

安全服务处理方法、装置、设备、存储介质及程序产品

本申请要求于2022年12月30日提交中国专利局、申请号为202211724025.7、申请名称为“安全服务处理方法、装置、设备、存储介质及程序产品”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。

5 技术领域

本申请涉及网络安全技术领域，特别涉及安全服务处理。

背景技术

随着网络技术的不断发展，越来越多的网络内容供应商通过互联网向用户提供多种多样的网络内容，相应的，网络安全问题也越来越受到重视。

10 在相关技术中，可以部署蜜罐系统来捕获或者分析网络攻击行为。具体的，相关系统中的蜜罐系统通过离线安装包的形式，由蜜罐系统的服务人员手动部署在网络内容供应商的机房中。

然而，上述相关技术中，蜜罐系统的服务人员离线部署蜜罐系统的方案的操作复杂度较高，对蜜罐系统的部署效率有很大的影响。

15 发明内容

本申请实施例提供了一种安全服务处理方法、装置、设备、存储介质及程序产品，可以提高蜜罐系统的部署效率，该技术方案如下：

一方面，提供了一种安全服务处理方法，所述方法由云端服务器执行，所述方法包括：

20 接收网络内容供应商发送的蜜罐服务部署请求；所述蜜罐服务部署请求用于指示探针服务类型以及蜜罐服务类型；所述探针服务类型用于指示流量牵引方式；

基于所述蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务；所述目标网络内容是所述网络内容供应商提供的网络内容；

建立所述探针服务类型的探针服务；所述探针服务用于将对所述目标网络内容的访问流量牵引至所述蜜罐服务。

25 另一方面，提供了一种安全服务处理装置，所述装置包括：

请求接收模块，用于接收网络内容供应商发送的蜜罐服务部署请求；所述蜜罐服务部署请求用于指示探针服务类型以及蜜罐服务类型；所述探针服务类型用于指示流量牵引方式；

30 蜜罐服务建立模块，用于基于所述蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务；所述目标网络内容是所述网络内容供应商提供的网络内容；

探针服务建立模块，用于建立所述探针服务类型的探针服务；所述探针服务用于将对所述目标网络内容的访问流量牵引至所述蜜罐服务。

在一种可能的实现方式中，所述探针服务类型包括侵入式流量牵引类型或者非侵入式流量牵引类型。

35 在一种可能的实现方式中，响应于所述探针服务类型包括侵入式流量牵引类型，所述探针服务建立模块，用于，

在云端创建所述探针服务的规则引擎和牵引引擎；

- 2 -

其中, 所述规则引擎用于识别对所述目标网络内容的访问流量是否为指定类型访问流量;

所述牵引引擎用于基于规则引擎的识别结果, 将所述指定类型访问流量牵引至所述蜜罐服务。

5 在一种可能的实现方式中, 所述装置还包括:

规则接收模块, 用于接收所述第一设备发送的流量识别规则; 所述流量识别规则用于指示所述指定类型访问流量的判别条件;

规则下发模块, 用于将所述流量识别规则下发至所述规则引擎。

10 在一种可能的实现方式中, 响应于所述探针服务类型包括非侵入式流量牵引类型, 所述探针服务建立模块, 用于,

创建供应商网络与所述蜜罐服务之间的弹性网卡; 所述供应商网络是提供所述目标网络内容的网络;

15 基于所述弹性网卡配置所述供应商网络与所述蜜罐服务之间的网络地址转换规则; 所述网络地址转换规则用于指示所述弹性网卡将对所述目标网络内容的访问流量转发至所述蜜罐服务。

在一种可能的实现方式中, 所述探针服务建立模块, 用于,

在所述供应商网络中创建虚拟私有云;

在所述虚拟私有云中插入所述弹性网卡, 所述弹性网卡与所述蜜罐服务绑定;

在所述虚拟私有云中申请所述弹性网卡的虚拟地址;

20 将所述弹性网卡的虚拟地址与所述供应商网络的公网地址或者内网地址进行绑定。

在一种可能的实现方式中, 所述探针服务建立模块, 用于,

在所述供应商网络的虚拟私有云中创建代理主机, 所述虚拟私有云对应于所述蜜罐服务;

25 基于所述代理主机创建目的地址转换DNAT规则, 所述DNAT规则用于将所述代理主机的流量转发至所述蜜罐服务;

在所述虚拟私有云中申请所述弹性网卡;

将所述弹性网卡绑定至所述代理主机。

30 在一种可能的实现方式中, 所述探针服务建立模块, 还用于为所述弹性网卡绑定安全组规则, 所述安全组规则用于禁止被牵引到所述蜜罐服务中的访问流量主动访问所述供应商网络。

在一种可能的实现方式中, 所述装置还包括:

获取模块, 用于获取所述蜜罐服务或者所述探针服务的建立结果以及建立次数;

重建模块, 用于响应于所述建立结果为建立失败, 且所述建立次数未达到次数阈值, 对建立失败的所述蜜罐服务或者所述探针服务进行重新建立。

35 在一种可能的实现方式中, 所述装置还包括:

信息返回模块, 用于响应于所述建立结果为建立失败, 且所述建立次数达到所述次数阈值, 向所述云端服务器的控制台返回所述蜜罐服务或者所述探针服务建立失败的信息。

在一种可能的实现方式中，所述装置还包括：
记录模块，用于记录所述蜜罐服务中的访问流量的行为记录；
发送模块，用于向所述网络内容供应商返回所述行为记录。

另一方面，提供了一种计算机设备，所述计算机设备包括处理器和存储器，所述存储器中存储由至少一条计算机程序，所述至少一条计算机程序由所述处理器加载并执行以实现上述安全服务处理方法。

另一方面，提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有至少一条计算机程序，所述计算机程序由处理器加载并执行以实现上述安全服务处理方法。

另一方面，提供了一种包括计算机程序的计算机程序产品，当其在计算机上运行时，使得所述计算机执行以上方面的安全服务处理方法。

本申请提供的技术方案可以包括以下有益效果：

云端服务器接收网络内容供应商的第一设备发送的蜜罐服务部署请求，并基于该请求指示的探针服务类型以及蜜罐服务类型，建立与目标网络内容对应的蜜罐服务以及探针服务，以通过探针服务将对目标网络内容的访问流量牵引至蜜罐服务；上述方案只需要网络内容供应商在线配置探针服务类型以及蜜罐服务类型，即可以自动在云端创建网络内容供应商的蜜罐服务，不需要蜜罐系统的服务人员离线部署蜜罐系统，从而提高蜜罐系统的部署效率。

附图说明

- 图1是本申请一示例性实施例涉及的系统的示意图；
- 图2是本申请一示例性实施例示出的安全服务处理方法的流程图；
- 图3是图2所示实施例涉及的一种蜜罐系统建立框架图；
- 图4是本申请一示例性实施例示出的安全服务处理方法的流程图；
- 图5是图4所示实施例涉及的侵入式流量牵引方式的蜜罐系统架构图；
- 图6是本申请一示例性实施例示出的安全服务处理方法的流程图；
- 图7是图6所示实施例涉及的探针服务的建立框架示意图；
- 图8是图6所示实施例涉及的探针服务的建立框架示意图；
- 图9是本申请提供的一种蜜罐创建和流量牵引流程图；
- 图10是本申请一个实施例提供的安全服务处理装置的方框图；
- 图11示出了本申请一示例性实施例示出的计算机设备的结构框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

