(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106411644 A
(43)申请公布日 2017.02.15

(21)申请号 201610866094.X

(22)申请日 2016.09.30

(71)申请人 苏州迈科网络安全技术股份有限公司

地址 215021 江苏省苏州市工业园区林泉街399号东南大学明德院3楼

(72)发明人 高祥 施雅各

(74)专利代理机构 南京苏科专利代理有限责任公司 32102

代理人 姚姣阳 陈忠辉

(51)Int.Cl.

H04L 12/26(2006.01)

权利要求书2页 说明书5页

(54)发明名称

基于DPI技术的网络共享设备检测方法及系统

(57)摘要

本发明揭示了基于DPI技术的网络共享设备检测方法及系统，包括如下步骤，S1，信息采集步骤：通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息；S2，判断步骤：根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。本发明的网络共享设备检测方法是直接获取终端设备信息和/或设备操作系统信息来进行判断，并且本方法和操作系统本身特性无关，同时目前还没有相应的反检测技术，因此检测准确性大大提高。

CN 106411644 A

1.基于DPI技术的网络共享设备检测方法，其特征在于：包括如下步骤：

S1，信息采集步骤：通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息；

S2，判断步骤：根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。

2.根据权利要求1所述的基于DPI技术的网络共享设备检测方法，其特征在于：所述S1，信息采集步骤包括如下过程：

S11，分析若干应用软件的请求信息，并提取特征字段，然后根据分析结果生成特征库；

S12，通过深度报文解析技术，对请求数据进行分析并得到应用协议信息，在特征库中查找匹配应用协议的特征规则，然后通过规则中的正则表达式去获取特定字段中的值，根据规则中的描述来确定该值是否是终端设备的操作系统类型或设备型号信息。

3.根据权利要求1所述的基于DPI技术的网络共享设备检测方法，其特征在于：在所述S2，判断步骤中：

当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个操作系统类型或至少两个操作系统版本，则判定所述设备为网络共享设备；和/或当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个品牌的终端设备或是至少两个设备型号，则判定该所述设备为网络共享设备。

4.根据权利要求1-3任一所述的基于DPI技术的网络共享设备检测方法，其特征在于：还包括S3，处理步骤，当判断存在网络共享设备时，对网络共享设备进行断网并通知网络管理员或在对网络共享设备进行断网后，并在移除所述网络共享设备且等待设定时间后，使网络自动恢复正常。

5.根据权利要求1-3任一所述的基于DPI技术的网络共享设备检测方法，其特征在于：还包括S4，识别步骤，识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在S2，判断步骤中识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

6.根据权利要求1-3任一所述的基于DPI技术的网络共享设备检测方法，其特征在于：还包括S5，预设置步骤：当企业中存在安装了虚拟系统且使用了NAT网络连接方式的设备时，将安装了虚拟系统且使用了NAT网络连接方式的设备通过黑/白名单方式进行配置，使该设备不会被断网。

7.基于DPI技术的网络共享设备检测系统，其特征在于：包括

信息采集单元，用于通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息；

判断单元，用于根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。

8.根据权利要求7所述的基于DPI技术的网络共享设备检测系统，其特征在于：还包括

处理单元，用于当判断存在网络共享设备时，对网络共享设备进行断网并通知网络管理员或在对网络共享设备进行断网后，并在移除所述网络共享设备并等待设定时间后，使网络自动恢复正常。

9.根据权利要求7所述的基于DPI技术的网络共享设备检测系统，其特征在于：还包括识别单元，用于识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在判断单元识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

10.根据权利要求7所述的基于DPI技术的网络共享设备检测系统，其特征在于：还包括预设置单元，用于当企业中存在安装了虚拟系统且使用了NAT网络连接方式的设备时，将安装了虚拟系统且使用了NAT网络连接方式的设备通过黑/白名单方式进行配置，使该设备不会被断网。

基于DPI技术的网络共享设备检测方法及系统

技术领域

[0001] 本发明涉及网络共享设备检测方法及系统，尤其是基于DPI技术的网络共享设备检测方法及系统。

背景技术

[0002] 企业为了保证网络安全，往往会对员工的网络访问做限制；但是一些员工会通过私接网络共享设备(随身WiFi、无线路由器等)来满足移动设备的无线上网需求，这会给企业网络带来较大的安全隐患。

[0003] 目前对网络共享设备的检测方法有IP_ID检测法、TTL检测法、TCP指纹检测法和TCP时间戳检测法。

[0004] 1、IP_ID检测法

基本原理：同一Windows主机发出的IP报文中的ID字段是连续变化的(呈递增趋势)，如果在一段时间内检测到某个设备出现不同的ID序列，则可以判定该设备为网络共享设备。

