[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/36 (2006.01)
H04L 12/56 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810142091.7

[43] 公开日 2010 年 3 月 3 日

[11] 公开号 CN 101662368A

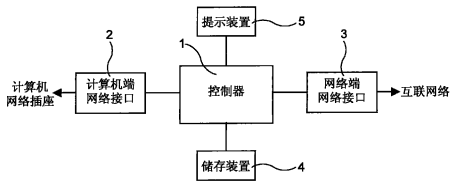
[22] 申请日 2008.8.28
[21] 申请号 200810142091.7
[71] 申请人 黄金富
地址 100032 北京市西城区金融街 27 号投资广场 B 座 19 层
[72] 发明人 黄金富
权利要求书 7 页 说明书 9 页 附图 3 页

[54] 发明名称

一种可对抗木马程式的网络数据过滤装置和相应方法

[57] 摘要

一种可对抗木马程式的网络数据过滤装置和相应方法，所述装置连接于计算机与网络之间，包括有控制器(1)、计算机端网络接口(2)、网络端网络接口(3)、储存装置(4)、提示装置(5)，储存装置(4)内储存有各可信任 IP 地址和各不信任 IP 地址，控制器(1)按预定程序运作，将计算机与网络之间传送的数据包进行过滤，拦截目的地 IP 地址和来源地 IP 地址为不信任 IP 地址的所有数据包。 本发明的网络数据过滤装置是独立于计算机以外的装置，与计算机是物理上隔离的，即使计算机感染了病毒和木马程式，也不会影响网络数据过滤装置的工作，保障用户的资料不会被木马程式盗走，特别适合一些经常连线到金融网站的计算机。



1. 一种网络数据过滤装置，连接于计算机与网络之间，主要用于过滤计算机与网络传送的数据包，其特征在于，所述的装置包括有控制器(1)、计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5），其中，控制器（1）分别与计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5）相电路连接，储存装置（4）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（1）按预定程序运作，将从计算机端网络接口（2）传送给网络端网络接口（3）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（3）传送给计算机端网络接口（2）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

2. 如权利要求 1 所述的网络数据过滤装置，其特征在于，所述的装置还包括有键盘端键盘接口（6）和计算机端键盘接口（7），其中，键盘端键盘接口（6）和计算机端键盘接口（7）相电路连接，键盘端键盘接口（6）通过连接电缆与外接的计算机键盘相连线，计算机端键盘接口（7）通过连接电缆与计算机键盘插座相连线，键盘端键盘接口（6）和计算机端键盘接口（7）主要用于将外接的计算机键盘连线到计算机键盘插座，以及，键盘端键盘接口（6）和计算机端键盘接口（7）与控制器（1）相电路连接，控制器（1）通过监察键盘端键盘接口（6）和计算机端键盘接口（7）之间所传送的按键信息，接收用户从键盘输入的操作指令信息。

3. 如权利要求 1 所述的网络数据过滤装置，其特征在于，所述的储存装置（4）内还储存有多个 IP 地址对应的网域名称资料，包括各个可信

任 IP 地址对应的网域名称资料、各个不信任 IP 地址对应的网域名称资料、其他 IP 地址对应的网域名称资料。

4. 如权利要求 1 所述的网络数据过滤装置，其特征在于，所述的装置还包括有开关掣（8），所述的开关掣（8）是网络数据过滤装置的总开关。

5. 如权利要求 1 或 2 或 3 所述的网络数据过滤装置，其特征在于，当所述的控制器（1）从计算机端网络接口（2）接收到数据包时，控制器（1）将该数据包的目的地 IP 地址与储存装置（4）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 A 组程序的其中一个程序；

程序 A1：当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同时，控制器（1）将该数据包拦截弃掉，并通过提示装置（5）发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文字信息 和/或 载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音；

程序 A2：当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同时，控制器（1）将该数据包输出到网络端网络接口（3）；

程序 A3：当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，控制器（1）通过提示装置（5）发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息 和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或 提示声音。

6. 如权利要求 5 所述的网络数据过滤装置，其特征在于，当控制器（1）发现从计算机端网络接口（2）接收到数据包的目的地 IP 地址为陌生 IP 地址时，控制器（1）通过提示装置（5）发出提示信息，然后控制器（1）监察键盘端键盘接口（6）与计算机端键盘接口（7）之间所传送的按键信息，当控制器（1）发现按键信息为操作指令信息时，根据操作指令信息时执行包括如下的 B 组程序的其中一个程序：

程序 B1：当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中；

程序 B2：当操作指令信息为确认可信任信息时，控制器（1）将该数据包输出到网络端网络接口（3），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

