(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111970301 B
(45)授权公告日 2022.11.04

(21)申请号 202010878587.1
(22)申请日 2020.08.27
(65)同一申请的已公布的文献号
申请公布号 CN 111970301 A
(43)申请公布日 2020.11.20
(73)专利权人 北京浪潮数据技术有限公司
地址 100085 北京市海淀区上地信息路2号C栋5层
(72)发明人 赵宝琦
(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 刘新雷
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)

审查员 魏慧慧

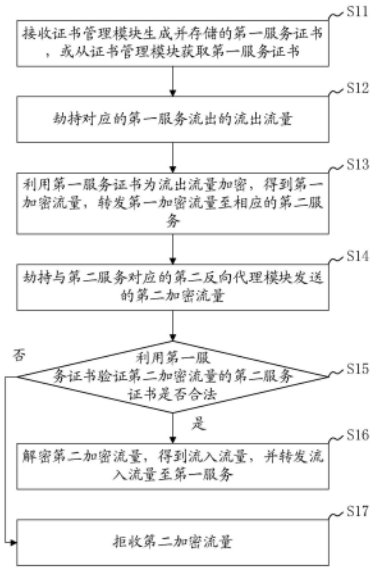
权利要求书3页 说明书7页 附图4页

(54)发明名称

一种容器云平台安全通信系统

(57)摘要

本申请公开了一种容器云平台安全通信系统，包括：证书管理模块，用于生成并存储第一服务证书，下发第一服务证书至第一反向代理模块；第一反向代理模块，包括证书获取子模块、流量加密子模块、流量验证子模块、解密子模块和拒收子模块；本申请容器云平台中每个服务都对应的设置有反向代理模块，通过证书管理模块管理每个反向代理模块的服务证书，每个反向代理模块劫持任何需要出入服务的流量，并进行相应的加密和验证，确保流入流量和流出流量在通信期间的安全性，并且实现了统一的安全管理，且对服务本身的运行过程无影响，实现了无感知的安全控制。



CN 111970301 B

1.一种容器云平台安全通信方法,其特征在于,应用于与第一服务对应的第一反向代理模块,包括:

接收证书管理模块生成并存储的第一服务证书,或从所述证书管理模块获取所述第一服务证书;

劫持对应的所述第一服务流出的流出流量;

利用所述第一服务证书为所述流出流量加密,得到第一加密流量,转发所述第一加密流量至相应的第二服务;

劫持与所述第二服务对应的第二反向代理模块发送的第二加密流量;

利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法,其中,所述第一服务对应的第一反向代理模块所使用的服务证书,与所述第二服务对应的第二反向代理模块所使用的服务证书相同;其中,所述第一服务证书与所述第二服务证书均为所述证书管理模块根据根证书生成;若所述第一服务对应的第一反向代理模块与所述第二服务对应的第二反向代理模块证书更新时间不相同,则所述第一服务证书与所述第二服务证书版本不同,所述利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法,包括:利用所述第一服务证书验证版本不同的所述第二服务证书是否合法;

若所述第二加密流量的所述第二服务证书合法,则解密所述第二加密流量,得到流入流量,并转发所述流入流量至所述第一服务;

若所述第二加密流量的所述第二服务证书不合法,则拒收所述第二加密流量。

2.根据权利要求1所述的容器云平台安全通信方法,其特征在于,还包括:

从安全认证模块获取认证名单;

根据所述认证名单判断所述第二加密流量对应的所述第二服务是否满足要求,若满足则利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法,若不满足,则拒收所述第二加密流量。

3.根据权利要求1所述的容器云平台安全通信方法,其特征在于,所述从所述证书管理模块获取所述第一服务证书的过程,包括:

定时从所述证书管理模块获取最新的所述第一服务证书。

4.根据权利要求2所述的容器云平台安全通信方法,其特征在于,所述从所述安全认证模块获取认证名单的过程,包括:

定时从所述安全认证模块获取最新的所述认证名单。

5.根据权利要求2所述的容器云平台安全通信方法,其特征在于,所述拒收所述第二加密流量之后,还包括:

发送拒收信息至所述第二反向代理模块。

6.根据权利要求1至5任一项所述的容器云平台安全通信方法,其特征在于,所述利用所述第一服务证书为所述流出流量加密,得到第一加密流量,转发所述第一加密流量至相应的第二服务的过程,包括:

利用所述第一服务证书为所述流出流量进行TLS加密,得到所述第一加密流量,转发所述第一加密流量至相应的第二服务;

所述若所述第二加密流量的所述第二服务证书合法,则解密所述第二加密流量,得到流入流量,并转发所述流入流量至所述第一服务的过程,包括:

若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则对所述第二加密流量进行TLS解密，得到所述流入流量，并转发所述流入流量至所述第一服务。