[0005] 不足之处：在新的Windows系统(Windows 8及Windows 10)上，IP报文中的ID字段已不存在这种规律。

[0006] 2、TTL检测法

基本原理：TTL(Time To Live)是IP报文中的一个字段，每当IP报文经过一个路由设备，TTL值就会减小1。如果检测到某个设备的报文存在多个TTL值，则可以判定该设备为网络共享设备。

[0007] 不足之处：现在很多网络共享设备已经实现了反TTL检测，IP报文经过设备后，TTL不会被改变。

[0008] 3、TCP指纹检测法

基本原理：各个操作系统、各个时期的版本对于同样的通讯规范的实现有相当多的不同之处，这其中最明显的差异来自于TCP参数和选项的选择；通过TCP起始窗口大小、起始TTL、扩展选项与顺序等作为TCP指纹可以来检测操作系统类型。如果检测到某个设备包含多种操作系统，则可以判定该设备为网络共享设备。

[0009] 不足之处：由于很多操作系统的TCP指纹有较多相近之处，这种技术的判别精度始终是个问题。

[0010] 4、TCP时间戳检测法

基本原理：实时获取同一IP发送的相邻两个TCP报文的系统时间及时间戳信息。根据设定的常量及算法判定这两个报文是否是两台主机发出的，如果判定是两台主机，则可以判定该设备为网络共享设备。

[0011] 不足之处：目前大部分操作系统默认都是不开启TCP时间戳的，有些文章描述了可以动态开启的方法，但是已经不适用于现在常见的操作系统。

[0012] 同时，随着终端系统不断升级以及网络共享设备具有反检测技术，目前对网络共享设备的检测方法已经不能满足需求。

发明内容

[0013] 本发明的目的就是为了解决现有技术中存在的上述问题，提供一种基于DPI技术的网络共享设备检测方法及系统。

[0014] 本发明的目的将通过以下技术方案得以实现：

基于DPI技术的网络共享设备检测方法，包括如下步骤：

S1，信息采集步骤：通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息；

S2，判断步骤：根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。

[0015] 优选的，所述的基于DPI技术的网络共享设备检测方法，其中：所述S1，信息采集步骤包括如下过程：

S11，分析若干应用软件的请求信息，并提取特征字段，然后根据分析结果生成特征库；

S12，通过深度报文解析技术，对请求数据进行分析并得到应用协议信息，在特征库中查找匹配应用协议的特征规则，然后通过规则中的正则表达式去获取特定字段中的值，根据规则中的描述来确定该值是否是终端设备的操作系统类型或设备型号信息。

[0016] 优选的，所述的基于DPI技术的网络共享设备检测方法，其中：在所述S2，判断步骤中：

当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个操作系统类型或至少两个操作系统版本，则判定所述设备为网络共享设备；和/或

当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个品牌的终端设备或是至少两个设备型号，则判定该所述设备为网络共享设备。

[0017] 优选的，所述的基于DPI技术的网络共享设备检测方法，其中：当判断存在网络共享设备时，对网络共享设备进行断网并通知网络管理员或在对网络共享设备进行断网后，并在移除所述网络共享设备且等待设定时间后，使网络自动恢复正常。

[0018] 优选的，所述的基于DPI技术的网络共享设备检测方法，其中：还包括S4，识别步骤，识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在S2，判断步骤中识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

[0019] 优选的，所述的基于DPI技术的网络共享设备检测方法，其中：还包括S5，预设置步骤：当企业中存在安装了虚拟系统且使用了NAT网络连接方式的设备时，将安装了虚拟系统且使用了NAT网络连接方式的设备通过黑/白名单方式进行配置，使该设备不会被断网。

[0020] 基于DPI技术的网络共享设备检测系统，包括

信息采集单元，用于通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备

型号信息；

判断单元，用于根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。

[0021] 优选的，所述的基于DPI技术的网络共享设备检测系统，其中：还包括处理单元，用于当判断存在网络共享设备时，对网络共享设备进行断网并通知网络管理员或在对网络共享设备进行断网后，并在移除所述网络共享设备并等待设定时间后，使网络自动恢复正常。

[0022] 优选的，所述的基于DPI技术的网络共享设备检测系统，其中：还包括识别单元，用于识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在判断单元识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

[0023] 优选的，所述的基于DPI技术的网络共享设备检测系统，其中：还包括预设置单元，用于当企业中存在安装了虚拟系统且使用了NAT网络连接方式的设备时，将安装了虚拟系统且使用了NAT网络连接方式的设备通过黑/白名单方式进行配置，使该设备不会被断网。

[0024] 本发明技术方案的优点主要体现在：

本发明的网络共享设备检测方法是直接获取终端设备信息和/或设备操作系统信息来进行判断，并且本方法和操作系统本身特性无关，同时目前还没有相应的反检测技术，因此检测准确性大大提高，并且通过设置自动的处理方法，能够及时、有效的对检测出的网络共享设备进行处理，降低了风险产生的概率。

