數字政策辦公室

資訊保安

互聯網通訊閘保安

實務指引

第 2.1 版

2024 年 7 月

版權公告

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	G50 互聯網通訊閘保安指引第 5.0 版已轉換成互聯網通訊閘保安實務指引。有關文件修訂可於政府資訊科技情報網查閱：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	基於最新的《資訊科技保安指引》(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	基於最新的《資訊科技保安指引》(G3) v10.0 而作出的修改	2, 8-9, 11,12, 29-31	2.0	2024 年 4 月
4	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」		2.1	2024 年 7 月

目錄

1. 簡介

任何支援互聯網設施的決策局／部門都需要保護本身的資訊系統及數據資產，防範非法接達或公共入侵。應令所有源自部門網絡的互聯網接達都統經中央安排的互聯網通訊閘或決策局／部門本身的互聯網通訊閘。

本文件為互聯網通訊閘提供技術指引，以安全地使用互聯網接達及服務。這些指引針對互聯網公開平台，是維持保安風險於可接受水平的良好作業模式。這份文件專為參與互聯網通訊閘操作及技術工作的人員而制訂。

由於本文件所載為一般性資料，不是為任何特定的電腦平台而編製，讀者應衡量個別環境考慮以選擇適用的資料。

1.1 目的

本文件就下列主要保安範疇提出指引：

- 互聯網通訊閘概覽
- 防火牆
- 路由器
- 郵件通訊閘保安
- 網站保安
- 遠程接達
- 域名系統伺服器
- 入侵偵測及監察
- 其他保安考慮事項

本文件旨在提供有關互聯網通訊閘良好作業模式的資料，並應與既定的《保安規例》、資訊科技保安政策、指引及程序一併使用。

1.2 參考標準

以下的參考文件為本文件在應用上的參考：

- 香港特別行政區政府《保安規例》
- 香港特別行政區政府《基準資訊科技保安政策》（S17）
- 香港特別行政區政府《資訊科技保安指引》（G3）

- 香港特別行政區政府 —《公開資料守則》
  http://ref.ccgo.hksarg/csogc/tc/c201002c.pdf
- “Site Security Handbook”, RFC2196, 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 術語及慣用詞

本文件將會採用《基準資訊科技保安政策》和《資訊科技保安指引》內所使用，以及以下的術語及慣用詞。

縮寫及術語	
無	無

1.4 聯絡方法

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電郵： it_security@digitalpolicy.gov.hk

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

CMMP 電郵： IT Security Team/DPO

2. 互聯網通訊閘概覽

互聯網通訊閘是互聯網專用連接的界面。不論界面與部門或政府內部網絡是否有連接，互聯網通訊閘提供了與互聯網的連接點。安全的互聯網通訊閘可收緊控制，並建立更具成本效益和安全的操作環境。

由於互聯網屬於開放性平台，加上複雜的網絡服務和應用系統發展迅速，通訊閘缺乏保安措施可能令內部網絡容易遭受攻擊。因此，互聯網通訊閘的配置必須恰當，並應採取適當的保安措施以保護通訊閘免被攻擊。

決策局／部門可利用数字政策办公室託管的中央互聯網通訊閘，但決策局／部門最終仍需要負責確保已實施足夠的保安措施。

在當今不斷轉變的網絡安全形勢中，當配置互聯網通訊閘時考慮到新興趨勢（例如零信任架構）是非常重要的。

零信任架構融合了網絡分段、微分段、強認證、最小權限、持續監察和強加密等原則，以確保更精細、穩健和動態的保安態勢。它強調了整個網絡中身份認證、授權和持續評估信任的重要性。

零信任架構並不完全依賴邊界防禦，而是同樣重視在任何位置的保護數據、應用系統和用戶的安全性。 這種方法符合現代網絡不斷轉變的特性，在現代網絡中，資源分佈在多個環境中，包括雲端服務、本地系統和遠程裝置。

決策局／部門需要辨識到基於邊界的架構的局限性，並考慮採用更先進的安全框架，例如零信任，以改善保安態勢，更有效地偵測和應對威脅，並適應當今互聯和動態網絡不斷變化的性質。

2.1 網絡互連

互聯網通訊閘往往與內部網絡互連，使內部網絡能夠接達通訊閘服務。然而，在互連網絡時必須加倍小心，以確保網絡互連不會降低或削弱現有保安水平至無法接受的程度，也不會損害所處理資料的安全性。因此，互連各方必須：

- 維持在自有網絡、主機和系統所實施的特定保安防衛措施
- 維持本身的保安政策和指引，但這些政策和指引應配合互聯網通訊閘的有關政策和指引
- 建立嚴格的互聯網通訊閘邏輯接達控制
- 為互聯網接達和服務制訂保安事故處理和報告程序

- 提醒並培訓用戶遵守及遵從相關的保安政策、指引和程序。

2.2 建議採用的保安措施

僅提供互聯網接達服務的安全互聯網通訊閘應配備以下保安功能：

- 防火牆（接達控制）
- 小包過濾路由器（通訊路由和小包過濾）
- 入侵偵測及防禦系統（記錄、監察、偵測及制止攻擊）
- 防範惡意軟件（監察網絡通訊，偵測惡意軟件，和防止系統受感染）

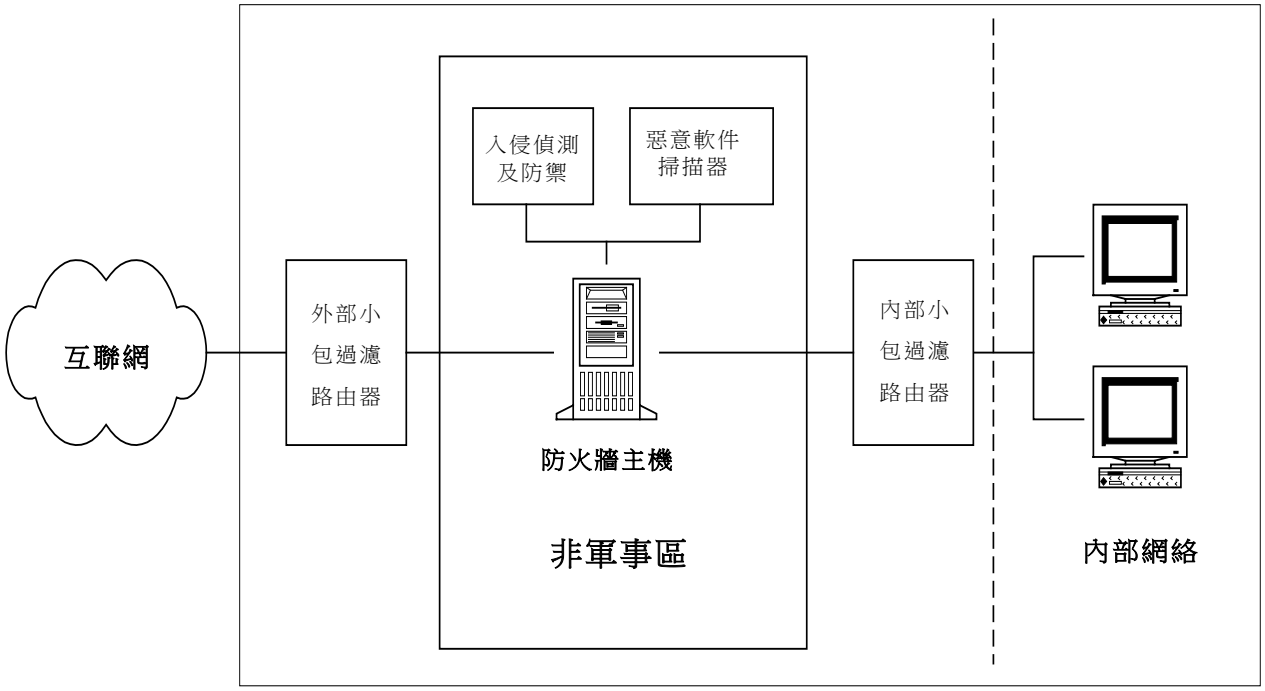

圖 1 具備建議保安保護措施的互聯網通訊閘

上圖所示是建議採用的互聯網通訊閘保安保護措施，互聯網通訊閘在毋須託管任何網站伺服器或郵件伺服器的情況下，提供了內部接達互聯網的途徑。非軍事區是保安措施所在的區域。

設立防火牆主機的目的是要過濾未獲授權或惡意的網絡通訊。值得注意的是架設防火牆並非解決所有保安問題的方案。防火牆無法抵禦的攻擊，包括但不限於：

- 拒絕服務攻擊，也無法保證數據的完整性
- 惡意用戶的攻擊
- 惡意軟件的攻擊

這些都是防火牆應與其他保安功能（例如入侵偵測及防範與惡意軟件掃描）一併使用的原因。然而，防火牆製造商不斷加強防火牆的功能（例如虛擬私有網絡、加密等），使防火牆與其他保安措施的分別日趨模糊。

