(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112422554 B
(45)授权公告日 2023.04.07

(21)申请号 202011284730.0

(22)申请日 2020.11.17

(65)同一申请的已公布的文献号
申请公布号 CN 112422554 A

(43)申请公布日 2021.02.26

(73)专利权人 杭州安恒信息技术股份有限公司
地址 310000 浙江省杭州市滨江区西兴街道联慧街188号

(72)发明人 柏琼涛 范渊 刘博

(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 张春辉

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

(56)对比文件
CN 109918902 A,2019.06.21
CN 110958251 A,2020.04.03
US 2008137542 A1,2008.06.12

审查员 程慧

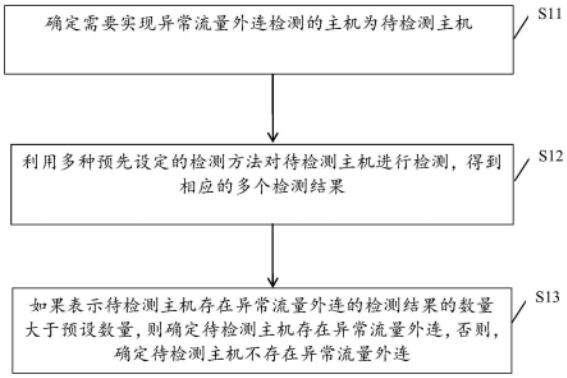
权利要求书2页 说明书11页 附图1页

(54)发明名称

一种检测异常流量外连的方法、装置、设备及存储介质

(57)摘要

本发明公开了一种检测异常流量外连的方法、装置、设备及存储介质，该方法包括：确定需要实现异常流量外连检测的主机为待检测主机；利用多种预先设定的检测方法对所述待检测主机进行检测，得到相应的多个检测结果；如果表示所述待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定所述待检测主机存在异常流量外连，否则，确定所述待检测主机不存在异常流量外连。可见，本申请中基于多种检测方法综合实现主机是否存在异常流量外连的检测，从而相对于现有技术中单一检测方法实现主机是否存在异常流量外连的检测，能够大大增加检测的准确性，有效降低检测的误报率。




CN 112422554 B

1.一种检测异常流量外连的方法,其特征在于,包括:

确定需要实现异常流量外连检测的主机为待检测主机;

利用多种预先设定的检测方法对所述待检测主机进行检测,得到相应的多个检测结果,所述多种预先设定的检测方法包括流量检测方法、位置检测方法、情报库检测方法、行为检测方法和会话检测方法中的任意几种;

如果表示所述待检测主机存在异常流量外连的检测结果的数量大于预设数量,则确定所述待检测主机存在异常流量外连,否则,确定所述待检测主机不存在异常流量外连;

利用所述流量检测方法对所述待检测主机进行检测得到相应的检测结果,包括:

获取距离当前时刻最近的第一预设时间段内所述待检测主机的流入数据量及流出数据量,将所述流入数据量及所述流出数据量相加得到数据量和值,如果所述流出数据量占所述数据量和值的比值大于预设比值,和/或所述流出数据量大于第一数据量,则得到表示所述待检测主机存在异常流量外连的检测结果,否则,得到表示所述待检测主机不存在异常流量外连的检测结果;

利用所述位置检测方法对所述待检测主机进行检测得到相应的检测结果,包括:

获取所述待检测主机的流出数据量所流向的设备所在物理位置为目的位置,如果在距离当前时刻最近的第二预设时间段内,所述待检测主机流向所述目的位置的流出数据量持续大于第二数据量,则得到表示所述待检测主机存在异常流量外连的检测结果,否则,得到表示所述待检测主机不存在异常流量外连的检测结果。

2.根据权利要求1所述的方法,其特征在于,所述检测方法包括情报库检测方法,利用所述情报库检测方法对所述待检测主机进行检测得到相应的检测结果,包括:

获取所述待检测主机的流出数据量所流向的设备的地址为目的地址,将所述目的地址与预先设置的情报库中各地址进行比对,如果所述情报库中存在与所述目的地址相同的地址,则得到表示所述待检测主机存在异常流量外连的检测结果,否则,得到表示所述待检测主机不存在异常流量外连的检测结果;其中,所述情报库中各地址为连接相应主机后使得所连接的主机发生异常流量外连的设备的地址。

3.根据权利要求2所述的方法,其特征在于,所述检测方法包括行为检测方法,利用所述行为检测方法对所述待检测主机进行检测得到相应的检测结果,包括:

获取所述待检测主机当前的行为特征为目的行为特征,并将所述目的行为特征与特征库中各行为特征进行比对,如果所述特征库中存在与所述目的行为特征相同的行为特征,则得到表示所述待检测主机不存在异常流量外连的检测结果,否则,得到表示所述待检测主机存在异常流量外连的检测结果;其中,所述特征库中行为特征为所述待检测主机正常情况下的行为特征。

4.根据权利要求3所述的方法,其特征在于,所述检测方法包括会话检测方法,利用所述会话检测方法对所述待检测主机进行检测得到相应的检测结果,包括:

监测所述待检测主机对应的各项会话,如果所述待测主机对应的会话符合预先设定的异常条件,则得到表示所述待检测主机存在异常流量外连的检测结果,否则,得到表示所述待检测主机不存在异常流量外连的检测结果;其中,所述异常条件为所述待检测主机存在异常流量外连时其具有的会话所体现的特征。