7.一种第一反向代理模块，其特征在于，包括：证书获取子模块、流出流量劫持子模块、流量加密子模块、流入流量劫持子模块、流量验证子模块、解密子模块和拒收子模块；

所述证书获取子模块，用于接收证书管理模块下发的第一服务证书，或从所述证书管理模块获取所述第一服务证书；

所述流出流量劫持子模块，用于劫持对应的第一服务流出的流出流量；

所述流量加密子模块，用于利用所述第一服务证书为所述流出流量加密，得到第一加密流量，转发所述第一加密流量至相应的第二服务；

所述流入流量劫持子模块，用于劫持所述第二反向代理模块发送第二加密流量；

所述流量验证子模块，用于利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法，其中，所述第一服务对应的第一反向代理模块所使用的服务证书，与所述第二服务对应的第二反向代理模块所使用的服务证书相同；

所述解密子模块，用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则解密所述第二加密流量，得到流入流量，并转发所述流入流量至所述第一服务；

所述拒收子模块，用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书不合法，则拒收所述第二加密流量；

其中，所述第一服务证书与所述第二服务证书均为所述证书管理模块根据根证书生成；若所述第一服务对应的第一反向代理模块与所述第二服务对应的第二反向代理模块证书更新时间不相同，则所述第一服务证书与所述第二服务证书版本不同；所述流量验证子模块，具体用于：利用所述第一服务证书验证版本不同的所述第二服务证书是否合法。

8.根据权利要求7所述的第一反向代理模块，其特征在于，还包括名单获取子模块和名单验证子模块；

所述名单获取子模块，用于从安全认证模块获取认证名单；

所述名单验证子模块，用于根据所述认证名单判断所述第二加密流量对应的所述第二服务是否满足要求，若满足则调用所述流量验证子模块，若不满足，则调用所述拒收子模块；

所述拒收子模块，还用于若所述名单验证子模块判定所述第二加密流量对应的所述第二服务不满足要求，则拒收所述第二加密流量。

9.根据权利要求7或8所述的第一反向代理模块，其特征在于，所述流量加密子模块，具体用于利用所述第一服务证书为所述流出流量进行TLS加密，得到所述第一加密流量，转发所述第一加密流量至相应的第二服务；

所述解密子模块，具体用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则对所述第二加密流量进行TLS解密，得到所述流入流量，并转发所述流入流量至所述第一服务。

10.一种容器云平台安全通信系统，其特征在于，包括：证书管理模块、安全认证模块、第一服务、如权利要求7所述的与所述第一服务对应的第一反向代理模块、第二服务和与所述第二服务对应的第二反向代理模块；

所述证书管理模块，用于生成并存储第一服务证书，下发所述第一服务证书至所述第一反向代理模块；

所述安全认证模块，用于存储认证名单；

所述证书管理模块，具体用于根据根证书生成所述第一服务证书与第二服务证书。

一种容器云平台安全通信系统

技术领域

[0001] 本发明涉及通信安全领域，特别涉及一种容器云平台安全通信系统。

背景技术

[0002] 在当前国产化容器云平台中，存在大量需要相互通信的服务，这些服务相互调用从而形成一种服务网络。

[0003] 但由于国产化容器生态环境限制，大部分服务均由第三方厂商提供，不同厂商的服务所应用的安全策略不尽相同，更有甚者完全未考虑安全因素。

[0004] 因此，需要一种统一有效的容器云平台安全通信系统，确保容器云平台内的通信安全。

发明内容

[0005] 有鉴于此，本发明的目的在于提供一种容器云平台安全通信系统，提高容器云平台内的通信安全。其具体方案如下：

[0006] 一种容器云平台安全通信方法，应用于与第一服务对应的第一反向代理模块，包括：

[0007] 接收证书管理模块生成并存储的第一服务证书，或从所述证书管理模块获取所述第一服务证书；

[0008] 劫持对应的所述第一服务流出的流出流量；

[0009] 利用所述第一服务证书为所述流出流量加密，得到第一加密流量，转发所述第一加密流量至相应的第二服务；

[0010] 劫持与所述第二服务对应的第二反向代理模块发送的第二加密流量；

[0011] 利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法；

[0012] 若所述第二加密流量的所述第二服务证书合法，则解密所述第二加密流量，得到流入流量，并转发所述流入流量至所述第一服务；

[0013] 若所述第二加密流量的所述第二服务证书不合法，则拒收所述第二加密流量。

[0014] 可选的，还包括：

[0015] 从安全认证模块获取认证名单；

[0016] 根据所述认证名单判断所述第二加密流量对应的所述第二服务是否满足要求，若满足则利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法，若不满足，则拒收所述第二加密流量。

