[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 200680009164.4

[45] 授权公告日 2009 年 11 月 18 日

[11] 授权公告号 CN 100561492C

[22] 申请日 2006.2.21
[21] 申请号 200680009164.4
[30] 优先权
[32] 2005.3.24 [33] EP [31] 05006462.5
[86] 国际申请 PCT/IB2006/050554 2006.2.21
[87] 国际公布 WO2006/100613 英 2006.9.28
[85] 进入国家阶段日期 2007.9.21
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 J·F·赖尔登 D·M·赞波尼
Y·杜邦彻 R·里斯曼
[56] 参考文献
WO2005/015370A1 2005.2.17
EP1330095A1 2003.7.23
WO2004/107706A1 2004.12.9
CN1450758A 2003.10.22
CN1585346A 2005.2.23
审查员 王骞
[74] 专利代理机构 北京市中咨律师事务所
代理人 于静 李峥

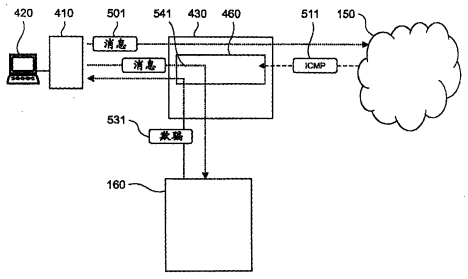
权利要求书 4 页 说明书 10 页 附图 6 页

[54] 发明名称

网络攻击检测的方法和装置

[57] 摘要

提供了一种用于检测数据通信网络上的攻击的方法和装置。所述装置包括路由器，所述路由器具有用于监控寻址于在所述路由器本地的始发用户系统的返回消息的机制。所述机制包括用于标识指定种类的返回消息的消息检验器，以及用于将来自所述始发用户系统的后续消息临时路由至入侵检测传感器的重选路由器。



1. 一种用于检测数据通信网络上的攻击的方法，所述方法包括:

监控（610）寻址于始发用户系统（420）的返回消息（511）;

标识（620）指定种类的返回消息（511）; 以及

将来自相同的始发用户系统（420）的后续消息临时路由（630）至入侵检测传感器（160）。

2. 根据权利要求 1 所述的方法，其中所述入侵检测传感器（160）被选择安排在所述始发用户系统（420）的本地。

3. 根据权利要求 1 或 2 所述的方法，其进一步包括: 所述入侵检测传感器（160）欺骗与所述始发用户系统（420）的交换。

4. 根据权利要求 1 所述的方法，其中所述返回消息（511）与由所述始发用户系统（420）发送至目的地址的消息（501）有关，并且所述临时路由（630）的步骤被应用于从所述始发用户系统（420）到所述目的地址的所有后续消息。

5. 根据权利要求 1 所述的方法，其中选择所述返回消息（511）的指定种类以指示目的地址是不可访问的。

6. 根据权利要求 1 所述的方法，其中选择所述返回消息（511）的指定种类以包括指示失败连接的因特网控制消息协议消息。

7. 根据权利要求 1 所述的方法，其中在预定的时间周期应用所述临时路由（630）。

8. 根据权利要求 1 所述的方法，其进一步包括: 如果已经将指定种类的一数目的返回消息（511）标识为寻址于始发用户系统（420），所述数目超过了预定阈值，则触发所述临时路由（630）。

9. 一种用于检测数据通信网络上的攻击的装置，所述装置包括:

路由器（430），所述路由器（430）包括用于监控寻址于在所述路由器（430）本地的始发用户系统（420）的返回消息（511）的部件（460）; 以及

入侵检测传感器（160）;

其中所述部件（460）包括:

消息检验器，所述消息检验器用于标识指定种类的返回消息（511）；以及

重选路由器，所述重选路由器用于将来自所述始发用户系统（420）的后续消息临时路由至所述入侵检测传感器（160）。

10. 根据权利要求 9 所述的装置，其中所述入侵检测传感器（160）在所述路由器（430）的本地。

11. 根据权利要求 9 或 10 所述的装置，其中所述入侵检测传感器（160）被设计以欺骗与所述始发用户系统（420）的交换。

12. 根据权利要求 11 所述的装置，其中所述入侵检测传感器（160）包括虚拟化基础设施，所述虚拟化基础设施具有各自欺骗服务的多个虚拟传感器（310-315）。

13. 根据权利要求 9 所述的装置，其中所述返回消息（511）与由所述始发用户系统（420）发送至目的地址的消息（500）有关，并且所述重选路由器在从所述始发用户系统（420）到所述目的地址的所有后续消息上操作。

14. 根据权利要求 9 所述的装置，其中所述返回消息（511）的指定种类指示目的地址是不可访问的。

15. 根据权利要求 9 所述的装置，其中所述返回消息（511）的指定种类是指示失败连接的因特网控制消息协议消息。

16. 根据权利要求 9 所述的装置，其中所述重选路由器在预定的时间周期有效。

17. 根据权利要求 9 所述的装置，其中所述重选路由器包括确定器，所述确定器用于确定已被标识寻址于始发用户系统（420）的指定种类的返回消息（510）的数目是否超过了预定阈值。

18. 一种路由器（430），其包括:

用于监控寻址于在所述路由器（430）本地的始发用户系统（420）的

返回消息（511）的部件（460）;

消息检验器，所述消息检验器用于标识指定种类的返回消息（511）;以及

重选路由器，所述重选路由器用于将来自所述始发用户系统（420）的后续消息临时路由至入侵检测传感器（160）。

19. 一种数据通信系统，其包括:

- 网络中的多个数据处理系统;

- 在所述数据处理系统本地的路由器（430），所述路由器（430）用于将消息路由至所述数据处理系统或者路由来自所述数据处理系统的消息;

所述路由器（430）包括用于监控寻址于作为在所述路由器（430）本地的数据处理系统之一的始发用户系统（420）的返回消息（511）的部件（460）;

