(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114826634 B
(45)授权公告日 2024.08.27

(21)申请号 202110117289.5
(22)申请日 2021.01.28
(65)同一申请的已公布的文献号
申请公布号 CN 114826634 A
(43)申请公布日 2022.07.29
(73)专利权人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋
(72)发明人 农乐安
(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 刘星雨 张颖玲
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 69/22(2022.01)

(56)对比文件
CN 102510385 A,2012.06.20
CN 107465625 A,2017.12.12

审查员 李斌

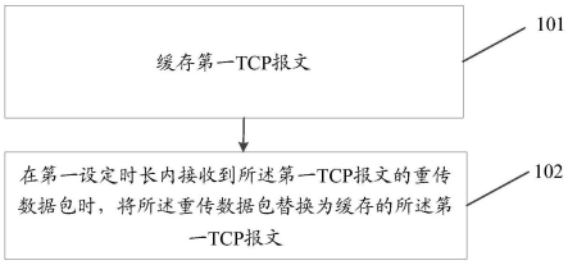
权利要求书3页 说明书13页 附图7页

(54)发明名称

一种报文检测方法、电子设备及存储介质

(57)摘要

本申请公开了一种报文检测方法、电子设备及存储介质。其中,方法包括:缓存第一TCP报文;所述第一TCP报文为接收到的表征不包含攻击的TCP报文;在第一设定时长内接收到所述第一TCP报文的重传数据包时,将所述重传数据包替换为缓存的所述第一TCP报文。



CN 114826634 B

1.一种报文检测方法,应用于防火墙,其特征在于,所述方法包括:

缓存第一传输控制协议TCP报文;所述第一TCP报文为接收到的表征不包含攻击的TCP报文;

在第一设定时长内接收到所述第一TCP报文的重传数据包时,将所述重传数据包替换为缓存的所述第一TCP报文;

将替换后的重传数据包发送至服务器。

2.根据权利要求1所述的报文检测方法,其特征在于,所述方法还包括:

在接收到第二TCP报文的情况下,释放缓存的所述第一TCP报文;所述第二TCP报文表征在向服务器发送所述第一TCP报文后,所述服务器返回的关于所述第一TCP报文的确认报文;

和/或,

在接收到所述第二TCP报文之后再接收到第三TCP报文的情况下,丢弃所述第三TCP报文;所述第三TCP报文的序列号小于所述第二TCP报文的序列号。

3.根据权利要求1所述的报文检测方法,其特征在于,在所述缓存第一TCP报文之前,所述方法还包括:

对接收的IP分片的头部字段进行检测,并在检测结果符合以下至少一项的情况下,确定接收的IP分片为混淆报文:

IP分片的生存时间TTL小于设定阈值;

IP分片的路由路径不是设定路由路径;

IP分片的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

IP分片的校验和存在错误;

IP分片的时间戳选项存在错误;

将确定出的不为混淆报文的IP分片进行报文重组,得到TCP报文,所述TCP报文用于后续进行攻击检测。

4.根据权利要求1-3中任一项所述的报文检测方法,其特征在于,在所述缓存第一TCP报文之前,所述方法还包括:

在至少两个IP分片的偏移存在重叠的情况下,将第一IP分片偏移的重叠部分覆盖至第二IP分片偏移的重叠部分;其中,

所述第一IP分片的接收时刻在所述第二IP分片的接收时刻之前。

5.根据权利要求1-3中任一项所述的报文检测方法,其特征在于,所述方法还包括:

对接收到的TCP报文进行TCP头部字段检测,并在检测结果符合以下至少一项的情况下,确定所述TCP报文为混淆报文:

所述TCP报文的校验和存在错误;

所述TCP报文的所有标志位都为空值;

所述TCP报文的所有标志位都不为空值;

所述TCP报文的紧急标志位不为空值,且存在有效载荷;

所述TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

所述TCP报文的设定选项字段存在错误;

将确定出不为混淆报文的TCP报文进行报文重组,得到应用层报文,所述应用层报文用于后续进行攻击检测。

6.根据权利要求1-3中任一项所述的报文检测方法,其特征在于,在所述缓存第一TCP报文之前,所述方法还包括:

在接收到的至少两个TCP报文的内容存在重叠时,将第一时刻接收到的TCP报文的内容的重叠部分覆盖至第二时刻接收到的TCP报文的内容的重叠部分;其中,

所述第一时刻在所述第二时刻之前。

7.一种报文检测方法,应用于防火墙,其特征在于,所述方法包括:

预判若将接收到的分段报文发送至服务器,所述服务器是否会执行丢弃操作;其中,若预判出所述服务器不会执行丢弃操作,确定对应的分段报文不为混淆报文;

将确定出的不为混淆报文的分段报文进行报文重组,基于重组后的报文进行攻击特征检测;

所述分段报文包括TCP报文;所述方法还包括:

将确定出的不为攻击报文的TCP报文进行缓存;

在接收到所述TCP报文的重传数据包时,将所述重传数据包替换为对应的已缓存的TCP报文;

将替换后的重传数据包发送至服务器。

8.根据权利要求7所述的报文检测方法,其特征在于,所述预判若将接收到的分段报文发送至服务器,所述服务器是否会执行丢弃操作,包括:

检测所述分段报文的头部字段是否满足设定条件;

若检测到所述分段报文的头部字段满足设定条件,确定所述服务器会执行丢弃操作。

9.根据权利要求8所述报文检测方法,其特征在于,所述分段报文包括IP分片报文;所述设定条件包括以下至少之一:

IP分片报文的生存时间TTL小于设定阈值;

IP分片报文的路由路径不是设定路由路径;

IP分片报文的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

IP分片报文的校验和存在错误;

IP分片报文的时间戳选项存在错误。

10.根据权利要求8或9所述的报文检测方法,其特征在于,所述分段报文包括TCP报文;所述设定条件包括以下至少之一:

TCP报文的校验和存在错误;

TCP报文的所有标志位都为空值;

TCP报文的所有标志位都不为空值;

TCP报文的紧急标志位不为空值,且存在有效载荷;

TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

TCP报文的设定选项字段存在错误。

11.如权利要求10所述的报文检测方法,其特征在于,所述设定选项字段为无法纠正错误的选项字段;

所述方法还包括：

若所述TCP报文中包括可修正错误的选项字段时，将可修正错误的选项字段修正为正确字段。

12.根据权利要求7中所述的报文检测方法，其特征在于，所述方法还包括：

在进行分段重组时，在接收到的至少两个分段报文的内容存在重叠时，将第一时刻接收到的分段报文的内容的重叠部分覆盖至第二时刻接收到的分段报文的内容的重叠部分；其中，所述第一时刻在所述第二时刻之前；

在基于重组后的报文未检测到攻击特征时，将覆盖后的各个分段报文发送至服务器。

13.根据权利要求7-9中任一项所述的报文检测方法，其特征在于，所述重组后的报文为应用层报文；所述方法还包括：

在基于应用层报文未检测到攻击特征时，基于应用层协议解析确定所述应用层报文的异常等级；

基于所述应用层报文的异常等级以及TCP层和IP层的对应报文是否具备混淆，确定是否执行拦截。

14.一种电子设备，其特征在于，包括：处理器和用于存储能够在处理器上运行的计算机程序的存储器，

其中，所述处理器用于运行所述计算机程序时，执行权利要求1-13任一项所述方法的步骤。

15.一种存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1-13任一项所述方法的步骤。

一种报文检测方法、电子设备及存储介质

技术领域

[0001] 本申请涉及防火墙检测技术领域,尤其涉及一种报文检测方法、电子设备及存储介质。

背景技术

[0002] 防火墙能够将内部网络和公共网络分隔开,能识别并丢弃公共网络中存在的可能会对内部网络产生攻击的报文,从而保证内部网络的安全。防火墙可以通过重传包检测的方式识别攻击报文,相关技术中,重传包检测存在识别攻击准确率低的问题。

