201640405

(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 201640405 A

(43)公開日： 中華民國 105 (2016) 年 11 月 16 日

(21)申請案號：104142502 (22)申請日： 中華民國 104 (2015) 年 12 月 17 日

(51)Int. Cl.： *G06F21/56 (2013.01)*

(30)優先權：2015/05/15 中國大陸 201510250887.4

(71)申請人：阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)

香港

(72)發明人：李晗 (CN) ；段亞雄 (CN) ；賈炯 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：12 項 圖式數：5 共 66 頁

(54)名稱

網站攻擊防禦方法及裝置

(57)摘要

本發明提供了一種網站攻擊防禦方法及裝置，其中，該網站攻擊防禦方法包括：獲取目標 IP 位址所對應的流量閾值；判斷該目標 IP 位址的即時訪問流量是否超過該流量閾值；根據判斷結果，對該目標 IP 位址的訪問流量進行處理。本發明根據目標 IP 位址對應的轉發到黑洞路由的流量閾值對該 IP 位址的流量進行處理，降低使用黑洞路由防禦網路攻擊的負面效果。

指定代表圖：

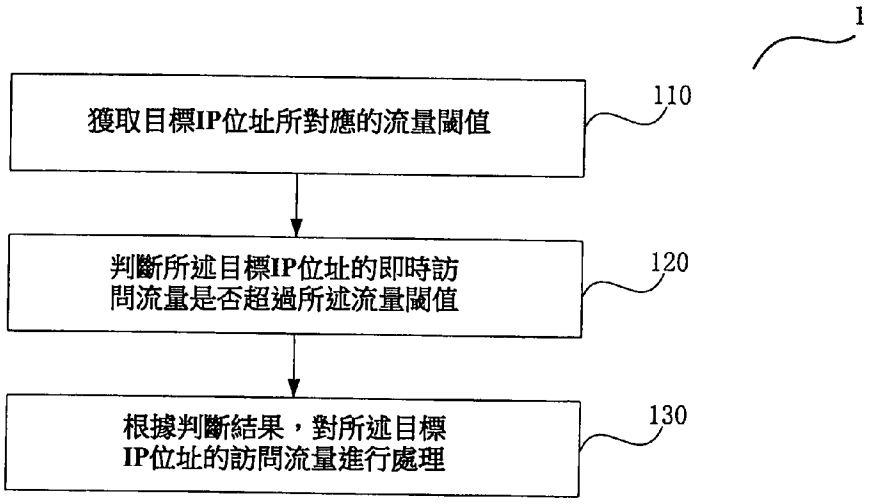

圖 1

201640405

發明摘要

※申請案號：104142502

※申請日：104 年 12 月 17 日　　※IPC 分類：G06F 21/56 (2013.01)

【發明名稱】(中文/英文)

網站攻擊防禦方法及裝置

【中文】

本發明提供了一種網站攻擊防禦方法及裝置，其中，該網站攻擊防禦方法包括：獲取目標 IP 位址所對應的流量閾值；判斷該目標 IP 位址的即時訪問流量是否超過該流量閾值；根據判斷結果，對該目標 IP 位址的訪問流量進行處理。本發明根據目標 IP 位址對應的轉發到黑洞路由的流量閾值對該 IP 位址的流量進行處理，降低使用黑洞路由防禦網路攻擊的負面效果。

【英文】

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】(中文/英文)

網站攻擊防禦方法及裝置

【技術領域】

本發明涉及網路安全技術領域，尤其涉及一種網站攻擊防禦方法及裝置。

【先前技術】

分散式拒絕服務(DDoS, Distributed Denial of Service)攻擊指借助於客戶/伺服器技術，將多個電腦聯合起來作為攻擊平臺，對一個或多個目標發動 DDoS 攻擊，從而成倍地提高拒絕服務攻擊的威力。通常，攻擊者將 DDoS 主控程式安裝在一個電腦上，在一個設定的時間主控程式將與大量代理程式通訊，代理程式被安裝在 Internet 上的電腦上。代理程式收到主控程式的指令就發動攻擊。利用客戶/伺服器技術，主控程式能在幾秒鐘內啟動成百上千次代理程式的執行。DDoS 攻擊的原理是找到被攻擊者的資源瓶頸，透過消耗資源使被攻擊者業務不可用。在目前的網際網路業務中，伺服器 CPU、記憶體、頻寬、資料庫等都可能成為資源瓶頸。隨著越來越多的使用者使用虛擬化資料中心和雲端服務，DDoS 攻擊開始轉向雲端計算。

在路由器上對被攻擊的 IP 位址配置黑洞路由是防禦

DDoS 攻擊的常用方法，黑洞路由就是將識別出的無關路由吸入其中，使它們有來無回的路由。黑洞路由的出介面被指定為 null0 介面，發送到 null0 介面的資料都會被丟棄，這樣能將受到攻擊的 IP 位址的所有流量都丟棄掉，透過犧牲被攻擊的 IP 位址的流量，保護其它未受攻擊 IP 位址的網路頻寬資源可用，且對系統負載影響非常小。

目前，通常採用的路由黑洞防禦方案是：給定一個流量閾值（黑洞閾值），當一個 IP 位址的訪問流量超過該黑洞閾值時，將該 IP 的流量發佈到黑洞路由。然而，給定流量閾值的防禦方式存在以下缺點：一方面，給定流量閾值的防禦方式不能適應不同使用者的業務和流量的不同，對各個使用者採用無差別的流量閾值進行防禦，使用者體驗不好；另一方面，使用者的流量被引入黑洞會導致使用者伺服器在一段時間內不能正常訪問，因此將受攻擊業務打進黑洞，實際上相當於攻擊成功，所以給定流量閾值的防禦方式很容易被駭客利用。

【發明內容】

本發明的一個目的是提供一種網站攻擊防禦方法及裝置，其能降低使用黑洞路由防禦攻擊的負面效果。

根據本發明的一方面，提供了一種網站攻擊防禦方法，該網站攻擊防禦方法包括：

獲取目標 IP 位址所對應的流量閾值；

判斷所述目標 IP 位址的即時訪問流量是否超過所述

流量閾值；

根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

根據本發明的另一方面，還提供了一種網站攻擊防禦裝置，該　網站攻擊防禦裝置包括：

第一獲取模組，用於獲取目標 IP 位址所對應的流量閾值；

第一判斷模組，用於判斷所述目標 IP 位址的即時訪問流量是否超過所述流量閾值；

第一處理模組，用於根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

與先前技術相比，本發明的實施例具有以下優點：透過獲取目標 IP 位址對應的流量閾值，判斷該目標 IP 位址的即時訪問流量是否超過對應的流量閾值，從而根據判斷結果，對該 IP 位址的訪問流量進行處理，其中，如果該 IP 位址的訪問流量超過對應的流量閾值，則將所述 IP 位址的訪問流量轉發到黑洞路由，實現了根據目標 IP 位址對應的轉發到黑洞路由的流量閾值對該 IP 位址的流量進行處理，從而，降低使用黑洞路由防禦網路攻擊的負面效果。

【圖式簡單說明】

透過閱讀參照以下圖式所作的對非限制性實施例所作的詳細描述，本發明的其它特徵、目的和優點將會變得更

明顯：

圖 1 為本發明一個實施例提供的方法的流程圖；

圖 2 為本發明另一個實施例的方法流程圖；

圖 3 為本發明又一個實施例的方法流程圖；

圖 4 為本發明一個實施例提供的裝置示意圖；

圖 5 為本發明另一個實施例的裝置示意圖。

圖式中相同或相似的元件符號代表相同或相似的部件。

【實施方式】

在更加詳細地討論示例性實施例之前應當提到的是，一些示例性實施例被描述成作為流程圖描繪的處理或方法。雖然流程圖將各項操作描述成順序的處理，但是其中的許多操作可以被平行地、並行地或者同時實施。此外，各項操作的順序可以被重新安排。當其操作完成時所述處理可以被終止，但是還可以具有未包括在圖式中的附加步驟。所述處理可以對應於方法、函數、規程、子常式、副程式等等。

在上下文中所稱“電腦設備”，也稱為“電腦”，是指可以透過執行預定程式或指令來執行數值計算和/或邏輯計算等預定處理過程的智慧電子設備，其可以包括處理器與記憶體，由處理器執行在記憶體中預存的存續指令來執行預定處理過程，或是由 ASIC、FPGA、DSP 等硬體執行預定處理過程，或是由上述二者組合來實現。電腦設備

包括但不限於伺服器、個人電腦、筆記型電腦、平板電腦、智慧型手機等。

所述電腦設備包括使用者設備與網路設備。其中，所述使用者設備包括但不限於電腦、智慧型手機、PDA 等；所述網路設備包括但不限於單個網路服務器、多個網路服務器組成的伺服器組或基於雲端計算（Cloud Computing）的由大量電腦或網路服務器構成的雲端，其中，雲端計算是分散式運算的一種，由一群鬆散耦合的電腦集組成的一個超級虛擬電腦。其中，所述電腦設備可單獨執行來實現本發明，也可接入網路並透過與網路中的其他電腦設備的交互操作來實現本發明。其中，所述電腦設備所處的網路包括但不限於網際網路、廣域網路、都會網路、區域網路、VPN 網路等。