5.一种检测异常流量外连的装置,其特征在于,包括:

确定模块，用于：确定需要实现异常流量外连检测的主机为待检测主机；

检测模块，用于：利用多种预先设定的检测方法对所述待检测主机进行检测，得到相应的多个检测结果，所述多种预先设定的检测方法包括流量检测方法、位置检测方法、情报库检测方法、行为检测方法和会话检测方法中的任意几种；

判定模块，用于：如果表示所述待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定所述待检测主机存在异常流量外连，否则，确定所述待检测主机不存在异常流量外连；

所述检测模块，包括：

第一检测单元，用于：获取距离当前时刻最近的第一预设时间段内待检测主机的流入数据量及流出数据量，将流入数据量及流出数据量相加得到数据量和值，如果流出数据量占数据量和值的比值大于预设比值，和/或流出数据量大于第一数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果；

所述检测模块，包括：

第二检测单元，用于：获取待检测主机的流出数据量所流向的设备所在物理位置为目的位置，如果在距离当前时刻最近的第二预设时间段内，待检测主机流向目的位置的流出数据量持续大于第二数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果。

6.一种检测异常流量外连的设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如权利要求1至4任一项所述检测异常流量外连的方法的步骤。

7.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至4任一项所述检测异常流量外连的方法的步骤。

# 一种检测异常流量外连的方法、装置、设备及存储介质

## 技术领域

[0001] 本发明涉及流量检测技术领域，更具体地说，涉及一种检测异常流量外连的方法、装置、设备及存储介质。

## 背景技术

[0002] 如果主机发生异常流量外连行为，则说明该主机已经失陷，主机被攻击者挂马或者控制，导致的直接结果则是主机敏感数据包、个人信息等被攻击者窃取回传，更严重情况攻击者会通过控制主机对局域网内其他主机横向控制导致更大的损失，因此对异常流量外连行为的检测则异常重要；目前常见的安全检测设备、安全检测软件是针对流量检测异常流量外连行为的，但是发明人发现，这种检测方法存在误报率较高的问题。

## 发明内容

[0003] 本发明的目的是提供一种检测异常流量外连的方法、装置、设备及存储介质，能够有效降低异常流量外连检测的误报率。

[0004] 为了实现上述目的，本发明提供如下技术方案：

[0005] 一种检测异常流量外连的方法，包括：

[0006] 确定需要实现异常流量外连检测的主机为待检测主机；

[0007] 利用多种预先设定的检测方法对所述待检测主机进行检测，得到相应的多个检测结果；

[0008] 如果表示所述待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定所述待检测主机存在异常流量外连，否则，确定所述待检测主机不存在异常流量外连。

[0009] 优选的，确定所述待检测主机存在异常流量外连之后，还包括：

[0010] 获取每个所述检测结果中包含的源地址，并确定值相同的源地址占全部源地址的百分比为所述待检测主机存在异常流量外连的可能性百分比；

[0011] 或者获取每个所述检测结果中包含的目的地址，并确定值相同的目的地址占全部目的地址的百分比为所述待检测主机存在异常流量外连的可能性百分比。

[0012] 优选的，所述检测方法包括流量检测方法，利用所述流量检测方法对所述待检测主机进行检测得到相应的检测结果，包括：

[0013] 获取距离当前时刻最近的第一预设时间段内所述待检测主机的流入数据量及流出数据量，将所述流入数据量及所述流出数据量相加得到数据量和值，如果所述流出数据量占所述数据量和值的比值大于预设比值，和/或所述流出数据量大于第一数据量，则得到表示所述待检测主机存在异常流量外连的检测结果，否则，得到表示所述待检测主机不存在异常流量外连的检测结果。

[0014] 优选的，所述检测方法包括位置检测方法，利用所述位置检测方法对所述待检测主机进行检测得到相应的检测结果，包括：

[0015] 获取所述待检测主机的流出数据量所流向的设备所在物理位置为目的位置，如果

在距离当前时刻最近的第二预设时间段内，所述待检测主机流向所述目的位置的流出数据量持续大于第二数据量，则得到表示所述待检测主机存在异常流量外连的检测结果，否则，得到表示所述待检测主机不存在异常流量外连的检测结果。

[0016] 优选的，所述检测方法包括情报库检测方法，利用所述情报库检测方法对所述待检测主机进行检测得到相应的检测结果，包括：

[0017] 获取所述待检测主机的流出数据量所流向的设备的地址为目的地址，将所述目的地址与预先设置的情报库中各地址进行比对，如果所述情报库中存在与所述目的地址相同的地址，则得到表示所述待检测主机存在异常流量外连的检测结果，否则，得到表示所述待检测主机不存在异常流量外连的检测结果；其中，所述情报库中各地址为连接相应主机后使得所连接的主机发生异常流量外连的设备的地址。

[0018] 优选的，所述检测方法包括行为检测方法，利用所述行为检测方法对所述待检测主机进行检测得到相应的检测结果，包括：

[0019] 获取所述待检测主机当前的行为特征为目的行为特征，并将所述目的行为特征与特征库中各行为特征进行比对，如果所述行为库中存在与所述目的行为特征相同的行为特征，则得到表示所述待检测主机不存在异常流量外连的检测结果，否则，得到表示所述待检测主机存在异常流量外连的检测结果；其中，所述特征库中行为特征为所述待检测主机正常情况下的行为特征。

