(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107873128 B
(45)授权公告日 2021.06.25

(21)申请号 201680021239.4
(22)申请日 2016.04.07
(65)同一申请的已公布的文献号
申请公布号 CN 107873128 A
(43)申请公布日 2018.04.03
(30)优先权数据
62/144,293 2015.04.07 US
62/151,174 2015.04.22 US
(85)PCT国际申请进入国家阶段日
2017.10.09
(86)PCT国际申请的申请数据
PCT/IB2016/000528 2016.04.07
(87)PCT国际申请的公布数据
WO2016/162748 EN 2016.10.13
(73)专利权人 安博科技有限公司
地址 中国香港皇后大道中340号华秦国际大厦20层2006室

(72)发明人 C·E·奥尔 J·E·鲁本斯坦
(74)专利代理机构 北京允天律师事务所 11697
代理人 李建航 高源
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
CN 102687480 A,2012.09.19
CN 1754161 A,2006.03.29
CN 1536824 A,2004.10.13
CN 103384992 A,2013.11.06
CN 101478533 A,2009.07.08
US 2014280911 A1,2014.09.18
US 2002046253 A1,2002.04.18
审查员 刘叶

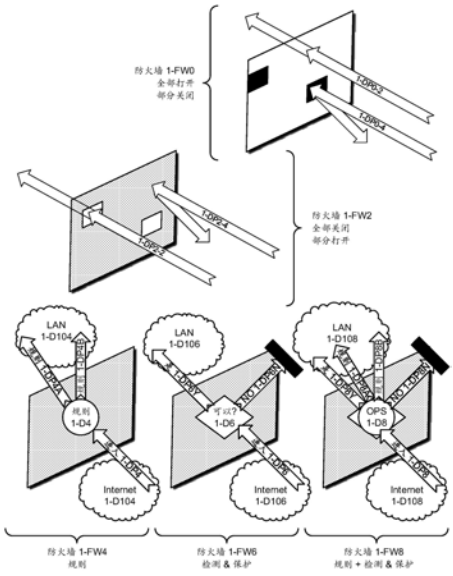
权利要求书1页 说明书21页 附图35页

(54)发明名称

在云端的多边界防火墙

(57)摘要

公开了通过全局虚拟网络提供多边界防火墙的系统和方法。在一个实施例中,网络系统可以包括与第一接入点服务器通信的出口入口点,与第一接入点服务器通信的第二接入点服务器,与第二接入点服务器通信的端点设备,第一防火墙与第一接入点服务器通信,以及与第二接入点服务器通信的第二防火墙。第一和第二防火墙可以阻止流量通过其各自的接入点服务器。第一防火墙和第二防火墙可以彼此通信并交换威胁信息。



CN 107873128 B

1.一种全局虚拟网络中的多边界防火墙,包括:出口入口点设备;

第一接入点服务器,所述第一接入点服务器与所述出口入口点设备通信;

第二接入点服务器,所述第二接入点服务器与所述第一接入点服务器通信;

端点设备,所述端点设备与所述第二接入点服务器通信;

第一边界防火墙,所述第一边界防火墙与所述第一接入点服务器通信,其中所述第一边界防火墙防止至少一些流量从所述第一接入点服务器传送到所述第二接入点服务器;以及

第二边界防火墙,所述第二边界防火墙与所述第二接入点服务器通信,其中所述第二边界防火墙防止至少一些流量从所述第二接入点服务器传送到所述端点设备,

其中所述第一边界防火墙和所述第二边界防火墙中的一个边界防火墙执行状态包检测,并且另一边界防火墙执行深度包检测。

2.根据权利要求1所述的多边界防火墙,其特征在于,所述接入点服务器中的至少一个用于执行防火墙服务。

3.根据权利要求1所述的多边界防火墙,其特征在于,所述第一边界防火墙与所述第二边界防火墙通信。

4.根据权利要求3所述的多边界防火墙,其特征在于,所述第一边界防火墙与所述第二边界防火墙之间的通信路径是全局虚拟网络隧道。

5.根据权利要求3所述的多边界防火墙,其特征在于,所述第一边界防火墙与所述第二边界防火墙之间的通信路径是全局虚拟网络反向通道。

6.根据权利要求3所述的多边界防火墙,其特征在于,所述第一边界防火墙和所述第二边界防火墙共享威胁信息,所述威胁信息包括启发式模式、已知威胁签名、已知恶意源头IP地址、或攻击向量中的任一个。

7.根据权利要求6所述的多边界防火墙,其特征在于,所述第一边界防火墙和所述第二边界防火墙与中央控制服务器共享威胁信息。

8.根据权利要求1所述的多边界防火墙,其特征在于,所述深度包检测在流经流量上执行。

9.根据权利要求1所述的多边界防火墙,其特征在于,所述深度包检测在所述流量的克隆拷贝上执行。

10.根据权利要求1所述的多边界防火墙,其特征在于,所述第一边界防火墙和所述第二边界防火墙中的至少一个包括云防火墙负载平衡器,所述云防火墙负载平衡器可根据需要分配云防火墙资源。

