



(12)发明专利申请

(10)申请公布号 CN 106790263 A

(43)申请公布日 2017.05.31

(21)申请号 201710069126.8

(22)申请日 2017.02.08

(71)申请人 佛山易识科技有限公司

地址 528000 广东省佛山市禅城区季华西路133号3座12层02单元

(72)发明人 吴启晖

(51)Int.Cl.

H04L 29/06(2006.01)

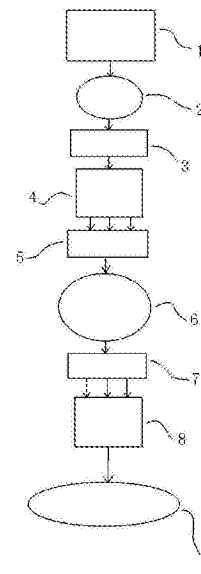
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种智能的敏感及私密数据传输保护方法

(57)摘要

本发明公开了一种智能的敏感及私密数据传输保护方法,包括发送数据包并区分标识敏感及私密数据、智能选择虚拟链路转发敏感及私密数据、接收数据包三个步骤,在传输过程中可对数据包进行分析并区分标识出敏感及私密数据,再智能选择虚拟链路来传输敏感及私密数据;具有可智能化分配流量,可增加对数据包传输的可控性及灵活调度,可提高资源利用率、降低费用成本和维护成本,可智能判断数据包等级、合理使用QOS技术发送数据包、可提高数据传输的安全和高效性,可扩展性好的特点;解决了现有的传统物理设备中不管是私密数据包还是常规数据包,都统一由物理交换机依次做转发及需要增加新链路区分重要数据包和普通数据包而存在的各种问题。



CN 106790263 A

1. 一种智能的敏感及私密数据传输保护方法,其特征在于,包括以下步骤:

a、发送数据包(10)并区分标识敏感及私密数据,客户端(1)发送数据包(10)经由路由器(2)转发给第一交换机(3),第一交换机(3)直接将数据包(10)转发给第一中间服务端(4),第一中间服务端(4)对数据包(10)进行分析匹配区分出敏感及私密数据(10a),并通过标签添加模块(41)对区分出的敏感及私密数据(10a)进行标识;

b、智能选择虚拟链路(50)转发敏感及私密数据(10a),第一中间服务端(4)和第二交换机(5)之间建立两条或两条以上的VXLAN虚拟链路(50)连接,虚拟链路(50)包括普通数据转发链路、敏感及私密数据转发链路两种,经由步骤a标识区分出的敏感及私密数据(10a)通过敏感及私密数据转发链路转发给第二交换机(5),并使用链路探测工具(42)探测敏感及私密数据转发链路的拥堵情况,如果敏感及私密数据转发链路拥堵则使用QOS加速模块(43)加速转发敏感及私密数据(10a),使敏感及私密数据(10a)第一时间转发到第二交换机(5);如果敏感及私密数据转发链路不拥堵则不需要使用QOS加速模块(43);步骤a中未标识的普通数据(10b)则经由普通数据转发链路直接转发给第二交换机(5);

c、接收数据包(10),第三交换机(7)通过中间网络(6)和第二交换机(5)连接,第二中间服务端(8)和第三交换机(7)之间建立两条或两条以上的VXLAN虚拟链路(50)连接,第二交换机(5)将接收到的敏感及私密数据(10a)、普通数据(10b)通过中间网络(6)转发给第三交换机(7),第三交换机(7)再通过敏感及私密数据转发链路将敏感及私密数据(10a)转发到第二中间服务端(8),通过普通数据转发链路直接将普通数据(10b)转发给第二中间服务端(8),敏感及私密数据(10a)、普通数据(10b)从第三交换机(7)转发到第二中间服务端(8)的过程与敏感及私密数据(10a)、普通数据(10b)在步骤b中从第一中间服务端(4)转发到第二交换机(5)的过程是相反的,最后由第二中间服务端(8)将敏感及私密数据(10a)、普通数据(10b)转发给接收终端(9)。

