(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101242416 B
(45)授权公告日 2011.11.16

(21)申请号 200810080903.X

(22)申请日 2002.12.10

(30)优先权数据
60/339,900 2001.12.10 US

(62)分案原申请数据
02824700.0 2002.12.10

(73)专利权人 思科技术公司
地址 美国加利福尼亚州

(72)发明人 耶胡达·埃菲克 拉菲·扎迪卡里奥丹·图伊图 阿纳·布雷姆列尔巴尔

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 宋鹤

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
H04L 12/56(2006.01)

(56)对比文件
CN 1236451 A,1999.11.24, 全文.
US 5987610 A,1999.11.16, 全文.
US 5623600 A,1997.04.22, 全文.
US 5511184 A,1996.04.23, 全文.
CN 1304089 A,2001.07.18, 全文.

审查员 鲁艳萍

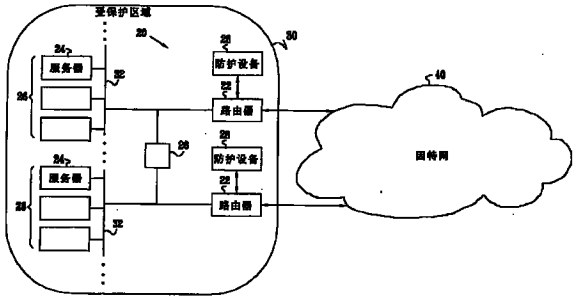
权利要求书 2 页 说明书 12 页 附图 5 页

(54)发明名称

用于过滤和分析基于分组的通信流量的方法和装置

(57)摘要

本发明公开了一种用于过滤基于分组的通信流量的方法。至少接收从源地址通过网络向目的地地址发送的第一数据分组。通过对所述第一数分组进行分析，确定所述第一数据分组是由蠕虫生成的。响应于所述确定，封堵从所述源地址通过所述网络发送的第二数据分组。



CN 101242416 B

1. 一种用于分析基于分组的通信流量的方法，包括：

将一个或多个网络地址指定为陷阱地址，所述陷阱地址被分配给一个或多个防护设备，但未被网络的其它元件所使用；

接收从源地址通过所述网络向所述陷阱地址中至少一个发送的数据分组；

响应于接收到所述分组，对所述分组进行分析，以确定其是否指示蠕虫活动；以及

响应于确定所述分组指示蠕虫活动，将所述源地址指出为恶意流量源。

2. 如权利要求 1 所述的方法，其中，接收所述数据分组包括接收从所述源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且其中，对所述分组进行分析包括对从所述源地址向所述陷阱地址中的所述一个或多个地址发送的数据分组的到达频率进行分析。

3. 如权利要求 1 所述的方法，其中，指出所述源地址包括将所述源地址指出为蠕虫生成流量的生成者。

4. 一种用于分析基于分组的通信流量的方法，包括：

将一个或多个网络地址指定为陷阱地址，所述陷阱地址被分配给一个或多个防护设备，但未被网络的其它元件所使用；

接收通过所述网络向所述陷阱地址中至少一个发送的数据分组；

响应于接收到所述分组，对所述分组进行分析，以确定其是否指示蠕虫活动；以及

响应于确定所述分组指示蠕虫活动，开始对从所述网络的受保护区域之外的源通过所述网络发送的另外的数据分组进行转移，以防止恶意流量到达所述网络的所述受保护区域。

5. 如权利要求 4 所述的方法，其中，开始所述转移包括防止蠕虫生成流量到达所述网络的所述受保护区域。

6. 如权利要求 4 所述的方法，其中，开始所述转移包括确定所述另外的数据分组中的一个分组是由蠕虫生成的，并且，响应于所述确定，封堵对该分组的传递。

7. 如权利要求 4 所述的方法，其中，接收所述数据分组包括接收从源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且其中，对所述分组进行分析包括对从所述源地址向所述陷阱地址中的所述一个或多个地址发送的数据分组的到达频率进行分析，并且响应于所述频率是非同寻常的高频率而确定所述分组指示蠕虫活动。

8. 一种用于分析基于分组的通信流量的装置，包括：

用于将一个或多个网络地址指定为陷阱地址的部件，所述陷阱地址被分配给一个或多个防护设备，但未被网络的其它元件所使用；

用于接收从源地址通过所述网络向所述陷阱地址中至少一个发送的数据分组的部件；

响应于接收到所述分组，对所述分组进行分析，以确定其是否指示蠕虫活动的部件；以及

响应于确定所述分组指示蠕虫活动，将所述源地址指出为恶意流量源的部件。

9. 如权利要求 8 所述的装置，其中，接收所述数据分组包括接收从所述源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且其中，对所述分组

进行分析包括对从所述源地址向所述陷阱地址中的所述一个或多个地址发送的数据分组的到达频率进行分析。

10. 如权利要求 8 所述的装置，其中，指出所述源地址包括将所述源地址指出为蠕虫生成流量的生成者。

11. 一种用于分析基于分组的通信流量的装置，包括：

用于将一个或多个网络地址指定为陷阱地址的部件，所述陷阱地址被分配给一个或多个防护设备，但未被网络的其它元件所使用；

用于接收通过所述网络向所述陷阱地址中至少一个发送的数据分组的部件；

响应于接收到所述分组，对所述分组进行分析，以确定其是否指示蠕虫活动的部件；以及

响应于确定所述分组指示蠕虫活动，开始对从所述网络的受保护区域之外的源通过所述网络发送的另外的数据分组进行转移，以防止恶意流量到达所述网络的所述受保护区域的部件。

12. 如权利要求 11 所述的装置，其中，开始所述转移包括防止蠕虫生成流量到达所述网络的所述受保护区域。

13. 如权利要求 11 所述的装置，其中，开始所述转移包括确定所述另外的数据分组中的一个分组是由蠕虫生成的，并且响应于所述确定，封堵对该分组的传递。

14. 如权利要求 11 所述的装置，其中，接收所述数据分组包括接收从源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且其中，对所述分组进行分析包括对从所述源地址向所述陷阱地址中的所述一个或多个地址发送的数据分组的到达频率进行分析，并且响应于所述频率是非同寻常的高频率而确定所述分组指示蠕虫活动。

用于过滤和分析基于分组的通信流量的方法和装置

[0001] 本申请是国家申请号为02824700.0(国际申请号为PCT/IL02/00996)、国际申请日为2002年12月10日、题为“防御恶意流量”的专利申请的分案申请。

技术领域

[0002] 本发明一般地涉及计算机网络,具体涉及用于在计算机网络中防御恶意流量的方法和系统。

背景技术

[0003] 本申请要求2001年12月10日提出的题为“Methods and Apparatus forProtecting Against Malicious Traffic in the Internet”的美国临时专利申请60/339,900的优先权。本申请是同时待审的美国专利申请09/929,877的部分继续,该申请的申请日是2001年8月14日,题为“Methods andApparatus for Protecting Against Overload Conditions on Nodes of aDistributed Network”,并被公开为美国专利申请公开20020083 175。这两个相关申请都被转让给本专利申请的受让人,其公开内容在此通过引用而包含进来。

[0004] 在服务拒绝(DoS)攻击中,攻击者用大量消息流量冲击受害的网络或服务器。这一流量过载消耗了受害者的可用带宽、CPU能力或其它关键的系统资源,最终使受害者陷入无法对其合法用户提供服务的状况当中。分布式DoS(DDoS)攻击甚至可能更具破坏性,因为这些攻击涉及同时从多个源创建人为的网络流量。在“传统的”海量带宽攻击(massive-bandwidth attack)中,可以在对进入的分组的源因特网协议(IP)地址进行的统计分析的帮助下,对攻击源进行跟踪。受害者随后可以滤去从受怀疑的IP地址发起的任何流量,并可以使用这一证据对攻击者采取法律行动。然而,现在许多攻击使用“地址盗用”(spoofed)IP分组——包含伪造的IP源地址的分组——这使得受害网络更难以防御其自身免遭攻击。