应当理解的是，在本文中提及的“多个”是指两个或两个以上。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。字符“/”一般表示前后关联对象是一种“或”的关系。

本申请实施例提供了一种用于云端的蜜罐服务部署方法，可以自动为网络内容供应商建立蜜罐系统，可以提升蜜罐系统的部署效率。为了便于理解，下面对本申请涉及的几个名词进行解释。

1) 云安全

- 5 云安全（Cloud Security）是指基于云计算商业模式应用的安全软件、硬件、用户、机构、安全云平台的总称。云安全融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，并发送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。
- 10 云安全研究方向包括：1、云计算安全，主要研究如何保障云自身及云上各种应用的安全，包括云计算系统安全、用户数据的安全存储与隔离、用户接入认证、信息传输安全、网络攻击防护、合规审计等；2、安全基础设施的云化，主要研究如何采用云计算新建与整合安全基础设施资源，优化安全防护机制，包括通过云计算技术构建超大规模安全事件、信息采集与处理平台，实现对海量信息的采集与关联分析，提升全网安全事件把控能力及风险控制能力；3、云安全服务，主要研究各种基于云计算平台为用户提供的安全服务，如防病毒服务等。
- 15

2) 蜜罐

- 一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁。
- 20

3) 弹性网卡（Elastic Network Interface, ENI）

 绑定私有网络（Virtual Private Cloud, VPC）内云端服务器的一种弹性网络接口，可在多个云端服务器间自由迁移。

4) 弹性公网IP（Elastic IP, EIP）

- 25 用户可以将EIP实例与云端服务器、负载均衡、NAT网关、VPN网关等实例绑定或解绑。

5) 负载均衡（Load Balance, LB）/传统型负载均衡（Classic LB, CLB）

 负载均衡建立在网络结构之上，它提供了一种廉价有效透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性，各企业通常将门户网站放置在LB上。

- 30 6) 虚拟私有云（Virtual Private Cloud, VPC）

 一种基于云平台构建的专属云上网络空间，为用户在云端上的资源提供网络服务，不同私有网络间可以实现逻辑隔离。

7) 真实服务器（Real Server, RS）

 用于真正处理用户的请求的服务器。

- 35 8) 高可用虚拟IP（High-Availability Virtual IP, HAVIP）

 一种从VPC子网CIDR分配的一个内网IP地址，通常和高可用软件配合使用，应用于搭建高可用主备集群场景。

9) 探针

蜜罐服务对外暴露的形式，比较常见的有：公网IP、内网IP、域名等等。

图1示出了本申请一示例性实施例提供的安全服务处理方法所使用的系统的示意图，如图1所示，该系统包括：服务器110以及终端120。

5 其中，上述服务器110可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN（Content Delivery Network，内容分发网络）、以及大数据和人工智能平台等基础云计算服务的云端服务器。

10 上述服务器110可以包括部署有蜜罐管理系统，并通过蜜罐管理系统向网络内容供应商用户提供蜜罐系统的部署、管理和运行的服务器，或者，上述服务器110也可以包括网络内容供应商部署的，用于向用户提供网络内容的服务器。

上述终端120可以是具有网络连接功能以及数据处理功能的终端设备，比如，终端120可以是智能手机、平板电脑、电子书阅读器、智能眼镜、智能手表、智能电视、膝上型便携计算机和台式计算机等等。

15 上述终端120可以包括网络内容供应商的用户终端，或者，上述终端120也可以包括对网络内容供应商提供的网络内容进行访问的用户终端。

可选的，上述系统中包含一个或者多个服务器110，以及多个终端120。本申请实施例对于服务器110和终端120的个数不做限制。

终端以及服务器通过通信网络相连。可选的，通信网络是有线网络或无线网络。

20 可选的，上述的无线网络或有线网络使用标准通信技术和/或协议。网络通常为因特网，但也可以是任何网络，包括但不限于局域网（Local Area Network，LAN）、城域网（Metropolitan Area Network，MAN）、广域网（Wide Area Network，WAN）、移动、有线或者无线网络、专用网络或者虚拟专用网络的任何组合。在一些实施例中，使用超文本标记语言（Hyper Text Mark-up Language，HTML）、可扩展标记语言（Extensible Markup Language，XML）等的技术和/或格式来代表通过网络交换的数据。还可以使用诸如安全套接字层（Secure Socket Layer，SSL）、传输层安全（Transport Layer Security，TLS）、虚拟专用网络（Virtual Private Network，VPN）、网际协议安全（Internet Protocol Security，IPsec）等常规加密技术来加密所有或者一些链路。在另一些实施例中，还可以使用定制和/或专用数据通信技术取代或者补充上述数据通信技术。本申请在此不做限制。

30 目前市面上大部分蜜罐系统，都需要根据公司的业务模型，去选择与之相匹配的蜜罐类型，并与正常业务隔离开。而传统蜜罐会部署在用户机房，通过离线安装包的形式，手动部署在各个区域：办公区、生产区。然后手动配置各类转发策略，使得蜜罐流量迁移符合预期。

35 作为蜜罐系统还有一个比较重要的问题，在攻击方攻破蜜罐，进一步逃逸之后，就能以蜜罐为跳板，扩大入侵范围，进而攻破租户更多的机器，对租户造成不可挽回的损失。传统的蜜罐系统在这一点会采用复杂的方案（嵌套虚拟化等）以保证攻击方难以逃逸，甚至在租户的部署网络中，因地制宜使用各种网络策略来限制蜜罐逃逸和横向移动的动作。

-6-

具体来说,传统的蜜罐系统部署和正常业务隔离开,对蜜罐的仿真度要求极高,同时需要通过各种方式去散播到网络,以诱导攻击方来踩中蜜罐。这种部署方式路径太长,无法做到正常业务按需引流,没办法提高蜜罐的使用率,对业务保护能力有限。

5 传统的蜜罐系统在部署上面需要花很多精力去安装蜜罐,这种部署引流方式,成本较高,往往需要蜜罐厂商提供技术人员支持才能让蜜罐正常运行。甚至需要租户的运维人员一起解决复杂的网络问题,才能将蜜罐部署到合适的位置。

传统的蜜罐系统在蜜罐网络隔离的问题上,会采用很多复杂的虚拟化技术,产品方案难度和稳定性都无法保证;或者,传统的蜜罐系统需要配置各类网络策略限制,如果不了解租户的网络拓步,配置复杂度会较高,有可能会因为错误的配置,影响租户自己的业务。

10 图2示出了本申请一示例性实施例示出的安全服务处理方法的流程图,该方法由计算机设备执行,该计算机设备可以实现为云端服务器,该云端服务器可以是图1所示的服务器110,如图2所示,该安全服务处理方法包括以下步骤:

步骤210: 接收网络内容供应商发送的蜜罐服务部署请求。

15 蜜罐服务部署请求用于指示探针服务类型以及蜜罐服务类型;探针服务类型用于指示流量牵引方式。该蜜罐服务部署请求可以是网络内容提供商通过设备生成并发送给云端服务器的,该设备例如可以是第一设备。探针服务类型所指示的流量牵引方式,可以标识将采用何种流量牵引方式,将访问目标网络内容的访问流量牵引到蜜罐服务中。

在一种可能的实现方式中,上述探针服务类型包括侵入式流量牵引类型或者非侵入式流量牵引类型。

20 其中,侵入式流量牵引类型,是一种通过探针服务介入网络内容供应商的业务流程的流量牵引类型,比如,侵入式流量牵引类型的探针服务可以将访问网络内容供应商提供的网络内容的恶意访问流量牵引到蜜罐服务,并对非恶意访问流量进行放行处理。

25 上述非侵入式流量牵引类型,是一种探针服务不介入网络内容供应商的业务流程的流量牵引类型,比如,非侵入式流量牵引类型的探针服务将访问网络内容供应商提供的网络内容的访问流量全量转发到蜜罐服务。

30 上述蜜罐服务类型指示可以是要建立的蜜罐服务的蜜罐类型,比如,数据库类蜜罐、网页类蜜罐、邮件类蜜罐、安全外壳(Secure Shell, SSH)类蜜罐、文件传输协议(File Transfer Protocol, FTP)类蜜罐等等。该蜜罐服务类型可以包括至少一种蜜罐类型,由于蜜罐服务是用于作为诱饵,欺骗攻击者以为访问到目标网络内容的服务,故蜜罐服务类型具体所包括的蜜罐类型可以与目标网络内容相关。

在本申请实施例中,云端服务器可以通过网页或者APP的方式向网络内容供应商推送蜜罐配置页面,网络内容供应商的运营人员可以通过该蜜罐配置页面配置所需要部署的蜜罐服务的探针服务类型以及蜜罐服务类型等信息。

35 在一种可能的实现方式中,上述探针服务类型以及蜜罐服务类型可以由蜜罐服务部署请求显式指示或者隐式指示。

比如,上述蜜罐服务部署请求中可以直接通过显式方式携带探针服务类型的指示信息,以及蜜罐服务类型的指示信息。比如,蜜罐服务部署请求中可以包含探针服务类型指示域,

以及蜜罐服务类型指示域，该探针服务类型指示域以及蜜罐服务类型指示域分别通过一个比特值来指示上述探针服务类型以及蜜罐服务类型。具体例如，探针服务类型指示域值为0时，表示探针服务类型为侵入式的流量牵引类型，探针服务类型指示域值为1时，表示探针服务类型为非侵入式的流量牵引类型。再例如，蜜罐服务类型指示域值为0时，表示蜜罐服务类型为SSH类型，蜜罐服务类型指示域值为1时，表示蜜罐服务类型为数据库类型。

再比如，上述蜜罐服务部署请求中可以通过显式方式携带探针服务类型的指示信息以及蜜罐服务类型的指示信息中的一种，并通过隐式方式指示探针服务类型和蜜罐服务类型中的另一种。例如，蜜罐服务部署请求中可以包含探针服务类型指示域，同时，该蜜罐服务部署请求的目的地址指示蜜罐服务类型（也就是说，请求建立不同类型的蜜罐服务的蜜罐服务部署请求被发送到不同的目的地址，从而实现不同类型的蜜罐服务建立的分流）。再例如，蜜罐服务部署请求中可以包含蜜罐服务类型指示域，同时，该蜜罐服务部署请求的目的地址指示探针服务类型（也就是说，请求建立不同类型的探针服务的蜜罐服务部署请求被发送到不同的目的地址，从而实现不同类型的探针服务建立的分流）。

再比如，上述蜜罐服务部署请求中可以通过隐式方式指示探针服务类型和蜜罐服务类型。例如，蜜罐服务部署请求的目的地址指示探针服务类型和蜜罐服务类型的组合，也就是说，请求建立不同类型的探针服务和蜜罐服务的蜜罐服务部署请求被发送到不同的目的地址，从而实现不同类型的探针服务和蜜罐服务建立的分流。

在一种可能的实现方式中，上述蜜罐服务部署请求中还可以指示探针服务类型以及蜜罐服务类型之外的其他信息，例如其他在云端部署蜜罐服务所需要的信息，比如，上述蜜罐服务部署请求还可以指示网络内容供应商需要保护的网络地址或者网络内容地址、部署蜜罐系统所需要的授权信息、网络内容供应商的自定义信息（比如自定义的流量识别规则）等等。

在另一种可能的实现方式中，上述其他信息也可以通过蜜罐服务部署请求之外的其他请求或者其他方式获取。比如，云端服务器可以从云端数据库读取预先存储的上述其他信息。

步骤220：基于蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务。

目标网络内容是网络内容供应商提供的网络内容。

在本申请实施例中，云端服务器可以维护一个蜜罐服务集群（可以称为蜜场），其中包含为各个网络内容供应商（可以称为租户）建立的蜜罐服务，在接收到上述蜜罐服务部署请求后，云端服务器可以根据蜜罐服务部署请求所指示的蜜罐服务类型，在蜜场中建立该网络内容供应商的蜜罐服务。

步骤230：建立探针服务类型的探针服务。

探针服务用于将对目标网络内容的访问流量牵引至蜜罐服务。

在本申请实施例中，在接收到上述蜜罐服务部署请求后，云端服务器可以根据蜜罐服务部署请求所指示的探针服务类型，为该网络内容供应商建立对应目标网络内容的探针服务，该探针服务可以实现将对目标网络内容的访问流量牵引至网络内容供应商的蜜罐服务的功能。

其中，上述蜜罐服务的建立步骤（步骤220）和探针服务的建立步骤（步骤230）可以先后执行，也可以同步执行；比如，云端服务器可以先执行步骤220的蜜罐服务建立步骤，再执行步骤230的探针服务建立步骤；或者，云端服务器可以先执行步骤230的探针服务建立步骤，再执行步骤220的蜜罐服务建立步骤；或者，云端服务器也可以同步执行步骤220和步骤230。

在上述探针服务和蜜罐服务建立过程中或者建立完成后，云端服务器即可以将探针服务和蜜罐服务绑定，以便后续探针服务将对网络内容提供商提供的网络内容的访问流量牵引到蜜罐服务。比如，云端服务器可以将蜜罐服务的标识信息（蜜罐服务的地址或者编号）配置到探针服务中。

请参考图3，其示出了本申请实施例涉及的一种蜜罐系统建立框架图。如图3所示：

S1，在网络内容供应商的网络310中，第一设备310a访问云端320中的云端服务器320a，云端服务器320a向第一设备310a推送蜜罐配置页面310b。

S2，第一设备310a的用户通过蜜罐配置页面310b配置探针服务类型以及蜜罐服务类型等信息。

S3，用户在蜜罐配置页面310b中完成配置后，第一设备310a向云端服务器320a发送蜜罐服务部署请求，该请求指示用户配置的探针服务类型以及蜜罐服务类型等信息。

S4，云端服务器320a建立探针服务320b以及蜜罐服务320c。

后续访问该网络内容供应商提供的目标网络内容的访问流量将通过探针服务320b部分或者全部被牵引至蜜罐服务320c。

在一种可能的实现方式中，为了提高蜜罐系统创建的稳定性，在有限的次数内尽量完成对蜜罐服务或者探针服务的建立。云端服务器还可以获取蜜罐服务或者探针服务的建立结果以及建立次数；响应于建立结果为建立失败，且建立次数未达到次数阈值，对建立失败的蜜罐服务或者探针服务进行重新建立。

