[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/00

[12] 发明专利说明书

[21] ZL 专利号 99115957.8

[45] 授权公告日 2004 年 3 月 10 日

[11] 授权公告号 CN 1141657C

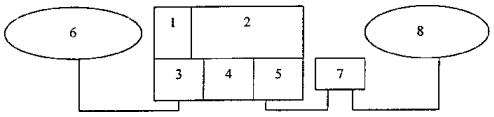
[22] 申请日 1999.12.29 [21] 申请号 99115957.8
[71] 专利权人 西安交通大学
地址 710049 陕西省西安市咸宁路 28 号
[72] 发明人 钱德沛 陆月明 刘 轶 王 磊 徐 斌
审查员 齐 霁

[74] 专利代理机构 西安通大专利代理有限责任公司
代理人 陈翠兰
权利要求书 1 页 说明书 5 页 附图 2 页

[54] 发明名称 基于透明网络地址翻译的防火墙代理网关

[57] 摘要

本发明公开了一种基于透明网络地址翻译的防火墙代理网关，网关是基于 PC 平台，通信连接采用系统总线；包括一个主板，主板内存中运行有 Web 服务器软件和 IP 地址翻译软件，主板上还连接有 100/10Mbps 的以太网接口卡、以太网卡接口卡和专用硬卡；网关内通过以太网接口卡连接内部私有网，网关外通过以太网卡接口卡连接路由器，通过路由器接入 Internet 网；该网关采用硬卡储存权限表和流量表信息，电池保护信息等措施，避免了存盘过程，保证了活动信息不丢失，解决了网关中用户权限不断变化和实时流量统计与查询的特殊情况。 可以解决国内/外 IP 地址块的区分、实时流量的统计和查询、内外网络 IP 地址的翻译和防火墙功能的实现。



ISSN1008-4274

知识产权出版社出版

1．基于透明网络地址翻译的防火墙代理网关，网关是基于 PC 平台，通信连接采用系统总线；包括一个主板，其特征在于，主板内存中运行有 Web 服务器软件（1）和 IP 地址翻译软件（2），主板上还连接有 100/10Mbps 的以太网接口卡（3）、以太网接口卡（5）和专用硬卡（4）；网关内通过以太网接口卡（3）连接内部私有网（6），网关外通过以太网卡接口卡（5）连接路由器（7），通过路由器（7）接入 Internet 网（8）；

Web 服务器软件（1）运行在网关上，Web 服务器软件（1）和以太网接口卡（3）的接收和发送缓冲区通信，Web 服务器软件（1）采用 CGI 程序与专用硬卡（4）的总线缓冲和锁存器（9）、缓冲器（14）、缓冲电路（15）和译码电路（16）通信；Web 服务器软件（1）允许内部的私有网（6）的用户访问 Web 服务器的页面，允许私有网（6）的用户通过网关上的 CGI 程序查询费用、修改访问权限、维护帐户等；

IP 地址翻译软件（2）与以太网接口卡（3）和以太网接口卡（5）的缓冲区、专用硬卡（4）通信；用于实现内部私有网 IP 地址的翻译与代理、包过滤、包转发、路由等功能；

以太网接口卡（3）和以太网接口卡（5）用于接收和发送数据帧；

专用硬卡（4）包括总线缓冲和锁存器（9）、译码电路（10）、存储器（11）、缓冲器（14）、缓冲电路（15）、译码电路（16）、电平监视电路（12）和可充电电池（13）；总线缓冲和锁存器（9）通过数据线和译码电路（10）相连，译码电路（10）通过控制线和地址线与存储器（11）相连，存储器（11）采用译码电路与缓冲器（14）、缓冲电路（15）相连，可充电电池（13）和电平监视电路（12）分别接入存储器（11）；

专用硬卡（4）通过数据线、地址线和控制线与网关通信，实现用户访问权限表、流量表等动态信息的存取和断电自动保存，权限表的解释，用户帐户的定位和维护等功能。

基于透明网络地址翻译的防火墙代理网关

本发明涉及一种网关，特别涉及一种基于透明网络地址翻译的防火墙代理网关。

目前，由于国内外防火墙在收费、访问控制、网络安全控制、信息安全控制等模式和国内/外 IP 地址块的区分和基于其上的访问控制在国内外防火墙很难实现，效率相当低。国内现在也开发了一些防火墙能实现区分国内/外 IP 地址块和基于其上的访问控制和计费，但都基于主机，采用软件实现，性能低，同时存在着活动信息不能很好保存，流量统计与查询达不到实时等问题。