- 入侵检测传感器（160）;

其中所述部件（460）包括:

消息检验器，所述消息检验器用于标识指定种类的返回消息（510）;以及

重选路由器，所述重选路由器用于将来自所述始发用户系统（420）的后续消息临时路由至所述入侵检测传感器（160）。

20. 一种用于检测数据通信网络上的攻击的设备，该设备包括:

用于监控（610）寻址于始发用户系统（420）的返回消息（511）的装置;

用于标识（620）指定种类的返回消息（510）的装置;以及

用于将来自所述始发用户系统（420）的后续消息临时路由（630）至入侵检测传感器（160）的装置。

21. 根据权利要求20所述的设备，其中所述返回消息（511）与由所述始发用户系统（420）发送至目的地址的消息（501）有关，并且所述用于将来自所述始发用户系统（420）的后续消息临时路由（630）至入侵检

测传感器（160）的装置对从所述始发用户系统（420）到所述目的地址的所有后续消息进行所述临时路由。

22. 根据权利要求 20 或 21 所述的设备，其中所述返回消息（511）的指定种类指示目的地址是不可访问的。

23. 根据权利要求 20 或 21 所述的设备，其中所述返回消息（511）的指定种类是指示失败连接的因特网控制消息协议消息。

24. 根据权利要求 20 或 21 所述的设备，其中所述临时路由（630）用于预定的时间周期。

25. 根据权利要求 20 或 21 所述的设备，进一步包括：如果已被标识为寻址于始发用户系统（420）的指定种类的返回消息（511）的数目超过了预定阈值，则触发所述临时路由（630）的装置。

26. 一种针对来自始发用户系统（420）的入侵而装备客户系统的方法，其包括以下步骤：

将入侵检测传感器（160）连接至路由器（430），

为所述路由器（430）配备以下能力：

- 监控（610）寻址于所述始发用户系统（420）的返回消息（511），
- 标识（620）指定种类的返回消息（511），以及
- 将来自相同的始发用户系统（420）的后续消息临时路由（630）至所述入侵检测传感器（160）。

网络攻击检测的方法和装置

技术领域

本发明涉及检测网络攻击的领域，并且特别涉及检测在攻击始发用户系统本地的数据通信网络上的攻击。

背景技术

因特网是由多个互连的数据网络所形成的广域数据通信网络。在操作中，因特网促进了一系列位于远程的数据处理系统之间的数据通信。通常，连接至因特网的终端用户数据处理系统被称为客户机数据处理系统或简称为客户机。类似地，对网站以及用于由终端用户通过因特网访问的服务进行托管（hosting）的数据处理系统被称为服务器数据处理系统或简称为服务器。存在一种通过终端用户数据处理系统与托管数据处理系统之间的因特网而完成的客户机-服务器关系。

因特网已经成为用于促进消费者、零售商以及服务提供商之间的电子实现的商业交互的重要通信网络。通常通过因特网服务提供商（ISP）向这样的实体提供对因特网的访问。每个 ISP 通常运营客户机预定的开放式网络。每个客户机均具备网络上唯一的因特网协议（IP）地址。类似地，网络上的每个服务器均具备唯一的 IP 地址。由 ISP 运营的网络通过通常被称为路由器的专用数据处理系统而连接至因特网。在操作中，路由器将来自因特网的入站（inbound）通信业务量导向网络上指定的 IP 地址。类似地，路由器将来自网络的出站（outbound）通信业务量导向因特网上指定 IP 地址的方向上。

很多人和商务所面临的问题是对他们使用的网络的电子攻击日益增长的频率。这样的攻击包括计算机病毒攻击以及所谓的“蠕虫”攻击。这类攻击在网络中引起显著的性能降低。连接至网络的受感染系统通常试图在

该网络内传播感染。很多用户并没有意识到其系统受到感染。

已知的入侵检测传感器欺骗（spoof）与潜在攻击者的服务交互。传感器通过欺骗在另外未使用的IP地址处存在机器和服务而发挥作用。由于没有另外使用这些地址，因此指定到这些地址的所有通信量都是先验可疑的（a priori suspicious）。传感器欺骗服务以确定通信量背后的意图。传感器本身提供这样的虚拟化基础设施，即该虚拟化基础设施允许写入单独的传感器，就好像这些传感器正运行在单个主机上一样。

WO 2004/107706 公开了一种用于检测数据通信网络上的攻击的入侵检测传感器（IDS）。IDS标识起始于任何分派的地址并且寻址于任何未分派的地址的、该网络上的数据业务量，针对表示攻击的数据而检查如此标识的数据业务量，并且如果需要的话，生成报警信号。

该上下文中使用术语“未分派的”作为对没有被分派给除了用于检测入侵或生成攻击签名的装置之外的物理设备的地址的涵盖。为了执行WO 2004/107706中所公开的方法而设计的装置是这样的设备，即那些“未分派的”地址实际被分派给了该设备以便利用该方法。那些地址在一定范围内未分派，是因为没有将它们分派给除了签名生成或入侵检测之外还具有另外的功能性的任何设备。

在上述IDS中，一块未分派的地址被指定给IDS，从而使得IDS可以欺骗对于到这些未分派地址的任何数据业务量的响应。此外，IDS可能在地理上远离数据业务量的始发用户系统而使其难于针对始发用户系统采取措施。

发明内容

本发明的目的是提供一种用于检测对未使用或不可访问的地址的攻击的系统。进一步的目的是提供本地问题的本地报告。另外，可以对攻击实体透明实现所述检测。

根据本发明的第一方面，提供了一种用于检测数据通信网络上的攻击的方法，该方法包括：监控寻址于始发用户系统的返回消息；标识指定种

类（**specified nature**）的返回消息；以及将来自所述始发用户系统的后续消息临时路由至入侵检测传感器。将术语“指定种类”理解为具有特定特性或属于预定类型的消息。也被称为消息检验器的监控装置充当检查所述返回消息是否具有所述特定特性的滤波器。如果识别出所述返回消息具有所述消息检验器正在寻找的特性，则所述返回消息受到重新路由。所述消息检验器因此可以被看作返回消息类型操作的开关。与此同时所述消息检验器可以检查不同的特定特性，并且如果发现存在那些特性中的一个或多个，则进行所述重新路由。