7. 如权利要求 6 所述的网络数据过滤装置，其特征在于，所述的 B 组程序还包括如下的程序 B3：

程序 B3：当操作指令信息为确认临时信任信息时，控制器（1）将该数据包输出到网络端网络接口（3），然后控制器（1）将所述的陌生 IP 地址设定为可信任 IP 地址储存到储存装置(4)中，并设定该可信任 IP 地址的有效时间，以及，控制器（1）在该有效时间过后从储存装置（4）中删除该可信任 IP 地址。

8. 如权利要求 1 或 2 或 3 所述的网络数据过滤装置，其特征在于，当所述的控制器（1）从网络端网络接口（3）接收到数据包时，控制器（1）将该数据包的来源地 IP 地址与储存装置（4）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 C 组程序的其中一个程序：

程序 C1：当数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，控制器（1）将该数据包拦截弃掉，并通过提示装置（5）发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文字信息 和/或 载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音；

程序 C2：当数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，控制器（1）将该数据包输出到计算机端网络接口（2）；

程序 C3：当数据包的来源地 IP 地址与任何一个可信任 IP 地址不相同，并且该来源地 IP 地址与任何一个不信任 IP 地址也不相同时，该来源地 IP 地址为陌生 IP 地址，控制器（1）通过提示装置（5）发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息 和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或 提示声音。

9. 如权利要求 8 所述的网络数据过滤装置，其特征在于，当控制器（1）发现从网络端网络接口（3）接收到数据包的来源地 IP 地址为陌生 IP 地址时，控制器（1）通过提示装置（5）发出提示信息，然后控制器（1）监察键盘端键盘接口（6）与计算机端键盘接口（7）之间所传送的按键信息，当控制器（1）发现按键信息为操作指令信息时，根据操作指令信息时执行包括如下的 D 组程序的其中一个程序：

程序 D1：当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中；

程序 D2：当操作指令信息为确认可信任信息时，控制器（1）将该数据包输出到计算机端网络接口（2），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

10. 如权利要求 9 所述的网络数据过滤装置，其特征在于，所述的 D 组程序还包括如下的程序 D3:

程序 D3: 当操作指令信息为确认临时信任信息时，控制器（1）将该数据包输出到计算机端网络接口（2），然后控制器（1）将所述的陌生 IP 地址设定为可信任 IP 地址储存到储存装置（4）中，并设定该可信任 IP 地址的有效时间，以及，控制器（1）在该有效时间过后从储存装置（4）中删除该可信任 IP 地址。

11. 一种网络数据过滤方法，采用如权利要求 1 至 10 任一项所述的网络数据过滤装置，用于过滤通过网络传送的数据包，其特征在于，所述的方法包括预先将各个可信任 IP 地址和各个不信任 IP 地址分别储存于网络数据过滤装置内，并对流过网络数据过滤装置的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

12. 如权利要求 11 所述的网络数据过滤方法，其特征在于，所述的方法对流过网络数据过滤装置的数据包进行过滤时，将数据包的目的地 IP 地址与网络数据过滤装置所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对 和/或 将数据包的来源地 IP 地址与网络数据过滤装置所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，并根据核对结果执行以下的 E 组步骤的其中一个步骤:

步骤 E1: 当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同或或数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，网络数据过滤装置将该数据包拦截弃掉，并发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文字信息 和/或

载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音;

步骤 E2: 当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同，并且数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，让该数据包流过网络数据过滤装置;

步骤 E3: 当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，网络数据过滤装置发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或提示声音;

或，

当数据包的来源地 IP 地址与任何一个可信任 IP 地址不相同，并且该来源地 IP 地址与任何一个不信任 IP 地址也不相同时，该来源地 IP 地址为陌生 IP 地址，网络数据过滤装置发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或提示声音。

13. 如权利要求 12 所述的网络数据过滤方法，其特征在于，当网络数据过滤装置发现 流过的数据包的目的地 IP 地址是陌生 IP 地址 或流过的数据包的来源地 IP 地址是陌生 IP 地址 时，网络数据过滤装置发出提示信息，然后网络数据过滤装置等候用户输入操作指令信息，并根据操作指令信息执行如下的 F 组步骤的其中一个步骤:

步骤 F1：当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中；

步骤 F2：当操作指令信息为确认可信任信息时，让该数据包流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

14. 如权利要求 13 所述的网络数据过滤方法，其特征在于，所述的 F 组步骤还包括如下的步骤 F3:

步骤 F3：当操作指令信息为确认临时信任信息时，让该数据包流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中，并设定该可信任 IP 地址的有效时间，以及，网络数据过滤装置在该有效时间过后从网络数据过滤装置中删除该可信任 IP 地址。

一种可对抗木马程式的网络数据过滤装置和相应方法

【技术领域】

本发明涉及计算机数据安全技术领域，特别是涉及一种可对抗木马程式的网络数据过滤装置和相应方法。

【背景技术】

随着时代的进步，资讯科技的应用非常普及，尤其是计算机和互联网的发展，金融机构如银行等，提供了很多利用资讯科技的服务，例如网上银行服务、网上证券买卖服务等，这些服务一般是将用户的交易信息通过互联网传送到金融机构，由金融机构核实用户的交易信息后，根据交易信息内容进行相应的操作。由于这些交易信息内包含有用户的重要资料，例如账户号码、账户口令等，只要盗取得这些资料就可以在用户不知情下操控用户的账户，盗取用户账户内的钱，所以有些黑客通过各种各样的入侵方法，将木马程式置于用户的计算机内，在用户连线到金融机构的服务器时，通过木马程式盗取用户的资料，包括账户号码、账户口令等，然后将这些资料传送到黑客指定的服务器。由于木马程式平常是隐藏于计算机内，即使被黑客利用木马程式盗取了用户的资料，用户一般是不会察觉，黑客继而使用这些资料盗取用户的账户内的钱，令用户蒙受损失，是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种可对抗木马程式的网络数据过滤装置和相应方法，使计算机连线上网与其他计算机通讯时，只能与用户信任的 IP 地址的主机进行交换信息，从而使黑客不能通过木马程式将所盗取的资料传送到非用户信任的 IP 地址。

本发明的目的是这样实现的，采用这样一种网络数据过滤装置，连接于计算机与网络之间，主要用于过滤计算机与网络传送的数据包，其特征在于，所述的装置包括有控制器（1）、计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5），其中，控制器（1）分别与计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5）相电路连接，储存装置（4）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（1）按预定程序运作，将从计算机端网络接口（2）传送给网络端网络接口（3）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（3）传送给计算机端网络接口（2）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

以及，采用这样一种网络数据过滤方法，采用如前所述的网络数据过滤装置，用于过滤通过网络传送的数据包，其特征在于，所述的方法包括预先将各个可信任 IP 地址和各个不信任 IP 地址分别储存于网络数据过滤装置内，并对流过网络数据过滤装置的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

这样就实现了本发明的目的。

采用了本发明的网络数据过滤装置的计算机，即使中了黑客的木马程式，当木马程式将所盗取的资料传送到黑客指定的 IP 地址时，网络数据过滤装置会即时发现该 IP 地址并非是用户所信任的 IP 地址，就不会让该资料传送到黑客指定的 IP 地址。

【附图说明】

图 1 是本发明的网络数据过滤装置的第一实施例的结构示意说明图；

图 2 是本发明的网络数据过滤装置的第二实施例的结构示意说明图；

图 3 是本发明的网络数据过滤装置的第三实施例的结构示意说明图;

图 4 是本发明的网络数据过滤装置的第三实施例的形像化立体示意说明图;

图 5 是本发明的网络数据过滤方法的示意说明图。

图中，相同的数字代表相同的系统、装置、部件器件，附图是示意性的，用以说明本发明的系统的构成和方法的主要步骤。

【具体实施方式】

下面结合附图，对本发明的方法作进一步详细说明。

参阅图 1，图 1 是本发明的网络数据过滤装置的第一实施例的结构示意说明图，图中示出的装置包括有控制器（1）、计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5），其中，控制器（1）分别与计算机端网络接口（2）、网络端网络接口（3）、储存装置（4）、提示装置（5）相电路连接，储存装置（4）内储存有各个可信任 IP 地址和各个不信任 IP 地址，控制器（1）按预定程序运作，将从计算机端网络接口（2）传送给网络端网络接口（3）的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 将从网络端网络接口（3）传送给计算机端网络接口（2）的数据包进行过滤，拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

参阅图 2，图 2 是本发明的网络数据过滤装置的第二实施例的结构示意说明图，与第一实施例相比，不同之处在于第二实施例增加了键盘接口，网络数据过滤装置可通过键盘接口接收用户输入的按键信息，根据按键信息对陌生 IP 地址的数据包进行相应的处理。继续参阅图 2，图中示出的装置还包括有键盘端键盘接口（6）和计算机端键盘接口（7），其中，键盘端键盘接口（6）和计算机端键盘接口（7）相电路连接，键盘端键盘接口（6）通过连接电缆与外接的计算机键盘相连线，计算机端键盘接口（7）