需要說明的是，所述使用者設備、網路設備和網路等僅為舉例，其他現有的或今後可能出現的電腦設備或網路如可適用於本發明，也應包含在本發明保護範圍以內，並以引用方式包含於此。

後面所討論的方法（其中一些透過流程圖示出）可以透過硬體、軟體、韌體、中介軟體、微程式、硬體描述語言或者其任意組合來實施。當用軟體、韌體、中介軟體或微程式來實施時，用以實施必要任務的程式碼或程式碼片段可以被儲存在機器或電腦可讀媒體（比如儲存媒體）中。（一個或多個）處理器可以實施必要的任務。

這裡所公開的具體結構和功能細節僅僅是代表性的，

並且是用於描述本發明的示例性實施例的目的。但是本發明可以透過許多替換形式來具體實現，並且不應當被解釋成僅僅受限於這裡所闡述的實施例。

應當理解的是，雖然在這裡可能使用了術語“第一”、“第二”等等來描述各個單元，但是這些單元不應當受這些術語限制。使用這些術語僅僅是為了將一個單元與另一個單元進行區分。舉例來說，在不背離示例性實施例的範圍的情況下，第一單元可以被稱為第二單元，並且類似地第二單元可以被稱為第一單元。這裡所使用的術語“和/或”包括其中一個或更多所列出的相關聯專案的任意和所有組合。

這裡所使用的術語僅僅是為了描述具體實施例而不意圖限制示例性實施例。除非上下文明確地另有所指，否則這裡所使用的單數形式“一個”、“一項”還意圖包括複數。還應當理解的是，這裡所使用的術語“包括”和/或“包含”規定所陳述的特徵、整數、步驟、操作、單元和/或元件的存在，而不排除存在或添加一個或更多其他特徵、整數、步驟、操作、單元、元件和/或其組合。

還應當提到的是，在一些替換實現方式中，所提到的功能/動作可以按照不同於圖式中標示的順序發生。舉例來說，取決於所涉及的功能/動作，相繼示出的兩幅圖實際上可以基本上同時執行或者有時可以按照相反的順序來執行。

下面結合圖式對本發明作進一步詳細描述。

圖 1 為本發明一個實施例的網站攻擊防禦方法流程圖。根據本發明的方法 1 至少包括步驟 110、步驟 120、步驟 130。

本發明主要用於防禦網路流量攻擊，尤其是分散式拒絕服務（DDoS,Distributed Denial of Service）攻擊。

該方法 1 例如可以在網路的入口閘道側使用，從而為進入網路的訪問流量配置合適的路由，以到達訪問流量應去往的位置。或者，該方法 1 可以由網路中配置的一個特殊的安全伺服器執行，所有進入網路的訪問流量要經過該安全伺服器處理後發往其應去往的位置。

在步驟 110 中，獲取目標 IP 位址所對應的流量閾值。

在根據本發明方法的攻擊防禦系統中，每個使用者（例如一個銀行）的源 IP 位址（使用者伺服器的 IP 位址）並不直接接受外部的訪問，而是透過源 IP 位址的多個轉發 IP 位址接受外部訪問。目標 IP 位址可以指實施本發明的攻擊防禦系統中任一使用者的多個轉發 IP 位址中的一個。攻擊防禦系統不只針對一個使用者進行攻擊防禦，也不只針對一個 IP 位址進行攻擊防禦。它針對例如網路中所有使用者的所有目標 IP 位址（例如轉發 IP 位址）進行防禦，負責將接收到的外部對每個使用者的每個目標 IP 位址的訪問流量進行處理。

其中，所述流量閾值是將所述目標 IP 位址的訪問流量轉發到黑洞路由的流量閾值。當到某一使用者的某一目

標 IP 位址的訪問流量過大（例如超出流量閾值），很可能與該目標 IP 位址受到了攻擊有關。

根據本發明的一個實施例，可以為使用者設置流量閾值，其中目標 IP 位址所對應的流量閾值是目標 IP 位址所屬的使用者的流量閾值。也就是說，屬於同一個使用者的目標 IP 位址對應的流量閾值相同。

其中，獲取目標 IP 位址所對應的流量閾值的步驟包括：根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，該目標 IP 位址所屬的使用者的使用者等級例如可以分為普通、白銀、黃金、鑽石。其中，可以根據等級劃分所依據的規則配置每個等級對應的等級參數。例如，若上述普通、白銀、黃金、鑽石使用者是根據等級由低至高劃分的，則根據等級高低配置普通、白銀、黃金、鑽石分別對應的等級參數為 1、2、3、4。所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。其中，歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數為歷史上特定時

間段內（例如，距離當前時間一個星期內）該使用者擁有的各個 IP 位址的訪問流量被轉發到黑洞路由的次數的總和。特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長為在該特定時間段內該使用者擁有的各個 IP 位址被攻擊的時長的總和。

更具體而言，根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值的一種具體實施方式為：

獲取預先配置的流量閾值確定規則；根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

具體地，可以根據該目標 IP 位址所屬的使用者的使用者等級、歷史上特定時間段內該目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、所述特定時間段內該目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長中的任意一項或多項，並結合預先配置的流量閾值確定規則，確定該目標 IP 位址所對應的流量閾值。其中，預先配置的流量閾值確定規則可以是根據大量歷史統計資訊中的相關資料進行分析而配置的。

例如，作為流量閾值確定規則的一個例子的流量閾值

公式可以配置為：

$$HoleThreshold = h_0 + Level_1(u) + Black_1(b) + AttackTime_1(t) \quad (1)$$

其中，$HoleThreshold$ 為流量閾值，單位 Gbps；h_0 為預設流量閾值，較佳地，h_0=5Gbps；$Level_1(u)$ 為目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數；$Black_1(b)$ 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數；$AttackTime_1(t)$ 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的流量閾值函數。上述各狀態資訊和歷史訪問資訊對應的流量閾值函數的值的單位均為 Gbps。

需要說明的是，上述公式（1）僅為本發明獲取預先配置的流量閾值確定規則的一種實施方式，目標 IP 位址的流量閾值可以為預設流量閾值 h_0 與上述任意一項或多項流量閾值函數之和。

例如，公式（1）還可以為：

$$HoleThreshold = h_0 + Level_1(u) + Black_1(b) \quad (1a)$$

或者

$$HoleThreshold = h_0 + Level_1(u) + AttackTime_1(t) \quad (1b)$$

或者

$$HoleThreshold = h_0 + Level_1(u) \quad (1c)$$

在一個具體實施例中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

具體地，可以預先配置各狀態資訊和歷史訪問資訊對應的流量閾值函數。

其中，使用者等級可以是根據使用者日常平均訪問流量的高低進行劃分的，也就是說，使用者的日常平均訪問流量越高，該使用者等級越高。因此，使用者等級越高，對應的流量閾值函數 $Level_1(u)$ 的值越高，流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數，則可以將使用者等級對應的流量閾值函數 $Level_1(u)$ 配置為使用者等級的增函數。

在一個具體例子中，目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數 $Level_1(u)$ 可以配置為：

$$Level_1(u) = l_1 u \quad (2)$$

或者

$$Level_1(u) = l_1 u + h_1 \quad (2')$$

或者

$$Level_1(u) = \begin{cases} 0, u = 1 \\ 1, u = 2 \\ 3, u = 3 \\ 5, u = 4 \end{cases} \qquad (2'')$$

上述公式（2）、（2’）和（2’’）中，u 為目標 IP 位址所屬的使用者的使用者等級，在上述公式（2）、（2’）和（2’’）中，目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數 $Level_1(u)$ 為使用者等級的增函數。

其中，目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數越多，該 IP 位址受到攻擊的危險性越大，因此，特定時間段內該 IP 位址的訪問流量被轉發到黑洞路由的次數越多，該 IP 位址對應的流量閾值應越小，因此，流量閾值是歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數，則特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1(b)$，可以配置為該特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數。

在一個具體的例子中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1(b)$ 可以配置為：

$$Black_1(b) = h_2 - l_2 b \qquad (3)$$

或者

$$Black_1(b) = l_3 h_2 - l_2 b \quad (3')$$

或者

$$Black_1(b) = \begin{cases} 5, b = 0 \\ 2, b = 1 \\ 0{,}1 < b < 5 \\ -1{,}5 \le b < 10 \\ -2, b \ge 10 \end{cases} \quad (3'')$$

上述公式（3）、（3’）和（3’’）中，b 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數。特定時間段例如可以為距當前時間一周，則 b 為上周目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數。在上述公式（3）、（3’）和（3’’）中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1(b)$ 為特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數。

其中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長越長，該使用者越常遭到攻擊（攻擊者的重點攻擊目標），因此，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長越長，流量閾值應該越低，因此，流量閾值是歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數，則可以將特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的流量閾值函

數 $AttackTime_1(t)$ 配置為特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

在一個具體的例子中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的流量閾值函數 $AttackTime_1(t)$ 可以配置為：

$$AttackTime_1(t) = h_3 - l_3 t \qquad (4)$$

或者

$$AttackTime_1(t) = l_4 h_3 - l_3 t \qquad (4')$$

或者

$$AttackTime(t) = \begin{cases} 0, t < 3 \\ -1, 3 \le t < 10 \\ -2, 10 \le t < 30 \\ -3, t \ge 30 \end{cases} \qquad (4'')$$