优选地，所述入侵检测传感器在所述始发用户系统的本地，即，所述入侵检测传感器连接至与所述始发系统相同的网络。术语“网络”在文中被理解为网络单元的集合，所述网络的边界由边界路由器或边缘路由器表示。这些路由器处理通往其它网络的连通性。网络可以是子网络或更大的网络。所述入侵检测传感器可以欺骗与所述始发用户系统的交换。以这样的方式，在发送至不可访问的地址的消息的始发用户系统本地的入侵检测传感器可以确定所述始发用户系统的意图的种类。换句话说，本发明允许检测和报告较为靠近攻击实体的攻击。

所述返回消息可以与由所述始发用户系统发送至目的地址的消息有关，并且所述临时路由的步骤可以将从所述始发用户系统导向所述目的地址的所有后续消息重新路由至所述入侵检测传感器。

所述返回消息的指定种类可以指示目的地址是不可访问的。例如，所述返回消息的指定种类可以是指示失败连接的因特网控制消息协议消息。

可以在预定的时间周期应用所述临时路由，此后重新开始正常的路由。所述方法还可以包括：如果已被标识为寻址于始发用户系统的指定种类的返回消息的数目超过了预定阈值，则触发所述临时路由。然后该阈值将可用于区分无害通信量与诸如垃圾邮件的有害通信量。

根据本发明的第二方面，提供了一种用于检测数据通信网络上的攻击的装置，所述装置包括：路由器，所述路由器包括用于监控寻址于在所述路由器本地的始发用户系统的返回消息的机制；以及入侵检测传感器；其

中所述机制包括：用于标识指定种类的返回消息的消息跟踪器；以及用于将来自所述始发用户系统的后续消息临时路由至所述入侵检测传感器的装置。

优选地，所述入侵检测传感器在所述路由器的本地。所述入侵检测传感器可以包括用于欺骗与所述始发用户系统的交换的装置。所述入侵检测传感器可以包括虚拟化基础设施，所述虚拟化基础设施具有各自欺骗服务的多个虚拟传感器。

根据本发明的第三方面，提供了一种路由器，其包括：用于监控寻址于在所述路由器本地的始发用户系统的返回消息的机制；用于标识指定种类的返回消息的装置；以及用于将来自所述始发用户系统的后续消息临时路由至入侵检测传感器的装置。

根据本发明的第四方面，提供了一种数据通信系统，其包括：网络中的多个数据处理系统；在所述数据处理系统本地的路由器，用于将消息路由至所述数据处理系统或者路由来自所述数据处理系统的消息；所述路由器包括一种机制，所述机制用于监控寻址于作为在所述路由器本地的数据处理系统之一的始发用户系统的返回消息；以及入侵检测传感器；其中所述机制包括：用于标识指定种类的返回消息的装置；以及用于将来自所述始发用户系统的后续消息临时路由至所述入侵检测传感器的装置。

根据本发明的第五方面，提供了一种计算机程序元件，其包括计算机程序代码装置，当加载到数据处理系统的处理器中时，所述计算机程序代码装置配置所述处理器以实现包括以下步骤的方法：监控寻址于始发用户系统的返回消息；标识指定种类的返回消息；以及将来自所述始发用户系统的后续消息临时路由至入侵检测传感器。

当来自始发用户系统的过程尝试联系未使用或不可访问的地址（例如，防火墙后面的地址）时，ICMP（因特网控制消息协议）消息被返回给在所述始发用户系统本地的路由器，告知所述始发用户系统目的地不可到达以及关于原因的一些细节。该消息被所述始发用户系统本地的路由器截获，并且来自所述始发用户系统的所有通信量都通过 IDS 被临时路由。

附图说明

现在将参照附图，仅通过例子来描述本发明的实施例，其中：

图 1 是现有技术中已知的数据处理系统的框图；

图 2 是示出了已知的入侵检测传感器的实施例的数据处理网络的框图；

图 3 是已知的入侵检测传感器的框图；

图 4 是依照本发明的数据处理网络的框图；

图 5 是示出了依照本发明重新路由消息的图 4 的数据处理网络的细节；以及

图 6 是依照本发明的方法或重新路由的流程图。

具体实施方式

首先参照图 1，数据处理系统包括中央处理器（CPU）10、输入/输出（I/O）子系统 20，以及存储子系统 40，其全部通过总线子系统 30 互连。存储子系统 40 可以包括随机访问存储器（RAM）、只读存储器（ROM），以及一个或多个数据存储设备，例如硬盘驱动器、光盘驱动器等。I/O 子系统 20 可以包括：显示器；打印机；键盘；诸如鼠标、跟踪球等的指点设备；以及准许通过数据通信网络在数据处理系统与一个或多个类似系统和/或外围设备之间通信的一个或多个网络连接。由这样的网络互连的这样的系统和设备的组合本身可以形成分布式数据处理系统。这样的分布式系统可以通过附加的数据通信网络自我互连。

在存储子系统 40 中存储了数据 60 以及可由 CPU 10 执行的计算机程序代码 50。程序代码 50 包括操作系统软件 90 以及应用软件 80。当由 CPU 10 执行时，操作系统软件 90 提供可以在其上执行应用软件 80 的平台。

现在参照图 2，其利用入侵检测传感器（IDS）的实施例示出了对因特网体系结构的示例摘取。在示例体系结构中示出了两个数据通信网络 100、200。应当理解这是示例体系结构并且可以提供很多不同形式的数据通信网