在云端的多边界防火墙

[0001] 本申请要求2015年4月7日提交的申请号为No.62/144,293的美国临时申请以及2015年4月22日提交的申请号为No.62/151,174的美国临时申请的优先权,每个申请都通过引用并入本文。

技术领域

[0002] 本申请总体上涉及网络技术,更具体地,涉及网络安全,该网络安全通过布置在云端多个边界的分布式防火墙(FW)设备的策略来保护通过全局虚拟网络或类似网络的流经流量。

背景技术

[0003] 人类能够感觉到200ms或更长的延迟,因为这通常是人类对事件的平均反应时间。如果延迟太高,诸如瘦客户端到基于云的服务器、客户关系管理(CR)、企业资源规划(EPVP)等在线系统将表现不佳,甚至可能由于超时而停止运行。高延迟结合高分组丢失可能导致连接不可用。即使数据通过,某个时候太慢也会导致用户体验不好(UX),在这种情况下,用户可以拒绝接受这些使传递不及格的服务变得无用的条件。

[0004] 为了解决其中的一些问题,已经开发了各种技术。一种这样的技术是WAN优化,通常涉及在局域网(LAN)边缘的硬件(HW)设备,该硬件(HW)设备在另一LAN边缘的另一WAN优化HW设备建立隧道,用以在它们之间形成广域网(WAN)。该技术假设两个设备通过其彼此连接的稳定连接。WAN优化器努力压缩和保护数据流,通常会导致速度增益。采用WAN优化的商业驱动是为了节省发送的数据量,以降低数据传输的成本。这样做的缺点是,当两台设备之间的连接不好时,由于它们往往是点对点的,因此它们之间几乎没有控制通过互联网的流量流动的路径。为了解决这个问题,WAN优化器的用户经常选择通过MPLS或DDN线路或其他专用电路运行WAN,这些会导致额外的费用,并且通常需要一个刚性的、固定的点对点连接。

[0005] 诸如MPLS、DDN、专用电路或其他类型的固定点对点连接的直接链路提供连接质量和服务质量(QoS)保证。它们是昂贵的,并且通常需要很长的时间来安装,因为需要从连接的每一侧的POP来物理上绘制线。当通过这个直接连接的WAN从一个LAN连接到另一个LAN的资源时,点到点拓扑结构很好。然而,当一般互联网的网关(GW)位于一端的LAN时,例如在公司总部,则来自附属国的远程LAN的业务可以通过GW被路由到互联网。由于流量通过互联网返回同一个国家的子公司的服务器,所以出现放缓。然后,流量必须通过WAN从LAN到GW所在的LAN,然后通过互联网返回到原籍国的服务器,然后通过互联网返回到GW,然后将专线退回到局域网内的客户端设备实际上,本质上会是两倍或三倍(或更差)的全球通行时间,而实际上访问这个附近的站点的时间仅需要全球延迟的一小部分。为了克服这种情况,通过适当的配置更改以及添加可将本来流量连接到互联网的设备,可以在此类系统的每个端点提供与另一个网络线的可替换连接。

[0006] 从一个局域网到另一个局域网创建WAN链路的另一个选择涉及在两个路由器、防火墙或等效边缘设备之间建立隧道,如IPSec或其他协议隧道。这些通常是加密的,并且可

以提供压缩和其他逻辑来尝试改善连接。这两点之间的路线很少甚至无法控制，因为它们依赖互联网上的各种中间玩家的政策，他们通过他们的网络进行流量，并与其他运营商和网络运营商进行对等。许多设备供应商的防火墙和路由器、交换机和其他设备通常在其固件中内置隧道选项。

[0007] 近年来，最后一公里的连通性大幅度提高，但受到距离、协议限制、对等、干扰等问题和威胁有关的问题，长距离连接和吞吐量仍然存在问题。因此，存在对在标准互联网连接顶部运行的安全网络优化服务的需求。

发明内容

[0008] 公开了通过虚拟全球网络提供多边界防火墙的系统和方法。该网络可以包括出口入口点设备、第一和第二接入点服务器、端点设备以及第一和第二防火墙。第一防火墙与第一接入点服务器通信，并且可以防止网络流量流经第一接入点服务器。第二防火墙与第二接入点服务器通信，并且可以防止网络流量流经第二接入点服务器。

[0009] 根据一个实施例，至少一个接入点服务器被配置为执行防火墙服务。

[0010] 根据另一实施例，第一防火墙与第二防火墙通信。第一和第二防火墙之间的通信路径可以是全局虚拟网络隧道或全局虚拟网络返回信道或API调用或其他。在一些实施例中，第一防火墙和第二防火墙共享包括启发式模式、已知威胁的签名、已知恶意源IP地址或攻击向量中的至少一个的威胁信息。威胁信息可以通过中央控制服务器共享。