兩部小包過濾路由器（外部及內部路由器各一部）從外部或內部網絡，過濾和引入經挑選的通訊至防火牆。為連接互聯網，外部小包過濾路由器是必需的設施。內部路由器則用來將非軍事區部分（下文將作詳細說明）與內部網絡隔開。與防火牆不同，這些路由器一般被視為具增值保安功能的網絡設備，而不是保安產品。

上文所述泛指可提供入侵偵測及防範功能的任何方法，可以是工具或程序，而不一定是實體裝置。可是，以基於程序機制去偵測及監察入侵是一個緩慢的手動方法，被認為不適合用於防禦急促轉變的入侵嘗試。使用入侵偵測及防禦系統工具有助將入侵偵測及防禦程序自動化、加快和促進入侵偵測及防禦程序。就此，決策局／部門應部署這些工具以偵測及制止入侵。

此外，為控制和監察互聯網通訊閘，還應制訂一系列保安政策和程序。在重大變更後或推行互聯網通訊閘前，須定期進行保安審計，可確保互聯網通訊閘是按照保安政策適當地設置。即使在沒有內部網絡的情況下，亦宜採取上述建議的保安保護措施。

附件 A 列表所載為建議就互聯網通訊閘保安採取的一些保安措施。

2.3 互聯網通訊閘架構示例

決策局／部門應為其系統實施多重防禦措施。下圖所示是互聯網通訊閘的邏輯網絡圖示例。各決策局／部門可根據個別需要、所提供的服務和現行的網絡結構，按下圖所示調整網絡架構。網絡構件的相對位置可能需要作出調整。

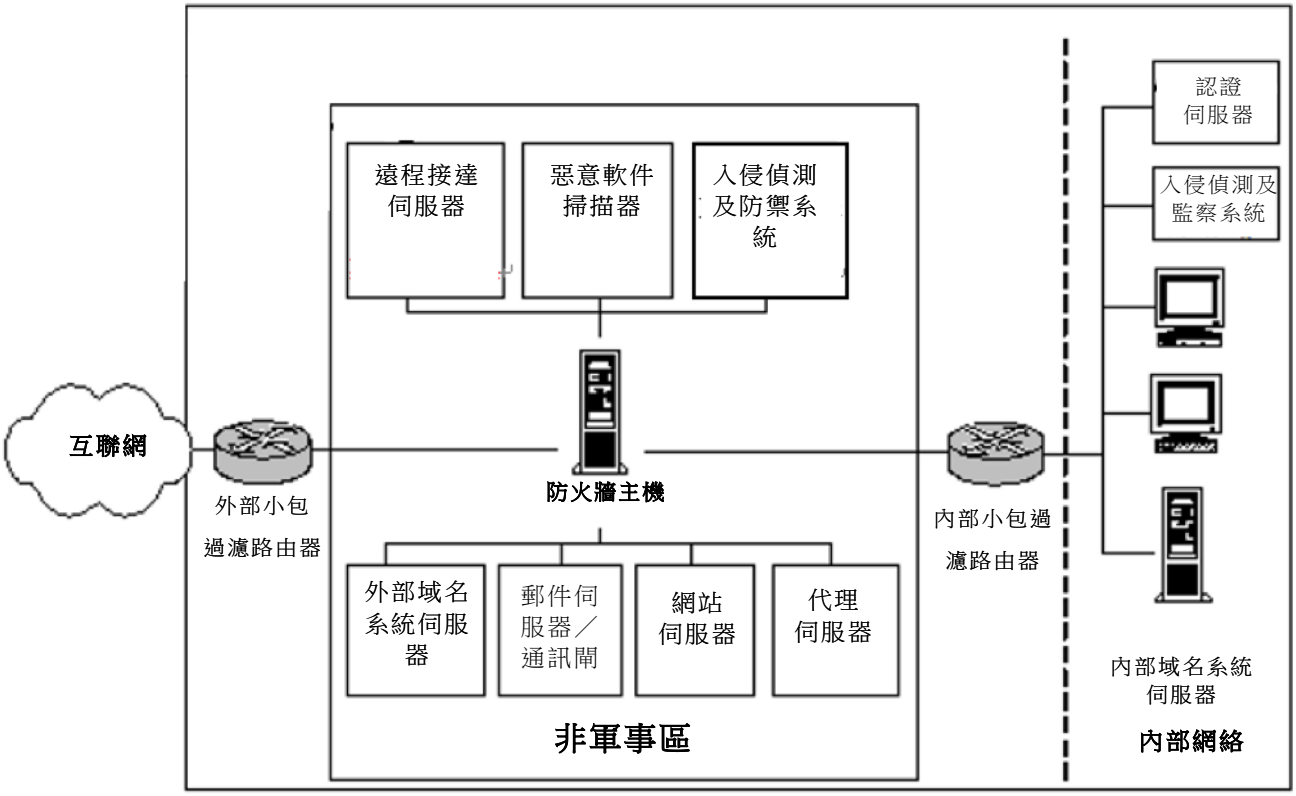

圖 2 具備非軍事區的互聯網通訊閘示例

網絡架構應保留防火牆系統、入侵偵測機制和惡意軟件掃描工具，為互聯網接達服務提供保安保護措施。因應所提供的服務，可考慮納入下列網絡設備：

- 認證伺服器（用戶識別及接達控制）
- 遠程接達伺服器（供遠程接達）
- 域名系統伺服器（供主機名稱及地址配對）
- 簡單郵遞傳送規約通訊閘及郵件伺服器（供互聯網電郵）
- 網站伺服器（供發佈資訊）
- 代理伺服器（供快取記憶、隱藏網址、接達控制）

下文將闡述適用於上述各構件的保安指引，以強調這些構件所需要的保安措施。

互聯網通訊閘架構可將內部網絡與外部網絡隔開，並可隱藏有關內部網絡的資料。非軍事區內可劃分個別的區段，以實施更有效的接達控制和保護。應採用網絡分段／隔離。此外，跨網絡連接應僅按需要而提供。

事實上，提供不同服務的互聯網通訊閘架構都須要因應網絡基建、所提供的服務、性能、操作模式和成本等多種因素作出特定的調整。

2.3.1 網站伺服器

- 如須向內部和外部用戶提供不同資料，便應使用不同的網站伺服器以限制接達。
- 網站伺服器可置於內部網絡內面或外面。一般用來向內部用戶提供資料的網站伺服器須放置在內部網絡內面，並禁止任何從公眾或外部用戶的連接。用來向公眾或外部用戶發佈資料的網站伺服器則應放置於非軍事區內，並由防火牆保護。所有放置在內部網絡外面的網站伺服器須與非軍事區內的防火牆連接，以隔開網絡界面。
- 網站伺服器、郵件伺服器或任何關鍵服務均應使用專用主機。個別主機應有保護措施防範來自其他受襲主機的攻擊。一旦遭受攻擊，可藉此減輕對其他服務的影響。

2.3.2 域名系統伺服器

- 儲存在外部域名系統伺服器中的所有主機名稱和網址，原則上是可公開的。因此，外部域名系統伺服器不可儲存與內部網絡相關的任何資料。若外部域名系統伺服器由互聯網服務供應商託管，則應考慮其復原能力以確保系統的可用性。
- 如需要內部領域資料，應另設一個域名系統伺服器，並將該伺服器置於內部網絡內，而有關資料不可在互聯網上披露。

2.3.3 入侵偵測及防禦

如上文所述，以基於程序的機制去偵測及監察入侵並不適合防範急促轉變的入侵嘗試。建議使用入侵偵測及防禦系統，因為它能提供有效方法辨認、回應及遏制入侵和可疑的網絡活動。此外，必須妥善備存、覆檢和分析所有關鍵構件的系統及應用系統記錄，並應適當地制訂及遵從覆檢、監察及回應程序。

入侵偵測系統監聽及檢查網絡內部的小包，以被動的方式監察網絡通訊，並將已知的攻擊活動識別碼與通訊模式作比對，在吻合時發出警報。

入侵偵測及防禦系統採取比入侵偵測系統更積極的方式阻截外來入侵，因爲此系統可予以配置，在發現攻擊模式後阻止攻擊，使目標受害者免受損毀或被盜取資料。與防火牆類似，入侵防禦系統可阻截及傳送小包，從而即時阻止攻擊。

這些基於網絡或主機的工具可偵測任何可疑的活動，並監察網絡通訊或系統活動。通常應當在網絡關鍵節點安裝入侵偵測及防禦系統。關鍵節點是指在關鍵資訊科技資產或者不同保安區域節點之前的策略性的連接點，例如關鍵

