(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112738089 B
(45)授权公告日 2023.03.28

(21)申请号 202011590004.1

(22)申请日 2020.12.29

(65)同一申请的已公布的文献号
申请公布号 CN 112738089 A

(43)申请公布日 2021.04.30

(73)专利权人 中国建设银行股份有限公司
地址 100033 北京市西城区金融大街25号

(72)发明人 李明昊 李巍 杨愚非 瞿威
牛文超 曾锴 蔡啸 陈家书

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 骆宗力

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 111556083 A,2020.08.18
WO 2016188294 A1,2016.12.01

审查员 李云志

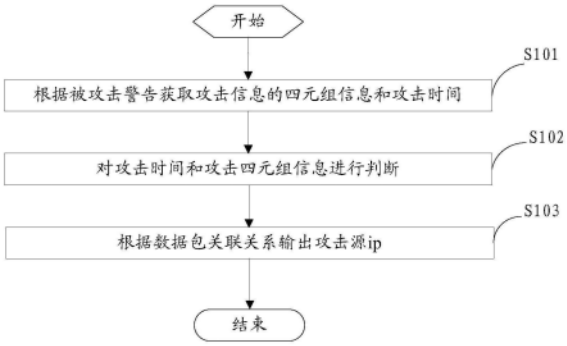
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种复杂网络环境下的源ip自动回溯方法和装置

(57)摘要

本申请提供了一种复杂网络环境下的源ip自动回溯方法和装置，该方法和装置应用于网站，具体为根据被攻击警告获取攻击信息的攻击四元组信息和攻击时间；判断攻击时间是否处于会话的时间内，且攻击四元组信息是否与网站的任一节点的四元组信息相同；如果攻击时间处于会话的时间内，且攻击四元组信息和节点的四元组信息相同，则根据数据包关联关系和节点的四元组信息输出攻击源ip。从而实现源ip的回溯，当发生网络攻击时基于该源ip能够及时找到攻击源。



CN 112738089 B

1.一种复杂网络环境下的源ip自动回溯方法,应用于网站,其特征在于,所述源ip自动回溯方法包括步骤:

响应所述网站的安全设备发出的被攻击警告,获取攻击信息的攻击四元组信息和攻击时间,所述攻击四元组信息为攻击数据包的四元组信息;

判断所述攻击时间是否处于会话的时间内,且所述攻击四元组信息是否与所述网站的任一节点的四元组信息相同;

根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系;

根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系;

如果所述攻击时间处于所述会话的时间内,且所述攻击四元组信息和所述节点的四元组信息相同,则根据所述数据包关联关系和所述节点的四元组信息输出攻击源ip。

2.如权利要求1所述的源ip自动回溯方法,其特征在于,所述根据数据包关联关系和所述节点的四元组信息输出攻击源ip,包括步骤:

输出与所述节点的四元组信息关联的防火墙之前的源ip;

以预设颜色将所述防火墙之前的源ip作为所述攻击源ip予以显示。

3.如权利要求1所述的源ip自动回溯方法,其特征在于,所述根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系,包括步骤:

获取防火墙前的数据包的四元组信息和在tcp层的第一序号;

获取防火墙后的数据包的四元组信息和在tcp层的第二序号;

如果所述第一序号和所述第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为所述数据包关联关系。

4.如权利要求1所述的源ip自动回溯方法,其特征在于,所述根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系,包括步骤:

在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;

在负载均衡设备之后获取所述入访的数据包的XFF字段和XCP字段;

对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为所述数据包关联关系。

5.一种复杂网络环境下的源ip自动回溯中转站,应用于网站,其特征在于,所述源ip自动回溯装置包括:

信息获取模块,用于响应所述网站的安全设备发出的被攻击警告,获取攻击信息的攻击四元组信息和攻击时间,所述攻击四元组信息为攻击数据包的四元组信息;

信息判断模块,用于判断所述攻击时间是否处于会话的时间内,且所述攻击四元组信息是否与所述网站的任一节点的四元组信息相同;