[0020] 优选的，所述检测方法包括会话检测方法，利用所述会话检测方法对所述待检测主机进行检测得到相应的检测结果，包括：

[0021] 监测所述待检测主机对应的各项会话，如果所述待测主机对应的会话符合预先设定的异常条件，则得到表示所述待检测主机存在异常流量外连的检测结果，否则，得到表示所述待检测主机不存在异常流量外连的检测结果；其中，所述异常条件为所述待检测主机存在异常流量外连时其具有的会话所体现的特征。

[0022] 一种检测异常流量外连的装置，包括：

[0023] 确定模块，用于：确定需要实现异常流量外连检测的主机为待检测主机；

[0024] 检测模块，用于：利用多种预先设定的检测方法对所述待检测主机进行检测，得到相应的多个检测结果；

[0025] 判定模块，用于：如果表示所述待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定所述待检测主机存在异常流量外连，否则，确定所述待检测主机不存在异常流量外连。

[0026] 一种检测异常流量外连的设备，包括：

[0027] 存储器，用于存储计算机程序；

[0028] 处理器，用于执行所述计算机程序时实现如上任一项所述检测异常流量外连的方法的步骤。

[0029] 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上任一项所述检测异常流量外连的方法的步骤。

[0030] 本发明提供了一种检测异常流量外连的方法、装置、设备及存储介质，该方法包括：确定需要实现异常流量外连检测的主机为待检测主机；利用多种预先设定的检测方法对所述待检测主机进行检测，得到相应的多个检测结果；如果表示所述待检测主机存在异

常流量外连的检测结果的数量大于预设数量，则确定所述待检测主机存在异常流量外连，否则，确定所述待检测主机不存在异常流量外连。本申请公开的技术方案中，对于需要实现异常流量外连检测的主机，通过预先设定的多种检测方法对主机实现异常流量外连的检测，进而通过对该多种检测方法所得检测结果的关联分析，确定主机是否存在异常流量外连；可见，本申请中基于多种检测方法综合实现主机是否存在异常流量外连的检测，从而相对于现有技术中单一检测方法实现主机是否存在异常流量外连的检测，能够大大增加检测的准确性，有效降低检测的误报率。

## 附图说明

[0031] 为了更清楚地说明本发明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发明的实施例，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，还可以根据提供的附图获得其他的附图。

[0032] 图1为本发明实施例提供的一种检测异常流量外连的方法的流程图；

[0033] 图2为本发明实施例提供的一种检测异常流量外连的方法的实现示例图；

[0034] 图3为本发明实施例提供的一种检测异常流量外连的装置的结构示意图。

## 具体实施方式

[0035] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0036] 请参阅图1，其示出了本发明实施例提供的一种检测异常流量外连的方法的流程图，可以包括：

[0037] S11：确定需要实现异常流量外连检测的主机为待检测主机。

[0038] 本发明实施例提供的一种检测异常流量外连的方法的执行主体可以为对应的装置；在需要对某主机进行异常流量外连的检测时，可以确定该需要进行异常流量外连的检测的主机为待检测主机，进而对待检测主机实现相应的异常流量外连的检测。

[0039] S12：利用多种预先设定的检测方法对待检测主机进行检测，得到相应的多个检测结果。

[0040] 在对待检测主机进行异常流量外连的检测时，可以利用预先设定的多种检测方法分别对待检测主机进行异常流量外连的检测，从而得到分别与每种检测方法对应的结果作为检测结果，也即本申请利用每种预先设定的检测方法分别对待检测主机进行异常流量外连的检测，从而得到分别与每种检测方法一一对应的检测结果。其中，不同的检测方法可以是基于待检测主机对应不同参数实现的，如可以基于待检测主机的流量实现、基于与待检测主机通信的位置实现、基于与待检测主机通信的地址实现、基于待检测主机的行为特征实现、基于待检测主机的会话实现等，进而通过待检测主机的不同参数实现对其是否发生异常流量外连行为的检测。

[0041] S13：如果表示待检测主机存在异常流量外连的检测结果的数量大于预设数量，则

确定待检测主机存在异常流量外连，否则，确定待检测主机不存在异常流量外连。

[0042] 在得到表示待检测主机是否存在异常流量外连的每个检测结果中，可以对这些检测结果进行关联分析，如果表示待检测主机存在异常流量外连行为的检测结果的数量大于预设数量，则说明具有足够多的检测方法检测出待检测主机存在异常流量外连行为，因此，可以基于此确定待检测主机存在异常流量外连行为，否则，说明具有足够多的检测方法检测出待检测主机不存在异常流量外连行为，因此，可以基于此确定待检测主机不存在异常流量外连行为，从而通过这种方式，实现多种检测方法所得检测结果的统计。另外，预设数量可以根据实际进行设定，如可以设定为检测方法的总数量的二分之一，由此，在确定待检测主机是否存在异常流量外连时则是以大部分检测方法对应检测结果为准，当然根据实际需要进行的其他设定也均在本发明的保护范围之内。