[0011] 在一些实施例中，至少一个防火墙执行深度包检测。在其他实施例中，至少一个防火墙执行状态包检测。在其他实施例中，一个防火墙执行状态包检测，而另一个防火墙执行状态包检测。

[0012] 在一些实施例中，防火墙中的至少一个包括可以按需分配云防火墙资源的云防火墙负载平衡器。

附图说明

[0013] 为了更好地理解本公开，现在参考附图，其中相同的元件以相同的附图标记或附图标记。这些附图不应被解释为对本公开的限制，而是仅仅是说明性的。

[0014] 图1示出了五种类型的防火墙设备操作。

[0015] 图2示出了通过防火墙的流量可能性。

[0016] 图3示出了状态包检测和深度包检测。

[0017] 图4示出了从分组流生成组合的有效载荷。

[0018] 图5示出了从互联网到LAN的广泛的网络攻击路径。

[0019] 图6展示了由于相对网络上发生的高流量大规模攻击而对网络造成的负面回弹效应。

[0020] 图7示出了位于云端的多边界防火墙。

[0021] 图8示出了位于云端的多边界防火墙的可扩展性。

[0022] 图9示出了在互联网连接之上的GVN之上的多边界防火墙。

[0023] 图10是从起点到目的地的GVN可用的各种路线的流程图。

[0024] 图11示出了状态包检测(SPI)防火墙和深度包检测(DPI)防火墙之间的通信。

[0025] 图12示出了由全局虚拟网络启用的云端多边界防火墙(MPFW)。

[0026] 图13示出了全局虚拟网络的设备之间的信息流。

[0027] 图14示出了支持个人端点设备的云端的多边界防火墙(MPFW)。

[0028] 图15说明了GVN中自动化设备和防火墙协作和信息交换所需的模块。

[0029] 图16示出了GVN中设备到设备的信息交换。

[0030] 图17示出了GVN中多边界防火墙与其他系统的集成。

[0031] 图18示出了基于云的防火墙负载平衡器连接的基于云的防火墙提供的可扩展性的防火墙的拓扑和相应布局。

[0032] 图19示出了GVN拓扑,包括互联网或暗光纤上的骨干段。

[0033] 图20示出了用于向终端设备(EPD)和互联网的信息流的设备的拓扑和连接。

[0034] 图21示出了多边界防火墙算法。

[0035] 图22示出了用于云防火墙设备、云防火墙负载平衡器设备、中央控制服务器、接入点服务器和端点设备的软件架构的逻辑视图。

[0036] 图23示出了通过中央控制服务器(SRV_CNTRL)从防火墙(FW)到全局虚拟网络(GVN)中的各种设备的信息流。

[0037] 图24是描述用于分析流过防火墙、防火墙负载平衡器和/或通过防火墙阵列的流量的算法的流程图。

[0038] 图25示出了处理和处理威胁的系统堆栈中的各个层。

[0039] 图26示出了在启动过程期间自动解密加密卷的方法。

[0040] 图27示出了如何基于特定于该设备的多个因素来为设备一致地计算唯一用户标识(UUID)。

[0041] 图28示出了安全引导机构的模块。

[0042] 图29示出了后通道机构的细节。

[0043] 图30示出了多个端点设备(EPD)和后向通道服务器(SRV_BC)之间的连接。

[0044] 图31示出了使用对于每一行唯一的旋转和计算的密钥将加密数据写入数据库的一行中的选定字段。

[0045] 图32示出了使用键、键调节器和使用框架来计算键的其他因素从从单个行来解密数据。

[0046] 图33示出了当客户端经由端点设备(EPD)请求的图形用户界面(GUI)内容和请求内容被存储在锁定的卷内时会发生什么。

[0047] 图34示出了互联网的高级框图。

[0048] 图35是通过域名系统(DNS)对数字互联网协议(IP)地址的通用资源定位符(URL)展示分辨率的框图。

具体实施方式

[0049] GVN在其标准互联网连接的顶部为客户提供安全的网络优化服务。这是GVN的组成部分的概述以及可用作GVN元素的相关技术的描述。GVN元素可以独立运行,也可以在GVN生态系统内运行,例如为了自己的目的利用GVN框架,或者可以部署GVN元件来提高GVN的性能和效率。该概述还描述了其他技术如何从GVN中获益,作为使用GVN的一些或所有组件的独