发明内容

[0003] 有鉴于此,本申请实施例的主要目的在于提供一种报文检测方法、电子设备及存储介质,以解决重传包检测存在识别攻击准确率低的技术问题。

[0004] 为达到上述目的,本申请实施例的技术方案是这样实现的:

[0005] 本申请实施例提供了一种报文检测方法,所述方法包括:

[0006] 缓存第一传输控制协议(TCP,Transmission Control Protocol)报文;所述第一TCP报文为接收到的表征不包含攻击的TCP报文;

[0007] 在第一设定时长内接收到所述第一TCP报文的重传数据包时,将所述重传数据包替换为缓存的所述第一TCP报文。

[0008] 本申请实施例还提供了另一种报文检测方法,所述方法包括:

[0009] 预判若将接收到的分段报文发送至服务器,所述服务器是否会执行丢弃操作;其中,若预判出所述服务器不会执行丢弃操作,确定对应的分段报文不为混淆报文;

[0010] 将确定出的不为混淆报文的分段报文进行报文重组,基于重组后的报文进行攻击特征检测。

[0011] 通过预先判断服务器是否会对接收的分段报文执行丢弃操作,并将确定出不为混淆报文的分段报文进行重组,对重组后的报文进行攻击特征检测,可以先筛除掉字段异常的报文,对字段正常的报文重组出的报文再进行检测,可以进一步确定报文是否存在攻击,从而提高了报文攻击检测的准确性。

[0012] 本申请实施例还提供了一种电子设备,其特征在于,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,

[0013] 其中,所述处理器用于运行所述计算机程序时,执行上述任一方法的步骤。

[0014] 本申请实施例还提供了一种存储介质,其上存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现上述任一方法的步骤。

[0015] 在本申请实施例中,通过缓存第一TCP报文;第一TCP报文为接收到的表征不包含攻击的TCP报文;在第一设定时长内接收到第一TCP报文的重传数据包时,将重传数据包替换为缓存的第一TCP报文,保证了转发给服务器的数据包不是携带攻击的重传数据包,从而使服务器避免受到重传数据包的攻击,提高了重传包检测识别攻击的准确率。

附图说明

[0016] 图1为本申请实施例提供的报文检测方法的实现流程示意图；

[0017] 图2a示出了实际应用中常用的检测部署场景；

[0018] 图2b示出了实际应用中另一常用的检测部署场景；

[0019] 图3为本申请实施例提供的另一报文检测方法的实现流程示意图；

[0020] 图4为本申请实施例提供的IP报文的头部结构的示意图；

[0021] 图5为本申请实施例提供的TCP报文的头部结构的示意图；

[0022] 图6为本申请实施例提供的另一报文检测方法的实现流程示意图；

[0023] 图7为本申请实施例提供的另一报文检测方法的实现流程示意图；

[0024] 图8为本申请实施例提供的电子设备的结构的示意图。

具体实施方式

[0025] 下面结合附图及实施例对本申请再作进一步详细的描述。

[0026] 超时重传是TCP协议保证数据可靠性的一个重要机制,在发送一个数据后开启一个计时器,在一定的时间内如果没有收到关于该数据的确认报文,就会重新发送该数据,直至收到关于该数据的确认报文。

[0027] TCP重传包是指重复发送的序列号相同、长度相同的TCP报文,TCP协议的可靠性正是由超时重传机制来保证,但攻击者会利用超时重传的机制,重复发送序列号一致但内容不一致的报文,造成混淆。相关技术中,防火墙不检测报文内容是否一致就直接将报文转发给服务器,当序列号一致但内容不一致的重传报文为攻击报文时,服务器在接收到这类报文后可能会遭受攻击。也就是说,相关技术中,重传包检测并不能有效识别出攻击报文并进行拦截。

[0028] 基于此,本申请实施例提供了一种报文检测方法、电子设备及存储介质,通过缓存第一TCP报文,在第一设定时间内接收到第一TCP报文的重传数据包时,将重传数据包替换为缓存的第一TCP报文,保证了转发给服务器的数据包不是携带攻击的重传数据包,从而使服务器避免受到重传数据包的攻击,提高了重传包检测识别攻击的准确率。

[0029] 图1为本申请实施例的报文检测方法的实现流程示意图。如图1所示,所述方法包括:

[0030] 步骤101:缓存第一TCP报文;所述第一TCP报文为接收到的表征不包含攻击的TCP报文。

[0031] 这里,经过检测,发现接收的TCP报文不包含攻击时,将该TCP报文作为第一TCP报文缓存起来,以便后续重传使用。

[0032] 步骤102:在第一设定时长内接收到所述第一TCP报文的重传数据包时,将所述重传数据包替换为缓存的所述第一TCP报文。

[0033] 这里,在接收到所述第一TCP报文的重传数据包时,并不是直接将重传数据包转发至服务器,而是丢弃收到的重传数据包,并用缓存的所述第一TCP报文来代替重传数据包发送给服务器。这样,即使重传数据包中存在攻击,也不会对服务器造成影响,从而避免了服务器受到重传数据包的攻击。

[0034] 为了实现本申请实施例的方法,图2a和图2b示出了实际应用中常用的检测部署场

景。图2a示出了在因特网网络入口处搭建防火墙,外部流量经过防火墙时,防火墙进行检测,检测到攻击流量时拦截下来,防止黑客入侵。图2b示出了以旁路部署防火墙,防火墙与交换机相连的接口中设置为镜像模式,流经交换机的所有流量都复制一份放到防火墙中进行检测,或者在交换机中配置策略路由,引流到防火墙中进行检测,发送给防火墙的流量经防火墙进行检测后,如果有异常,则在防火墙中进行异常标记。

[0035] 在本申请实施例中,通过缓存第一TCP报文;第一TCP报文为接收到的表征不包含攻击的TCP报文;在第一设定时长内接收到第一TCP报文的重传数据包时,将重传数据包替换为缓存的第一TCP报文,从而保证了转发给服务器的数据包不是携带攻击的重传数据包,使服务器避免受到重传数据包的攻击,提高了重传包检测识别攻击的准确率。

[0036] 此外,在本申请实施例中,可以假设首次接收的TCP报文为不包含攻击的TCP报文,将首次接收到的进行缓存,替换后续的TCP报文。该方案也在本申请的保护范围内,这种方式避免了执行攻击特征检测,可以提高防火墙等设备的运行效率,节约内存资源。

[0037] 在一实施例中,所述方法还包括:

[0038] 在接收到第二TCP报文的情况下,释放缓存的所述第一TCP报文;所述第二TCP报文表征在向服务器发送所述第一TCP报文后,所述服务器返回的关于所述第一TCP报文的确认报文;

[0039] 和/或,

[0040] 在接收到所述第二TCP报文之后再接收到第三TCP报文的情况下,丢弃所述第三TCP报文;所述第三TCP报文的序列号小于所述第二TCP报文的序列号。

[0041] 将所述第一TCP报文的重传数据包,替换为缓存的所述第一TCP报文后,将替换后的第一TCP报文发送至服务器。服务器在接收到所述第一TCP报文后,返回一个关于所述第一TCP报文的确认报文,确认报文表示发送来的第一TCP报文已经确认接收无误。因此,接收到服务器基于所述第一TCP报文发送的确认报文时,表示第一TCP报文已经成功被接收,此次重传过程已经成功,所以释放缓存的第一TCP报文,避免造成缓冲区溢出,从而保证能继续接收后续发送过来的第一TCP报文。

[0042] 此外,在收到服务器的确认报文之前,重传过程一直在继续,所述第一TCP报文会持续发送给服务器,按照时间顺序,最先发送给服务器的第一TCP报文会最早收到服务器的确认报文,最晚发送给服务器的第一TCP报文会最晚收到确认报文,而在首次接收到服务器返回的关于第一TCP报文的确认报文之后,代表已经成功重传,此次重传过程结束。在重传过程已经结束后,再接收到序列号比服务器发送的确认报文的序列号小的报文时,直接丢弃该报文,避免了重复确认。