[0043] 本申请公开的技术方案中，对于需要实现异常流量外连检测的主机，通过预先设定的多种检测方法对主机实现异常流量外连的检测，进而通过对该多种检测方法所得检测结果的关联分析，确定主机是否存在异常流量外连；可见，本申请中基于多种检测方法综合实现主机是否存在异常流量外连的检测，从而相对于现有技术中单一检测方法实现主机是否存在异常流量外连的检测，能够大大增加检测的准确性，有效降低检测的误报率。

[0044] 本发明实施例提供的一种检测异常流量外连的方法，确定待检测主机存在异常流量外连之后，还可以包括：

[0045] 获取每个检测结果中包含的源地址，并确定值相同的源地址占全部源地址的百分比为待检测主机存在异常流量外连的可能性百分比；

[0046] 或者获取每个检测结果中包含的目的地址，并确定值相同的目的地址占全部目的地址的百分比为待检测主机存在异常流量外连的可能性百分比。

[0047] 需要说明的是，每种检测方法对待检测主机进行异常流量外连行为的检测后得出的检测结果，还会包括srcAddress的字段及destAddress的字段，其中，srcAddress(源地址)则为待检测主机与其他设备之间进行数据包通信时发送数据包的一方，而destAddress(目的地址)则为待检测主机与其他设备之间进行数据包通信时接收数据包的一方。本申请实施例在确定出待检测主机存在异常流量外连行为后，还会通过检测结果中包含的上述字段确定得出的待检测主机存在异常流量外连行为这一结果的准确性或者说待检测主机存在异常流量外连行为的可能性；具体来说，在基于源地址确定待检测主机存在异常流量外连行为的可能性时，本申请实施例可以获取每个检测结果中srcAddress的字段的值，如果这些值是相同的(也即为同一个IP地址)，则可以确定待检测主机100％存在异常流量外连行为，也即待检测主机存在异常流量外连行为的可能性为100％，如果这些值各不相同，则可以确定待检测主机0％存在异常流量外连行为，也即待检测主机存在异常流量外连行为的可能性为0％，而其他情况下则确定源地址的值相同的检测结果数量占全部检测结果数量的百分比则为待检测主机存在异常流量外连行为的百分比，从而基于各检测结果中的源地址统计得到待检测主机存在异常流量外连行为的可能性大小，供工作人员基于此进一步实现对待检测主机是否存在异常流量外连行为的判定；在基于目的地址确定待检测主机存在异常流量外连行为的可能性时，本申请实施例可以获取每个检测结果中srcAddress的字段的值，如果这些值是相同的(也即为同一个IP地址)，则可以确定待检测主机100％存在异常流量外连行为，也即待检测主机存在异常流量外连行为的可能性为100％，如果这些值各

不相同，则可以确定待检测主机0％存在异常流量外连行为，也即待检测主机存在异常流量外连行为的可能性为0％，而其他情况下则确定目的地址的值相同的检测结果数量占全部检测结果数量的百分比则为待检测主机存在异常流量外连行为的百分比，从而基于各检测结果中的目的地址统计得到待检测主机存在异常流量外连行为的可能性大小，供工作人员基于此进一步实现对待检测主机是否存在异常流量外连行为的判定。可见，本申请中基于不同检测结果中包含的地址的值得到待检测主机是否存在异常流量外连行为的可能性大小，供工作人员在实现待检测主机的异常流量外连行为检测时作参考，进一步保证了对待检测主机是否存在异常流量外连行为判定时的准确性。

[0048] 本发明实施例提供的一种检测异常流量外连的方法，检测方法包括流量检测方法，利用流量检测方法对待检测主机进行检测得到相应的检测结果，可以包括：

[0049] 获取距离当前时刻最近的第一预设时间段内待检测主机的流入数据量及流出数据量，将流入数据量及流出数据量相加得到数据量和值，如果流出数据量占数据量和值的比值大于预设比值，和/或流出数据量大于第一数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果。

[0050] 其中，流入数据量则为待检测主机接收的数据包的量，而流出数据量则为待检测主机发送的数据包的量，第一预设时间段可以根据实际需要进行设定，如可以为12小时、24小时等；预设比值可以根据实际需要进行设定，如1.5、2等，一般为在待检测主机未发生异常流量外连行为时，流出数据量占全部数据量(流出数据量及流入数据量的和)的最大比值；第一数据量也可以根据实际需要进行设定，一般为在待检测主机未发生异常流量外连行为时，流出数据量的最大值。由于主机存在异常流量外连行为时，通常会大量流出数据包，或者流出数据包远多于流入数据包，因此本申请中获取刚过去的一段时间内待检测数据包的流入数据量及流出数据量后，则可以得到这段时间内流出数据量在全部数据量的占比，如果该占比过大(也即大于预设比值)和/或该流出数据量大于第一数据量，则可以确定待检测主机存在异常流量外连行为，否则，确定待检测主机不存在异常流量外连行为。从而通过这种流量检测方法可以简便有效的确定出待检测主机是否存在异常流量外连。

