[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/24
H04L 9/00

[12] 发明专利申请公开说明书

[21] 申请号 02117285.4

[43] 公开日 2003 年 4 月 16 日

[11] 公开号 CN 1411208A

[22] 申请日 2002.4.23 [21] 申请号 02117285.4
[71] 申请人 华为技术有限公司
地址 517057 广东省深圳市科技园科发路华为用户服务中心大厦知识产权部
[72] 发明人 胡宇驰 周 雯

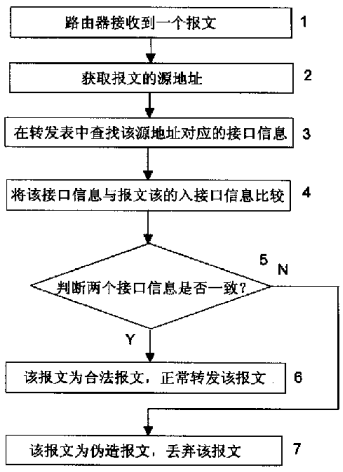
[74] 专利代理机构 北京集佳专利商标事务所
代理人 逯长明

权利要求书 2 页 说明书 5 页 附图 1 页

[54] 发明名称 防范网络攻击的方法

[57] 摘要

本发明涉及一种防范网络攻击的方法。该方法包括：首先在网络设备中配置网络地址与接口信息对应关系表；即与该网络设备接口相连的其它网络设备的网络地址与其它网络设备连接于该网络设备上所应用的接口信息对应关系表；在路由器由中则可以应用其中的路由转发表；然后，网络设备根据所接收报文的源地址查找该对应关系表，并根据查询结果判断该报文是否为伪造网络地址的报文，以确定其网络可访问性。因此，本发明可以有效地防止部分用户恶意伪造源址地进行网络攻击及通过伪造源地址更改自己的访问权限等，为网络的安全提供了进一步的保证。同时，本发明具有实现简单、占用资源少、效率高等优点。



ISSN1008-4274

1、一种防范网络攻击的方法，包括：

(1)在网络设备中配置网络设备接口与其网络地址的对应关系信息；

（2）网络设备根据所接收报文的源地址查找网络地址与接口信息对应关系表；

（3）根据查询结果和报文的实际入接口信息判断该报文是否为伪造网络地址的报文，以确定其网络可访问性。

2、根据权利要求1所述的防范网络攻击的方法，其特征在于所述的步骤（2）包括：

（21）获取报文中承载的报文的源地址；

（22）在网络设备接口与其网络地址的对应关系信息中查找该源地址对应的接口信息。

3、根据权利要求2所述的防范网络攻击的方法，其特征在于所述的步骤（3）包括：

（31）判断源地址在网络设备接口与其网络地址的对应关系信息中所对应的接口信息与报文的实际入接口信息是否一致，如果一致，执行步骤（32），否则，执行步骤（33）；

（32）该报文为合法报文，正常转发该报文；

（33）该报文为伪造报文，丢弃该报文。

4、根据权利要求1所述的防范网络攻击的方法，其特征在于所述的步骤（1）包括：建立用于存放网络设备接口与其网络地址的对应关系信息的映射表。

5、根据权利要求1所述的防范网络攻击的方法，其特征在于所述的网络设备接口与其网络地址的对应关系信息为路由器的路由转发表中的相应信息。

果采第二种基于流量统计的网络访问控制方法，虽然具有动态统计特性，并可以适应攻击的变化，但统计方法实现复杂、占用较多路由器资源，而且仍然无法从根据本上解决伪造源地址进行网络攻击的问题。因此，目前对伪造源地址进行网络攻击的行为并没有直接有效的解决办法。

发明内容

本发明的目的是提供一种防范网络攻击的方法，以实现针对伪造网络地址进行网络访问的报文进行访问控制。

本发明的目的是这样实现的：防范网络攻击的方法，包括：

(1)在网络设备中配置网络设备接口与其网络地址的对应关系信息；

（2）网络设备根据所接收报文的源地址查找网络地址与接口信息对应关系表；

（3）根据查询结果和报文的实际入接口信息判断该报文是否为伪造网络地址的报文，以确定其网络可访问性。

所述的步骤（2）包括：

（21）获取报文中承载的报文的源地址；

（22）在网络设备接口与其网络地址的对应关系信息中查找该源地址对应的接口信息。

所述的步骤（3）包括：

（31）判断源地址在网络设备接口与其网络地址的对应关系信息中所对应的接口信息与报文的实际入接口信息是否一致，如果一致，执行步骤（32），否则，执行步骤（33）；

防范网络攻击的方法

技术领域

本发明涉及一种网络访问控制技术,尤其涉及一种防范网络攻击的方法.