络。

图 2 示出了第一数据通信网络 100，其具有用于分派给第一网络 100 中的数据处理系统 120 的多个地址 110，以及第二数据通信网络 200，其具有用于分派给第二网络 200 中的数据处理系统 220 的多个地址 210。网络 100、200 可以作为具有多个可分派的因特网协议（IP）地址 110、210 的因特网服务设备。网络 100、200 各自通过路由器 130、230 连接至因特网 150。

通过对以数据分组的形式在因特网 150 与网络 100、200 之间路由通信业务量的任务进行适当的编程，可以以如文中之前参照图 1 专门描述的数据处理系统的形式实现路由器 130、230，其中路由器 130、230 基于在数据分组中指定的 IP 地址数据连接至网络 100、200。

在第一数据通信网络 100 中，存在分派给属于因特网服务的用户的系统 120 的 IP 地址 110。每个系统 120 可以是如文中之前参照图 1 所描述的数据处理系统。网络 100 上的第二组 IP 地址 140 是空闲的。更具体而言，第二组 IP 地址 140 没有被分派给用户系统。入侵检测传感器（IDS）160 连接至网络 100。IDS 160 还连接至路由器 130。

诸如蠕虫或其它攻击的过程 240 可以源自第二数据通信网络 200 上的用户系统 220。过程 240 可以寻址于其它网络 100 上宽范围选择的地址。如果过程 240 寻址于未分派的地址，例如未被分派给用户系统的、第一网络 100 上的第二组 IP 地址 140 之一，则将过程 240 路由至欺骗对过程 240 的回复并且发出警报的 IDS 160。

图 3 中较为详细的示出了 IDS 160 的示例内部体系结构。其它形式的 IDS 是已知的并且可以在本发明中使用。IDS 160 通过欺骗在另外未使用的 IP 地址处存在机器和服务而进行操作。因为 IP 地址未被另外使用，所以指定到这些地址的所有通信量都是先验可疑的。IDS 160 欺骗服务，而不是仅仅记录所尝试的连接，以便确定通信量背后的意图。

IDS 160 建立于不提供超出受限登录之外的真实服务的高安全性（security-hardened）机器之上。IDS 160 提供这样的虚拟化基础设施 310，

即该虚拟化基础设施310允许操作单独的传感器311-315，就好像它们正在单个主机上运行一样。基于允许对由虚拟传感器311-315的数目而产生的大量数据进行相关和分析的关系数据库330，其还提供了登录基础设施320。由虚拟传感器311-315提供的服务可以包括超文本传输协议(HTTP)、微软的分布式构件对象模型（Microsoft's Distributed Component Object Model）、结构化查询语言（Structured Query Language）以及Windows文件共享和打印（SMB）。

参照图4，在本发明的示例实施例中，提供了具有用户系统420的第一数据通信网络400，该用户系统420具有IP地址410，由此地址始发诸如恶意蠕虫过程的过程440。过程440可以寻址于其它网络（例如图4中所示出的第二网络500）上的用户系统520的一系列IP地址510。

过程440可以寻址于未使用或不可访问（例如，在防火墙后面）的IP地址540。如果是这种情况，则从在不可访问的地址本地的路由器530返回ICMP（因特网控制消息协议）消息，在该例中是第二网络500的路由器530。ICMP消息寻址于过程440的始发用户系统420，指示目的地不可到达以及关于原因的一些细节。

提供了一种机制以便在始发用户系统420本地的路由器430处捕获ICMP消息。ICMP消息告知在始发用户系统420本地的路由器430：从始发用户系统420到目的地的所有业务量都应当被给予本地入侵检测传感器（IDS）160或者通过本地入侵检测传感器（IDS）160而被路由。本地IDS 160然后可以与始发用户系统420交互以确定导致尝试连接的根源。

每个网络400、500均具有其路由器430、530，该路由器管理因特网150上的业务量。路由器打开数据的IP分组以读取目的地址，计算最佳路由，并且然后向其最终目的地发送分组。如果目的地与发送计算机在相同的网络上，则路由器直接向目的计算机发送分组。如果分组要前往本地网络外部的目的地，则路由器改为向更靠近目的地的另一路由器发送分组。该路由器接着向更靠近的路由器发送分组，直到该分组到达其最终目的地。

路由器430、530具有两个或更多的物理端口：输入端口和输出端口。

当输入端口接收到分组时，运行被称为路由过程的软件例程。该过程向内察看 IP 分组中的报头信息，并且找到正向其发送数据的地址。然后其将该地址与内部数据库进行比较，该内部数据库被称为路由表，其具有关于应当将具有各种 IP 地址的分组发送到的端口的详细信息。基于其在路由器表中找到的内容，路由器将分组发送至特定的输出端口，该输出端口将数据发送至下一路由器或其目的地。

因特网的操作是由路由器监控的，并且当不能够完成连接时，由 ICMP（因特网控制消息协议）报告该事件。定义了各种不同类型的 ICMP 消息并且每种消息类型均被封装在 IP 分组中。例如，当子网络或路由器不能够定位主机目的地时，使用“目的地不可到达”消息，并且当不能够定位目的地的网络时，使用“网络不可到达”消息。

参照图 5，在本发明的示例实施例中，路由器 430 中的重选路由机制 460（也被称为重选路由器（rerouter））标识正返回给在路由器 430 本地的 IP 地址 410 的消息的种类。具有始发 IP 地址 410 的始发用户系统 420 向目的地址发送消息 501。如果返回消息 511 被机制 460 标识为指示不可到达的目的地的 ICMP 消息，则机制 460 建立临时路由 541 以便将寻址于该不可到达的目的地的业务量从始发 IP 地址 410 导向在路由器 430 本地的 IDS 160。这里机制 460 可以包括能够分析所截获的返回消息 511 的种类并且标识属于指定种类的那些消息的消息检验器。该标识就像不影响不属于指定种类的返回消息的滤波器一样工作。其它消息 511 由重选路由器重新路由至 IDS 160。重选路由器不需要单独的硬件设备。依照策略重新路由返回消息 511 可以是路由器 430 的一种功能性。路由器 430 可以运行一个或多个策略来确定重定向和重新路由的种类。例如，只有在监控类型的返回消息 511 的数目超过预定阈值的情况下，重定向才会发生。可以将临时路由 541 定时成持续预定的时间周期，例如 30 秒。