上述公式（4）、（4'）和（4''）中，t 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長，單位為小時，例如，t 可以為上周目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。在上述公式（4）、（4'）和（4''）中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的流量閾值函數是特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

上述公式（2）、（2'）、（3）、（3'）、（4）、（4'）中的參數 h_1、h_2、h_3 和 l_1、l_2、l_3、l_4 可以根據對歷史統計資訊中的相關資料進行分析獲得。上述公式

（2''）、（3''）、（4''）為預先對歷史統計資訊中的相關資料的進行分析後而配置的。

根據上述預先配置的目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數、歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數、所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的流量閾值函數中的任意一項或多項，可以確定該目標 IP 位址所對應的流量閾值；其中，該目標 IP 位址對應的流量閾值為上述任意一項或多項與預設流量閾值的和。

下面舉一個獲取目標 IP 位址對應的流量閾值的例子：

例如，預設流量閾值 h_0 為 5Gbps；獲取到目標 IP 位址所屬的使用者等級為白銀使用者， u=2；上周該使用者所有 IP 位址被轉發到黑洞路由的次數為 6 次，即 b=6；上周該使用者所有 IP 位址被攻擊總時長為 19 小時，即 t=19；

利用公式（2''）、（3''）、（4''）可以得到該使用者各項流量閾值函數對應的數值分別為 $Level_1(u)$ =1，$Black_1(b)$ =-1，$AttackTime_1(t)$ =-2，再根據公式（1）可以得到該目標 IP 位址對應的流量閾值為 3Gbps。

根據本發明的另一個實施例，可以為使用者的 IP 位址分別設置流量閾值，其中目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的流量閾值。也就是說，屬於

同一個使用者的目標 IP 位址對應的流量閾值不一定相同。

其中，獲取目標 IP 位址所對應的流量閾值的步驟包括：根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

具體而言，根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值的一種具體實施方式為：

獲取預先配置的流量閾值確定規則；根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

具體地，可以根據該目標 IP 位址所屬的使用者的使用者等級、歷史上特定時間段內該目標 IP 位址的訪問流量被轉發到黑洞路由的次數、所述特定時間段內該目標 IP 位址被攻擊的總時長中的任意一項或多項，並結合預先配置的流量閾值確定規則，確定該目標 IP 位址所對應的流量閾值。其中，預先配置的流量閾值確定規則可以是根據

大量歷史統計資訊中的相關資料進行分析而配置的。

例如，作為流量閾值確定規則的一個例子的流量閾值公式可以配置為前述的公式（1）。

需說明的是，在本實施例中公式（1）中的各個流量閾值函數的含義與前述實施例中不同。其中，*HoleThreshold* 為流量閾值，單位 Gbps；h_0 為預設流量閾值，較佳地，h_0=5Gbps；$Level_1(u)$ 為目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數；$Black_1(b)$ 為歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數；$AttackTime_1(t)$ 為歷史上特定時間段內目標 IP 位址被攻擊的總時長對應的流量閾值函數。上述各狀態資訊和歷史訪問資訊對應的流量閾值函數的值的單位均為 Gbps。

上述公式（1）僅為本發明獲取預先配置的流量閾值確定規則的一種實施方式，目標 IP 位址的流量閾值可以為預設流量閾值 h_0 與上述任意一項或多項流量閾值函數之和。例如，公式（1）還可以為前述實施例中的公式（1a）、（1b）或（1c）。

在一個具體實施例中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的減函數。

具體地，可以預先配置各狀態資訊和歷史訪問資訊對

應的流量閾值函數。

其中，可以將目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數 $Level_1(u)$ 配置為使用者等級的增函數。

在一個具體例子中，目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數 $Level_1(u)$ 可以配置為前述實施例中的公式（2）或（2'）或（2''）。在本實施例中，u 為目標 IP 位址所屬的使用者的使用者等級。在公式（2）、（2'）和（2''）中，目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數 $Level_1(u)$ 為使用者等級的增函數。

其中，可以將特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1(b)$，配置為特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數。

在一個具體的例子中，特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1(b)$ 可以配置為前述實施例中的（3）、（3'）或（3''）。在本實施例中，b 為歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數。特定時間段例如可以為距當前時間一周，則 b 為上周目標 IP 位址的訪問流量被轉發到黑洞路由的次數。在上述公式（3）、（3'）和（3''）中，特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數 $Black_1$

（*b*）為特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數。

其中，可以將特定時間段內目標 IP 位址被攻擊的總時長對應的流量閾值函數 $AttackTime_1(t)$ 配置為特定時間段內目標 IP 位址被攻擊的總時長的減函數。

在一個具體的例子中，特定時間段內目標 IP 位址被攻擊的總時長對應的流量閾值函數 $AttackTime_1(t)$ 可以配置為前述實施例中的公式（4）、（4'）或（4''）。在本實施例中，*t* 為歷史上特定時間段內目標 IP 位址被攻擊的總時長，單位為小時，例如，*t* 可以為上周目標 IP 位址被攻擊的總時長。在上述公式（4）、（4'）和（4''）中，特定時間段內目標 IP 位址被攻擊的總時長對應的流量閾值函數是特定時間段內目標 IP 位址被攻擊的總時長的減函數。

根據上述預先配置的目標 IP 位址所屬的使用者的使用者等級對應的流量閾值函數、歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的流量閾值函數、所述特定時間段內目標 IP 位址被攻擊的總時長對應的流量閾值函數中的任意一項或多項，可以確定該目標 IP 位址所對應的流量閾值，其中，該目標 IP 位址對應的流量閾值為上述任意一項或多項與預設流量閾值的和。

在步驟 120 中，判斷所述目標 IP 位址的即時訪問流量是否超過所述流量閾值。

其中，即時訪問流量就是即時獲取的該目標 IP 位址

當前時間的訪問流量，也就是說，即時判斷該目標 IP 位址當前訪問流量是否超過起其對應的流量閾值。

在步驟 130 中，根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

具體地，判斷所述目標 IP 位址的即時訪問流量是否超過所述流量閾值判斷結果包括該目標 IP 位址的即時訪問流量超過其對應的流量閾值和該目標 IP 位址的即時訪問流量未超過其對應的流量閾值兩種，可以根據判斷結果對該 IP 位址的訪問流量進行處理。其中，如果所述 IP 位址的訪問流量未超過所述流量閾值，則可以對所述 IP 位址的訪問流量進行流量清洗。如果所述 IP 位址的訪問流量超過所述流量閾值，則可以將所述 IP 位址的訪問流量轉發到黑洞路由。

在一個實施例中，步驟 130 可以進一步包括步驟 131。

參考圖 2，在步驟 131 中，如果所述目標 IP 位址的訪問流量超過所述流量閾值，則為所述目標 IP 位址配置黑洞路由，從而將所述目標 IP 位址的訪問流量轉發到黑洞路由。

具體地，若該目標 IP 位址的訪問流量超過相應的流量閾值，則該 IP 位址可能遭到流量攻擊，則可以透過為該 IP 位址配置黑洞路由的方式將該 IP 位址的訪問流量轉到黑洞路由，從而將該 IP 位址的訪問流量丟棄掉。其中，為該 IP 位址配置黑洞路由即是建立一個路由條目，

將該 IP 位址轉向 null0 介面。其中，發送到介面的資料都會被丟棄，這樣能將該 IP 位址的所有流量都丟棄掉。

採用這種方式，如果目標 IP 位址被攻擊，則透過犧牲該被攻擊的 IP 位址的訪問流量，保護其它未受攻擊 IP 位址的網路頻寬資源可用，且對系統負載影響非常小。

基於上述實施例，可選地，網站攻擊防禦方法還包括步驟 140~步驟 160。

參考圖 3，在步驟 140 中，獲取所述目標 IP 位址所對應的黑洞路由解除時間。

其中，將所述目標 IP 位址所屬的使用者的目標 IP 位址的訪問流量轉發到黑洞路由後，經過一段時間還需解除該 IP 位址的黑洞路由。所述黑洞路由解除時間是將所述目標 IP 位址所屬的使用者的目標 IP 位址的訪問流量轉發到黑洞路由的保持時間，當達到該目標 IP 位址所對應的黑洞路由解除時間，則解除該目標 IP 位址的黑洞路由。其中，每個目標 IP 位址具有一個對應的黑洞路由解除時間。

根據本發明的一個實施例，可以為使用者設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為所述目標 IP 位址所屬的使用者設置的黑洞路由解除時間。也就是說，屬於同一個使用者的目標 IP 位址對應的黑洞路由解除時間相同。

其中，獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟可以包括：根據所述目標 IP 位址所屬的使用

者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者的使用者等級例如可以分為普通、白銀、黃金、鑽石。其中，可以根據等級劃分所依據的規則配置每個等級對應的等級參數，例如，若上述普通、白銀、黃金、鑽石使用者是根據等級由低至高劃分的，則根據等級高低配置普通、白銀、黃金、鑽石分別對應的等級參數為 1、2、3、4。所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。其中，歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數為歷史上特定時間段內（例如，距離當前時間一個星期內）該使用者擁有的各個 IP 位址的訪問流量被轉發到黑洞路由的次數的總和。所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量為在該特定時間段內該目標 IP 位址所屬的使用者擁有的各個 IP 位址中被攻擊的最大流量。所述特定時間