通过连接电缆与计算机键盘插座相连线，键盘端键盘接口（6）和计算机端键盘接口（7）主要用于将外接的计算机键盘连线到计算机键盘插座，以及，键盘端键盘接口（6）和计算机端键盘接口（7）与控制器（1）相电路连接，控制器（1）通过监察键盘端键盘接口（6）和计算机端键盘接口（7）之间所传送的按键信息，接收用户从键盘输入的操作指令信息。

在本发明中，计算机端网络接口（2）是通过网络电缆连接到计算机上的网络插座，网络端网络接口（3）是通过网络电缆连接网络，也就是网络数据过滤装置是置于计算机与网络之间，由网络数据过滤装置对流过的数据进行过滤，包括从计算机端网络接口（2）传送给网络端网络接口（3）的数据包，和从网络端网络接口（3）传送给计算机端网络接口（2）的数据包，以下将分别作进一步详细说明。此外，储存装置（4）内还储存有多个 IP 地址对应的网域名称资料，包括各个可信任 IP 地址对应的网域名称资料、各个不信任 IP 地址对应的网域名称资料、其他 IP 地址对应的网域名称资料。只要预先将各 IP 地址对应的网域名称资料储存于储存装置（4）内，当网络数据过滤装置发现并非是可信任 IP 地址的数据包时，就可立即找出该 IP 对应的网域名称显示给用户看，用户从网域名称就可知道计算机正在跟什么主机连线通讯。

以下是网络数据过滤装置工作时，将计算机传送给网络的数据包进行过滤的过程，当所述的控制器（1）从计算机端网络接口（2）接收到数据包时，控制器（1）将该数据包的目的地 IP 地址与储存装置（4）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 A 组程序的其中一个程序：

程序 A1：当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同时，控制器（1）将该数据包拦截弃掉，并通过提示装置（5）发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文

字信息 和/或 载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音;

程序 A2: 当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同时，控制器（1）将该数据包输出到网络端网络接口（3）;

程序 A3: 当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，控制器（1）通过提示装置（5）发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息 和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或 提示声音。

当控制器（1）发现从计算机端网络接口（2）接收到数据包的目的地 IP 地址为陌生 IP 地址时，控制器（1）通过提示装置（5）发出提示信息，然后控制器（1）监察键盘端键盘接口（6）与计算机端键盘接口（7）之间所传送的按键信息，当控制器（1）发现按键信息为操作指令信息时，根据操作指令信息时执行包括如下的 B 组程序的其中一个程序:

程序 B1: 当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中;

程序 B2: 当操作指令信息为确认可信任信息时，控制器（1）将该数据包输出到网络端网络接口（3），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

以及，所述的 B 组程序还包括如下的程序 B3:

程序 B3: 当操作指令信息为确认临时信任信息时，控制器（1）将该数据包输出到网络端网络接口（3），然后控制器（1）将所述的陌生 IP 地址即所述的数据包的目的地 IP 地址设定为可信任 IP 地址储存到储存装置（4）中，并设定该可信任 IP 地址

的有效时间，以及，控制器（1）在该有效时间过后从储存装置（4）中删除该可信任 IP 地址。

以下是网络数据过滤装置工作时，将计算机从网络接收回来的数据包进行过滤的过程，当所述的控制器（1）从网络端网络接口（3）接收到数据包时，控制器（1）将该数据包的来源地 IP 地址与储存装置（4）所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，然后根据核对结果执行如下的 C 组程序的其中一个程序：

程序 C1：当数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，控制器（1）将该数据包拦截弃掉，并通过提示装置（5）发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文字信息 和/或 载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音；

程序 C2：当数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，控制器（1）将该数据包输出到计算机端网络接口（2）；

程序 C3：当数据包的来源地 IP 地址与任何一个可信任 IP 地址不相同，并且该来源地 IP 地址与任何一个不信任 IP 地址也不相同时，该来源地 IP 地址为陌生 IP 地址，控制器（1）通过提示装置（5）发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息 和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或 提示声音。

当控制器（1）发现从网络端网络接口（3）接收到数据包的来源地 IP 地址为陌生 IP 地址时，控制器（1）通过提示装置（5）发出提示信息，然后控制器（1）监察键盘端键盘接口（6）与计算机端键盘接口（7）之间所传送的按键信息，当控制器（1）发现按键信息为操作指令信息时，根据操作指令信息时执行包括如下的 D 组程序的其中一个程序：