背景技术

目前，网络访问控制的实现方式有两种：一种网络访问控制方法为定义了一系列的访问控制规则，访问控制规则中包括基于网络地址的控制规则等，规则中规定了哪些报文可以通过，哪些报文不可以通过，这样，当报文进入路由器时，就会去匹配这些规则，不符合规则的报文则被丢弃掉，符合规则的报文便可以继续传送；另一种为基于流量统计的访问控制方法，该方法可以根据报文的某些特征统计流量，如果具备相应特征的报文的流量超过了规定值，则路由器可以限制该类型报文的流量，或者拒绝接收该类型的报文，以保护路由器资源。

而在目前的网络访问中，存在大量的源地址欺骗攻击行为。攻击者通过伪造网络上其他使用者的源地址向服务器发出请求，占用大量服务器资源，如果服务器响应请求的话，将向该源地址的实际使用者发送应答报文，应答报文大量地占用了该源地址实际使用者的资源，严重情况下将导致服务器及源地址实际使用者无法响应其他请求，甚至死机。

针对上述现有技术所存在的问题，如果采用第一种网络访问控制方法，则因为访问控制规则不具有动态特性，且规则的配置只能针对已知的非法和合法的报文，所以无法检测出未知的伪造成合法源地址的报文。如

（32）该报文为合法报文，正常转发该报文；

（33）该报文为伪造报文，丢弃该报文。

所述的步骤（1）包括：建立用于存放网络设备接口与其网络地址的对应关系信息的映射表。

所述的网络设备接口与其网络地址的对应关系信息为路由器的路由转发表中的相应信息。

由上述本发明所提供的技术方案可以看出，路由器等网络设备接收到报文后，根据报文的目的地址查找路由转发表之前，首先要根据报文的源地址查找路由转发表，以确定该报文是否为伪造源地址的报文，并根据该结果做相应处理。因此，本发明可以方便、有效地阻止部分用户恶意伪造源地址进行网络攻击及通过伪造源地址更改自己访问权限等不合法行为，为网络的安全提供了进一步的保证。同时，本发明具有实现简单、占用资源少、效率高等优点。

附图说明

图1为本发明的流程图；

图2为本发明的应用实例示意图。

具体实施方式

通常情况下，网络设备路由器接收到一个报文后，会根据报文的目的地址查找路由转发表，如果找到该目的地址对应的路由器的出接口，则将报文由相应的接口转发出去，如果该目的地址为路由器本身，则将报文交由上层继续处理，路由器中的路由转发表中包括网络地址与接口的对应关

系信息，路由转发表可以为用户配置生成，也可以为路由器自动学习生成。结合上述现有技术状况，本发明所述的防范网络攻击的方法的具体实施方式如下，参见图1：

步骤1：路由器接收到一个IP报文，报文中承载有报文的源地址、目的地址及进入路由器时所经过的接口等信息；

步骤2：网络设备获取该IP报文的源地址，以便利用该源地址查询与该源地址对就的接口信息；

步骤3：在路由器的路由转发表中查找该源地址所对应的接口信息，即查询来源于该源地址的报文应该经过的路由器接口信息，并保存该接口信息；

步骤4：在IP报文的正常处理流程中获取报文所承载的实际入接口信息，将步骤3中保存的接口信息与该报文进入路由器时所经过的实际入接口信息进行比较；

步骤5：判断源地址在路由转发表中所对应的接口信息与报文的实际入接口信息是否一致，如果一致，执行步骤6，否则，执行步骤7；

步骤6：报文源地址在路由转发表中所对应的接口信息与报文的实际入接口信息一致，则说明该报文的源地址非伪造源地址，即该报文为合法报文，这样，路由器便可以正常地处理并转发该报文；