第一关联模块,用于根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两

个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系;

第二关联模块,用于根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系;

攻击源输出模块,用于如果所述攻击时间处于所述会话的时间内,且所述攻击四元组信息和所述节点的四元组信息相同,则所述根据数据包关联关系和所述节点的四元组信息输出攻击源ip。

6.如权利要求5所述的源ip自动回溯装置,其特征在于,所述攻击源输出模块包括:

输出控制单元,用于输出与所述节点的四元组信息关联的防火墙之前的源ip;

显示控制单元,用于以预设颜色将所述防火墙之前的源ip作为所述攻击源ip予以显示。

7.如权利要求5所述的源ip自动回溯装置,其特征在于,所述第一关联模块包括:

第一获取单元,用于获取防火墙前的数据包的四元组信息和在tcp层的第一序号;

第二获取单元,用于获取防火墙后的数据包的四元组信息和在tcp层的第二序号;

第一关联单元,用于如果所述第一序号和所述第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为所述数据包关联关系。

8.如权利要求5所述的源ip自动回溯装置,其特征在于,第二挂链模块包括:

字头处理单元,用于在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;

字头获取单元,用于在负载均衡设备之后获取所述入访的数据包的XFF字段和XCP字段;

第二关联单元,用于对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为所述数据包关联关系。

一种复杂网络环境下的源ip自动回溯方法和装置

技术领域

[0001] 本申请涉及互联网技术领域，更具体地说，涉及一种复杂网络环境下的源ip自动回溯方法和装置。

背景技术

[0002] 随着Web2.0、社交网络、微博等等一系列新型的互联网产品的诞生，基于Web环境的互联网应用越来越广泛，很多业务也都依赖互联网，例如网上银行、网络购物、网游等。且企业信息化的过程中各种应用也都架设在Web平台上，Web业务的迅速发展也引起黑客们的强烈关注，黑客利用网站操作系统的漏洞和Web服务程序的SQL注入漏洞等得到Web服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。

[0003] 当前网站的安全设备仅能对攻击行为单纯进行阻断，无法找到攻击源，但是只有找到攻击源才能够一劳永逸的解决该威胁点。当前网络环境复杂，数据中心日常运行中中，为了安全、负载均衡或ip地址数量的限制，大量的使用了地址转换，导致在发生网络攻击时无法及时有效的找到攻击源，也就就无法彻底阻止黑客的攻击行为。

发明内容

[0004] 有鉴于此，本申请提供一种复杂网络环境下的源ip自动回溯方法和装置，用于根据需要实现源ip的自动回溯，以便于在发生网络攻击时及时找到攻击源。

[0005] 为了实现上述目的，现提出的方案如下：

[0006] 一种复杂网络环境下的源ip自动回溯方法，应用于网站，所述源ip自动回溯方法包括步骤：

[0007] 响应所述网站的安全设备发出的被攻击警告，获取攻击信息的攻击四元组信息和攻击时间；

[0008] 判断所述攻击时间是否处于会话的时间内，且所述攻击四元组信息是否与所述网站的任一节点的四元组信息相同；

[0009] 如果所述攻击时间处于所述会话的时间内，且所述攻击四元组信息和所述节点的四元组信息相同，则根据数据包关联关系和所述节点的四元组信息输出攻击源ip。

[0010] 可选的，所述根据数据包关联关系和所述节点的四元组信息输出攻击源ip，包括步骤：

[0011] 输出与所述节点的四元组信息关联的防火墙之前的源ip；

[0012] 以预设颜色将所述防火墙之前的源ip作为所述攻击源ip予以显示。

[0013] 可选的，还包括步骤：

[0014] 根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包，如果是同一数据包则将此关联关系记录为所述数据包关联关系；

[0015] 根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据

包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系。

[0016] 可选的,所述根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系,包括步骤:

[0017] 获取防火墙前的数据包的四元组信息和在tcp层的第一序号;

[0018] 获取防火墙后的数据包的四元组信息和在tcp层的第二序号;