資訊系統、具有敏感資料的伺服器、互聯網通訊閘、遠程接達通訊閘、高層人員樓層等。下文列出設置入侵偵測系統的一些建議：

- 入侵偵測及防禦系統應保持更新保安威脅的最新識別碼和識別模式，亦應安裝最新的修補程式。
- 入侵偵測及防禦系統應置於網絡關鍵節點，例如非軍事區內，以偵測外來攻擊或者設置於內部網絡內，以在有需要時偵測內部攻擊。
- 應盡可能隱蔽入侵偵測及防禦系統的運作。防火牆系統應掩護和保護入侵偵測及防禦系統，以防止該系統受到攻擊。
- 不應只依賴入侵偵測及防禦系統保護網絡。入侵偵測及防禦系統只是在發生異常或可疑活動時向用戶發出警報的實時偵測工具。最重要的措施仍是適當地配置網絡，並確保已採取所需的保安機制。此外，亦應密切監察及定期覆檢整個網絡，以盡早發現保安漏洞或配置不當之處。

2.3.4 防火牆

根據用戶的保安要求，串列使用兩部或以上的防火牆或路由器有助加強防衛水平。舉例來說，兩部串列的防火牆（一部經內部路由器連接至內部網絡，另一部則經外部路由器連接至外部網絡）可提供不同的保護措施。如果有一部遠程接達伺服器（例如虛擬私人網絡通訊閘）與非軍事區連接，並設置於內部及外部防火牆之間，外部防火牆可用來堵截來自互聯網的惡意網絡通訊，而內部防火牆則可堵截來自內部網絡用戶及連接遠程接達伺服器的惡意網絡通訊。

如果是出於平衡負荷或性能的理由而平行使用多部防火牆，各部防火牆的配置應互相配合。

2.3.5 防範惡意軟件

- 應一併設置獨立主機與防火牆，以便在數據經過防火牆時，檢驗其中是否存有任何惡意軟件。此配置可由中央控制個別惡意軟件的識別碼的更新，以防止惡意軟件進入網站或郵件伺服器。
- 宜在不同的位置（如郵件伺服器或網站伺服器等）採用可偵測惡意軟件的措施，以保護特定的伺服器。
- 在哪個位置採用偵測惡意軟件的措施，取決於網絡性能、需要保護的系統或數據及須達到的防範水平等多個因素。在通常情況下，因許多惡意軟件都是以電郵附件的形式入侵系統，因此郵件伺服器應採用偵測惡意軟件的措施。

2.3.6 遠程接達伺服器

遠程接達伺服器是支援遠程或流動資訊處理的網絡互連設備。虛擬私人網絡通訊閘是其中一種遠程接達伺服器。它容許透過不可靠網絡上安全地以遠程連接接駁到內部網絡。遠程接達伺服器亦可以與調解器群一起提供撥號接達服務。

- 獲授權用戶可在沒有互聯網的情況下，透過使用遠程接達功能進行遠距離接達至內部網絡。由於這種功能可能存有保安漏洞，因此應妥善地推行和管理。遠程接達的要求應在有合適的理據下審批 。
- 須以一套驗証機制控制遠程或撥號接達。

2.3.7 代理伺服器

代理伺服器是指運行簡單程式或程序檢驗通過的小包的伺服器。代理伺服器一般被視為加強性能的設備，為內部網絡用戶提供增值保安服務。代理伺服器擔當了在通訊兩方（例如客戶和伺服器）之間調解通訊及確定通訊方向的中介角色。換言之，各方均與代理伺服器通訊，而不是直接與另一方連接。至於代理伺服器的配置，除應提供已獲授權的服務外，亦應限制用戶接達未經授權之目的地。代理伺服器還提供其他支援服務，例如快取記憶最近登入的網頁、接達控制、記錄、內容過濾，甚至隱藏網址。

圖 2 所示的代理伺服器協助控制內部用戶接達互聯網。代理伺服器可以配置為堵截對個人網絡電郵、公共雲端儲存和網絡版即時通訊服務的未獲授權接達。任何已知或疑似惡意的互聯網規約地址或網站均須被堵截。

部分防火牆可加強代理伺服器最常提供的服務，例如遠程登錄、檔案傳送規約、超文本傳輸規約及簡單郵遞傳送規約，以防止未經過應用系統層調解的通訊穿過防火牆。

2.3.8 認證伺服器

防火牆和代理伺服器在某程度上具備用戶身分鑑定功能。用戶還可考慮使用被稱為「認證伺服器」的中央資料庫，以作中央儲存所有鑑定用戶身分及授權用戶所需的資料，例如用戶密碼和接達權限。此外，這些認證伺服器還支援更有效的認證模式，例如運用權標和智能卡，而代理伺服器不一定支援這些認證模式。

舉例來說，遠程認證撥號用戶服務和終端機存取控制器控制系統是常見的遠程認證模式。圖 2 所示的認證伺服器可在遠程撥號用戶獲授權接達網絡前，用來鑑定遠程撥號用戶的身分。

- 應為用戶裝置及認證伺服器間的通訊加密，以及保護有關通訊，防範保安威脅，例如竊聽及重放攻擊。
- 儲存在認證資料庫內的資料應經過加密，而且應受到嚴密保護，以免被未獲授權接達或竄改。
- 應使用獨立及專用的電腦，並將此機放置在安全的地方保管。
- 應適當配置伺服器，以記錄管理事項、帳戶使用資料及認證事項，例如錯誤的登入。
- 如果使用一部或以上的認證伺服器作復原用途，應確保儲存在認證資料庫內的資料已傳送到所有其他備用伺服器。
- 應定期審閱系統記錄檔案以發現任何未獲授權建立帳戶或權限修改。

在制訂電子政府服務的電子認證要求時，決策局／部門亦應遵從《電子認證風險評估參考架構》的指引。該參考架構旨在提供一個統一的方法給決策局／部門在制訂其電子政府服務的認證方法時作為參考，務求令市民／人員於使用有類似認證要求的電子政府服務時會有一致的經驗及介面。決策局／部門應在決定及推行其電子政府服務時，盡量跟從該架構。有關該架構的詳細資料，可於政府資訊科技情報網內的「電子認證架構」主題專頁查閱(https://itginfo.ccgo.hksarg/content/eauth)

3. 防火牆

防火牆可視為防止入侵者侵入，以保護機構資源的保安措施。防火牆是保安基礎設施的重要部分。在探討防火牆的設計前，須徹底了解防火牆的特點、功能、限制，以及與傳輸控制規約／聯網規約相關的保安威脅和漏洞。

防火牆應安裝在內部網絡（例如部門網絡）與外部網絡（例如互聯網）之間的所有網絡接口，以及須檢驗、限制、過濾或重新引導數據流的任何網絡點。

市場上提供多種防火牆產品。在選擇防火牆產品時，應考慮以下主要標準：

- 產品功能
- 性能／處理能力
- 與現有網絡的互用性
- 可靠性
- 復原能力
- 管理的便利程度
- 供應商的支援
- 產品核證（例如 GB/T 20281, GB/T 32917, ISO/IEC 15408）
- 認證服務的支援（例如遠程認證撥號用戶服務）系統容量和擴展能力
- 記錄
- 價格
- 客戶參考
- 所需的技術人員
- 保安要求

最重要的是，應適當配置及管理防火牆。

3.1 防火牆配置

防火牆應經適當配置，以過濾網絡通訊、控制接達和過濾數據內容。防火牆配置不當或有誤可能導致安全假象，而安全假象比沒有設置防火牆更為危險。決策局／部門應評估保安風險，並根據業務需求確定適當的配置。

以下列舉一些配置防火牆時應注意的事項，以供參考：

- 應以防火牆為進出互聯網的唯一通道，強制所有傳入及發出的互聯網通訊經過防火牆。

- 由一個保守的防火牆保安政策開始，即「除明確獲准的服務外，拒絕所有服務」。用戶不宜盲目遵從防火牆預設的設定。
- 應審慎規劃和評估獲准經過防火牆的所有服務。
- 配置防火牆時，可啟動網絡位址轉換，以隱藏互聯網規約地址等內部網絡資料。就採用互聯網規約版本 6 的網絡而言，決策局／部門可因應操作需要，允許以端對端方式連接互聯網，但應考慮採取適當的保安措施，如使用臨時互聯網規約地址，使其他人無法對用戶活動進行分析。
- 配置防火牆時應啟動掃描通訊內容、惡意軟件的功能。
- 防火牆應配置為堵截對個人網絡電郵、公共雲端儲存和網絡版即時通訊服務的未獲授權接達。
- 防火牆應適當配置互聯網規約地址層過濾功能。任何已知或被懷疑是惡意的互聯網規約地址或網站均須被堵截。
- 配置防火牆時應堵截不使用的通訊埠和過濾不必要的通訊，例如不必要的內進或外出互聯網控制信息規約通訊。
- 應確保防火牆本身的實體安全。
- 防火牆政策應富彈性，以配合未來發展和適應保安要求的改變。
- 正確設定和編配防火牆檔案權限。應盡可能限制系統檔案權限。
- 應徹底測試防火牆，在正式推出作服務前應適當地檢驗防火牆配置。
- 在防火牆經過重大改動或升級後須進行測試。
- 應定期以修補程式和錯誤修補程式，更正及更新在防火牆安裝的所有軟件，以確保使用的軟件版本恰當。
- 應為緊急事故設定實時警報機制。
- 應開啟審計追蹤功能，讓任何由管理員或入侵者作出的配置修改都能得以追查。