程序 D1：当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中；

程序 D2：当操作指令信息为确认可信任信息时，控制器（1）将该数据包输出到计算机端网络接口（2），然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

以及，所述的 D 组程序还包括如下的程序 D3：

程序 D3：当操作指令信息为确认临时信任信息时，控制器（1）将该数据包输出到计算机端网络接口（2），然后控制器（1）将所述的陌生 IP 地址即所述的数据包的来源地 IP 地址设定为可信任 IP 地址储存到储存装置（4）中，并设定该可信任 IP 地址的有效时间，以及，控制器（1）在该有效时间过后从储存装置（4）中删除该可信任 IP 地址。

参阅图 3 和图 4，图 3 是本发明的网络数据过滤装置的第三实施例的结构示意说明图，图 4 是本发明的网络数据过滤装置的第三实施例的形像化立体示意说明图，图 3 和图 4 示出的装置还包括有开关掣（8），所述的开关掣（8）是网络数据过滤装置的总开关。与第二实施例相比，不同之处在于第三实施例增加了开关掣（8），其余与第二实施例相同。继续参阅图 4，图中示出的提示装置（5）包括有用于显示文字信息的显示屏（501）和发声装置（502），控制器（1）可以通过显示屏（501）显示流过网络数据过滤装置的数据包的来源地/目的地 IP 地址和对应的网域名称，可方便用户了解计算机正在跟什么主机连线通讯。此外，图 4 中示出的网络数据过滤装置是采用记忆卡作为储存装置（4），可以预先将各个可信任 IP 地址及其对应的网域名称、各个不信任 IP 地址及其对应的网域名称、其他 IP 地址及其对应的网域名称等等的资料写到记忆卡，然后才将记忆卡插到网络数据过滤装置上使用。

参阅图 5，图 5 是本发明的网络数据过滤方法的示意说明图，图中示出了本发明的网络数据过滤方法的主要步骤，在本发明的网络数据过滤方法中，包括预先将各个可信任 IP 地址和各个不信任 IP 地址分别储存于网络数据过滤装置内，并对流过网络数据过滤装置的数据包进行过滤，拦截目的地 IP 地址为不信任 IP 地址的所有数据包 和/或 拦截来源地 IP 地址为不信任 IP 地址的所有数据包。

继续参阅图 5，图中示出的方法对流过网络数据过滤装置的数据包进行过滤时，将数据包的目的地 IP 地址与网络数据过滤装置所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对 和/或 将数据包的来源地 IP 地址与网络数据过滤装置所储存的各个可信任 IP 地址和各个不信任 IP 地址进行核对，并根据核对结果执行以下的 E 组步骤的其中一个步骤：

步骤 E1：当数据包的目的地 IP 地址与其中一个不信任 IP 地址相同或或数据包的来源地 IP 地址与其中一个不信任 IP 地址相同时，网络数据过滤装置将该数据包拦截弃掉，并发出告警信息，所述的告警信息包括载有该不信任 IP 地址的文字信息 和/或载有该不信任 IP 地址对应的网域名称的文字信息和/或 提示声音；

步骤 E2：当数据包的目的地 IP 地址与其中一个可信任 IP 地址相同，并且数据包的来源地 IP 地址与其中一个可信任 IP 地址相同时，让该数据包流过网络数据过滤装置；

步骤 E3：当数据包的目的地 IP 地址与任何一个可信任 IP 地址不相同，并且该目的地 IP 地址与任何一个不信任 IP 地址也不相同时，该目的地 IP 地址为陌生 IP 地址，网络数据过滤装置发出提示信息，所述的提示信息包括载有该陌生 IP 地址的文字信息和/或 载有该陌生 IP 地址对应的网域名称的文字信息和/或提示声音；

当网络数据过滤装置发现 流过的数据包的目的地 IP 地址是陌生 IP 地址 或流过的数据包的来源地 IP 地址是陌生 IP 地址 时，网络数据过滤装置发出提示信息，然后网络数据过滤装置等候用户输入操作指令信息，并根据操作指令信息执行如下的 F 组步骤的其中一个步骤:

步骤 F1: 当操作指令信息为确认不信任信息时，将该数据包拦截弃掉，使该数据包不能流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为不信任 IP 地址储存到网络数据过滤装置中;

步骤 F2: 当操作指令信息为确认可信任信息时，让该数据包流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中。

以及，所述的 F 组步骤还包括如下的步骤 F3:

步骤 F3: 当操作指令信息为确认临时信任信息时，让该数据包流过网络数据过滤装置，然后将所述的陌生 IP 地址设定为可信任 IP 地址储存到网络数据过滤装置中，并设定该可信任 IP 地址的有效时间，以及，网络数据过滤装置在该有效时间过后从网络数据过滤装置中删除该可信任 IP 地址。

以上已经详细说明了本发明的网络数据过滤装置和网络数据过滤方法，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

本发明的网络数据过滤装置是独立于计算机以外的一个装置，与计算机是物理上隔离的，即使计算机感染了病毒和木马程式，也不会影响网络数据过滤装置的工作。本发明的实施，保障了用户的资料不会被木马程式盗走，特别适合应用于一些经常连线到金融网站的计算机。

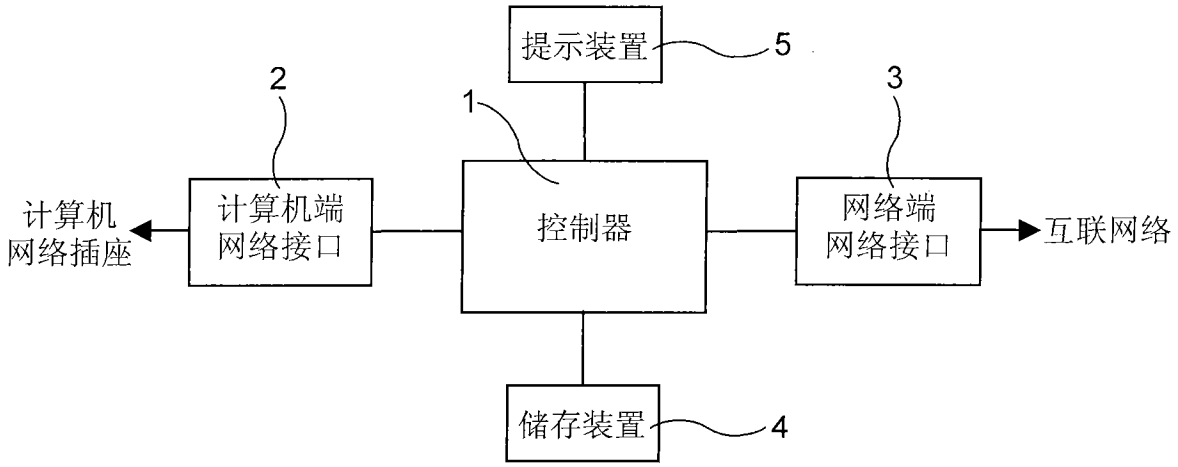

提示装置
5
2
1
3
计算机
网络插座
计算机端
网络接口
控制器
网络端
网络接口
互联网络
储存装置
4

图 1

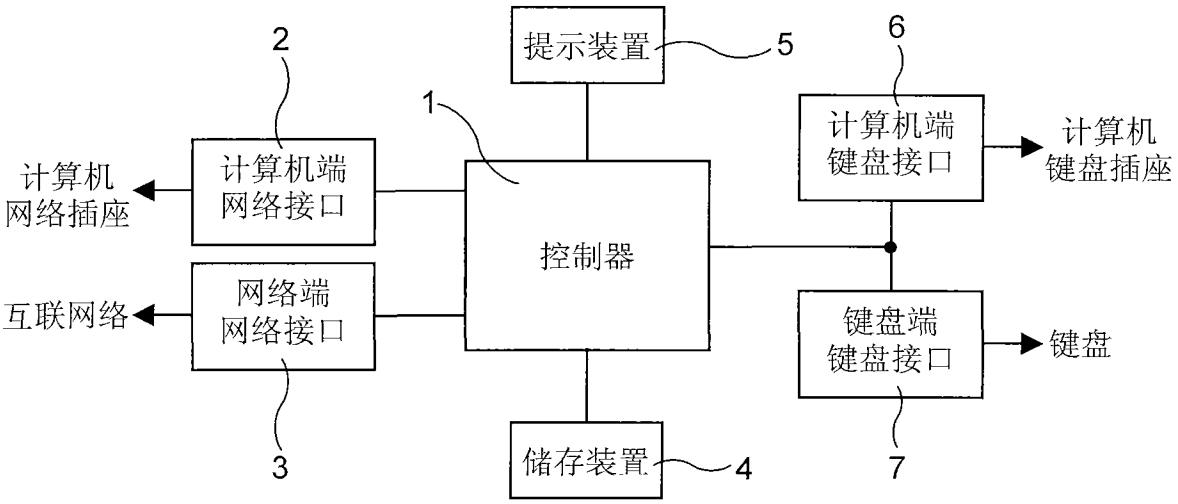

提示装置
5
6
2
1
计算机端
键盘接口
计算机
键盘插座
计算机
网络插座
计算机端
网络接口
控制器
互联网络
网络端
网络接口
键盘端
键盘接口
键盘
3
储存装置
4
7