[0051] 在一种具体实现方式中，本申请可以在得到待检测主机在一段时间内的流入数据量及流出数据量后，可以得到流入数据量在这段时间内的曲线图及流出数据量在这段时间内的曲线图，进一步，还可以得到在这段时间内流出数据量占全部数据量的比值的曲线图，如果流出数据量的曲线与待检测主机未存在异常流量外连行为时一段时间内流出数据量的曲线(可以称为基线流出数据量曲线)对比，超过基线流出数据量曲线一定倍数(如1)，则可以认为流出数据量大于第一数据量；和/或，流出数据量占全部数据量的比值的曲线与待检测主机未存在异常流量外连行为时一段时间内流出数据量占全部数据量的比值的曲线(可以称为基线比值曲线)对比，超过基线比值曲线一定倍数(如1)，则可以认为流出数据量与流入数据量的比值大于预设比值；从而通过曲线比对实现相应的判断。而在上述实现流量检测方法的过程中需要用到的字段可以包括：startTime、appProtocol、bytesIn、bytesOut、srcAddress、destAddress等。

[0052] 本发明实施例提供的一种检测异常流量外连的方法，检测方法包括位置检测方法，利用位置检测方法对待检测主机进行检测得到相应的检测结果，可以包括：

[0053] 获取待检测主机的流出数据量所流向的设备所在物理位置为目的位置，如果在距

离当前时刻最近的第二预设时间段内，待检测主机流向目的位置的流出数据量持续大于第二数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果。

[0054] 其中，第二预设时间段可以与第一预设时间段相同，也可以不同，第二数据流可以与第一数据量相同，也可以不同，具体根据实际需要进行的设定均在本发明的保护范围之内。待检测主机的流出数据量所流向的设备，也即主机发送数据包至的设备，从而获取待检测主机发送数据包至的设备所在的具体物理位置为目的位置；如果在第二预设时间段内待检测主机至目的位置的流出数据量大于第二数据量且持续，则可以说明该目的位置的设备在一段时间内持续由待检测主机获取大量的数据包，因此可以确定该目的位置的设备可能为对待检测主机进行异常流量外连的设备，也即待检测主机存在异常流量外连，从而通过这种位置检测方法简便有效的确定出待检测主机是否存在异常流量外连。

[0055] 在一种具体实现方式中，本申请可以基于数据包分析流出数据量对应的目的位置，而在上述实现位置检测方法的过程中需要用到的字段可以包括：destGeoAddress、destGeoRegion、destAddress等。

[0056] 本发明实施例提供的一种检测异常流量外连的方法，检测方法包括情报库检测方法，利用情报库检测方法对待检测主机进行检测得到相应的检测结果，可以包括：

[0057] 获取待检测主机的流出数据量所流向的设备的地址为目的地址，将目的地址与预先设置的情报库中各地址进行比对，如果情报库中存在与目的地址相同的地址，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果；其中，情报库中各地址为连接相应主机后使得所连接的主机发生异常流量外连的设备的地址。

[0058] 其中，地址具体可以为IP地址，而情报库则可以为预先创建的，情报库中包含的地址均是连接任意主机后会使得该任意主机发生异常流量外连的设备的地址，也即会攻击主机的设备的地址；基于此，本申请实施例获取待检测主机的流出数据量所流向的设备的地址为目的地址，具体可以是从待检测主机发送的数据包中获取其所携带的数据包需要发送至的地址，则为数据包需要发送至的设备的地址，也即为目的地址；在获取到目的地址后，将目的地址与情报库中各地址进行比对，如果情报库中具有与目的地址相同的地址，则说明目的地址的设备则为会攻击主机进而导致相应主机发生异常流量外连的恶意的设备，因此说明待检测主机与该恶意的设备相连接，因此很可能待检测主机存在异常流量外连。基于情报库检测方法，仅需创建情报库，即可基于情报库快速准确的确定出待检测主机是否与恶意的设备连接，也即确定出待检测主机是否存在异常流量外连。另外，在上述实现情报库检测方法的过程中需要用到的字段可以包括：destAddress等。

[0059] 本发明实施例提供的一种检测异常流量外连的方法，检测方法包括行为检测方法，利用行为检测方法对待检测主机进行检测得到相应的检测结果，可以包括：

[0060] 获取待检测主机当前的行为特征为目的行为特征，并将目的行为特征与特征库中各行为特征进行比对，如果行为库中存在与目的行为特征相同的行为特征，则得到表示待检测主机不存在异常流量外连的检测结果，否则，得到表示待检测主机存在异常流量外连的检测结果；其中，特征库中行为特征为待检测主机正常情况下的行为特征。

[0061] 需要说明的是，本申请在待检测主机不存在异常流量外连的正常情况下分析待检

测主机的行为特征，具体待检测主机的行为特征可以包括：访问IP、访问方法、目的地址、请求时间、应用响应时间、响应码、协议分布、流量占比等等，并将分析得到的待检测主机正常情况下的行为特征存储至特征库中；进而在基于行为检测方法对待检测主机进行检测时，则可以获取待检测主机当前的行为特征作为目的行为特征，将目的行为特征与特征库中各行为特征进行比对，如果特征库中存在与目的行为特征相同的行为特征，则说明待检测主机当前的行为特征为其正常情况下的行为特征，也即待检测主机不存在异常流量外连，否则，确定待检测主机存在异常流量外连，从而通过这种方式有效确定出待检测主机是否存在异常流量外连。