在一种可能的实现方式中，为了使得开发人员或者维护人员及时了解蜜罐系统的漏洞或者问题，云端服务器响应于建立结果为建立失败，且建立次数达到次数阈值，向云端服务器的控制台返回蜜罐服务或者探针服务建立失败的信息。

也就是说，当多次尝试后依然不能成功建立蜜罐服务或者探针服务时，通过返回建立失败的信息，可以让云端服务器的控制方能够及时了解到出现了问题，并进行解决。同时，在建立失败次数达到次数阈值后停止重新建立一直为建立成功的蜜罐服务或者探针服务，也可以有效的节约系统资源。

在一种可能的实现方式中，云端服务器还可以记录蜜罐服务中的访问流量的行为记录；向网络内容供应商返回该行为记录。

在本实现方式中，通过将蜜罐服务中的访问流量的行为记录返回给网络内容供应商，可以让网络内容供应商清晰的了解到针对目标网络内容的异常访问流量，以及相应的异常行为。网络内容供应商可以通过设备接收该行为记录，例如第二设备。

在本申请实施例中，由于蜜罐服务建立并运行在云端，而在不是网络内容供应商的网络中，为了使得网络内容供应商能够及时了解目标网络内容被攻击的情况，云端服务器还

可以将蜜罐服务中的访问流量的行为记录发送给网络内容供应商的第二设备,使得网络内容供应商能够及时了解、分析攻击目标网络内容的恶意访问流量的来源、攻击方式等等,以便做出安全防护方面的应对。

其中,上述蜜罐服务中的访问流量的行为记录可以包括跳转行为、隐私消息读取行为等与网络安全相关的行为。

综上所述,本申请实施例所示的方案,云端服务器接收网络内容供应商的第一设备发送的蜜罐服务部署请求,并基于该请求指示的探针服务类型以及蜜罐服务类型,建立与目标网络内容对应的蜜罐服务以及探针服务,以通过探针服务将对目标网络内容的访问流量牵引至蜜罐服务;上述方案只需要网络内容供应商在线配置探针服务类型以及蜜罐服务类型,即可以自动在云端创建网络内容供应商的蜜罐服务,不需要蜜罐系统的服务人员离线部署蜜罐系统,从而提高蜜罐系统的部署效率。

基于上述图2所示的方案,图4示出了本申请一示例性实施例示出的安全服务处理方法的流程图,也就是说,在探针服务类型包括侵入式流量牵引类型的情况下,步骤230可以替换为步骤230a。

步骤230a: 在云端创建探针服务的规则引擎和牵引引擎。

规则引擎用于识别对目标网络内容的访问流量是否为指定类型访问流量;牵引引擎用于基于规则引擎的识别结果,将指定类型访问流量牵引至蜜罐服务。

在本申请实施例中,响应于探针服务类型包括侵入式流量牵引类型,云端服务器可以在云端(比如云端防火墙)建立包含规则引擎和牵引引擎的探针服务。

比如,以在云端防火墙中建立包含规则引擎和牵引引擎的探针服务为例,在一种可能的实现方式中,云端防火墙中可以预先设置有探针服务建立组件,比如该探针服务组件可以是一个虚拟机,响应于探针服务类型包括侵入式流量牵引类型,云端服务器向该探针服务建立组件发送探针服务建立指示,该探针服务建立组件接收探针服务建立指示,并根据该探针服务建立指示建立一个包含规则引擎和牵引引擎的探针服务,并向云端服务器返回该探针服务的标识信息,比如探针服务的地址或者编号;云端服务器将探针服务的标识信息与网络内容供应商的标识信息(比如网络内容供应商的账号、网络内容供应商提供的网络内容的访问地址等等)进行绑定。

其中,在云端建立包含规则引擎和牵引引擎的探针服务后,访问目标网络内容的访问流量可以被转发至规则引擎,由规则引擎判断该访问流量是否为恶意访问流量,若判断为恶意访问流量,则将该访问流量被牵引至蜜罐服务;若判断为非恶意访问流量,则该访问流量将被放行,以访问该目标网络内容的RS。

请参考图5,其示出了本申请实施例涉及的侵入式流量牵引方式的蜜罐系统架构图。以结合云端防火墙建立探针服务为例,如图5所示,基于侵入式流量牵引方式的蜜罐系统的创建和运行过程如下:

S1,某用户访问云上租户(即网络内容提供商)部署的门户网站(比如www.test.com)。

S2,流量经过云端转发集群进行转发,当前默认用户接入了云端防火墙,因此流量会通过虚拟扩展局域网(Virtual Extensible Local Area Network, VXLAN)隧道技术封包+通

用路由封装, 或者通用网络虚拟化封装 (Generic Routing Encapsulation- Generic Network Virtualization Encapsulation, GRE-GENEVE) 隧道两种方式, 将原始L3的报文转给云端防火墙引擎。

5 S3, 防火墙引擎首先会经过访问控制列表 (Access Control List, ACL) 访问控制模块, 过滤用户配置的访问控制规则, 放行白名单流量, 阻断黑名单流量。经过ACL访问控制模块放行的流量会再经过解码模块, 该解码模块可以先解析流量协议, 实现流会话重组, 针对重组后的流量, 进行常见的解码 (如: base64、路径解码 (urlDecode)、混淆字符串过滤等)。然后, 通过探针服务的规则引擎对解码后的报文匹配开箱规则或者预先配置的规则, 如果命中了规则, 则可以判定报文为恶意攻击; 若未命中规则, 则可以判定报文为正常流量。

10 S4, 如果当前流量为正常业务请求, 探针服务的规则引擎放行该会话, 不做任务处理, 通过Vxlan隧道和Gre-Geneve隧道, 按照原路由走回到转发集群。

S5, 转发集群收到回传回来的数据报文, 根据当前路由转发策略, 直接将流量路由到租户部署的真实服务上, 用户就能正常收到返回超文本传输协议 (Hyper Text Transfer Protocol, HTTP) 状态 (Status) 200页面, 功能正常。

S6, 如果当前报文经过匹配命中规则, 则判定当前报文为攻击报文, 此时探针服务的规则引擎将当前流量的报文发送到动态牵引模块 (即上述探针服务的牵引引擎) 进行处理。

S7, 动态迁移模块根据预先配置的后台蜜罐地址 (即租户的蜜罐服务的地址), 可以执行以下两种步骤:

20 A) 丢掉当前请求, 不再转发请求到客户的真实业务, 从而保护当前资产免受攻击;
B) 同时直接回复当前用户HTTP状态为302, 并把跳转指向预先配置的蜜罐服务, 比如 www.test.com/login。

25 S8, 用户的终端收到HTTP Status为302跳转之后, 直接重定向到了www.test.com/login的蜜罐服务, 蜜罐服务再接收恶意攻击, 然后将执行后的结果反馈给用户, 后续交互由用户和蜜罐服务进行直接交互, 避免真实业务受到干扰。

其中, 上述方案以探针服务建立在云端防火墙服务中为例介绍侵入式流量牵引的探针服务部署方式, 可选的, 上述侵入式流量牵引的探针服务也可以部署在其他云端服务 (比如云端网络应用防护服务、云端分布式拒绝服务攻击防护系统等安全服务) 中。

30 在一种可能的实现方式中, 云端服务器还可以接收第一设备发送的流量识别规则; 流量识别规则用于指示指定类型访问流量的判别条件; 将流量识别规则下发至规则引擎。

其中, 上述指定类型访问流量可以为恶意访问流量。

35 在本申请实施例中, 还支持由网络内容供应商自定义恶意访问流量的判别条件, 并将网络内容供应商自定义的判别条件 (即上述流量识别规则) 下发到对应的规则引擎中, 后续规则引擎即可以根据网络内容供应商自定义的判别条件判断哪些访问流量为恶意访问流量。由此可见, 通过流量识别规则, 可以让规则引擎能够准确的识别与当前场景相关的恶意访问流量, 并且使用者还可以基于应用场景的变换针对性的调整流量识别规则, 提升了侵入式部署方式的适配范围。

其中，侵入式部署方式是一种通用思路，可以和各种安全产品结合，比如防火墙、网页应用防护系统、分布式拒绝服务攻击系统等，接入方式比较简单，不需要修改数据包源目的网协地址（Internet Protocol，IP），部署效率高。

综上所述，本申请实施例所示的方案，云端服务器通过在云端建立侵入式流量牵引的
5 探针服务，对访问目标网络内容的访问流量进行过滤，仅将恶意访问流量牵引至蜜罐服务，减少了蜜罐服务处理的访问流量，节约了处理资源和带宽资源，提高系统资源的使用效率。

此外，本申请实施例所示的方案，还支持目标网络供应商自定义的恶意访问流量的判别条件，提高了蜜罐系统的部署灵活性和个性化。

基于上述图2所示的方案，图6示出了本申请一示例性实施例示出的安全服务处理方法的流程图，也就是说，在探针服务类型包括非侵入式流量牵引类型的情况下，步骤230可以
10 替换为步骤230b和步骤230c。

步骤230b：创建供应商网络与蜜罐服务之间的弹性网卡。

供应商网络是提供目标网络内容的网络。

其中，按照流量牵引模式的不同，上述弹性网卡可以部署在供应商网络侧，也可以部
15 署在云端。

其中，上述流量牵引模式可以包括公网IP（EIP）模式、内网IP模式以及负载均衡LB模式等等。

其中，上述公网IP模式是指通过公网IP进行访问流量转发的流量牵引模式。

上述内网IP模式是指通过内网IP进行访问流量转发的流量牵引模式。

20 上述负载均衡模式是指通过负载均衡的方式进行访问流量转发的流量牵引模式。

步骤230c：基于弹性网卡配置供应商网络与蜜罐服务之间的网络地址转换规则。

网络地址转换规则用于指示弹性网卡将对目标网络内容的访问流量转发至蜜罐服务。

在本申请实施例所示的方案中，云端服务器可以配置有供应商网络与蜜罐服务之间的网络地址转换规则的弹性网卡，建立上述基于非侵入式流量牵引的探针服务。

25 在一种可能的实现方式中，在流量牵引模式为公网IP模式或者内网IP模式的情况下，创建供应商网络与蜜罐服务之间的弹性网卡，包括：

在供应商网络中创建虚拟私有云；

在虚拟私有云中插入弹性网卡，弹性网卡与所述蜜罐服务绑定；

在虚拟私有云中申请弹性网卡的虚拟地址；

30 将弹性网卡的虚拟地址与供应商网络的公网地址或者内网地址进行绑定。

在一种可能的实现方式中，上述公网IP模式或者内网IP模式的情况下，创建供应商网络与蜜罐服务之间的弹性网卡，以及基于弹性网卡配置供应商网络与蜜罐服务之间的网络地址转换规则的步骤，可以通过安装在供应商网络的控制终端/配置终端中的配置组件执行，该配置组件可以由控制终端/配置终端从云端服务器下载并安装，比如，该配置组件可以为
35 应用程序、插件、中间件等形式的软件组件；云端服务器在公网IP模式或者内网IP模式的情况下，创建供应商网络与蜜罐服务之间的弹性网卡，以及基于弹性网卡配置供应商网络与蜜罐服务之间的网络地址转换规则的步骤时，可以将相关的第一配置信息发送给配置组

件，由配置组件根据上述第一配置信息，在供应商网络中创建供应商网络与蜜罐服务之间的弹性网卡，以及基于弹性网卡配置供应商网络与蜜罐服务之间的网络地址转换规则；上述第一配置信息可以包括供应商网络与蜜罐服务之间的网络地址转换规则等。

在一种可能的实现方式中，在流量牵引模式为LB模式的情况下，创建供应商网络与蜜罐服务之间的弹性网卡，包括：

在供应商网络的虚拟私有云中创建代理主机；

基于代理主机创建目的地址转换DNAT规则，DNAT规则用于将代理主机的流量转发至蜜罐服务；

在蜜罐服务所在的虚拟私有云中申请弹性网卡；

将弹性网卡绑定至代理主机。

其中，上述在供应商网络的虚拟私有云中创建代理主机、基于代理主机创建目的地址转换DNAT规则、以及将弹性网卡绑定至代理主机的过程可以通过安装在供应商网络的控制终端/配置终端中的配置组件执行；比如，云端服务器流量牵引模式为LB模式的情况下，可以将相关的第二配置信息发送给配置组件，由配置组件根据上述第二配置信息，在供应商网络的虚拟私有云中创建代理主机、基于代理主机创建目的地址转换DNAT规则、以及将弹性网卡绑定至代理主机；上述第二配置信息可以包括上述DNAT规则、弹性网卡的标识信息（比如弹性网卡的虚拟地址）等。

在一种可能的实现方式中云端服务器还可以为弹性网卡绑定安全组规则，该安全组规则用于禁止被牵引到蜜罐服务中的访问流量主动访问供应商网络。

其中，在上述弹性网卡配置在供应商网络中的情况下，上述为弹性网卡绑定安全组规则的过程也可以通过安装在供应商网络的控制终端/配置终端中的配置组件执行；比如，云端服务器可以将相关的第三配置信息发送给配置组件，由配置组件根据上述第三配置信息，为弹性网卡绑定安全组规则；上述第三配置信息可以包括上述安全组规则等信息。

在本申请实施例中，针对攻击方攻破蜜罐，进一步逃逸之后，就能以蜜罐为跳板，扩大入侵范围的问题，云端服务器可以通过为弹性网卡绑定安全组规则，使得蜜罐服务和租户的生产环境只能单向流通，避免了攻击方的恶意访问流量横向移动到租户的其他资产的情况，从而提高安全性。