立部署,或者可以利用其优点将其作为独立机制快速部署为现有GVN之上的独立机制。

[0050] 基于软件(SW)的虚拟专用网络(VPN)通过客户端设备和VPN服务器之间的隧道提供隐私。这些具有加密以及在某些情况下同时压缩的优点。但是,再一次的,VPN客户端和VPN服务器之间以及VPN服务器与主机服务器、主机客户端或目的地的其他设备之间的流量几乎无法控制。这些通常是点对点连接,需要使用VPN安装每个设备的客户端软件,并且某些技术熟练程度来维护每个设备的连接。如果VPN服务器出口点通过到目的主机服务器或主机客户端的高质量通信路径靠近,则性能将会很好。如果没有,那么从可用性的角度来看,性能和不满将会引人注目。VPN用户通常需要断开与一个VPN服务器的连接,并重新连接到另一个VPN服务器,以便对来自某个区域的内容与来自其他区域的内容确保质量或本地访问。

[0051] 全局虚拟网络(GVN)是互联网上的一种计算机网络,通过利用世界各地的分布在世界各地的设备网络、通过高级隧道相互连接、通过应用程序接口(API)进行协作和通信、数据库(DB)复制等方法能够提供全球安全网络优化。GVN中的流量路由总是通过由高级智能路由(ASR)管理的最佳通信路径,该自动化系统由自动化系统提供支持,这些自动化系统将建立者、管理者、测试人员、算法分析和其他方法结合起来,以适应不断变化的条件和随时间的学习,以配置和重新配置系统。

[0052] GVN在一个或多个常规互联网连接之上提供服务,以提供安全、可靠、快速、稳定、精确和集中的并行连接。这些优点是通过压缩在EPD和EPD附近的接入点服务器(SRV_AP)之间转换包,伪装和加密隧道的多个连接的数据流来实现的。EPD与SRV_AP的连接质量不断受到监控。

[0053] GVN是硬件(HW)、端点设备(EPD)、安装软件(SW)、数据库(DB)和GVN系统的其他自动化模块(如中性应用程序编程接口机制(NAPIM)),后端通道管理器、隧道管理器以及将EPD连接到GVN内的接入点服务器(SRV_AP)和中央服务器(SRV_CNTRL)等分布式基础设施设备的更多功能的集合。

[0054] 算法持续分析当前的网络状态,同时考虑尾随趋势加上长期历史性能,以确定流量采取的最佳路由,以及哪些是最佳的SRV_AP或一系列的SRV_AP服务器来推动流量通过。配置、通信路径和其他更改是自动进行的,并且需要最少的用户交互或干预。

[0055] EPD和SRV_AP中的高级智能路由确保通过尽可能简单的GVN“第三层”,流量通过从原点到目的地的最理想路径流动。这个第三层被连接到GVN的客户端设备看作是一个普通的互联网路径,但跳数较少,安全性更好,在大多数情况下,比通过普通互联网流向同一个目的地的流量更低的延迟。逻辑和自动化在GVN的“第二层”中运行,在此,GVN的软件自动监视和控制虚拟接口(VIF)的底层路由和构造、多个隧道和通信路径的绑定。GVN的第三层和第二层存在于与底层互联网网络的设备交互的GVN的可操作“第一层”之上。

[0056] 从技术和网络的角度来看,云是指通过开放互联网连接并可用于其他设备的设备或组或阵列或设备集群。这些设备的物理位置并不重要,因为它们经常将多个数据复制到多个位置,并通过使用内容传送网络(CDN)或其他此类技术传送到/从请求客户端的最靠近的服务器来加速连接,从而增强用户体验(UX)。

[0057] 本发明基于防火墙(FW)的行业的标准使用,通过将周边延伸到云端来提高其效用值。防火墙是主要设计用于保护内部网络免受来自外部网络的外部威胁的设备,以及保护

信息数据从内部网络泄漏的设备。传统上,防火墙被放置在诸如局域网(LAN)的一个网络和另一个网络之间的边缘,例如其上行链路到更广泛的网络。网络管理员对FW的放置和可信度敏感,因为它们依赖它来保护其网络。

[0058] GVN的附加组件包括安全引导机制(SBM)和后通道机制(BCM)。安全引导机制通过将密钥存储在远程服务器上并且仅通过SBM使密钥可用来保护安全卷的密钥。后通道机构允许GVN的许多设备的管理和/或交互。在隧道故障时网络性能不佳的时候,BCM向不能达到的设备提供通道,包括访问从开放互联网无法访问的设备。这种机制通过屏障提供反向穿孔,以保持通信通道畅通。GVN的其他安全组件包括使用每行键的UUTD硬件绑定和精细粒度数据加密。

[0059] 图34示出了互联网的高级框图。一般用户对互联网功能的理解非常粗略。主机源34-100是起始点,其可以是计算机、移动电话、平板电脑、膝上型计算机或其他此类客户端的客户端设备。该客户端通过互联网34-200连接到主机服务器34-300以发送或检索内容,或者连接到另一个主机客户端34-302来发送或接收信息。

[0060] 一个非技术性的用户可能会认为到主机服务器的流量遵循路径2P002,甚至不了解他们的数据将通过互联网传输。或者他们可能认为流量将通过路径2P006直接流向另一个客户端设备。

