202137735

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 202137735 A

(43)公開日： 中華民國 110 (2021) 年 10 月 01 日

(21)申請案號：109143724 (22)申請日： 中華民國 109 (2020) 年 12 月 10 日

(51)Int. Cl.： *H04L12/801 (2013.01)*

(30)優先權：2019/12/10 美國 16/709,444

(71)申請人：克瑞安尼斯 詹姆士 (美國) KYRIANNIS, JAMES (US)
美國
克瑞安尼斯 明 (美國) KYRIANNIS, MIN (US)
美國

(72)發明人：克瑞安尼斯 詹姆士 KYRIANNIS, JAMES (US)；克瑞安尼斯 明 KYRIANNIS, MIN (US)

(74)代理人：蔡清福；蔡馭理

申請實體審查：無 申請專利範圍項數：22 項 圖式數：7 共 42 頁

(54)名稱

網路基礎架構可程式切換裝置

(57)摘要

在一網路基礎架構內的一種可程式切換裝置包括至少一連接埠、以及通訊耦接至該至少一連接埠的至少一可程式過濾器，其中該至少一可程式過濾器係配置以根據一組定義規則來許可/拒絕正傳送至連接到該至少一連接埠之一連網裝置的資料封包、或正從連接到該至少一連接埠之一連網裝置傳送的資料封包。

A programmable switching device within a network infrastructure that includes at least one port; and at least one programmable filter communicatively coupled to the at least one port, wherein the at least one programmable filter is configured to permit/deny data packets being transmitted to or from a networked device connected to the at least one port based on a set of defined rules.

指定代表圖：

TW 202137735 A

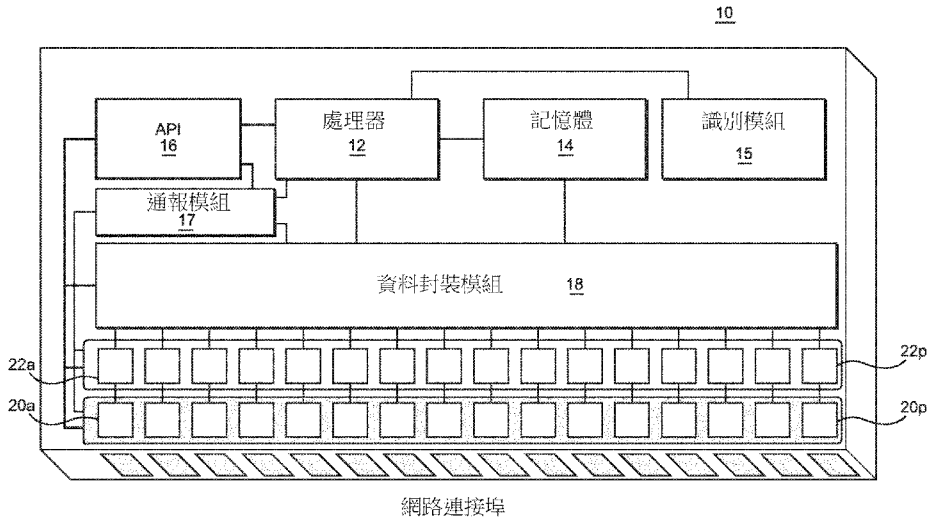

圖 1

符號簡單說明：

10:可程式切換裝置

12:處理器

14:記憶體

15:識別模組

16:應用程式編程介面(API)

17:通報模組

18:資料封裝模組

20a-20p:I/O 網路連接埠

22a-22p:可程式過濾器

202137735

【發明摘要】

【中文發明名稱】 網路基礎架構可程式切換裝置

【英文發明名稱】 Programmable Switching Device For Network Infrastructures

【中文】

在一網路基礎架構內的一種可程式切換裝置包括至少一連接埠、以及通訊耦接至該至少一連接埠的至少一可程式過濾器，其中該至少一可程式過濾器係配置以根據一組定義規則來許可/拒絕正傳送至連接到該至少一連接埠之一連網裝置的資料封包、或正從連接到該至少一連接埠之一連網裝置傳送的資料封包。

【英文】

A programmable switching device within a network infrastructure that includes at least one port; and at least one programmable filter communicatively coupled to the at least one port, wherein the at least one programmable filter is configured to permit/deny data packets being transmitted to or from a networked device connected to the at least one port based on a set of defined rules.

【指定代表圖】 圖 1

【代表圖之符號簡單說明】

10：可程式切換裝置

12：處理器

14：記憶體

15：識別模組

16：應用程式編程介面（API）

17：通報模組

18：資料封裝模組

20a-20p：I/O 網路連接埠

22a-22p：可程式過濾器

【發明說明書】

【中文發明名稱】 網路基礎架構可程式切換裝置

【英文發明名稱】 Programmable Switching Device For Network Infrastructures

【技術領域】

【0001】網路是由資料或電信架構的各種基礎架構元件所連結的電腦系統之互連群組。具體而言，基礎架構是指其各種部件及其配置的組織：從個別的連網電腦到路由器、纜線、無線存取點、切換器、骨幹網路、網路協定、以及網路存取方法。基礎架構可以是開放的或是封閉的，例如網際網路的開放架構、或是私人內部網路的封閉架構。它們可以在連線或無線網路連接、或兩者之組合上運作。

【0002】網路基礎架構的最簡單形式一般包括一或複數電腦、一網路或網際網路連接、以及一切換器以將電腦連結到網路連接並將各種系統彼此綁定在一起。切換器僅是連結電腦，但不限制對任何一系統或來自任何一系統的資料流。路由器可用以使網路互相連結，並根據每一網路的規則為資料交換提供共同語言。路由器可以控制或限制網路之間的存取並調節資料流。

【0003】辦公室內部網路與全球網際網路類似，但在僅可由其內部人員存取的一封閉網路基礎架構上運作。辦公室內部網路系統一般是由一中央資料儲存單元（其可包括一台或多台被稱為伺服器的電腦）以及乙太網路纜線、無線存取點、路由器、切換器和可存取該中央資料儲存單元存取的各個電腦所組成。個別電腦可經由纜線連接或無線存取而連接至網路。路由器和切換器則可接著決定每一各別電腦可以有何存取等級，並作用為訊務導引器（traffic directors）以將各別電腦指向伺服器上的中央資料儲存單元。當各別電腦發送或接收資料時，路由器和切換器即協同運作以確保資料抵達適當處。

【0004】在建置網路基礎架構時，網路安全性通常是基本的考量。防火牆是電腦系統或網路的一部分，其係設計以阻擋未經授權的內部存取，同時許可外部通訊。大部分的架構利用專用的防火牆或具有內建防火牆的路由器及軟體，其控制使用者存取的軟體來進行資料封包監視，並且限制對已定義協定和網路服務的存取。也可以藉由調整各別系統上的網路分享特性來控制安全性，其限制網路上的其他使用者所能看見的檔案夾和檔案。

【0005】整個網路基礎架構是互相連接的，並且可被用於內部通訊、外部通訊、或二者。典型的網路基礎架構包括：連網硬體（例如路由器、切換器、以硬體為基礎的防火牆、LAN 卡、無線路由器、纜線等）、連網軟體（例如網路操作與管理、操作系統、以軟體為基礎的防火牆、網路安全性應用程式等）、以及網路服務（例如通訊連結、網際網路、衛星、無線協定、IP 定址等）。

【0006】網路基礎架構的層 1（Layer 1）定義了用於啟動、維護和停用終端系統之間的實體連結的電性、機械性、程序性和功能性規格。一些常見實例為乙太網網段，例如 SONET、光學的和寬頻之類的商業連結。這些層 1 網路裝置傳送資料，但這些裝置並不管理任何流過它的訊務，例如乙太網光學收發器。換言之，進入連接埠的任何封包會在不經任何額外的處理下被遞送到輸出連接埠。

【0007】層 2（Layer 2）定義了資料是如何格式化以供傳輸、以及如何控制對實體媒介的存取。層 2 網路裝置可於連網裝置和實體媒介之間提供一介面，例如安裝在主機、路由器或切換器上的網路介面控制器（NIC）。層 2 網路裝置可為一多連接埠裝置，其使用硬體位址（例如 MAC 位址）於資料連結層（層 2）處理及轉送資料。切換器作為層 2 網路裝置係互連在家庭或辦公室中的裝置，緩衝進入的封包，並且調整傳輸速度。

【0008】本地區域網路切換是資料網路中所使用的一種封包切換形式。LAN切換技術對於網路設計而言至關重要，因為它們允許訊務僅被發送至預期的目的地，而不將訊務發送到網路上的全部主機。LAN 切換可使用不同種類的網路切換器，而且切換器之間的互連可以利用例如擴展樹協定（Spanning Tree Protocols，STP）來加以調節。

【0009】在使用時，電腦和其他的連網裝置可經由一網路切換器通過連線或無線連接而互連。這些切換器可以次分為更小的、各別的切換器以產生虛擬LANs（VLANs）。傳統切換器不對同一 VLAN 上的連網裝置之間的網路通訊施加安全性控制。換言之，在一 LAN 上的全部裝置都可以與彼此自由通訊。

【0010】層 3 利用可跨越地理上分離的網路的協定來提供兩個主機系統之間的連接性和路徑選擇。在主機的情況中，這是資料連結層（層 2）、網路操作系統（Network Operating System，NOS）的上層、以及正與之通訊的主機上的對應層之間的連結。路由器利用例如 IP（網際網路協定）之協定建立了 LANs（層 2）之間的層 3 連結。

【0011】層 3 切換器一般都支援切換器上所配置 VLANs 之間的 IP 路由。相同的層 3 切換器支援路由器用以於網路之間交換資訊的路由協定。整體而言，由於路由器可互連在層 3 處運作的複數 LANs，因此這能夠將一網路的規模調整到每個 LAN 允許超過至 250 個連網裝置。路由器也可互連 LANs 與 WANs(Wide Area Networks，廣域網路），例如長距離建置連結、對雲端服務的連接、以及網際網路。

【0012】路由器的主要功能在於要引導各種網路（LANs、WANs 等）之間的訊務(traffic)。路由器一般都有一些基本網路過濾能力以控制網路之間的訊務，但無法過濾其網路內的訊務。

【0013】防火牆互連在層 3（網路位址）、層 4（網路連接）和更上層（應用程式）處運作的網路。防火牆的主要功能在於檢查或控制（例如許可/拒絕）網路之間的訊務。防火牆無法過濾網路內的訊務。

【先前技術】

【發明內容】

【0014】所揭技術為一種可程式切換裝置，其包括各別的可程式連接埠。這些各別的可程式連接埠在每一各別切換器連接埠處執行安全性控制。這些各別的可程式連接埠過濾傳入和傳出的資料，以拒絕網路上的任何連網裝置的任何未經授權的入或出的存取。換言之，所揭技術的可程式切換裝置能夠控制流進一 LAN（或 VLAN）、流出一 LAN（或 VLAN）、以及在一 LAN（或 VLAN）內的網路訊務，並且可以保護每一連網裝置免受其網路內每一其他連網裝置的影響，同時允許預期的連網裝置在一 LAN（或 VLAN）上彼此私下通訊。可程式切換裝置可藉此於一開放的 LAN 上產生真正的網路隔離。

【0015】所揭技術的可程式切換裝置可與一網路控制器一起使用，該網路控制器許可網路具有特徵，例如自動操作、學習行為網路訊務模式、以及經由通過例如軟體設計連網（Software Designed Networking，SDN）技術的白名單模型來應用安全性控制。這也可以具有 SDN 能力，其響應安全威脅而即時進行可程式切換裝置的動態編程，並自主地回應未經授權的活動。

【0016】SDN 啟用的基礎架構進一步提供了活動的安全編程介面，其使得網路控制器對其操作參數可即時查詢基礎架構，並發送編程至該可程式切換裝置，以響應新的條件而動態地調整其連接埠操作。網路控制器也可以規模和速度來主控網路的運作，不這樣的話，其採用傳統網路及利用外部資料來源（外

部資料庫、遙測資料等）是不可能的，外部資料來源不這樣的話不可供傳統網路裝置處理。

【0017】所揭技術的可程式切換裝置允許網路也具有獨特的軟體特徵，例如自動的網路流量發現、LAN 裝置辨識、流量許可及授權程序、安全性控制、用以保護 LAN 裝置之邏輯、未經授權的出站流量的自動偵測、根據所需安全性控制之可程式切換裝置的自動編程、以及裝置同盟與虛擬化等。

【0018】在一種實施方式中，可程式切換裝置可包括至少一連接埠、以及通訊耦接至該至少一連接埠的至少一可程式過濾器，其中該至少一可程式過濾器係配置以根據一組定義規則許可/拒絕正傳送到連接至該至少一連接埠的一連網裝置的資料封包、或來自連接至該至少一連接埠的一連網裝置的資料封包。