响应于消息 501，由因特网 150 中的远程路由器将 ICMP 消息 511 返回至在始发用户系统 420 本地的路由器 430。机制 460 截获该 ICMP 消息 511。由于返回消息 511 被标识成属于指定种类，即这里指示不可到达的目

的地，因此机制 460 将进行重新路由，以便从始发用户系统 420 到目的地的所有业务量都被给予本地 IDS 160 或者都通过本地 IDS 160 而被路由。机制 460 建立临时路由 541，以便将从始发 IP 地址 410 发送至不可访问的地址的任何后续消息重新路由至 IDS 160。IDS 160 可以通过假装是不可访问的地址来欺骗与始发用户系统 420 的交换 531。IDS 160 然后可以确定始发用户系统 420 到不可访问的地址的尝试联系的种类，并且如果该尝试联系是恶意的，则可以在相同的路由器网络内本地发出警报。

图 6 示出了在路由器 430 处的机制 460 的过程 600 的流程图。过程 600 涉及机制 460，该机制 460 监控 610 寻址于始发用户系统的返回消息 511、标识 620 指定种类的返回消息 511，以及将来自始发用户系统 420 的后续消息临时路由 630 至入侵检测传感器 160。IDS 160 可以是如文中之前所描述的传感器，其欺骗对始发用户系统 420 的回复。

除了常规 IDS 的所有优点之外，该机制更为准确地传递更为本地的警报，因此降低了对重分布体系结构的需要。这直接解决了有效检测本地网络中受感染的机器的问题（这对本地网络管理员是有价值的信息），而不检测远程受感染的系统（本地网络管理员对此无能为力）。所以本发明允许检测更靠近入侵者的入侵，从而允许负责包括该入侵者的域的网络管理员通过适当的动作对该入侵作出反应。入侵检测的位置越靠近入侵者，管理员就能够越好地进行这样的动作。

另一优点在于不同网络上现有的每个未使用或不可访问的地址均会导致返回的 ICMP 消息 511。因此，不需要将未使用的地址分派给 IDS。该机制依赖于返回的 ICMP 消息 511，其指示目的地址是不可访问的。

本发明通常作为计算机程序产品来实现，其包括用于控制计算机或类似设备的程序指令集。这些指令可以被提供预加载到系统中或记录到诸如 CD-ROM 的存储介质上，或者可提供用于通过诸如因特网或移动电话网的网络下载。

本发明还可以通过向接受服务的实体（也被称为客户系统）提供服务的服务实体来实现。该服务可以是以下中的一个或多个：在接受服务的实

体的环境中或者为接受服务的实体的环境安装根据本发明的设备或系统、部署可用于在其上实现的基础设施，特别是部署或集成计算基础设施，包括将计算机可读代码集成到计算系统中，其中结合计算系统的代码能够实现根据本发明的方法。在本发明的上下文中，服务实体可以针对来自始发用户系统的入侵来装备客户系统。由此，服务实体可以在接受服务的实体的网络中提供对受感染机器的高效检测或者检测攻击接受服务的实体的网络的受感染机器。装备方法可以包括以下步骤：将入侵检测传感器 160 连接至路由器 430，为路由器 430 配备以下能力：监控 610 寻址于始发用户系统 420 的返回消息 511、标识 620 指定种类的返回消息 511，以及将来自相同的始发用户系统 420 的后续消息临时路由 630 至所述入侵检测传感器 160。IDS 160 可以是由服务实体拥有或租用的装备。特别地，服务实体可以同时为几个接受服务的实体使用该 IDS 160，从而共享该资源。这具有的优点在于，在 IDS 160 上进行的关于入侵可检测性性能的更新对所有连接的接受服务的实体具有其影响。另一优点在于可以对接受服务的实体透明实现该服务。