[0061] 具有对其工作方式有更多了解的用户将了解流量通过路径2P004流向互联网34-200,然后通过路径2P102通过主机服务器目标34-300或通过路径2P104到主机(客户端)目标34-302。

[0062] 具有更多技术知识的用户将进一步了解,当发送电子邮件时,该电子邮件将离开他们的客户端设备34-100,通过路径2P004传输到互联网34-200,然后通过路径2P202传送到邮件服务器34-202。然后,电子邮件的收件人将通过其主机客户端34-302沿着路径2P104向互联网提取电子邮件请求,然后将路径2P204下发到邮件服务器34-202。

[0063] 这与普通人对互联网的理解有关。

[0064] 图35是通过域名系统(DNS)对数字互联网协议(IP)地址的通用资源定位符(URL)展示分辨率的框图。

[0065] 内容请求35-000或从主机客户端(C)35-100推送到主机服务器(S)35-300,作为从主机客户端(C)35-100到主机服务器(S)的文件或流或数据块35-300。响应或内容传递35-002从主机S返回给主机C作为文件或数据流或数据块。与主机服务器(S)的客户端-服务器(CS)关系中的主机客户端设备35-100使得请求从远程主机服务器(S)访问内容,或者通过通用资源定位器向远程主机服务器(S)发送数据(URL)或其他网络可达地址。

[0066] 从主机客户机(C)35-100到互联网35-206的初始连接显示为3P02-从主机客户机(C)到直接面对的存在点(POP)35-102的连接。在其他情况下,主机客户机(C)可以位于局域网(LAN)中,然后局域网(LAN)经由存在点(POP)连接到互联网,并且可被称为最后一公里连接。存在点(POP)35-102表示由互联网服务提供商(ISP)从终端通过其网络及其互连向互联网提供的连接。这可以是但不限于电缆、光纤、DSL、以太网、卫星、拨号和其他连接。如果URL是域名而不是数字地址,则将该URL发送到域名系统(DNS)服务器35-104,其中将域名转换为IPv4或IPv6或其他地址以进行路由。

[0067] 主机客户端(C)35-100到主机服务器(S)35-300的流量通过互联网35-206路由,用

于代表POP(35-102和35-302)之间的转移,包括对等、回程或其他网络传输边界。

[0068] 用于从通用资源定位符(URL)查找号码地址以获取目标服务器(S)的IPv4地址或其他数字地址的POP35-102和域名系统35-104之间的连接3P04可以从POP直接访问,也可以通过互联网35-206。从ISP 35-102到互联网35-206的连接3P06可以是单宿主或多宿主的。类似地,从互联网35-206到远程ISP的连接3P08也可以是单宿主或多宿主的。这种连接通常是ISP或Internet数据中心(IDC)面向互联网的POP 35-302。从远程ISP的POP 35-302到主机服务器(S)的连接3P10可以是直接的或通过多跳。

[0069] 通过域名系统从URL或主机名到数字地址的查找是Internet上的标准,系统假设DNS服务器是一体的,DNS服务器的结果是最新的,并可以被信任。

[0070] 图19示出了GVN拓扑,通信路径包括通过互联网或暗光纤的骨干段,并且指示在各种周边位置处包括各种类型的防火墙(FW)设备的各种设备的布置。它显示了各种地理区域或区域或领域如何通过各种类型的路径连接在一起。该图说明了各种类型的网络结构可以组合成更大的网络挂毯。这些编织网络可以如美国临时专利申请No.62/174,394中所述无缝地结合在一起。

[0071] 参见图19,显示了多个区域:LAN区域0(ZL00),LAN区域1(ZL10),互联网区域0(ZI00),互联网区域1(ZI10),互联网区域2(ZI20),互联网区域3ZI30),互联网数据中心2区(ZD20)和互联网数据中心3区(ZD30)。

[0072] LAN区域0 19-ZL00描述了典型的局域网(LAN),其包括在LAN和外部网络GVN OTT 19-202和互联网19-30之间相对于端点设备(EPD)19-100的防火墙的放置。LAN 19-04和EPD19-100之间有硬件防火墙FW19-40。另一个硬件或软件FW 19-42位于EPD 19-100和出口入口点(EIP)19-20之间,以保护EPD免受来自互联网19-30的外部威胁。

[0073] LAN区域19-ZL10的拓扑类似于LAN区域零19-ZL00,不同之处在EPD 19-110和LAN 19-46之间没有防火墙。

[0074] 互联网区域0 19-ZI00描述了在接近19-ZL00的区域中的示例互联网拓扑。互联网区一个19-ZI10描述了一个在19-ZL10附近的区域中的一个示例互联网拓扑。互联网区域19-ZI20描述了一个在19-ZD20附近的区域中的互联网拓扑。互联网区域19-ZI30描述了一个在19-ZD30附近的区域中的互联网拓扑。