【0019】在一些實施方式中，一控制器可對該至少一可程式過濾器傳送該組定義規則。在一些實施方式中，該控制器可為通訊耦接至該可程式切換裝置的一網路裝置。在一些實施方式中，該控制器可以是由一防火牆保護的一 SDN 啟用裝置。在一些實施方式中，該控制器可以是在一受保護電腦上運行的一應用程式。在一些實施方式中，一應用程式編程介面可將該控制器連結至該可程式切換裝置。

【0020】在一些實施方式中，該控制器可內嵌在該可程式切換裝置內，並且對該至少一可程式過濾器傳送該組定義規則。在一些實施方式中，此內嵌控制器可經由一應用程式編程介面（Application Programming Interface，API）主控二或複數可程式切換裝置。

【0021】在一些實施方式中，一通報模組可被配置以將遙測（例如網路、主機或資料流特徵）傳送至該控制器。在一些實施方式中，該控制器可分析遙測，並且根據分析自動地更新該組定義規則。

【0022】在一些實施方式中，該組定義規則係由一網路管理員所配置。在一些實施例中，該組定義規則係藉由機器學習或人工智慧（Artificial Intelligence，AI）技術加以配置。在一些實施方式中，該組定義規則係由自動化技術加以配置。

【0023】在一些實施方式中，一識別模組可為該可程式切換裝置和網路提供識別協定。

【0024】在一些實施方式中，一資料封裝模組可被配置以自該可程式切換裝置接收和傳送資料。在一些實施方式中，該至少一連接埠可以是一連線連接點。在一些實施方式中，該至少一連接埠可以是一無線連接點。在一些實施方式中，該至少一連接埠可以是另一種類型的連網連接埠，例如一串列介面。

【0025】在另一實施方式中，一網路基礎架構可包括：至少兩個可程式切換裝置，該至少二可程式切換裝置各具有至少兩個連接埠，其中每一連接埠係通訊耦接至至少一可程式過濾器；以及一控制器，該控制器係通訊耦接至該至少二可程式切換裝置，其中該控制器以一組定義規則填充(populate)通訊耦接至該至少二可程式切換裝置的每一連接埠的該可程式過濾器。

【0026】在一些實施方式中，該組定義規則可許可/拒絕資料封包傳送至一連網裝置或自連網裝置傳送，該連網裝置係通訊耦接至該至少兩個可程式切換裝置的該至少二連接埠的其中一個。在一些實施方式中，該組定義規則可由一網路管理員所配置。在一些實施方式中，該組定義規則可藉由機器學習或人工智慧（AI）技術加以配置。在一些實施方式中，該組定義規則可由自動化技術加以配置。

【0027】在一些實施方式中，一通報模組可被配置以對該控制器傳送遙測，例如網路、主機或資料流特徵。在一些實施方式中，該控制器可分析遙測，並根據分析自動更新該組定義規則。

【圖式簡單說明】

【0028】圖 1 是所揭露技術之一可程式切換裝置的方塊圖；

圖 2 是所揭露技術之一可程式切換裝置的例示實施例；

圖 3 是一流程圖，說明利用所揭露技術之可程式切換裝置將資料封包從連網裝置傳送至網路；

圖 4 是一流程圖，說明利用所揭露技術之可程式切換裝置將資料封包從網路傳送至連網裝置；

圖 5 是具有內嵌控制器之所揭露技術之可程式切換裝置的實施方式的方塊圖；

圖 6 是所揭露技術之可程式切換裝置的無線實施方式的方塊圖；以及

圖 7 是利用所揭露技術之可程式切換裝置的網路的一例示實施例。

【實施方式】

【0029】辦公室內部網路與全球網際網路類似，但在僅可由其內部人員存取的一封閉網路基礎架構上運作。運作技術（Operational Technology，OT）和物聯網（Internet of Things，IoT）裝置在這些內部網路上運行，並且大量存在於建築物的實體基礎架構內。然而，這些裝置都未受良好保護，鮮少針對安全缺陷進行更新，需要網路和網際網路存取來正常運作，而且代表系統之大型安全性標的，例如、但不限於建築物管理系統、實體安全性系統、視聽系統等。

【0030】駭客以這些裝置為目標以將惡意軟體植入一網路，其可例如修改建築物的安全特徵，從而產生生命安全風險，以一公司的伺服器為目標以擷取敏感資料，或使用公司的網路作為起始點進行其他攻擊。

【0031】傳統網路安全性大部分是仰賴防火牆來作為不安全的（「外部」）網路（亦即網際網路）和安全的（「內部」）網路之間的邊界。在這些安全的網路中，當北向流量朝向外部時，網路訊務以通常稱為「北-南」的方向流動行進，例如網際網路。相反的，在一內部網路內或其間的流量是以「東-西」方向行進。

【0032】與這些傳統網路一起使用的防火牆經由管理員所安裝的安全性政策「規則」來過濾流量。這些規則以人可讀方式表示，通常被辨識為存取控制清單（Access Control Lists），其指定過濾器屬性、以及在將封包與該屬性進行匹配時所採取的動作。在使用時，防火牆以「有狀態」的方式運作，以控制哪些流量進入安全網路。防火牆可允許從外部客戶端傳入的「南向」流量存取公司的安全網路上的「網際網路面向」伺服器（例如公司的網站）。防火牆也可允許響應於從網路內起始的連接之南向流量進入安全網路（例如，桌上型電腦存取一網站或視頻服務）。這些「有狀態」的防火牆會追蹤離開安全網路的每一「北向」流量，進以僅允許響應回傳。然而，一般對於北向流量會有較少的、或甚至是沒有控制來限制哪些通訊會離開網路。簡言之，現代的防火牆是作為堡壘周圍的護城河，在網路的外圍（「邊緣」）處提供邊界；規則是堡壘通道的看守者，篩選可能進入的人員。

【0033】多重防火牆可被安裝在這些傳統的安全網路上，生成多道邊界讓駭客去克服。舉例而言，防火牆可以置於網際網路邊緣（Internet Edge）、資料中心邊緣（Data Center Edge）、廣域網路（Wide Area Network，WAN）等處。現代的伺服器一般是在其操作系統內也運行防火牆。不同的製造者及類型的各種防火牆之間的協調是非常困難的。這種拼湊系統之類型會在整個網路安全性態勢上產生漏洞，這導致網路和系統脆弱性。

問題情況 A

【0034】可靠的防火牆規則的創建和其持續的管理是一項巨大的挑戰，而在保護企業網路的現代防火牆中配置的規則數量之多更加劇了此一挑戰，其中該規則數量可達到數萬規則甚至更多。防火牆規則的排序、以及在整個序列中在位置上適當插入新的規則會對其他規則（以及網路的安全性態勢）有衝擊，而且也會影響插入的新規則的有效性。因此，在此類型系統內創建防火牆規則是非常繁複也容易出錯的，這是由嘗試對不完全瞭解的應用程式和系統的通訊進行控制的個人所進行的。此外，傳統的「列黑名單（Blacklisting）」方法作為防火牆規則通常是由管理員相信進入安全網路是有惡意或非所要活動的而創建，而且預設允許其他通訊進入的主觀清單。這與看守者允許被認為是惡意個人以外的每一人進入堡壘的情況類似。這種方法是非常有風險的，因為無法阻擋甚至一次惡意流量可讓駭客進入安全網路。當安全性問題在網際網路上較非流行時，「列黑名單」是常態，而且這種技術在多年來一直存在，因為網路管理員不願意去破除這些複雜防火牆規則的脆弱序列，其未必為幾世代的網路操作人員所能良好理解。

【0035】基於上述理由，「列白名單（Whitelisting）」方式被視為是「最佳方式」，但較不常見。這種方式僅允許預期的傳入通訊進入安全網路，並且預設是阻擋所有其他通訊。這類似於看守者允許無人進入堡壘，除非其明確地符合進入條件。這種方式安全許多：一關鍵優點為，無法考慮流量導致其拒絕進入該安全網路之存取。

【0036】這種列白名單的方式對於開發和維護而言也具有挑戰，因為其需要對網路上的全部應用程式和系統有詳細的了解。舉例而言，有些規則將會永久保留在防火牆中，因為管理員擔心移除對於生產服務有所影響的舊規則，因為對可能影響企業運作的技術中斷是沒有容忍度的。隨著應用程式的淘汰以及新系統重複使用具有不同安全性需求的舊網路位址，這將使漏洞不斷增加。

問題情況 B

【0037】如上述說明，防火牆可在網路邊緣處運作。一旦駭客已經進入安全網路，便可實質上自由跨網路橫向（「東-西」）移動以破壞其他的系統和應用程式。一旦系統被破壞，網路即無法限制離開網路且洩漏敏感資料的流量、或用於對其他網路進行對抗之攻擊的流量。遺失信用卡、SSN、醫療或其他 PII(個人識別資訊）資料、公司資產和其他機密資訊的公司的普遍存在即證明有這種主要脆弱性。駭客使用被破壞的系統來越過複數網路以掩蔽其位置。利用在被破壞的系統內的脆弱性，駭客利用系統本身的軟體來攻擊其他網路。駭客可將其出站流量偽裝為網頁客戶端並加密其通訊。要解密合法的出站流量、然後對其進行控制是非常困難的。

【0038】隨著基於雲端的服務激增，幾乎無法得知哪一網際網路（IP）位址目的地是合法的。駭客還將其操作基礎定位在相同的雲端服務中，使得其難以被偵測。因為出站所起始的合法流量常常遠比入站所起始的要多出許多，故出站流量的大小和複雜性係令人不堪負荷。使得問題更加複雜的是，比起應用程式或裝置的出站流量，製造者將傳入流量記載地更好。因此，在有合法出站流量大量灌注的情況下，更容易會忽略惡意的出站流量。

【0039】舉例而言，有些連網產品越來越依賴出站流量和網際網路存取，以「打電話回家（phone home）」給其製造者尋求支援，並且整合更大的雲端基礎技術及服務生態系統（例如，平面式螢幕 TV 接觸其製造者尋求軟體更新、使用資料和統計資料；電視上的應用程式存取 YouTube、Netflix 等）。在一些情況中，甚至「打電話回家」的能力會是不需要的，因為它會洩漏個人的敏感資料或行為資訊。

問題情況 C

【0040】理解及控制桌上型電腦和膝上型電腦的網路使用是可以被良好理解且可以被管理的。然而，行動式和 IoT 裝置並沒有理解和控制其於網路內的活動所需之診斷式介面和支援。舉例而言，運作技術（Operational Technology，OT）（以及統稱為物聯網（IoT）者）即容易受到北-南和東-西為基礎的攻擊，且因其缺乏適當的工具而難以受保護。

【0041】用於背景，OT 可以為設施運作及安全性提供關鍵的支援，例如照明、HVAC、電廠/發電機、監控攝影機、安全存取、會議室系統和顯示器、電梯、列印裝置、洗衣系統、自動販賣機、銷售點系統、車輛、飛行器等。就歷史上而言，這些裝置都是硬連線以控制系統，但是將 OT 裝置連結到網路是更有成本效益的，其於各種技術間實現了更大的整合性，並且提供了與其製造者的「打電話回家」之支援。

【0042】然而，許多具有數十年 OT 產品開發經驗的大型製造者在網路技術與安全性方面並不純熟。這些製造者通常認為安全性是網路管理員所要解決的問題，而在其自身的 OT 裝置中則幾乎未建置安全性。舉例而言，OT 技術一般並不支援基本的企業級安全性技術，例如用於進入到網路上之許可的個人裝置認證（亦即，802.1x 協定、WPA2 企業版、以憑證為基礎之認證等）。此外，極少甚至不支援以網路為基礎的診斷，與理解 OT 裝置在網路上的即時行為。此外，OT 裝置「打電話回家」的能力通常都是昂貴的支援合約所授權，其迫使 IT 部門提供具有網際網路存取的 OT 裝置。

【0043】此外，隨著製造者進入到下一 R&D 項目，要求客戶升級以取得新的特性，用於 OT 系統之軟體和安全性更新的持續開發通常會受到限制。購買新產品以解決安全缺陷的負擔使得具有網路脆弱性的傳統關鍵技術一直存在多年。日常技術（例如平面螢幕 TV 和家用路由器）受到影響，而且它們在 1 至 2 年內已經過時，因而沒有提供進一步的軟體或安全性更新。在大型網路上存在

