子认证架构」主题专页查阅（https://itginfo.ccgo.hksarg/content/eauth）

3. 防火墙

防火墙可视为防止入侵者侵入，以保护机构资源的安全措施。防火墙是安全基础设施的重要部分。在探讨防火墙的设计前，须彻底了解防火墙的特点、功能、限制，以及与传输控制规约／联网规约相关的安全威胁和漏洞。

防火墙应安装在内部网络（例如部门网络）与外部网络（例如互联网）之间的所有网络接口，以及须检验、限制、过滤或重新引导数据流的任何网络点。

市场上提供多种防火墙产品。在选择防火墙产品时，应考虑以下主要标准：

- 产品功能
- 性能／处理能力
- 与现有网络的互用性
- 可靠性
- 复原能力
- 管理的便利程度
- 供货商的支援
- 产品核证（例如 GB/T 20281, GB/T 32917, ISO/IEC 15408）
- 认证服务的支持（例如远程认证拨号用户服务）
- 系统容量和扩展能力
- 记录
- 价格
- 客户参考
- 所需的技术人员
- 安全要求

最重要的是，应适当配置及管理防火墙。

3.1 防火墙配置

防火墙应经适当配置，以过滤网络通讯、控制访问和过滤数据内容。防火墙配置不当或有误可能导致安全假象，而安全假象比没有设置防火墙更为危险。决策局／部门应评估安全风险，并根据业务需要确定适当的配置。

以下列举一些配置防火墙时应注意的事项，以供参考：

- 应以防火墙为进出互联网的唯一通道，强制所有传入及发出的互联网通讯经过防火墙。
- 由一个保守的防火墙安全政策开始，即「除明确获准的服务外，拒绝所有服务」。用户不宜盲目遵从防火墙预设的设定。
- 应审慎规划和评估获准经过防火墙的所有服务。
- 配置防火墙时，可启动网络地址转换，以隐藏互联网规约地址等内部网络数据。就采用互联网规约版本6的网络而言，决策局 / 部门可因应操作需要，允许以端对端方式连接互联网，但应考虑采取适当的安全措施，如使用临时互联网规约地址，使其他人无法对用户活动进行分析。
- 配置防火墙时应启动扫描通讯内容、恶意软件的功能。
- 防火墙应配置为堵截对个人网络电邮、公共云端存储和网络版即时通讯服务的未获授权访问。
- 防火墙应适当配置互联网规约地址层过滤功能。 任何已知或被怀疑是恶意的互联网规约地址或网站均须被堵截。
- 配置防火墙时应堵截不使用的通讯端口和过滤不必要的通讯，例如不必要的内进或外出互联网控制信息规约通讯。
- 应确保防火墙本身的实体安全。
- 防火墙政策应富弹性，以配合未来发展和适应安全要求的改变。
- 正确设定和编配防火墙档案权限。应尽可能限制系统档案权限。
- 应彻底测试防火墙，在正式推出作服务前应适当地检验防火墙配置。
- 在防火墙经过重大改动或升级后须进行测试。
- 应定期以修补程序和错误修补程序，更正及更新在防火墙安装的所有软件，以确保使用的软件版本恰当。
- 应为紧急事故设定实时警报机制。
- 应开启审计追踪功能，让任何由管理员或入侵者作出的配置修改都能得以追查。

3.2 防火墙管理

- 应妥善记录防火墙配置、管理及操作程序。
- 平行使用多部防火墙的配置应完全一致。
- 在可行的情况下，应以检验和来检查防火墙配置档案的完整性。
- 应定期记录及覆检防火墙的记录。
- 应为防火墙系统和配置档案备份。
- 妥善备存用户帐目是十分重要的。只有防火墙管理员和备份管理员获发防火墙用户帐目。对获授权用户应实施严格的访问控制，他们只可操作有助其履行职务的必要功能。
- 为防火墙管理员提供持续培训，这对防火墙的维修和管理至关重要。

- 应指派至少两名防火墙管理员（一名为主要管理员，另一名为辅助管理员）管理防火墙的运作。
- 局部区域网络管理员和防火墙管理员之间应建立有效的沟通渠道。
- 定期进行安全审计。主机系统亦应定期进行扫描和检查，以侦测常见的配置漏洞和错误。

4. 路由器

路由器用来连接两个或以上的网络。与应用系统代理服务器相似，路由器可过滤通讯，并限制访问到服务器或网络构件。

在配置及管理网络路由器时，应遵守以下指引：

- 与防火墙类似，路由器亦应妥善配置，除获准的服务外，应预设为拒绝所有服务。应关闭源路由功能，惟检修故障时，则作别论。
- 如同防火墙一样，路由器应妥善进行记录、备份和其它管理的工作。
- 在实际运作前应进行彻底测试。
- 如果路由器与防火墙一并使用，则路由器应符合防火墙政策。

5. 邮件网关安全

建立安全的邮件网关，应遵守和遵从下列指引。

5.1 邮件服务器设计及配置

- 邮件服务器应由防火墙系统作掩护，防火墙系统可以限制对邮件服务器的访问，并提供各种安全保护措施。
- 适当配置防火墙或路由器，以拦截不必要的通讯（例如由某个已知滥发电邮者的互联网规约地址所发出的通讯）进入邮件服务器或网关。
- 应采用抗恶意软件防护，过滤带有恶意软件附件的进出电邮。
- 电邮系统不应披露内部网络或系统的名称或互联网规约地址。
- 应适当配置电邮系统，以避免透过电邮的标题泄露内部系统或配置的资料。
- 内部电邮地址目录不应对外公开。
- 邮件网关应能记录所有电邮标题作审计之用。邮件网关应提供电邮如何、何时及何地寄入或发出等资料。
- 如有电邮轰炸或滥发电邮等情况，应尝试找出电邮的来源或真正源头，然后配置路由器或防火墙，以拦截或弃置有关电邮。
- 应关闭为未获授权用户或互联网规约地址传递邮件功能。
- 应为独立电邮系统启用发件人策略框架，并为寄出的邮件戳上域名密钥识别邮件签署，让收件方核实电邮是由政府寄出。
- 互联网邮件须受「网域型邮件验证、报告与一致性」规约的保护，这是一种邮件认证规约，可以让邮件网域拥有者能够保护他们的网域不受未经授权的访问，例如电邮仿冒。