[0075] 互联网数据中心二区19-ZD20描述了基于云的防火墙CFW 19-46的拓扑和布局,包括云防火墙负载平衡器后面的虚拟化防火墙设备。互联网数据中心三区19-ZD30描述了基于云的防火墙CFW 19-48的拓扑和布局,包括云防火墙负载平衡器后的虚拟化防火墙设备。

[0076] 区域或区域ZD20中的SRV_BBX 19-72可通过暗光纤19-220通过暗光纤连接19-P220连接到另一区域或区域ZD30中的SRV_BBX 19-80。SRV_BBX 19-72可以通过远程直接存储器访问(RDMA)通过19-P220直接将文件写入并行文件存储PFS 19-82,通过路径19-P82绕过SRV_BB 19-80的堆栈。SRV_BBX 19-80可以通过19-P220的远程直接存储器访问(RDMA)直接将文件写入并行文件存储PFS 19-74,通过路径19-P74绕过SRV_BBX 19-72的堆栈。

[0077] 路径19-P210可以是IPv4或某种标准化的互联网协议,流量从SRV_AP19-300通过隧道上的GVN的顶部通过路径19-P210从SRV_AP 19-310流向SRV_AP 19-310或者其他类型的通信路径。

[0078] 虽然所示的拓扑结构在GVN路径中没有防火墙或流量监控设备,但是可以根据需

要将这些设备放置在这里,以进一步确保数据流。

[0079] 图13示出了全局虚拟网络的设备之间的信息流。一个由数据库B200和文件存储HFS200组成的中央存储库驻留在中央服务器(SRV_CNTRL)200上。

[0080] 标记为P###的设备之间的通信路径可以表示为API调用、数据库复制、直接文件传输、通过API调用的数据库复制或其他形式的信息交换等组合。13-P100300,13-P300500和13-P100500的粗线表示GVN设备之间的直接通信,GVN设备之间具有对等配对,因此具有彼此的特权关系。

[0081] 通过13-P200100从SRV_CNTRL 200到EPD 100,经由13-P200300或者通过13-P200500的其他设备13-500示出了对等通信的圆形模式。EPD100经由13-P100200与SRV_CNTRL 200进行通信,SRV_AP 300经由13-P300200通过SRV_CNTRL 200进行通信,其他设备13-500经由13-P500200与SRV_CNTRL 200进行通信。

[0082] 在一些情况下,存在设备之间共享的信息循环,例如在EPD 100可以经由13-P100200从SRV_CNTRL 200请求信息的情况下,其中该信息经由13-P200100发送回EPD 100。

[0083] 在其他情况下,一个设备可以将与其他设备、例如SRV_AP 200相关的信息经由13-P300200报告给SRV_CNTRL 200,然后SRV_CNTRL 200经由13-P200100将该信息发送到EPD 100和SRV_AP 300,而还通过13-P200300报告SRV_AP并且也通过13-P200500发送到其他设备13-500。

[0084] 在其他情况下,不需要完整循环,例如通过13-P100200从诸如EPD 100的设备发送日志信息到SRV_CNTRL 200,不需要进一步向前转发该信息。但是,日后记录信息可能会在稍后时间从SRV_CNTRL 200上的存储库移动到长期日志存储服务器13-500或通过13-P200500到其他设备。

[0085] 直接链路13-P100300位于设备EPD100和SRV_AP300之间。直接链路13-P300500从SRV_AP 300到其他设备13-500。直接链路涉及不需要SRV_CNTRL 200参与的设备之间的通信。

[0086] 来自SRV_CNTRL 200的SRV_CNTRL 13-306的推送(馈送)可以是通过13-P306发布的RSS馈送或其他类型的信息。对SRV_CNTRL 13-302的API-查询调用SRV_CNTRL 200可以是传统的API事务或RESTful API调用,并具有通过13-P302REQ进行请求和通过13-P302RESP接收响应。PUSH 13-306和API 13-302元件来说明与不与GVN设备共享对等关系、特权状态和/或类似系统架构但可以从信息中受益的设备的通信。

[0087] 图1说明了五种类型的防火墙设备操作。防火墙1-FWO演示了一个具有一些关闭显示的全开防火墙。路径1-DPO-2表示因为没有明确阻止而允许通过防火墙的流量流。路径1-DPO-4显示了由于被明确阻止而不能通过防火墙的流量。

[0088] 防火墙1-FW2演示了一个带有一些开口显示的全封闭防火墙。路径1-DP2-4表示通过规则未明确允许的流量,因此被阻塞。路径1-DP2-2表示明确允许的流量,因此流量畅通无阻。

[0089] 防火墙1-FW4演示了基于规则的防火墙,其中显示了两个规则。来自互联网1-D104的流量通过路径传入1-DP4到用于转发或其他处理的规则1-D4的表。如果进入的流量匹配一个规则,它将通过路径规则1-DP4A流向LAN 1-D104。如果它匹配另一个规则,它将通过路径规则1-DP4B流向LAN1-D104中的另一个位置。