有成千上萬的這種裝置，通常在其年份、軟體版本、配置和安全性態勢方面也所差異。OT 是一重要的安全性標的，因為其能相對容易受到破壞、以及駭客對公司的負面影響。

【0044】為了克服上述問題，開發了一種可程式切換裝置，其包括個別可程式的一組連接埠（但可協調成統一的連貫系統）。目前在網路內的每一連接埠都可利用其自身的個別存取規則加以保護，同時在整個網路上全面協調這些規則，以利用存取規則範例來建立基於安全性的分段模型或基於安全性的隔離模型。

【0045】 如圖 1 所示，所揭露技術之可程式切換裝置 10 可包括一處理器 12、一記憶體 14、一識別模組 15、一應用程式編程介面（Application Programming Interface，API）16、一通報模組 17、一資料封裝模組 18、I/O 網路連接埠 20a-20p、以及可程式過濾器 22a-22p。

【0046】I/O 網路連接埠 20a-20p 可以是任何類型的傳統 I/O 連接埠 20a-20p，其允許任何類型的連網裝置（路由器、切換器、電腦、IoT 裝置等）連接到該可程式切換裝置 10，使得資料可以被傳入、傳出一網路基礎架構，以及在網路基礎架構內傳遞。I/O 網路連接埠 20a-20p 可被配置為以各種模式運作，例如開放、學習、許可、限制和有狀態的（其可能需要在可程式切換裝置內的有狀態的防火牆機制）。

【0047】每一 I/O 網路連接埠（連接埠 20a-20p）可通訊地耦接至其本身的個別可程式過濾器 22a-22p。可程式過濾器 22a-22p 可經由一網路控制器（下文將更完整說明）利用一組定義規則來設定，其可控制連網裝置在網路內的互動。該組定義規則可由一網路管理員、由機器學習或人工智慧（AI）技術、由自動化技術或由任何其他傳統方法設定。在一些實施方式中，這些規則是以可人為讀取的形式來表示成存取控制清單（ACL）。

【0048】在一實施方式中，該組定義規則可利用下述中其一或多者來定義：(1)流量策略模板（Flow Policy Templates，FPT），其為存取規則集合，控制網路的一連網裝置的使用；(2)流量策略網段（Flow Policy Segments，FPS），其為 FPT 的集合，控制網路上一連網裝置集合之存取範圍；以及(3)流量策略群組（Flow Policy Groups），其為連網裝置的集合，這些連網裝置的 IP 連接具有在 FPS 內的 FPT，亦即共享同一 FPS 內 IP 連接的連網裝置的集合。也可考慮其他類型的定義規則模板。

【0049】在一些實施方式中，該組定義規則可儲存在記憶體 14 上並由可程式切換裝置 10 的處理器 12 來實施，使得可程式過濾器 22a-22p 可依需要存取記憶體和處理器。在其他實施方式中，可程式過濾器 22a-22p 可具有其自身的資料儲存、處理、記日誌或統計能力。

【0050】在一些實施方式中，可程式切換裝置 10 可包括一 API 16。該 API 16 可以是任何類型的介面或通訊協定，其連結了可程式切換裝置 10 和控制器 50，使得控制器 50 可針對每一個別可程式過濾器 22a-22p 對該可程式切換裝置 10 傳送該組定義規則、收集通報資料、以及以其他方式管理和操作該可程式切換裝置。

【0051】當主機和其資料流量被授權存取網路，利用處理器 12 和記憶體 14，資料封裝模組 18 在從連網裝置被請求時可封裝及傳送資料。在一些實施方式中，資料封裝模組可獨立於處理器自主運作，並且直接經由 API 加以編程。此外，當資料從網路進入可程式切換裝置，利用處理器 12 和記憶體 14，資料封裝模組 18 可以接收及保留資料，直到給予存取以允許資料被傳送到連網裝置為止。換言之，當切換器接收資料時，在切換器內的資料流量即暫時停止。一旦流量被准予，資料流量即被允許流到所需的連網裝置。

【0052】可程式切換裝置 10 也可利用通報模組 17 從通過可程式切換裝置 10 的資料中收集資料流量特徵。這些資料流量特徵可接著經由 API 模組 16 轉傳到控制器 50，因而可對該資料流量特徵進行分析，例如，存取即時威脅並且學習哪種類型的資料流量是典型針對一給定連接埠，或識別出異常的網路行為。舉例而言，分析屬性和結果的日誌可被生成，並可選地記錄在可程式切換裝置內、及/或發送至控制器。也可記錄例如匹配/非匹配計數等之統計資訊。

【0053】可程式切換裝置 10 也可包括一識別模組 15。識別模組 15 可包括用於該可程式切換裝置 10 之一唯一 ID。在使用時，控制器 50（示於圖 2）將在任何可程式切換裝置 10 連接到網路之前被給予該唯一 ID。若可程式切換裝置連接到網路、但該裝置具有未經控制器 50 辨識的 ID，則新連接的切換裝置將無法連接至網路，而且會有警示發出。此一識別機制可由一安全程序加以保護，例如基於密碼及/或密鑰的機制。

【0054】在圖 2 中，可程式切換裝置 28 包括 I/O 網路連接埠 41-48。在此一實施方式中係使用了八個連接埠，但也可利用任何數量的連接埠，例如，大型的切換裝置可配置有數百個連接埠。這些 I/O 網路連接埠 41-48 中的每一可通訊地耦接至個別的連網裝置 30-36（例如，連接埠 41 連接到控制器，連接埠 42 連接到安全裝置 30，連接埠 43、44、47 連接到安全相機 31、32、35，而連接埠 45、46 和 48 連接到電腦 33、34、36）。

【0055】與每一連接埠 41-48 相關聯的可程式過濾器 22a-22p 可以從控制器 50 加以編程。在一些實施方式中，控制器 50 可以是外部或分立的控制器。在其他實施方式中，控制器可以內嵌在可程式切換裝置上，如下文更完整說明者。

【0056】在一些實施方式中，控制器 50 可為例如任何類型的 SDN 啟用控制器（其他類型的控制器也是可以考慮的）。SDN 啟用控制器可連接到網路，並且經由防火牆而受保護，或是可具有一專用線路連至可程式切換裝置中。SDN

啟用控制器 50 和可程式切換裝置 28 經由活動的安全編程介面進行通訊，該安全編程介面使得控制器 50 與網路基礎架構即時、或接近即時地進行其操作參數之互動，並對可程式切換裝置發送規則更動，從而響應新條件（例如惡意軟體攻擊）而動態地調整它們的操作。這允許控制器 50 以規模和速度來主控網路的運作，若不如此，這是傳統網路所無法實現。在一些實施方式中，可以在所揭露網路上實施傳統網路所不可用的外部資料來源（例如外部資料庫、遙測資料等）。

【0057】如圖 2 所示，連網裝置 30-36 可與經由控制器 50 設定的 FPT 規則 60-63 相關聯。舉例而言，安全裝置 30 可被授權存取以對相機 31、32、35 和管理站 36 傳送資料（FPT 規則 60），管理站 36 和相機 31、32、35 可被授權存取以對安全裝置 30 傳送資料（FPT 規則 61），桌上型電腦 33 可傳送至桌上型電腦 34（FPT 規則 62），而桌上型電腦 34 可傳送至桌上型電腦 33（FPT 規則 63）。（請注意，其他的規則及其變化也可以應用於每一連接埠的過濾器，以進行入站和出站控制）。

【0058】圖 3 為一流程圖，其說明如何認可從受保護的連網裝置所接收的資料封包。在步驟 1，從一受保護的連網裝置傳送資料封包。在步驟 2，該資料封包被輸入到可程式切換裝置的網路連接埠中。接著，將資料封包關聯到與連網裝置相關聯的可程式過濾器，此為步驟 3。利用與該網路連接埠過濾器相關聯的 FPT 規則對該資料封包執行分析，此為步驟 4。作出關於封包傳送的決定，此為步驟 5。若封包落在 FPT 規則的參數內，則該資料封包即被許可存取該網路，此為步驟 5A。接著該封包被傳送至網路，此為步驟 6A。若該封包未落於 FPT 規則的參數內，則該資料封包被拒絕存取該網路，此為步驟 5B。該封包即被阻擋而無法傳送，此為步驟 6B。

【0059】圖 4 為一流程圖，說明如何准許從一外部來源接收的資料封包。在步驟 10，資料封包被傳送到可程式切換裝置。在步驟 11，對於該資料封包要

傳向哪一網路連接埠進行確定。將資料封包關聯到與所確定連網裝置相關聯的可程式過濾器，此為步驟 12。利用與該網路連接埠過濾器相關聯的 FPT 規則對該資料封包執行分析，此為步驟 13。作出關於封包傳送的決定。（步驟 14）。若封包落在 FPT 規則的參數內，則該資料封包即被許可傳送到目的地連網裝置，此為步驟 15A。若該封包未落於 FPT 規則的參數內，則該資料封包被拒絕存取目的地連網裝置，此為步驟 15B。

【0060】如圖 5 所示，可程式切換裝置 150 可包括一內嵌控制器。該可程式切換裝置 150 可包括一處理器 152、一記憶體 154、識別模組 155、一控制器 156、一通報模組 157、一資料封裝模組 158、I/O 網路連接埠 160a-160p、以及具有記日誌(logging)和統計能力的可程式過濾器 162a-162p。可程式切換裝置 150 與內嵌控制器 156 係以類似於可程式切換裝置 10 的形式作用，其中所接收和傳送的資料封包都受制於上述 FPT 規則。在一些實施方式中，內嵌控制器可經由其 API 來主控一或複數可程式切換裝置。

【0061】內嵌控制器 156 可利用例如運行一虛擬控制應用程式之一網頁介面或實體連網裝置來加以存取，以設定該定義規則並且管理該可程式切換裝置。

【0062】圖 6 說明所揭露技術之一無線可程式切換裝置 110 的實施方式。該無線可程式切換裝置 110 可包括一處理器 112、一記憶體 114、識別模組 115、一 API 116、一通報模組 117、一資料封裝模組 118、I/O 網路連接埠 120a-120b、以及具有記日誌和統計能力的可程式過濾器 122a-122b。無線可程式切換裝置 110 是以類似於可程式切換裝置 10 的形式作用，其中無線接收和傳送的資料封包係受制於上述 FPT 規則。在一些實施方式中，無線可程式切換裝置 110 可含有一內嵌控制器 156，即如同可程式切換裝置 150 中所示。

【0063】一旦該組定義規則被配置到所揭露技術之可程式切換裝置中，則幾乎不可能對連網裝置有未經授權的進或出的存取，因為每一連網裝置都基於一授權存取模型而完全隔離，這對於其他的網路技術而言是不可能的。

【0064】所揭技術之可程式切換裝置的獨特特徵可包括：(1)基於一連網裝置的 IP 和 MAC 位址的 LAN 防火牆方式；(2)通過於一共享 LAN 上之安全性控制的基於流量策略分段；(3)基於 SDN 之 LAN 控制，例如基於切換器或控制器的策略管理；(4)自動流量偵測和流量策略模板創建；(5)流量接收和管理；(6)防止非所要的出站（北向）流量和潛在的資料洩漏；以及(7)在單一或複數 LAN（或 VLAN）上的分散式防火牆策略。

【0065】 所揭技術之可編程切換裝置也可於一連網裝置的來源 IP 位址（IPv4 或 IPv6）以及 MAC 位址上運作，並且使用作為其他 LAN 連網裝置看不見的透明層 2 裝置。在一些實施方式中，可程式切換裝置也可於一網路訊框標頭、封包標頭、或網路訊框或封包的內容的其他元素上透明地運作。

【0066】所揭技術之可程式切換裝置也可經由一來源與目的地 IP 及/或 MAC 位址創建防火牆策略，其允許創建在 LAN 內以及在 LAN（或 VLAN）之間的流量策略網段（FPS）。所揭露技術之可程式切換裝置可進一步在 LAN 或複數 LAN（或 VLAN）上的連網裝置之間創建基於防火牆且封閉的通訊路徑。舉例而言，流量策略網段可許可流量來自一個別來源位址或 IP 位址區塊至可選地具有附加屬性的一個別目的地位址或 IP 位址區塊，例如、但不限於：協定類型與連接埠數量。在其他實施方式中，FPSes 可以通過同盟而應用於二或更多個可程式切換裝置之間，如下文更完整之說明者。

【0067】相較於具有相對少連接埠且非常大量規則集合的傳統防火牆而言，所揭露技術的可程式切換裝置可利用較小的防火牆規則集合，其可分散於

更廣數量的連接埠，並且應用至個別網路連接埠上的所有連網裝置、或特定的連網裝置 IP 位址。

【0068】所揭露技術之可程式切換裝置可進一步仰賴 SDN 來動態地識別、追蹤及創建策略，以通過流量策略模板的創建來限制網路流量，其可接著接著被應用至一連網裝置的 IP 位址。SDN 也使得流量策略模板可設定白名單規則並主控它們的運作，如下文將更完整說明者。