段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長為在該特定時間段內該使用者擁有的各個 IP 位址被攻擊的時長的總和。

更具體而言，所述根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間的一種具體實施方式為：

獲取預先配置的黑洞路由解除時間確定規則；根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

具體地，可以根據所述目標 IP 位址所屬的使用者的使用者等級、歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量、所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長中的任意一項或多項，並結合預先配置的黑洞路由解除時間確定規則，確定該 IP 位址所對應的黑洞路由解除時間。其中，預先配置的黑洞路由解除時間確定規則可以是根據大量歷史統計資訊中的相關資料進行分析而配置的。

例如，作為黑洞路由解除時間確定規則的一個例子的黑洞路由解除時間公式可以配置為：

$$\text{Re}\,liefTime = t_0 + Level_2(\text{u}) + Black_2(b) + Peak_2(a) + AttackTime_2(t) \quad (5)$$

其中，*ReliefTime* 為黑洞路由解除時間，單位為小時，t_0 為預設黑洞解除時間，較佳地，t_0=2.5 小時；$Level_2(u)$ 為使用者等級對應的黑洞路由解除時間函數；$Black_2(b)$ 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數；$Peak_2(a)$ 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數；$AttackTime_2(t)$ 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數。上述各狀態資訊或歷史訪問資訊對應的黑洞路由解除時間函數的值的單位均為小時。

需要說明的是，上述公式（5）僅為本發明獲取預先配置的黑洞路由解除時間確定規則的一種實施方式，黑洞路由解除時間可以為預設黑洞路由解除時間 t_0 與上述任意一項或多項黑洞路由解除時間函數之和。

例如，公式（5）還可以為：

$$\text{Re}\,liefTime = t_0 + Level_2(\text{u}) + Black_2(b) + Peak_2(a) \quad (5a)$$

或者

$$\text{Re}\,liefTime = t_0 + Level_2(\text{u}) + Black_2(b) + AttackTime_2(t) \quad (5b)$$

或者

$$\text{Re}\,liefTime = t_0 + Level_2(\text{u}) + Black_2(b) \tag{5c}$$

或者

$$\text{Re}\,liefTime = t_0 + Level_2(\text{u}) + AttackTime_2(t) \tag{5d}$$

在一個具體實施例中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

其中，使用者等級可以是根據使用者日常平均訪問流量的高低進行劃分的，使用者等級越高，該使用者的日常平均訪問流量越高，而日常平均訪問流量越高，表示該使用者的業務越繁忙，因此該使用者也就需要更短的黑洞路由解除時間。因此，可以將使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 配置為使用者等級的減函數。

在一個具體例子中，使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 可以配置為：

$$level_2(u) = t_1 - r_1 u \tag{6}$$

或者

$$level_2(u) = r_2 t_1 - r_1 u \qquad (6')$$

或者

$$Level_2(u) = \begin{cases} 0, u = 1 \\ -0.2, u = 2 \\ -0.5, u = 3 \\ -1, u = 4 \end{cases} \qquad (6'')$$

上述公式（6）、（6’）和（6’’）中，u 為目標 IP 位址所屬的使用者的使用者等級，在上述公式（6）、（6’）和（6’’）中，使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 為使用者等級的減函數。

其中，目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數越多，表明該 IP 位址受到攻擊的危險性越大，因此，特定時間段內該 IP 位址的訪問流量被轉發到黑洞路由的次數越多，該 IP 位址對應的黑洞路由解除時間應越長，因此，黑洞路由解除時間可以為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數，則可以將特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數 $Black_2(b)$ 配置為該特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數。

在一個具體例子中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的

次數對應的黑洞路由解除時間函數 $Black_2(b)$ 可以配置為：

$$Black_2(b) = r_3 b \qquad (7)$$

或者

$$Black_2(b) = r_3 b + t_2 \qquad (7')$$

或者

$$Black_2(b) = \begin{cases} -0.5, b = 0 \\ 0, b = 1 \\ 0.5,1 < b < 5 \\ 1,5 \le b < 10 \\ 1.5, b \ge 10 \end{cases} \qquad (7'')$$

上述公式（7）、（7'）和（7''）中，b 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數。其中，特定時間段例如可以為距當前時間一周，則 b 為上周目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數。在上述公式（7）、（7'）和（7''）中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數 $Black_2(b)$ 為特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數。

其中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量越大，該使用者越常遭到攻擊（攻擊者的重點攻擊目標），因此，特定時間段內目標

IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量越大，該 IP 位址對應的黑洞路由解除時間應越長，因此，黑洞路由解除時間可以為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數，則可以將特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 配置為該特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數。

在一個具體例子中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 可以配置為：

$$Peak_2(a) = r_4 a \qquad (8)$$

或者

$$Peak_2(a) = r_4 a + t_3 \qquad (8')$$

或者

$$Peak_2(a) = \begin{cases} 0, & a < 5 \\ 0.2,5 \le a < 10 \\ 0.5,10 \le a < 20 \\ 1,20 \le a < 50 \\ 2, & a \ge 50 \end{cases} \qquad (8'')$$

上述公式（8）、（8'）和（8''）中，a 是特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量，單位為 Gbps，例如，a 可以為上周目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量；在上述公式（8）、（8'）和（8''）中，特定時間段內目標 IP 位

址所屬的使用者擁有的 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 是特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數。

特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長越長，該 IP 位址對應的黑洞路由解除時間也應越長，因此，黑洞路由解除時間可以為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數，則可以將特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 配置為特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

在一個具體例子中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 可以配置為：

$$AttackTime_1(t) = t_4 + t \qquad (9)$$

或者

$$AttackTime_1(t) = r_5 t_4 + t \qquad (9')$$

或者

$$AttackTime_2(t) = \begin{cases} 0, t < 3 \\ 0.2,3 \le t < 10 \\ 0.5,10 \le t < 30 \\ 1, t \ge 30 \end{cases} \qquad (9'')$$

上述公式（9）、（9’）和（9’’）中，t 為歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長，單位為小時，例如，t 可以為上周該使用者擁有的 IP 位址被攻擊的總時長。在上述公式（9）、（9’）和（9’’）中，特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 是特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

上述公式（6）、（6’）、（7）、（7’）、（8）、（8’）、（9）、（9’）中的參數 t_1、t_2、t_3、t_4 和 r_1、r_2、r_3、r_4、r_5 可以根據對歷史統計資訊中的相關資料進行分析獲得。上述公式（6’’）、（7’’）、（8’’）、（9’’）為預先對歷史統計資訊中的相關資料的進行分析後而配置的。

根據上述預先配置的目標 IP 位址所屬的使用者的使用者等級對應的黑洞路由解除時間函數、歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數、特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數、所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數中的任意一項或多項，可以確定該 IP 位址所對應的黑洞路由解除時間。其中，該 IP 位址對應的黑洞路由解除時間為上述任意一項

或多項與預設黑洞路由解除時間的和。

下面舉一個獲取目標 IP 位址對應的黑洞路由解除時間的例子：

例如，預設黑洞路由解除時間 t_0 為 2.5 小時；獲取到目標 IP 位址所屬的使用者等級為白銀使用者，即 u=2；上周該使用者擁有的 IP 位址被轉發到黑洞路由的次數為 6 次，即 b=6；上周該使用者擁有的 IP 位址被攻擊的峰值流量為 8Gbps，即 a=8；上周該使用者擁有的 IP 位址被攻擊總時長為 19 小時，即 t=19；

根據公式（6''）、（7''）、（8''）、（9''）可以得到該使用者各項黑洞路由解除時間函數對應的數值分別為 $Level_1(u)$ =-0.2，$Black_1(b)$ =1，$Peak_2(a)$ =0.2，$AttackTime_1(t)$ =0.5，再根據公式（5）可以得到，該目標 IP 位址對應的黑洞路由解除時間為 4 小時。

根據本發明的另一個實施例，可以為使用者擁有的 IP 位址分別設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為該目標 IP 位址設置的黑洞路由解除時間。也就是說，屬於同一個使用者的目標 IP 位址對應的黑洞路由解除時間不一定相同。

其中，獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟可以包括：根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

更具體而言，根據所述目標 IP 位址所屬的使用者的

狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間的一種具體實施方式為：

獲取預先配置的黑洞路由解除時間確定規則；根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

具體地，可以根據所述目標 IP 位址所屬的使用者的使用者等級、歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數、所述特定時間段內所述目標 IP 位址被攻擊的峰值流量、所述特定時間段內所述目標 IP 位址被攻擊的總時長中的任意一項或多項，並結合預先配置的黑洞路由解除時間確定規則，確定該 IP 位址所對應的黑洞路由解除時間。其中，預先配置的黑洞路由解除時間確定規則可以是根據大量歷史統計資訊中的相關資料進行分析而配置的。