5.2 电邮轰炸、电邮滥发及电邮仿冒

电邮轰炸是指重复地发出电邮，以塞满某个邮件网关或电邮信箱。电邮滥发是指向电邮用户发出他们不需要的电邮。电邮轰炸及电邮滥发均使互联网充斥着垃圾电邮。电邮轰炸／滥发者通常劫持其它邮件服务器，然后透过这些服务器发送邮件。

电邮仿冒是指用假冒身分来改动电邮发件人或电邮标题的其它部分等资料，使之看似另一用户或来源。如同时使用电邮仿冒和电邮轰炸／滥发进行攻击，将更难让人确定电邮发送者的真正身分。

邮件服务器如未能适当配置，便可能受到上述电邮攻击。电邮系统的所有资源被滥发电邮者掠夺后，可能因而瘫痪、不胜负荷，甚至遗失内部资料，而将服务回复正常的成本亦可能十分高昂。

以下是受到电邮攻击的一些迹象：

- 拒绝服务，例如磁盘已满或系统关闭。
- 大量电邮在很短时间之内由同一发件人寄入 / 寄出。
- 大量电邮从无效的来源地址寄入，或向无法寄达的地址寄出。
- 电邮从来历不明的源头寄入 / 寄出。
- 声称由管理员发出，要求用户寄出其密码或其它敏感资料复本的电邮。
- 要求用户将密码改为某指定值或字符串的电邮。
- 引导接收者至看似合法机构的欺诈性网站，以欺骗用户提供个人身分数据及私人数据（例如信用卡数据）。

以下是防范电邮轰炸、滥发电邮及电邮仿冒的一些提示：

- 移除不用的电邮服务器程序，例如 Sendmail。
- 确保邮件网关使用最新的版本。
- 开启记录功能，以记录仿冒电邮讯息的来源和标题。使用入侵侦测及防御系统来侦测任何可疑的活动，例如某寄件人所寄入 / 寄出的电邮突然大量增加的情况等，以协助侦测 / 防御电邮轰炸。
- 适当配置防火墙和路由器，只容许符合简单邮递传送规约的外来连接连结到指定的邮件网关或服务器，以集中记录和控制通讯。
- 应堵截来自未获授权或不存在的地址使用邮件转递。例如，邮件服务器应只容许一些指定的内部互联网规约地址或已获授权内部用户，使用邮件转递，而并非供外部用户使用。
- 应适当地配置电邮服务器程序或邮件网关软件所配备的过滤无效讯息功能，以清除一些未获授权网域所发出的垃圾邮件或无效的讯息。
- 限定每个电邮邮件大小上限，或在特定时段内可传送邮件数量的上限，以避免因电邮泛滥而耗尽网络资源或磁盘容量。
- 定期更新滥发电邮者名单。
- 设置电邮滥发的阻截系统，藉以过滤不需要的电邮。此电邮滥发阻截系统可发挥邮件网关的功能，按照多项标准（例如电邮标题、内容、电邮滥发黑名单、电邮滥发白名单、反向域名系统查询、发件人政策框架及邮件戳上域名密钥识别邮件资料）在电邮进入电邮服务器之前，筛除滥发电邮。

5.3 访问控制

- 只有获授权的用户可使用电邮服务。
- 利用密码或数码签署等认证模式以认证电邮。在传送电邮过程中，可确保邮件的来源和完整性。
- 限制获准访问电邮服务器的用户人数。
- 储存邮件在具有适当访问控制的地方。应小心处理邮件，确保其私隐。

6. 网站安全

网站安全是保护网站服务器、用户及内部网络的一系列程序、作业模式和技术。网站服务器及其组件如网站服务器操作系统、网络、应用程序 / 软件等，以及储存于网站内的数据都很容易招致互联网攻击。

由于网站服务器完全面对互联网，所以必须采取严密的主机和网络安全防护措施。本节所述的网站安全指南，应予严格遵守和遵从。有关网站及网上应用程序防范网上威胁的良好作业模式，请参阅《网站及网上应用程序实务指南》。

6.1 网站服务器配置及管理

网站服务器软件是在主机系统上运作，向用户提供数据或网上服务的应用程序。因应网站服务器往往面向互联网，以下的良好作业模式对架设及维持一个安全的网站服务器，至为重要。