[0017] 可选的，所述从所述证书管理模块获取所述第一服务证书的过程，包括：

[0018] 定时从所述证书管理模块获取最新的所述第一服务证书。

[0019] 可选的，所述从所述安全认证模块获取认证名单的过程，包括：

[0020] 定时从所述安全认证模块获取最新的所述认证名单。

[0021] 可选的，所述拒收所述第二加密流量之后，还包括：

[0022] 发送拒收信息至所述第二反向代理模块。

[0023] 可选的，所述利用所述第一服务证书为所述流出流量加密，得到第一加密流量，转发所述第一加密流量至相应的第二服务的过程，包括：

[0024] 利用所述第一服务证书为所述流出流量进行TLS加密，得到所述第一加密流量，转发所述第一加密流量至相应的第二服务；

[0025] 所述若所述第二加密流量的所述第二服务证书合法，则解密所述第二加密流量，得到流入流量，并转发所述流入流量至所述第一服务的过程，包括：

[0026] 若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则对所述第二加密流量进行TLS解密，得到所述流入流量，并转发所述流入流量至所述第一服务。

[0027] 本发明还公开了一种第一反向代理模块，包括：证书获取子模块、流出流量劫持子模块、流量加密子模块、流入流量劫持子模块、流量验证子模块、解密子模块和拒收子模块；

[0028] 所述证书获取子模块，用于接收证书管理模块下发的所述第一服务证书，或从所述证书管理模块获取所述第一服务证书；

[0029] 所述流出流量劫持子模块，用于劫持对应的第一服务流出的流出流量；

[0030] 所述流量加密子模块，用于利用所述第一服务证书为所述流出流量加密，得到第一加密流量，转发所述第一加密流量至相应的第二服务；

[0031] 所述流入流量劫持子模块，用于劫持所述第二反向代理模块发送第二加密流量；

[0032] 所述流量验证子模块，用于利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法；

[0033] 所述解密子模块，用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则解密所述第二加密流量，得到流入流量，并转发所述流入流量至所述第一服务；

[0034] 所述拒收子模块，用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书不合法，则拒收所述第二加密流量。

[0035] 可选的，还包括名单获取子模块和名单验证子模块；

[0036] 所述名单获取子模块，用于从安全认证模块获取认证名单；

[0037] 所述名单验证子模块，用于根据所述认证名单判断所述第二加密流量对应的所述第二服务是否满足要求，若满足则调用所述流量验证子模块，若不满足，则调用所述拒收子模块；

[0038] 所述拒收子模块，还用于若所述名单验证子模块判定所述第二加密流量对应的所述第二服务不满足要求，则拒收所述第二加密流量。

[0039] 可选的，所述流量加密子模块，具体用于利用所述第一服务证书为所述流出流量进行TLS加密，得到所述第一加密流量，转发所述第一加密流量至相应的第二服务；

[0040] 所述解密子模块，具体用于若所述流量验证子模块判定所述第二加密流量的所述第二服务证书合法，则对所述第二加密流量进行TLS解密，得到所述流入流量，并转发所述流入流量至所述第一服务。

[0041] 本发明还公开了一种容器云平台安全通信系统，包括：证书管理模块、安全认证模块、第一服务、如前述的包括与所述第一服务对应的第一反向代理模块、第二服务和与所述第二服务对应的第二反向代理模块；

[0042] 所述证书管理模块，用于生成并存储第一服务证书，下发所述第一服务证书至所述第一反向代理模块；

[0043] 所述安全认证模块，用于存储认证名单。

[0044] 本发明中，容器云平台安全通信方法，应用于与第一服务对应的第一反向代理模块，包括：接收所述证书管理模块生成并存储的第一服务证书，或从所述证书管理模块获取所述第一服务证书；劫持对应的所述第一服务流出的流出流量；利用所述第一服务证书为所述流出流量加密，得到第一加密流量，转发所述第一加密流量至相应的第二服务；劫持与所述第二服务对应的第二反向代理模块发送的第二加密流量；利用所述第一服务证书验证所述第二加密流量的第二服务证书是否合法；若所述第二加密流量的所述第二服务证书合法，则解密所述第二加密流量，得到流入流量，并转发所述流入流量至所述第一服务；若所述第二加密流量的所述第二服务证书不合法，则拒收所述第二加密流量。

[0045] 本发明容器云平台中每个服务都对应的设置有反向代理模块，通过证书管理模块管理每个反向代理模块的服务证书，每个反向代理模块劫持任何需要出入服务的流量，并进行相应的加密和验证，确保流入流量和流出流量在通信期间的安全性，并且实现了统一的安全管理，且对服务本身的运行过程无影响，实现了无感知的安全控制。