例如，作為黑洞路由解除時間確定規則的一個例子的黑洞路由解除時間公式可以配置為前述實施例中的公式（5）。

需說明的是，在本實施例中公式（5）中的各個黑洞路由解除時間函數的含義與前述實施例中不同。其中，$ReliefTime$ 為黑洞路由解除時間，單位為小時，t_0 為預設黑洞解除時間，較佳地，t_0=2.5 小時；$Level_2(u)$ 為目標 IP 位址所屬的使用者的使用者等級對應的黑洞路由解除時間函數；$Black_2(b)$ 為歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數；$Peak_2(a)$ 為歷史上特定時間段內目標 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數；$AttackTime_2(t)$ 為歷史上特定時間段內目標 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數。上述各狀態資訊或歷史訪問資訊對應的黑洞路由解除時間函數的值的單位均為小時。

需要說明的是，上述公式（5）僅為本發明獲取預先配置的黑洞路由解除時間確定規則的一種實施方式，黑洞路由解除時間可以為預設黑洞路由解除時間 t_0 與上述任意一項或多項黑洞路由解除時間函數之和。

例如，公式（5）還可以為前述實施例中的公式中的（5a）、（5b）、（5c）或（5d）。

在一個具體實施例中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所

述特定時間段內目標 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的增函數。

其中，可以將目標 IP 位址所屬的使用者的使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 配置為使用者等級的減函數。

在一個具體例子中，目標 IP 位址所屬的使用者的使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 可以配置為前述實施例中的公式（6）、（6'）或（6''）。在本實施例中，u 為目標 IP 位址所屬的使用者的使用者等級。在公式（6）、（6'）和（6''）中，目標 IP 位址所屬的使用者等級對應的黑洞路由解除時間函數 $Level_2(u)$ 為使用者等級的減函數。

其中，可以將特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數 $Black_2(b)$ 配置為該特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數。

在一個具體例子中，特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數 $Black_2(b)$ 可以配置為前述實施例中的公式（7）、（7'）或（7''）。在本實施例中，b 為歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數。其中，特定時間段例如可以為距當前時間一周，則 b 為上周該標 IP 位址的訪問流量被轉發到黑洞路由的次數。在公

式（7）、（7’）和（7’’）中，特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數 $Black_2(b)$ 為特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數。

其中，可以將特定時間段內目標 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 配置為該特定時間段內目標 IP 位址被攻擊的峰值流量的增函數。

在一個具體例子中，特定時間段內目標 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 可以配置為前述實施例中的公式（8）、（8’）或（8’’）。在本實施例中，a 是特定時間段內目標 IP 位址被攻擊的峰值流量，單位為 Gbps，例如，a 可以為上周目標 IP 位址被攻擊的峰值流量。在公式（8）、（8’）和（8’’）中，特定時間段內目標 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數 $Peak_2(a)$ 是特定時間段內目標 IP 位址被攻擊的峰值流量的增函數。

其中，可以將特定時間段內目標 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 配置為特定時間段內目標 IP 位址被攻擊的總時長的增函數。

在一個具體例子中，特定時間段內目標 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 可以配置為前述實施例中的公式（9）、（9’）或（9’’）。在本實施例中，t 為歷史上特定時間段內目標 IP 位址被攻擊的總時長，單位為小時，例如，t 可以為上周

該目標 IP 位址被攻擊的總時長。在公式（9）、（9'）和（9''）中，特定時間段內目標 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數 $AttackTime_2(t)$ 是特定時間段內目標 IP 位址被攻擊的總時長的增函數。

根據上述預先配置的目標 IP 位址所屬的使用者的使用者等級對應的黑洞路由解除時間函數、歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數對應的黑洞路由解除時間函數、特定時間段內目標 IP 位址被攻擊的峰值流量對應的黑洞路由解除時間函數、所述特定時間段內目標 IP 位址被攻擊的總時長對應的黑洞路由解除時間函數中的任意一項或多項，可以確定該 IP 位址所對應的黑洞路由解除時間。其中，該 IP 位址對應的黑洞路由解除時間為上述任意一項或多項與預設黑洞路由解除時間的和。

在步驟 150 中，判斷將所述目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到所述黑洞路由解除時間。

具體地，判斷將該目標 IP 位址的訪問流量轉發到黑洞路由的持續時間是否達到了該 IP 位址對應的黑洞路由解除時間。如果判斷出將該 IP 位址轉發到黑洞路由的時間達到所述黑洞路由解除時間，則執行步驟 160。

在步驟 160 中，如果判斷出所述轉發到黑洞路由的時間達到所述黑洞路由解除時間，停止為所述目標 IP 位址配置黑洞路由。

具體地，停止為該 IP 位址配置黑洞路由可以將為該

IP 位址配置的黑洞路由刪除，從而將該 IP 位址的訪問流量轉到正常的路由，即恢復該 IP 位址的正常路由。

本發明實施例提供的技術方案，透過獲取目標 IP 位址對應的流量閾值，判斷該目標 IP 位址的即時訪問流量是否超過對應的流量閾值，並根據判斷結果對該 IP 位址的訪問流量進行處理，從而根據該 IP 位址訪問流量是否超過對應的流量閾值，確定是否將該 IP 位址的訪問流量轉發到黑洞路由。並且，本發明為使用者設置流量閾值，或者為使用者的 IP 位址分別設置流量閾值，實現了根據不同的目標 IP 位址或不同的使用者的目標 IP 位址對應的訪問流量轉發到黑洞路由的流量閾值，對其訪問流量進行處理，從而，降低使用黑洞路由防禦網路攻擊的負面效果。本發明還針對訪問流量被轉發到黑洞路由的目標 IP 位址，透過獲取該 IP 位址對應的黑洞路由解除時間，從而，根據該對應的黑洞路由解除時間解除該 IP 位址的黑洞路由。並且，本發明為使用者設置黑洞路由解除時間，或者為使用者的 IP 位址分別設置黑洞路由解除時間，從而，實現了合理配置不同使用者或不同 IP 位址的黑洞路由解除時間。

基於與方法同樣的發明構思，本發明還提供一種網站攻擊防禦裝置，圖 4 所示為網站攻擊防禦裝置 4 示意圖。該網站攻擊防禦裝置 4 包括：

第一獲取模組 410，用於獲取目標 IP 位址所對應的流量閾值；

第一判斷模組 420，用於判斷所述目標 IP 位址的即時訪問流量是否超過所述流量閾值；

第一處理模組 430，用於根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

其中，所述第一處理模組 430 被配置為：

如果所述目標 IP 位址的訪問流量超過所述流量閾值，則為所述目標 IP 位址配置黑洞路由，從而將所述目標 IP 位址的訪問流量轉發到黑洞路由。

其中，參考圖 5，該網站攻擊防禦裝置還包括：

第二獲取模組 440，用於獲取所述目標 IP 位址所對應的黑洞路由解除時間；

第二判斷模組 450，用於判斷將所述目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到所述黑洞路由解除時間；

第二處理模組 460，用於如果判斷出所述轉發到黑洞路由的時間達到所述黑洞路由解除時間，停止為所述目標 IP 位址配置黑洞路由。

根據本發明的一個實施例，其中，所述第一獲取模組 410 被配置為：為使用者設置流量閾值，其中目標 IP 位址所對應的流量閾值是目標 IP 位址所屬的使用者的流量閾值。

其中，所述第一獲取模組 410 被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問

資訊獲取所述目標 IP 位址所對應的流量閾值。

其中，所述第一獲取模組 410 進一步包括：

第一獲取子模組，用於獲取預先配置的流量閾值確定規則；

第一確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

根據本發明的另一個實施例，所述第一獲取模組 410 被配置為：為使用者的 IP 位址分別設置流量閾值，其中目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的

流量閾值。

其中，所述第一獲取模組 410 被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

其中，所述第一獲取模組 410 進一步包括：

第一獲取子模組，用於獲取預先配置的流量閾值確定規則；

第一確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的減函數。

根據本發明的一個實施例，其中，所述第二獲取模組 440 被配置為：為使用者設置黑洞路由解除時間，所述目

標 IP 位址所對應的黑洞路由解除時間是為所述目標 IP 位址所屬的使用者設置的黑洞路由解除時間。

其中，所述第二獲取模組 440 被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

其中，所述第二獲取模組 440 進一步包括：

第二獲取子模組，用於獲取預先配置的黑洞路由解除時間確定規則；

第二確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

根據本發明的另一個實施例，所述第二獲取模組 440 被配置為：為使用者擁有的 IP 位址分別設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為該目標 IP 位址設置的黑洞路由解除時間。

其中，所述第二獲取模組 440 被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

其中，所述第二獲取模組 440 進一步包括：

第二獲取子模組，用於獲取預先配置的黑洞路由解除時間確定規則；

第二確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

其中，所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目

標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的增函數。

由於本實施例的裝置所實現的功能基本相應於前述圖 1 至圖 3 所示的方法實施例，故本實施例的描述中未詳盡之處，可以參見前述實施例中的相關說明，在此不做贅述。

需要注意的是，本發明可在軟體和/或軟體與硬體的組合體中被實施，例如，本發明的各個裝置可採用專用積體電路（ASIC）或任何其他類似硬體設備來實現。在一個實施例中，本發明的軟體程式可以透過處理器執行以實現上文所述步驟或功能。同樣地，本發明的軟體程式（包括相關的資料結構）可以被儲存到電腦可讀記錄媒體中，例如，RAM 記憶體，磁或光驅動器或軟碟及類似設備。另外，本發明的一些步驟或功能可採用硬體來實現，例