[0090] 防火墙1-FW6演示防火墙操作，例如使用决策矩阵1-D6进行检测和保护，以检查流量是否可行，并且应该允许通过路径“是1-DP6Y”到LAN1-D106，或者如果检测到威胁并且流量被阻挡和/或黑洞(blackholed)或以其他方式通过路径“否1-DP6N”来处理。

[0091] 防火墙1-FW8演示了具有规则组合的防火墙加上检测和保护操作1-D8。来自Internet 1-D108的流量可以通过LAN 1-D108的规则路径规则1-DP8A或规则1-DP8B匹配规则和流量，或者可以通过路径YES 1-DP8Y通过直接和保护过滤器来允许。如果不允许流量，将被阻塞或黑洞或以其他方式通过路径NO 1-DP8N来处理。

[0092] 未示出的另一种类型的防火墙是防火墙1-FWO或防火墙1-FW2和防火墙1-FW8的组合。还有不同类型的检测和保护防火墙，如状态包检测(SPI)，深度包检测(DPI)和其他类型的防火墙。

[0093] 图2示出了通过防火墙的流量可能性。最后一公里POP 2-022和LAN2-114之间的连接路径是通过从POP到FW 2-144的2-CP144和从LAN2-114到FW 2-144的2-CP114。可能被捕获的恶意、违规或已知的威胁流量可以通过路径2-TR6A到2-TR6B被发送到黑洞2-148或通过路径2-TR4A到2-TR4B数据隔离在FW-隔离(Quarantine)2-144Q中。良好、无挑战或允许的交通路径可以通过2-TR2流动。外部攻击流量外部由2-ATK-434和2-ATK-432表示。

[0094] 图3说明防火墙可以执行的两种检查：状态包检测和深度包检测。在防火墙位于一个物理设备中的情况下，存在对SPI或DPI的选择，作为速度与全面性的权衡。SPI防火墙3-SP中显示状态包检测(SPI)，DPI防火墙3-DP中显示深度包检测(DPI)。

[0095] 当执行SPI时，防火墙会检查数据包的报头3-SPO-H，3-SP2-H和3-SP4-H，以识别有害信息，而忽略数据包的有效载荷3-SPO-P，3-SP2-P和3-SP4-P。SPI比DPI的优势在于它的速度很快，它占用较低的处理器、RAM和资源。缺点是防火墙不查看数据包的有效载荷内的内容。

[0096] DPI超过报头(headers)3-DPO-H、3-DP2-H、3-DP4-H、3-DP6-H及3-DP8-H，并检查内容，例如，有效载荷3-DPO-P，3-DP2-P，3-DP4-P，3-DP6-P和3-DP8-P。其优点在于，在不仅仅一个数据包的有效负载内，而且来自一系列多个数据包3-DPO，3-DP2，3-DP4-H，3-DP6以及3-DP8的编译有效载荷3-DP-ALL的内容中，这种检查是更全面的。DPI的缺点是它比SPI慢得多，并且它比SPI消耗更多的处理器、RAM和其他资源。

[0097] 图4示出了从数据包流生成组合的有效载荷。在该示例中，向DPI防火墙提供包4-DP流。有效负载3-DPO-P6，3-DP2-P6，3-DP4-P6，3-DP6-P6和3-DP8-P被连接到组合有效载荷3-DP-ALL中，然后由DPI防火墙4-DP-AL分析。

[0098] 深度包检测通过检查一个或多个数据包的有效载荷来进行。它仔细观察有效载荷的内容，并且可以搜索：搜索字符串、已知的病毒签名或指示病毒的启发式签名、恶意软件模式、伪装成不同数据类型的畸形二进制点(Blob)或其他已知或未知的威胁。

[0099] 图5示出了从互联网002到LAN 114的广泛的网络攻击路径。该图示出了每个网段的相对管道大小或带宽。内部LAN NTSP08可能以10GigE的速度运行。该网段包括ISP的POP022和内部防火墙FW144之间的连接CP114。本地ISP的网络NTSP04也可以是10GigE。该网段包括互联网和ISP的POP 022之间的连接CP022。互联网骨干网NTSP02的速度通常会快得多，比如多宿主(multi-honed)3*100GigE网络。

[0100] 但是，ISP的客户端防火墙FW 144和POP 022之间的“最后一公里”连接网络NTSP06

通常会慢一些。例如,FW 144和POP 022之间的连接CP 144可以是200Mbps连接,而不是NTSP04或NTSP08的更快的10GigE速度。因为这种连接具有较小的带宽,例如较慢,这种连接可以通过协调的基于互联网的攻击而容易地饱和。ISP的POP 022也可能饱和,不仅影响客户端的连接,还影响其他用户。