本发明的目的在于克服上述现有技术的缺点，提出一种基于透明网络地址翻译的防火墙代理网关，采用硬卡实现活动信息断电自动保存、用户帐户的自动定位和维护以及用户权限的硬件解释，采用 IP 地址翻译软件和硬卡配合实现内部私有 IP 地址的代理，采用包过滤软件和硬卡结合实现防火墙功能，它可以解决国内/外 IP 地址块的区分、实时流量的统计和查询、内外网络 IP 地址的翻译和防火墙功能的实现。

图 1 是基于透明网络地址翻译的防火墙代理网关的结构示意图；

图 2 是本发明的硬卡结构示意图；

图 3 是网关两边的吞吐量之和与网关每包时延平均值的关系图；

图 4 是网关两边的吞吐量之和与代理网关吞吐量的关系图。

下面结合附图对本发明的结构原理作详细说明。

基于透明网络地址翻译的防火墙代理网关的结构如图 1，由 1～8 个单元组成，包括一个主板，其特点是，主板内存中运行有 Web 服务器软件 1 和 IP 地址翻译软件 2，主板上还连接有 100/10Mbps 的以太网接口卡 3、以太网卡接口卡 5 和专用硬卡 4；网关内通过以太网接口卡 3 连接内部私有网 6，网关外通过以太网卡接口卡 5 连接路由器 7，通过路由器 7 接入 Internet 网 8；

Web 服务器 1 允许内部的私有网 6 的用户访问 Web 服务器软件 1 的页面，允许私有网 6 的用户通过网关上的 CGI 程序查询费用、修改访问权限、维护帐户等；

IP 地址翻译软件 2 与以太网接口卡 3 和以太网接口卡 5 的缓冲区、专用硬卡 4 通信；用于实现内部私有网 IP 地址的翻译与代理、包过滤、包转发、路由等功能；

以太网接口卡 3 和以太网接口卡 5 用于接收和发送数据帧；

专用硬卡 4 通过数据线、地址线和控制线与网关通信，实现用户访问权限表、流量表等动态信息的存取和断电自动保存，权限表的解释，用户帐户的定位和维护等功能；

Web 服务器软件 1 运行在网关上，Web 服务器软件 1 和以太网接口卡 3 的接收和发送缓冲区通信，Web 服务器软件（1）采用 CGI 程序与专用硬卡 4 的锁存器 9、缓冲器 14、缓冲电路 15 和译码电路 16 通信。

参见图 2，专用硬卡 4 由 9～16 八个部分组成。包括总线缓冲和锁存器 9，保存 32 位 IP 地址；可编程器件实现的译码电路 10 采用可编程器件器件实现对 IP 地址的译码；直流和电池双路供电的存储器 11 字长 192 位，保存权限和流量信息；以比较电路实现的电平监视电路 12 在上电和掉电时禁止访问权限和流量信息，以防止电压过渡时对存储器的误写入；可充电池 13 在线充电，掉电时维持权限表、流量表内容。缓冲器 14 储存硬件解释的权限表内容；将 192 位字长映射到 PC 总线的访问电路和缓冲电路 15；译码电路 16 主要用来缓冲命令。

下面结合附图说明它们之间的连接方式：

Web 服务器软件 1 以软件的形式运行在网关上，和以太网接口卡 3 的接收和发送缓冲区通信，采用 CGI 程序与专用硬卡 4 的总线缓冲和锁存器 9、缓冲器 14、缓冲电路 15 和译码电路 16 通信；

IP 地址翻译软件 2 与以太网接口卡 3 和以太网接口卡 5 的缓冲区、专用硬卡 4 通信；

以太网接口卡 3 通过网线与内部私有网 6 相连，以太网接口卡 5 通过网线与路由器 7 相连。

专用硬卡 4 由总线缓冲和锁存器 9、译码电路 10、存储器 11、缓冲器 14、缓冲电路 15、译码电路 16、电平监视电路 12 和可充电电池 13 组成；总线缓冲和锁存器 9 通过数据线和译码电路 10 相连，译码电路 10 通过控制线和地址线与存储器 11 相连，存储器 11 采用译码电路与缓冲器 14、缓冲电路 15 相连，可充电电池 13 和电平监视电路 12 分别接入存储器 11；