[0005] 为了启动有效的DDoS攻击,攻击者一般试图控制因特网上的大量服务器。获得这种控制的一种方法是使用“蠕虫”(worm),“蠕虫”是利用广泛使用的服务中的安全漏洞而在因特网上自我复制的程序。在取得对服务器的控制之后,蠕虫通常使用该服务器来参与DDoS攻击。最近的著名蠕虫包括红码(Code Red)(I和II)和Nimba。例如,红码I在2001年夏季期间利用Microsoft ® IIS网络服务器(Web server)的安全漏洞而传播。一旦它感染了服务器,该蠕虫就通过启动99个线程而传播,其中每个线程都生成随机的IP地址并试图危害处于这些地址的服务器。除了这种自我复制之外,红码I还在受感染的服务器上同时自我激活,以启动对www.whitehouse.gov域的协同DDoS攻击。

[0006] 除了对受害于蠕虫启动的DDoS攻击的域所造成的破坏以外,被蠕虫感染的服务器和网络还常常遭遇性能的下降。这种下降部分地是由于被感染的服务器在其试图发现并感染处于随机IP地址的服务器(称为“扫描”)时所生成和接收的分组、以及被感染的服务器在其参与DDoS攻击时所生成的分组所造成的。例如,被感染的服务器可能将大量SYN请

求分组发送到随机 IP 地址，其中每个地址可能都用 SYN-ACK 响应分组来应答。这种流量可能消耗被感染的网络与因特网之间的连接的大部分带宽。此外，SYN 请求一般会被发送服务器缓冲一段时间，这占用了服务器资源。

发明内容

[0007] 在本发明的实施例中，网络防护系统检测并封堵 (block) 蠕虫所生成的进入和 / 或外出分组。一般而言，防护系统通过 (a) 检查分组是否包含已知的蠕虫特征，和 / 或 (b) 监视分组的源以发现对应于与蠕虫所生成的流量相关联的模式的异常流量模式，来检测这种受感染的分组。一旦防护系统检测到可疑的分组或流量模式，它就可以将来自同一源的分组的全部或部分封堵一段时间，或者采取其它预防性行动。未被感染的分组被转发到其预期目的地。

[0008] 对于某些应用，网络防护系统监视进入分组，以防止恶意源与网络的受保护区域内的服务器建立连接。在本发明的一些这种实施例中，用网络防护系统来保护的网络将分配给该网络的一组网络地址（例如 IP 地址）指定为“陷阱”(trap) 地址。这些陷阱地址被分配给一个或多个防护设备，但未被网络的其它元件所使用。当寻址到这种陷阱地址的分组进入受保护的网络时，该分组被转发到所分配的防护设备，该防护设备对流量进行分析。防护设备例如可以基于流量的内容或统计特性，确定来自给定源地址的流量是可疑的。然后，防护设备可以封堵或以其它方式过滤来自受怀疑的源地址的进入流量，以降低网络的受保护区域内的服务器被蠕虫感染的可能性。代替性地或附加性地，防护设备然后可以开始对进入网络受保护区域的所有分组进行监视。这些用于防御进入的蠕虫生成流量的技术可以降低受保护的网络和诸如因特网之类的广域网之间的带宽消耗。例如，这些技术可以降低受保护区域中的元件响应于进入流量而生成的外出流量，例如内部服务器在试图建立与被感染的外部服务器的握手时所生成的 SYN-ACK 响应。

[0009] 代替性地或附加性地，网络防护系统对从受保护区域中的服务器发起的外出分组进行监视。一般而言，防护系统通过确定服务器正在短时间内试图创建到不同地址的大量连接、或者创建与不存在的地址的连接，来检测被感染的服务器。通过检测和封堵被感染的外出分组，防护系统防止感染了蠕虫的服务器与受保护区域之外的服务器建立特定类型的连接。此技术还可以降低受保护的网络和诸如因特网之类的广域网之间的带宽消耗，这是通过 (a) 降低感染了蠕虫的服务器在试图传播蠕虫和参与 DDoS 攻击这两种情况下所生成的输出流量，以及 (b) 降低响应于恶意输出流量而生成的输入流量而实现的，所述输入流量例如是外部服务器在试图建立与被感染的内部服务器的握手时所生成的 SYN-ACK 响应。此外，当检测到被感染的服务器时，防护系统一般生成网络管理员警报，使得管理员可以采取适当的行动，例如清理被感染的服务器。

[0010] 在此所描述的用于检测和转移 (divert) 蠕虫生成流量的技术可以单独使用，或者结合其它补充性技术来使用，用于防止 DDoS 攻击。例如，这种技术在上文中所引用的美国专利申请公开 20020083175 中、以及在美国专利申请 10/232,993 中进行了描述，美国专利申请 10/232,993 的申请日是 2002 年 8 月 29 日，题为“Protecting Against Distributed Denial of ServiceAttacks”，该专利申请被转让给本专利申请的受让人，在此通过引用而包含了该申请。

[0011] 因此，根据本发明一个实施例，提供了一种用于过滤基于分组的通信流量的方法，该方法包括：

[0012] 至少接收从源地址通过网络向目的地地址发送的第一数据分组；

[0013] 通过分析所述第一数据分组，确定所述第一数据分组是由蠕虫生成的；以及

[0014] 响应于所述确定，封堵从所述源地址通过所述网络发送的第二数据分组。

[0015] 进行所述确定可以包括将所述第一数据分组的属性与已知的蠕虫生成分组的一组属性相比较，并且当发现所述第一数据分组的属性与所述组中的属性之一相匹配时，封堵所述第一数据分组。

[0016] 在一个实施例中，封堵所述第二数据分组包括在从作出所述第一数据分组是由蠕虫生成的这一确定开始的一段时间内封堵所述第二数据分组，而此后不封堵所述第二数据分组。

[0017] 在一个实施例中，所述目的地地址位于所述网络的受保护区域内，并且接收所述第一数据分组包括接收来自位于所述受保护区域之外的源的第一数据分组。或者，所述源地址属于位于所述网络的受保护区域内的网络元件，所述目的地地址位于所述受保护区域之外，并且接收所述第一数据分组包括在所述受保护区域内接收所述第一数据分组。

[0018] 进行所述确定可以包括生成管理员警报，该管理员警报表示所述第一数据分组是由所述蠕虫生成的。

[0019] 在一个实施例中，所述第一数据分组具有端口指定，并且进行所述确定包括确定所述端口指定不对应于在所述目的地地址处运行的应用。代替性地或附加性地，用于一个应用的服务器驻留在所述目的地地址处，并且进行所述确定包括确定所述第一数据分组不对应于所述应用。

[0020] 在一个实施例中，接收所述第一数据分组包括接收因特网协议 (IP) 分组，并且进行所述确定包括对所述 IP 分组的序列号的模式进行分析。代替性地或附加性地，接收所述第一数据分组包括接收传输控制协议 (TCP)SYN 分组。接收所述 SYN 分组可以包括接收分别寻址到多个目的地地址的多个 SYN 分组，并且进行所述确定包括对蠕虫的地址扫描特性的模式进行检测。

[0021] 在一个实施例中，进行所述确定包括确定所述目的地地址无效。进行所述确定可以包括将一个或多个地址指定为陷阱地址，并且确定所述目的地地址是所述陷阱地址之一。进行所述确定还可以包括对从所述源地址向所述陷阱地址中的一个或多个地址发送的数据分组的到达频率进行分析，以确定所述分组是不是由蠕虫生成的。

[0022] 在一个实施例中，进行所述确定包括将所述第一数据分组的源地址存储在黑名单上，并且封堵所述第二数据分组包括响应于所述黑名单而封堵所述第二数据分组。存储在所述黑名单上可以包括当确定出接收自所述源地址的分组频率已经降低时，将所述第一数据分组的源地址从黑名单上去除。