[0043] 图3示出了另一报文检测方法的实现流程示意图,请参见图3,所述方法包括:

[0044] 在一实施例中,在所述缓存第一TCP报文之前,所述方法还包括:

[0045] 对接收的IP分片的头部字段进行检测,并在检测结果符合以下至少一项的情况下,确定接收的IP分片为混淆报文:

[0046] IP分片的生存时间TTL小于设定阈值;

[0047] IP分片的路由路径不是设定路由路径;

[0048] IP分片的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

[0049] IP分片的校验和存在错误;

[0050] IP分片的时间戳选项存在错误;

[0051] 将确定出的不为混淆报文的IP分片进行报文重组,得到TCP报文,所述TCP报文用于后续进行攻击检测。

[0052] 图4示出了IP报文的头部结构的示意图,请参见图4,Version表示IP协议的版本号,IHL表示头部长度,Type of Service表示服务类型,Total Length表示总长度,Identification表示标识,Flags表示标志,Fragment Offset表示片偏移,Time to Live表示生存时间,Protocol表示协议,Header Checksum表示头部校验和,Source Address表示源端IP地址,Destination Address表示目的端IP地址,Options表示选项,Padding表示填充。

[0053] 这里,TTL是IP分片在计算机网络中可以转发的最大跳数,IP分片每经转发一次,TTL值会减一。在防火墙接收到一份TTL特别小的混淆报文,再接收到一份字段相同但TTL正常的攻击报文时,如果防火墙不对报文的TTL是否存在异常进行检测,直接把TTL很小的报文和TTL正常的报文放入IP分片重组,有可能会检测不出攻击。

[0054] 通常,在一条会话中,报文经过的网络设备基本是稳定的,TTL不会出现较大的波动,如果突然出现非常小的TTL值,如TTL值突变为1甚至变为0,那么这条报文很可能是混淆报文,存在绕过防火墙检测的行为,因此,将TTL值小于设定阈值的报文确定为混淆报文,确定为混淆报文之后,可以直接进行丢弃。

[0055] 在混淆报文中使用非法的严格路由,如路由的下一跳地址为测试专用的本地机地址127.0.0.1或表示所有主机IP地址的0.0.0.0,或在防火墙接收到报文时,报文的路由地址并不在防火墙设定的路由地址中,这些也会使报文存在绕过防火墙检测的行为。因此,按照RFC971中严格路由的定义,如果路由路径定义为A->B->C->D,那么,每一跳都必须是严格对应的地址,如,A的下一跳路由地址必须是B,B的下一跳路由地址必须是C。所以,在防火墙检测到IP分片中的路由选项的路由路径不是设定路由路径,具体包括下一跳路由地址不是设定路由路径中的路由地址;或检测到报文的最后一跳的路由地址为防火墙的地址时,确定这些路由地址异常的报文为混淆报文,直接进行丢弃。

[0056] 校验和的目的是检验报文传输途中报文是否被篡改,如果检测到IP分片的校验和存在错误,代表所述IP分片很可能被篡改过,所以将校验和存在错误的IP分片确定为混淆报文,直接进行丢弃。

[0057] 如果检测到IP分片的时间戳选项存在错误,将所述IP分片确定为混淆报文,并丢弃所述IP分片。通过对IP分片头部字段的TTL、路由地址、校验和以及时间戳选项的检测,在IP分片的头部字段检测过程中检测出异常时直接对报文进行丢弃,可以防止异常报文进入后续检测过程造成攻击,也提高了IP分片头部字段检测的准确率。

[0058] 在一实施例中,在步骤101之前,所述方法还包括:

[0059] 在至少两个IP分片的偏移存在重叠的情况下,将第一IP分片偏移的重叠部分覆盖至第二IP分片偏移的重叠部分;其中,

[0060] 所述第一IP分片的接收时刻在所述第二IP分片的接收时刻之前。

[0061] 一个IP数据包从源主机传输到目的主机可能需要经过多个不同的物理网络,由于各个网络的数据帧都有一个最大传输单元(MTU,Maximum Transmission Unit),因此,当数

据包的大小超过了出口链路的最大传输单元时,会将该IP数据包分解成很多足够小的片段,以便能够在目标链路上进行传输。这些IP分片重新封装一个IP数据包独立传输,在达到目标主机时会被重组起来。

[0062] IP分片重组是指在接收到报文时,如果IP头部的标志Flags中指示了分片,按照分片偏移Fragment Offset拼接组装成完整的报文。

[0063] 在各个IP分片的偏移存在重叠或包含的情况下,如IP分片①的后半段和IP分片②的前半段的内容存在重叠,对内容重叠部分的处理,不同的服务器操作系统的处理方法不一致,有些操作系统是将IP分片②的重叠部分覆盖至IP分片①的重叠部分,有些操作系统是将IP分片①的重叠部分覆盖至IP分片②的重叠部分,攻击者利用这种处理的差异性,使防火墙接收到混淆报文,从而绕过防火墙的检测。在本申请实施例中,默认以先接收到的第一IP分片的内容为准,在接收到内容重叠的IP分片时,将先接收的第一IP分片偏移的重叠部分覆盖至后接收的第二IP分片偏移的重叠部分,如IP分片①的后半段和IP分片②的前半段内容存在重叠,将IP分片①的重叠部分覆盖至IP分片②的重叠部分,IP分片①的接收时刻在IP分片②的接收时刻之前,通过对IP分片偏移的重叠部分进行统一的处理,从而保证了服务器接收的报文和防火墙中进行检测的报文是一致的,避免了攻击者利用IP分片重组过程做出攻击行为。

[0064] 在一实施例中,所述方法还包括:

[0065] 对接收到的TCP报文进行TCP头部字段检测,并在检测结果符合以下至少一项的情况下,确定所述TCP报文为混淆报文:

[0066] 所述TCP报文的校验和存在错误;

[0067] 所述TCP报文的所有标志位都为空值;

[0068] 所述TCP报文的所有标志位都不为空值;

[0069] 所述TCP报文的紧急标志位不为空值,且存在有效载荷;

[0070] 所述TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

[0071] 所述TCP报文的设定选项字段存在错误;

[0072] 将确定出不为混淆报文的TCP报文进行报文重组,得到应用层报文,所述应用层报文用于后续进行攻击检测。

[0073] 图5示出了TCP报文的头部结构的示意图,请参照图5,Source Port是源端口,Destination Port是目的端口,Sequence Number是发送数据包中的第一个字节的序列号,Acknowledgment Number是确认序列号,Data Offset是数据偏移。URG是紧急标志位,ACK是确认标志位,PSH是推位,RST是复位标志,SYN是同步序列编号,FIN是结束标志。Window表示接收缓冲区的空闲空间,Checksum是校验和,Urgent Pointers是紧急指针,只有URG标志位被设置时该字段才有意义,表示紧急数据相对序列号(Sequence Number)字段的值的偏移。

[0074] 校验和的目的是检验报文传输途中报文是否被篡改,如果检测到TCP报文的校验和存在错误,代表所述TCP报文很可能被篡改过,所以将校验和存在错误的TCP报文确定为混淆报文,直接进行丢弃。

[0075] 这里,检测到TCP报文的所有标志位为空值时,丢弃所述TCP报文。所有标志位为空值,是指没有SYN/ACK/PSH/FIN/RST/URG任何标志,根据RFC793规范,除了最初发送的SYN报文,其他报文都必须有ACK标志位,在报文的所有标志位为空值的情况下,报文很可能是混

淆报文,因此,将所有标志位为空值的TCP报文确定为混淆报文,直接进行丢弃。

[0076] 在检测到TCP报文的所有标志位都不为空值时,如果SYN/ACK/PSH/FIN/RST/URG每一个标志位都有值,那么服务器无法得知报文想表达的含义,因此,同样将所有标志位不为空值的TCP报文确定为混淆报文,直接进行丢弃。