3.2 防火牆管理

- 應妥善記錄防火牆配置、管理及操作程序。
- 平行使用多部防火牆的配置應完全一致。
- 在可行的情況下，應以檢驗和來檢查防火牆配置檔案的完整性。
- 應定期記錄及覆檢防火牆的記錄。
- 應為防火牆系統和配置檔案備份。
- 妥善備存用戶帳目是十分重要的。只有防火牆管理員和備份管理員獲發防火牆用戶帳目。對獲授權用戶應實施嚴格的接達控制，他們只可操作有助其履行職務的必要功能。
- 為防火牆管理員提供持續培訓，這對防火牆的維修和管理至關重要。
- 應指派至少兩名防火牆管理員（一名為主要管理員，另一名為輔助管理員）管理防火牆的運作。
- 局部區域網絡管理員和防火牆管理員之間應建立有效的溝通渠道。

- 定期進行保安審計。主機系統亦應定期進行掃描和檢查，以偵測常見的配置漏洞和錯誤。

4. 路由器

路由器用來連接兩個或以上的網絡。與應用系統代理伺服器相似，路由器可過濾通訊，並限制接達到伺服器或網絡構件。

在配置及管理網絡路由器時，應遵守以下指引：

- 與防火牆類似，路由器亦應妥善配置，除獲准的服務外，應預設為拒絕所有服務。應關閉源路由功能，惟檢修故障時，則作別論。
- 如同防火牆一樣，路由器應妥善進行記錄、備份和其他管理的工作。
- 在實際運作前應進行徹底測試。
- 如果路由器與防火牆一併使用，則路由器應符合防火牆政策。

5. 郵件通訊閘保安

建立安全的郵件通訊閘，應遵守和遵從下列指引。

5.1 郵件伺服器設計及配置

- 郵件伺服器應由防火牆系統作掩護，防火牆系統可以限制對郵件伺服器的接達，並提供各種保安保護措施。
- 適當配置防火牆或路由器，以攔截不必要的通訊（例如由某個已知濫發電郵者的互聯網規約地址所發出的通訊）進入郵件伺服器或通訊閘。
- 應採用抗惡意軟件防護，過濾帶有惡意軟件附件的進出電郵。
- 電郵系統不應披露內部網絡或系統的名稱或互聯網規約地址。
- 應適當配置電郵系統，以避免透過電郵的標題泄露內部系統或配置的資料。
- 內部電郵地址目錄不應對外公開。
- 郵件通訊閘應能記錄所有電郵標題作審計之用。郵件通訊閘應提供電郵如何、何時及何地寄入或發出等資料。
- 如有電郵轟炸或濫發電郵等情況，應嘗試找出電郵的來源或真正源頭，然後配置路由器或防火牆，以攔截或棄置有關電郵。
- 應關閉為未獲授權用戶或互聯網規約地址傳遞郵件功能。
- 應為獨立電郵系統啟用發件人策略框架，並為寄出的郵件戳上域名密鑰識別郵件簽署，讓收件方核實電郵是由政府寄出。
- 互聯網郵件須受「網域型郵件驗證、報告與一致性」規約的保護，這是一種郵件認證規約，可以讓郵件網域擁有者能夠保護他們的網域不受未經授權的接達，例如電郵仿冒。

5.2 電郵轟炸、電郵濫發及電郵仿冒

電郵轟炸是指重複地發出電郵，以塞滿某個郵件通訊閘或電郵信箱。電郵濫發是指向電郵用戶發出他們不需要的電郵。電郵轟炸及電郵濫發均使互聯網充斥着垃圾電郵。電郵轟炸／濫發者通常劫持其他郵件伺服器，然後透過這些伺服器發送郵件。

電郵仿冒是指用假冒身分來改動電郵發件人或電郵標題的其他部分等資料，使之看似另一用戶或來源。如同時使用電郵仿冒和電郵轟炸／濫發進行攻擊，將更難讓人確定電郵發送者的真正身分。

郵件伺服器如未能適當配置，便可能受到上述電郵攻擊。電郵系統的所有資源被濫發電郵者掠奪後，可能因而癱瘓、不勝負荷，甚至遺失內部資料，而將服務回復正常的成本亦可能十分高昂。

以下是受到電郵攻擊的一些跡象：

- 拒絕服務，例如磁碟已滿或系統關閉。
- 大量電郵在很短時間之內由同一發件人寄入／寄出。
- 大量電郵從無效的來源地址寄入，或向無法寄達的地址寄出。
- 電郵從來歷不明的源頭寄入／寄出。
- 聲稱由管理員發出，要求用戶寄出其密碼或其他敏感資料複本的電郵。
- 要求用戶將密碼改為某指定值或字串的電郵。
- 引導接收者至看似合法機構的欺詐性網站，以欺騙用戶提供個人身分資料及私人資料（例如信用卡資料）。

以下是防範電郵轟炸、濫發電郵及電郵仿冒的一些提示：

- 移除不用的電郵伺服器程式，例如 Sendmail。
- 確保郵件通訊閘使用最新的版本。
- 開啟記錄功能，以記錄仿冒電郵訊息的來源和標題。使用入侵偵測及防禦系統來偵測任何可疑的活動，例如某寄件人所寄入／寄出的電郵突然大量增加的情況等，以協助偵測／防禦電郵轟炸。
- 適當配置防火牆和路由器，只容許符合簡單郵遞傳送規約的外來連接連結到指定的郵件通訊閘或伺服器，以集中記錄和控制通訊。
- 應堵截來自未獲授權或不存在的地址使用郵件轉遞。例如，郵件伺服器應只容許一些指定的內部互聯網規約地址或已獲授權內部用戶，使用郵件轉遞，而並非供外部用戶使用。
- 應適當地配置電郵伺服器程式或郵件通訊閘軟件所配備的過濾無效訊息功能，以清除一些未獲授權網域所發出的垃圾郵件或無效的訊息。
- 限定每個電郵郵件大小上限，或在特定時段內可傳送郵件數量的上限，以避免因電郵泛濫而耗盡網絡資源或磁碟容量。
- 定期更新濫發電郵者名單。
- 設置電郵濫發的阻截系統，藉以過濾不需要的電郵。此電郵濫發阻截系統可發揮郵件通訊閘的功能，按照多項標準（例如電郵標題、內容、電郵濫發黑名單、電郵濫發白名單、反向域名系統查詢、發件人政策框架及郵件域名密鑰識別郵件資料）在電郵進入電郵伺服器之前，篩除濫發電郵。

5.3 接達控制

- 只有獲授權的用戶可使用電郵服務。
- 利用密碼或數碼簽署等認證模式以認證電郵。在傳送電郵過程中，可確保郵件的來源和完整性。
- 限制獲准接達電郵伺服器的用戶人數。
- 儲存郵件在具有適當接達控制的地方。應小心處理郵件，確保其私隱。

6. 網站保安

網站保安是保護網站伺服器、用戶及內部網絡的一系列程序、作業模式和技術。網站伺服器及其組件如網站伺服器操作系統、網絡、應用程式／軟件等，以及儲存於網站內的資料都很容易招致互聯網攻擊。

由於網站伺服器完全面對互聯網，所以必須採取嚴密的主機和網絡保安防護措施。本節所述的網站保安指引，應予嚴格遵守和遵從。有關網站及網上應用系統防範網上威脅的良好作業模式，請參閱《網站及網上應用系統實務指引》。

6.1 網站伺服器配置及管理

網站伺服器軟件是在主機系統上運作，向用戶提供資料或網上服務的應用程式。因應網站伺服器往往面向互聯網，以下的良好作業模式對架設及維持一個安全的網站伺服器，至為重要。

- 關鍵網站、高負荷網站，或易受網上攻擊的網站應寄存在分開的網站伺服器內，以減少或避免網站伺服器面對互聯網時的潛在牽連傷害。要進一步加強保安，就應考慮讓每個網站於分開的專屬主機上運作。
- 網站伺服器應配置為不提供任何簡單郵遞傳送規約服務，以免外部用戶利用網站伺服器傳遞郵件。
- 所有伺服器軟件和應用程式的運行必須符合最小權限原則，尤其不應以管理員、超級用戶或以根權限運行。
- 為網站伺服器內的目錄、檔案和網頁制訂適當的接達權限。
- 所有不必要的網絡服務、應用程式或互聯網規約均不應該預設運行於網站伺服器上。尤其是伺服器管理員和內容更新渠道（例如檔案傳送規約、安全檔案傳送規約、安全殼規約）不應於互聯網上公開。
- 盡可能移除或限制任何源自伺服器端不必要的可執行程式碼，例如共用網間連接界面程式及伺服器插入式部件。
- 在可行的情況下，為網站伺服器指定一個獨立的工作目錄，以便在程序執行時建立／管理工作檔案，並確保文件於工作完成後會被刪除。
- 網站伺服器管理工具，應只限獲授權管理員透過有日誌記錄的身份認證系統才能接達。重要的配置檔案，應只限管理員負責更新。
- 應每日密切監察網站的完整性和可用性，並運用入侵偵測及防禦系統，偵測可疑活動，於未獲授權竄改或接達發生時通知管理員及阻止有關活動。
- 停用所有不使用的帳戶，包括用戶帳戶、服務和預設帳戶。
- 移除網站伺服器上的所有預設檔案或示範檔案。