- 关键网站、高负荷网站，或易受网上攻击的网站应寄存在分开的网站服务器内，以减少或避免网站服务器面对互联网时的潜在牵连伤害。要进一步加强安全，就应考虑让每个网站于分开的专属主机上运作。
- 网站服务器应配置为不提供任何简单邮递传送规约服务，以免外部用户利用网站服务器传递邮件。
- 所有服务器软件和应用程序的运行必须符合最小权限原则，尤其不应以管理员、超级用户或以根权限运行。
- 为网站服务器内的目录、档案和网页制订适当的访问权限。
- 所有不必要的网络服务、应用程序或互联网规约均不应该预设运行于网站服务器上。尤其是服务器管理员和内容更新渠道（例如档案传送规约、安全档案传送规约、安全壳规约）不应于互联网上公开。
- 尽可能移除或限制任何源自服务器端不必要的可执行程序代码，例如共享网间连接界面程序及服务器插入式部件。
- 在可行的情况下，为网站服务器指定一个独立的工作目录，以便在程序执行时建立 / 管理工作档案，并确保文件于工作完成后会被删除。
- 网站服务器管理工具，应只限获授权管理员透过有日志记录的身份认证系统才能访问。重要的配置档案，应只限管理员负责更新。
- 应每日密切监察网站的完整性和可用性，并运用入侵侦测及防御系统，侦测可疑活动，于未获授权窜改或访问发生时通知管理员及阻止有关活动。
- 停用所有不使用的账户，包括用户账户、服务和预设账户。
- 移除网站服务器上的所有预设档案或示范档案。

- 对网络爬虫程序施加限制，以免公众搜寻器搜寻到和储存不打算公开的内容。
- 应定期更换这些管理工具的密码，并禁止重复使用相同的密码。不要使用这些管理工具的预设密码。

6.2 访问控制

- 应使用强认证方法进行用户认证。不应只以互联网规约地址限制作用户认证，因为来源的互联网规约地址可以是仿冒的。
- 禁止匿名或未获授权用户，访问或更新目录或数据档案。
- 只有已登记用户才可享有访问权限。限制可供登入服务器的账户数目。审查和定期删除的账户。
- 应关闭所有不需要的账户，尤其是访客账户。
- 访问记录必须符合适当的管理程序 / 账户。
- 储存于外部网站服务器上的敏感信息，应采取强化的加密并要求认证的措施以作保护。

6.3 网站内容管理

- 在生产前或重大改动后，彻底测试和检查所有网站和网页。
- 应实施控制以确保除获委托及获授权人士外，其它人无权在生产环境张贴和更新网页。
- 如果不同的组别，甚至不同部门须共享网站服务器，各组别、部门应使用不同的网站内容目录或资源，这些目录应实施访问控制，以限制访问、执行和储存有关的网站应用程序。
- 网站应用程序不得设置连结通往储存于指定网站目录以外的内部档案。
- 应对资料夹及档案采取适当的访问控制，确保用户不能访问任何储存在网站服务器内，非让用户访问的档案。
- 应保存用户访问记录，例如对系统档案尝试进行非授权访问，使任何不正常或可疑的活动能得以追查
- 不应授权网站内容开发人员管理操作系统和网站服务器。
- 为在网站服务器张贴或更新网页和应用程序，制订网站内容管理程序。
- 对于接受用户数据输入的网页窗体或应用系统，所有输入的数据在进入后端应用系统前，应先进行适当的核对、验证及净化，使任何预期以外的输入，包括过于长的输入、不正确的数据种类、以及预期以外的负数、数据范围或字符，能被妥善地处理，而不会成为攻击应用系统的途径。
- 应移除生产服务器内不需要的内容，如显示于系统横幅的平台资料、说明数据库、联机软件手册及预设或示范档案等，以免披露系统资料。

6.4 共享网间连接界面程序及应用程序界面

共享网间连接界面程序及应用程序界面通常用来扩充网站服务器，以加强性能。与网站服务器一并供应的预设共享网间连接界面程序可能在无意中提供了访问网站内容的「后门」。程序可泄漏有关主机系统的内部资料，而且很容易招致攻击。此外，共享网间连接界面程序往往允许用户输入数据。

应遵守和遵从的项目如下：

- 适当设计、测试和检查共享网间连接界面程序和建基于应用程序界面的程序，确保脚本和程序只能够提供所需的功能。除非预设或特制共享网间连接界面程序及应用程序界面已经过彻底测试和验证，否则不得保留在服务器内。
- 应在受限制的环境（例如在指定目录）中运行及储存这些程序，以限制访问，同时可便于进行维修。
- 这些脚本及程序只可获授权执行，但并无阅读或写入权限。对系统资源的使用应予限制，例如中央处理器时间、超时时间和磁盘使用情况。同时，应适当限制访问其它数据档案或资料。
- 编译程序、解译程序、介壳程序及脚本引擎等程序不应放置在程序档案的预设目录内，而应安全地放置在适当的目录。如果不再需要这些脚本及程序，应彻底将它们从网站服务器移除。
- 应在传送到服务器软件或相关操作系统前适当地检查、核对和净化，用户在这些程序所输入的数据，以防止数据在指令行运行。

6.5 认证

- 在可行的情况下，远程管理控制应采用数码证书、智能卡和权标等强化认证模式，这些强化认证模式亦可用于关键应用系统、服务器和客户的认证程序。
- 采用如安全超文本传输规约的加密联机，以传送敏感资料。安全超文本传输规约须在所有互联网服务中推行，以增强互联网服务的真确性以及内容的完整性。

6.6 网络浏览器

应适当地配置网络浏览器。以下是配置网络浏览器的一些建议：

- 应通过获授权通讯渠道，例如互联网网关访问互联网。
- 关闭电邮应用系统 / 浏览器的启动动态内容的任何选项，例如 Java、JavaScript 和 ActiveX，与可信赖来源通讯则除外。

- 在开启任何下载档案前先行扫描恶意软件。
- 使用最新的浏览器，并采用最新的安全修补程序。
- 关闭自动输入密码 / 密码记忆功能。
- 除非所连接的网站可信赖，否则启动拦截弹出窗口功能。
- 定期移除浏览器内的快取档案或临时档案，以保障资料私隐。
- 安装插入式部件、附加组件或软件前，应先检查及测试有关程序。安装过程亦只应由获授权人士进行。