本网关能使内部私有 IP 地址通过一个全球统一 IP 地址访问 Internet，具体过程如下：

私有网中站点的一个客户程序要访问外部 Internet 上的一个服务器，客户程序采用内部私有 IP 地址和外部服务器进行通信，当客户程序发出的包经过网关时，网关的处理过程为：

IP 地址翻译软件 2 把 IP 数据包的 IP 地址写入总线缓冲和锁存器 9 中，如果缓冲器 14 显示合法，缓冲电路 15 中即是对应的权限和流量信息。IP 地址翻译软件 2 根据缓冲电路 15 中权限表中的服务类型等权限检查包，允许或禁止包通过，根据包长发命令到译码电路 16，更新存储器 11 中的流量表，否则丢弃该包。对于检查为合法的包，IP 地址翻译软件 2 采用网络翻译技术（请见 IETF 于 1994 年发布的 RFC1631， http：//www.ietf.org）翻译客户程序发出的 IP 包，然后网关把该包发向 Internet。

从服务器返回的包，经过网关时的处理过程为：

IP 地址翻译软件 2 采用网络翻译技术翻译客户程序发出的 IP 包，然后 IP 地址翻译软件 2 把 IP 地址写入总线缓冲和锁存器 9 中，如果缓冲器 14 显示合法，缓冲电路 15 中显示对应的权限和流量信息，根据缓冲电路 15 中权限表中的服务类型等权限检查包，允许或禁止包通过，根据包长发命令到译码电路 16，更新存储器 11 中的流量表，然后把包发向私有网，否则丢弃该包。

本网关通过 Web 服务器软件采用 CGI 程序接受用户的请求，完成硬卡上的

权限表的更改、流量查询等功能。过程为：

CGI 程序获得用户命令后进行编码，然后输入到译码器电路 16 中更改权限表，查询流量信息等。

本说明以 HTTP 为例，假设

1）客户程序所在的站点的 IP 地址为 10.10.10.2；

2）本网关的全球统一的 IP 地址为 200.76.35.5，和内部私有网相接的接口 IP 地址为 10.10.10.1 且为私有网的网关；

3）外部服务器的 IP 地址为 203.4.2.3。

客户程序首先发 IP 包，用 P（10.10.10.2：2000，203.4.2.3：80）表示，其中 10.10.10.2 为源 IP 地址，2000 为源端口号，203.4.2.3 为目的 IP 地址，80 为目的端口号。

IP 包到达本网关后，IP 地址翻译软件 2 把 10.10.10.2 写入锁存器 9 中，如果缓冲器 14 输出一个非法值，IP 地址翻译软件 2 把该包丢弃，如果判定为合法 IP 地址，IP 地址翻译软件 2 读取缓冲电路 15 中的权限表和流量信息，根据权限表检查包的端口号、访问的服务器的 IP 地址是否在国外等信息，从而允许或禁止包通过，并进行分国内、国外分别统计流量，最后把修改的流量信息输入译码电路 16，更新存储器 11 中的流量表。

如果包 P（10.10.10.2：2000，203.4.2.3：80）判定为合法，IP 地址翻译软件 2 采用透明地址翻译技术对此包进行翻译{假如翻译得到的包为 P（203.76.35.5：3000，203.4.2.3：80）}，然后发向外部 Internet。

从外部返回的包 P（203.4.2.3：80，200.76.35.5：3000），IP 地址翻译软件 2 采用透明地址翻译技术把此包翻译成 P（10.10.10.2：2000，203.4.2.3：80），然后把 10.10.10.2 写入锁存器 9 中如果缓冲器 14 输出一个非法值，IP 地址翻译软件 2 把该包丢弃，如果判定为合法 IP 地址，IP 地址翻译软件 2 读取缓冲电路 15 中的权限表和流量信息，根据权限表检查包的端口号、访问的服务器

的 IP 地址是否在国外等信息，从而允许或禁止包通过，并进行分国内、国外分别统计流量，最后把修改的流量信息输入译码电路 16，更新存储器 11 中的流量表。

本网关采用硬卡储存权限表和流量表信息，电池保护信息等措施，避免了存盘过程，保证了活动信息不丢失，解决了网关中用户权限不断变化和实时流量统计与查询的特殊情况。本网关又采用硬卡实现 IP 地址和用户帐户相绑定的策略，采用硬件实现 IP 地址直接定位用户帐户，加快了网关定位帐户的速度，提高了网关的性能，本网关需要透明地址翻译的策略，在性能上要高于应用层代理服务器。

