[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)

[12] 实用新型专利说明书

专利号 ZL 200520039242.8

[45] 授权公告日 2006 年 9 月 20 日

[11] 授权公告号 CN 2819663Y

[22] 申请日 2005.1.25

[21] 申请号 200520039242.8

[73] 专利权人 上海宝信软件股份有限公司

地址 201203 上海市浦东张江高科技园区郭守敬路 515 号

[72] 设计人 覃明贵 董文生 周 明 苗 舒 李 刚 闻 扬 余 彬 徐培杰

[74] 专利代理机构 中原信达知识产权代理有限责任公司

代理人 郑 玮

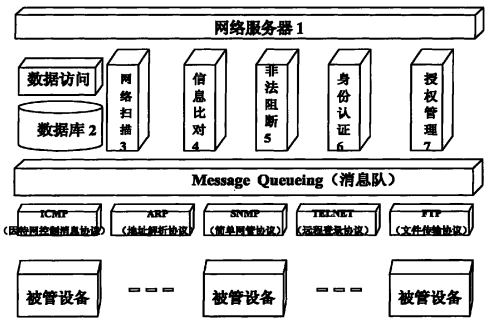
权利要求书 1 页 说明书 4 页 附图 1 页

[54] 实用新型名称

内网 IP 地址发现与阻断系统

[57] 摘要

本实用新型提供一种内网 IP 地址发现与阻断系统，包括：网络扫描模块，其扫描在线主机的 IP 地址、mac 地址、主机名、工作组等信息，将信息流发送给信息比对模块；信息比对模块，其将接收的信息流与已经设定的合法配置进行比对，将比对出的非法站点的列表发送给非法阻断模块；非法阻断模块，其对非法主机进行阻断攻击。 这样，使用本发明可在保证网络整体性能前提下，实现对局域网主机的及时发现和阻断，且不影响任何网络流量和传输的国际标准。



1、一种内网 IP 地址发现与阻断系统，其特征在于，包括：

网络扫描模块（3），其扫描在线主机的 IP 地址、mac 地址、主机名、工作组等信息，将信息流发送给信息比对模块；

信息比对模块（4），其将接收的信息流与已经设定的合法配置进行比对，将比对出的非法站点的列表发送给非法阻断模块；

非法阻断模块（5），其对非法主机进行阻断攻击；

网络服务器（1），其提供对外的接口调用；

身份认证模块（6），其用于用户登陆时对身份标识进行处理；

授权管理模块（7），其将该用户拥有权限的页面加载；

所述的网络扫描模块（3）、信息对比模块（4）、非法阻断模块(5)、拨号监控模块、设备管理模块、身份认证模块(6)、授权管理模块（7）之间相互通信连接。

内网 IP 地址发现与阻断系统

技术领域

本实用新型涉及一种局域网络安全管理系统，尤其涉及一种内网 IP 地址发现与阻断系统。

背景技术

现今互联网络的应用已经成为各大公司提高劳动生产率和利润率的革命性因素，它们通过电子商务和广域网获得了新的商机。与此同时，越来越多的雇员通过互联网络的标准协议 TCP/IP 连接到一起，这就导致了一个严重的问题，即成倍增长的 IP 地址超出了公司 IT 部门所能控制的范围。当今各大公司网络的扩展是极其迅猛的，同时对网络 IP 地址和名字空间的有序性和可靠性也提出了更高的要求。因此，如何有效防止 IP 地址的非法盗用以及非法网络设备接入网络是很多组织头疼的问题。

地址解析协议（ARP）用于实现 IP 地址到网络接口硬件地址的映射。当某主机要向以太网中的另一台主机发送 IP 数据时，它首先根据目的主机的 IP 地址到相应以太网地址的映射表。如果查到匹配的节点，则相应的以太网地址被写入以太网帧首部，数据报备加入到输出队列等候发送。如果查询失败，ARP 会先保留待发送的 IP 数据报，然后广播一个询问目的主机硬件地址的 ARP 报文，等收到回答后再将 IP 数据报发送出去。