请参考图7，其示出了本申请实施例涉及的探针服务的建立框架示意图。如图7所示，以EIP模式为例，基于非侵入式流量牵引类型的探针服务的建立过程可以如下：

S1，在租户的网络里面创建一个VPC，固定CIDR网段（如192.168.1.0/24）。

S2，在租户的VPC里面插入一张跨租户弹性网卡（比如eni-4rihkbgn），绑定到蜜罐母机的RS。

S3，在租户的VPC申请HAVIP（比如192.168.1.4），然后刷到网卡eni-4rihkbgn。

S4，绑定租户的EIP和HAVIP，实现了租户的EIP和网卡直连，即111.230.202.86和192.168.1.4进行了绑定，因此打通了租户网络和蜜场网络。

在图7中，虚线左边为租户网络，右边为蜜场网络，两者网络隔离。

S5，在HAVIP上虚拟不同的蜜罐服务，比如设置192.168.1.4:2222转发到SSH蜜罐。

— 13 —

S6, 此时数据单向路由已经配置好, 在添加一条回程路由, 即可实现网络联通。

比如, 新增路由表: ip route add default via 192.168.1.4 dev eth1 table 100;

新增源路由策略: ip rule add from 192.168.1.4 table 100。

5 S7, 当用户 (139.196.1.85) 访问探针EIP (111.230.202.86) 2222端口, 就相当于访问了SSH蜜罐服务。

S8, 最后为ETH1网卡绑定安全组规则, 禁止蜜场的流量主动访问租户的网络。

内网IP模式的非侵入式流量牵引类型的探针服务建立的原理与EIP模式的非侵入式流量牵引类型的探针服务建立的原理类似, 此处不再赘述。

10 LB模式引流, 可以基于租户当前的域名的不同的统一资源标识符 (Uniform Resource Identifier, URI) 转发到不同的蜜罐, 能较好的隐藏在真实业务中。请参考图8, 其示出了本申请实施例涉及的探针服务的建立框架示意图。如图8所示, 以 LB模式为例, 基于非侵入式流量牵引类型的探针服务的建立过程可以如下:

S1, 反向插网卡 (即蜜场的网卡绑定到租户的机器), 过程如下:

15 A) 在租户的CLB的VPC建立一台机器, 称为Proxy (10.10.1.7);
B) 在蜜场里面创建蜜罐母机RS (192.168.100.4), 并创建对应的蜜罐服务;
C) 创建DNAT规则, 使192.168.100.4IP的流量转发到蜜罐服务;
D) 在蜜罐引擎RS的VPC申请一张跨租户弹性网卡EHT1 (192.168.100.3), 并绑定到租户的Proxy机器。

S2, 此刻租户的网络和蜜场网络已经通过ETH1实现逻辑互通。

20 其中, 若是将需要域名的80端口的访问流量转发到蜜场, 需要在租户的PROXY机器上配置DNAT转发策略, 即: 10.10.1.7:80 ->192.168.100.4:801; 此刻域名的80端口流量即可以通过ETH1, 转发到了蜜罐服务中。

S3, 最后为ETH1网卡绑定安全组规则, 禁止蜜场的流量主动访问租户的网络。

25 综上所述, 本申请实施例所示的方案, 云端服务器通过建立非侵入式流量牵引的探针服务, 将访问目标网络内容的访问流量全量牵引到蜜罐服务, 避免对网络内容供应商的服务业务产生影响。

此外, 本申请实施例所示的方案, 还支持禁止蜜场的流量主动访问租户的网络, 提高了蜜罐系统的安全性。

30 基于本申请上述实施例所示的方案, 租户无需关心具体的网络拓扑, 无需配置复杂的网络策略, 只需要按需选择部署方式以及指定好蜜罐部署位置, 就能一键解决部署问题, 将指定流量牵引到蜜罐系统种。其中, 侵入式部署能最大程度上防护业务, 探测已知的恶意攻击, 适合安全性要求较高的业务; 非侵入式部署提供了常见的业务部署方式, 使得真实业务和蜜罐业务难以区分。同时蜜网和租户的生产环境只能单向流通, 避免了攻击方的恶意流量横向移动到租户的其他资产。

35 基于上述图2、图4或图6所示的方案, 请参考图9, 其示出了本申请提供的一种蜜罐创建和流量牵引流程图。如图9所示, 该蜜罐创建和流量牵引过程如下:

S1, 租户在WEB控制台选择创建探针类型以及蜜罐服务, 支持创建探针类型为: 侵入

式动态流量牵引和非侵入式全量流量牵引。

S2, 云端将创建配置信息保存在数据库(比如MYSQL数据库), 后台服务(HONEYPOT管理服务)从MYSQL读取当前用户所有规则, 创建租户选择的探针类型, 进行流量牵引。

S3, 将租户选择的蜜罐类型下发到蜜场, 创建指定类型的蜜罐服务。

5 S4, 建立探针服务。

其中, 侵入式动态流量牵引创建流程可以包括:

A) 下发租户当前的恶意流量识别特征, 命中特征的流量会被转发到蜜罐;

B) 下发租户转发蜜罐地址。

非侵入式全量流量迁移创建流程可以包括:

10 A) 弹性网卡和蜜场种的蜜罐均已创建之后, 配置对应的DNAT和SNAT规则, 使得探针IP和端口的流量能够转发到对应蜜罐服务;

B) 给跨租户网卡配置安全组策略, 阻止蜜场的流量主动访问探针侧的网络, 保证蜜罐即使被攻破, 租户的生产环境也不会受到影响。

15 S5, 如果探针或者蜜场任意一个创建失败, 则上抛消息给HONEYPOT后台服务进行重试处理; 如果重试依旧失败, 则将具体的错误回显给控制台展示。

S6, 如果服务都创建成功, 侵入部署模式下, 当用户访问用户正常业务, 此刻返回正常页面, 如果用户访问正常业务带了攻击特征, 则该流量会被重定向到用户的蜜罐集群中。非侵入模式下, 当用户访问或者扫描到了用户暴露的蜜罐探针, 此时跨租户弹性网卡, 会将流量从租户的网络转到蜜场种, 然后根据对应的IP和端口映射到不同的蜜罐服务。

20 S7, 用户的访问流量进入到了蜜罐服务之后, 可能会做一系列的动作, 比如横向移动扫描、爆破、拉取虚拟资源采集样本等, 蜜罐服务实时记录这些动作, 然后上报到租户控制台并呈现给租户。

本申请公开了一种基于云租户动态引流的蜜罐集群实现方案, 包括: 侵入式动态流量牵引蜜罐方案和非侵入式全量流量牵引蜜罐方案。

25 其中侵入式动态流量牵引蜜罐方案是指: 蜜罐业务完全侵入到正常业务中, 当感知系统检测到业务流量中有恶意攻击, 就会动态生成转发规则, 将恶意会话转发给蜜罐集群, 保护云上资产。而当感知系统检测到正常流量, 则会放行当前会话, 原路转发给客户真实业务; 非侵入性全量流量牵引蜜罐方案是指: 蜜罐业务和正常业务剥离开, 蜜罐业务单独部署, 结合客户自己的业务模型, 通过公网IP、指定域名URI(负载均衡)、内网IP等多种类型探针, 对请求的流量进行全量牵引到预先布置好的蜜罐集群。