附图说明

[0046] 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。

[0047] 图1为本发明实施例公开的一种容器云平台安全通信方法流程示意图；

[0048] 图2为本发明实施例公开的另一种容器云平台安全通信方法流程示意图；

[0049] 图3为本发明实施例公开的一种第一反向代理模块结构示意图；

[0050] 图4为本发明实施例公开的一种容器云平台安全通信系统结构示意图。

具体实施方式

[0051] 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。

[0052] 本发明实施例公开了一种容器云平台安全通信方法，参见图1所示，应用于与第一服务对应的第一反向代理模块，该方法包括：

[0053] S11：接收证书管理模块生成并存储的第一服务证书，或从证书管理模块获取第一服务证书。

[0054] 具体的，证书管理模块中存储每个反向代理模块用于加密和验证的服务证书，每个反向代理模块所使用的服务证书相同，即如果每个反向代理模块中的服务证书未被修改或未异步更新，则所有反向代理模块中的服务证书均一样，例如，第一服务证书与第二服务证书一致为同一证书，因此，第一服务证书能够验证第二服务证书。

[0055] 具体的，证书管理模块可以定期下发服务证书至每个反向代理模块，从而确保每个反向代理模块中的服务证书的正确，避免过期，因此，可以接收证书管理模块下发其生成并存储的第一服务证书。当然，第一反向代理模块13也可以主动从证书管理模块中获取第一服务证书。

[0056] S12：劫持对应的第一服务流出的流出流量；

[0057] S13：利用第一服务证书为流出流量加密，得到第一加密流量，转发第一加密流量至相应的第二服务。

[0058] 具体的，第一反向代理模块获取第一服务证书后便可以利用第一服务证书对第一服务发送给第二服务的流出流量进行加密，第一反向代理模块，以劫持的方式截获第一服务发送给第二服务的流出流量，即第一服务在发送流出流量时，是以第二服务为目的地进行发送，但实际上会被第一反向代理模块首先截获到，由第一反向代理模块对流出流量进行加密后，再将加密流量按照流出流量原先对应的目的地，转发至第二服务，从而实现无感知的数据加密。

[0059] S14：劫持与第二服务对应的第二反向代理模块发送的第二加密流量；

[0060] S15：利用第一服务证书验证第二加密流量的第二服务证书是否合法。

[0061] 具体的，第一反向代理模块同时还会劫持第二反向代理模块向第一服务发送的第二加密流量，第一反向代理模块利用第一服务证书验证利用第二服务证书的合法性。在第二服务证书未被修改，第一反向代理模块与第二反向代理模块服务证书更新时间相同的情况下，第一服务证书与第二服务证书相同均为证书管理模块中生成并存储的服务证书，因此，可以利用第一服务证书对第二服务证书进行合法性验证，如果第二反向代理模块中的第二服务证书被篡改，第一反向代理模块无法利用第一服务证书验证第二服务证书，因此，会拒收第二加密流量，只有在验证通过的前提下，才会对第二加密流量进行解密，得到流入流量，并第一反向代理模块将流入流量发送至第一服务。

[0062] 需要说明的是，每个反向代理模块的证书更新时间不完全相同，因此，第一服务证书与第二服务证书因反向代理模块没能及时更新服务证书，导致服务证书版本可能会不一样，但即使服务证书版本不一样，第一服务证书仍能够对版本不一样的第二服务证书进行有效的合法性验证，因为，第一服务证书与第二服务证书均为证书管理模块根据根证书生成的，因此，第一服务证书与第二服务证书即使版本不一致，能够有效验证，通常只有当服务证书被篡改后，服务证书之间才会无法验证合法性，出现拒收的情况；当然，为了避免旧证书泄露导致的安全问题，还可以为旧版本的服务证书设置失效时间，当超过失效时间后，则认定为不合法，如果未超过，则认定为合法，失效时间由证书管理模块在生成最新版本的服务证书后对旧版本的历史服务证书进行设置，在反向代理模块获取最新版本的服务证书或下发最新版本的服务证书时，同最新版本的服务证书一并告知反向代理模块旧版本的历史服务证书的失效时间。

[0063] S16：若第二加密流量的第二服务证书合法，则解密第二加密流量，得到流入流量，并转发流入流量至第一服务。

[0064] 具体的，若利用第一服务证书验证通过，则可以利用第一服务证书对第二加密流量进行解密，得到流入流量。

[0065] S17：若第二加密流量的第二服务证书不合法，则拒收第二加密流量。具体的，容器

云平台中可以搭载大量的服务，每个服务都相当于第一服务和第二服务，每个服务都配有对应的反向代理模块，每个服务流入流出的流量均需要通过反向代理模块的验证和加密。

[0066] 需要说明的是，第一反向代理模块为第一服务对应的反向代理模块，第二反向代理模块为第二服务对应的反向代理模块，第一反向代理模块和第二反向代理模块其作用相同，只是服务对象不同。