[0025] 通过对特殊情况，即安装了虚拟系统且使用了NAT网络连接方式的设备的设置，能够有效规避特殊情况对识别精度的干扰，从而进一步提高识别的准确性。

具体实施方式

[0026] 本发明揭示的基于DPI技术的网络共享设备检测系统，包括

信息采集单元，用于通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息；

判断单元，用于根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备；

以及处理单元，用于当判断存在网络共享设备时，对网络共享设备进行断网并通知网络管理员或在对网络共享设备进行断网后，并在移除所述网络共享设备并等待设定时间后，使网络自动恢复正常。

[0027] 进一步，所述基于DPI技术的网络共享设备检测系统还包括识别单元，用于识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在判断单元识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

[0028] 更进一步，所述的基于DPI技术的网络共享设备检测系统还包括预设置单元，用于当企业中存在安装了虚拟系统且使用了NAT网络连接方式的设备时，将安装了虚拟系统且

使用了NAT网络连接方式的设备通过黑/白名单方式进行配置，使该设备不会被断网，当然也可以采用其他可行的方式进行配置，使该设备不会被断网。

[0029] 采用上述的基于DPI技术的网络共享设备检测系统，其工作过程如下：

S1，信息采集步骤：通过深度报文检测技术检测若干终端设备中安装的应用软件发给服务器的请求数据，并识别出请求数据中包含的所在终端设备的操作系统类型和/或设备型号信息。

[0030] 详细的，所述S1，信息采集步骤包括如下过程：

S11，分析若干应用软件的请求信息，并提取特征字段，然后根据分析结果生成特征库；

S12，通过深度报文解析技术，对请求数据进行分析并得到应用协议信息，在特征库中查找匹配应用协议的特征规则，然后通过规则中的正则表达式去获取特定字段(如HTTP头部的User-Agent字段及HTTP Payload部分等)中的值，根据规则中的描述来确定该值是否是终端设备的操作系统类型或设备型号信息。

[0031] S2，判断步骤：根据各种应用软件通过某一设备在一段时间内发送的请求数据中的设备操作系统类型和/或设备型号的数量，从而判断是否存在网络共享设备。

[0032] 详细的，在上述判断过程中：

由于所述的设备在网络层的表现形式为一个IP地址，如果设备为网络共享设备，那么此IP地址就会被多台设备共享使用，所以就可能看到多种操作系统类型或操作系统版本，而常见的操作系统有Windows、iOS、Android、Linux等，每种操作系统又有很多个版本，因此，当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个操作系统类型或至少两个操作系统版本，则判定所述设备为网络共享设备。

[0033] 另外，常见的智能终端有很多品牌，每个品牌又包含很多种型号的设备，因此，当通过深度报文检测技术分析出各种应用软件通过某一设备在一段时间内发送的请求数据中包括至少两个品牌的终端设备或是至少两个设备型号，由于只有当一台设备作为网络共享设备时，它发送的数据才可能包含多种设备品牌或设备型号，则判定该所述设备为网络共享设备。

[0034] 上述的两种判断条件只要满足两者中的一个或全部满足，都可以认定存在网络共享设备。

[0035] 并且，当判断存在网络共享设备时，对网络共享设备进行断网(比如对该IP发出的数据包进行丢弃)并通知网络管理员进行处理，也可以进行动态处理，如断网后的自动恢复网络的机制，即：在对网络共享设备进行断网后，在一段时间内所述IP没有再被检测为网络共享设备(比如所述网络共享设备被移除)，并等待设定时间后，使网络自动恢复正常。

[0036] 但是，一些比较特殊的情况是：当电脑上安装了虚拟机(虚拟系统)且使用了NAT网络连接方式，该电脑也会被识别为网络共享设备，这就会影响上述网络共享设备识别的准确性，因此在判断存在网络共享设备时，还包括S4，识别步骤，识别是否存在安装了虚拟系统且使用了NAT网络连接方式的设备，当判断存在安装了虚拟系统且使用了NAT网络连接方式的设备且在S2，判断步骤中识别存在网络共享设备时，判断识别出的网络共享设备是否是安装了虚拟系统且使用了NAT网络连接方式的设备，如是，则对该设备不做处理。

[0037] 当然，针对上述情况，也可以根据实际网控环境，采用其他可行方式进行处理，例

如,在事先知道企业中已存在或检测得到存在安装了虚拟系统且使用了NAT网络连接方式的设备(如电脑)时,可以将安装了虚拟系统且使用了NAT网络连接方式的电脑通过黑/白名单方式进行配置以满足需求,即可以允许网络管理员把该电脑IP加入白名单,保证该电脑不会被断网。

[0038] 本发明尚有多种实施方式,凡采用等同变换或者等效变换而形成的所有技术方案,均落在本发明的保护范围之内。