[0077] 检测到TCP报文的紧急标志位不为空值时,对于紧急报文,操作系统通常只取其中的一个字节进行处理,对其他字节不做处理,所以需要检测其他字节是否存在有效载荷,在检测结果显示其他报文存在有效载荷时,将这一紧急标志位不为空值且存在有效载荷的TCP报文确定为混淆报文,直接进行丢弃。

[0078] 在检测到TCP报文在已建立连接的会话上重复发送SYN标志时,发送SYN标志表示要建立新的TCP连接会话,而在已建立连接的会话上重复发送SYN标志的TCP报文,会给防火墙造成混淆,重新初始化连接,因此确定所述TCP报文为混淆报文,丢弃所述TCP报文。

[0079] TCP报文的选项包括最大报文长度(MSS,Max Segment Size)选项、窗口扩大因子选项,选择性确认(SACK,Selective Acknowledgement)选项、时间戳选项、自定义选项,不同网络协议对TCP选项异常的处理方法不一样,有的是忽略选项,有的是丢弃报文,为了使所有服务器接收到的都是同样的报文,防火墙在检测到TCP报文中存在可纠正的选项错误,如窗口扩大因子选项和MSS选项时,直接将这些可纠正的选项错误纠正为正确的选项值。

[0080] 检测到TCP报文头部字段的选项字段存在无法纠正的错误时,对于无法纠正的选项错误,如时间戳、SACK、自定义选项,确定所述报文为混淆报文,直接丢弃存在无法纠正的选项错误的TCP报文。

[0081] 通过对TCP报文进行TCP头部字段检测,有效识别出TCP头部字段中可能存在的会造成混淆攻击的报文并丢弃,避免了TCP头部字段检测中存在的攻击行为,提高了识别攻击的准确率。

[0082] 在一实施例中,在步骤101之前,所述方法还包括:

[0083] 在接收到的至少两个TCP报文的内容存在重叠时,将第一时刻接收到的TCP报文的内容的重叠部分覆盖至第二时刻接收到的TCP报文的内容的重叠部分;其中,

[0084] 所述第一时刻在所述第二时刻之前。

[0085] 在所述至少两个TCP的报文的内容存在重叠的情况下,默认以先接收到的TCP报文的内容为准,在接收到内容重叠的另一TCP报文时,将第一时刻接收的TCP报文的内容的重叠部分覆盖至第二时刻接收的TCP报文的内容的重叠部分,其中,第一时刻在第二时刻之前。如报文①的后半段和报文②的前半段内容存在重叠,将报文①的重叠部分覆盖至报文②的重叠部分,报文①的接收时刻在报文②的接收时刻之前,从而保证了服务器接收的报文和防火墙中进行检测的报文是一致的,避免了TCP流重组过程中存在的攻击行为。

[0086] 在一实施例中,在步骤102之后,所述方法还包括:

[0087] 检测传输到应用层的报文,使用漏洞、攻击指纹等特征库或语法语义引擎,与报文的内容进行匹配检测,如果报文和漏洞或攻击指纹能匹配,则认为报文存在攻击,拦截该报文。通过对应用层的报文进行检测,避免了应用层存在的攻击行为。

[0088] 图6示出了本申请实施例另一报文检测方法的流程图,请参照图6,在一实施例中,所述方法还包括:

[0089] 步骤601:预判若将接收到的分段报文发送至服务器,所述服务器是否会执行丢弃

操作;其中,若预判出所述服务器不会执行丢弃操作,确定对应的分段报文不为混淆报文。

[0090] 这里,预先判断一下,如果将接收的分段报文发送至服务器,服务器是否会执行丢弃操作。通常,服务器在接收到字段异常的分段报文时,会执行丢弃操作。

[0091] 若不会执行丢弃操作,表示所述分段报文不是字段异常的报文,确定所述分段报文不为混淆报文。

[0092] 如果判断得出服务器会执行丢弃操作,表示所述分段报文是字段异常的报文,将所述分段报文确定为混淆报文。

[0093] 步骤602:将确定出的不为混淆报文的分段报文进行报文重组,基于重组后的报文进行攻击特征检测。

[0094] 这里,确定所述报文不是混淆报文后,将所述确定出的报文进行报文重组,对重组后的报文进行攻击特征,也就是说,需要对重组后的报文进行进一步的检测,从而确定所述重组后的报文是否为攻击报文。

[0095] 通过预先判断服务器是否会对接收的分段报文执行丢弃操作,并将确定出不为混淆报文的分段报文进行重组,对重组后的报文进行攻击特征检测,可以先筛除掉字段异常的报文,对字段正常的报文重组出的报文再进行检测,可以进一步确定报文是否存在攻击,从而提高了报文攻击检测的准确性。

[0096] 这里的预判操作,并不代表着一定要通过和服务器通信来确定其是否会执行丢弃操作,可以通过RFC文档等来确定服务器是否大概率会执行丢弃操作,这里仅仅是一种预判,预判结果可能与服务器真实的操作不一致。

[0097] 在一实施例中,所述步骤601还包括:

[0098] 检测所述分段报文的头部字段是否满足设定条件;

[0099] 若检测到所述分段报文的头部字段满足设定条件,确定所述服务器会执行丢弃操作。

[0100] 这里,通过检测所述分段报文的头部字段是否满足设定条件,来判断服务器是否会执行丢弃操作。所述设定条件可以是所述分段报文头部字段存在异常。如果检测到所述分段报文的报文头部字段存在异常,则确定所述服务器会执行丢弃操作。

[0101] 通过检测分段报文是否满足设定条件来判断服务器是否会执行丢弃操作,提高了判断效率。

[0102] 在一实施例中,所述分段报文包括IP分片;所述设定条件包括以下至少之一:

[0103] IP分片的生存时间TTL小于设定阈值;

[0104] IP分片的路由路径不是设定路由路径;

[0105] IP分片的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

[0106] IP分片的校验和存在错误;

[0107] IP分片的时间戳选项存在错误。

[0108] 通过对分段报文头部字段的TTL、路由地址、校验和以及时间戳选项的检测,在IP分片的头部字段检测过程中检测出异常时直接对报文进行丢弃,可以防止异常报文进入后续检测过程造成攻击,也提高了IP分片头部字段检测的准确率。在一实施例中,所述分段报文包括TCP报文;所述设定条件包括以下至少之一:

[0109] TCP报文的校验和存在错误;

[0110] TCP报文的所有标志位都为空值;

[0111] TCP报文的所有标志位都不为空值;

[0112] TCP报文的紧急标志位不为空值,且存在有效载荷;

[0113] TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

[0114] TCP报文的设定选项字段存在错误。

[0115] 通过对TCP报文进行TCP头部字段检测,有效识别出TCP头部字段中可能存在的会造成混淆攻击的报文并丢弃,避免了TCP头部字段检测中存在的攻击行为,提高了识别攻击的准确率。

[0116] 在一实施例中,所述设定选项字段为无法纠正错误的选项字段;

[0117] 所述方法还包括:

[0118] 若所述TCP报文中包括可修正错误的选项字段时,将可修正错误的选项字段修正为正确字段。

[0119] 这里,由于不同网络协议对TCP选项字段异常的处理方法不一样,有的是忽略选项,有的是丢弃报文,为了使所有服务器接收到的都是同样的报文,防火墙在检测到TCP报文中存在可修正的选项错误,如窗口扩大因子选项和MSS选项时,直接将这些可修正的选项错误修正为正确的选项值。

[0120] 而在检测到TCP报文头部字段的选项字段存在无法纠正的错误时,对于无法纠正的选项错误,如时间戳、SACK、自定义选项,确定所述报文为混淆报文,直接丢弃存在无法纠正的选项错误的TCP报文。

[0121] 通过对TCP报文进行选项字段检测,有效识别出TCP选项字段中可能存在的会造成混淆攻击的报文并丢弃,避免了TCP选项字段检测中存在的攻击行为,提高了识别攻击的准确率。