【0069】對於流量策略模板的模板類型方式以及其奠基的存取控制清單也可使得可程式切換裝置對流量輪廓模板及其存取控制清單的元素和屬性、以及從而對連接埠過濾器應用例如替換及處理邏輯之運作，以創建一獨特的動態且可適應的網路存取範例。例如節點 ID（NodeID）、訊框或封包標頭及內文、即時網路流量資料、以及來自外部來源的資料等資料係可依演進的安全性策略的動態需求被槓桿式運作來調整流量策略模板、流量策略網段和流量策略群組的特性和行為。通過使用包括例如模式匹配、替換、算術運作、比較和處理邏輯等運作，施用一種語言來促進這些動態調整的應用。

【0070】所揭技術之可程式切換裝置可另外以集中式或分散式配置方式運作，其具有一切換器作用為控制器、或是具有專用的控制器。

【0071】所揭露技術之可程式切換裝置也可以傳統切換器（無防火牆保護）或以可編程模式運作。可程式切換裝置的通用設定可用以迫使所有的連接埠以可編程模式運作，以避免在安全性態勢中的空隙。在一些實施方式中，需要有複合式配置，其具有以任一模式運作的連接埠組合。

【0072】所揭技術之可程式切換裝置和其控制器可識別出網路上新的流量，並且將該流量的本質特性化為：內部到外部、內部到內部、外部到外部、來源和目的地位址、協定、以及連接埠數量。在一些實施方式中，可程式切換

裝置也可特性化網路訊框標頭、封包標頭、或網路訊框或封包的內容的其他元素。

【0073】若偵測到一連網裝置的新流量，則可根據一配置策略來觸發警示，以允許、拒絕或等待核准。此外，所有的流量都可登錄在一流量策略模板內，而且「開放的」連接埠可以流量策略模板運作，其允許「任何到任何」的流量。

【0074】所揭技術之可程式切換裝置和其控制器可產生關於異常流量模式的警示，該異常訊務模式與策略模板不一致，並且可能是表示惡意或不希望的活動。舉例而言，產生過量動態流量（其無法受到具有可縮放的有限數量規則的策略模板所限制）的一連網裝置將觸發對一傳統有狀態的防火牆方案的回退、或對網路管理員發送聲音或書面的警示。

【0075】流量策略模板可根據流量接受模式來創建，例如：(1)「開放模式」：允許所有流量；(2)「學習模式」：控制器允許及追蹤通過該連接埠的所有流量，並建立描述訊務的流量策略模板；(3)「核准模式」：所有的新流量在它們被許可通過連接埠以及到連網裝置之前都必須經過手動核准，從而手動創建流量策略模板；(4)「限制模式」：在流量策略模板為活動狀態且限制切換器連接埠上的訊務的情況下正常運作；以及(5)「有狀態模式」：有狀態地允許所有的出站流量，拒絕所有的非狀態入站流量（已核准者除外）。亦可考慮有其他模式。

【0076】在一實施方式中，列白名單模型僅可許可流量策略模板所明確允許的流量。流量策略模板內未出現的流量則不被許可進入流量策略網段，因而避免不希望的入站訊務，例如網路掃描或攻擊。流量策略模板內未出現的流量不被許可離開流量策略網段，因而可避免不希望的出站訊務，例如網路掃描、攻擊、嘗試與其他軟體整合或接觸第三方。此一實施方式藉由僅允許與流量策略模板相符的出站流量來避免資料洩漏到流量策略網段外部。

【0077】在另一實施方式中，運作技術（OT）和物聯網（IoT）裝置如往常缺乏企業等級的特性來安全地登入及存取網路。這種連網裝置僅可利用節點ID（NodeID）由網路來識別，例如 MAC 位址、IP 位址（IPv4 或 IPv6、無類別網域間路由（CIDR）標註）或其組合。所揭露技術可利用兩個唯一參數來定義一網路位置識別（LocID），例如一連網裝置的附件裝置（例如網路切換器或無線存取點（WAP））以及一附件識別符（例如網路切換器上的連接埠或無線關聯 ID）。在這種情況下，LocID 可等於（切換器 ID＋切換器連接埠）或（WAP＋無線關聯 ID）等。這些網路位置識別符指定可為網路上的所有連網裝置建立位置，例如 LocNodeID＝LocID＋NodeID。

【0078】在使用時，當跨企業讓切換器同盟時，網路可於其整個拓樸中辨識 NodeID 和 LocNodeID。利用這些指定，新穎的揭露技術允許安全性策略跨越整個網路。舉例而言，可創建虛擬拓樸（vTopology），以允許在一組實體基礎架構上有多種拓樸，創建可跨越一或複數實體可程式切換器的虛擬切換器架構，或針對不同的使用情況來將可程式切換裝置群組在一起（例如管理網域）。其他的虛擬拓樸使用也是可考慮的。在一虛擬網路拓樸內的連網裝置位置可為例如（vTopLocID＝vTopologyID＋LocID）或（vTopLocNodeID＝vTopologyID＋LocNodeID）。

【0079】此外，該連網裝置在網路上的行為在資料流經其所連接的可程式切換裝置時，可以通過其唯一的傳輸來特性化。連網裝置的流量的設定可藉由軟體定義連網（Software Defined Networking，SDN）技術來特性化，並且表示為流量策略模板（FPT）。舉例而言，如上述說明，運作技術（OT）和物聯網（IoT）裝置通常不會生成大量的唯一且動態的流量，而是生成有限數量的重複流量到例如一管理系統、製造者的伺服器、或是在相似的裝置之間等。這些訊務模式可以經由 SDN 技術而被學習、特性化、模板化、以及編程到所揭露技術

的可程式切換裝置中。換言之，特性化運作技術（OT）和物聯網（IoT）裝置所生成的流量模式會是相對的簡單，因為與人所使用的互動裝置（例如桌上型、膝上型、手持等裝置，其中的流量模式更加複雜許多）相比，它們的流量類型在數量上係受限制。

【0080】此外，彼此通訊的連網裝置可共享一共同的流量策略模板、或互相連結的不同流量策略模板的部分。每一連網裝置的網路位置 ID（vTopLocNodeID）都可連結到一 FPT，其含有一入站和出站存取控制清單。FPT 的存取控制清單為例如白名單，其指定要允許什麼訊務並拒絕所有其他的。

【0081】流量策略模板可以被建構以指定：FPT ID、方向（入站或出站，因為每一連接的連網裝置都會有此二者）、連結的 FPS（FPT 所連結的 FSP ID）、來源（vTopLocNodeID，且必須是入站 FPTs 上的連接的連網裝置）、協定（IP 協定類型）、連接埠（連接埠號碼或協定次識別符，且對於動態的客戶側連接埠號碼而言可以是動態的）、目的地（vTopLocNodeID，且必須是出站 FPTs 上的目標連網裝置）、動作（此流量所採取的動作，且能包括許可/拒絕、或軟體定義（SDN 控制））以及預設的最終規則（無法移除：拒絕從所有連網裝置到所有連網裝置的訊務（強制列白名單））。其他的動作和 FPT 元素也是可考慮的。

【0082】所有新連接的連網裝置（或連網裝置的類型）都可具有初始 FPTs，其模板是設定為所需的策略，允許針對相似裝置的類別進行模板化的安全性控制，例如，應用含有其所連結 FPS ID 的 FPT 於所需的策略。

【0083】在另一實施方式中，一流量策略模板（FPT）可被連結到一連網裝置的 NodeID。此一 FPT 在整個網路上可依循一電腦或一連網裝置。在這種實施方式中，雖然所編程過濾器被應用至一受保護連網裝置在一給定時刻所連接的一切換器上的一連接埠（或該電腦所正維持的無線關聯/連接），若該受保護

的連網裝置從切換器上的一連接埠中斷連接，並且移動到同一或不同切換器上的另一連接埠（或是若該受保護的電腦從一房間無線地移動到另一房間並轉換到另一 WAP），該 FPT 內的此一連網裝置之規則即被應用至其新的連接埠。意即，FPT 可從原本的切換器連接埠轉換到新的連接埠（或從原本的無線關聯 ID 轉換到新的無線關聯 ID）。FPT 的轉換可以藉由控制器來完成，因為控制器對於網路上的所有切換器（或 WAPs）都有監督。在此一實施方式中，切換器（或 WAP）也可具有智能來警示控制器受保護的電腦已經移動，並且可接受在新的連接埠（或無線關聯）上 FPT 的過濾器的編程。

【0084】通過將流量策略模板跨一或複數可程式切換裝置而應用來創建流量策略網段（FPS），也可於網路上隔離或分段連網裝置。FPS 係 FPTs 的集合，該 FPTs 互相連結以創建出由每一連網裝置的網路連接上之存取控制清單所執行的一整體網路策略。每一 FPS 具有一入站和一出站流量策略。流量策略網段為私密的通訊路徑，其在所有切換器入口和出口連接埠上都經由反映在其 FPTs 內表達的安全性控制的存取控制清單而受到保護。無一者可進入或離開該 FPS，除非其被連結到 FPS 的 FPT 明確許可。

【0085】流量策略網段可以被建構以指定 FPS ID、FPS 名稱（32 個字元的文字（無空格））、描述（255 個字元的自由格式可印出文字）、拓樸 ID（此一 FPS 做為成員的 vTopology ID）、FPT 清單（連結到此 FPS 的所有 FPT 的清單）。FPT 可具有一入站和出站方向，於 FPS 上創建一雙向策略。FPT 可針對類似連網裝置的類型而加以模板化，例如：所有的連網裝置、連網裝置子集合、或連網裝置的類型等。其他的 FPS 元素也是可考慮的。

【0086】SDN 技術可學習連網裝置各類型的行為，並跨由一或複數可程式切換器組成的小型或大型網路足跡應用已學習或定義的 FPT 作為大量的類似連網裝置（即視頻監控相機、卡片存取讀取機、建築物偵測器等）之模板。FPT

係經由 SDN 應用至一 vTopLovNodeID、或應用至一相同類別的 vTopLocNodeIDs 的成員，並且可隨著裝置的網路使用演進（由於更新等）而動態地加以維護。SDN 也可用以動態地確定一 FPT 內存取規則的動作（即許可/拒絕、或經軟體定義）。

【0087】圖 7 說明使用所揭露技術之可程式切換裝置的一網路結構 200 的實施例。在圖 7 中，一企業網路切換裝置 204 可以是網路結構 200 之一第一層切換裝置。該企業網路切換裝置 204 可在連接埠 1 處通訊連接至網際網路 202，在連接埠 2 處通訊連接至網路控制器 206，並且在連接埠 7 處通訊連接至一或複數第二層切換裝置（例如：混合用途的切換裝置 220），在連接埠 6（Port 6）處通訊連接至一 OT 切換裝置 230，以及在連接埠 5（Port 5）處連接至一混合用途的切換裝置 240。

【0088】混合用途的切換裝置 220 可通訊耦接至數種不同類型的連網裝置，例如：在連接埠 8、連接埠 7 處分別耦接至桌上型電腦 221、222，在連接埠 6、連接埠 5 處分別耦接至安全相機 223、224。OT 切換裝置 230 可通訊耦接至數個建築物基礎架構的連網裝置，例如：在連接埠 8 處耦接至一實體安全性控制面板 231，在連接埠 7、6 處分別耦接至安全相機 232、233，並且在連接埠 5 處耦接至 HVAC 管理站 234。混合用途的切換裝置 240 可以通訊耦接至數種不同類型的連網裝置，例如，在連接埠 6、連接埠 5 處分別耦接至桌上型電腦 243、244，在連接埠 8、連接埠 7 處分別耦接至無線存取點 241、242。無線存取點 241、242 可無線地連接至例如一或複數膝上型電腦 245。

【0089】在使用時，網路控制器可針對企業網路切換裝置 204、混合用途的切換裝置 220、240 以及 OT 切換裝置 230，利用防火牆規則或存取控制清單來編程個別的過濾器，如上述說明。

【0090】在本說明書中所描述的標的內容的實施例和運作係可於數位電子電路中、或電腦軟體、韌體或硬體中實施，包括本說明書中所揭露的結構以及其結構等效例、或是它們中的一或複數的組合。本說明書中所描述的標的內容的實施例可實施為一或複數電腦程式，即電腦程式指令中的一或複數模組，編碼於一電腦儲存媒體上以供資料處理設備執行、或控制資料處理設備的運作。可替代地、或除此之外，程式指令可編碼於一人工生成的傳播訊號上，例如機器生成的電氣、光學、或電磁訊號，其被生成以編碼資訊供傳輸至適合的接收器設備以由一資料處理設備執行。電腦儲存媒體可以是（或包含於）一電腦可讀取儲存裝置、一電腦可讀取儲存基材、一隨機或串行存取記憶體陣列或裝置、或它們之中一或複數的組合。