2. 如权利要求1所述的一种智能的敏感及私密数据传输保护方法,其特征在于,第一中间服务端(4)是根据数据包(10)中源MAC地址及源IP地址来分析匹配区分出敏感及私密数据(10a)的。

## 一种智能的敏感及私密数据传输保护方法

### 技术领域

[0001] 本发明涉及网络数据包传输技术领域,具体涉及一种敏感及私密数据传输保护方法。

### 背景技术

[0002] 网络数据包传输与现实物流是一样的,过程类似于货物选择、货物装车、运输线路选择等,在运输过程中还伴随着线路拥堵、货物丢失等情况;在现有的传统物理设备中不管是私密数据包还是常规数据包,都是统一由物理交换机依次做转发,当需要区分重要数据包和普通数据包时,则需要增加新链路区分两种数据包的走向,其通过排序方式依次转发,不区分数据包优先级大小,当网络使用率达到最大化时则会出现网络拥堵延迟,数据包容易发生丢包情况,不能保证数据的安全性;其需要增加链路来发送不同的数据包,增加了费用成本和维护成本;物理设备往往因为地区或时间段的不同导致其中一条或多条链路达到饱和状态,而其他链路则处于空闲状态,导致资源利用率低。

### 发明内容

[0003] 针对现有技术的不足,本发明旨在提供一种在传输过程中可对数据包进行分析并区分出敏感及私密数据,对敏感及私密数据进行标识后可智能选择虚拟链路来传输敏感及私密数据的智能的敏感及私密数据传输保护方法。

[0004] 为实现上述目的,本发明采用如下技术方案:

一种智能的敏感及私密数据传输保护方法,包括以下步骤:

a、发送数据包并区分标识敏感及私密数据,客户端发送数据包经由路由器转发给第一交换机,第一交换机直接将数据包转发给第一中间服务端,第一中间服务端对数据包进行分析匹配区分出敏感及私密数据,并通过标签添加模块对区分出的敏感及私密数据进行标识;

b、智能选择虚拟链路转发敏感及私密数据,第一中间服务端和第二交换机之间建立两条或两条以上的VXLAN虚拟链路连接,虚拟链路包括普通数据转发链路、敏感及私密数据转发链路两种,经由步骤a标识区分出的敏感及私密数据通过敏感及私密数据转发链路转发给第二交换机,并使用链路探测工具探测敏感及私密数据转发链路的拥堵情况,如果敏感及私密数据转发链路拥堵则使用QOS加速模块加速转发敏感及私密数据,使敏感及私密数据第一时间转发到第二交换机;如果敏感及私密数据转发链路不拥堵则不需要使用QOS加速模块;步骤a中未标识的普通数据则经由普通数据转发链路直接转发给第二交换机;

c、接收数据包,第三交换机通过中间网络和第二交换机连接,第二中间服务端和第三交换机之间建立两条或两条以上的VXLAN虚拟链路连接,第二交换机将接收到的敏感及私密数据、普通数据通过中间网络转发给第三交换机,第三交换机再通过敏感及私密数据转发链路将敏感及私密数据转发到第二中间服务端,通过普通数据转发链路直接将普通数据转发给第二中间服务端,敏感及私密数据、普通数据从第三交换机转发到第二中间服务端

的过程与敏感及私密数据、普通数据在步骤b中从第一中间服务端转发到第二交换机的过程是相反的,最后由第二中间服务端将敏感及私密数据、普通数据转发给接收终端。

[0005] 进一步的,第一中间服务端是根据数据包中源MAC地址及源IP地址来分析匹配区分出敏感及私密数据的。

[0006] 本发明具有如下有益效果:

本发明一种智能的敏感及私密数据传输保护方法,其在传输过程中可对数据包进行分析并区分出敏感及私密数据,对敏感及私密数据进行标识后可智能选择虚拟链路来传输敏感及私密数据;具有可智能化分配流量,可增加对数据包传输的可控性及灵活调度,可提高资源利用率、降低费用成本和维护成本,可智能判断数据包等级、合理使用QOS技术发送数据包、可提高数据传输的安全和高效性,可扩展性好的特点。