[0067] 具体的，在服务角度上来说，服务之间仍是按照无安全系统的方式进行流量发送，但实际上服务之间的流量交互全部有安全系统进行验证和管理，实现了无感知的安全通信保护。

[0068] 可以理解的是，第一反向代理模块和第二反向代理模块中的“第一”和“第二”只是为了区分第一反向代理模块和第二反向代理模块服务于不同的服务，其功能和作用是相同的，第一服务证书与第二服务证书中的第一和第二也是用于区分存放于不同反向带模块中的服务证书，其本质都是由证书管理模块生成并存储的服务证书，能够互相验证合法性。

[0069] 可见，本发明实施例容器云平台中每个服务都对应的设置有反向代理模块，通过证书管理模块管理每个反向代理模块的服务证书，每个反向代理模块劫持任何需要出入服务的流量，并进行相应的加密和验证，确保流入流量和流出流量在通信期间的安全性，并且实现了统一的安全管理，且对服务本身的运行过程无影响，实现了无感知的安全控制。

[0070] 本发明实施例公开了一种具体的容器云平台安全通信方法，相对于上一实施例，本实施例对技术方案作了进一步的说明和优化。参见图2所示，具体的：

[0071] S21：接收证书管理模块生成并存储的第一服务证书，或从证书管理模块获取第一服务证书；

[0072] S22：劫持对应的第一服务流出的流出流量；

[0073] S23：利用第一服务证书为流出流量进行TLS加密，得到第一加密流量，转发第一加密流量至相应的第二服务。

[0074] S24：从安全认证模块获取认证名单。

[0075] 具体的，S24获取认证名单与S21至S23之间不存在执行先后顺序，可以先执行S24，也可以在S21至S23之间任一步骤后执行，在此不做限定，当然，S24也可以在S25之后执行

[0076] S25：劫持与第二服务对应的第二反向代理模块发送的第二加密流量；

[0077] S26：根据认证名单判断第二加密流量对应的第二服务是否满足要求；

[0078] 具体的，认证名单相当于白名单或黑名单，当为白名单时，名单验证子模块则判断第二加密流量对应的第二服务是否在白名单中，如果在则调用流量验证子模块，继续对第二加密流量进行验证，如果不在则可以省去验证过程直接拒收；当认证名单为黑名单时，则判断第二加密流量对应的第二服务是否在黑名单中，如果不在黑名单中则执行S27，继续对第二加密流量进行验证，如果在则可以省去验证过程直接拒收。

[0079] 具体的，可以定时从安全认证模块获取最新的认证名单。

[0080] S27：利用第一服务证书验证第二加密流量的第二服务证书是否合法；

[0081] S28：若第二加密流量的第二服务证书合法，则对第二加密流量进行TLS解密，得到流入流量，并转发流入流量至第一服务。

[0082] 具体的，利用TLS对流量进行加密解密，实现TLS双向加密，提高加密数据的安全性。

[0083] S29:若第二加密流量的第二服务证书不合法,则拒收第二加密流量。

[0084] 具体的,为了反馈给服务流量被拒的情况,在根据认证名单判断第二服务不满足要求或验证第二加密流量的第二服务证书不合法后,则可以发送拒收信息至第二反向代理模块;其中,拒收信息可以为一个状态码,例如,状态码400。

[0085] 相应的,本发明实施例还公开了一种第一反向代理模块,参见图3所示,该模块包括:证书获取子模块11、流出流量劫持子模块12、流量加密子模块13、流入流量劫持子模块14、流量验证子模块15、解密子模块16和拒收子模块17;

[0086] 证书获取子模块11,用于接收证书管理模块下发的第一服务证书,或从证书管理模块获取第一服务证书;

[0087] 流出流量劫持子模块12,用于劫持对应的第一服务流出的流出流量;

[0088] 流量加密子模块13,用于利用第一服务证书为流出流量加密,得到第一加密流量,转发第一加密流量至相应的第二服务;

[0089] 流入流量劫持子模块14,用于劫持第二反向代理模块发送第二加密流量;

[0090] 流量验证子模块15,用于利用第一服务证书验证第二加密流量的第二服务证书是否合法;

[0091] 解密子模块16,用于若流量验证子模块15判定第二加密流量的第二服务证书合法,则解密第二加密流量,得到流入流量,并转发流入流量至第一服务;

[0092] 拒收子模块17,用于若流量验证子模块15判定第二加密流量的第二服务证书不合法,则拒收第二加密流量。

[0093] 可见,本发明实施例容器云平台中每个服务都对应的设置有反向代理模块,通过证书管理模块管理每个反向代理模块的服务证书,每个反向代理模块劫持任何需要出入服务的流量,并进行相应的加密和验证,确保流入流量和流出流量在通信期间的安全性,并且实现了统一的安全管理,且对服务本身的运行过程无影响,实现了无感知的安全控制。