【0091】本說明書中所描述的運作可被實施為由一資料處理設備對於儲存在一或複數電腦可讀取儲存裝置上、或從其他來源所接收的資料執行的操作。術語「資料處理設備」涵蓋用於處理資料的所有種類之設備、裝置和機器，包括例如一可程式處理器、一電腦、一單晶片系統（System on a chip）、或它們的組合。該設備可包括專用邏輯電路，例如一 FPGA（場可程式閘極陣列）或一 ASIC（專用積體電路）。除了硬體以外，該設備還可包括為所討論的電腦程式創建出一執行環境的代碼，例如建構處理器韌體、協定堆疊、資料庫管理系統、作業系統、跨平台的運行時間環境（例如虛擬機器）或它們之中一或複數的組合的代碼。該設備和執行環境可實現各種計算模型基礎架構，例如網頁服務、分佈式計算和網格計算基礎架構。

【0092】電腦程式（也稱為程式、軟體、軟體應用程式、腳本或代碼）可用任何形式的程式語言來撰寫，包括編譯或解譯語言、聲明性或程序性語言，而且其可以任何形式部署，包括作為一分立程式或作為一模組、組件、副程式、物件、或適合於計算環境中使用的其他單元。電腦程式可以（但非必須）對應

於一檔案系統中的檔案。程式可被儲存於檔案中保留其他程式或資料的一部分檔案中（例如儲存於標記語言文件中的一或複數腳本）、儲存於專用於有關程式的一單一檔案中、或儲存於複數協調檔案中（例如儲存一或複數模組、子程式、或代碼部分的檔案）。電腦程式可部署以於一部電腦上執行，或於位於一場所或分散於複數場所且由一通訊網路互連的多部電腦上執行。

【0093】本說明書中所述的處理和邏輯流程可以由一或複數可程式處理器執行，該處理器執行一或複數電腦程式，以藉由對輸入資料運作並生成書出來執行功能。該處理和邏輯流程也可由專用邏輯電路來執行，且設備也可實施作為專用邏輯電路，例如 FPGA（場可程式閘極陣列）或 ASIC（專用積體電路）。

【0094】適用於電腦程式執行的處理器包括：例如通用和專用微處理器兩者、以及任何種類的數位電腦的任一或複數處理器。一般而言，處理器將接收來自一唯讀記憶體或一隨機存取記憶體或兩者的指令和資料。電腦的必要元件為用於執行或施行指令的處理器、以及用於儲存指令和資料的一或複數記憶體裝置。一般而言，電腦也將包括、或操作性地耦接而接收資料自、或移轉資料到(或兩者) 用於儲存資料的一或複數大容量儲存裝置，例如磁性、磁光碟片、或光學碟片。然而，電腦不需要具有這類裝置。此外，電腦可內嵌於另一裝置中，例如行動電話、個人數位助理（PDA）、行動式音頻或視頻播放器、遊戲機、全球定位系統（GPS）接收器、或一可攜式儲存裝置（例如通用串列匯流排（USB）快閃碟），僅舉數例。適合儲存電腦程式指令和資料的裝置包括所有形式的非揮發性記憶體、媒體和記憶體裝置，包括：例如半導體記憶體裝置，如 EPROM、EEPROM 和快閃記憶裝置；磁碟機，例如內建硬碟機或可移除碟機；磁光碟片；以及 CD-ROM 和 DVD-ROM 碟片。處理器和記憶體可由專用邏輯電路補增，或是併入專用邏輯電路中。

【0095】為可用於與使用者互動，本說明書中所描述的標的內容的實施例可以實施於具有顯示裝置、鍵盤和指示裝置的電腦上；該顯示裝置例如為一 CRT（陰極射線管）或 LCD（液晶顯示器）螢幕，用於對使用者顯示資訊；使用者可藉由鍵盤或該指示裝置（例如為滑鼠或軌跡球）對電腦提供輸入。也可使用其他種類的裝置來提供與使用者之互動；舉例而言，對使用者提供之反饋可以是任何形式的偵測反饋，例如視覺反饋、聽覺反饋或觸覺反饋；而且來自使用者的輸入也可以任何形式被接收，包括聲音、語音或觸覺輸入。除此之外，電腦可藉由發送文件到使用者所使用的裝置、或自使用者所使用的裝置接收文件而與使用者互動。

【0096】本說明書所述標的內容的實施例可實施於一計算系統中，其包括後端組件（例如控制器）、資料伺服器和中間件組件（例如應用程式伺服器）或前端組件，例如具有圖形使用者介面或網頁瀏覽器的客戶端電腦（使用者可通過其與本說明書所述標的內容的實施方式互動），或是這些後端、中間件、或前端組件中一或複數的任何組合。系統的組件可藉由任何形式或媒體的數位資料通訊（例如通訊網路）加以互連。通訊網路的實例包括：局部區域網路（Local Area Network，「LAN」）和廣域網路（Wide Area Network，「WAN」）、跨網路(inter-network)（例如網際網路）、以及點對點網路（例如 ad hoc 點對點網路）。

【0097】計算系統可包括客戶端和伺服器。客戶端和伺服器通常在彼此遠端，並且通常經由一通訊網路互動。客戶端和伺服器的關係是由於在各自的電腦上運行且具有對彼此之客戶-伺服器關係的電腦程式所產生。在一些實施方式中，伺服器傳送資料（例如，HTML 頁面）至一客戶端裝置（例如，為了對與該客戶端裝置互動的使用者顯示資料以及從該使用者接收使用者輸入）。在伺

服器處可從客戶端裝置接收在該客戶端裝置處生成的資料（例如，使用者互動的結果）。

【0098】應理解，前述詳細說明在各方面都是說明性和例示性的、並非是限制性的，而且本文所揭露之所揭技術的範圍並不是由前述詳細說明所決定，而是由根據專利法所允許的完整範圍而解釋的請求項來決定。應理解，本文所示和所述的實施例僅為所揭露技術的原理例示，而且熟習本領域技術之人士可在不脫離所揭技術的範疇和精神下進行各種修改。熟習本領域技術之人士可在不脫離所揭技術的範疇和精神下進行各種其他特徵組合。雖然已經以特定實例來描述本發明的實施例，但應理解本發明並不限於那些特定實例，而且對於本領域中具有通常知識者而言，各種其他變化、組合和修改都是顯而易見的，其皆不脫離參照如附請求項而決定之所揭技術的範疇和精神。

【符號說明】

【0099】1、2、3、4、5、6、7、8：連接埠

1、2、3、4、5、5A、5B、6A、6B、10、11、12、13、14、15A、15B：步驟

10、28、110、150：可程式切換裝置

12、112、152：處理器

14、114、154：記憶體

15、115、155：識別模組

16、116：應用程式編程介面（API）

17、117、157：通報模組

18、118、158：資料封裝模組

20a-20p、41、42、43、44、45、46、47、48、120a-120b、160a-160p：I/O網路連接埠

22a-22p、122a-122b、162a-162p：可程式過濾器

30：連網裝置、安全裝置

31、32、35：連網裝置、安全相機

33、34、36：連網裝置、電腦

50：控制器

60、61、62、63：FPT 規則

156：內嵌控制器

200：網路結構

202：網際網路

204：企業網路切換裝置

206：網路控制器

220、240：混合用途的切換裝置

221、222、243、244：桌上型電腦

223、224、232、233：安全相機

230：OT 切換裝置

231：實體安全性控制面板

234：HVAC 管理站

241、242：無線存取點

245：膝上型電腦

【發明申請專利範圍】

【請求項1】 一種可程式切換裝置，包括：

至少一連接埠；以及

至少一可程式過濾器，其通訊耦接至該至少一連接埠，

其中該至少一可程式過濾器係配置以根據一組定義規則許可/拒絕正傳送到或自連接至該至少一連接埠之一連網裝置的資料封包。

【請求項2】 如請求項 1 所述的可程式切換裝置，其中一控制器對該至少一可程式過濾器傳送該組定義規則。

【請求項3】 如請求項 2 所述的可程式切換裝置，其中該控制器是通訊耦接至該可程式切換裝置的一網路裝置。

【請求項4】 如請求項 2 所述的可程式切換裝置，其中該控制器是由一防火牆保護的一 SDN 啟用裝置。

【請求項5】 如請求項 2 所述的可程式切換裝置，更包括：

一應用程式編程介面，該應用程式編程介面連結該控制器至該可程式切換裝置。

【請求項6】 如請求項 1 所述的可程式切換裝置，更包括：

一控制器，係內嵌在該可程式切換裝置內，該控制器對該至少一可程式過濾器傳送該組定義規則。

【請求項7】 如請求項 2 所述的可程式切換裝置，更包括：

一通報模組，該通報模組係配置以對該控制器傳送資料流特徵。

【請求項8】 如請求項 7 所述的可程式切換裝置，其中該控制器分析該資料流特徵，並且根據該分析自動更新該組定義規則。

【請求項9】 如請求項 1 所述的可程式切換裝置，其中該組定義規則係由一網路管理員所配置。

【請求項10】 如請求項 1 所述的可程式切換裝置，其中該組定義規則係由至少一機器學習演算法、一人工智慧或一自動化技術所配置。

【請求項11】 如請求項 1 所述的可程式切換裝置，更包括：

一識別模組，該識別模組用於為該可程式切換裝置提供識別協定。

【請求項12】 如請求項 1 所述的可程式切換裝置，更包括：

一資料封裝模組，該資料封裝模組係配置以接收和傳送來自該可程式切換裝置的資料。

【請求項13】 如請求項 1 所述的可程式切換裝置，其中該至少一連接埠為一連線連接點。

【請求項14】 如請求項 1 所述的可程式切換裝置，其中該至少一連接埠為一無線連接點。

【請求項15】 一種網路基礎架構，包括：

至少二可程式切換裝置，該至少二可程式切換裝置各自具有至少二連接埠，其中每一連接埠係通訊耦接至一可程式過濾器；以及

一控制器，該控制器係通訊耦接至該至少二可程式切換裝置，

其中該控制器以一組定義規則填充通訊耦接至該至少二可程式切換裝置的每一連接埠的該可程式過濾器。

【請求項16】 如請求項 15 所述的網路基礎架構，其中該組定義規則許可/拒絕資料封包傳送到或自至少二連網裝置，該連網裝置通訊耦接至該至少二可程式切換裝置的該至少二連接埠的其中之一。