[0019] 如果所述第一序号和所述第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为所述数据包关联关系。

[0020] 可选的,所述根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系,包括步骤:

[0021] 在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;

[0022] 在负载均衡设备之后获取所述入访的数据包的XFF字段和XCP字段;

[0023] 对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为所述数据包关联关系。

[0024] 一种复杂网络环境下的源ip自动回溯中转站,应用于网站,所述源ip自动回溯装置包括:

[0025] 信息获取模块,用于响应所述网站的安全设备发出的被攻击警告,获取攻击信息的攻击四元组信息和攻击时间;

[0026] 信息判断模块,用于判断所述攻击时间是否处于会话的时间内,且所述攻击四元组信息是否与所述网站的任一节点的四元组信息相同;

[0027] 攻击源输出模块,用于如果所述攻击时间处于所述会话的时间内,且所述攻击四元组信息和所述节点的四元组信息相同,则根据数据包关联关系和所述节点的四元组信息输出攻击源ip。

[0028] 可选的,所述攻击源输出模块包括:

[0029] 输出控制单元,用于输出与所述节点的四元组信息关联的防火墙之前的源ip;

[0030] 显示控制单元,用于以预设颜色将所述防火墙之前的源ip作为所述攻击源ip予以显示。

[0031] 可选的,还包括:

[0032] 第一关联模块,用于根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系;

[0033] 第二关联模块,用于根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为所述数据包关联关系。

[0034] 可选的,所述第一关联模块包括:

[0035] 第一获取单元,用于获取防火墙前的数据包的四元组信息和在tcp层的第一序号;

[0036] 第二获取单元,用于获取防火墙后的数据包的四元组信息和在tcp层的第二序号;

[0037] 第一关联单元,用于如果所述第一序号和所述第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为所述数据包关联关系。

[0038] 可选的,所述第二挂链模块包括:

[0039] 字头处理单元,用于在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;

[0040] 字头获取单元,用于在负载均衡设备之后获取所述入访的数据包的XFF字段和XCP字段;

[0041] 第二关联单元,用于对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为所述数据包关联关系。

[0042] 从上述的技术方案可以看出,本申请公开了一种复杂网络环境下的源ip自动回溯方法和装置,该方法和装置应用于网站,具体为根据被攻击警告获取攻击信息的攻击四元组信息和攻击时间;判断攻击时间是否处于会话的时间内,且攻击四元组信息是否与网站的任一节点的四元组信息相同;如果攻击时间处于会话的时间内,且攻击四元组信息和节点的四元组信息相同,则根据数据包关联关系和节点的四元组信息输出攻击源ip。从而实现源ip的回溯,当发生网络攻击时基于该源ip能够及时找到攻击源。

附图说明

[0043] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0044] 图1为一种源ip回溯系统的示意图;

[0045] 图2为另一种源ip回溯系统的示意图;

[0046] 图3为本申请实施例的一种复杂网络环境下的源ip自动回溯方法的流程图;

[0047] 图4为本申请实施例的一种四元组信息关联方法的流程图;

[0048] 图5为本申请实施例的一种复杂网络环境下的源ip自动回溯装置的框图;

[0049] 图6为本申请实施例的另一种复杂网络环境下的源ip自动回溯装置的框图。

具体实施方式

[0050] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0051] 当前数据中心,一般真实源ip的回溯是通过负载均衡在http头部插入x-forwarded-for(XFF)字段来解决该问题,但是图1中的情况,却无法通过XFF来解决真实源ip的回溯问题,同时也无法通过http头部字段进行关联,确定真实源ip地址。本方法为解决该问题,设计了针对该场景下的源ip自动回溯系统。

[0052] 同一系统在每个节点的目的ip和目的port均一致,其中各设备操作如下:

[0053] 防火墙设备(FW):

[0054] a.对源ip进行了多对一或多对多的地址转换;

[0055] b.源port此时呈现为随机端口;

[0056] c.目的ip和目的port进行了一对一的转换;

[0057] 加解密设备(SSL):

[0058] a.对进入ssl设备的数据流进行解密;