6.7 主动式内容及小型文本文件

主动式内容使提供信息的服务器能够裁制在客户端浏览器显示的执行脚本，例如 Java 微应用程序和 ActiveX。须留意流动装置浏览器一般不支持插入式部件，而随着流动装置浏览器使用的增长，插入式部件的技术正逐步转移至无插入式部件技术。决策局 / 部门应在软件供货商的正式网站内检查插入式部件的支持终止日期，并事前准备一套可能的转移方案。

小型文本文件是服务器与客户端浏览器以无状态的超文本传输规约连接时，用来掌握用户状态资料的一种机制。

6.7.1 Java 微应用程序

Java 微应用程序是通常嵌入网页内的程序。客户端的浏览器可能会自动下载 Java 微应用程序以便执行。 Java 限制其微应用程序只可进行一部分安全操作，称为「沙盒」，使这些微应用程序难以破坏档案系统或计算机的开机扇区。在发展 Java 微应用程序时，发展人员应设计并限制 Java 微应用程序只可访问指定的目录、档案和操作系统。

在客户端运行 Java 微应用程序时，亦应考虑以下事项：

- 收紧对 Java 编译程序、解译程序及生成程序的安全控制。在生产环境中，删除并不需要的编译程序、解译程序及生成程序。
- 了解有关 Java 微应用程序安全漏洞的最新资料，并采用最新的修补程序。
- 宜只在有需要的时候才在浏览器内启用 Java 微应用程序。

6.7.2 ActiveX

ActiveX 是一种可透过网页浏览器使用的软件控件，可用于创建分布式应用系统的工作。ActiveX 控制是设计以让网络浏览器能下载和执行。ActiveX 控件是被嵌入在网页内，但对于 ActiveX 所能够进行的操作却并无限制。例如，

ActiveX控件可留驻在系统中，亦可在没有用户授权的情况下删除数据或写入本机硬磁盘。并且，浏览器也无法记录这些控件在客户端计算机进行过的操作。

应默认关闭 ActiveX。若有需要执行 ActiveX，应小心验证及评估有关的ActiveX 控件。相关的安装亦只应由获授权人士进行。软件编写者可以于ActiveX控件内采用由核证机关发出的认证数码签署技术。通过这种方式，客户端可以根据验证签名确认作者的身份，然后才决定接受或拒绝控制的运行。切记，数码签署只能够显示 ActiveX 控件由何人编写，但不能协助用户决定控件是否可以信赖。用户应认真考虑并只接受来自可信赖来源的控件，或应评估并于浏览器设置中禁止「ActiveX 控件和插件」，以禁止系统上不需要的ActiveX运行。

6.7.3 小型文本文件

小型文本文件是服务器上的机制，将资料储存在客户端以供服务器提取。小型文本文件向服务器提供如曾访问的网址、用户电邮地址和敏感资料等用户状态资料。攻击者可仿冒服务器，以撷取客户端的小型文本文件。

系统发展人员应注意让小型文本文件储存过多私人数据并不恰当。不要在小型文本文件储存纯文本的用户名称和密码。如果小型文本文件须要储存认证资料，应对整个小型文本文件进行加密。系统设计人员还可加入一些控制资料，例如到期日期及时间来限制小型文本文件有效期，以减低小型文本文件的潜在危害。

7. 远程访问

远程访问是指在没有直接连接网络的远程地点使用网络资源。远程访问有很多不同的方式，例如拨号访问及虚拟专用网络。

7.1 拨号访问

拨号访问是在公共电话网络上进行远程访问的一种形式。只有获授权人士可使用拨号访问。决策局／部门应不断更新其拨号访问点及调解器线路的清单。建议透过用户认证保护拨号访问，且应定期更换拨号密码。在某些情况下，可能需采取双重认证。

决策局／部门亦应考虑使用回拨安全功能。启动回拨安全功能后，应答调解器会接收拨入的呼叫并认证用户身分。当用户通过认证，调解器会中断呼叫，然后使用默认数据库内的电话号码向用户回拨。该项功能有助于防止未获授权访问或使用窃取的凭证。虽然回拨功能可加强安全，但攻击者仍有可能透过呼叫转移入侵系统，因此还应采取其他安全控制措施（如对拨号连接至敏感环境的连接实行双重认证）。

每次拨号要求应留下访问记录。记录至少应包括以下资料：访问日期、时间、访问持续的时间、用户名称及连接的通讯端口。访问记录应可供有关主管检阅。

此外，就拨号访问，应跟从以下的良好作业模式：

- 清晰界定哪些用户会获得远程访问权限，以及他们会得到什么类型服务。
- 只应让获授权用户在适当认证及记录下，获得网络的远程访问。
- 妥善配置防火墙系统以限制远程访问。
- 远程访问服务器及调解器群应得到实体保护。
- 建议使用中央调解器群，提供简易及有效的管理和控制。
- 应记录对远程访问服务器的连接，包括记录登入会话的起始及终结、连接开始及终止的时间，及对远程访问服务器用户帐户的更新或删除等。
- 应在这些连结上进行传送时，以加密方法保护用户凭证或数据。
- 接入服务可以因重复的拨号而服务中断。可设定逾时计时器或拨入时间限制减底服务被中断的机会。

7.2 虚拟专用网络

虚拟专用网络透过一种称为隧道的技术在不可靠的网络上建立安全连接。隧道技术在第二层或第三层网络协议运作，将讯息小包封装，以便在网络上传输。现时有不同的隧道协议，例如互联网协议安全及第二层隧道协议。