[0062] 在一种具体实现方式中，如果获取的待检测主机的目的行为特征包含多个，则与特征库中行为特征相同的目的行为特征所对应的与待检测主机通信的设备则为正常的设备，也即该设备并未对待检测主机进行攻击造成待检测主机存在异常流量外连，与特征库中行为特征不同的目的行为特征所对应的与待检测主机通信的设备则为恶意的设备，也即该设备对待检测主机进行了攻击造成待检测主机存在异常流量外连；因此本申请基于待检测主机正常情况下的情况特征，可以判断出哪些与待检测主机通信的设备为恶意的设备(对应的数据包为异常流量外连)，哪些与待检测主机通信的设备为正常的设备(对应的数据包不为异常流量外连)。并且，只要存在至少一项目的行为特征与特征库中行为特征均不同，则可确定待检测主机存在异常流量外连。

[0063] 本发明实施例提供的一种检测异常流量外连的方法，检测方法包括会话检测方法，利用会话检测方法对待检测主机进行检测得到相应的检测结果，可以包括：

[0064] 监测待检测主机对应的各项会话，如果待测主机对应的会话符合预先设定的异常条件，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果；其中，异常条件为待检测主机存在异常流量外连时其具有的会话所体现的特征。

[0065] 需要说明的是，本申请在待检测主机存在异常流量外连的异常情况下分析待检测主机的会话(cookie)的特征，得到表示待检测主机异常情况下的会话的特征的异常条件，由此，只有检测出待检测主机对应的至少一项会话符合异常条件，则可以确定待检测主机存在异常流量外连，否则，确定待检测主机不存在异常流量外连。具体来说，恶意的设备(或者称之为异常流量制造者)会利用多机器交叉刷码方式，机器数据量多、IP地址分散，本申请实施例可以基于大数据分析会话的产生时间及稳定性，对应的，异常条件则可以包括新生成的会话数量猛增(或者说距离当前时刻最近的过一段时间内会话增长数量达到预想设定的最大值)、会话有规律的连接断开(同一会话每经过一定的时间间隔则不断的循环的连接及断开)等；还可以基于大数据分析会话的时长，对应的，异常条件可以包括某个会话的访问行为在一定的时间段(根据实际需要进行设定，如1小时)内一直保持连接不断、访问行为过于有规律(如同一会话每经过一定的时间间隔则进行访问行为)等；当然根据实际需要设定的其他异常条件也均在本发明的保护范围之内。从而通过会话检测方法有效的实现待检测主机是否存在异常流量外连的检测。

[0066] 在一种具体应用场景中，本申请实施例提供的一种检测异常流量外连的方法可以表示为图2，具体可以包括以下步骤：

[0067] A)基于时间、流量占比维度模型分析(流量检测方法)：

[0068] a)基于大数据分析待检测主机流入数据量、流出数据量的曲线图,基于时间范围(第一预设时间段,如24小时等)分析待检测主机主机流量流入数据量占比及流出数据量占比,得到占比(占全部数据量的比值)的曲线图,如果待检测主机存在异常流量外连行为会产生大量流出的数据包,或者流出的数据包远多于流入的数据包,因此在流出数据量的曲线图与基线曲线(待检测主机正常情况下流出数据量的曲线)对比超过N+1倍,则认为待检测主机存在异常流量外连行为(N即曲线图对应时间节点值),N为待检测主机正常时的一个时间范围(时间节点)内的基线曲线。

[0069] b)分析24小时内待检测主机流入数据量占比、流出数据量占比的曲线图,依据待检测主机正常情况下24小时内流出数据量的曲线图为样板进行对比,如果大于样本的曲线值且增幅达N+1倍,则认为待检测主机存在异常流量外连行为(N即曲线图对应时间节点值)。

[0070] 分析字段:startTime、appProtocol、bytesIn、bytesOut、srcAddress、destAddress。

[0071] B)基于物理位置维度模型分析(位置检测方法):

[0072] a)基于大数据分析流出数据量所流入的设备的物理位置为目的位置,某时间段内待检测数据主机流出到目的位置的数据包的量大于N+1倍数量且持续(N即历史数据时间节点对应值),则认为待检测主机存在异常流量外连行为;其中,历史数据为历史上待检测主机流出数据量的数据,基于待检测主机正常时的一个时间范围(时间节点)内的历史数据可以分析出在这个时间范围内待检测主机流出数据量的波动区间(以及上下峰值波动情况),N表示分析所得在这个时间范围内正常的流出数据量(或者说数据包的大小,如在这个时间范围内流出数据量的均值等)。

[0073] 分析字段:destGeoAddress、destGeoRegion、destAddress

[0074] C)基于情报库碰撞模型分析(情报库检测方法):

[0075] a)基于情报库匹配:待检测主机的数据包中携带通信的设备的地址为目的地址,如果目的地址与情报库中任意地址匹配且该任意地址被标注恶意(情报库中的地址可以均为恶意的设备的地址,此时只要目的地址与情报库中任意地址匹配,则可确定待检测主机存在异常流量外连行为;情报库中也可以同时包括恶意的设备的地址及正常的设备的地址,此时则需要目的地址与被标注恶意的地址匹配,才能确定待检测主机存在异常流量外连行为),则判断待检测主机存在异常流量外连行为。

[0076] 分析字段:destAddress关联情报库分析。

[0077] D)基于主机行为基线模型分析(行为检测方法):

[0078] a)主机基准线分析,分析待检测主机正常情况下行为特征,包括:访问IP、访问方法、目的地址、请求时间、应用响应时间、响应码、协议分布、流量占比等等;基于正常情况下的行为特征,能判断哪些数据包为异常外连流量。