## 附图说明

[0007] 图1为本发明一种智能的敏感及私密数据传输保护方法的简单原理示意图;

图2为本发明一种智能的敏感及私密数据传输保护方法其标识敏感及私密数据的简单原理示意图;

图3为本发明一种智能的敏感及私密数据传输保护方法其敏感及私密数据、普通数据在第一中间服务端和第二交换机之间转发的简单过程示意图。

[0008] 图中:1、客户端;2、路由器;3、第一交换机;4、第一中间服务端;5、第二交换机;6、中间网络;7、第三交换机;8、第二中间服务端;9、接收终端;10、数据包;10a、敏感及私密数据;10b、普通数据;41、标签添加模块;42、链路探测工具;43、QOS加速模块;50、VXLAN虚拟链路。

## 具体实施方式

[0009] 下面结合附图及具体实施例,对本发明作进一步的描述,以便于更清楚地理解本发明要求保护的技术思想。

[0010] 如图1-3所示本发明一种智能的敏感及私密数据传输保护方法,包括以下步骤:a、发送数据包10并区分标识敏感及私密数据,客户端1发送数据包10经由路由器2转发给第一交换机3,第一交换机3直接将数据包10转发给第一中间服务端4,第一中间服务端4对数据包10进行分析匹配区分出敏感及私密数据10a,并通过标签添加模块41对区分出的敏感及私密数据10a进行标识;

b、智能选择虚拟链路50转发敏感及私密数据10a,第一中间服务端4和第二交换机5之间建立两条或两条以上的VXLAN虚拟链路50连接,虚拟链路50包括普通数据转发链路、敏感及私密数据转发链路两种,经由步骤a标识区分出的敏感及私密数据10a通过敏感及私密数据转发链路转发给第二交换机5,并使用链路探测工具42探测敏感及私密数据转发链路的拥堵情况,如果敏感及私密数据转发链路拥堵则使用QOS加速模块43加速转发敏感及私密数据10a,使敏感及私密数据10a第一时间转发到第二交换机5;如果敏感及私密数据转发链路不拥堵则不需要使用QOS加速模块43;步骤a中未标识的普通数据10b则经由普通数据转发链路直接转发给第二交换机5;

c、接收数据包10,第三交换机7通过中间网络6和第二交换机5连接,第二中间服务端8

和第三交换机7之间建立两条或两条以上的VXLAN虚拟链路50连接,第二交换机5将接收到的敏感及私密数据10a、普通数据10b通过中间网络6转发给第三交换机7,第三交换机7再通过敏感及私密数据转发链路将敏感及私密数据10a转发到第二中间服务端8,通过普通数据转发链路直接将普通数据10b转发给第二中间服务端8,敏感及私密数据10a、普通数据10b从第三交换机7转发到第二中间服务端8的过程与敏感及私密数据10a、普通数据10b在步骤b中从第一中间服务端4转发到第二交换机5的过程是相反的,最后由第二中间服务端8将敏感及私密数据10a、普通数据10b转发给接收终端9。

[0011] 具体的,第一中间服务端4是根据数据包10中源MAC地址及源IP地址来分析匹配区分出敏感及私密数据10a的。

[0012] 本发明其在传输过程中可对数据包10进行分析并区分出敏感及私密数据10a,对敏感及私密数据10a进行标识后可智能选择虚拟链路50来传输敏感及私密数据10a;具有可智能化分配流量,可增加对数据包10传输的可控性及灵活调度,可提高资源利用率、降低费用成本和维护成本,可智能判断数据包10等级、合理使用QOS技术发送数据包10、可提高数据传输的安全和高效性,可扩展性好的特点。

[0013] 对于本领域的技术人员来说,可根据以上描述的技术方案以及构思,做出其它各种相应的改变以及变形,而所有的这些改变以及变形都应该属于本发明权利要求的保护范围之内。