[0023] 至少接收所述第一数据分组可以包括接收来自所述源地址的多个数据分组，这些数据分组分别寻址到多个目的地地址，并且进行所述确定包括对发送自所述源地址的所述多个数据分组进行分析。进行所述确定可以包括对所述数据分组的到达频率进行分析。代替性地或附加性地，进行所述确定包括将所述目的地地址的模式与和已知的蠕虫生成流量相关联的至少一种模式相比较。接收来自所述源地址的所述数据分组可以包括接收来自属

于一个子网的多个源地址的数据分组，并且封堵所述第二数据分组包括封堵从所述子网通过所述网络发送的另外的数据分组。

[0024] 在一个实施例中，接收所述第一数据分组包括在所述第一数据分组到达所述目的地地址之前拦截所述第一数据分组，该方法还包括当确定出所述第一数据分组不是由所述蠕虫生成的时，将所述第一数据分组传递到所述目的地地址。接收所述第一数据分组可以包括接收寻址到特定端口的因特网协议（IP）分组，并且拦截所述第一数据分组包括响应于所述 IP 分组所寻址到的特定端口而拦截所述第一数据分组。拦截所述第一数据分组可以包括仅当所述第一数据分组包括传输控制协议（TCP）SYN 分组并且所述第一数据分组寻址到端口 80 时，才拦截所述第一数据分组。

[0025] 根据本发明一个实施例，还提供了一种用于分析基于分组的通信流量的方法，该方法包括：

[0026] 接收从源地址通过网络发送、并分别寻址到多个目的地地址的多个数据分组；

[0027] 确定将所述数据分组从所述源地址向所述多个目的地地址发送的频率；以及

[0028] 响应于所述频率，将所述源地址指出为恶意流量源。

[0029] 接收所述数据分组可以包括接收传输控制协议（TCP）SYN 分组。指出所述源地址可以包括将所述源地址指出为蠕虫生成流量的生成者。

[0030] 在一个实施例中，接收所述数据分组包括接收分别具有端口指定的因特网协议（IP）分组，并且确定所述频率包括确定下述数据分组的发送频率，所述数据分组各自的端口指定不对应于在所述目的地地址处运行的应用。确定所述频率可以包括确定寻址到用于某个应用的服务器所驻留的目的地地址的数据分组的发送频率，所述应用不同于所述分组中所指明的应用。

[0031] 根据本发明一个实施例，提供了一种用于分析基于分组的通信流量的方法，该方法包括：

[0032] 将一个或多个网络地址指定为陷阱地址；

[0033] 接收从源地址通过所述网络向所述陷阱地址之一发送的数据分组；以及

[0034] 响应于接收到所述分组，将所述源地址指出为恶意流量源。

[0035] 在一个实施例中，接收所述数据分组包括接收从所述源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且指出所述源地址包括对从所述源地址向所述陷阱地址中的所述一个或多个发送的数据分组的到达频率进行分析。指出所述源地址可以包括将所述源地址指出为蠕虫生成流量的生成者。

[0036] 根据本发明一个实施例，还提供了一种用于分析基于分组的通信流量的方法，该方法包括：

[0037] 将一个或多个网络地址指定为陷阱地址；

[0038] 接收通过所述网络向所述陷阱地址之一发送的数据分组；以及

[0039] 响应于接收到所述分组，开始对从所述网络的受保护区域之外的源通过所述网络发送的另外的数据分组进行转移，以防止恶意流量到达所述网络的受保护区域。

[0040] 开始所述转移可以包括开始转移以防止蠕虫生成流量到达所述网络的受保护区域。在一个实施例中，开始所述转移包括确定所述另外的数据分组中的一个分组是由蠕虫生成的，并且，响应于所述确定，封堵对该分组的传递。接收所述数据分组可以包括接收从

源地址通过所述网络向所述陷阱地址中的一个或多个地址发送的多个数据分组，并且开始所述转移包括对从所述源地址向所述陷阱地址中的所述一个或多个发送的数据分组的到达频率进行分析。

[0041] 根据本发明一个实施例，另外提供了一种用于分析基于分组的通信流量的方法，该方法包括：

[0042] 接收从源地址通过网络向目的地地址发送的数据分组；

[0043] 将所述数据分组的属性与已知的蠕虫生成流量的一组属性相比较；以及

[0044] 当发现所述分组的属性与所述组中的属性之一相匹配时，将所述源地址指出为蠕虫生成流量的源。

[0045] 所述属性可以包括所述数据分组的长度或所述分组的签名。

[0046] 根据本发明一个实施例，另外还提供了用于过滤基于分组的通信流量的装置，该装置包括防护设备，该防护设备适于执行以下操作：至少接收从源地址通过网络向目的地地址发送的第一数据分组；通过分析所述第一数据分组，确定所述第一数据分组是由蠕虫生成的；以及响应于所述确定，封堵从所述源地址通过所述网络发送的第二数据分组。

[0047] 根据本发明一个实施例，还提供了用于分析基于分组的通信流量的装置，该装置包括防护设备，该防护设备适于执行以下操作：接收从源地址通过网络发送、并分别寻址到多个目的地地址的多个数据分组；确定将所述数据分组从所述源地址向所述多个目的地地址发送的频率；以及响应于所述频率，将所述源地址指出为恶意流量源。

[0048] 根据本发明一个实施例，又提供了用于分析基于分组的通信流量的装置，该装置包括防护设备，该防护设备适于执行以下操作：将一个或多个网络地址指定为陷阱地址；接收从源地址通过所述网络向所述陷阱地址之一发送的数据分组；以及响应于接收到所述分组，将所述源地址指出为恶意流量源。

[0049] 根据本发明一个实施例，还提供了用于分析基于分组的通信流量的装置，该装置包括防护设备，该防护设备适于执行以下操作：将一个或多个网络地址指定为陷阱地址；接收通过所述网络向所述陷阱地址之一发送的数据分组；以及响应于接收到所述分组，开始对从所述网络的受保护区域之外的源通过所述网络发送的另外的数据分组进行转移，以防止恶意流量到达所述网络的所述受保护区域。

[0050] 根据本发明一个实施例，另外提供了用于分析基于分组的通信流量的装置，该装置包括防护设备，该防护设备适于执行以下操作：接收从源地址通过网络向目的地地址发送的数据分组；将所述数据分组的属性与已知的蠕虫生成分组的一组属性相比较；以及当发现所述分组的属性与所述组中的属性之一相匹配时，将所述源地址指出为蠕虫生成流量的源。

[0051] 根据本发明一个实施例，另外还提供了一种用于过滤基于分组的通信流量的计算机软件产品，该产品包括计算机可读介质，程序指令存储在所述介质中，所述指令当被计算机读取时，使得计算机执行以下操作：至少接收从源地址通过网络向目的地地址发送的第一数据分组；通过分析所述第一数据分组，确定所述第一数据分组是由蠕虫生成的；以及响应于所述确定，封堵从所述源地址通过所述网络发送的第二数据分组。

[0052] 根据本发明一个实施例，还提供了一种用于分析基于分组的通信流量的计算机软件产品，该产品包括计算机可读介质，程序指令存储在所述介质中，所述指令当被计算机读

取时，使得计算机执行以下操作：接收从源地址通过网络发送、并分别寻址到多个目的地地址的多个数据分组；确定将所述数据分组从所述源地址向所述多个目的地地址发送的频率；以及响应于所述频率，将所述源地址指出为恶意流量源。