除传统的第二层及第三层虚拟专用网络外，安全套接层虚拟专用网络是另一种可提供网络隧道技术保护的虚拟专用网络技术。在安全套接层虚拟专用网络中，网络隧道技术应用于传输层安全通讯对话。安全套接层虚拟专用网络与传统的虚拟专用网络不同，它的运作不需要虚拟专用网络客户软件，而传统的虚拟专用网络通常需要客户软件。

设立虚拟专用网络是建立安全通讯渠道的可行方法，可让在办公室以外地点工作的人员使用。在推行虚拟专用网络前，决策局 / 部门应评估虚拟专用网络与现行网络是否兼容并考虑执行下述虚拟专用网络安全指引：

- 使用令牌等一次性密码认证机制，或以较复杂密码组成的公开 / 私人密码匙系统认证，作为远程接达的第二重认证。
- 如在一段指定的时间内没有操作，应自动终止与政府内部网络的连接。用户须重新登入才能与网络连接。
- 禁止使用双重（分隔）隧道技术。只允许单一网络连接。
- 保护所有透过虚拟专用网络与政府内部网络连接的计算机或装置，如使用个人防火墙、最新安全修补程序、抗恶意软件侦测与修复软件。所有这些安全措施应经常处于启动状态，且具有最新的恶意软件标识符及定义。
- 为登记用户和端点设置白名单。
- 远程访问计算机或装置的使用须遵从政府信息技术安全要求。私人拥有的信息技术设施不可连接至政府内部网络。若有运作上的需要，须先征求部门信息技术安全主任的批准。
- 透过记录及审计功能以记录网络连接情况，尤其是记录未能访问的情况。此外，亦应定期覆检记录，以识别任何可疑的活动。
- 提醒拥有虚拟专用网络使用权限的用户，他们有责任适当地使用账户，及确保未获授权用户不得使用该帐户访问政府内部网络。
- 培训局部区域网络／系统管理员、支持人员及远程用户，以确保他们在建立及使用虚拟专用网络时遵守安全良好作业模式及政策。
- 安装防火墙于网关，以控制从虚拟专用网络客户至获授权信息系统或服务器之间的网络通讯。

8. 域名系统服务器

域名系统服务器提供域名与互联网规约地址配对的支持。域名系统服务器可提供不同数据，例如在指定领域内所有主机的互联网规约地址清单、互联网规约地址转为主机名称的配对及用户电邮地址等。

为保障域名系统服务器的安全，应遵守和遵从下列指南：

- 使用最新的域名系统服务器软件或服务套装软件。
- 对域名系统采取安全保护措施，例如控制域名系统数据库档案的访问权限，和使用强化加密系统。
- 记录互联网规约地址的赋值资料，例如主机位置和主机资料。这些记录可作为域名系统服务器遭攻击时的备份、检验和审计清单。
- 对于向内部用户提供域名系统解析服务的域名系统服务器，应备存域名系统查询的使用趋势基准，以便在发生异常状况下，对可疑恶意活动或从内部网络连接外部的非法连接通道作出调查。
- 对于向公众提供域名系统解析服务的域名系统服务器，应关闭递回搜寻功能，并应限制域名系统的回应速率，以防止域名系统服务器参与域名系统放大分布式拒绝服务攻击。亦应阻止对知名网站或不会产生域名系统查询的地址作回应，以防止参与攻击重要基本建设，例如十三个根域名系统服务器及服务国家和地区顶级域名的域名系统服务器。

8.1 域名系统安全扩展

域名系统经常受到难以抵御的中间人、仿冒及快取污染等攻击。域名系统安全扩展可核实域名系统的回复信息，为网络提供多一重保护。域名系统安全扩展采用公开密码匙加密技术，以验证域名系统记录的真确性。通过查核数码证书，客户端计算机可相信所接收的资料未遭修改或窜改。此外，域名系统安全扩展可保护用户免被引导往恶意网站。

为加强互联网资源的真确性，互联网网域的资源记录须受域名系统安全扩展保护。就域名系统安全扩展的推行，决策局 / 部门应考虑：

- 设计签发系统 — 须考虑如何整合该系统与现有的域名系统结构，以及现行域名系统管理程序的修订。
- 在测试环境中签发 — 对外推出系统前，应测试整个系统，包括在测试环境中测试所有订明程序。
- 检查域名系统服务器 — 核证支持域名系统安全扩展的外部具权威的域名服务器。

- 产生及管理密码匙 — 应策划产生、发布和管理密码匙的程序，以及密码匙的长短与使用期限。
- 制订紧急程序 — 应就密码匙破解事故制订程序，以便重新产生密码匙及签发区域。

内容分发网络服务提供了更快的内容分发，以分布式方式复制和储存内容。然而，内容分发网络在支持域名系统安全扩展的程度上有可能出现局限。若此情况出现，由决策局 / 部门拥有的网域名记录须由域名系统安全扩展保护，而较低层的网域名应尽可能由域名系统安全扩展保护。

8.2 域名系统堵截

域名系统堵截是决策局 / 部门保护其网络免受在线威胁的一项重要功能。它包括使用域名系统堵截域名以阻止对特定网站或在线资源的访问。决策局 / 部门应评估安全风险，并根据业务需要决定适当的堵截机制。

域名系统堵截的工作原理是根据预定的黑名单检查域名堵截用户请求。如果发现该域名在黑名单中，则域名系统服务器会回应被堵截信息不是互联网规约地址，从而阻止用户访问该网站。