[0122] 在一实施例中,所述方法还包括:

[0123] 在进行分段重组时,在接收到的所述至少两个分段报文的内容存在重叠时,将第一时刻接收到的分段报文的内容的重叠部分覆盖至第二时刻接收到的分段报文的内容的重叠部分;其中,所述第一时刻在所述第二时刻之前;

[0124] 在基于重组后的报文未检测到攻击特征时,将覆盖后的各个分段报文发送至服务器。

[0125] 这里,如果重组后的报文中没有检测到攻击特征,说明重组后的报文是正常的报文,因此将执行覆盖操作后的分段报文发送至服务器,从而保证了服务器接收的分段报文和防火墙中进行检测的分段报文是一致的,避免了重组过程中存在的攻击行为。

[0126] 在一实施例中,所述报文包括TCP报文;所述方法还包括:

[0127] 将确定出的不为攻击报文的TCP报文进行缓存;

[0128] 在接收到所述TCP报文的重传数据包时,将所述重传数据包替换为对应的已缓存的TCP报文;

[0129] 将替换后的重传数据包发送至服务器。

[0130] 这里,如果重组后的报文中没有检测到攻击特征,说明重组后的报文是正常报文,因此将执行替换操作后的重传数据包发送至服务器,从而保证了服务器接收的是不包含攻

击内容的重传数据包,避免了重传过程中存在的攻击行为。在一实施例中,所述方法还包括:

[0131] 在接收到第二TCP报文的情况下,释放缓存的所述第一TCP报文;所述第二TCP报文表征在向服务器发送所述第一TCP报文后,所述服务器返回的关于所述第一TCP报文的确认报文;

[0132] 和/或,

[0133] 在接收到所述二TCP报文之后再接收到第三TCP报文的情况下,丢弃所述第三TCP报文;所述第三TCP报文的序列号小于所述二TCP报文的序列号。

[0134] 通过释放缓存的第一TCP报文,可以避免造成缓冲区溢出,从而保证能继续接收后续发送过来的第一TCP报文。

[0135] 在重传过程已经结束后,再接收到序列号比服务器发送的确认报文的序列号小的报文时,直接丢弃该报文,避免了重复确认。

[0136] 图7为本申请实施例提供的另一报文检测方法的实现流程示意图,请参见图7,所述重组后的报文为应用层报文,所述方法还包括:

[0137] 在基于应用层报文未检测到攻击特征时,基于应用层协议解析确定所述应用层报文的异常等级;

[0138] 基于所述应用层报文的异常等级以及所述TCP层和IP层的对应报文是否具备混淆,确定是否执行拦截。

[0139] 具体地,在基于应用层协议解析的应用层报文的异常等级为第一设定等级的情况下,拦截所述应用层报文;

[0140] 在基于应用层协议解析的应用层报文的异常等级不为第一设定等级的情况下,基于TCP/IP层协议解析确定对应报文的异常等级;

[0141] 在基于TCP/IP层协议解析的对应报文的异常等级为第一设定等级的情况下,拦截所述对应报文;

[0142] 在基于TCP/IP层协议解析的对应报文的异常等级为第二设定等级,且对应的报文为攻击报文的情况下,拦截所述对应报文;

[0143] 在基于TCP/IP层协议解析的对应报文的异常等级为第三设定等级的情况下,放行所述对应报文;其中,

[0144] 所述第一设定等级高于所述第二设定等级,所述第二设定等级高于所述第三设定等级。

[0145] 这里,基于应用层协议解析确定所述应用层报文的异常等级,所述异常等级可以根据应用层报文异常的影响程度进行划分。

[0146] 通过对经过应用层和TCP/IP层协议解析的报文划分异常等级,可以更方便、直观地对存在异常的报文进行拦截,提高了识别异常报文的效率。

[0147] 为了实现本申请实施例的方法,本申请实施例还提供了一种电子设备。图8为本申请实施例电子设备的硬件组成结构示意图,如图8所示,电子设备包括:

[0148] 通信接口801,能够与其它设备比如网络设备等进行信息交互;

[0149] 处理器802,与所述通信接口801连接,以实现与其它设备进行信息交互,用于运行计算机程序时,执行上述电子设备侧一个或多个技术方案提供的方法。而所述计算机程序

存储在存储器803上。

[0150] 具体地,所述处理器802,用于缓存第一TCP报文;所述第一TCP报文为接收到的表征不包含攻击的TCP报文;在第一设定时长内接收到所述第一TCP报文的重传数据包时,将所述重传数据包替换为缓存的所述第一TCP报文。

[0151] 在一实施例中,所述处理器802,还用于在接收到第二TCP报文的情况下,释放缓存的所述第一TCP报文;所述第二TCP报文表征在向服务器发送所述第一TCP报文后,所述服务器返回的关于所述第一TCP报文的确认报文;

[0152] 和/或,

[0153] 在接收到所述二TCP报文之后再接收到第三TCP报文的情况下,丢弃所述第三TCP报文;所述第三TCP报文的序列号小于所述二TCP报文的序列号。

[0154] 在一实施例中,在所述接收到第一TCP报文之前,所述处理器802,还用于对接收的IP分片的头部字段进行检测,并在检测结果符合以下至少一项的情况下,确定接收的IP分片为混淆报文:

[0155] IP分片的生存时间TTL小于设定阈值;

[0156] IP分片的路由路径不是设定路由路径;

[0157] IP分片的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

[0158] IP分片的校验和存在错误;

[0159] IP分片的时间戳选项存在错误;

[0160] 将确定出的不为混淆报文的IP分片进行报文重组,得到TCP报文,所述TCP报文用于后续进行攻击检测。

[0161] 在一实施例中,所述处理器802,还用于在所述缓存第一TCP报文之前,在至少两个IP分片的偏移存在重叠的情况下,将第一IP分片偏移的重叠部分覆盖至第二IP分片偏移的重叠部分;其中,

[0162] 所述第一IP分片的接收时刻在所述第二IP分片的接收时刻之前。

[0163] 在一实施例中,所述处理器802,还用于对接收到的TCP报文进行TCP头部字段检测,并在检测结果符合以下至少一项的情况下,确定所述TCP报文为混淆报文:

[0164] 所述TCP报文的校验和存在错误;

[0165] 所述TCP报文的所有标志位都为空值;

[0166] 所述TCP报文的所有标志位都不为空值;

[0167] 所述TCP报文的紧急标志位不为空值,且存在有效载荷;

[0168] 所述TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

[0169] 所述TCP报文的设定选项字段存在错误;

[0170] 将确定出不为混淆报文的TCP报文进行报文重组,得到应用层报文,所述应用层报文用于后续进行攻击检测。

[0171] 在一实施例中,所述处理器802,还用于在所述缓存第一TCP报文之前,在接收到的至少两个TCP报文的内容存在重叠时,将第一时刻接收到的TCP报文的内容的重叠部分覆盖至第二时刻接收到的TCP报文的内容的重叠部分;

[0172] 其中,

[0173] 所述第一时刻在所述第二时刻之前。

[0174] 在一实施例中,所述处理器802,还用于预判若将接收到的分段报文发送至服务器,所述服务器是否会执行丢弃操作;其中,若预判出所述服务器不会执行丢弃操作,确定对应的分段报文不为混淆报文;

[0175] 将确定出的不为混淆报文的分段报文进行报文重组,基于重组后的报文进行攻击特征检测。

[0176] 在一实施例中,所述处理器802,还用于检测所述分段报文的头部字段是否满足设定条件;

[0177] 若检测到所述分段报文的头部字段满足设定条件,确定所述服务器会执行丢弃操作。

[0178] 在一实施例中,所述报文包括IP分片报文;所述设定条件包括以下至少之

[0179] 一:IP报文的生存时间TTL小于设定阈值;

[0180] IP分片报文的路由路径不是设定路由路径;

[0181] IP分片报文的最后一跳的路由地址为设定路由地址;所述设定路由地址表征防火墙的地址;