【請求項17】 如請求項 16 所述的網路基礎架構，其中該組定義規則在該連網裝置之間創建基於網路安全性之隔離。

【請求項18】 如請求項 16 所述的網路基礎架構，其中該組定義規則在該連網裝置之間創建基於網路安全性之分段。

【請求項19】 如請求項 15 所述的網路基礎架構，其中該組定義規則係由一網路管理員所配置。

【請求項20】 如請求項 15 所述的網路基礎架構，其中該組定義規則係由至少一機器學習演算法、一人工智慧或一自動化技術所配置。

【請求項21】 如請求項 15 所述的網路基礎架構，更包括：

一通報模組，該通報模組係配置以對該控制器傳送資料流特徵。

【請求項22】 如請求項 21 所述的網路基礎架構，其中該控制器分析該資料流特徵，並且根據該分析自動更新該組定義規則。

【發明圖式】

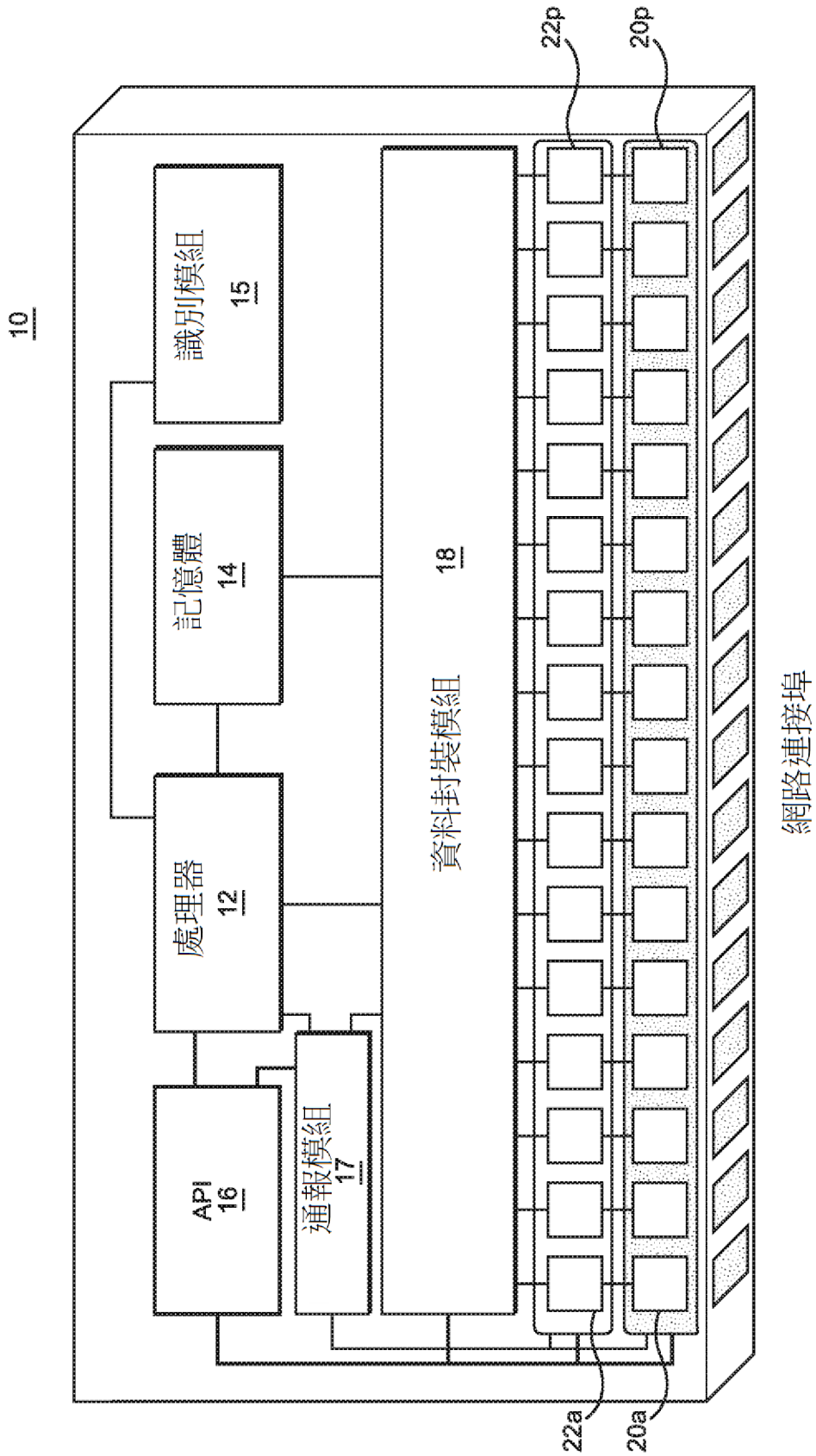
10
識別模組
15
記憶體
14
處理器
12
API
16
通報模組
17
資料封裝模組
18
22p
20p
22a
20a
網路連接埠

圖 1

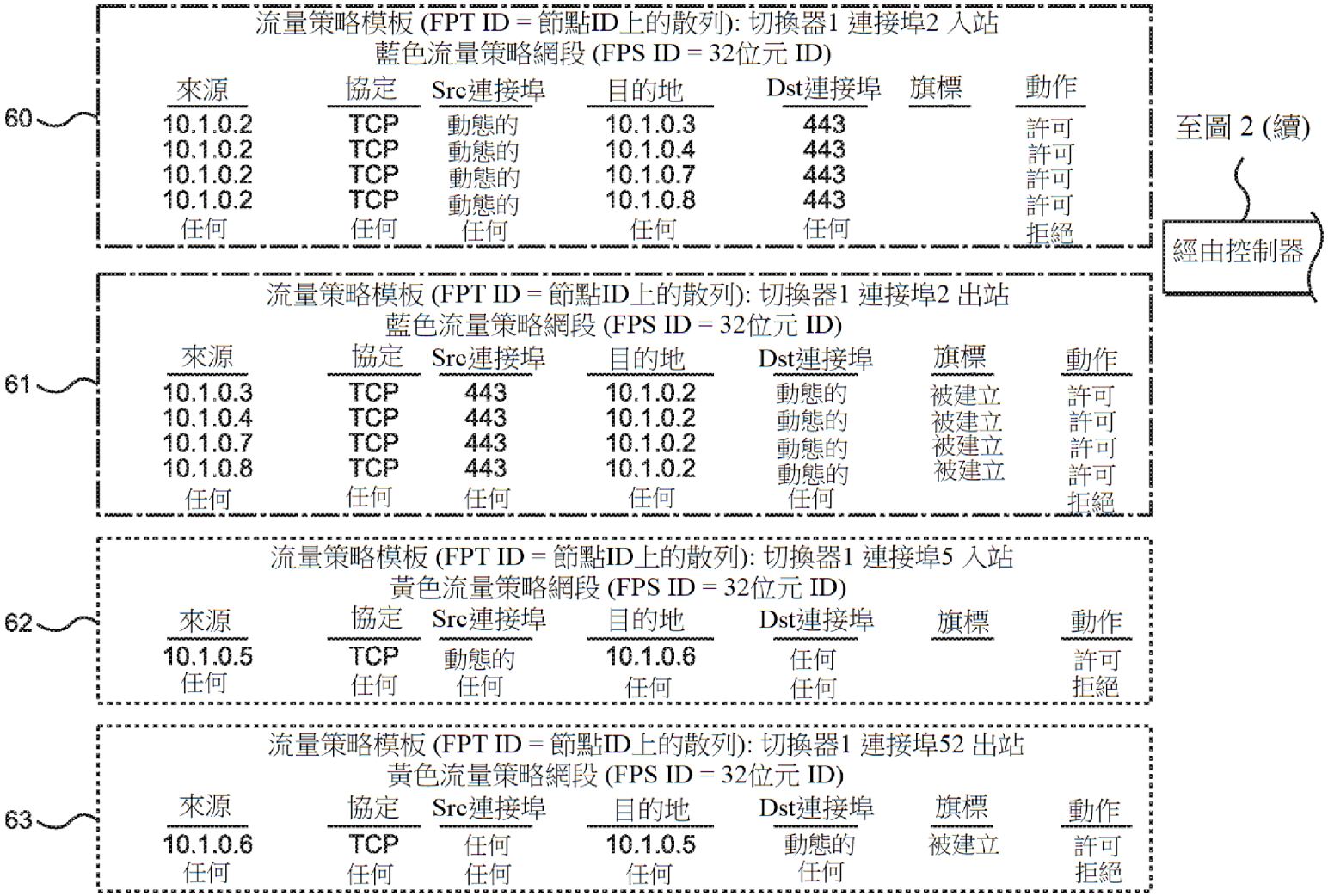
流量策略模板 (FPT ID = 節點ID上的散列): 切換器1 連接埠2 入站
藍色流量策略網段 (FPS ID = 32位元 ID)
60
來源 協定 Src連接埠 目的地 Dst連接埠 旗標 動作
10.1.0.2 TCP 動態的 10.1.0.3 443 許可
10.1.0.2 TCP 動態的 10.1.0.4 443 許可
10.1.0.2 TCP 動態的 10.1.0.7 443 許可
10.1.0.2 TCP 動態的 10.1.0.8 443 許可
任何 任何 任何 任何 任何 拒絕
至圖 2 (續)
經由控制器
流量策略模板 (FPT ID = 節點ID上的散列): 切換器1 連接埠2 出站
藍色流量策略網段 (FPS ID = 32位元 ID)
61
來源 協定 Src連接埠 目的地 Dst連接埠 旗標 動作
10.1.0.3 TCP 443 10.1.0.2 動態的 被建立 許可
10.1.0.4 TCP 443 10.1.0.2 動態的 被建立 許可
10.1.0.7 TCP 443 10.1.0.2 動態的 被建立 許可
10.1.0.8 TCP 443 10.1.0.2 動態的 被建立 許可
任何 任何 任何 任何 任何 拒絕
流量策略模板 (FPT ID = 節點ID上的散列): 切換器1 連接埠5 入站
黃色流量策略網段 (FPS ID = 32位元 ID)
62
來源 協定 Src連接埠 目的地 Dst連接埠 旗標 動作
10.1.0.5 TCP 動態的 10.1.0.6 任何 許可
任何 任何 任何 任何 任何 拒絕
流量策略模板 (FPT ID = 節點ID上的散列): 切換器1 連接埠52 出站
黃色流量策略網段 (FPS ID = 32位元 ID)
63
來源 協定 Src連接埠 目的地 Dst連接埠 旗標 動作
10.1.0.6 TCP 任何 10.1.0.5 動態的 被建立 許可
任何 任何 任何 任何 任何 拒絕

圖 2

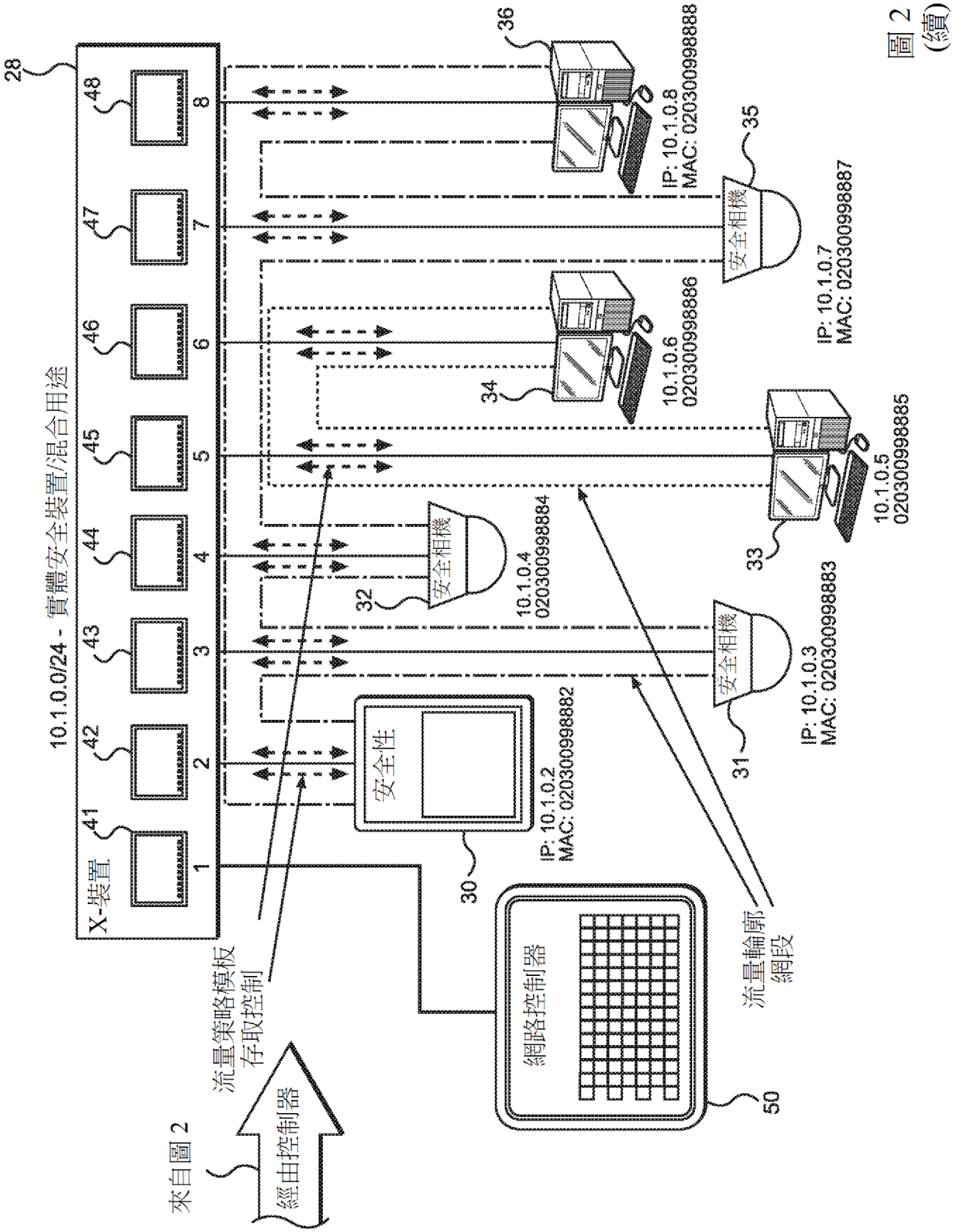
28
10.1.0.0/24 - 實體安全裝置/混合用途
X-裝置
41
42
43
44
45
46
47
48
1
2
3
4
5
6
7
8
36
IP: 10.1.0.8
MAC: 020300998888
35
安全相機
IP: 10.1.0.7
MAC: 020300998887
34
10.1.0.6
020300998886
33
10.1.0.5
020300998885
32
安全相機
10.1.0.4
020300998884
31
安全相機
IP: 10.1.0.3
MAC: 020300998883
30
安全性
IP: 10.1.0.2
MAC: 020300998882
50
網路控制器
流量輪廓
網段
流量策略模板
存取控制
經由控制器
來自圖 2