[0053] 根据本发明一个实施例，又提供了一种用于分析基于分组的通信流量的计算机软件产品，该产品包括计算机可读介质，程序指令存储在所述介质中，所述指令当被计算机读取时，使得计算机执行以下操作：将一个或多个网络地址指定为陷阱地址；接收从源地址通过所述网络向所述陷阱地址之一发送的数据分组；以及响应于接收到所述分组，将所述源地址指出为恶意流量源。

[0054] 根据本发明一个实施例，还提供了一种用于分析基于分组的通信流量的计算机软件产品，该产品包括计算机可读介质，程序指令存储在所述介质中，所述指令当被计算机读取时，使得计算机执行以下操作：将一个或多个网络地址指定为陷阱地址；接收通过所述网络向所述陷阱地址之发送的数据分组；以及响应于接收到所述分组，开始对从所述网络的受保护区域之外的源通过所述网络发送的另外的数据分组进行转移，以防止恶意流量到达所述网络的所述受保护区域。

[0055] 根据本发明一个实施例，另外提供了一种用于分析基于分组的通信流量的计算机软件产品，该产品包括计算机可读介质，程序指令存储在所述介质中，所述指令当被计算机读取时，使得计算机执行以下操作：接收从源地址通过网络向目的地地址发送的数据分组；将所述数据分组的属性与已知的蠕虫生成分组的一组属性相比较；以及当发现所述分组的属性与所述组中的属性之一相匹配时，将所述源地址指出为蠕虫生成流量的源。

附图说明

[0056] 根据以下对本发明实施例的详细描述，并结合附图，将会更充分地理解本发明，在附图中：

[0057] 图 1 是一个框图，其示意性地示出了根据本发明一个实施例的网络防护系统；

[0058] 图 2 是一个框图，其示意性地示出了根据本发明一个实施例，因特网服务提供商 (ISP) 所部署的网络防护系统；

[0059] 图 3 是一个流程图，其示意性地示出了根据本发明一个实施例，用于检测蠕虫所生成的流量的方法；

[0060] 图 4 是一个流程图，其示意性地示出了根据本发明一个实施例，用于过滤和封堵流量的方法；并且

[0061] 图 5 是一个流程图，其示意性地示出了根据本发明一个实施例，用于检测蠕虫所生成的流量的另一种方法。

具体实施方式

[0062] 图 1 是一个框图，其示意性地示出了根据本发明一个实施例的网络防护系统 20。网络的受保护区域 30 通过一个或多个路由器 22，与通常是因特网的广域网 (WAN)40 相通信。受保护区域 30 包括各种网络元件 26，例如服务器 24、客户端、交换器、内部路由器和网桥，它们般由一个或多个局域网 (LAN)32 相连接。如下文所述，受保护区域 30 一般（但非必须）包括诸如企业网或校园网等的专用网络，或者由因特网服务提供商 (ISP) 运营的网

络。

[0063] 为了防止服务器 24 感染蠕虫，防护设备 28 拦截来自 WAN 40 的寻址到网络元件 26 的进入分组。防护设备 28 对这些进入分组进行分析，以检测被怀疑感染了蠕虫的分组，这一般是使用在下文中参照图 3 和 5 而描述的技术来进行的。一旦已检测到被感染的分组或流量模式，防护设备 28 就将来自同一源的分组的全部或一部分封堵一段时间，这一般是使用下文中参照图 4 而描述的技术来进行的。未被感染的分组被转发到其预期目的地。

[0064] 代替性地或者附加性地，防护设备 28 对从服务器 24 经由 WAN 40 发送到受保护区域 30 之外的外出分组进行监视。通过检测并封堵被感染的外出分组，防护设备 28 防止感染了蠕虫的服务器 24 与受保护区域 30 之外的服务器建立连接。结果，被感染的服务器 24 无法危害外部服务器或参与对受保护区域 30 之外的网络元件的 DDoS 攻击。封堵这种被感染的流量还减轻了路由器 22 和 WAN 40 之间的链路上的压力，使得合法流量不被恶意行动所妨碍。

[0065] 防护设备 28 可以一直执行这些分组过滤和转移 (diversion) 功能，或者其可以仅在压力条件 (stress condition) 下才变为有效，在所述压力条件下，预计或怀疑会有对服务器 24 的攻击或由服务器 24 进行的攻击。例如，防护设备 28 可以在以下情况下变为有效：当检测到非同寻常的大量进入的 SYN 请求分组时、当其它流量统计指示出可能有攻击正在进行时、当已经使用“陷阱”地址而检测到蠕虫所生成的流量时（如在下文中参照图 5 所描述的那样）、和 / 或当网络管理员知道蠕虫正活跃在因特网上时。

[0066] 一般而言，防护设备 28 包括通用计算机，该计算机被以软件编程，以实现此处所描述的功能。所述软件可以例如通过网络而以电子形式下载到所述计算机中，或者可以在诸如 CD-ROM 之类的有形介质上被提供给所述计算机。又或者，可以在专用硬件逻辑中、或使用硬件和软件元件的组合来实现防护设备 28。防护设备可以是一个独立单元，或者它可与其它通信或计算设备集成在一起，所述设备例如是路由器 22、防火墙或入侵检测系统（未示出）。

[0067] 在实际应用中，可以用一个或多个防护设备 28 来保护服务器 24 的集群，或者可以用它们来保护流量被转移到了这些防护设备的整个 LAN、内部网或服务器集合。可以将防护功能分布到设在对受保护区域 30 的一个或多个访问点处的多个防护设备 28 当中。在使用多于一个防护设备的应用中，这些防护设备可以共享一个或多个公共数据存储库，或者可以用其它方式彼此通信，例如执行集合统计分析和 / 或维护对受怀疑的恶意分组源的公共记录。所述防护设备可以部署在与本领域内公知的防火墙类似的配置中。优选地，防护设备具有足够的处理能力，使得它们自身不会在蠕虫攻击时变为瓶颈。虽然在此针对过滤去往 / 来自服务器 24 的进入和 / 或外出流量而描述了某些技术，但这些技术也可以被用来过滤去往 / 来自其它网络元件 26 的进入和 / 或外出流量，所述网络元件例如是可能被蠕虫感染的客户端计算机。路由器 22 可以包括商业上可获得并且普遍用在 IP 网络上的类型的路由器，或者能够重定向流量并在其它方面提供路由器通常执行的功能的其它网络元件。

[0068] 图 2 是一个框图，其示意性地示出了根据本发明一个实施例，部署在属于因特网服务提供商 (ISP) 的网络中的受保护区域 30 上的网络防护系统 20。受保护区域 30 一般通过一个或多个路由器 22 与外部网络通信，所述外部网络例如是 (a) 公众广域网 (WAN)40，如上所述其一般是因特网，又例如是 (b) 位于专用或公众对等点处的其它 ISP 42，以及 (c)

客户的网络 44。受保护区域 30 包括各种网络元件 26，例如路由器、交换机、网桥、服务器和客户端。一个或多个防护设备 28 处理来自 / 去往外部网络的进入和 / 或外出分组。一般而言，每个防护设备都以“棒棒糖”(lollipop) 方式连接到相应路由器的多个端口之一。路由器基于预先编程的路由准则，将某些进入和 / 或外出分组（或者在某些情况下，所有的进入和 / 或外出分组）传递到防护设备用于分析。防护设备 28 使用此处所描述的技术来分析所述分组，以防止蠕虫和 / 或蠕虫所生成的流量在不同的外部网络间、以及在外部网络与网络元件 26 间传播。

[0069] 尽管在图 1 和 2 中，每个防护设备 28 都被示出为与单一邻接路由器 22 直接相连，但本领域技术人员在阅读了本专利申请之后，将会很清楚代替性的配置。例如，在防护设备与路由器之间不需要有一对一的对应关系，并且防护设备和路由器例如可以由交换机分开物理上或网络上的距离。