[0059] b.源ip和源port不进行转换;

[0060] c.目的ip和目的port进行了一对一的转换;

[0061] 负载均衡设备(LB):

[0062] a.为一个七层代理设备;

[0063] b.对源ip转换进行了多对多的地址转换;

[0064] c.源port此时呈现为随机端口;

[0065] d.目的ip和目的port进行了一对一的转换;

[0066] 负载均衡设备将源ip通过XFF字段插入到http头部,对真实用户的源ip进行回溯分析。

[0067] 如图2所示,对于服务器,其通过XFF字段看到用户1、2、3的ip地址均为sf-ip1,此时通过XFF字段无法区分用户。

[0068] 基于以上分析,本申请提供下面的实施例,以解决攻击源ip回溯问题。

[0069] 实施例一

[0070] 图3为本申请实施例的一种复杂网络环境下的源ip自动回溯方法的流程图。

[0071] 如图3所示,本实施例提供的源ip自动回溯方法应用于网站等网络环境,其具体包括如下步骤:

[0072] S101、根据被攻击警告获取攻击信息的四元组信息和攻击时间。

[0073] 即在网站的安全设备发出被攻击警告时,第一时间对被确定的攻击信息进行处理,从中得到该攻击信息或者说用于攻击的数据包的四元组信息和攻击时间,为了方便描述,鉴于该四元组信息为攻击数据包的四元组信息,我们将此四元组信息描述为攻击四元组信息。

[0074] S102、对攻击时间和攻击四元组信息进行判断。

[0075] 即对攻击时间是否处于会话时间内,且攻击四元组信息是否与该网站的任一节点的四元组信息相同。

[0076] S103、根据数据包关联关系输出攻击源ip。

[0077] 通过上面的比较,如果该攻击时间处于该会话时间内,且攻击四元组信息与网站内四元组信息相同,此时判定该网站内的四元组信息与攻击数据包的四元组信息有关联关系,此时根据该网站内的四元组信息的源ip输出攻击源ip,从而实现源ip的回溯。

[0078] 在具体实施时,在确定关联关系后,输出与节点的四元组信息关联的防火墙前的源ip作为该攻击源ip;在输出时,以预设颜色如红色将该攻击源ip予以显示。

[0079] 从上述技术方案可以看出,本实施例提供了一种复杂网络环境下的源ip自动回溯方法,该方法应用于网站,具体为根据被攻击警告获取攻击信息的攻击四元组信息和攻击

时间;判断攻击时间是否处于会话的时间内,且攻击四元组信息是否与网站的任一节点的四元组信息相同;如果攻击时间处于会话的时间内,且攻击四元组信息和节点的四元组信息相同,则根据数据包关联关系和节点的四元组信息输出攻击源ip。从而实现源ip的回溯,当发生网络攻击时基于该源ip能够及时找到攻击源。

[0080] 另外,在本实施例中还包括相应的关联方案,用于将同一数据包进行关联处理,具体包括如下步骤,如图4所示。

[0081] S201、根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为数据包关联关系。

[0082] 在具体实施时,首先,获取防火墙前的数据包的四元组信息和在tcp层的序号,将其描述为第一序号;

[0083] 然后,获取防火墙后的数据包的四元组信息和在tcp层的序号,将其描述为第二序号;

[0084] 最后,如果第一序号和第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为数据包关联关系。

[0085] S202、根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为数据包关联关系。

[0086] 具体实施时,首先,在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;XCP是X-Client-Port的缩写,意思是客户端端口.