[0182] IP分片报文的校验和存在错误;

[0183] IP分片报文的时间戳选项存在错误。

[0184] 在一实施例中,所述报文包括TCP报文;所述设定条件包括以下至少之一:

[0185] TCP报文的校验和存在错误;

[0186] TCP报文的所有标志位都为空值;

[0187] TCP报文的所有标志位都不为空值;

[0188] TCP报文的紧急标志位不为空值,且存在有效载荷;

[0189] TCP报文在已建立连接的会话上重复发送同步序列编号SYN标志;

[0190] TCP报文的设定选项字段存在错误。

[0191] 在一实施例中,所述设定选项字段为无法纠正错误的选项字段;所述处理器802,还用于若所述TCP报文中包括可修正错误的选项字段时,将可修正错误的选项字段修正为正确字段。

[0192] 在一实施例中,所述处理器802,还用于在进行分段重组时,在接收到的所述至少两个分段报文的内容存在重叠时,将第一时刻接收到的分段报文的内容的重叠部分覆盖至第二时刻接收到的分段报文的内容的重叠部分;其中,所述第一时刻在所述第二时刻之前;

[0193] 在基于重组后的报文未检测到攻击特征时,将覆盖后的各个分段报文发送至服务器。

[0194] 在一实施例中,所述报文包括TCP报文;所述处理器802,还用于将确定出的不为攻击报文的TCP报文进行缓存;

[0195] 在接收到所述TCP报文的重传数据包时,将所述重传数据包替换为对应的已缓存的TCP报文;

[0196] 将替换后的重传数据包发送至服务器。

[0197] 在一实施例中,所述重组后的报文为应用层报文,所述处理器802,还用于在基于应用层报文未检测到攻击特征时,基于应用层协议解析确定所述应用层报文的异常等级;

[0198] 基于所述应用层报文的异常等级以及所述TCP层和IP层的对应报文是否具备混淆,确定是否执行拦截。

[0199] 当然,实际应用时,电子设备中的各个组件通过总线系统804耦合在一起。可理解,总线系统804用于实现这些组件之间的连接通信。总线系统804除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图8中将各种总线都标为总线系统804。

[0200] 本申请实施例中的存储器803用于存储各种类型的数据以支持电子设备的操作。这些数据的示例包括:用于在电子设备上操作的任何计算机程序。

[0201] 可以理解,存储器803可以是易失性存储器或非易失性存储器,也可包括易失性和非易失性存储器两者。其中,非易失性存储器可以是只读存储器(ROM,Read Only Memory)、可编程只读存储器(PROM,Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM,Erasable Programmable Read-Only Memory)、电可擦除可编程只读存储器(EEPROM,Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器(FRAM,ferromagnetic random access memory)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(CD-ROM,Compact Disc Read-Only Memory);磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器(RAM,Random Access Memory),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(SRAM,Static Random Access Memory)、同步静态随机存取存储器(SSRAM,Synchronous Static Random Access Memory)、动态随机存取存储器(DRAM,Dynamic Random Access Memory)、同步动态随机存取存储器(SDRAM,Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器(DDRSDRAM,Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器(ESDRAM,Enhanced Synchronous Dynamic Random Access Memory)、同步连接动态随机存取存储器(SLDRAM,SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器(DRRAM,Direct Rambus Random Access Memory)。本申请实施例描述的存储器803旨在包括但不限于这些和任意其它适合类型的存储器。

[0202] 上述本申请实施例揭示的方法可以应用于处理器802中,或者由处理器802实现。处理器802可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器802中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器802可以是通用处理器、DSP,或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器802可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于存储器803,处理器802读取存储器803中的程序,结合其硬件完成前述方法的步骤。

[0203] 处理器802执行所述程序时实现本申请实施例的各个方法中的相应流程。

[0204] 在示例性实施例中,本申请实施例还提供了一种存储介质,即计算机存储介质,具体为计算机可读存储介质,例如包括存储计算机程序的存储器803,上述计算机程序可由处理器802执行,以完成前述方法所述步骤。计算机可读存储介质可以是FRAM、ROM、PROM、

EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或CD-ROM等存储器。

[0205] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置、终端和方法,可以通过其它的方式实现。以上所描述的设备实施例仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。

[0206] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元,即可以位于一个地方,也可以分布到多个网络单元上;可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0207] 另外,在本申请各实施例中的各功能单元可以全部集成在一个处理单元中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0208] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于一计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0209] 或者,本申请上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台电子设备(可以是个人计算机、服务器、或者网络设备等)执行本申请各个实施例所述方法的全部或部分。而前述的存储介质包括:移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0210] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。因此,本申请的保护范围应以所述权利要求的保护范围为准。