下面列出了建立和维护黑名单时的注意事项：

- 恶意域名
- 可疑域名
- 指令与控制服务器
- 仿冒诈骗和诈骗域名
- 已知的恶意互联网规约地址
- 新出现的威胁

通过实施域名系统堵截，决策局 / 部门可以执行内容过滤政策、预防访问恶意网站、防范仿冒诈骗攻击，并降低恶意软件感染或数据泄露的风险。 它充当额外的防御层，与其他安全措施相辅相成，增强决策局 / 部门的整体安全策略。

8.3 保护性域名系统

保护性域名系统阻碍了使用域名系统散布和操作恶意软件。保护性域名系统的核心功能是能够根据威胁情报对域名进行分类。保护性域名系统服务通常利用已知恶意域名的开放源代码、商业和政府信息源。这些信息源可以覆盖网络入侵周期中多个阶段发现的域名。

保护用户的域名系统查询是一项关键防御措施，因为网络威胁者在整个网络入侵周期中都使用域名：用户在尝试导航到已知良好的网站时会经常错误输入域名，从而无意中访问恶意网站；威胁者在仿冒诈骗电邮中嵌入恶意链接；被入侵的装置可能会从远程指令和控制服务器寻求指令；威胁者可能会从被入侵的装置向远程主机泄漏数据。恶意内容相关的域名通常是已知的或可知的，防止对其域名进行解析可以保护个人用户和企业。

保护性域名系统可从源头上阻止如恶意软件、勒索软件、网络钓鱼攻击、病毒、恶意网站和间谍软件的访问。保护性域名系统数据可以作为威胁情报来源纳入安全信息和事件管理工具中，以帮助识别和防范威胁。通过将此类数据纳入安全信息和事件管理，决策局 / 部门可以将各种安全日志整合到单一接口仪表板视图，为保护性域名系统的堵截提供进一步的背景信息。

在选择保护性域名系统服务供应商时，决策局 / 部门应考虑以下能力：

- 堵截恶意软件域名
- 堵截仿冒诈骗域名
- 恶意软件域名生成算法保护
- 利用机器学习或其他启发式方法来增强威胁来源频道
- 内容过滤
- 支持应用系统开发界面访问以进行安全信息和事件管理集成或自订分析
- 网页界面仪表板
- 验证域名系统安全扩展
- 具备域名系统的安全规约 / 通过传输层安全规约来加密并打包域名系统的安全规约
- 支持按组、装置或网络定制政策
- 可跨混合架构部署

9. 入侵侦测及防御

要维持互联网网关的安全，需要持续及全面的系统操作、支持和监察，以对不当、异常或可疑的活动或事故，作出防范、侦测、应急和升级处理。通过适当的人手操作程序，如覆检和分析记录或统计，测试并演习事故处理程序，便可达到上述目的。

在可能的情况下，应在策略性位置使用及安装入侵侦测及防御系统工具，不断收集及检查可疑活动的数据。可一并使用基于网络和基于主机的入侵侦测及防御系统工具。前者负责检查在网络传输的网络小包，后者则负责监察单一主机系统上的系统配置和应用程序活动。

不当配置和使用不当工具可导致向攻击者泄露资料，并造成安全假象。

- 使用入侵侦测及防御系统工具鉴别网络和主机的可疑活动，尤其是网站服务器和邮件服务器。
- 设置由电子信息或流动传呼自动发出警告或警报的功能，在侦测到攻击迹象时向系统管理员发出警报。
- 在可行的情况下，采用能够针对可疑网络活动作出应急的系统或功能，以及时中断或堵截可疑网络活动的连接，并作记录以供事后分析。
- 在使用入侵侦测工具前应适当地测试和检验这些工具。
- 妥善控制和限制这些工具的使用和管理。
- 应适当配置防火墙系统，尽可能保护和隐藏这些工具。
- 应确保使用最新的攻击识别码档案。
- 正式使用最新的标识符档案及拦截规则前应彻底测试及验证。应测试更新内的新 / 修改后标识符和拦截规则是否能如预期般运作，以及会否与原来标识符和拦截规则发生冲突。
- 就使用入侵侦测工具应制订适当的操作、管理和监察程序。这些程序应当定期覆检以确保网络配置的更新。

入侵侦测及防御系统工具的策略性位置，可以是防火墙、主机或者任何重要的信息资产。可以在互联网通讯闸基础设施中引入安全的互联网通讯闸作为第一重防线部署在互联网和现有的互联网通讯闸之间以防范来自互联网的威胁。可以将这类安全的互联网通讯闸配置成允许入侵侦测及防御，做到网络过滤，超文本传输安全规约通讯检查，侦测恶意互联网规约地址和网域，或者阻止及监测网络通讯，侦测恶意软件并防止信息系统被感染。

10. 其它安全考虑事项

除上述特定的网络构件外，还有一些安全问题应予考虑。下一节将讨论部分相关问题。

10.1 实体安全

- 确保所有网关构件的实体安全，所有构件应放置在受管制的地点。
- 放置这些设备的计算机室应具备完善的设施，以防范实体或自然灾害。
- 使用可上锁的储物架，以存放这些构件。
- 定期监察及覆检现有的实体安全情况，例如检查场地的出入口或访问记录、检查是否有任何未获授权窃听线路、检查储物架的门锁和粘贴标签。
- 在弃置储存媒体前，移除及删除所有资料，尤其是有关系统配置的资料。