[0087] 然后,在负载均衡设备之后获取入访的数据包的XFF字段和XCP字段;

[0088] 最后,对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为数据包关联关系。

[0089] 实施例二

[0090] 图5为本申请实施例的一种复杂网络环境下的源ip自动回溯装置的框图。

[0091] 如图5所示,本实施例提供的源ip自动回溯装置应用于网站等网络环境,其具体包括信息获取模块10、信息判断模块20和攻击源输出模块30。

[0092] 信息获取模块用于根据被攻击警告获取攻击信息的四元组信息和攻击时间。

[0093] 即在网站的安全设备发出被攻击警告时,第一时间对被确定的攻击信息进行处理,从中得到该攻击信息或者说用于攻击的数据包的四元组信息和攻击时间,为了方便描述,鉴于该四元组信息为攻击数据包的四元组信息,我们将此四元组信息描述为攻击四元组信息。

[0094] 信息判断模块用于对攻击时间和攻击四元组信息进行判断。

[0095] 即对攻击时间是否处于会话时间内,且攻击四元组信息是否与该网站的任一节点的四元组信息相同。

[0096] 攻击源输出模块用于根据数据包关联关系输出攻击源ip。

[0097] 通过上面的比较,如果该攻击时间处于该会话时间内,且攻击四元组信息与网站内四元组信息相同,此时判定该网站内的四元组信息与攻击数据包的四元组信息有关联关系,此时根据该网站内的四元组信息的源ip输出攻击源ip,从而实现源ip的回溯。

[0098] 该模块具体包括输出控制单元和显示控制单元,输出控制单元用于在确定关联关

系后,输出与节点的四元组信息关联的防火墙前的源ip作为该攻击源ip;显示控制单元用于在输出控制单元输出时,以预设颜色如红色将该攻击源ip予以显示。

[0099] 从上述技术方案可以看出,本实施例提供了一种复杂网络环境下的源ip自动回溯装置,该装置应用于网站,具体为根据被攻击警告获取攻击信息的攻击四元组信息和攻击时间;判断攻击时间是否处于会话的时间内,且攻击四元组信息是否与网站的任一节点的四元组信息相同;如果攻击时间处于会话的时间内,且攻击四元组信息和节点的四元组信息相同,则根据数据包关联关系和节点的四元组信息输出攻击源ip。从而实现源ip的回溯,当发生网络攻击时基于该源ip能够及时找到攻击源。

[0100] 另外,在本实施例中还包括相应的关联方案,用于将同一数据包进行关联处理,即本实施例还包括第一关联模块40和第二关联模块,如图6所示。

[0101] 第一关联模块用于根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为数据包关联关系;该模块包括第一获取单元、第二获取单元和第一关联单元。

[0102] 第一获取单元用于获取防火墙前的数据包的四元组信息和在tcp层的序号,将其描述为第一序号;

[0103] 第二获取单元用于获取防火墙后的数据包的四元组信息和在tcp层的序号,将其描述为第二序号;

[0104] 如果第一序号和第二序号相同,则防火墙前的数据包与防火墙后的数据包为同一数据包,此时第一关联单元用于将防火墙前数据包的四元组信息和防火墙后的四元组信息进行关联,并记录为数据包关联关系。

[0105] 第二关联模块用于根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包,如果是同一数据包则将此关联关系记录为数据包关联关系。该模块包括字头处理单元、字头获取单元和第二关联单元。

[0106] 字头处理单元用于在负载均衡设备之前在入访的数据包的http头上通过XFF字段和XCP字段加上源ip和源端口;

[0107] 字头获取单元用于在负载均衡设备之后获取入访的数据包的XFF字段和XCP字段;

[0108] 第二关联单元用于对源ip和源端口与XFF字段和XCP字段的源ip和源端口进行比较,如果两者相同,则将负载均衡设备前后的数据包记录为数据包关联关系。

[0109] 本说明书中的各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似的部分互相参见即可。

[0110] 本领域内的技术人员应明白,本发明实施例的实施例可提供为方法、装置、或计算机程序产品。因此,本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0111] 本发明实施例是参照根据本发明实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设

备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0112] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0113] 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0114] 尽管已描述了本发明实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明实施例范围的所有变更和修改。

[0115] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0116] 以上对本发明所提供的技术方案进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