- 對網絡爬蟲程式施加限制，以免公眾搜尋器搜尋到和儲存不打算公開的內容。
- 應定期更換這些管理工具的密碼，並禁止重複使用相同的密碼。不要使用這些管理工具的預設密碼。

6.2 接達控制

- 應使用強認証方法進行用戶認証。不應只以互聯網規約地址限制作用戶認証，因為來源的互聯網規約地址可以是仿冒的。
- 禁止匿名或未獲授權用戶，接達或更新目錄或數據檔案。
- 只有已登記用戶才可享有接達權限。限制可供登入伺服器的帳戶數目。審查和定期刪除的帳戶。
- 應關閉所有不需要的帳戶，尤其是訪客帳戶。
- 接達記錄必須符合適當的管理程序／帳戶。
- 儲存於外部網站伺服器上的敏感信息，應採取強化的加密並要求認證的措施以作保護。

6.3 網站內容管理

- 在生產前或重大改動後，徹底測試和檢查所有網站和網頁。
- 應實施控制以確保除獲委託及獲授權人士外，其他人無權在生產環境張貼和更新網頁。
- 如果不同的組別，甚至不同部門須共用網站伺服器，各組別、部門應使用不同的網站內容目錄或資源，這些目錄應實施接達控制，以限制接達、執行和儲存有關的網站應用程式。
- 網站應用程式不得設置連結通往儲存於指定網站目錄以外的內部檔案。
- 應對資料夾及檔案採取適當的接達控制，確保用戶不能接達任何儲存在網站伺服器內，非讓用戶接達的檔案。
- 應保存用戶接達記錄，例如對系統檔案嘗試進行非授權接達，使任何不正常或可疑的活動能得以追查。
- 不應授權網站內容開發人員管理操作系統和網站伺服器。
- 為在網站伺服器張貼或更新網頁和應用程式，制訂網站內容管理程序。
- 對於接受用戶數據輸入的網頁表單或應用系統，所有輸入的數據在進入後端應用系統前，應先進行適當的核對、驗證及淨化，使任何預期以外的輸入， 括過於長的輸入、不正確的數據種類、以及預期以外的負數、數據範圍或字符，能被妥善地處理，而不會成為攻擊應用系統的途徑。
- 應移除生產伺服器內不需要的內容，如顯示於系統橫幅的平台資料、說明資料庫、聯機軟件手冊及預設或示範檔案等，以免披露系統資料。

6.4 共用網間連接界面程式及應用程式界面

共用網間連接界面程式及應用程式界面通常用來擴充網站伺服器，以加強性能。與網站伺服器一併供應的預設共用網間連接界面程式可能在無意中提供了接達網站內容的「後門」。程式可泄漏有關主機系統的內部資料，而且很容易招致攻擊。此外，共用網間連接界面程式往往允許用戶輸入數據。

應遵守和遵從的項目如下：

- 適當設計、測試和檢查共用網間連接界面和建基於應用程式界面的程式，確保腳本和程式只能夠提供所需的功能。除非預設或特製共用網間連接界面程式及應用程式界面已經過徹底測試和驗證，否則不得保留在伺服器內。
- 應在受限制的環境（例如在指定目錄）中運行及儲存這些程式，以限制接達，同時可便於進行維修。
- 這些腳本及程式只可獲授權執行，但並無閱讀或寫入權限。對系統資源的使用應予限制，例如中央處理器時間、超時時間和磁碟使用情況。同時，應適當限制接達其他數據檔案或資料。
- 編譯程式、解譯程式、介殼程式及腳本引擎等程式不應放置在程式檔案的預設目錄內，而應安全地放置在適當的目錄。如果不再需要這些腳本及程式，應徹底將它們從網站伺服器移除。
- 應在傳送到伺服器軟件或相關操作系統前適當地檢查、核對和淨化，用戶在這些程式所輸入的數據，以防止數據在指令行運行。

6.5 認證

- 在可行的情況下，遠程管理控制應採用數碼證書、智能卡和權標等強化認證模式，這些強化認證模式亦可用於關鍵應用系統、伺服器和客戶的認證程序。
- 採用如安全超文本傳輸規約的加密連線，以傳送敏感資料。安全超文本傳輸規約須在所有互聯網服務中推行，以增強互聯網服務的真確性以及內容的完整性。

6.6 網絡瀏覽器

應適當地配置網絡瀏覽器。以下是配置網絡瀏覽器的一些建議：

- 應通過獲授權通訊渠道，例如互聯網通訊閘接達互聯網。
- 關閉電郵應用系統／瀏覽器的啟動動態內容的任何選項，例如 Java、JavaScript 和 ActiveX，與可信賴來源通訊則除外。
- 在開啟任何下載檔案前先行掃描惡意軟件。

- 使用最新的瀏覽器，並採用最新的保安修補程式。
- 關閉自動輸入密碼／密碼記憶功能。
- 除非所連接的網站可信賴，否則啓動攔截彈出視窗功能。
- 定期移除瀏覽器內的快取檔案或臨時檔案，以保障資料私隱。
- 安裝插入式部件、附加元件或軟件前，應先檢查及測試有關程式。安裝過程亦只應由獲授權人士進行。

6.7 主動式內容及小型文字檔案

主動式內容使提供資訊的伺服器能夠裁製在用戶端瀏覽器顯示的執行腳本，例如 Java 微應用程式和 ActiveX。須留意流動裝置瀏覽器一般不支援插入式部件，而隨著流動裝置瀏覽器使用的增長，插入式部件的技術正逐步轉移至無插入式部件技術。決策局／部門應在軟件供應商的正式網站內檢查插入式部件的支援終止日期，並事前準備一套可能的轉移方案。

小型文字檔案是伺服器與用戶端瀏覽器以無狀態的超文本傳輸規約連接時，用來掌握用戶狀態資料的一種機制。

6.7.1 Java 微應用程式

Java 微應用程式是通常嵌入網頁內的程式。用戶端的瀏覽器可能會自動下載 Java 微應用程式以便執行。 Java 限制其微應用程式只可進行一部分安全操作，稱為「沙箱」，使這些微應用程式難以破壞檔案系統或電腦的開機磁區。在發展 Java 微應用程式時，發展人員應設計並限制 Java 微應用程式只可接達指定的目錄、檔案和操作系統。

在用戶端運行 Java 微應用程式時，亦應考慮以下事項：

- 收緊對 Java 編譯程式、解譯程式及生成程式的保安控制。在生產環境中，刪除並不需要的編譯程式、解譯程式及生成程式。
- 了解有關 Java 微應用程式保安漏洞的最新資料，並採用最新的修補程式。
- 宜只在有需要的時候才在瀏覽器內啟用 Java 微應用程式。

6.7.2 ActiveX

ActiveX 是一種可透過網頁瀏覽器使用的軟件控件，可用於創建分佈式應用系統的工作。ActiveX 控制是設計以讓網絡瀏覽器能下載和執行。ActiveX 控件是被嵌入在網頁內，但對於 ActiveX 所能夠進行的操作卻並無限制。例如，ActiveX 控件可留駐在系統中，亦可在沒有用戶授權的情況下刪除數據或寫入本機硬磁碟。並且，瀏覽器也無法記錄這些控件在用戶端電腦進行過的操作。

應預設關閉 ActiveX。若有需要執行 ActiveX，應小心驗証及評估有關的 ActiveX 控件。相關的安裝亦只應由獲授權人士進行。軟件編寫者可以於 ActiveX 控件內採用由核證機關發出的認證數碼簽署技術。通過這種方式，客戶端可以根據驗證簽名確認作者的身份，然後才決定接受或拒絕控制的運行。切記，數碼簽署只能夠顯示 ActiveX 控件由何人編寫，但不能協助用戶決定控件是否可以信賴。用戶應認真考慮並只接受來自可信賴來源的控件，或應評估並於瀏覽器設置中禁止「ActiveX 控件和插件」，以禁止系統上不需要的 ActiveX 運行。

6.7.3 小型文字檔案

小型文字檔案是伺服器上的機制，將資料儲存在用戶端以供伺服器提取。小型文字檔案向伺服器提供如曾接達的網址、用戶電郵地址和敏感資料等用戶狀態資料。攻擊者可仿冒伺服器，以擷取客戶端的小型文字檔案。