在不背离本发明的范围的情况下可以对前述内容进行改进和修改。

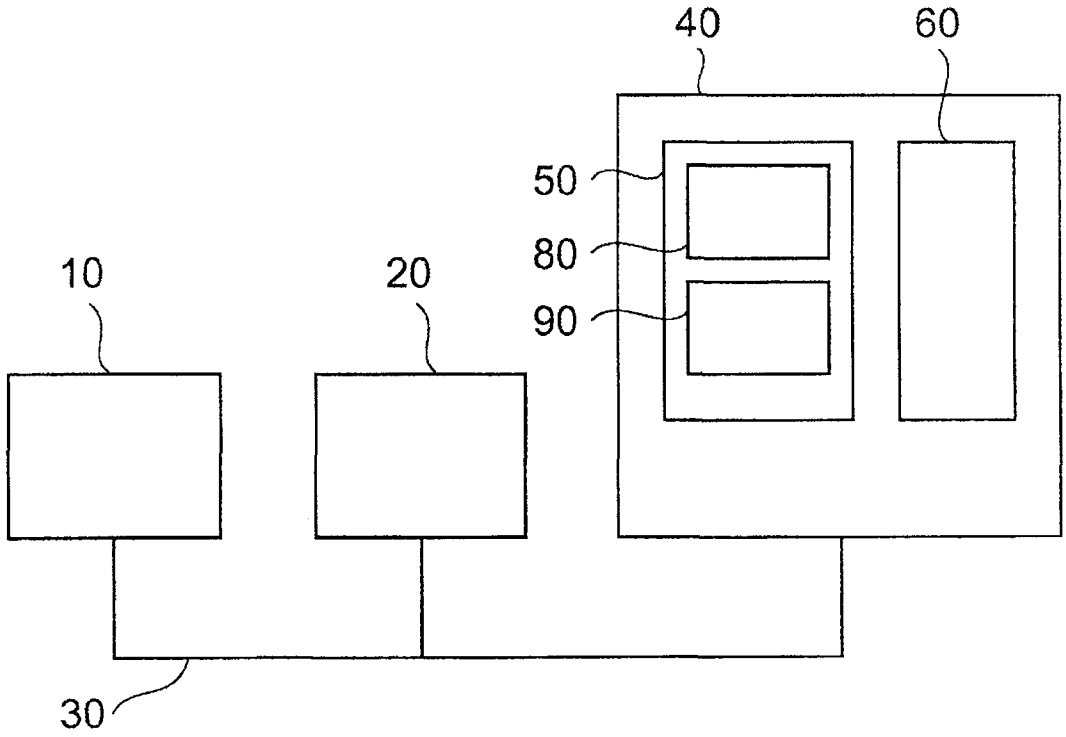


图 1

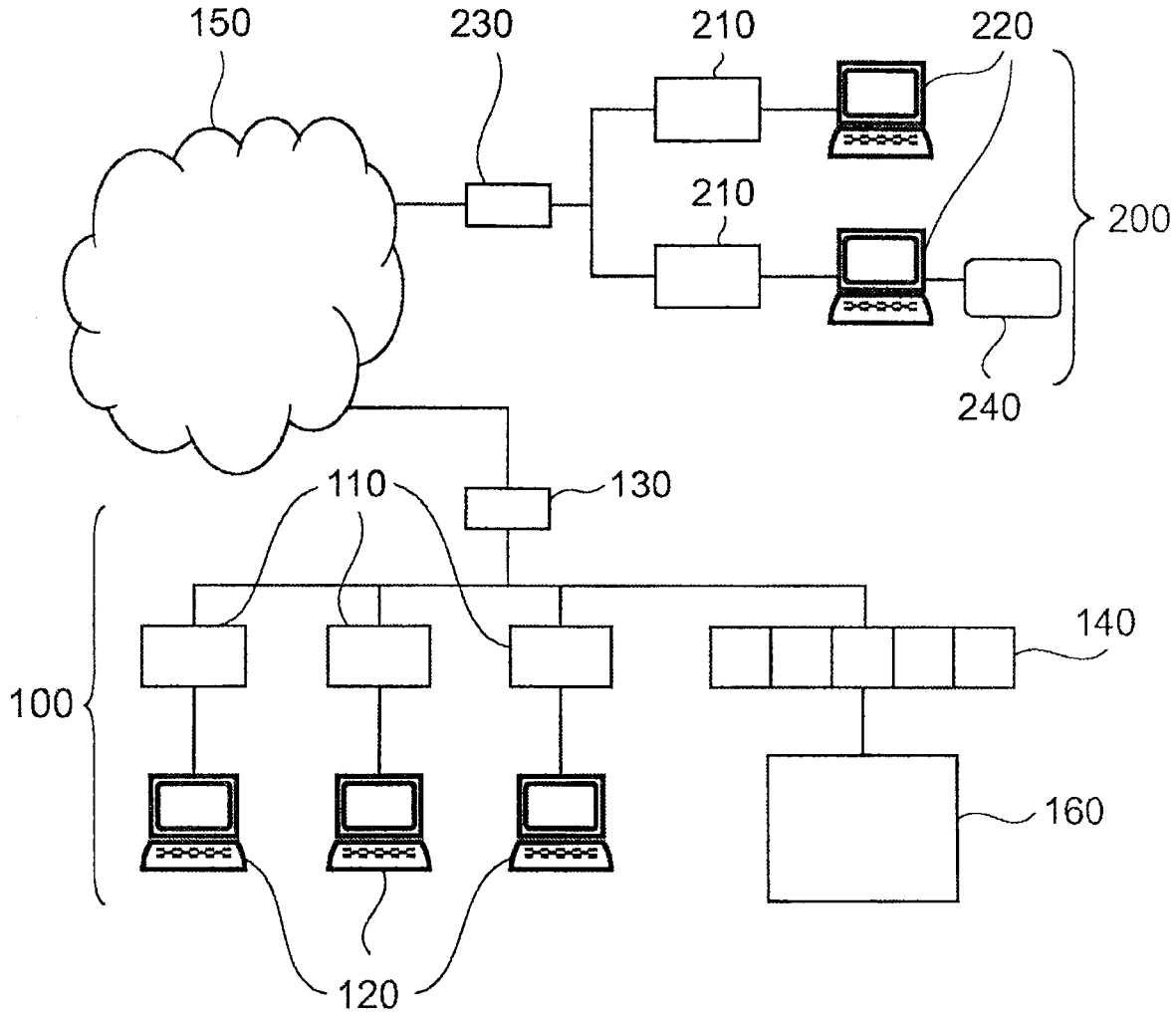