如，作為與處理器配合從而執行各個步驟或功能的電路。

對於本領域技術人員而言，顯然本發明不限於上述示範性實施例的細節，而且在不背離本發明的精神或基本特徵的情況下，能夠以其他的具體形式實現本發明。因此，無論從哪一點來看，均應將實施例看作是示範性的，而且是非限制性的，本發明的範圍由所附申請專利範圍而不是上述說明限定，因此旨在將落在申請專利範圍的等同要件的含義和範圍內的所有變化涵括在本發明內。不應將申請專利範圍中的任何元件符號視為限制所涉及的申請專利範圍。此外，顯然“包括”一詞不排除其他單元或步驟，單數不排除複數。系統申請專利範圍中陳述的多個單元或裝置也可以由一個單元或裝置透過軟體或者硬體來實現。第一，第二等詞語用來表示名稱，而並不表示任何特定的順序。

雖然前面特別示出並且描述了示例性實施例，但是本領域具有通常知識者將會理解的是，在不背離申請專利範圍書的精神和範圍的情況下，在其形式和細節方面可以有所變化。這裡所尋求的保護在所附申請專利範圍中做了闡述。在下列編號條款中規定了各個實施例的這些和其他方面：

1、一種網站攻擊防禦方法，其中，該網站攻擊防禦方法包括以下步驟：

獲取目標 IP 位址所對應的流量閾值；

判斷所述目標 IP 位址的即時訪問流量是否超過所述

流量閾值；

根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

2、條款 1 的網站攻擊防禦方法，其中，所述根據判斷結果，對所述目標 IP 位址的訪問流量進行處理的步驟包括：

如果所述目標 IP 位址的訪問流量超過所述流量閾值，則為所述目標 IP 位址配置黑洞路由，從而將所述目標 IP 位址的訪問流量轉發到黑洞路由。

3、條款 2 的網站攻擊防禦方法，其中，還包括：

獲取所述目標 IP 位址所對應的黑洞路由解除時間；

判斷將所述目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到所述黑洞路由解除時間；

如果判斷出所述轉發到黑洞路由的時間達到所述黑洞路由解除時間，停止為所述目標 IP 位址配置黑洞路由。

4、條款 1 的網站攻擊防禦方法，其中，為使用者設置流量閾值，其中目標 IP 位址所對應的流量閾值是目標 IP 位址所屬的使用者的流量閾值。

5、條款 1 的網站攻擊防禦方法，其中，為使用者的 IP 位址分別設置流量閾值，其中目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的流量閾值。

6、條款 4 的網站攻擊防禦方法，其中，所述獲取目標 IP 位址所對應的流量閾值的步驟包括：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或

所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

7、條款 5 的網站攻擊防禦方法，其中，所述獲取目標 IP 位址所對應的流量閾值的步驟包括：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

8、條款 6 的網站攻擊防禦方法，其中，所述根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值的步驟進一步包括：

獲取預先配置的流量閾值確定規則；

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

9、條款 8 的網站攻擊防禦方法，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

10、條款 9 的網站攻擊防禦方法，其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

11、條款 7 的網站攻擊防禦方法，其中，所述根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值的步驟進一步包括：

獲取預先配置的流量閾值確定規則；

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

12、條款 11 的網站攻擊防禦方法，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

13、條款 12 的網站攻擊防禦方法，其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級

的增函數、和/或歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的減函數。

14、條款 3 的網站攻擊防禦方法，其中，為使用者設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為所述目標 IP 位址所屬的使用者設置的黑洞路由解除時間。

15、條款 3 的網站攻擊防禦方法，其中，為使用者擁有的 IP 位址分別設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為該目標 IP 位址設置的黑洞路由解除時間。

16、條款 14 的網站攻擊防禦方法，其中，所述獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟包括：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

17、條款 15 的網站攻擊防禦方法，其中，所述獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟包括：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

18、條款 16 的網站攻擊防禦方法，其中，所述根據

所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟進一步包括：

獲取預先配置的黑洞路由解除時間確定規則；

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

19、條款 18 的網站攻擊防禦方法，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

20、條款 19 的網站攻擊防禦方法，其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址

所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

21、條款 17 的網站攻擊防禦方法，其中，所述根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間的步驟進一步包括：

獲取預先配置的黑洞路由解除時間確定規則；

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

22、條款 21 的網站攻擊防禦方法，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

23、條款 22 的網站攻擊防禦方法，其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所

述特定時間段內目標 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的增函數。

24、一種網站攻擊防禦裝置，其中，該網站攻擊防禦裝置包括：

第一獲取模組，用於獲取目標 IP 位址所對應的流量閾值；

第一判斷模組，用於判斷所述目標 IP 位址的即時訪問流量是否超過所述流量閾值；

第一處理模組，用於根據判斷結果，對所述目標 IP 位址的訪問流量進行處理。

25、條款 24 的網站攻擊防禦裝置，其中，所述第一處理模組被配置為：

如果所述目標 IP 位址的訪問流量超過所述流量閾值，則為所述目標 IP 位址配置黑洞路由，從而將所述目標 IP 位址的訪問流量轉發到黑洞路由。

26、條款 25 的網站攻擊防禦裝置，其中，還包括：

第二獲取模組，用於獲取所述目標 IP 位址所對應的黑洞路由解除時間；

第二判斷模組，用於判斷將所述目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到所述黑洞路由解除時間；

第二處理模組，用於如果判斷出所述轉發到黑洞路由的時間達到所述黑洞路由解除時間，停止為所述目標 IP

位址配置黑洞路由。

27、條款 24 的網站攻擊防禦裝置，其中，所述第一獲取模組被配置為：為使用者設置流量閾值，其中目標 IP 位址所對應的流量閾值是目標 IP 位址所屬的使用者的流量閾值。

28、條款 24 的網站攻擊防禦裝置，其中，所述第一獲取模組被配置為：為使用者的 IP 位址分別設置流量閾值，其中目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的流量閾值。

29、條款 27 的網站攻擊防禦裝置，其中，所述第一獲取模組被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

30、條款 28 的網站攻擊防禦裝置，其中，所述第一獲取模組被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的流量閾值。

31、條款 29 的網站攻擊防禦裝置，其中，所述第一獲取模組進一步包括：

第一獲取子模組，用於獲取預先配置的流量閾值確定規則；

第一確定子模組，用於根據所述目標 IP 位址所屬的

使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

32、條款 31 的網站攻擊防禦裝置，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

33、條款 32 的網站攻擊防禦裝置，其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的減函數。

34、條款 30 的網站攻擊防禦裝置，其中，所述第一獲取模組進一步包括：

第一獲取子模組，用於獲取預先配置的流量閾值確定規則；

第一確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資

訊，結合所述流量閾值確定規則，確定所述目標 IP 位址所對應的流量閾值。

35、條款 34 的網站攻擊防禦裝置，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

36、條款 35 的網站攻擊防禦裝置，其中，所述流量閾值確定規則包括：

流量閾值是目標 IP 位址所屬的使用者的使用者等級的增函數、和/或歷史上特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的減函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的減函數。

37、條款 26 的網站攻擊防禦裝置，其中，所述第二獲取模組被配置為：為使用者設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為所述目標 IP 位址所屬的使用者設置的黑洞路由解除時間。

38、條款 26 的網站攻擊防禦裝置，其中，所述第二獲取模組被配置為：為使用者擁有的 IP 位址分別設置黑洞路由解除時間，所述目標 IP 位址所對應的黑洞路由解除時間是為該目標 IP 位址設置的黑洞路由解除時間。

39、條款 37 的網站攻擊防禦裝置，其中，所述第二獲取模組被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

40、條款 38 的網站攻擊防禦裝置，其中，所述第二獲取模組被配置為：

根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊獲取所述目標 IP 位址所對應的黑洞路由解除時間。

41、條款 39 的網站攻擊防禦裝置，其中，所述第二獲取模組進一步包括：

第二獲取子模組，用於獲取預先配置的黑洞路由解除時間確定規則；

第二確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

42、條款 39 的網站攻擊防禦裝置，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址

被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長。

43、條款 42 的網站攻擊防禦裝置，其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址所屬的使用者擁有的 IP 位址被攻擊的總時長的增函數。

44、條款 40 的網站攻擊防禦裝置，其中，所述第二獲取模組進一步包括：

第二獲取子模組，用於獲取預先配置的黑洞路由解除時間確定規則；

第二確定子模組，用於根據所述目標 IP 位址所屬的使用者的狀態資訊和/或所述目標 IP 位址的歷史訪問資訊，結合所述黑洞路由解除時間確定規則，確定所述目標 IP 位址所對應的黑洞路由解除時間。

45、條款 44 的網站攻擊防禦裝置，其中，

所述目標 IP 位址所屬的使用者的狀態資訊包括所述目標 IP 位址所屬的使用者的使用者等級，所述目標 IP 位址的歷史訪問資訊包括歷史上特定時間段內所述目標 IP 位址的訪問流量被轉發到黑洞路由的次數、和/或所述特