[0094] 具体的,还可以包括名单获取子模块和名单验证子模块;

[0095] 名单获取子模块,用于从安全认证模块获取认证名单;

[0096] 名单验证子模块,用于根据认证名单判断第二加密流量对应的第二服务是否满足要求,若满足则调用流量验证子模块15,若不满足,则调用拒收子模块17;

[0097] 拒收子模块17,还用于若名单验证子模块判定第二加密流量对应的第二服务不满足要求,则拒收第二加密流量。

[0098] 具体的,上述证书获取子模块11,可以具体用于定时从证书管理模块获取最新的第一服务证书。

[0099] 具体的,上述名单获取子模块,可以具体用于定时从安全认证模块获取最新的认证名单。

[0100] 具体的,上述拒收子模块17,还可以用于若根据认证名单判断第二服务不满足要求或流量验证子模块15判定第二加密流量的第二服务证书不合法后,则发送拒收信息至第二反向代理模块。

[0101] 具体的,上述流量加密子模块13,可以具体用于利用第一服务证书为流出流量进行TLS加密,得到第一加密流量,转发第一加密流量至相应的第二服务;

[0102] 上述解密子模块16,可以具体用于若流量验证子模块15判定第二加密流量的第二

服务证书合法，则对第二加密流量进行TLS解密，得到流入流量，并转发流入流量至第一服务。

[0103] 此外，本发明还公开了一种容器云平台安全通信系统，参见图4所示，该系统包括：证书管理模块21、安全认证模块26、第一服务22、如前述的包括与第一服务22对应的第一反向代理模块23、第二服务25和与第二服务25对应的第二反向代理模块24；

[0104] 证书管理模块21，用于生成并存储第一服务22证书，下发第一服务22证书至第一反向代理模块23；

[0105] 安全认证模块26，用于存储认证名单。

[0106] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0107] 专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0108] 以上对本发明所提供的技术内容进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