图 2

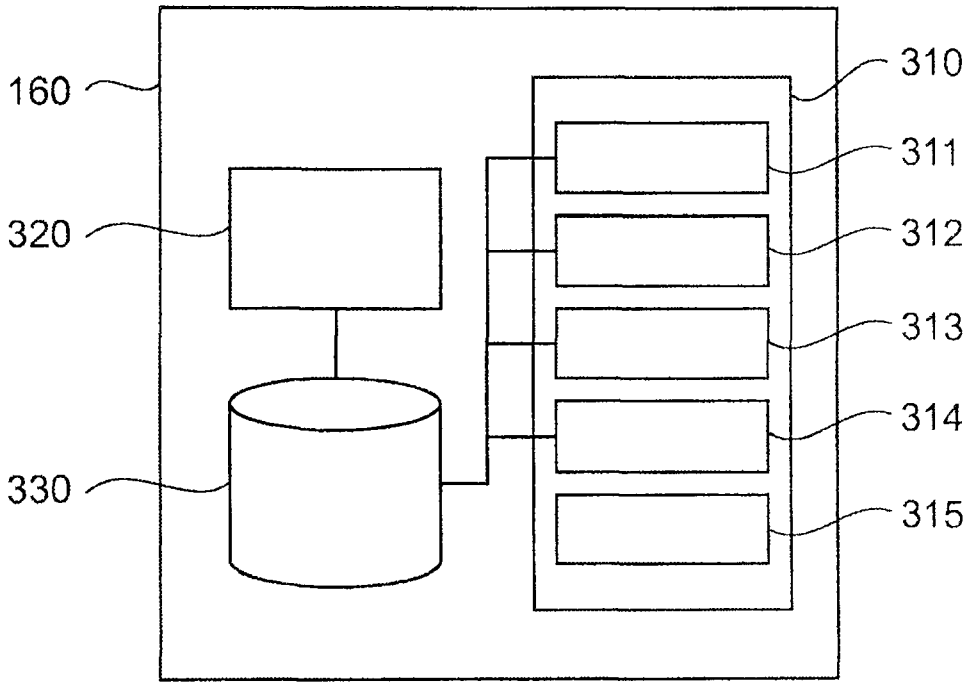


图 3

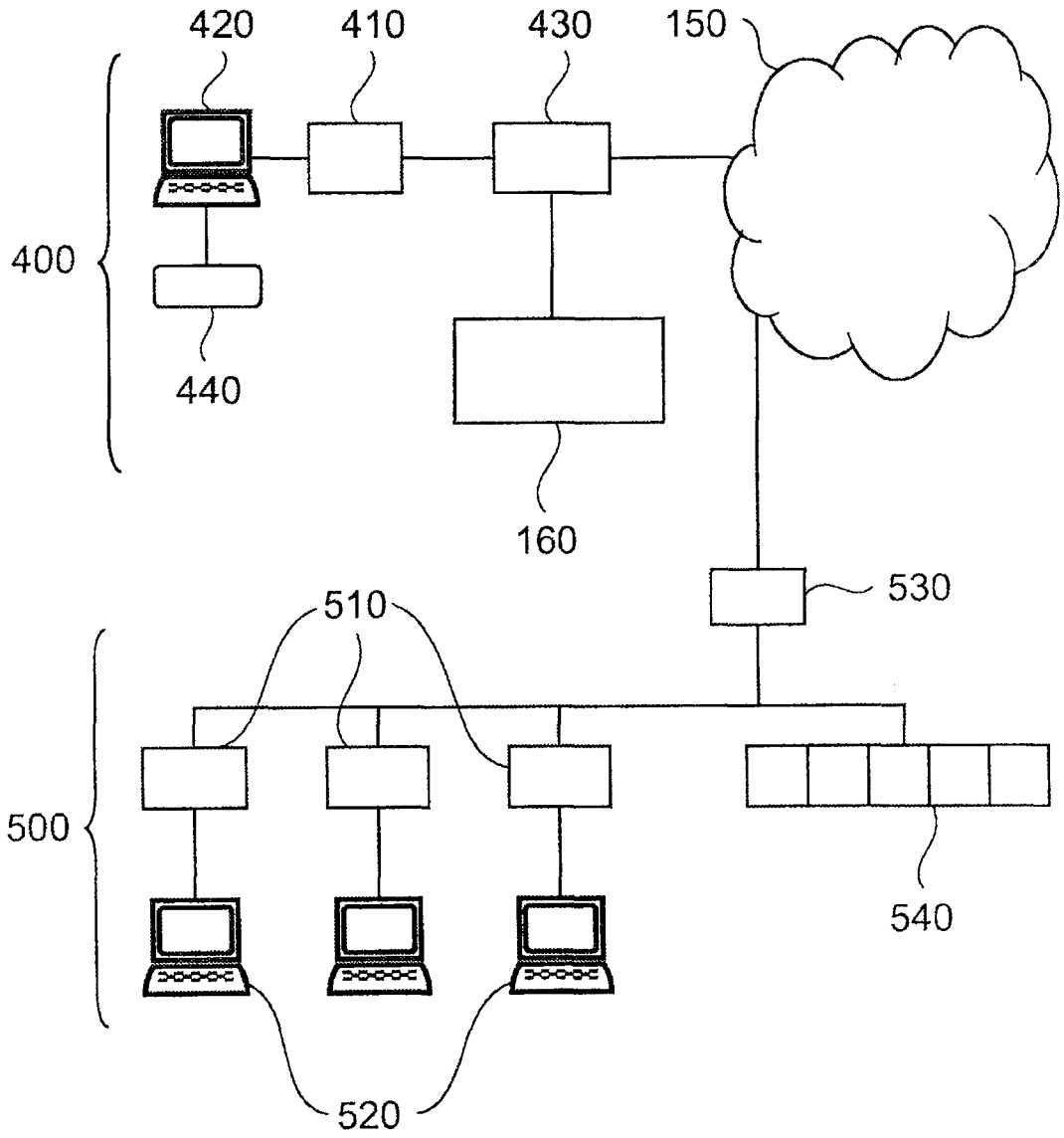