[0070] 图 3 是一个流程图，其示意性地示出了根据本发明一个实施例，用于检测蠕虫所生成的流量的方法。该方法可以被一直执行，或者仅在某些时间或某些情况下执行，这取决于所关心的防护设备和路由器的配置。例如，所述方法可以在已手动或自动检测到压力条件时发起，或者为对流量进行采样而间断地发起。发起时，在流量转移步骤 50 将所有类型的流量或所选择的类型的流量从路由器 22 转移到防护设备 28。优选地，仅转移可能携带蠕虫的类型的流量。例如，响应于特定的网络配置和条件，可以仅转移去往与某些应用相对应的端口的流量（例如，用于 HTTP 应用的端口 80，或用于 FTP 的端口 21）。为了使流量的转移最小化，对于一些应用可能仅转移端口 80 SYN 分组就足够了，这一转移使得能够阻止蠕虫通过在 HTTP 上运行的应用的传播。

[0071] 在本发明的一些实施例中，使用以下技术中的一种或多种来实现转移：

[0072] • Web 缓存控制协议 (WCCP) 版本 1（由加利福尼亚州圣何塞的 Cisco ® Systems 公司发布）可用于将所有端口 80 流量无缝地转移到防护设备 28。

[0073] •对于支持 WCCP 版本 2 的路由器 22，在合适的情况下可以使用更专门的选择标准来实现转移。例如，可以转移所有 SYN 请求（或者所有去往端口 80 的 SYN 请求），或者可以仅转移来自特定源 IP 地址的 SYN 请求或其它流量。

[0074] • Cisco 的基于策略的路由 (PBR) 可用于基于使用访问控制列表 (ACL) 而规定的标准来改变流量的方向，所述标准例如是目的地端口、分组类型（例如 SYN 分组）或接收到流量的接口。

[0075] • 可以通过发出边界网关协议 (BGP) 通告，将流量重新路由以从去往其预期接受者改为去往防护设备 28，来实现转移。

[0076] 还可以使用在上文中引用的美国专利申请公开 20020083175 中所描述的、或者本领域内公知的其它转移技术，例如用于防火墙的转移技术。本发明的转移技术可以结合美国专利申请公开 20020083175 中所描述的其它转移技术来实现。

[0077] 现在回到图 3，已经转移了流量之后，在分组拦截步骤 52，防护设备 28 拦截所有被转移的分组。在分组分析步骤 54，防护设备 28 逐一和 / 或集合地分析所拦截的分组，以检测被怀疑感染了蠕虫或者是由蠕虫生成的分组。这种被感染的分组可能携带蠕虫代码本身，和 / 或它们可能是由蠕虫所生成、用来扫描以发现易受感染的服务器或准备让这些服务器接收蠕虫代码的。此外，被感染的分组（一般而言，主要是外出分组）可能是由参与 DDoS

攻击的被蠕虫感染的服务器 24 所生成的。

[0078] 一般使用以下技术中的一种或多种来分析分组，这取决于所实施的特定警告，或由网络管理员确定：

[0079] •对分组的目的地地址进行分析，以检测指示出恶意活动的模式。根据源地址或用子网源地址将分组，并且防护设备 28 执行以下分析中的一种或多种：

[0080] ■根据第一种分析方法，将从同一源或子网源地址去往多个目的地地址的诸如 SYN 分组之类的非同寻常的高频率分组解释为对蠕虫所生成的“扫描”流量的指示。该分析可以排除对诸如代理服务器之类在正常情况下显示出这和行为的源的怀疑，这是通过将所述源的活动与它们所测量到的基准活动 (baseline activity) 相比较而实现的。

[0081] ■根据第二种分析方法，将来自同一源或子网源的目的地地址的异常模式解释为对蠕虫所生成的流量的指示。例如，所述异常模式可能对应于诸如红码或 Nimba 之类的已知蠕虫的恶意扫描模式。或者，所述异常模式可能与蠕虫已知的或预料到的行为模式类似。

[0082] ■根据第三种分析方法，寻址到无效地址的分组，例如不存在的目的地分组或没有服务器的目的地地址，被认为极有可能是蠕虫所生成的。

[0083] ■根据第四种分析方法，去往特定应用或端口的非同寻常的高频率分组（一般是 SYN 分组），当寻址到不是用于所述特定应用或端口的服务器的目的地时，被解释为可能的对蠕虫所生成的流量的指示。例如，这种 SYN 分组可能或者寻址到不是 HTTP 服务器的设备的端口 80，或者寻址到未使用的地址。

[0084] ■根据第五种分析方法，对 SYN 请求或请求消息的参数进行统计分析，以检测到指示蠕虫感染的源的行为的模式。例如，这种参数可能包括源所使用的序列号。

[0085] • 对单独的分组进行分析，以检测已知的蠕虫的特征。优选地，为了有效地检查分组，首先对照已知的承载蠕虫的分组大小，来检查分组的大小。通过在消息主体内检查已知的蠕虫的数字模式，进一步过滤具有相匹配的大小的分组。已知的蠕虫的一次出现就足以确定地识别出恶意源。

[0086] • 对分组的目的地地址进行分析，以检测无效地址，无效地址可能是对分组是蠕虫所生成的指示。例如，因特网 IP 地址中有许多段是众所周知未使用的（例如为测试或组播而预留的地址）。此外，防护设备可以维护一个当前未被分配的因特网 IP 地址的最新列表。而且，如下文中参照图 5 所描述的那样，被指定为“陷阱”地址的地址已知是无效的。

[0087] 这些技术对于检测进入和外出流量中蠕虫所生成的或承载蠕虫的流量一般都是有效的。对于一些应用，使用在上文中引用的美国专利申请公开 20020083175 中所描述的统计收集和智能学习技术，实现了这些分析技术中的一些或全部，并已进行了必要的修正。

[0088] 继续图 3 的方法，在执行所述分析之后，在蠕虫发现检查步骤 56 确定是否已识别出感染了蠕虫的源。如果还未发现蠕虫，则在无行动步骤 58，防护设备对所拦截的分组不采取任何行动。另一方面，如果已经识别出蠕虫，则在黑名单步骤 60，可能是源地址，也可能是子网源地址被添加到受怀疑的或已知的感染了蠕虫的源的黑名单上。该黑名单被存储在诸如数据库之类的存储库中。（或者，基本上任意合适的存储器设备和数据结构都可以用来存储黑名单，不仅仅是数据库。）当在区域 30 中部署了多个防护设备时，它们优选地但不是必须地共享一个公共的黑名单，以使得能够更彻底地封堵被列入黑名单的源。

[0089] 在将被感染的源添加到黑名单上之后，在警报生成步骤 62，防护设备 28 一般生成

一个网络管理员警报和/或日志条目。管理员可以使用这一信息来采取预防性或补救性措施。例如，当在外出流量中检测到了蠕虫（即，感染受保护区域 30 内的服务器 24 的蠕虫）时，管理员可以清理被感染的服务器，并安装适当的补丁以纠正产生了易受感染性的安全缺陷。在一些情况下，尤其是当在进入流量中检测到了蠕虫时，管理员可能希望配置路由器 22 和/或防火墙中的一个或多个来直接封堵恶意源，而不使用防护设备 28。

[0090] 蠕虫扫描者（被配置为通过将分组发送到多个地址来扫描以发现易受感染的服务器的蠕虫）有时使用盗用地址的 IP 分组，如在上文的“背景技术”部分中所描述的那样。结果，防护设备可能确定出某个源地址感染了蠕虫，但实际上该源地址只是被位于 WAN 上其它地方的蠕虫盗用了地址而已。这样，防护设备就可能在某种情况下错误地封堵了无辜的未被感染的客户端或服务器的源地址。在本发明一个实施例中，防护设备采用反地址盗用机制来防止这种错误的封堵，所述机制例如是在上述专利申请中所描述的反地址盗用机制，或者本领域中公知的其它技术，例如 SYN 小甜饼 (cookie) 或 RST 小甜饼。