30 侵入式动态引流是检测到攻击之后可以返回302给用户, 从而使攻击方跳转访问蜜罐; 非侵入式全量引流会通过跨租户弹性网卡和路由策略转发到蜜网集群, 不同的端口流量转发到不同的类型的蜜罐; 恶意流量实际上是和蜜罐进行交互, 以套取攻击方各类攻击手法和延缓攻击速度, 争取更多的时间给防守者。最后将全部流量日志和主机行为日志捕获到, 35 生成对应的失陷告警, 将告警日志展示在用户防火墙控制台, 以提醒用户云上蜜罐受到过攻击, 从而提醒用户, 当前攻击的源IP尝试用某种手段攻击用户资产。更进一步, 可以结合其他安全产品: 防火墙、网页应用防火墙、安全运营中心、主机等采取封禁源IP等措施,

限制该IP进一步扩大攻击范围，从而保护云上核心资产免受攻击。

本申请提供的基于云租户动态引流方案，有别于传统蜜罐部署模式，用户只需要选择部署模式，然后一键操作，后台即可完成所有资源分配和策略配置，用户无需关注底层复杂的网络拓扑和配置策略。

- 5 传统蜜罐在蜜场和租户的生产环境隔离方面没有很好的通用解决方案，只能通过大量缓解措施来保证安全性，复杂度较高，而本申请提供的蜜罐通过合理的网络划分，以及对连接租户和蜜场的弹性网卡绑定安全组的方式，保证网络访问只能是探针到蜜场单向访问，不能由蜜场返回到租户的生产环境，保证了租户的网络隔离安全。在部署方式上面，提供了侵入式部署和非侵入式部署，分别满足不同业务场景的需求。侵入式部署能够满足对安全性要求较高的业务，不允许有已知攻击流量走向业务后台服务，同时提供了用户自定义特征转发，极大丰富了转发规则的自由度。也避免了后台服务各类补丁升级等一些列维护动作，减轻运维压力。非侵入式部署提供丰富的暴露形式，从云上资产常见暴露方式出发，支持EIP和CLB等方式，保证了蜜罐的暴露形式不脱离真实业务，提高蜜罐的伪装度，起到很好的伪装效果。同时支持内网探针，能第一时间感知用户失陷后，攻击方的恶意流量发起的横向移动行为，攻击告警推送给用户，使得租户能及时处理攻击行为，减少资产损失。
- 10 15

图10示出了本申请一示例性实施例示出的安全服务处理装置的方框图，该装置可以用于执行如图2、图4或图6所示方法中的全部或部分步骤；如图10所示，该装置包括：

- 请求接收模块1001，用于接收网络内容供应商发送的蜜罐服务部署请求；所述蜜罐服务部署请求用于指示探针服务类型以及蜜罐服务类型；所述探针服务类型用于指示流量牵引方式；
- 20

蜜罐服务建立模块1002，用于基于所述蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务；所述目标网络内容是所述网络内容供应商提供的网络内容；

探针服务建立模块1003，用于基建立所述探针服务类型的探针服务；所述探针服务用于将所述目标网络内容的访问流量牵引至所述蜜罐服务。

- 25 在一种可能的实现方式中，所述探针服务类型包括侵入式流量牵引类型或者非侵入式流量牵引类型。

在一种可能的实现方式中，响应于所述探针服务类型包括侵入式流量牵引类型，所述探针服务建立模块1003，用于，

在云端创建所述探针服务的规则引擎和牵引引擎；

- 30 其中，所述规则引擎用于识别对所述目标网络内容的访问流量是否为指定类型访问流量；

所述牵引引擎用于基于规则引擎的识别结果，将所述指定类型访问流量牵引至所述蜜罐服务。

在一种可能的实现方式中，所述装置还包括：

- 35 规则接收模块，用于接收所述第一设备发送的流量识别规则；所述流量识别规则用于指示所述指定类型访问流量的判别条件；

规则下发模块，用于将所述流量识别规则下发至所述规则引擎。

在一种可能的实现方式中，响应于所述探针服务类型包括非侵入式流量牵引类型，所述探针服务建立模块1003，用于，

创建供应商网络与所述蜜罐服务之间的弹性网卡；所述供应商网络是提供所述目标网络内容的网络；

5 基于所述弹性网卡配置所述供应商网络与所述蜜罐服务之间的网络地址转换规则；所述网络地址转换规则用于指示所述弹性网卡将对所述目标网络内容的访问流量转发至所述蜜罐服务。

在一种可能的实现方式中，所述探针服务建立模块1003，用于，

在所述供应商网络中创建虚拟私有云；

10 在所述虚拟私有云中插入所述弹性网卡，所述弹性网卡与所述蜜罐服务绑定；

在所述虚拟私有云中申请所述弹性网卡的虚拟地址；

将所述弹性网卡的虚拟地址与所述供应商网络的公网地址或者内网地址进行绑定。

在一种可能的实现方式中，所述探针服务建立模块1003，用于，

15 在所述供应商网络的虚拟私有云中创建代理主机，所述虚拟私有云对应于所述蜜罐服务；

基于所述代理主机创建目的地址转换DNAT规则，所述DNAT规则用于将所述代理主机的流量转发至所述蜜罐服务；

在所述虚拟私有云中申请所述弹性网卡；

将所述弹性网卡绑定至所述代理主机。

20 在一种可能的实现方式中，所述探针服务建立模块1003，还用于为所述弹性网卡绑定安全组规则，所述安全组规则用于禁止被牵引到所述蜜罐服务中的访问流量主动访问所述供应商网络。

在一种可能的实现方式中，所述装置还包括：

获取模块，用于获取所述蜜罐服务或者所述探针服务的建立结果以及建立次数；

25 重建模块，用于响应于所述建立结果为建立失败，且所述建立次数未达到次数阈值，对建立失败的所述蜜罐服务或者所述探针服务进行重新建立。

在一种可能的实现方式中，所述装置还包括：

信息返回模块，用于响应于所述建立结果为建立失败，且所述建立次数达到所述次数阈值，向所述云端服务器的控制台返回所述蜜罐服务或者所述探针服务建立失败的信息。

30 在一种可能的实现方式中，所述装置还包括：

记录模块，用于记录所述蜜罐服务中的访问流量的行为记录；

发送模块，用于向所述网络内容供应商返回所述行为记录。

图11示出了本申请一示例性实施例示出的计算机设备1100的结构框图。该计算机设备可以实现为本申请上述方案中的云端服务器。该计算机设备1100包括中央处理单元（Central Processing Unit, CPU）1101、包括随机存取存储器（Random Access Memory, RAM）1102和只读存储器（Read-Only Memory, ROM）1103的系统存储器1104，以及连接系统存储器1104和中央处理单元1101的系统总线1105。该计算机设备1100还包括用于存储操作系统