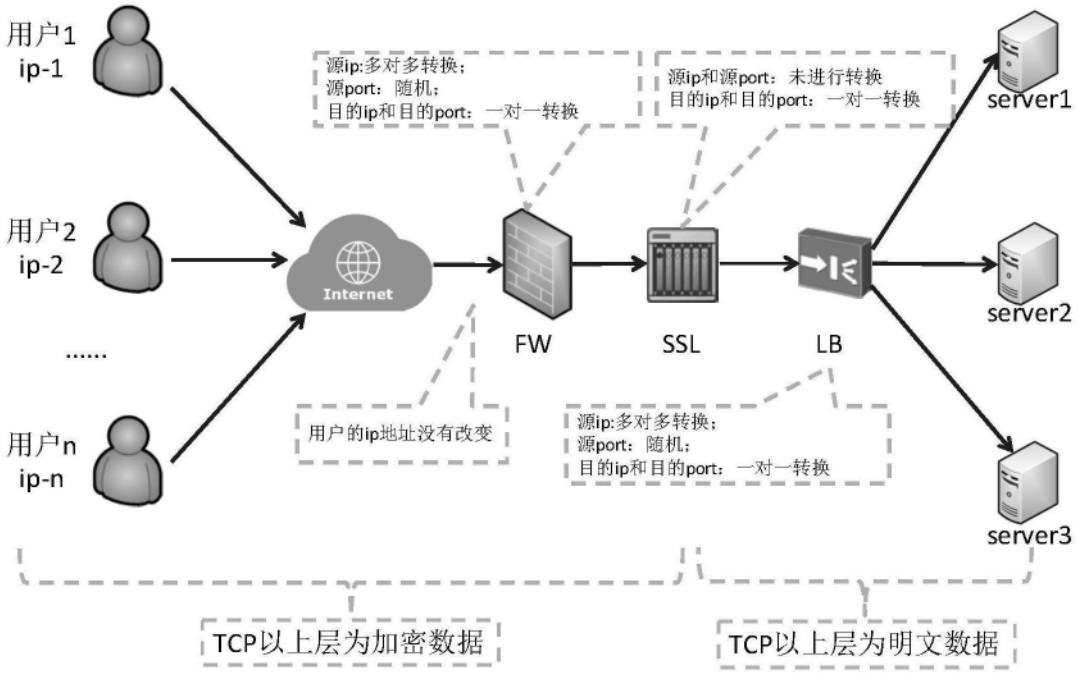

用户1
ip-1
用户2
ip-2
.....
用户n
ip-n
Internet
源ip:多对多转换；
源port：随机；
目的ip和目的port：一对一转换
源ip和源port：未进行转换
目的ip和目的port：一对一转换
FW
SSL
LB
server1
server2
server3
用户的ip地址没有改变
源ip:多对多转换；
源port：随机；
目的ip和目的port：一对一转换
TCP以上层为加密数据
TCP以上层为明文数据