图 2

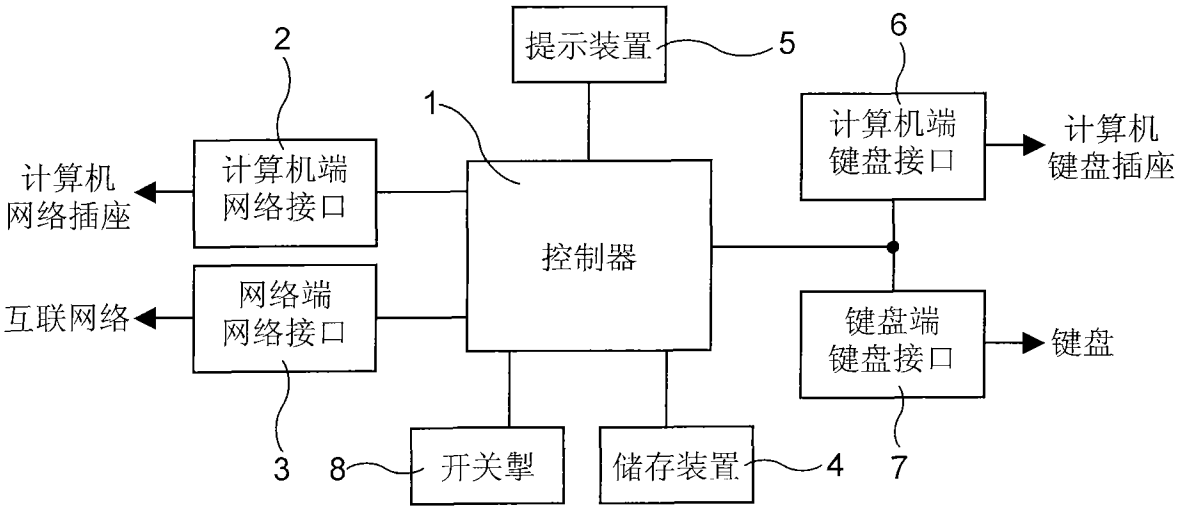

提示装置
5
6
2
1
计算机端
键盘接口
计算机
键盘插座
计算机
网络插座
计算机端
网络接口
控制器
网络端
网络接口
互联网络
键盘端
键盘接口
键盘
3
8
开关掣
储存装置
4
7

图 3

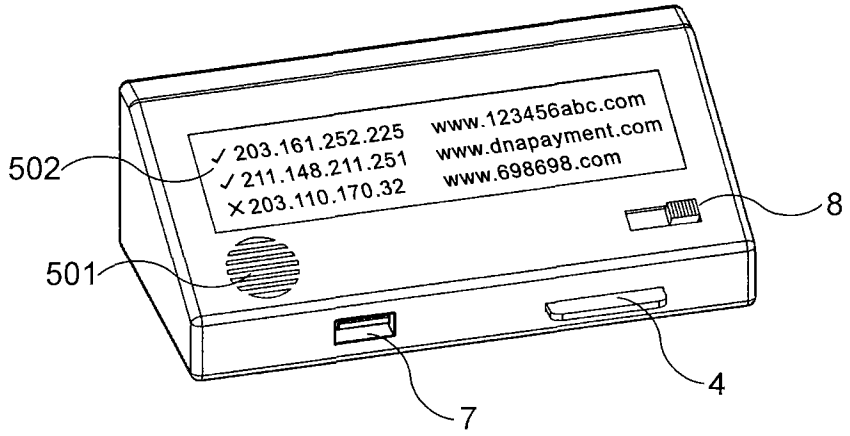

✓203.161.252.225
✓211.148.211.251
×203.110.170.32
www.123456abc.com
www.dnapayment.com
www.698698.com
502
501
8
4
7