图 4

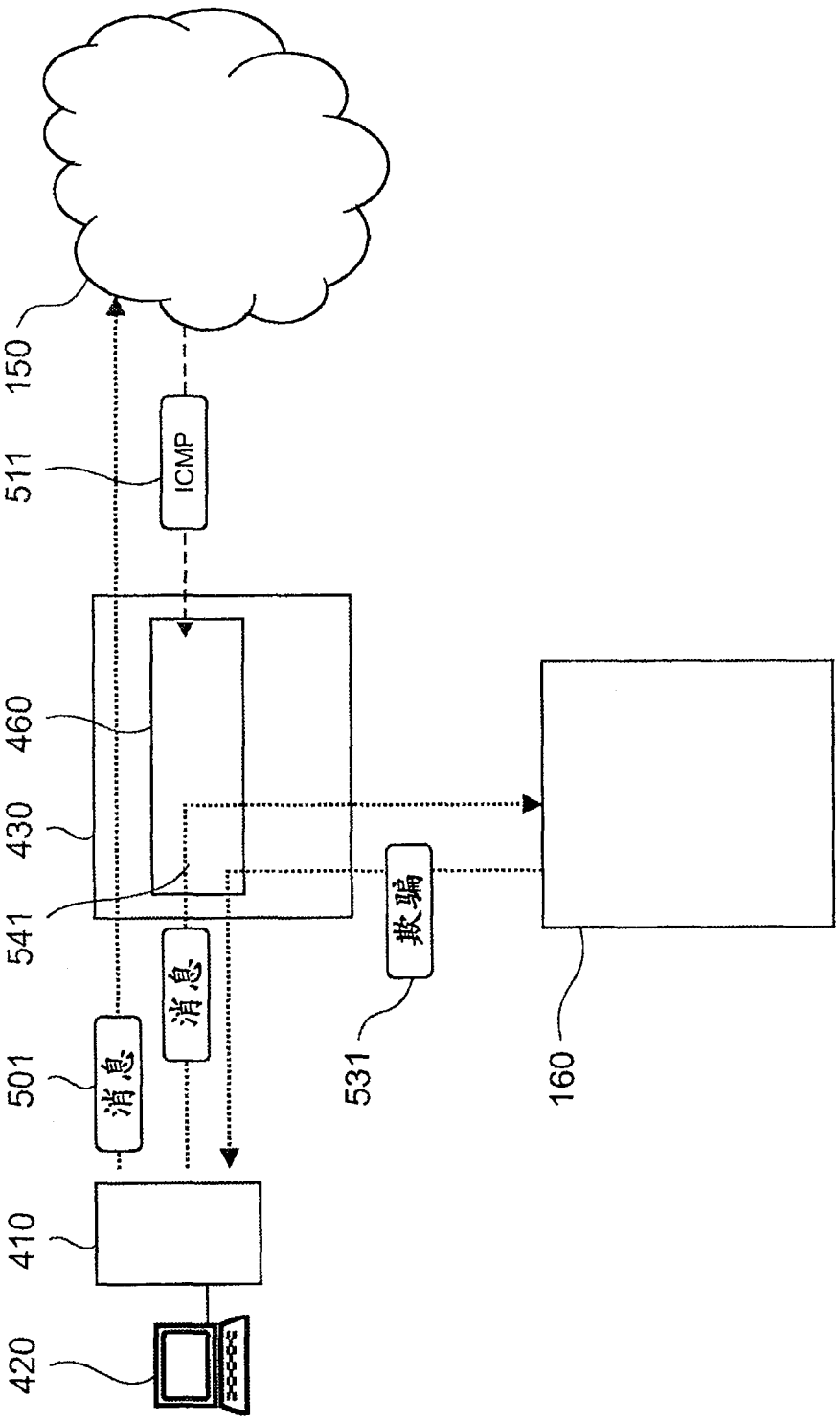


图 5

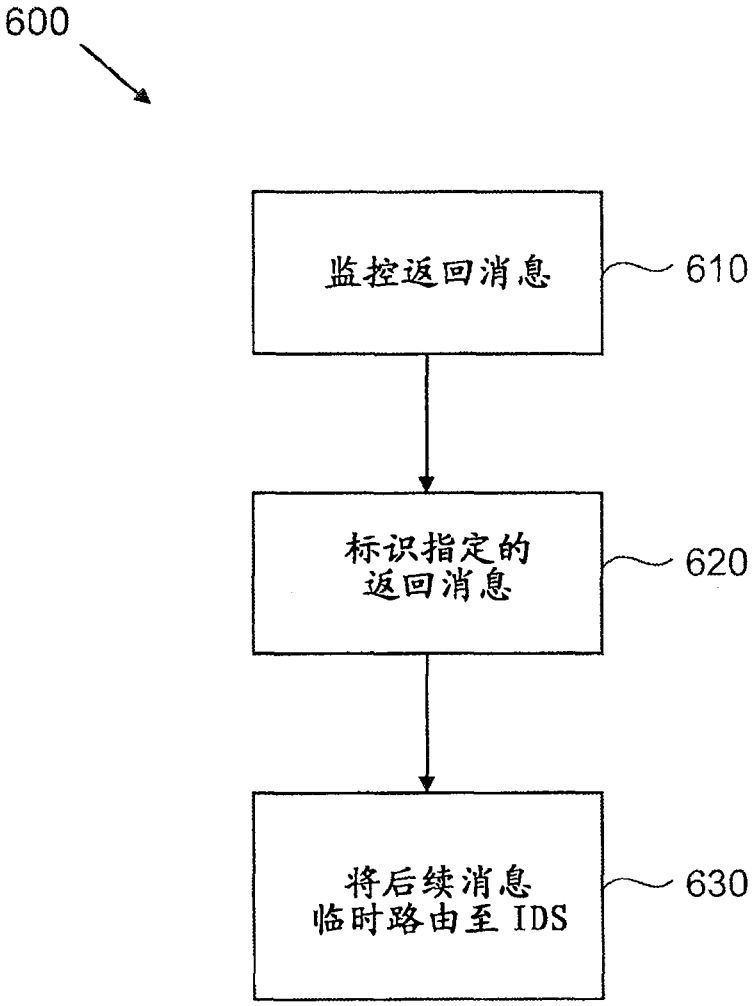


图 6