10.2 记录

- 在可行的情况下，应开启防火墙、路由器、操作系统、网站服务器和邮件服务器的记录功能。
- 备存记录，如误差记录、系统记录、访问记录、网站服务器记录和邮件服务器记录，并确定有足够的可用存储容量。
- 记录信息，例如无效账户登录的尝试、网站账户的滥用、非法或未经授权到网站的尝试、管理和配置更新、或具体访问信息，如要求者的互联网规约地址、主机名、划一资源定地址和访问文件的名称等。
- 定期覆检记录，并将记录存放在安全的地方不少于一星期。可使用只读光盘等一次性写入设备记录这些档案。
- 应妥善保留载有入侵和攻击数据的记录，以供调查和记录。
- 在设计记录数据的类型和细节时，应考虑到私隐权。

10.3 备份及复原

- 应制订并妥善记录正式的备份及复原程序。
- 应定期或在更改配置时，为所有网关构件的配置、记录档案、系统档案、程序、数据和系统的其它数据作备份。必要时可将备份资料加密。
- 备份复本应存放在安全的地方。系统配置宜备存两份备份复本，一份放置于场内，另一份则存放在场外。

10.4 防范恶意软件

- 启动抗恶意软件保护功能或恶意软件侦测功能，以检查所有来自互联网的通讯，并自动清除恶意软件。
- 配置网关时应过滤、隔离 / 删除含有恶意内容的网络通讯，并建立审计记录以供日后调查。
- 应定期更新恶意软件识别码及定义。宜配置为自动更新，且至少应每日更新一次。
- 倘若无法进行自动更新（例如并非经常访问网络的流动计算机），则至少应每周手动更新一次。
- 用户亦应注意，突发性及严重的恶意软件会不时爆发。如果发生上述情况，用户应遵从有关指示，并实时更新最新的恶意软件识别码及定义，以防范恶意软件爆发。
- 定期为安装数据服务器的主机进行恶意软件扫描。

10.5 操作系统安全

由于网络应用软件均在操作系统上运作，所以选择操作系统时应慎重考虑安全要求。操作系统的弱点或安全漏洞可能会影响应用软件的安全。

在选择操作系统时，尤其是防火墙和关键服务器，应挑选安全的操作系统平台。在各种操作系统中，宜选择具备下列功能的操作系统：

- 多重同步程序
- 安全档案访问权限和控制
- 能否追究用户和系统行动的责任，并对此进行审计，例如具备详尽的事件记录
- 对系统的所有用户进行识别和认证。在签名 / 定义更新后，用户应在电脑上进行全系统扫描，以侦测任何可能存在的有关恶意软件。
- 资源分隔，例如控制重新使用系统对象（已删除的档案、配置记忆）

不同的操作系统有不同的方式令配置更为安全。以下所列举的示例可供一般操作系统参考。

- 移除或关闭所有非必要服务或程序，尤其是不用的预设操作服务和程序。
- 在可能的情况下移除非必要预设账户，或以强化密码作为所有预设账户的密码。
- 高权限操作程序的数目应减至最低。严格分配操作权限。

- 为预设档案权限设定限定默认值。
- 为系统管理员账户设立强化密码，并定期更改密码。
- 规范操作系统版本和软件，并将操作系统版本和软件的数目减到最低，以便安装和维修。
- 定期安装操作系统更新程序，并采用最新的操作系统修补程序，尤其是与安全问题相关的修补程序。

10.6 点对点网络

点对点档案分享系统是一种基于网络的应用程序，让点与点（即参与的计算机）之间利用互联网互相直接交换档案。点对点档案分享系统利用点对点网络模型，让每部计算机都是同时扮演用户端与服务器的角色。这开放了一个渠道，让储存在内部网络中用户计算机裹的档案上传到互联中的其他计算机。

点对点技术的潜在安全风险包括：

- 不当配置可能会导致资料于使用点对点应用程序时外泄。被分享档案以外，储存在同一工作站或储存装置内的其他档案亦可能不知情地遭外泄。档案一旦上传到其他计算机后，就很难从点对点网络上完全删除。
- 点对点应用程序需要于防火墙开放一定数量的埠后才能运作。每个在防火墙开放的埠都可能成为攻击者用作攻击网络的途径。
- 由于点对点网络促进计算机与计算机间的档案分享，恶意软件亦可利用这途径，将自己传播到其他计算机上。
- 点对点应用程序可能本身存有漏洞，能让攻击者传播恶意软件，入侵网络或发动拒绝服务攻击。
- 当使用点对点软件下载档案时，几乎不可能知道档案由谁制造或档案是不是可靠。若档案牵涉任何非法内容，下载档案的人士有可能需要面对刑事或民事诉讼。
- 在决策局 / 部门网络内使用点对点应用程序可能会产生大量网络流量，垄断网络带宽，影响其他重要业务应用程序。
- 因为点对点技术依靠用户工作站，不能从服务器端管理，所以所有在服务器端推行的安全措施都不会对点对点分享有任何作用。

以下列出减低点对点技术带来的风险的良好作业模式：

- 决策局 / 部门应对业务环境中采用点对点技术作出慎重考虑。除非有强烈及特殊业务情况支持，否则并不鼓励使用点对点技术作档案分享。任何情况下，保密或个人资料都不应在点对点网络上分享。
- 若无需使用点对点网络，就应制订安全政策以阻挡所有无需使用的埠。应定期提醒人员不要在工作站上安装点对点应用程序。

- 关键网络上的通讯应由入侵侦测及防御系统监察，并应对任何未经批准的点对点通讯进行调查及阻截。应订立清晰的防火墙政策，容许最少数量而有需要使用的网络埠。
- 若认为有需要使用点对点技术，有关软件应安装在配有专用互联网连线，及经谨慎配置的独立工作站上，而有关的默认设定亦必须在使用前经过检查。应删除所有不必要的用户权限及工作站上共享的档案／目录，以避免非分享用的档案遭意外外泄。