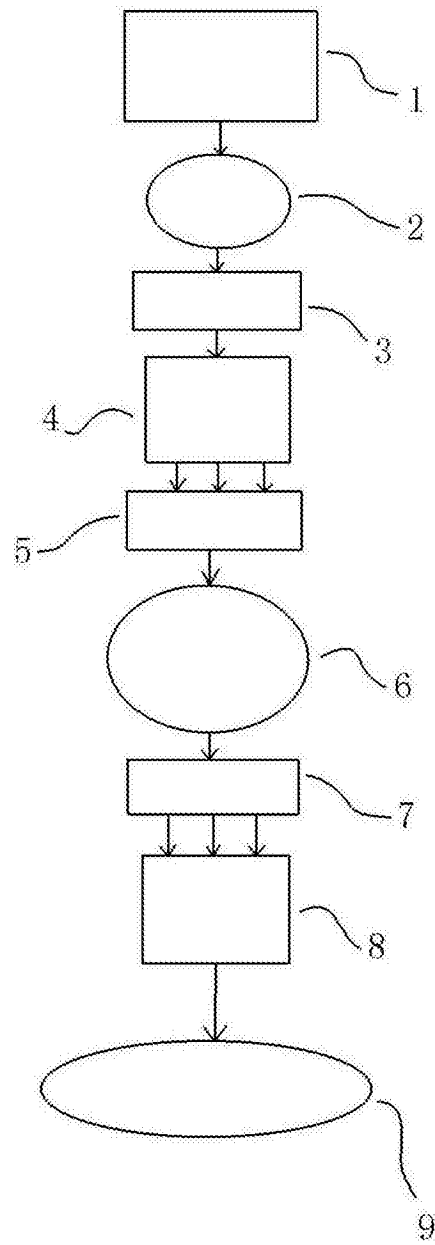


图1

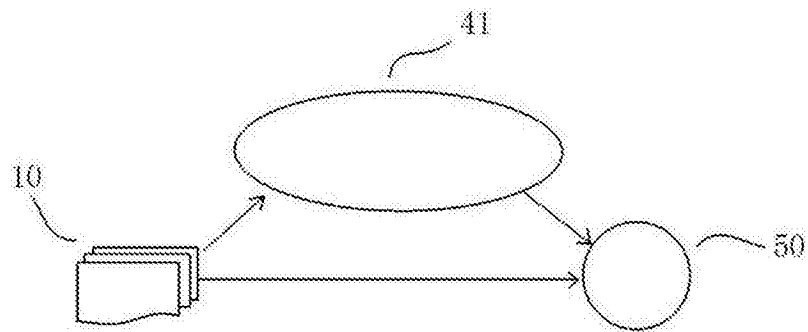


图2

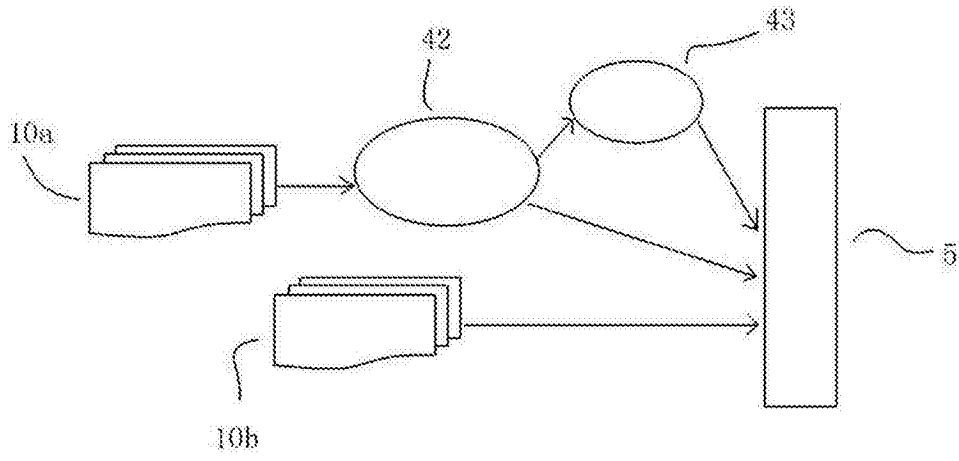


图3