[0091] 图 4 是一个流程图，其示意性地示出了根据本发明一个实施例，用于过滤和封堵流量的方法。和参照图 3 描述的方法中一样，根据防护设备 28 的配置，此方法发起于流量转移步骤 50。对于一些应用，图 4 的方法的发起与图 3 的方法的发起同时进行。或者，图 4 的方法仅在黑名单包含至少一个源地址时发起。一般而言，当图 3 的方法和图 4 的方法都已发起时，这两个方法在并行的过程中运行，或者在同一防护设备上，或者在不同的防护设备上。一般而言，在图 3 和图 4 的两种方法中所转移的是相同类型的流量，尽管对于某些应用，在图 4 的方法中所转移的分组集比图 3 的方法中所转移的更大或更小。转移一般是使用在上文中参照图 3 所描述的方法中的一种或多种来实现的。

[0092] 在转移了流量之后，在分组拦截步骤 52，防护设备 28 拦截所有被转移的分组。在黑名单查找步骤 64，防护设备 28 在黑名单上查找每个分组的源地址或子网源地址。在地址检查步骤 66，防护设备 28 确定分组的地址是否在黑名单上。如果在黑名单上未找到分组地址，则在转发分组步骤 68，防护设备将分组沿其正常路径转发到其预期的目的地地址。

[0093] 另一方面，如果在黑名单上找到了分组的地址，则在封堵步骤 70，防护设备 28 封堵对该分组的进一步传输。一般而言，防护设备只是丢弃所封堵的分组，但是，防护设备或者也可以分析分组内容（甚至可以在发现该分组内容合法的情况下，采取行动以传递该分组或将其从黑名单上去除）。或者，在步骤 70，防护设备仅封堵试图与受保护区域之外的服务器建立特定类型连接的那些分组。在日志步骤 72，防护设备一般将对分组的接收和封堵记成日志。在此步骤生成的日志可以由系统管理员用于报告或分析。在信息记录步骤 74，防护设备还将关于所封堵的分组的信息添加到诸如数据库之类的封堵分组存储库中。这种信息优选地包括对从每个源地址封堵的分组的数量的计数值。当使用多于一个的防护设备 28 时，这些多个防护设备可以共享一个公共的封堵分组存储库，以允许对封堵模式进行更广泛的统计分析。

[0094] 在存储库分析步骤 76，防护设备中的至少一个连续或周期性地对封堵分组存储库中的数据进行分析，以确定来自一个源或子网源地址的攻击是否已终止。在流量消退检查步骤 78，防护设备一般通过检测来自源的流量是否已消退了一段时间，来确定出攻击已经终止。如果恶意流量还未消退，则在“留在黑名单上”步骤 80，防护设备将该源地址留在黑名单上。另一方面，如果流量已经消退了足够长的一段时间，则在“从黑名单上去除”步骤

82，防护设备将所述源地址从黑名单上去除。一般而言，在管理员警报步骤 84，当将源地址从黑名单上去除时，防护设备生成管理员警报或日志条目。

[0095] 图 5 是一个流程图，其示意性地示出了根据本发明一个实施例，用于检测蠕虫所生成的流量的另一种方法。此方法可被用作单独的检测方法，或者可以与其它检测方法结合使用，所述其它方法例如是在上文中参照图 3 描述的检测方法。可以用图 4 的方法来过滤和封堵来自由图 5 的方法添加到黑名单上的源地址的流量。或者，可以使用其它方法来过滤和封堵来自由图 5 的方法识别出的源的流量。

[0096] 在此方法中，在设置陷阱步骤 90，将分配给受保护区域 30（图 1 和 2）的一组网络地址（例如 IP 地址）指定为“陷阱”地址。所述陷阱地址是由 WAN 40 路由到路由器 22 的地址，但不被设备 26 中的任何设备所使用。这样，寻址到这些陷阱地址的任何流量都被认为是可疑的。路由器 22 被配置为在转移步骤 92 将寻址到陷阱地址的流量转移到防护设备 28 中的至少一个。一般而言，转移是通过静态地配置路由器以将具有这些目的地地址的所有流量都转移到防护设备来实现的。或者，也可以使用其它转移方法，如上文中参照图 3 所描述的那样。

[0097] 当一个寻址到陷阱地址的分组进入受保护区域 30 时，在路由器接收步骤 94，该分组被路由器 22 之一所接收。在转发步骤 96，该路由器将所述分组转发到防护设备。在分析步骤 98，防护设备对所述分组进行分析，以确定其是否指示蠕虫活动。例如，防护设备可以对接收自同一源或子网源地址的分组进行统计分析，这一分析是使用关于刚接收到的分组的信息、并结合关于记录在统计存储库中的先前接收到的分组的信息而进行的，如下文参照步骤 102 而描述的那样。根据一种用于检测蠕虫扫描者所生成的流量的方法，将从单一源或子网源地址发送到陷阱地址的非同寻常的大数量或高频率分组解释为对蠕虫活动的指示。代替性地或者附加性地，可以使用以上参照图 3 的分组分析步骤 54 而描述的蠕虫检测方法中的一种或多种，来检测蠕虫扫描者和 / 或参与 DDoS 攻击的蠕虫所生成的流量。

[0098] 在进行分析之后，在蠕虫发现检查步骤 100 确定是否已识别出感染了蠕虫的源。如果还未发现蠕虫，则在无行动步骤 102，防护设备不对陷入分组采取任何行动。另一方面，如果已识别出蠕虫，则在黑名单步骤 104，以类似于以上参照图 3 中的步骤 60 所描述的类似的方式，可能是源地址，也可能是子网源地址被添加到受怀疑的或已知的感染了蠕虫的源的黑名单上。对于结合利用了图 3 和图 5 的检测方法的应用，可以将被感染的源地址存储在公共黑名单上。

[0099] 或者，当已识别出蠕虫时，不是将源地址添加到黑名单上，而是防护设备开始将来自该源地址的流量转移到一个或多个防护设备以用于过滤，但不一定封堵。代替性地或者附加性地，当已识别出蠕虫时，防护设备开始将所有进入网络的受保护区域的流量（包括来自被感染的源地址以外的地址的流量）都转移到一个或多个防护设备，以用于过滤或者可能用于封堵。

[0100] 在将被感染的源添加到黑名单上或者转移流量之后，在警报生成步骤 106，防护设备 28 一般生成网络管理员警报和 / 或日志条目。管理员可以使用此信息来采取预防性或补救性步骤，例如在上文中参照图 3 的步骤 62 而描述的那些步骤。

[0101] 虽然在此描述的实施例参照了特定的通信协议和惯例，但本发明的原理可以类似地应用于其它数据通信上下文中。例如，此处所描述的技术可以应用于防御通过 SMTP 发送

的蠕虫生成流量。

[0102] 从而应该意识到，以上所描述的实施例是示例性地引用的，并且本发明不限于在上文中具体示出和描述的那些内容。确切地说，本发明的范围包括上文中所描述的各种特征的组合和子组合，以及本领域技术人员在阅读前面的描述时将会想到的、未在现有技术中公开的其变化和修改。