系統發展人員應注意讓小型文字檔案儲存過多私人資料並不恰當。不要在小型文字檔案儲存純文本的用戶名稱和密碼。如果小型文字檔案須要儲存認證資料，應對整個小型文字檔案進行加密。系統設計人員還可加入一些控制資料，例如到期日期及時間來限制小型文字檔案有效期，以減低小型文字檔案的潛在危害。

7. 遠程接達

遠程接達是指在沒有直接連接網絡的遠程地點使用網絡資源。遠程接達有很多不同的方式，例如撥號接達及虛擬私人網絡。

7.1 撥號接達

撥號接達是在公共電話網絡上進行遠程接達的一種形式。只有獲授權人士可使用撥號接達。決策局／部門應不斷更新其撥號接達點及調解器線路的清單。建議透過用戶認證保護撥號接達，且應定期更換撥號密碼。在某些情況下，可能需採取雙重認證。

決策局／部門亦應考慮使用回撥保安功能。啓動回撥保安功能後，應答調解器會接收撥入的呼叫並認證用戶身分。當用戶通過認證，調解器會中斷呼叫，然後使用預設數據庫內的電話號碼向用戶回撥。該項功能有助於防止未獲授權接達或使用竊取的憑證。雖然回撥功能可加強保安，但攻擊者仍有可能透過呼叫轉移入侵系統，因此還應採取其他保安控制措施（如對撥號連接至敏感環境的連接實行雙重認證）。

每次撥號要求應留下接達記錄。記錄至少應包括以下資料：接達日期、時間、接達持續的時間、用戶名稱及連接的通訊埠。接達記錄應可供有關主管檢閱。

此外，就撥號接達，應跟從以下的良好作業模式：

- 清晰界定哪些用戶會獲得遠程接達權限，以及他們會得到甚麼類型服務。
- 只應讓獲授權用戶在適當認証及記錄下，獲得網絡的遠程接達。
- 妥善配置防火牆系統以限制遠程接達。
- 遠程接達伺服器及調解器群應得到實體保護。
- 建議使用中央調解器群，提供簡易及有效的管理和控制。
- 應記錄對遠程接達伺服器的連接，包括記錄登入對話的起始及終結、連接開始及終止的時間，及對遠程接達伺服器用戶帳戶的更新或刪除等。
- 應在這些連結上進行傳送時，以加密方法保護用戶憑証或數據。
- 接入服務可以因重複的撥號而服務中斷。可設定逾時計時器或撥入時間限制減底服務被中斷的機會。

7.2 虛擬私有網絡

虛擬私有網絡透過一種稱為隧道的技術在不可靠的網絡上建立安全連接。隧道技術在第二層或第三層網絡規約運作，將訊息小包封裝，以便在網絡上傳輸。現時有不同的隧道規約，例如互聯網規約保安及第二層隧道規約 。

除傳統的第二層及第三層虛擬私有網絡外，保密插口層虛擬私有網絡是另一種可提供網絡隧道技術保護的虛擬私有網絡技術。在保密插口層虛擬私有網絡中，網絡隧道技術應用於傳輸層保安通訊對話。保密插口層虛擬私有網絡與傳統的虛擬私有網絡不同，它的運作不需要虛擬私有網絡客戶軟件，而傳統的虛擬私有網絡通常需要客戶軟件。

設立虛擬私有網絡是建立安全通訊渠道的可行方法，可讓在辦公室以外地點工作的人員使用。在推行虛擬私有網絡前，決策局／部門應評估虛擬私有網絡與現行網絡是否兼容並考慮執行下述虛擬私有網絡保安指引：

- 使用權標等一次性密碼認證機制，或以較複雜密碼組成的公開／私人密碼匙系統認證，作爲遠程接達的第二重認證。
- 如在一段指定的時間內沒有操作，應自動終止與政府內部網絡的連接。用戶須重新登入才能與網絡連接。
- 禁止使用雙重（分隔）隧道技術。只允許單一網絡連接。
- 保護所有透過虛擬私有網絡與政府內部網絡連接的電腦或裝置，如使用個人防火牆、最新保安修補程式、抗惡意軟件偵測與修復軟件。所有這些保安措施應經常處於啓動狀態，且具有最新的惡意軟件識別碼及定義。
- 為登記用戶和端點設置白名單。
- 遠程接達電腦或裝置的使用須遵從政府資訊科技保安要求。私人擁有的資訊科技設施不可連接至政府內部網絡。若有運作上的需要，須先徵求部門資訊科技保安主任的批准。
- 透過記錄及審計功能以記錄網絡連接情況，尤其是記錄未能接達的情況。此外，亦應定期覆檢記錄，以識別任何可疑的活動。
- 提醒擁有虛擬私有網絡使用權限的用戶，他們有責任適當地使用帳戶，及確保未獲授權用戶不得使用該帳戶接達政府內部網絡。
- 培訓局部區域網絡／系統管理員、支援人員及遠程用戶，以確保他們在建立及使用虛擬私有網絡時遵守保安良好作業模式及政策。
- 安裝防火牆於通訊閘，以控制從虛擬私有網絡客戶至獲授權資訊系統或伺服器之間的網絡通訊。

8. 域名系統伺服器

域名系統伺服器提供域名與互聯網規約地址配對的支援。域名系統伺服器可提供不同資料，例如在指定領域內所有主機的互聯網規約地址清單、互聯網規約地址轉為主機名稱的配對及用戶電郵地址等。

為保障域名系統伺服器的安全，應遵守和遵從下列指引：

- 使用最新的域名系統伺服器軟件或服務套裝軟件。
- 對域名系統採取保安保護措施，例如控制域名系統資料庫檔案的接達權限，和使用強化加密系統。
- 記錄互聯網規約地址的賦值資料，例如主機位置和主機資料。這些記錄可作為域名系統伺服器遭攻擊時的備份、檢驗和審計清單。
- 對於向內部用戶提供域名系統解析服務的域名系統伺服器，應備有域名系統查詢的使用趨勢基準，以便在發生異常狀況下，對可疑惡意活動或從內部網絡連接外部的非法連接通道作出調查。
- 對於向公眾提供域名系統解析服務的域名系統伺服器，應關閉遞迴搜尋功能，並應限制域名系統的回應速率，以防止域名系統伺服器參與域名系統放大分布式拒絕服務攻擊。亦應阻止對知名網站或不會產生域名系統查詢的地址作回應，以防止參與攻擊重要基礎建設，例如十三個根域名系統伺服器及服務國家和地區頂級域名的域名系統伺服器。

8.1 域名系統安全擴展

域名系統經常受到難以抵禦的中間人、仿冒及快取污染等攻擊。域名系統安全擴展可核實域名系統的回覆信息，為網絡提供多一重保護。域名系統安全擴展採用公開密碼匙加密技術，以驗證域名系統記錄的真確性。通過查核數碼證書，客戶端電腦可相信所接收的資料未遭修改或竄改。此外，域名系統安全擴展可保護用戶免被引導往惡意網站。

為加強互聯網資源的真確性，互聯網網域的資源記錄須受域名系統安全擴展保護。就域名系統安全擴展的推行，決策局／部門應考慮：

- 設計簽發系統 － 須考慮如何整合該系統與現有的域名系統結構，以及現行域名系統管理程序的修訂。
- 在測試環境中簽發 － 對外推出系統前，應測試整個系統，包括在測試環境中測試所有訂明程序。
- 檢查域名系統伺服器 － 核證支援域名系統安全擴展的外部具權威的域名伺服器。

- 產生及管理密碼匙 － 應策劃產生、發布和管理密碼匙的程序，以及密碼匙的長短與使用期限。
- 制訂緊急程序 － 應就密碼匙破解事故制訂程序，以便重新產生密碼匙及簽發區域。

內容分發網絡服務提供了更快的內容分發，以分佈式方式複製和儲存內容。然而，內容分發網絡在支持域名系統安全擴展的程度上有可能出現局限。若此情況出現，由決策局／部門擁有的網域名記錄須由域名系統安全擴展保護，而較低層的網域名應盡可能由域名系統安全擴展保護。

8.2 域名系統堵截

域名系統堵截是決策局／部門保護其網絡免受線上威脅的一項重要功能。它包括使用域名系統堵截域名以阻止對特定網站或線上資源的接達。決策局／部門應評估保安風險，並根據業務需要決定適當的堵截機制。

域名系統堵截的工作原理是根據預定的黑名單檢查域名堵截用戶請求。如果發現該域名在黑名單中，則域名系統伺服器會回應被堵截訊息不是互聯網規約地址，從而阻止用戶接達該網站。