图 3 是网关两边的吞吐量之和与网关每包时延平均值的关系。

图 4 是网关两边的吞吐量之和与代理网关吞吐量的关系，其中横坐标是网关两边的吞吐量之和，单位为 pps，纵坐标是网关的吞吐量，单位为 pps。

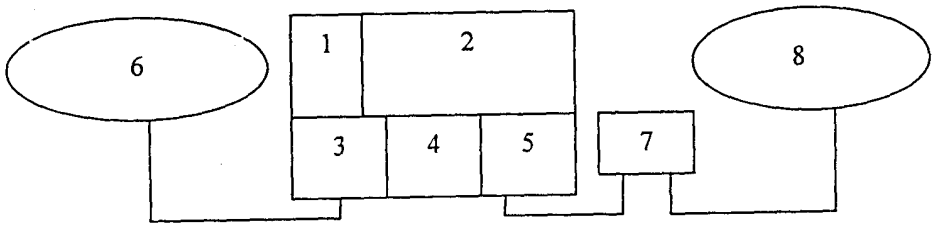


图 1

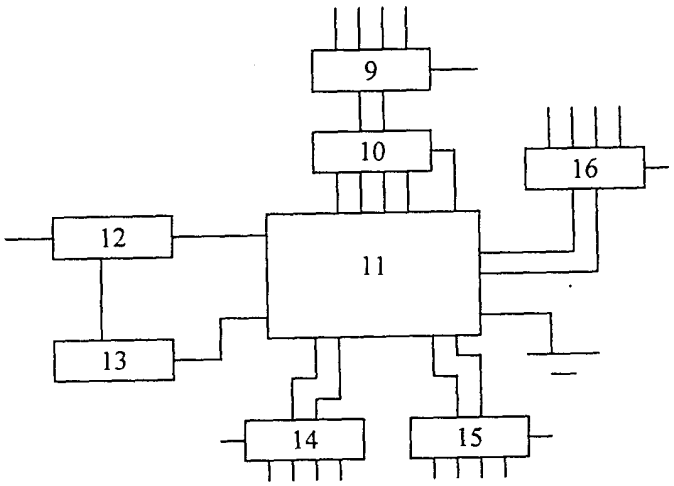


图 2

代理网关两边吞吐量之和/pps	代理网关的每包时延平均值
2760	0.5 ms
3560	1.2ms
4860	2ms
5634	3.5ms
6836	4.8ms
7320	6.5ms
8346	36ms
9420	386ms
1125	超时概率为 84%

图 3

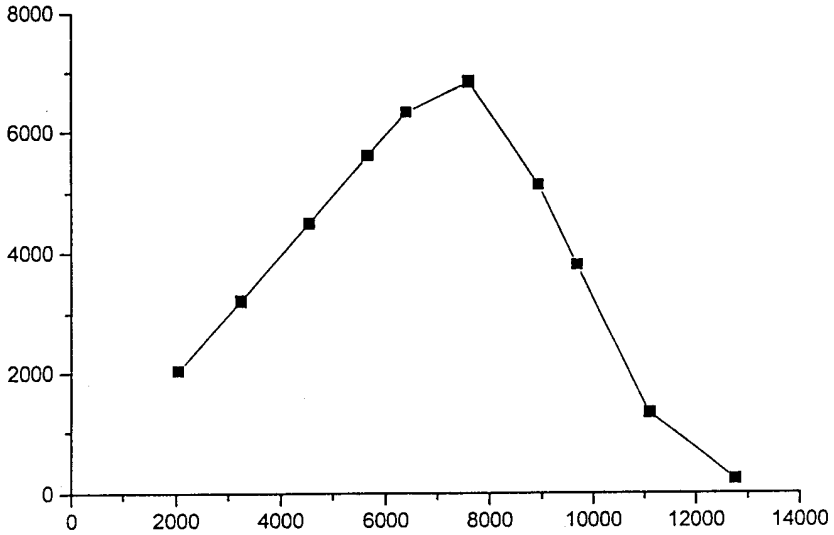


图 4