圖 2
(續)

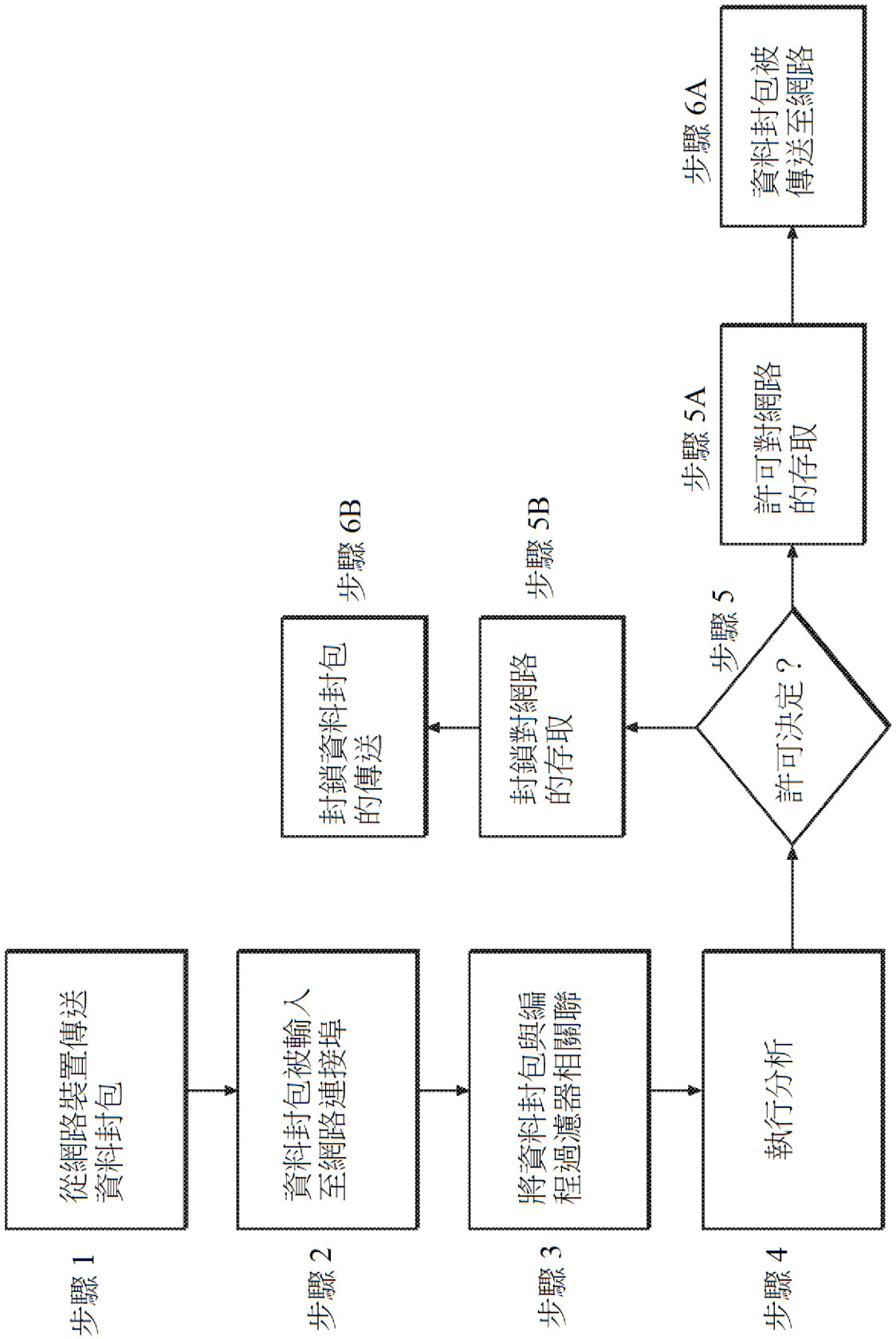
從網路裝置傳送資料封包
步驟 1
資料封包被輸入至網路連接埠
步驟 2
將資料封包與編程過濾器相關聯
步驟 3
執行分析
步驟 4
許可決定？
步驟 5
步驟 5A
許可對網路的存取
步驟 6A
資料封包被傳送至網路
步驟 5B
封鎖對網路的存取
步驟 6B
封鎖資料封包的傳送

圖 3

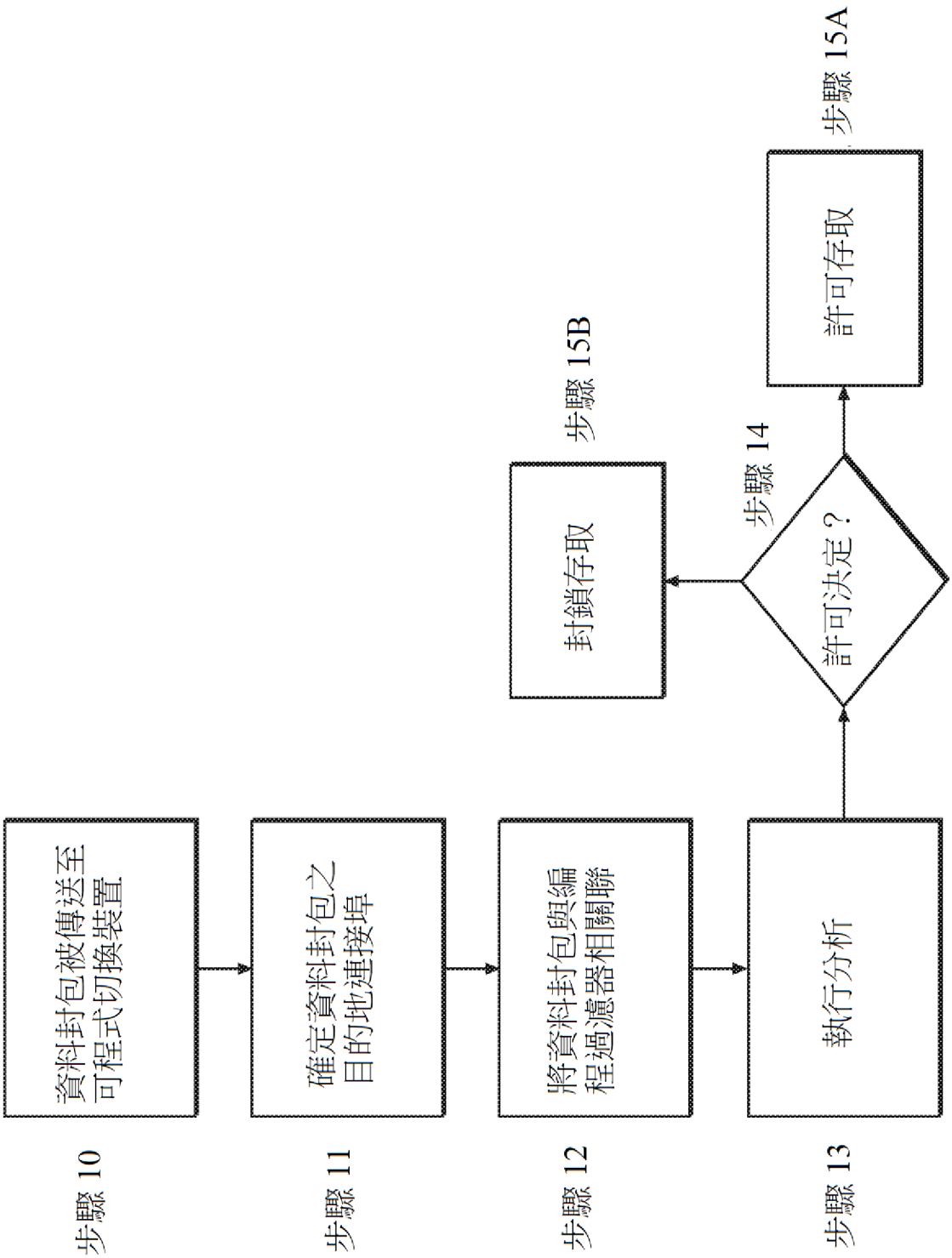
步驟 10
資料封包被傳送至可程式切換裝置
步驟 11
確定資料封包之目的地連接埠
步驟 12
將資料封包與編程過濾器相關聯
步驟 13
執行分析
步驟 14
許可決定？
步驟 15B
封鎖存取
步驟 15A
許可存取

圖 4

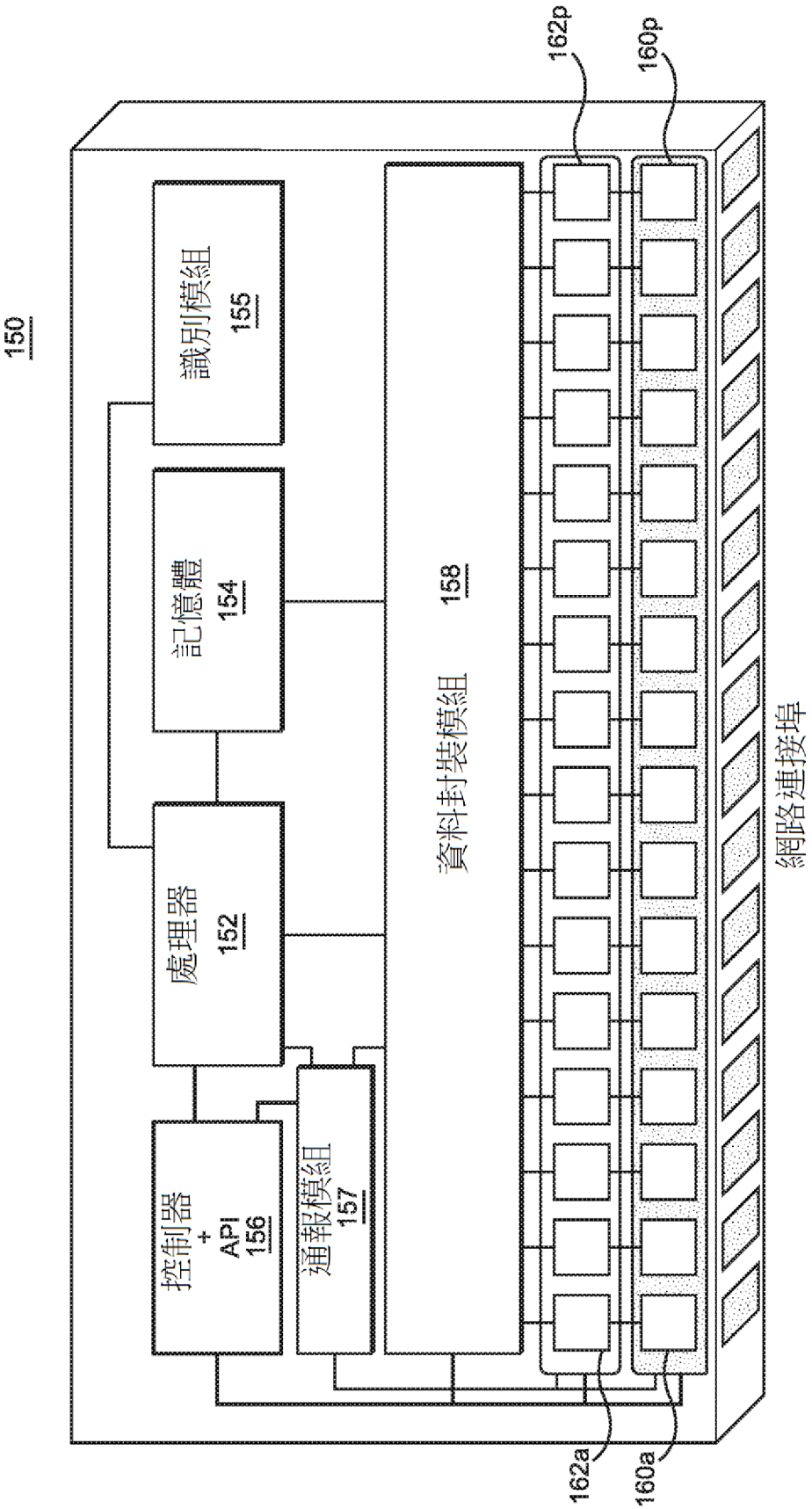
150
識別模組
155
記憶體
154
處理器
152
控制器
+
API
156
通報模組
157
資料封裝模組
158
162p
160p
162a
160a
網路連接埠