下面列出了建立和維護黑名單時的注意事項：

- 惡意域名
- 可疑域名
- 指令與控制伺服器
- 仿冒詐騙和詐騙域名
- 已知的惡意互聯網規約地址
- 新出現的威脅

通過實施域名系統堵截，決策局／部門可以執行內容過濾政策、預防接達惡意網站、防範仿冒詐騙攻擊，並降低惡意軟件感染或資料洩露的風險。 它充當額外的防禦層，與其他保安措施相輔相成，增強決策局／部門的整體保安策略。

8.3 保護性域名系統

保護性域名系統阻礙了使用域名系統散佈和操作惡意軟件。保護性域名系統的核心功能是能夠根據威脅情報對域名進行分類。保護性域名系統服務通常利用已知惡意域名的開放原始碼、商業和政府資訊源。 這些資訊源可以覆蓋網絡入侵周期中多個階段發現的域名。

保護用戶的域名系統查詢是一項關鍵防禦措施，因為網絡威脅者在整個網絡入侵周期中都使用域名：用戶在嘗試導航到已知良好的網站時會經常錯誤輸入域名，從而無意中接達惡意網站；威脅者在仿冒詐騙電郵中嵌入惡意連結；被入侵的裝置可能會從遠程指令和控制伺服器尋求指令；威脅者可能會從被入侵的裝置向遠程主機洩漏資料。惡意內容相關的域名通常是已知的或可知的，防止對其域名進行解析可以保護個人用戶和企業。

保護性域名系統可從源頭上阻止對惡意軟件、勒索軟件、仿冒詐騙攻擊、病毒、惡意網站和間諜軟件的接達。保護性域名系統堵截數據可以作為威脅情報來源納入安全資訊和事件管理工具中，以幫助識別和修復威脅。通過將此類數據納入安全資訊和事件管理，決策局／部門可以將各種保安日誌整合到單一介面，為保護性域名系統的堵截提供進一步的背景信息。

在選擇保護性域名系統服務供應商時，決策局／部門應考慮以下能力：

- 堵截惡意軟件域名
- 堵截仿冒詐騙域名
- 惡意軟件域名生成算法保護
- 利用機器學習或其他啟發式方法來增強威脅頻道
- 內容過濾
- 支援應用系統開發介面接達以進行安全資訊和事件管理集成或自訂分析
- 網頁介面儀表盤板
- 驗證域名系統安全擴展
- 具備域名系統的安全規約／通過傳輸層安全規約來加密並打包域名系統的安全規約
- 支援按組、裝置或網絡定制政策
- 可跨混合架構部署

9. 入侵偵測及防禦

要維持互聯網通訊閘的安全，需要持續及全面的系統操作、支援和監察，以對不當、異常或可疑的活動或事故，作出防範、偵測、應變和升級處理。通過適當的人手操作程序，如覆檢和分析記錄或統計，測試並演習事故處理程序，便可達到上述目的。

在可能的情況下，應在策略性位置使用及安裝入侵偵測及防禦系統工具，不斷收集及檢查可疑活動的資料。可一併使用基於網絡和基於主機的入侵偵測及防禦系統工具。前者負責檢查在網絡傳輸的網絡小包，後者則負責監察單一主機系統上的系統配置和應用程式活動。

不當配置和使用不當工具可導致向攻擊者泄露資料，並造成安全假象。

- 使用入侵偵測及防禦系統工具鑑別網絡和主機的可疑活動，尤其是網站伺服器和郵件伺服器。
- 設置由電子信息或流動傳呼自動發出警告或警報的功能，在偵測到攻擊跡象時向系統管理員發出警報。
- 在可行的情況下，採用能夠針對可疑網絡活動作出應變的系統或功能，以及時中斷或堵截可疑網絡活動的連接，並作記錄以供事後分析。
- 在使用入侵偵測工具前應適當地測試和檢驗這些工具。
- 妥善控制和限制這些工具的使用和管理。
- 應適當配置防火牆系統，盡可能保護和隱藏這些工具。
- 應確保使用最新的攻擊識別碼檔案。
- 正式使用最新的識別碼檔案及攔截規則前應徹底測試及驗証。應測試更新內的新／修改後識別碼和攔截規則是否能如預期般運作，以及會否與原來識別碼和攔截規則發生衝突。
- 就使用入侵偵測工具應制訂適當的操作、管理和監察程序。這些程序應當定期覆檢以確保網絡配置的更新。

入侵偵測及防禦系統工具的策略性位置，可以是防火牆、主機或者任何重要的資訊資產。可以在互聯網通訊閘基礎設施中引入安全的互聯網通訊閘作爲第一重防綫部署在互聯網和現有的互聯網通訊閘之間以防範來自互聯網的威脅。可以將這類安全的互聯網通訊閘配置成允許入侵偵測及防禦，做到網絡過濾，超文本傳輸安全規約通訊檢查，偵測惡意互聯網規約地址和網域，或者阻止及監測網絡通訊，偵測惡意軟件並防止信息系統被感染。

10. 其他保安考慮事項

除上述特定的網絡構件外，還有一些保安問題應予考慮。下一節將討論部分相關問題。

10.1 實體保安

- 確保所有通訊閘構件的實體安全，所有構件應放置在受管制的地點。
- 放置這些設備的電腦室應具備完善的設施，以防範實體或自然災害。
- 使用可上鎖的儲物架，以存放這些構件。
- 定期監察及覆檢現有的實體保安情況，例如檢查場地的出入口或接達記錄、檢查是否有任何未獲授權竊聽線路、檢查儲物架的門鎖和粘貼標籤。
- 在棄置儲存媒體前，移除及刪除所有資料，尤其是有關系統配置的資料。

10.2 記錄

- 在可行的情況下，應開啟防火牆、路由器、操作系統、網站伺服器和郵件伺服器的記錄功能。
- 備存記錄，如誤差記錄、系統記錄、接達記錄、網站伺服器記錄和郵件伺服器記錄，並確定有足夠的可用存儲容量。
- 記錄信息，例如無效帳戶登錄的嘗試、網站帳戶的濫用、非法或未經授權到網站的嘗試、管理和配置更新、或具體接達信息，如要求者的互聯網規約地址、主機名、劃一資源定位址和接達文件的名稱等。
- 定期覆檢記錄，並將記錄存放在安全的地方不少於一星期。可使用唯讀光碟等一次性寫入設備記錄這些檔案。
- 應妥善保留載有入侵和攻擊資料的記錄，以供調查和記錄。
- 在設計記錄資料的類型和細節時，應考慮到私隱權。

10.3 備份及復原

- 應制訂並妥善記錄正式的備份及復原程序。
- 應定期或在更改配置時，為所有通訊閘構件的配置、記錄檔案、系統檔案、程式、數據和系統的其他資料作備份。必要時可將備份資料加密。
- 備份複本應存放在安全的地方。系統配置宜備存兩份備份複本，一份放置於場內，另一份則存放在場外。

10.4 防範惡意軟件

- 啟動抗惡意軟件保護功能或惡意軟件偵測功能，以檢查所有來自互聯網的通訊，並自動清除惡意軟件。
- 配置通訊閘時應過濾、隔離／刪除含有惡意內容的網絡通訊，並建立審計記錄以供日後調查。
- 應定期更新惡意軟件識別碼及定義。宜配置為自動更新，且至少應每日更新一次。
- 倘若無法進行自動更新（例如並非經常接達網絡的流動電腦），則至少應每週手動更新一次。
- 用戶亦應注意，突發性及嚴重的惡意軟件會不時爆發。如果發生上述情況，用戶應遵從有關指示，並即時更新最新的惡意軟件識別碼及定義，以防範惡意軟件爆發。在簽名／定義更新後，用戶應在電腦上進行全系統掃描，以偵測任何可能存在的有關惡意軟件。
- 定期為安裝資料伺服器的主機進行惡意軟件掃描。

10.5 操作系統保安

由於網絡應用軟件均在操作系統上運作，所以選擇操作系統時應慎重考慮保安要求。操作系統的弱點或保安漏洞可能會影響應用軟件的保安。

在選擇操作系統時，尤其是防火牆和關鍵伺服器，應挑選安全的操作系統平台。在各種操作系統中，宜選擇具備下列功能的操作系統：

- 多重同步程序
- 安全檔案接達權限和控制
- 能否追究用戶和系統行動的責任，並對此進行審計，例如具備詳盡的事件記錄
- 對系統的所有用戶進行識別和認證
- 資源分隔，例如控制重新使用系統物件（已刪除的檔案、配置記憶）

不同的操作系統有不同的方式令配置更為安全。以下所列舉的示例可供一般操作系統參考。

- 移除或關閉所有非必要服務或程序，尤其是不用的預設操作服務和程序。
- 在可能的情況下移除非必要預設帳戶，或以強化密碼作為所有預設帳戶的密碼。
- 高權限操作程序的數目應減至最低。嚴格分配操作權限。