图 4

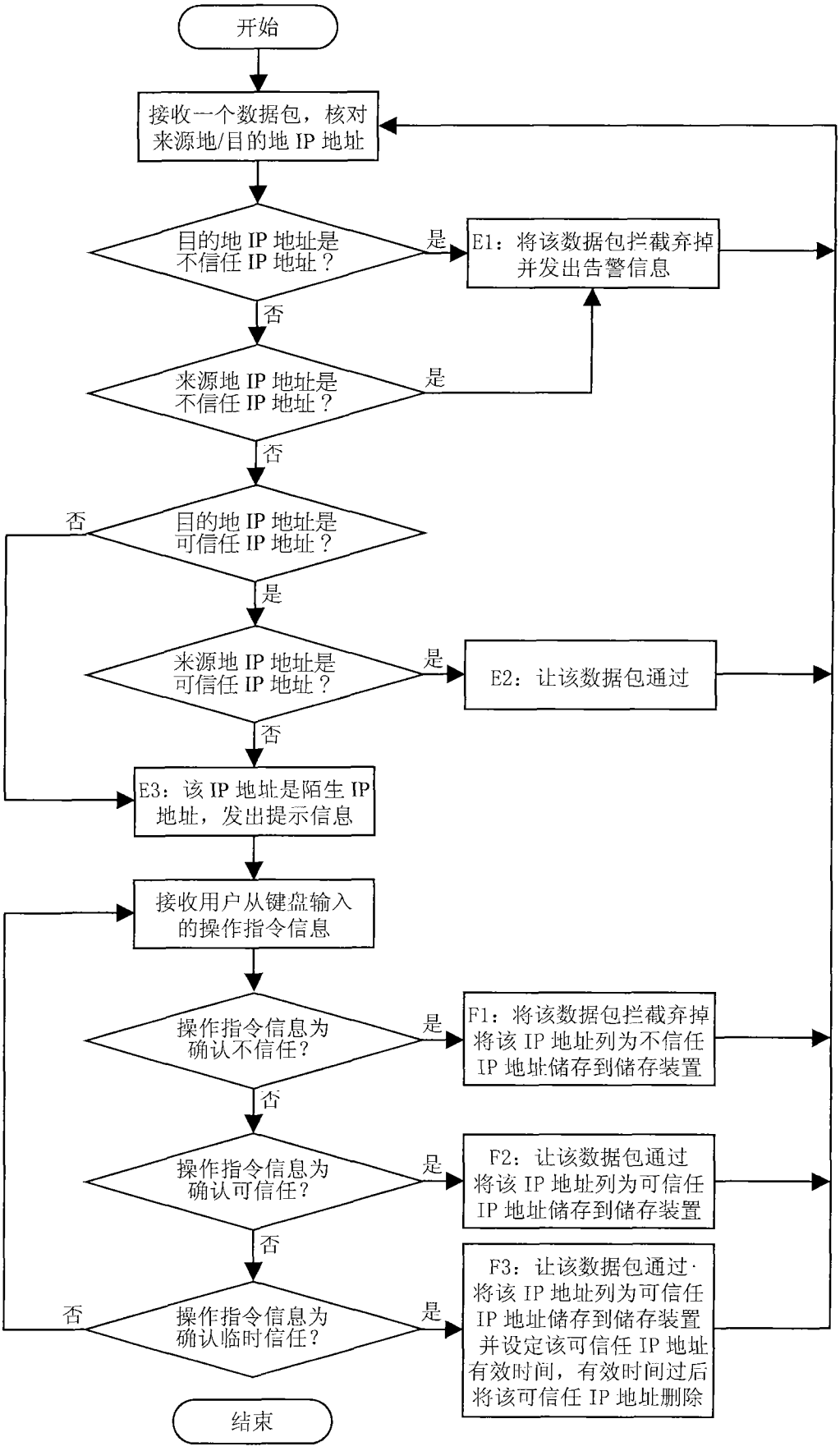

开始
接收一个数据包，核对来源地/目的地 IP 地址
目的地 IP 地址是不信任 IP 地址？
是
E1：将该数据包拦截弃掉并发出告警信息
否
来源地 IP 地址是不信任 IP 地址？
是
否
目的地 IP 地址是可信任 IP 地址？
否
是
来源地 IP 地址是可信任 IP 地址？
是
E2：让该数据包通过
否
E3：该 IP 地址是陌生 IP 地址，发出提示信息
接收用户从键盘输入的操作指令信息
操作指令信息为确认不信任？
是
F1：将该数据包拦截弃掉将该 IP 地址列为不信任 IP 地址储存到储存装置
否
操作指令信息为确认可信任？
是
F2：让该数据包通过将该 IP 地址列为可信任 IP 地址储存到储存装置
否
操作指令信息为确认临时信任？
否
是
F3：让该数据包通过·将该 IP 地址列为可信任 IP 地址储存到储存装置并设定该可信任 IP 地址有效时间，有效时间过后将该可信任 IP 地址删除
结束

图 5