10.7 安全风险评估及审计

应定期、在重大变更后及运作前进行安全风险评估。安全风险评估须每两年进行一次，其目的在于覆检现行的安全措施，以及找出任何潜在的安全漏洞。

安全审计可以是对现行安全政策的一般覆检，也可以是利用各种安全评估工具进行的技术覆检。应审慎使用这些工具来扫描主机系统和网络，以找出安全漏洞。安全审计的目的是确保现有的保护机制符合现行安全政策。

- 应明确界定审计范围和目标，确保审计已涵盖所有目标网络构件。
- 在运作前应进行技术审计覆检。网关内的各个主机都需要进行基于主机的扫描，尤其是操作服务和档案权限。
- 应彻底审计防火墙政策的规则及获准的服务。
- 应检查密码机制及确保其功效。
- 应从网络构件移除审计测试结果和数据，而有关结果和数据应存放在安全的地方。
- 应控制扫描工具的使用，以防止未获授权人士使用。
- 尽快跟进审计建议。

10.8 系统管理及操作

- 应妥善管理及维护用户账户。
- 未经决策局局长／部门首长正式批准，禁止用户或人员安装或运作网站服务器或邮件服务器，以访问互联网。
- 明确界定和分派并记录全体系统管理人员的职务和职责。
- 应妥善制订并遵守互联网网关程序，例如变更及配置管理控制程序（尤其是防火墙）、备份及复原程序、网站内容管理程序和其它相关程序。
- 应在主机安装和运作安全模式的程序或软件以防止意外的改动，并安装修补程序或更新程序。
- 关键组件应由内部连接的终端机直接管理，或采用权标、智能卡、质疑／应答或一次性密码等强化认证工具。
- 定期检查联机安全讯息或档案，例如技术建议和安全事故或漏洞。

- 应覆检和修改配置，以对应更改要求、新兴的安全威胁或漏洞等环境转变。
- 系统所显示的欢迎登入、问候或错误信息可能会泄露系统资料。适当时应关闭这些信息功能。
- 在可能的情况下，安装管理工具或服务，例如使用全场安装修补程序软件，以集中系统的管理和安装工作。

完

附件 A　建议就互联网网关安全采用的保护措施的样本清单

项目	建议的保护措施
防火墙	*防火墙配置*
	传入 / 发出的所有通讯应经过防火墙
	以「除明确获准的服务外，拒绝所有服务」的防火墙政策为基础
	审慎规划和评估获准的服务
	开启网络地址转换功能（如有）
	开启内容过滤和恶意软件扫描功能
	堵截对个人网络电邮、公共云端存储和网络版即时通讯服务的未获授权的访问
	适当配置互联网规约层过滤并堵截恶意网络规约地址
	制订富弹性的防火墙政策，以备未来发展
	正确设定和编配防火墙档案权限
	在运作前和重大变更后彻底测试防火墙
	确保防火墙安装的所有软件均为恰当版本的软件
	设定实时警报机制
	如非必要，否则禁止由外部网络所发的档案传送规约或远程登录通讯传送到内部网络
	保障安装防火墙的操作系统的安全
	防火墙管理
	妥善记录防火墙配置、管理及操作程序
	当平行使用多部防火墙时，使用完全相同的配置
	定期检查配置档案的完整性，例如运用校验和
	定期记录和覆检防火墙记录
	定期为系统和配置档案备份
	妥善备存管理和用户账户，并定期更改密码
	为防火墙管理员提供持续培训
	指派至少两名防火墙管理员
	列防火墙管理成为安全事故处理的一部分
	在局部区域网络管理员与防火墙管理员之间，建立有效的沟通渠道
	定期进行安全风险评估和审计

项目	建议的保护措施
入侵侦测及防御	*操作控制*
	制订人手操作控制程序
	定期覆检及分析记录
	监察及分析用户及系统活动
	入侵侦测及防御系统工具（如已使用）
	使用这些工具于网络和主机，尤其是网站或邮件服务器
	设置自动发出警告或警报功能
	采用能够针对可疑活动而作出应急的功能，例如中断或堵截连接
	在使用前适当测试和检验
	控制和限制这些工具的使用
	适当保护及隐藏这些工具
	确保使用最新的攻击识别码档案
	为使用这些工具制订并覆检操作、管理及监察程序
防范恶意软件	*侦测及防御恶意软件*
	启动抗恶意软件措施以扫描所有输入的通讯。配置网关时应过滤、隔离 / 删除含有恶意内容的通讯，并建立审计记录以供日后调查
	采用最新的恶意软件识别码及定义
	定期进行恶意软件扫描
	开发中或用作测试的计算机设备或软件亦应遵守相关的信息安全措施及程序
	在计算机访问政府网络之前，对计算机进行全面扫描
	外聘供货商应在安装新机、维修服务和安装软件后以最新的恶意软件识别码进行恶意软件扫描
安全政策、指南及标准	*制订及执行安全政策、指南及标准*
	自订互联网网关安全政策
	制订相关的操作程序，例如变更和配置管理控制程序、备份及复原程序、网站内容管理程序
	制订安全事故处理和报告程序并定期进行测试
	分派和界定系统管理及维修人员的职务和职责

项目	建议的保护措施
	提醒并培训用户遵守及遵从政策
安全风险评估及审计	*进行安全风险评估及审计*
	至少每两年进行一次安全风险评估，并定期进行安全审计
	在正式运作前或重大变更前进行安全风险评估
	明确界定安全风险评估及审计的范围和目标
	由第三者进行审计
	审计防火墙政策
	确保密码管理的有效性
	保障审计结果和数据的安全
	控制对评估及审计工具（如有）的访问
	尽快跟进评估及审计建议