定時間段內所述目標 IP 位址被攻擊的峰值流量、和/或所述特定時間段內所述目標 IP 位址被攻擊的總時長。

46、條款 45 的網站攻擊防禦裝置，其中，黑洞路由解除時間確定規則為：

黑洞路由解除時間是目標 IP 位址所屬的使用者的使用者等級的減函數、和/或所述特定時間段內目標 IP 位址的訪問流量被轉發到黑洞路由的次數的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的峰值流量的增函數、和/或所述特定時間段內目標 IP 位址被攻擊的總時長的增函數。

申請專利範圍

1. 一種網站攻擊防禦方法，其中，該網站攻擊防禦方法包括以下步驟：

獲取目標 IP 位址所對應的流量閾值；

判斷該目標 IP 位址的即時訪問流量是否超過該流量閾值；

根據判斷結果，對該目標 IP 位址的訪問流量進行處理。

2. 根據申請專利範圍第 1 項所述的網站攻擊防禦方法，其中，該根據判斷結果，對該目標 IP 位址的訪問流量進行處理的步驟包括：

如果該目標 IP 位址的訪問流量超過該流量閾值，則為該目標 IP 位址配置黑洞路由，從而將該目標 IP 位址的訪問流量轉發到黑洞路由。

3. 根據申請專利範圍第 2 項所述的網站攻擊防禦方法，其中，還包括：

獲取該目標 IP 位址所對應的黑洞路由解除時間；

判斷將該目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到該黑洞路由解除時間；

如果判斷出該轉發到黑洞路由的時間達到該黑洞路由解除時間，停止為該目標 IP 位址配置黑洞路由。

4. 根據申請專利範圍第 1 項所述的網站攻擊防禦方法，其中，為使用者設置流量閾值，其中該目標 IP 位址所對應的流量閾值是該目標 IP 位址所屬的使用者的流量

閾值。

5. 根據申請專利範圍第 1 項所述的網站攻擊防禦方法，其中，為使用者的 IP 位址分別設置流量閾值，其中該目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的流量閾值。

6. 一種網站攻擊防禦裝置，其中，該網站攻擊防禦裝置包括：

第一獲取模組，用於獲取目標 IP 位址所對應的流量閾值；

第一判斷模組，用於判斷該目標 IP 位址的即時訪問流量是否超過該流量閾值；

第一處理模組，用於根據判斷結果，對該目標 IP 位址的訪問流量進行處理。

7. 根據申請專利範圍第 6 項所述的網站攻擊防禦裝置，其中，該第一處理模組被配置為：

如果該目標 IP 位址的訪問流量超過該流量閾值，則為該目標 IP 位址配置黑洞路由，從而將該目標 IP 位址的訪問流量轉發到黑洞路由。

8. 根據申請專利範圍第 7 項所述的網站攻擊防禦裝置，其中，還包括：

第二獲取模組，用於獲取該目標 IP 位址所對應的黑洞路由解除時間；

第二判斷模組，用於判斷將該目標 IP 位址的訪問流量轉發到黑洞路由的時間是否達到該黑洞路由解除時間；

第二處理模組，用於如果判斷出該轉發到黑洞路由的時間達到該黑洞路由解除時間，停止為該目標 IP 位址配置黑洞路由。

9. 根據申請專利範圍第 6 項所述的網站攻擊防禦裝置，其中，該第一獲取模組被配置為：為使用者設置流量閾值，其中該目標 IP 位址所對應的流量閾值是該目標 IP 位址所屬的使用者的流量閾值。

10. 根據申請專利範圍第 6 項所述的網站攻擊防禦裝置，其中，該第一獲取模組被配置為：為使用者的 IP 位址分別設置流量閾值，其中該目標 IP 位址所對應的流量閾值是為該目標 IP 位址設置的流量閾值。

11. 根據申請專利範圍第 9 項所述的網站攻擊防禦裝置，其中，該第一獲取模組被配置為：

根據該目標 IP 位址所屬的使用者的狀態資訊和/或該目標 IP 位址所屬的使用者擁有的 IP 位址的歷史訪問資訊獲取該目標 IP 位址所對應的流量閾值。

12. 根據申請專利範圍第 10 項所述的網站攻擊防禦裝置，其中，該第一獲取模組被配置為：

根據該目標 IP 位址所屬的使用者的狀態資訊和/或該目標 IP 位址的歷史訪問資訊獲取該目標 IP 位址所對應的流量閾值。

圖 式

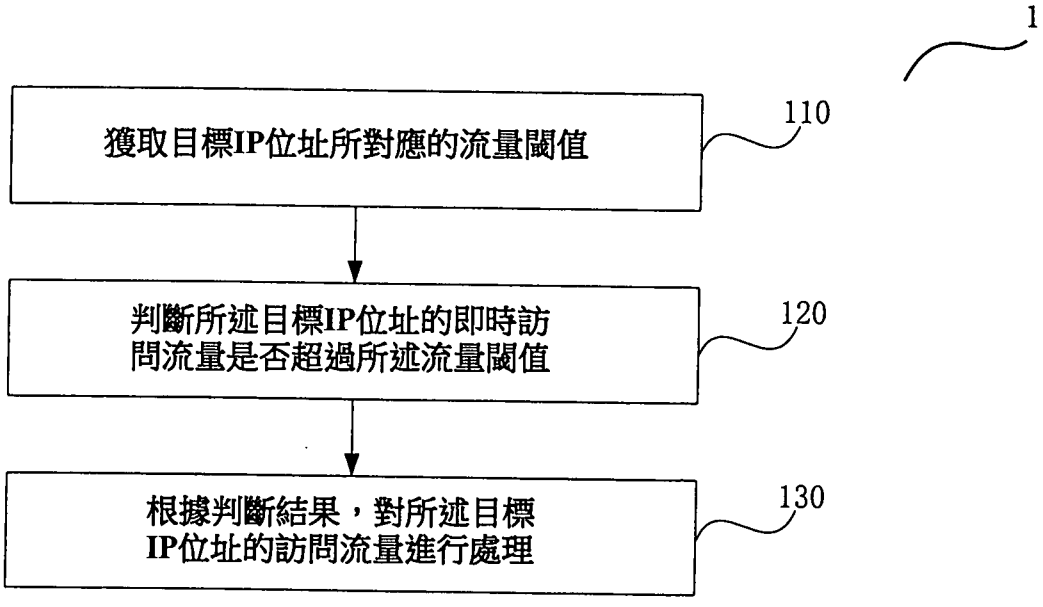
1
獲取目標IP位址所對應的流量閾值
110
判斷所述目標IP位址的即時訪問流量是否超過所述流量閾值
120
根據判斷結果，對所述目標IP位址的訪問流量進行處理
130

圖 1

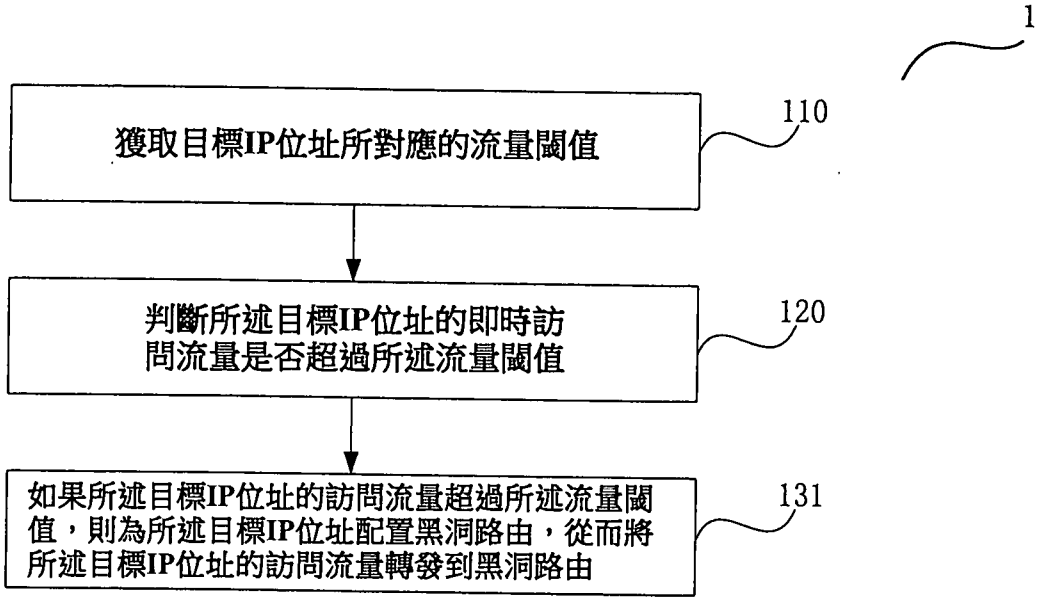
1
獲取目標IP位址所對應的流量閾值
110
判斷所述目標IP位址的即時訪問流量是否超過所述流量閾值
120
如果所述目標IP位址的訪問流量超過所述流量閾值，則為所述目標IP位址配置黑洞路由，從而將所述目標IP位址的訪問流量轉發到黑洞路由
131