图1

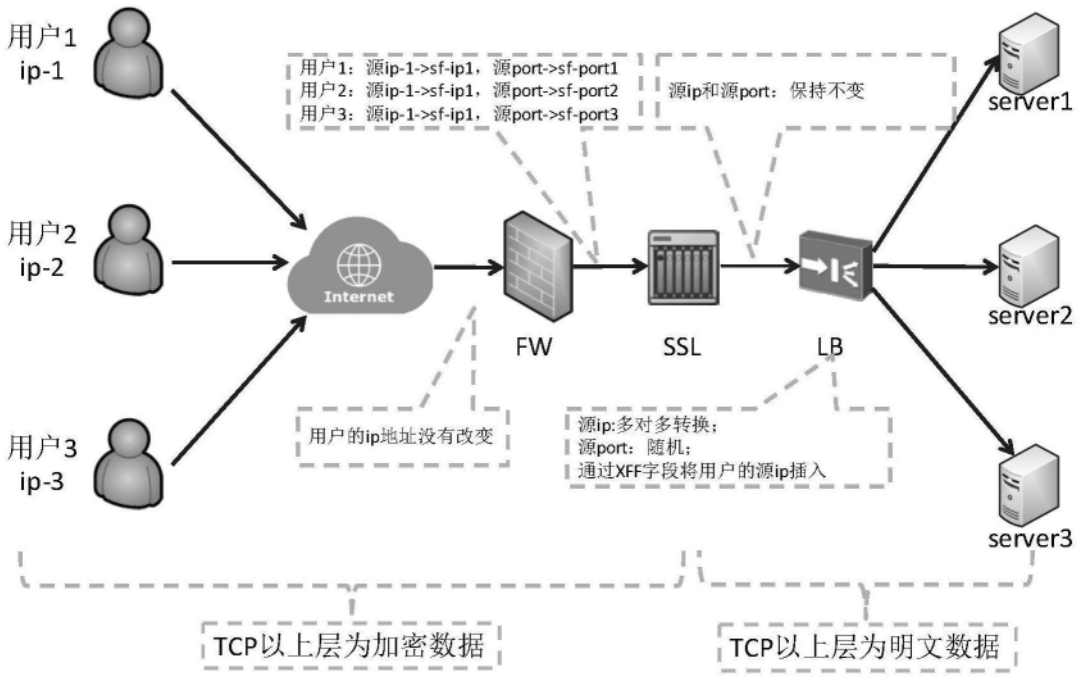

用户1
ip-1
用户2
ip-2
用户3
ip-3
Internet
用户1：源ip-1->sf-ip1，源port->sf-port1
用户2：源ip-1->sf-ip1，源port->sf-port2
用户3：源ip-1->sf-ip1，源port->sf-port3
源ip和源port：保持不变
FW
SSL
LB
server1
server2
server3
用户的ip地址没有改变
源ip:多对多转换；
源port：随机；
通过XFF字段将用户的源ip插入
TCP以上层为加密数据
TCP以上层为明文数据