发明内容

本实用新型所要解决的技术问题是提供一种内网 IP 地址发现与阻断系统，其可在保证网络整体性能前提下，实现对局域网主机的及时发现和阻断，

且不影响任何网络流量和传输的国际标准。

为了解决上述技术问题，本实用新型的技术方案为：提供一种内网 IP 地址发现与阻断系统，包括：

网络扫描模块，其扫描在线主机的 IP 地址、mac 地址、主机名、工作组等信息，将信息流发送给信息比对模块；

信息比对模块，其将接收的信息流与已经设定的合法配置进行比对，将比对出的非法站点的列表发送给非法阻断模块；

非法阻断模块，其对非法主机进行阻断攻击。

这样，本实用新型的优点如下：

本实用新型的系统以 Java、Web 技术为架构，采用面向对象和 Message Queueing 技术构件信息交换平台，使产品的各项功能构建于该平台之上，使整个系统具备灵活的扩展性。本实用新型可实现如下功能：1、物理端口防护；2、在线设备 IP 地址的实时检测与分析；3、IP 地址、MAC 地址等信息的合法性判定；4、警告并自动阻断非法的 IP 地址；5、查询非法 IP 地址的使用历史；6、支持主动检测、被动侦听等多种检测方式；7、同时支持动态分配 IP 地址和静态设定 IP 地址。

附图说明

图 1 是本实用新型的系统的结构示意图。

具体实施方式

如图 1 所示：本实用新型的系统系统使用 Java Servlet（Servlet 是用 Java 编写的 Server 端程序）容器 Tomcat（一个 Web 容器的名称）作为网络服务器 1，在最高层向用户提供 Web 方式的操作界面，系统内置 Postgresql（一种数据库的名称）数据库 2，该系统主要划分为网络扫描模块 3、信息比对模块 4、非法阻断模块 5、身份认证模块 6 和授权管理模块 7 七个模块，各

模块之间通过消息对的方法（Message Queueing）相互通信，在最底层通过ICMP（因特网控制消息协议）、ARP（地址解析协议）、SNMP（简单网管协议）、TELNET（远程登录协议）、FTP（文件传输协议）等标准协议获取被管设备的信息。

其中，网络服务器 1（WebService）提供对外的接口调用；

网络扫描模块 3 扫描在线主机的 IP 地址、mac（Media Access Control，介质访问控制）地址、主机名、工作组等信息，将信息流发送给信息比对模块；

信息比对模块 4 将接收的信息流与已经设定的合法配置进行比对，将比对出的非法站点的列表发送给非法阻断模块；

非法阻断模块 5 对非法主机进行阻断攻击。

在用户登陆系统时，身份认证模块 6 对身份标识进行处理，并调用授权管理模块 7 将该用户拥有权限的页面加载。各子模块通过 ODBC（Open Database Connectivity，开放数据库互连）或 JDBC（Java Database Connectivity，Java 数据库互连）访问数据库。

其中，所述的授权管理模块 7 采用 ePass 授权验证管理系统。ePass 授权验证管理系统是一个管理一个或多个应用系统的资源权限的通用软件系统，它可以对应用中的资源，比如应用系统菜单、画面、报表和文档等资源的使用权进行集中管理，同时对应用系统使用者的帐号进行集中管理，提供统一的标准登录界面和应用画面模板，提供对指定帐号、指定资源权限检查的接口。

所述的网络扫描模块 3 对 IP 地址的自动扫描发现可以通过 ICMP、ARP 等协议来完成，考虑扫描效率以及 MAC 地址发现的情况，本实用新型采用 ARP 协议来进行网络扫描。而主机名的自动发现则可通过 SNMP、Samba、