[0079] 分析字段:srcAddress、destAddress、requestTime、responseTime、appProtocol、requestTime、startTime、responseCode、protocolType。

[0080] E)基于cookie及会话时长维度模型分析(会话检测方法):

[0081] a)异常流量制造者会利用多机器交叉刷码方式,机器数据量多、IP地址分散,可以基于大数据分析cookie产生时间、稳定性,如新生成的cookie数量猛增、cookie有规律连接

断开等判断待检测主机存在异常流量外连；

[0082] b、基于大数据分析会话时长；某个cookie访问行为在1小时时间跨度内一直保持连接不断，访问行为过于有规律判断待检测主机存在异常流量外连。

[0083] F)关联分析：

[0084] a)基于上述五种模型所得检测结果再进行关联分析，提高检测准确率及精准度。

[0085] b)上述五种模型输出的检测结果都会包含srcAddress字段，五种模型输出检测结果srcAddress字段值为同一个IP地址，则待检测主机100％存在异常流量外连行为，五种模型输出的检测结果srcAddress字段值有四种相等，则待检测主机80％存在异常流量外连行为，五种模型输出的检测结果srcAddress字段值有三种相等，则待检测主机60％存在异常流量外连行为，五种模型输出的检测结果srcAddress字段值有两种相等，则待检测主机40％存在异常流量外连行为，以此类推。

[0086] c)上述五种模型输出的检测结果都会包含destAddress字段。五种模型输出检测结果destAddress字段值为同一个IP地址，则待检测主机100％存在异常流量外连行为，五种模型输出的检测结果destAddress字段值有四种相等，则待检测主机80％存在异常流量外连行为，五种模型输出的检测结果destAddress字段值有三种相等，则待检测主机60％存在异常流量外连行为，五种模型输出的检测结果destAddress字段值有两种相等，则待检测主机40％存在异常流量外连行为，以此类推。

[0087] 可见，本申请利用探针采集流量数据、主机流量日志数据、情报数据等，通过时间维度、流量维度、主机基线维度、情报库碰撞、cookie维度、地理位置维度、会话时长维度建立模型分析，基于大数据分析时间维度、流量占比维度、主机行为基线维度、情报库碰撞、地址位置维度、cookie维度、会话时长维度等多维度关联分析找出网络中异常流量外连行为；从而提高了异常外连流量检测效率和检测准确度，及时发现异常流量外连行为，协助安全人员快速定位被攻击主机资产，如资产已失陷可为企业及时止损。

[0088] 本发明实施例还提供了一种检测异常流量外连的装置，如图3所示，可以包括：

[0089] 确定模块11，用于：确定需要实现异常流量外连检测的主机为待检测主机；

[0090] 检测模块12，用于：利用多种预先设定的检测方法对待检测主机进行检测，得到相应的多个检测结果；

[0091] 判定模块13，用于：如果表示待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定待检测主机存在异常流量外连，否则，确定待检测主机不存在异常流量外连。

[0092] 本发明实施例提供的一种检测异常流量外连的装置，还可以包括：

[0093] 分析模块，用于：确定待检测主机存在异常流量外连之后，获取每个检测结果中包含的源地址，并确定值相同的源地址占全部源地址的百分比为待检测主机存在异常流量外连的可能性百分比；或者获取每个检测结果中包含的目的地址，并确定值相同的目的地址占全部目的地址的百分比为待检测主机存在异常流量外连的可能性百分比。

[0094] 本发明实施例提供的一种检测异常流量外连的装置，检测方法包括流量检测方法，检测模块可以包括：

[0095] 第一检测单元，用于：获取距离当前时刻最近的第一预设时间段内待检测主机的流入数据量及流出数据量，将流入数据量及流出数据量相加得到数据量和值，如果流出数

据量占数据量和值的比值大于预设比值，和/或流出数据量大于第一数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果。

[0096] 本发明实施例提供的一种检测异常流量外连的装置，检测方法包括位置检测方法，检测模块可以包括：

[0097] 第二检测单元，用于：获取待检测主机的流出数据量所流向的设备所在物理位置为目的位置，如果在距离当前时刻最近的第二预设时间段内，待检测主机流向目的位置的流出数据量持续大于第二数据量，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果。

[0098] 本发明实施例提供的一种检测异常流量外连的装置，检测方法包括情报库检测方法，检测模块可以包括：

[0099] 第三检测单元，用于：获取待检测主机的流出数据量所流向的设备的地址为目的地址，将目的地址与预先设置的情报库中各地址进行比对，如果情报库中存在与目的地址相同的地址，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果；其中，情报库中各地址为连接相应主机后使得所连接的主机发生异常流量外连的设备的地址。

[0100] 本发明实施例提供的一种检测异常流量外连的装置，检测方法包括行为检测方法，检测模块可以包括：

[0101] 第四检测单元，用于：获取待检测主机当前的行为特征为目的行为特征，并将目的行为特征与特征库中各行为特征进行比对，如果行为库中存在与目的行为特征相同的行为特征，则得到表示待检测主机不存在异常流量外连的检测结果，否则，得到表示待检测主机存在异常流量外连的检测结果；其中，特征库中行为特征为待检测主机正常情况下的行为特征。