圖 2

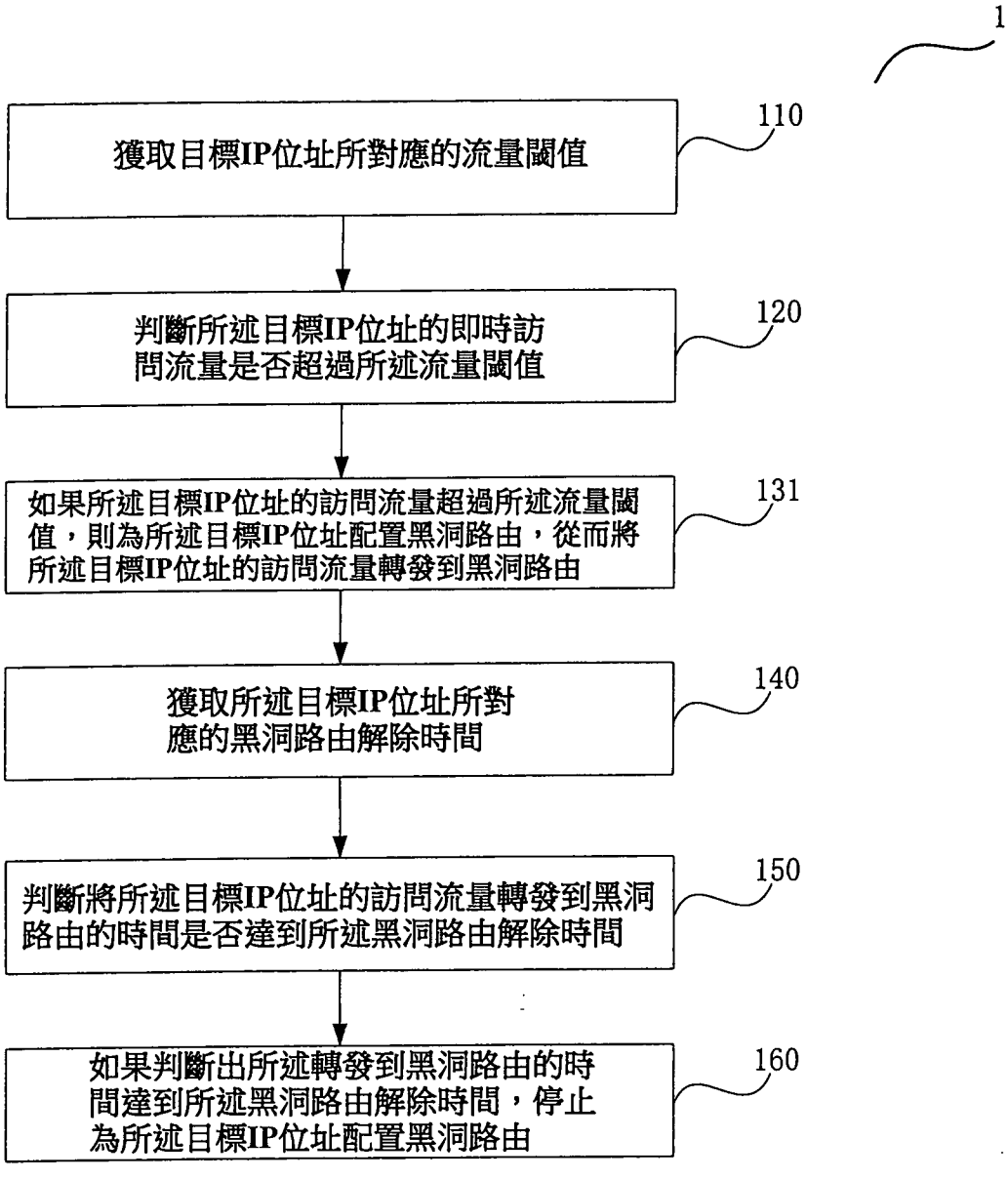
1
獲取目標IP位址所對應的流量閾值
110
判斷所述目標IP位址的即時訪問流量是否超過所述流量閾值
120
如果所述目標IP位址的訪問流量超過所述流量閾值，則為所述目標IP位址配置黑洞路由，從而將所述目標IP位址的訪問流量轉發到黑洞路由
131
獲取所述目標IP位址所對應的黑洞路由解除時間
140
判斷將所述目標IP位址的訪問流量轉發到黑洞路由的時間是否達到所述黑洞路由解除時間
150
如果判斷出所述轉發到黑洞路由的時間達到所述黑洞路由解除時間，停止為所述目標IP位址配置黑洞路由
160

圖 3

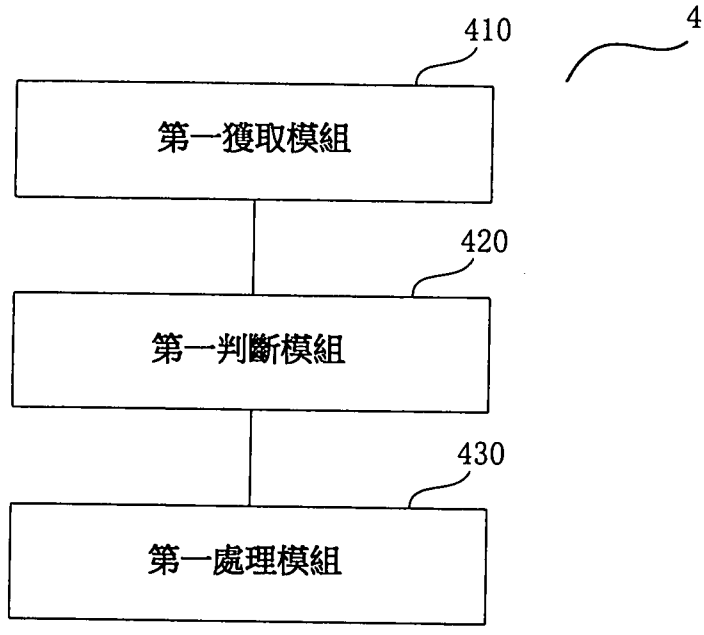

圖 4

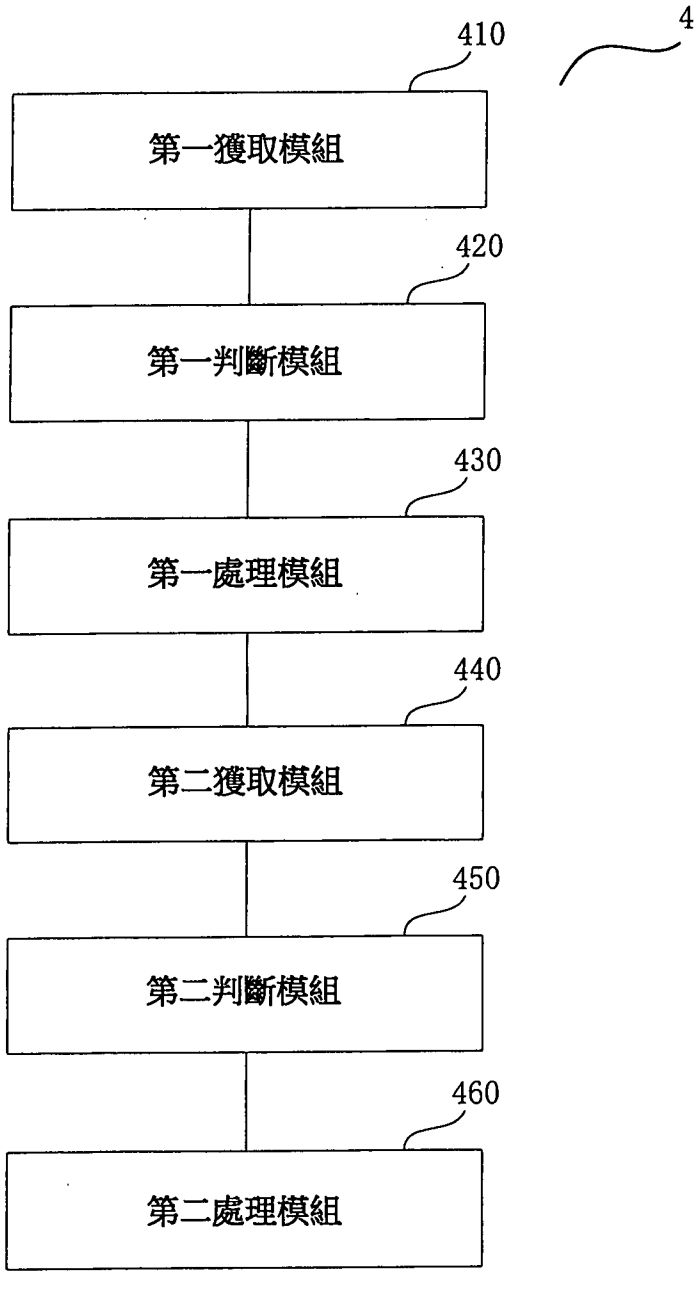
4
410
第一獲取模組
420
第一判斷模組
430
第一處理模組
440
第二獲取模組
450
第二判斷模組
460
第二處理模組

圖 5