Ftp、Telnet等多种技术结合实现。

本实用新型的数据交换方法可以采用两种方法，一种是通过Message Queue消息同步机制，使用在不同系统之间传递消息，再通过应用程序做出一定的处理，完成数据同步工作；另外一种是通过XML文件来表示数据库数据，再通过网络将XML文件发送到同步端。Message Queue数据交换技术适用于实时性要求比较高，数据量相对较小的场合，XML(eXtensible Markup Language，可扩展标记语言)数据交换技术则适用于实时性要求较低，数据量相对较大的场合。

本实有新型采用BSMQ（Baosight Message Queuing,宝信消息队列）通信中间件作为数据同步的基础技术。BSMQ提供了在不同供应商平台上的连通性，向开发人员提供了标准的信息交互的方法。

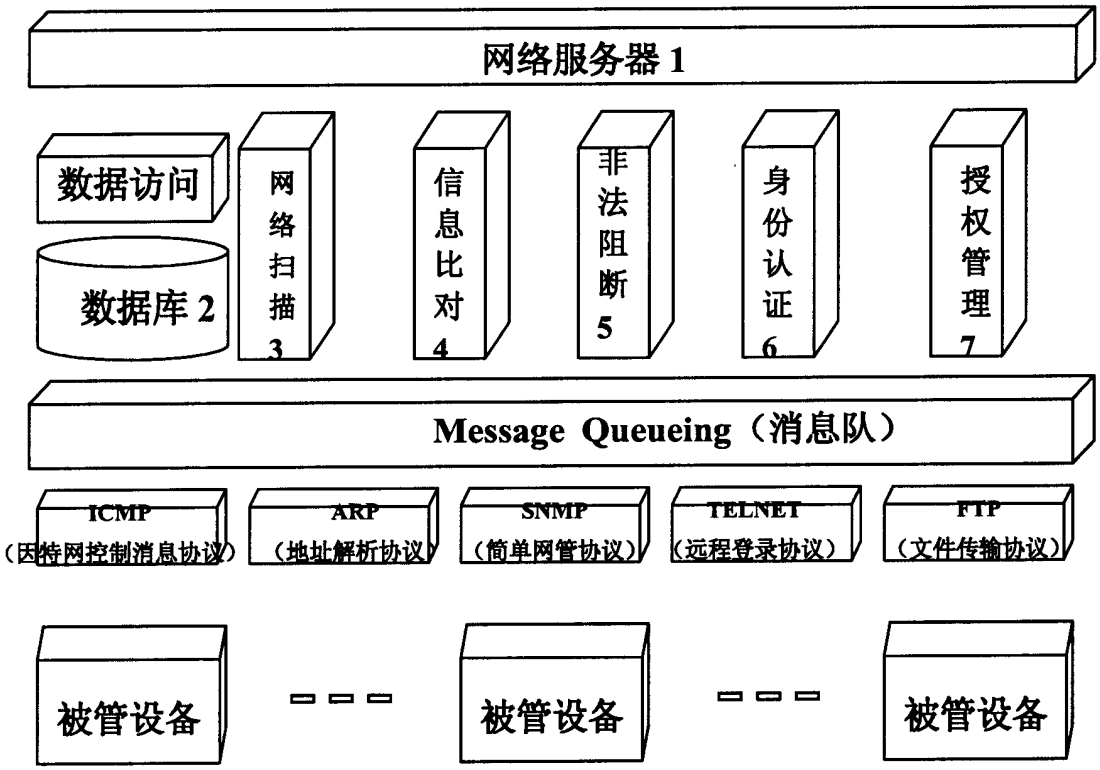

网络服务器 1
数据访问
数据库 2
网络扫描 3
信息比对 4
非法阻断 5
身份认证 6
授权管理 7
Message Queueing（消息队）
ICMP
（因特网控制消息协议）
ARP
（地址解析协议）
SNMP
（简单网管协议）
TELNET
（远程登录协议）
FTP
（文件传输协议）
被管设备
被管设备
被管设备

图 1