圖 5

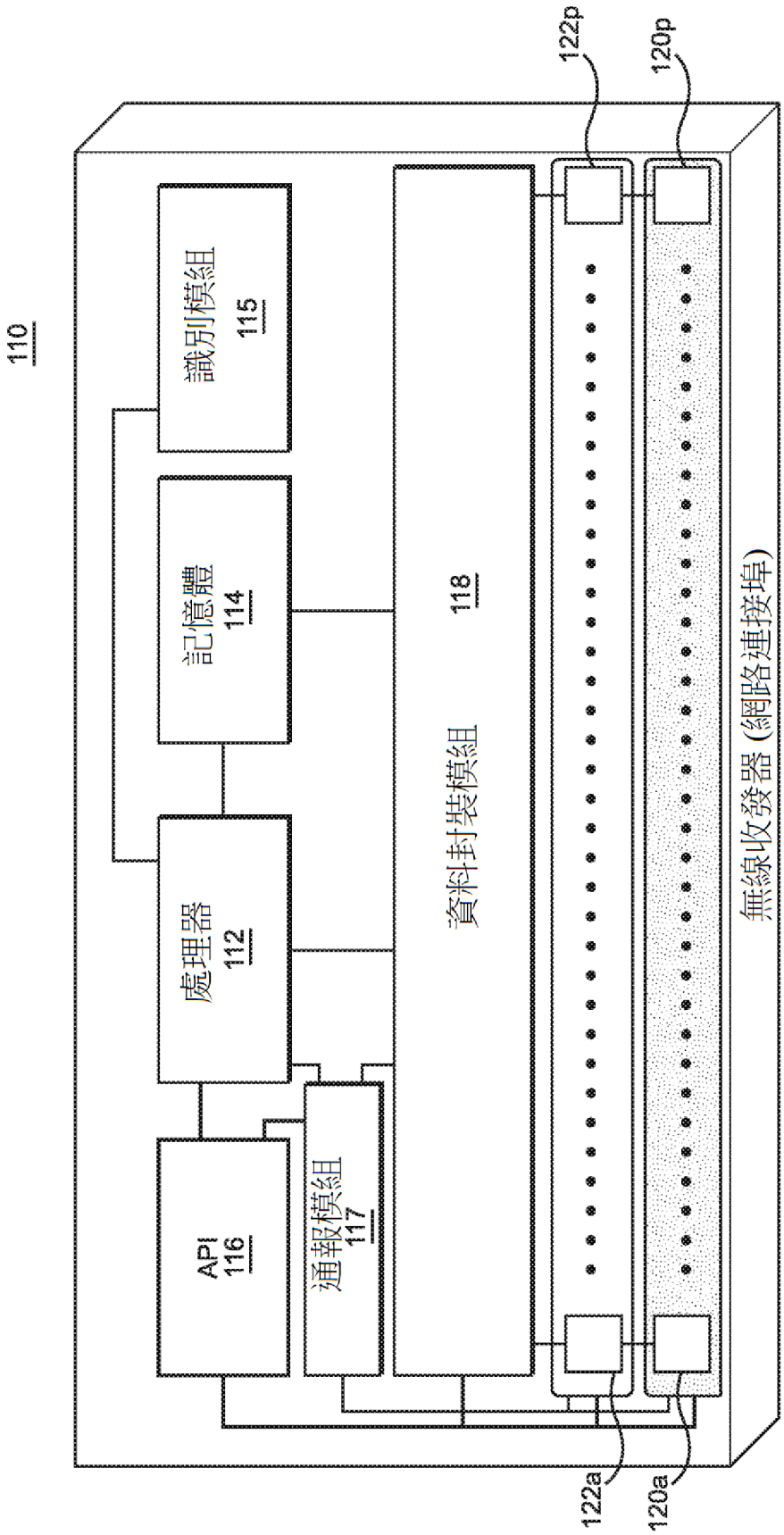
110
識別模組
115
記憶體
114
處理器
112
API
116
通報模組
117
資料封裝模組
118
無線收發器 (網路連接埠)
122p
120p
122a
120a

圖 6

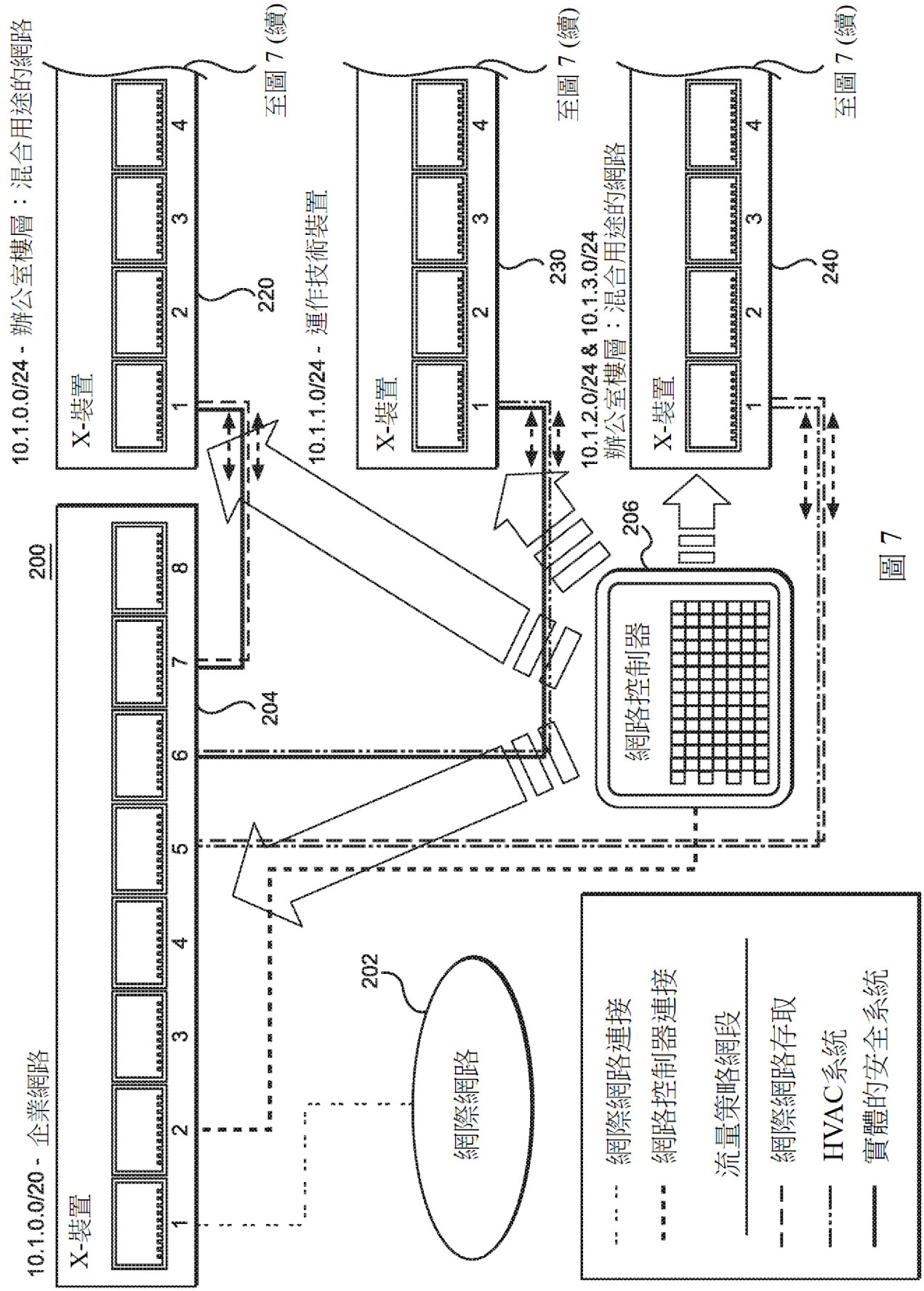
10.1.0.0/20 - 企業網路
X-裝置
200
1
2
3
4
5
6
7
8
202
網際網路
204
10.1.0.0/24 - 辦公室樓層：混合用途的網路
X-裝置
220
至圖 7 (續)
10.1.1.0/24 - 運作技術裝置
X-裝置
230
至圖 7 (續)
10.1.2.0/24 & 10.1.3.0/24
辦公室樓層：混合用途的網路
X-裝置
240
至圖 7 (續)
206
網路控制器
網際網路連接
網路控制器連接
流量策略網段
網際網路存取
HVAC系統
實體的安全系統

圖 7

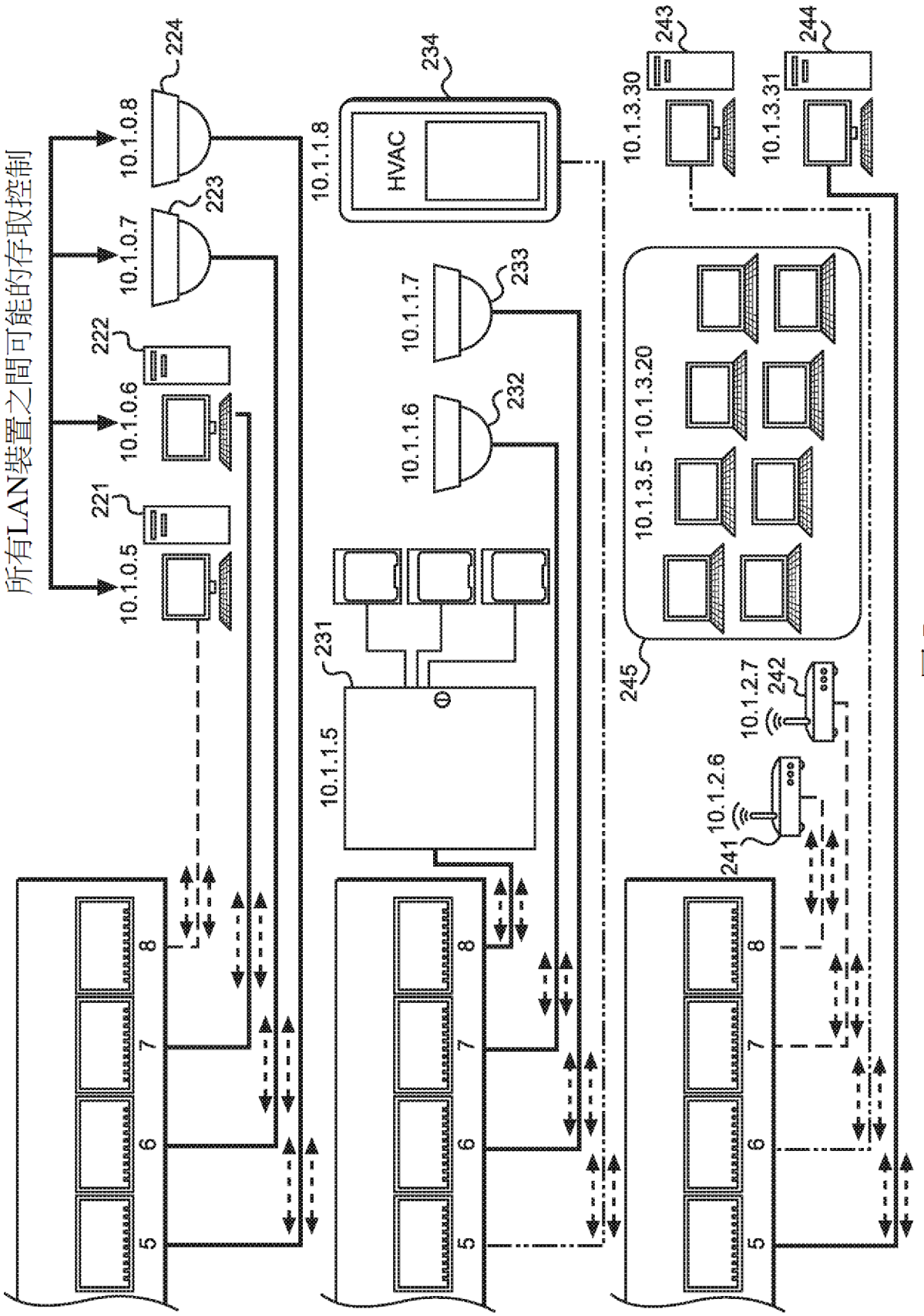
LAN上的限制網路存取
所有LAN裝置之間可能的存取控制
10.1.0.5
221
10.1.0.6
222
10.1.0.7
223
10.1.0.8
224
10.1.1.5
231
10.1.1.6
232
10.1.1.7
233
10.1.1.8
234
HVAC
10.1.3.5 - 10.1.3.20
245
10.1.2.6
241
10.1.2.7
242
10.1.3.30
243
10.1.3.31
244
5
6
7
8

圖 7
(續)