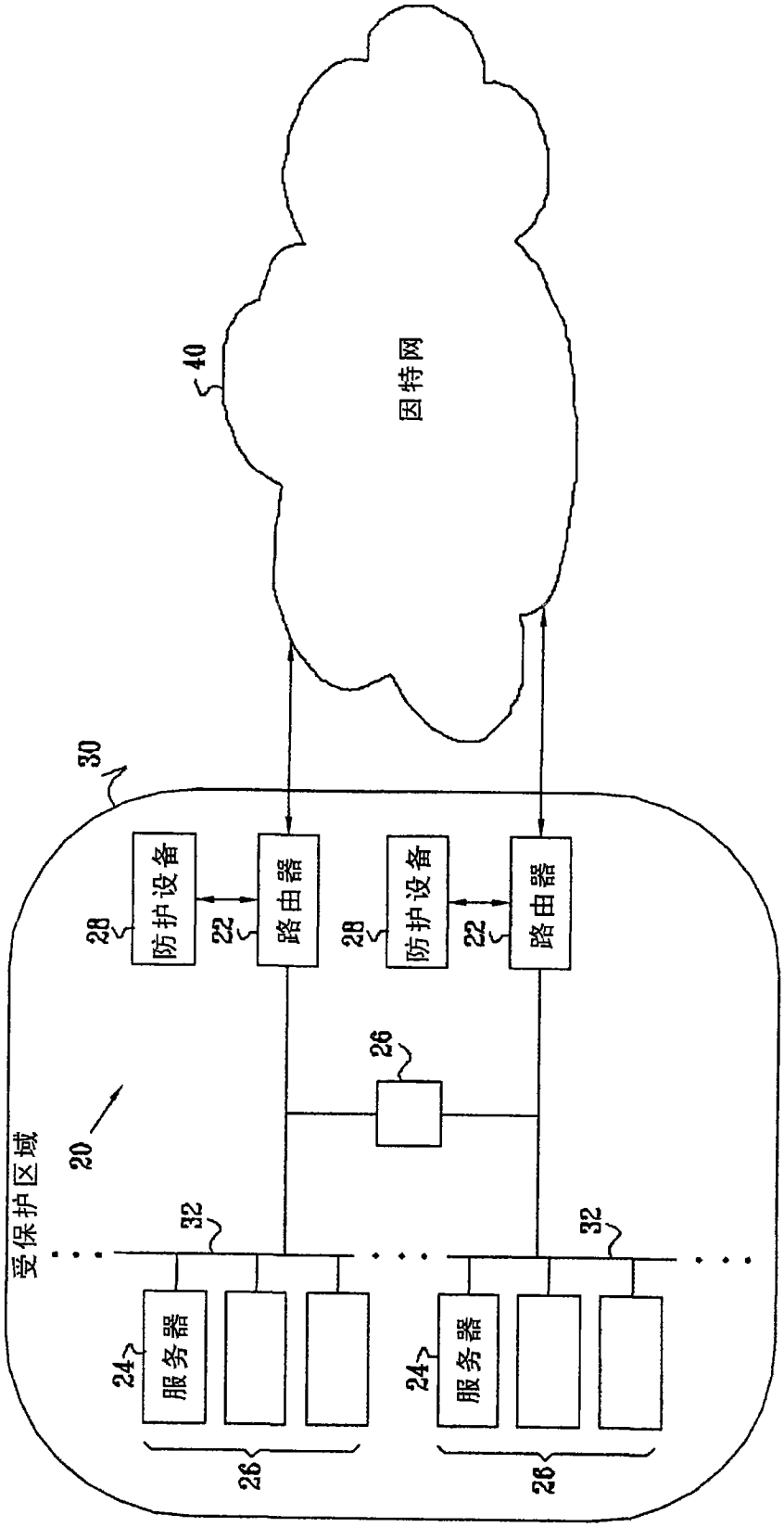

因特网
40
30
防护设备
28
路由器
22
防护设备
28
路由器
22
26
20
受保护区域
32
32
服务器
24
服务器
24
26
26

图1

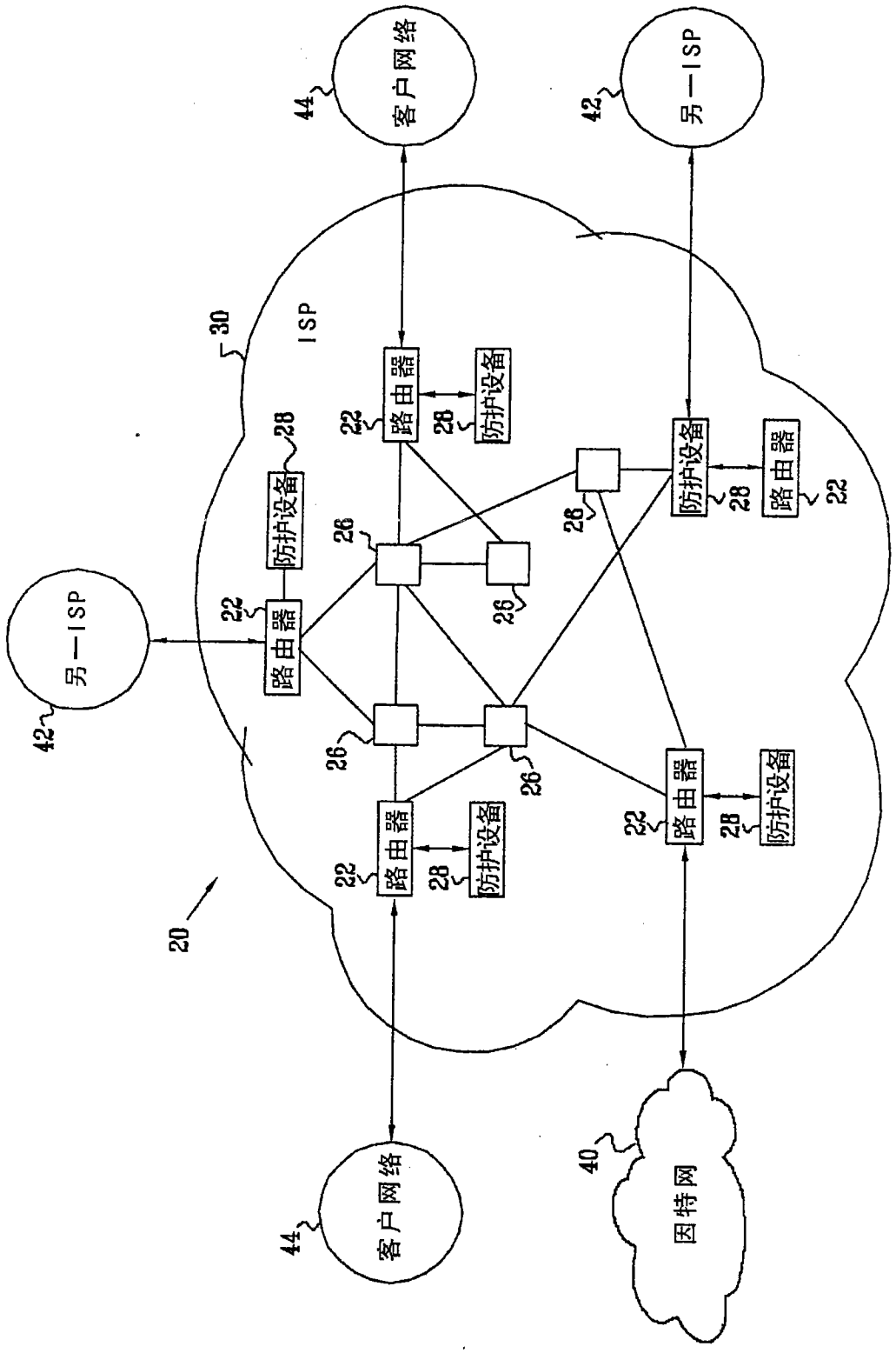


图2

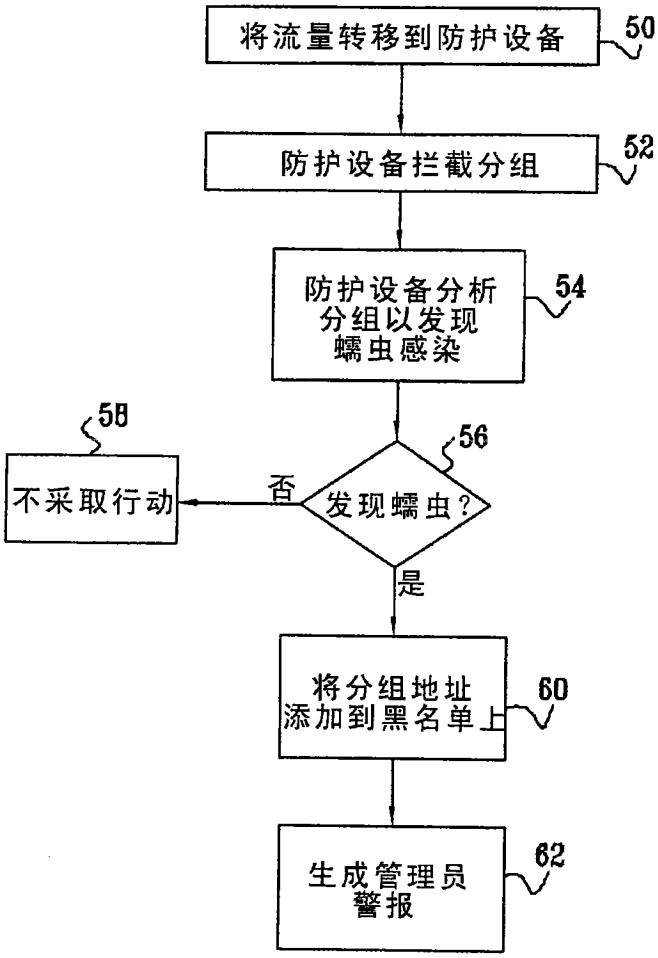

将流量转移到防护设备
50
防护设备拦截分组
52
防护设备分析分组以发现蠕虫感染
54
56
发现蠕虫?
否
58
不采取行动
是
将分组地址添加到黑名单上
60
生成管理员警报
62

图3

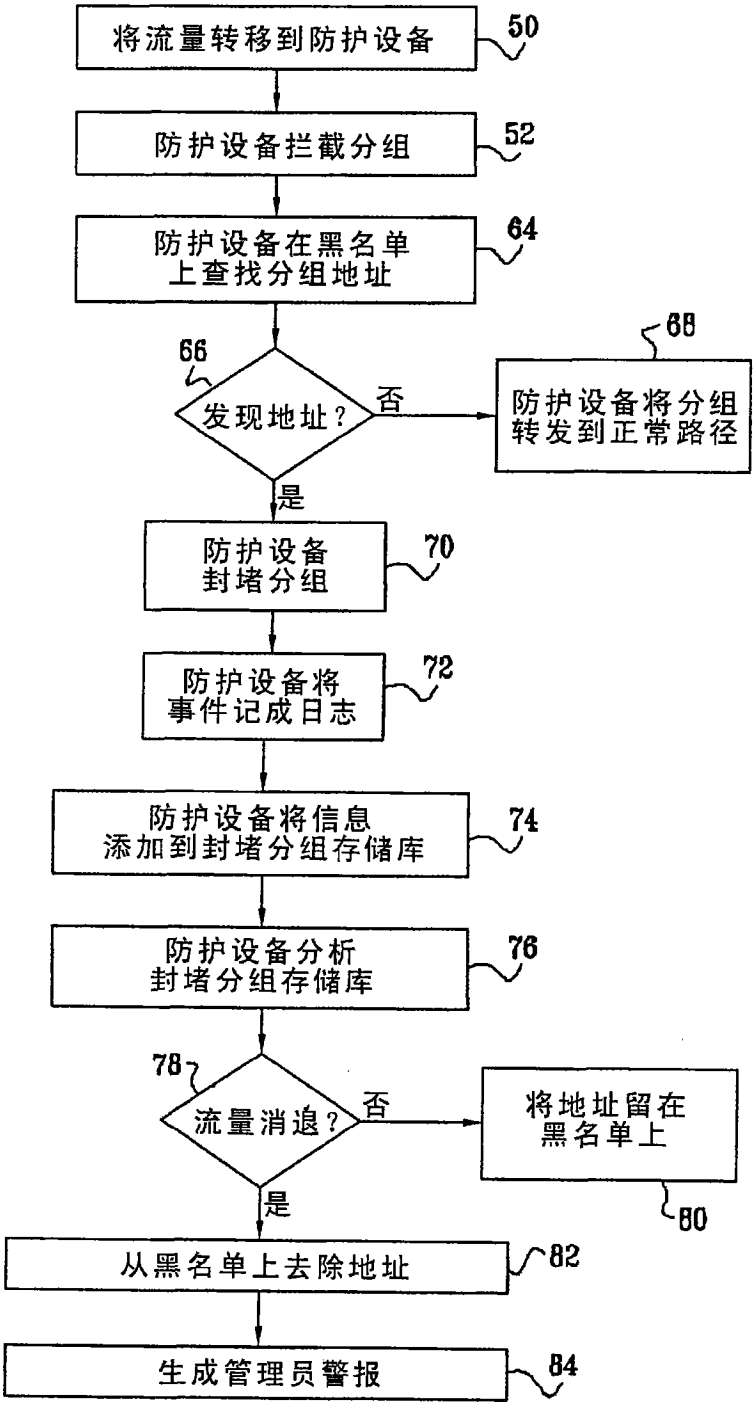

将流量转移到防护设备
50