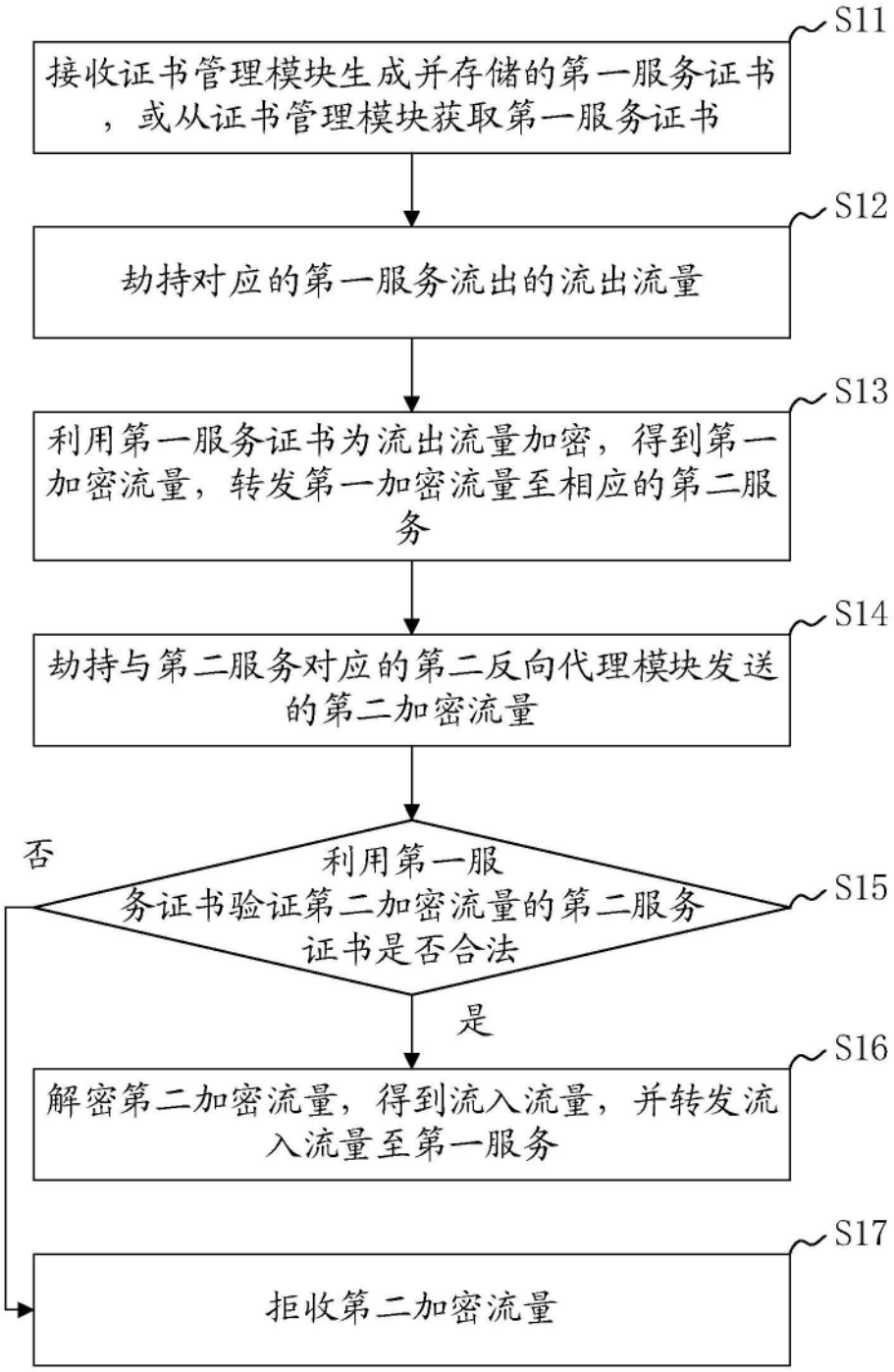

S11
接收证书管理模块生成并存储的第一服务证书，或从证书管理模块获取第一服务证书
S12
劫持对应的第一服务流出的流出流量
S13
利用第一服务证书为流出流量加密，得到第一加密流量，转发第一加密流量至相应的第二服务
S14
劫持与第二服务对应的第二反向代理模块发送的第二加密流量
利用第一服务证书验证第二加密流量的第二服务证书是否合法
S15
否
是
S16
解密第二加密流量，得到流入流量，并转发流入流量至第一服务
S17
拒收第二加密流量