[0102] 本发明实施例提供的一种检测异常流量外连的装置，检测方法包括会话检测方法，检测模块可以包括：

[0103] 第五检测单元，用于：监测待检测主机对应的各项会话，如果待测主机对应的会话符合预先设定的异常条件，则得到表示待检测主机存在异常流量外连的检测结果，否则，得到表示待检测主机不存在异常流量外连的检测结果；其中，异常条件为待检测主机存在异常流量外连时其具有的会话所体现的特征。

[0104] 本发明实施例还提供了一种检测异常流量外连的设备，可以包括：

[0105] 存储器，用于存储计算机程序；

[0106] 处理器，用于执行计算机程序时实现如上任一项检测异常流量外连的方法的步骤。

[0107] 本发明实施例还提供了一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，计算机程序被处理器执行时可以实现如上任一项检测异常流量外连的方法的步骤。

[0108] 需要说明的是，本发明实施例提供的一种检测异常流量外连的装置、设备及存储介质中相关部分的说明请参见本发明实施例提供的一种检测异常流量外连的方法中对应部分的详细说明，在此不再赘述。另外，本发明实施例提供的上述技术方案中与现有技术中

对应技术方案实现原理一致的部分并未详细说明，以免过多赘述。

[0109] 对所公开的实施例的上述说明，使本领域技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

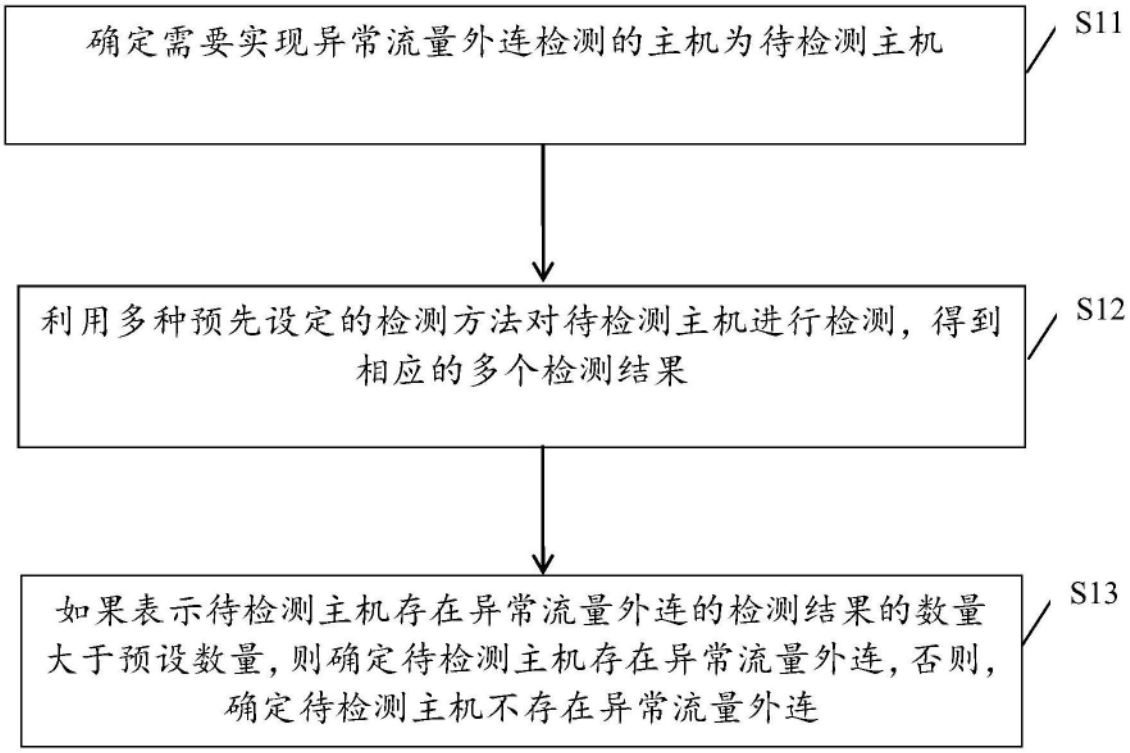

确定需要实现异常流量外连检测的主机为待检测主机
S11
利用多种预先设定的检测方法对待检测主机进行检测，得到相应的多个检测结果
S12
如果表示待检测主机存在异常流量外连的检测结果的数量大于预设数量，则确定待检测主机存在异常流量外连，否则，确定待检测主机不存在异常流量外连
S13

图1


基于时间、流量占比维度模型分析
基于物理位置维度模型分析
基于情报库碰撞模型分析
基于主机行为基线模型分析
基于cookie及会话时长维度模型分析
大数据分析
关联分析
异常流量外连结果

图2

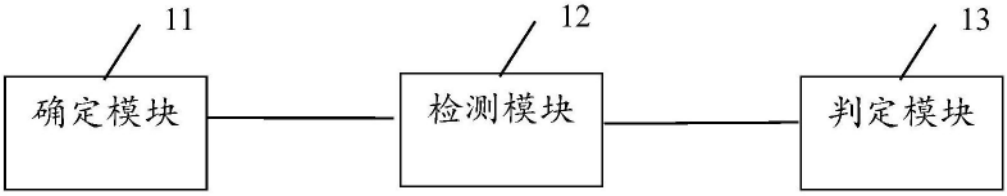

11
确定模块
12
检测模块
13
判定模块

图3