35

1109、应用程序1110和其他程序模块1111的大容量存储设备1106。

该大容量存储设备1106通过连接到系统总线1105的大容量存储控制器（未示出）连接到中央处理单元1101。该大容量存储设备1106及其相关联的计算机可读介质为计算机设备1100提供非易失性存储。也就是说，该大容量存储设备1106可以包括诸如硬盘或者只读光盘（Compact Disc Read-Only Memory, CD-ROM）驱动器之类的计算机可读介质（未示出）。

不失一般性，该计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其他数据等信息的任何方法或技术实现的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括RAM、ROM、可擦除可编程只读存储器（Erasable Programmable Read Only Memory, EPROM）、电子抹除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory, EEPROM）闪存或其他固态存储其技术，CD-ROM、数字多功能光盘（Digital Versatile Disc, DVD）或其他光学存储、磁带盒、磁带、磁盘存储或其他磁性存储设备。当然，本领域技术人员可知该计算机存储介质不局限于上述几种。上述的系统存储器1104和大容量存储设备1106可以统称为存储器。

根据本公开的各种实施例，该计算机设备1100还可以通过诸如因特网等网络连接到网络上的远程计算机运行。也即计算机设备1100可以通过连接在该系统总线1105上的网络接口单元1107连接到网络1108，或者说，也可以使用网络接口单元1107来连接到其他类型的网络或远程计算机系统（未示出）。

该存储器还包括至少一条计算机程序，该至少一条计算机程序存储于存储器中，中央处理器1101通过执行该至少一条计算机程序来实现上述各个实施例所示的方法中的全部或部分步骤。

在一示例性实施例中，还提供了一种计算机可读存储介质，用于存储有至少一条计算机程序，该至少一条计算机程序由处理器加载并执行以实现上述各个实施例所示的方法中的全部或部分步骤。例如，该计算机可读存储介质可以是只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、只读光盘（Compact Disc Read-Only Memory, CD-ROM）、磁带、软盘和光数据存储设备等。

在一示例性实施例中，本申请实施例还提供了一种包括计算机程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述实施例提供的方法。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。

权 利 要 求

- 1.一种安全服务处理方法，所述方法由云端服务器执行，所述方法包括：
接收网络内容供应商发送的蜜罐服务部署请求，所述蜜罐服务部署请求用于指示探针
服务类型以及蜜罐服务类型，所述探针服务类型用于指示流量牵引方式；
5 基于所述蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务，所述目标网络内
容是所述网络内容供应商提供的网络内容；
 建立所述探针服务类型的探针服务，所述探针服务用于将对所述目标网络内容的访问
流量牵引至所述蜜罐服务。
- 2.根据权利要求1所述的方法，所述探针服务类型包括侵入式流量牵引类型或者非侵入
10 式流量牵引类型。
- 3.根据权利要求2所述的方法，响应于所述探针服务类型包括侵入式流量牵引类型，所
述建立所述探针服务类型的探针服务，包括：
 在云端创建所述探针服务的规则引擎和牵引引擎；
 其中，所述规则引擎用于识别对所述目标网络内容的访问流量是否为指定类型访问流
15 量；
 所述牵引引擎用于基于规则引擎的识别结果，将所述指定类型访问流量牵引至所述蜜
罐服务。
- 4.根据权利要求3所述的方法，所述方法还包括：
 接收所述第一设备发送的流量识别规则，所述流量识别规则用于指示所述指定类型访
20 问流量的判别条件；
 将所述流量识别规则下发至所述规则引擎。
- 5.根据权利要求2所述的方法，响应于所述探针服务类型包括非侵入式流量牵引类型，
所述建立所述探针服务类型的探针服务，包括：
 创建供应商网络与所述蜜罐服务之间的弹性网卡，所述供应商网络是提供所述目标网
25 络内容的网络；
 基于所述弹性网卡配置所述供应商网络与所述蜜罐服务之间的网络地址转换规则，所
述网络地址转换规则用于指示所述弹性网卡将对所述目标网络内容的访问流量转发至所述
蜜罐服务。
- 6.根据权利要求5所述的方法，所述创建供应商网络与所述蜜罐服务之间的弹性网卡，
30 包括：
 在所述供应商网络中创建虚拟私有云；
 在所述虚拟私有云中插入所述弹性网卡，所述弹性网卡与所述蜜罐服务绑定；
 在所述虚拟私有云中申请所述弹性网卡的虚拟地址；
 将所述弹性网卡的虚拟地址与所述供应商网络的公网地址或者内网地址进行绑定。
- 7.根据权利要求5所述的方法，所述创建供应商网络与所述蜜罐服务之间的弹性网卡，
35 包括：
 在所述供应商网络的虚拟私有云中创建代理主机，所述虚拟私有云对应于所述蜜罐服

务;

基于所述代理主机创建目的地址转换DNAT规则,所述DNAT规则用于将所述代理主机的流量转发至所述蜜罐服务;

在所述虚拟私有云中申请所述弹性网卡;

5 将所述弹性网卡绑定至所述代理主机。

8.根据权利要求5至7任一所述的方法,所述方法还包括:

为所述弹性网卡绑定安全组规则,所述安全组规则用于禁止被牵引到所述蜜罐服务中的访问流量主动访问所述供应商网络。

9.根据权利要求1所述的方法,所述方法还包括:

10 获取所述蜜罐服务或者所述探针服务的建立结果以及建立次数;

响应于所述建立结果为建立失败,且所述建立次数未达到次数阈值,对建立失败的所述蜜罐服务或者所述探针服务进行重新建立。

10.根据权利要求9所述的方法,所述方法还包括:

15 响应于所述建立结果为建立失败,且所述建立次数达到所述次数阈值,向所述云端服务器的控制台返回所述蜜罐服务或者所述探针服务建立失败的信息。

11.根据权利要求1所述的方法,所述方法还包括:

记录所述蜜罐服务中的访问流量的行为记录;

向所述网络内容供应商返回所述行为记录。

12.一种安全服务处理装置,所述装置包括:

20 请求接收模块,用于接收网络内容供应商的第一设备发送的蜜罐服务部署请求;所述蜜罐服务部署请求用于指示探针服务类型以及蜜罐服务类型;所述探针服务类型用于指示流量牵引方式;

蜜罐服务建立模块,用于基于所述蜜罐服务类型在云端建立与目标网络内容对应的蜜罐服务;所述目标网络内容是所述网络内容供应商提供的网络内容;

25 探针服务建立模块,用于基于所述探针服务类型建立所述网络内容供应商的探针服务;所述探针服务用于将对所述目标网络内容的访问流量牵引至所述蜜罐服务。

13.一种计算机设备,所述计算机设备包括处理器和存储器,所述存储器存储有至少一条计算机程序,所述至少一条计算机程序由所述处理器加载并执行以实现如权利要求1至11任一所述的安全服务处理方法。

30 14.一种计算机可读存储介质,所述计算机可读存储介质中存储有至少一条计算机程序,所述计算机程序由处理器加载并执行以实现如权利要求1至11任一所述的安全服务处理方法。

35 15.一种包括计算机程序的计算机程序产品,当其在计算机上运行时,使得所述计算机执行权利要求1至11任一所述的安全服务处理方法。