图2

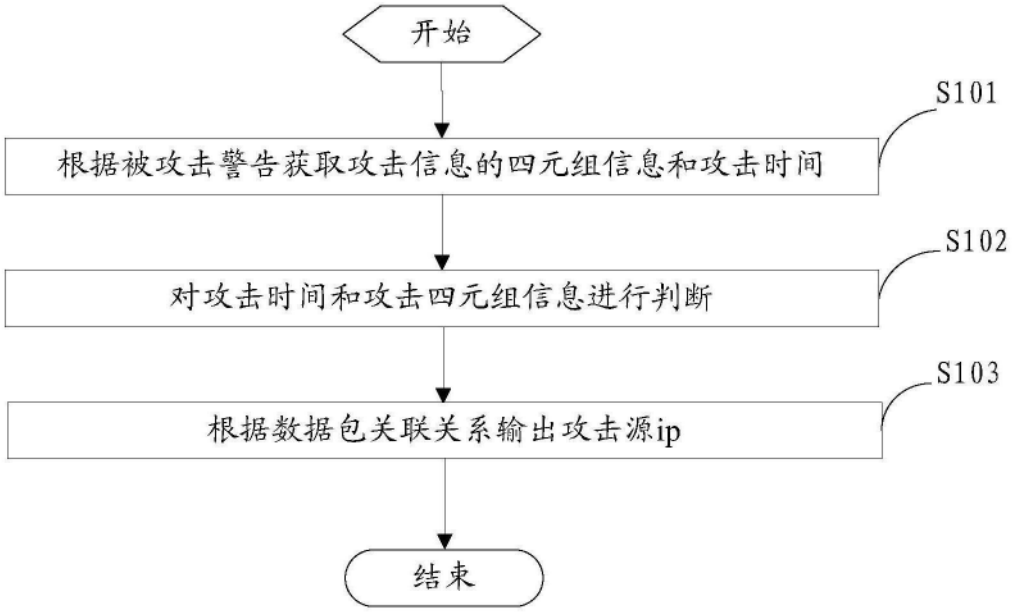

开始
S101
根据被攻击警告获取攻击信息的四元组信息和攻击时间
S102
对攻击时间和攻击四元组信息进行判断
S103
根据数据包关联关系输出攻击源ip
结束

图3

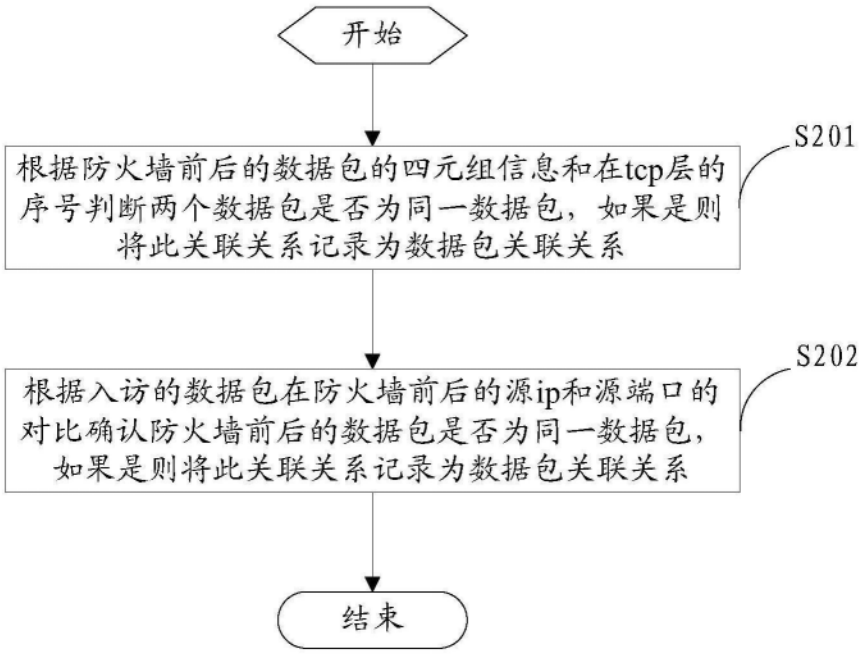

开始
S201
根据防火墙前后的数据包的四元组信息和在tcp层的序号判断两个数据包是否为同一数据包，如果是则将此关联关系记录为数据包关联关系
S202
根据入访的数据包在防火墙前后的源ip和源端口的对比确认防火墙前后的数据包是否为同一数据包，如果是则将此关联关系记录为数据包关联关系
结束

图4


信息获取模块
10
信息判断模块
20
攻击源输出模块
30

图5

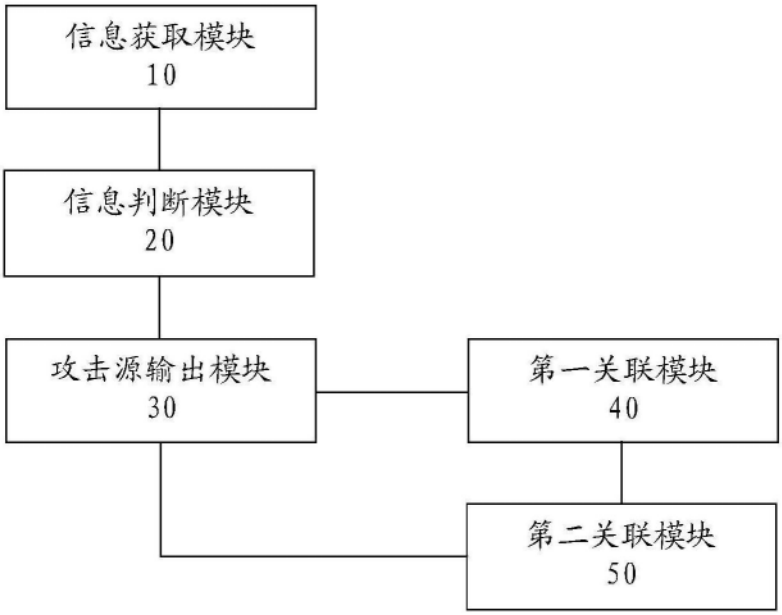

信息获取模块
10
信息判断模块
20
攻击源输出模块
30
第一关联模块
40
第二关联模块
50

图6