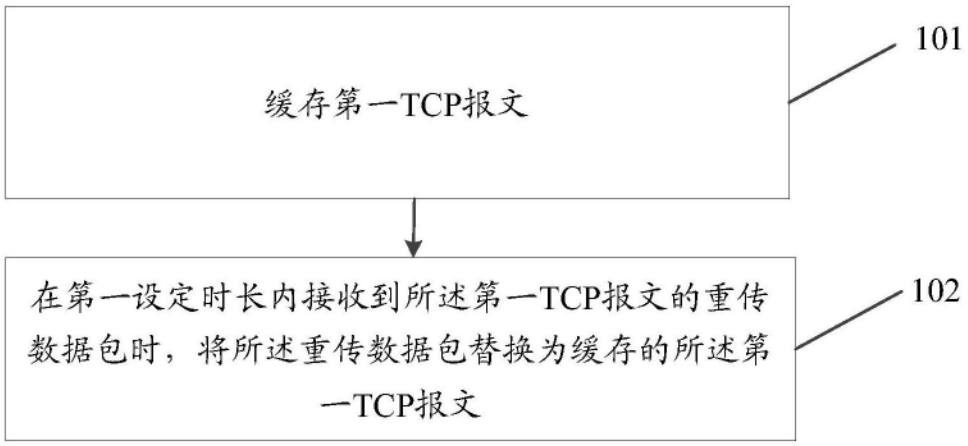

缓存第一TCP报文
101
在第一设定时长内接收到所述第一TCP报文的重传数据包时，将所述重传数据包替换为缓存的所述第一TCP报文
102

图1

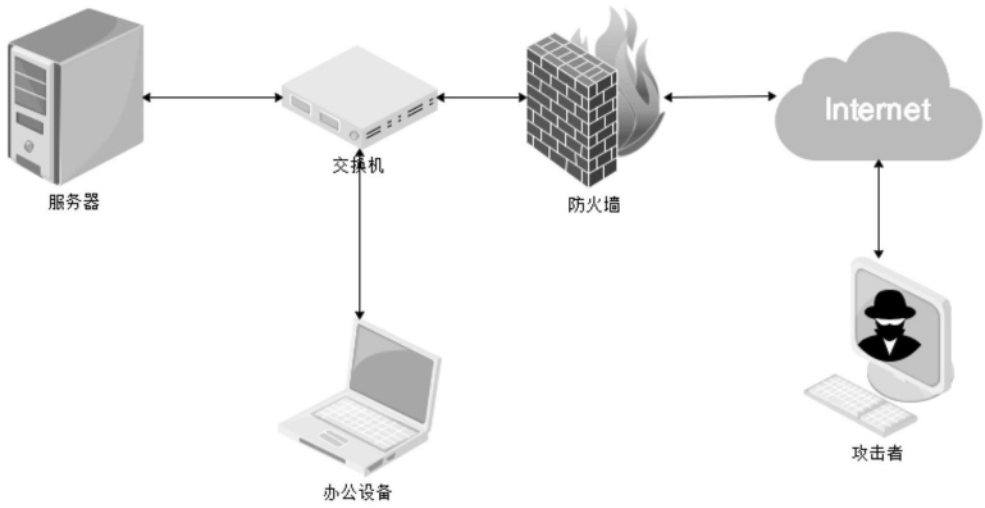

服务器
交换机
防火墙
Internet
攻击者
办公设备

图2a

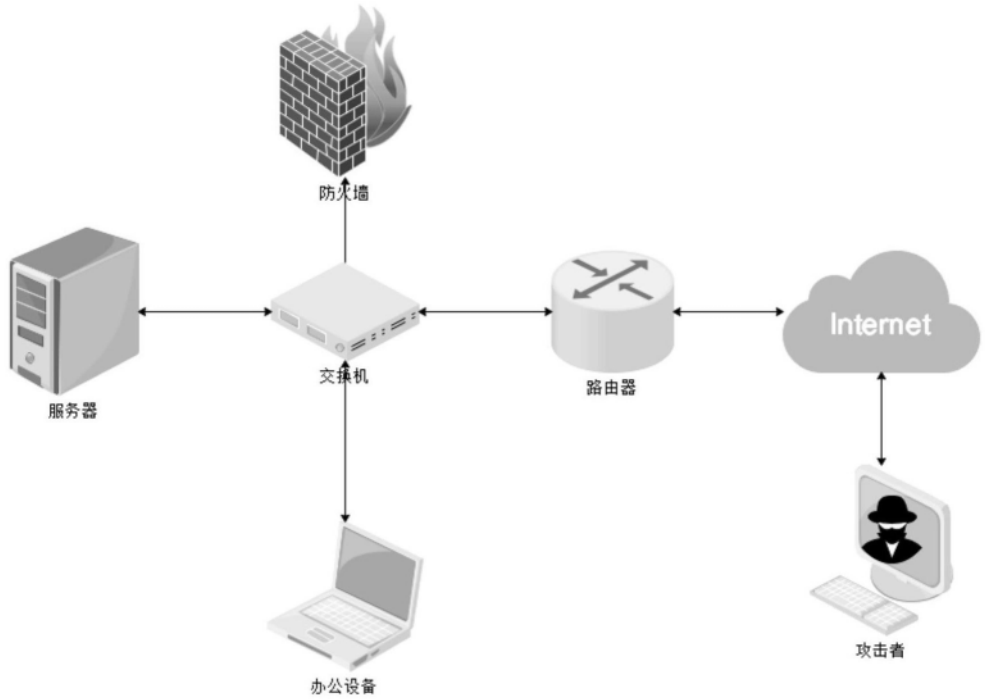


图2b

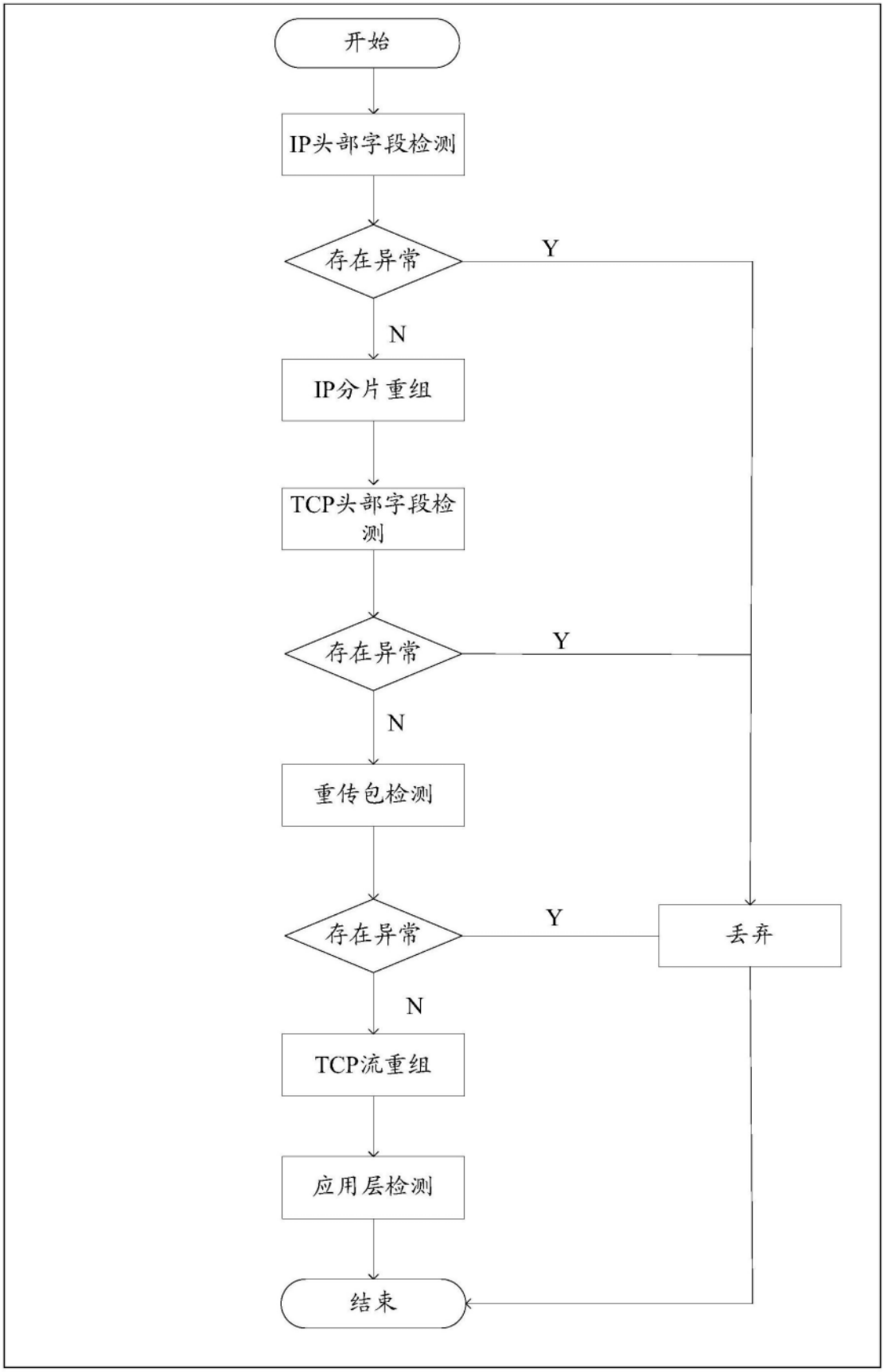

开始
IP头部字段检测
存在异常
Y
N
IP分片重组
TCP头部字段检测
存在异常
Y
N
重传包检测
存在异常
Y
丢弃
N
TCP流重组
应用层检测
结束

图3

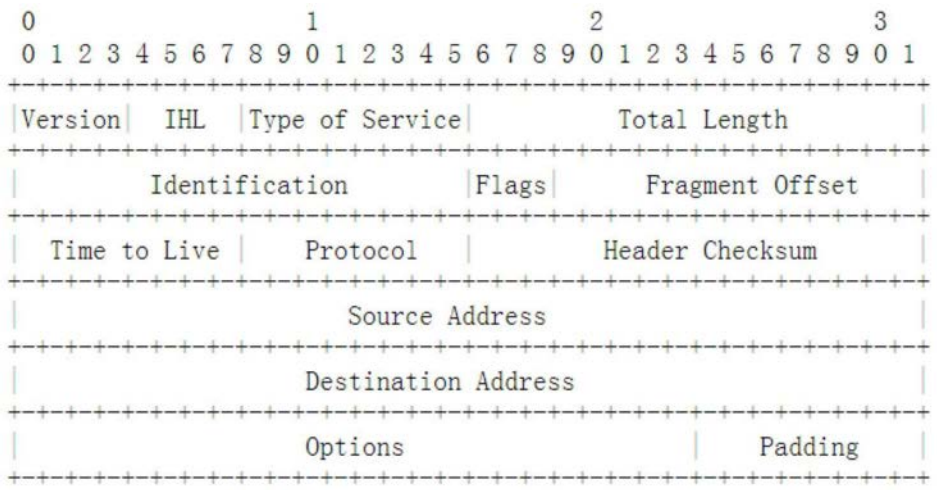