防护设备拦截分组
52
防护设备在黑名单上查找分组地址
64
66
发现地址？
否
68
防护设备将分组转发到正常路径
是
防护设备封堵分组
70
防护设备将事件记成日志
72
防护设备将信息添加到封堵分组存储库
74
防护设备分析封堵分组存储库
76
78
流量消退？
否
将地址留在黑名单上
80
是
从黑名单上去除地址
82
生成管理员警报
84

图4

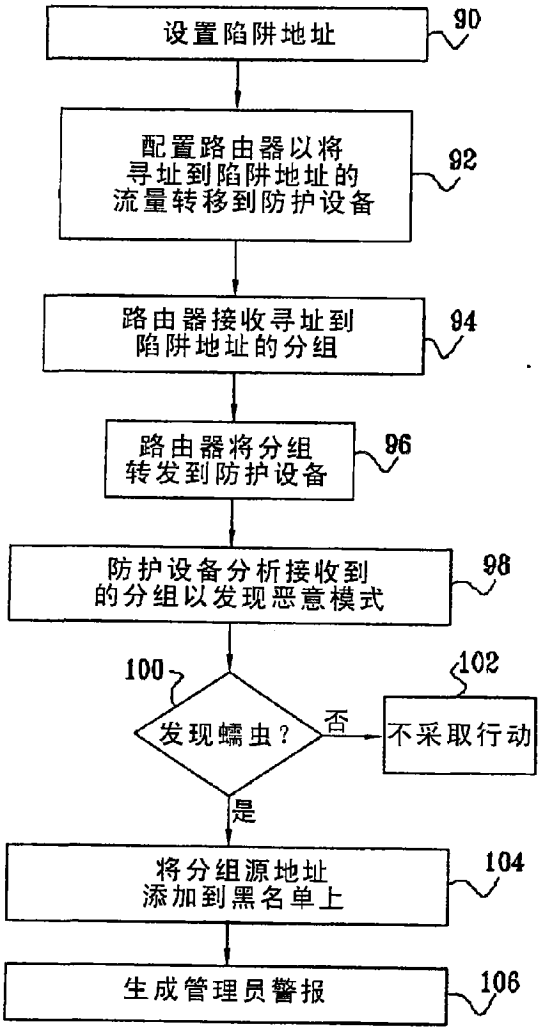

设置陷阱地址
90
配置路由器以将寻址到陷阱地址的流量转移到防护设备
92
路由器接收寻址到陷阱地址的分组
94
路由器将分组转发到防护设备
96
防护设备分析接收到的分组以发现恶意模式
98
100
发现蠕虫？
否
102
不采取行动
是
将分组源地址添加到黑名单上
104
生成管理员警报
106

图5