- 為預設檔案權限設定限定預設值。
- 為系統管理員帳戶設立強化密碼，並定期更改密碼。
- 規範操作系統版本和軟件，並將操作系統版本和軟件的數目減到最低，以便安裝和維修。
- 定期安裝操作系統更新程式，並採用最新的操作系統修補程式，尤其是與保安問題相關的修補程式。

10.6 點對點網絡

點對點檔案分享系統是一種基於網絡的應用系統，讓點與點（即參與的電腦）之間利用互聯網互相直接交換檔案。點對點檔案分享系統利用點對點網絡模型，讓每部電腦都是同時扮演用戶端與伺服器的角色。這開放了一個渠道，讓儲存在內部網絡中用戶電腦裏的檔案上載到互聯網中的其他電腦。

點對點技術的潛在保安風險包括：

- 不當配置可能會導致資料於使用點對點應用系統時外泄。被分享檔案以外，儲存在同一工作站或儲存裝置內的其他檔案亦可能不知情地遭外泄。檔案一旦上載到其他電腦後，就很難從點對點網絡上完全刪除。
- 點對點應用系統需要於防火牆開放一定數量的埠後才能運作。每個在防火牆開放的埠都可能成為攻擊者用作攻擊網絡的途徑。
- 由於點對點網絡促進電腦與電腦間的檔案分享，惡意軟件亦可利用這途徑，將自己傳播到其他電腦上。
- 點對點應用系統可能本身存有漏洞，能讓攻擊者傳播惡意軟件，入侵網絡或發動拒絕服務攻擊。
- 當使用點對點軟件下載檔案時，幾乎不可能知道檔案由誰製造或檔案是不是可靠。若檔案牽涉任何非法內容，下載檔案的人士有可能需要面對刑事或民事訴訟。
- 在決策局／部門網絡內使用點對點應用系統可能會產生大量網絡流量，壟斷網絡帶寬，影響其他重要業務應用系統。
- 因為點對點技術依靠用戶工作站，不能從伺服器端管理，所以所有在伺服器端推行的保安措施都不會對點對點分享有任何作用。

以下列出減低點對點技術帶來的風險的良好作業模式：

- 決策局／部門應對業務環境中採用點對點技術作出慎重考慮。除非有強烈及特殊業務情況支持，否則並不鼓勵使用點對點技術作檔案分享。任何情況下，保密或個人資料都不應在點對點網絡上分享。
- 若無需使用點對點網絡，就應制訂保安政策以阻擋所有無需使用的埠。應定期提醒人員不要在工作站上安裝點對點應用程式。

- 關鍵網絡上的通訊應由入侵偵測及防禦系統監察，並應對任何未經批准的點對點通訊進行調查及阻截。應訂立清晰的防火牆政策，容許最少數量而有需要使用的網絡埠。
- 若認為有需要使用點對點技術，有關軟件應安裝在配有專用互聯網連線，及經謹慎配置的獨立工作站上，而有關的預設設定亦必須在使用前經過檢查。應刪除所有不必要的用戶權限及工作站上共用的檔案／目錄，以避免非分享用的檔案遭意外外泄。

10.7 保安風險評估及審計

應定期、在重大變更後及運作前進行保安風險評估。保安風險評估須每兩年進行一次，其目的在於覆檢現行的保安措施，以及找出任何潛在的保安漏洞。

保安審計可以是對現行保安政策的一般覆檢，也可以是利用各種保安評估工具進行的技術覆檢。應審慎使用這些工具來掃描主機系統和網絡，以找出保安漏洞。保安審計的目的是確保現有的保護機制符合現行保安政策。

- 應明確界定審計範圍和目標，確保審計已涵蓋所有目標網絡構件。
- 在運作前應進行技術審計覆檢。通訊閘內的各個主機都需要進行基於主機的掃描，尤其是操作服務和檔案權限。
- 應徹底審計防火牆政策的規則及獲准的服務。
- 應檢查密碼機制及確保其功效。
- 應從網絡構件移除審計測試結果和數據，而有關結果和數據應存放在安全的地方。
- 應控制掃描工具的使用，以防止未獲授權人士使用。
- 盡快跟進審計建議。

10.8 系統管理及操作

- 應妥善管理及維護用戶帳戶。
- 未經決策局局長／部門首長正式批准，禁止用戶或人員安裝或運作網站伺服器或郵件伺服器，以接達互聯網。
- 明確界定和分派並記錄全體系統管理人員的職務和職責。
- 應妥善制訂並遵守互聯網通訊閘程序，例如變更及配置管理控制程序（尤其是防火牆）、備份及復原程序、網站內容管理程序和其他相關程序。
- 應在主機安裝和運作安全模式的程式或軟件以防止意外的改動，並安裝修補程式或更新程式。
- 關鍵組件應由內部連接的終端機直接管理，或採用權標、智能卡、質疑／應答或一次性密碼等強化認證工具。

- 定期檢查聯機保安訊息或檔案，例如技術建議和保安事故或漏洞。
- 應覆檢和修改配置，以對應更改要求、新興的保安威脅或漏洞等環境轉變。
- 系統所顯示的歡迎登入、問候或錯誤信息可能會泄露系統資料。適當時應關閉這些信息功能。
- 在可能的情況下，安裝管理工具或服務，例如使用全場安裝修補程式軟件，以集中系統的管理和安裝工作。

完

附錄 A　建議就互聯網通訊閘保安採用的保護措施的樣本清單

項目	建議的保護措施
防火牆	*防火牆配置*
	傳入／發出的所有通訊應經過防火牆
	以「除明確獲准的服務外，拒絕所有服務」的防火牆政策為基礎
	審慎規劃和評估獲准的服務
	開啟網絡位址轉換功能（如有）
	開啟內容過濾和惡意軟件掃描功能
	堵截對個人網絡電郵、公共雲端儲存和網絡版即時通訊服務的未獲授權的接達
	適當配置互聯網規約層過濾並堵截惡意網絡規約地址
	制訂富彈性的防火牆政策，以備未來發展
	正確設定和編配防火牆檔案權限
	在運作前和重大變更後徹底測試防火牆
	確保防火牆安裝的所有軟件均為恰當版本的軟件
	設定實時警報機制
	如非必要，否則禁止由外部網絡所發的檔案傳送規約或遠程登錄通訊傳送到內部網絡
	保障安裝防火牆的操作系統的安全
	防火牆管理
	妥善記錄防火牆配置、管理及操作程序
	當平行使用多部防火牆時，使用完全相同的配置
	定期檢查配置檔案的完整性，例如運用檢驗和
	定期記錄和覆檢防火牆記錄
	定期為系統和配置檔案備份
	妥善備存管理和用戶帳戶，並定期更改密碼
	為防火牆管理員提供持續培訓
	指派至少兩名防火牆管理員
	列防火牆管理成為保安事故處理的一部分
	在局部區域網絡管理員與防火牆管理員之間，建立有效的溝通渠道
	定期進行保安風險評估和審計

項目	建議的保護措施
入侵偵測及防禦	*操作控制*
	制訂人手操作控制程序
	定期覆檢及分析記錄
	監察及分析用戶及系統活動
	入侵偵測及防禦系統工具（如已使用）
	使用這些工具於網絡和主機，尤其是網站或郵件伺服器
	設置自動發出警告或警報功能
	採用能夠針對可疑活動而作出應變的功能，例如中斷或堵截連接
	在使用前適當測試和檢驗
	控制和限制這些工具的使用
	適當保護及隱藏這些工具
	確保使用最新的攻擊識別碼檔案
	為使用這些工具制訂並覆檢操作、管理及監察程序
防範惡意軟件	*偵測及防禦惡意軟件*
	啟動抗惡意軟件措施以掃描所有輸入的通訊。配置通訊閘時應過濾、隔離／刪除含有惡意內容的通訊，並建立審計記錄以供日後調查
	採用最新的惡意軟件識別碼及定義
	定期進行惡意軟件碼掃描
	開發中或用作測試的電腦設備或軟件亦應遵守相關的資訊保安措施及程序
	在電腦接達政府網絡之前，對電腦進行全面掃描
	外聘供應商應在安裝新機、維修服務和安裝軟件後以最新的惡意軟件識別碼進行惡意軟件掃描
保安政策、指引及標準	*制訂及執行保安政策、指引及標準*
	自訂互聯網通訊閘保安政策
	制訂相關的操作程序，例如變更和配置管理控制程序、備份及復原程序、網站內容管理程序
	制訂保安事故處理和報告程序並定期進行測試
	分派和界定系統管理及維修人員的職務和職責

項目	建議的保護措施
	提醒並培訓用戶遵守及遵從政策
保安風險評估及審計	*進行保安風險評估及審計*
	至少每兩年進行一次保安風險評估，並定期進行保安審計
	在正式運作前或重大變更前進行保安風險評估
	明確界定保安風險評估及審計的範圍和目標
	由第三者進行審計
	審計防火牆政策
	確保密碼管理的有效性
	保障審計結果和數據的安全
	控制對評估及審計工具（如有）的接達
	盡快跟進評估及審計建議