图1

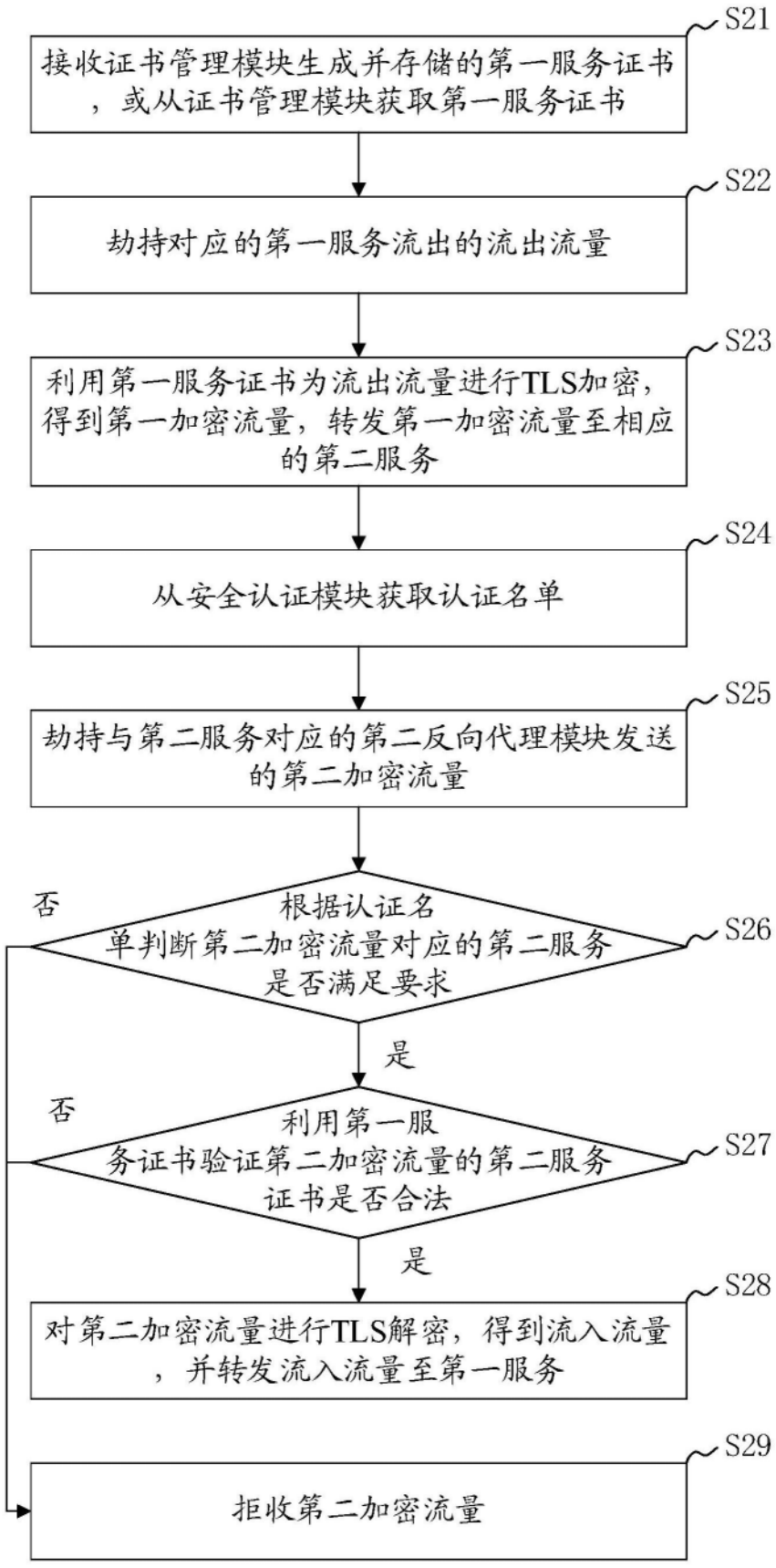

S21
接收证书管理模块生成并存储的第一服务证书，或从证书管理模块获取第一服务证书
S22
劫持对应的第一服务流出的流出流量
S23
利用第一服务证书为流出流量进行TLS加密，得到第一加密流量，转发第一加密流量至相应的第二服务
S24
从安全认证模块获取认证名单
S25
劫持与第二服务对应的第二反向代理模块发送的第二加密流量
根据认证名单判断第二加密流量对应的第二服务是否满足要求
S26
否
是
利用第一服务证书验证第二加密流量的第二服务证书是否合法
S27
否
是
S28
对第二加密流量进行TLS解密，得到流入流量，并转发流入流量至第一服务
S29
拒收第二加密流量

图2

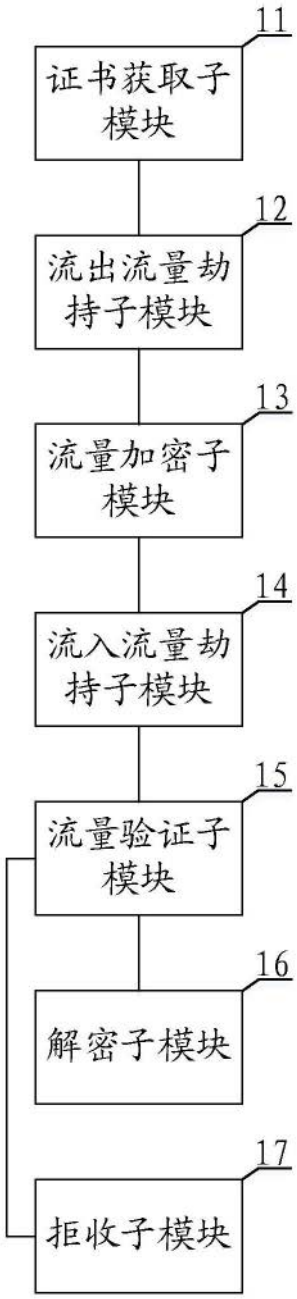

11
证书获取子模块
12
流出流量劫持子模块
13
流量加密子模块
14
流入流量劫持子模块
15
流量验证子模块
16
解密子模块
17
拒收子模块

图3

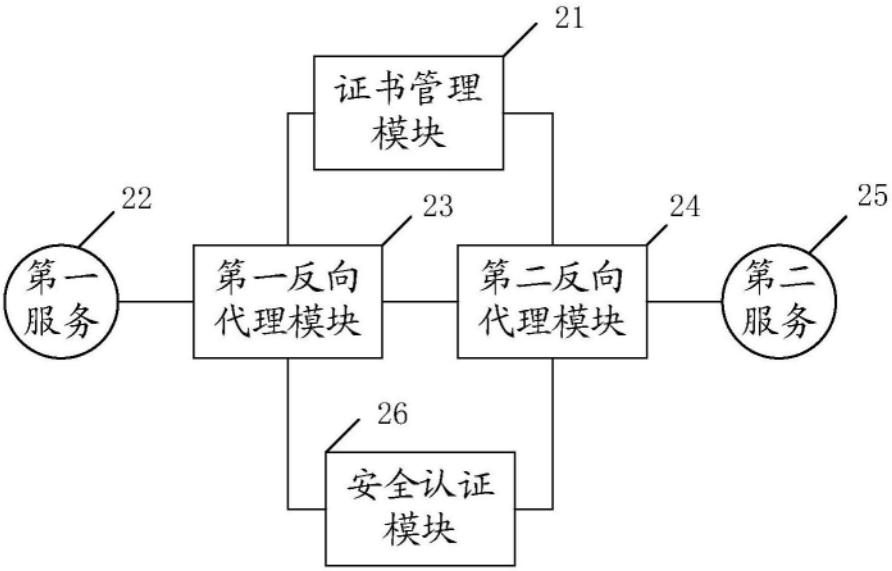


图4