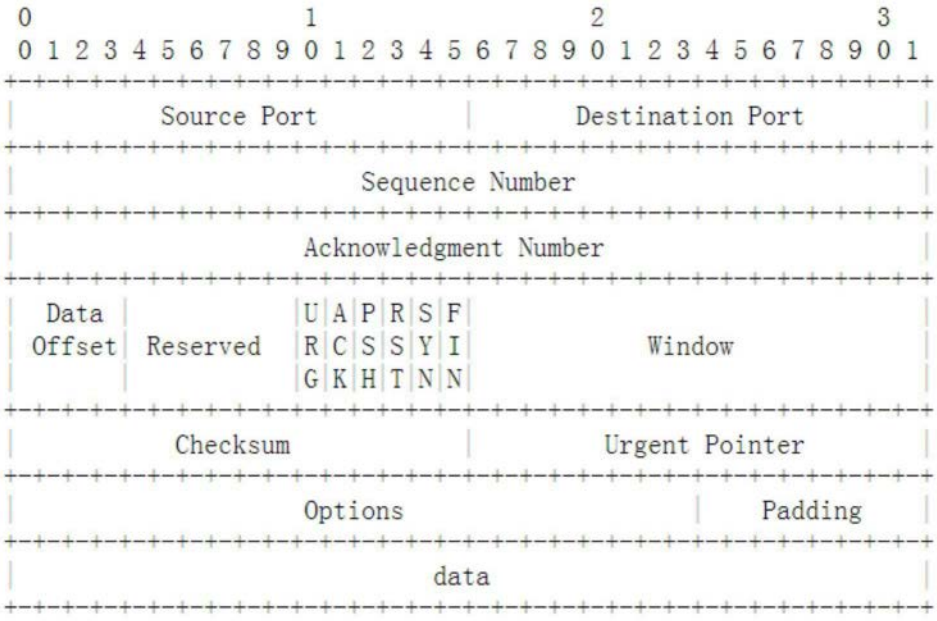


图4



TCP Header Format

图5

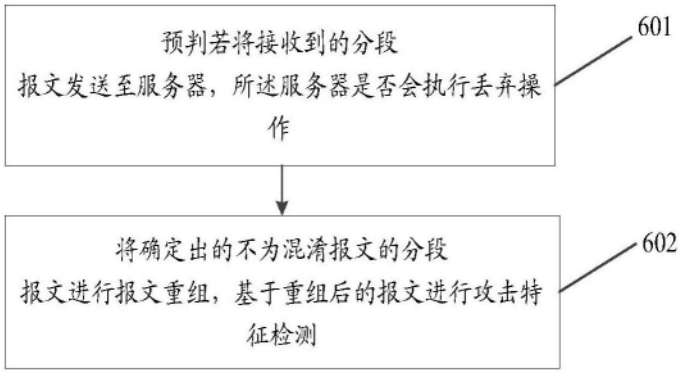

预判若将接收到的分段
报文发送至服务器，所述服务器是否会执行丢弃操作
601
将确定出的不为混淆报文的分段
报文进行报文重组，基于重组后的报文进行攻击特征检测
602

图6

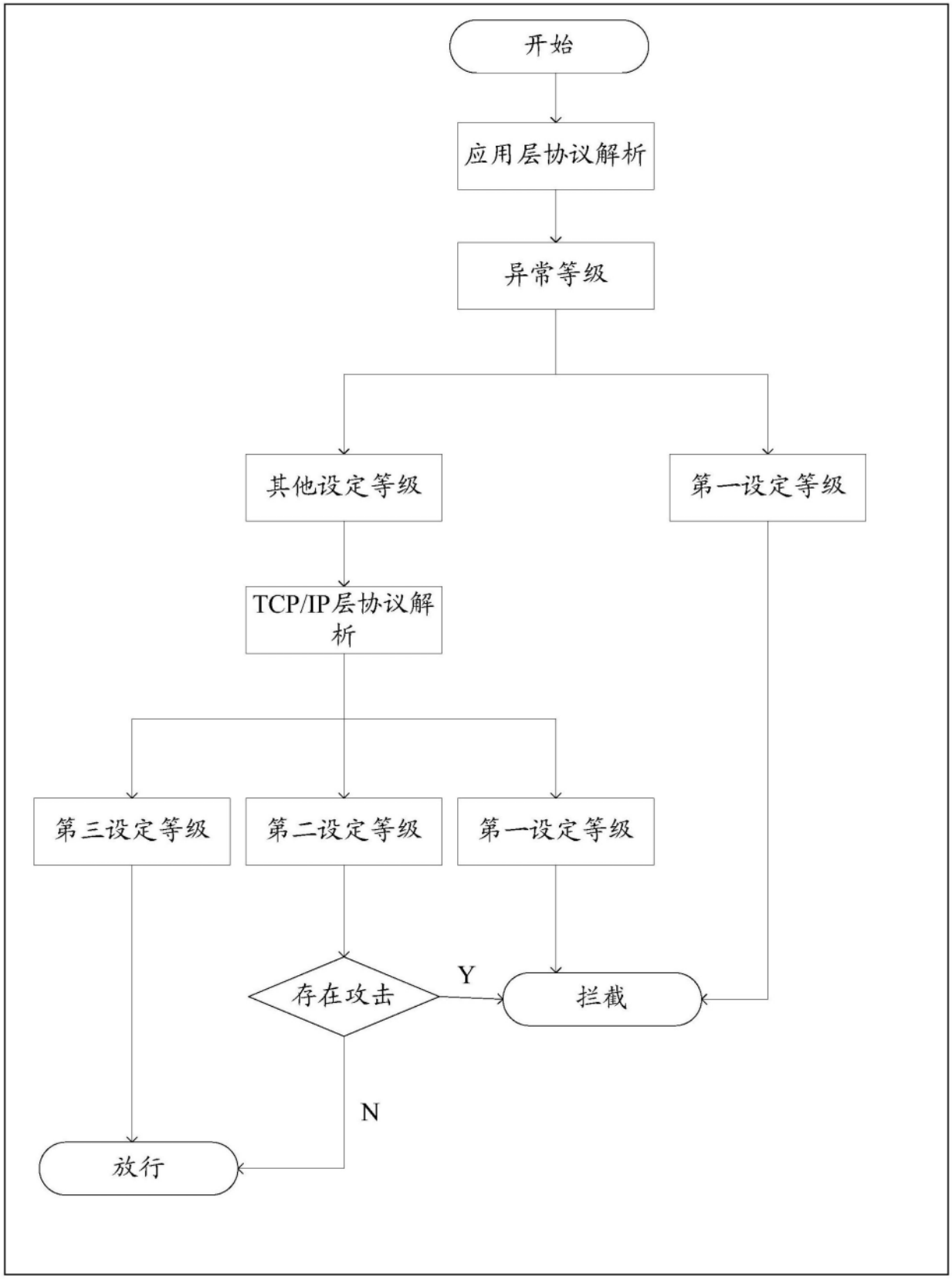

开始
应用层协议解析
异常等级
其他设定等级
第一设定等级
TCP/IP层协议解析
第三设定等级
第二设定等级
第一设定等级
存在攻击
Y
拦截
N
放行

图7

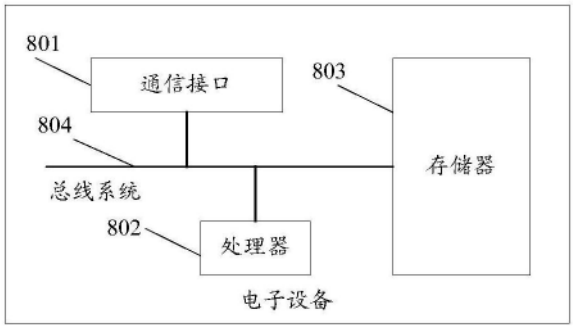


图8