步骤7： 报文源地址在路由转发表中所对应的接口信息与报文的实际入接口信息不一致，则说明该报文的源地址为伪造源地址，即该报文为伪造报文，丢弃该报文，以保证网络的安全及网络的合理访问权限。

通过上述本发明所提供的技术方案，即可以很容易地将伪造源地址的报文与合法的报文区分开来，从而控制伪造源地址的报文进行网络访问，保证网络的安全。本发明可以根据网络运营商等网络设备用户的需求设置于相应网络设备的相应接口，对由该接口接收来的报文进行相应的安全检查，例如，本发明可以应用于提供服务的网络与客户网络相连的路由器上的相应接口。

另外，上述本发明的实施方案是应用路由器中已经存在的路由转发表做为网络地址与接口信息对应关系表，用户也可以根据需要自己配置网络地址与接口信息对应关系表。

下面结合具体应用实例对本发明做进一步的说明，参见图2：路由器RTA的IP地址为1.1.1.1，路由器RTC的IP地址为2.1.1.1，路由器RTA上伪造源地址为2.1.1.1的IP报文，该报文的访问目的是路由器RTB，我们在路由器RTB上应用了本发明所提供的技术方案，路由器RTB收到这个伪造报文后，根据其源地址2.1.1.1查找路由器RTB的转发表，发现地址2.1.1.1所对应的接口是右边的接口，而该报文记录实际进行入路由器RTB经过的是左边的接口，则路由器RTB认为该报文是伪造源地址的报文，并丢弃该报文。这样便可以方便、有效地防止部分用户恶意伪造源地址进行网络攻击或更改自己的访问权限等。

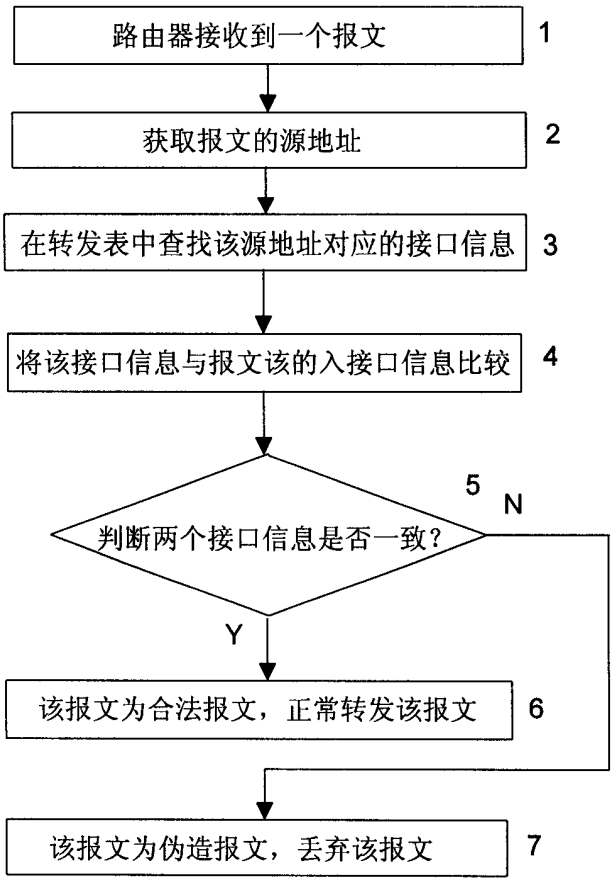

路由器接收到一个报文
1
获取报文的源地址
2
在转发表中查找该源地址对应的接口信息
3
将该接口信息与报文该的入接口信息比较
4
判断两个接口信息是否一致?
5
N
Y
该报文为合法报文，正常转发该报文
6
该报文为伪造报文，丢弃该报文
7

图1

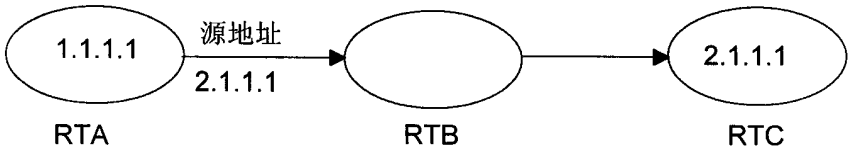

1.1.1.1
源地址
2.1.1.1
2.1.1.1
RTA
RTB
RTC

图2