[0101] 图6显示了由于在应用网络上发生的高流量攻击而对网络造成的负面反击效应。当路径CP 144被攻击流量ATK-432和ATK-434过饱和时,这可能对网络路径CP 142(连接到防火墙FW 142和路径CP 112到LAN 1120)和CP 146(连接到防火墙FW 146和路径CP16至LAN 116)产生负面影响。这是由于CP142和CP146与CP144的紧密接近以及通过POP 022的共享上行路径。

[0102] CP 142和CP 146的负面影响可能是由于CP144共享交换机端口拥塞以及其他因素。此外,CP022从网络到POP 022的拥塞问题影响了ISP的POP 022和互联网002之间的所有流量。拥塞问题POP 022还可能影响通过POP的流量流动并使ISP带宽饱和,从而对其产生负面影响设备流量吞吐量。

[0103] 虽然CP 142和CP 146可能不会被直接攻击,但仍然会受到通过POP022和路径CP022对CP 144的攻击的不利影响。

[0104] 图7示出了位于云端的多边界防火墙。在云端定位多边界防火墙具有在传统防火墙位置上游的一个点识别和隔离问题流量的优点。通过在云CFB 7-144LB中部署多边界防火墙,在ISP的骨干网7-NTSP02上识别和隔离问题流量。问题流量被转移,没有到达“最后一公里”连接网络7-NTSP06。这意味着缓慢的200Mbps“最后一英里”连接网络7-NTSP06被隔离和保护,免受来自更快的3x 100GigE骨干网7-NTSP02上存在的多个并发攻击向量的大量流量的影响。

[0105] 图8示出了位于云端的多边界防火墙的可扩展性,并演示了如何通过GVN启用云端的分布式防火墙(FW)功能。基于云的防火墙可以通过云防火墙负载平衡机制进行动态扩展,可根据需要在线提供更多资源。由于GVN拓扑的性质,设备到设备的通信和安全的流量路径,防火墙机制可以是基于云的,也可以被虚拟化。防火墙8-144位于互联网8-000和GVN 8-028之间的云端。防火墙8-144可以包括云防火墙(CFW)负载平衡器8-144LB,它可以根据需要分配云防火墙资源,如8-144-2,8-144-3等。这种按需可扩展性为GVN的客户端提供了许多优点。

[0106] 首先,通过吸收云端的入侵威胁的攻击命中,客户端的最后一公里连接不受影响。第二,将云防火墙与控制节点和分析器结合使得受攻击的区域中的防火墙能够了解攻击的性质、源、签名和其他功能,以便防火墙能够意识到并准备挫败如果目标转移到不同的客户端网络的攻击。此外,关于过去和当前攻击的信息可以通过GVN的中立API机制(NAPIM)与其他CFW实例共享,这样全局威胁意识(awareness)是可能的。

[0107] 最后,如下图12所示,云防火墙同时提供了运行不同防火墙机制(如SPI和DPI)的优势。

[0108] 图9示出了跨越互联网连接的顶部(OTT)的GVN的顶部(OTT)的多边界防火墙。该图显示了其他分层功能的顶层(OTT)构建的分层功能。例如,多边界防火墙(MPFWM)9-88是全局虚拟网络(GVN)9-86的OTT^{2} 9-TOP88。GVN 9-86是链接到互联网9-TOP82的ISP网络服务层处的基础互联网连接(Base Internet Connectivity)9-82的OTT^{1} 9-TOP86。

[0109] OTT2是第二度的顶级意思，意味着某些东西超越了其他东西本身就是OTT1的东西。

[0110] 图10是通过GVN从原点C10-002到目的地S10-502可用的各种路线的流程图。这里可以有更多可能的没有显示或论述的组合。

[0111] 从客户端C10-002到EPD 10-108的路径10-CP00可用于测量从客户端经过局域网到EPD的性能。在测试和评估可用路径的实时数据之后，实现最佳路由的匹配。GVN入口通过第一跳10-CP00从EPD 10-108到接入点服务器(SRV_AP)10-102,10-104,10-106,10-202,10-204。从EPD 10-108到第一个SRV_AP的路径可以定义为从EPD 10-108到GVN的入口点，并相应地进行测量。从SRV_AP到SRV_AP的内部跳跃遵循始终尝试维持最佳路径连通性的内部路由。这些路由可以是OTT互联网、骨干网、暗光纤或其他相关路由。GVN中的最佳出口指标也可以在本地、远程地区以及整个网络从始发地到目的地整个轨道。

[0112] 可以考虑各种因素进行评估，每个细分可以运行测试，分段的组合以及从头到尾的总网络路径。流量类型和路径确定可以取决于数据属性和配置文件QoS要求。主要路径选择总是基于路径上流量的最佳因素。这种机制的功能是匹配目的地和起点之间的路径，以便最佳的双向路由流动。

[0113] GVN内的高级智能路由(ASR)的核心存储在磁盘、内存或数据库表中的索引上，索引包含一个要保留本地的IP地址列表，并通过同一地区的EIP退出。对于通过GVN到其他区域的流量，通过SRV_AP设备和路径的路由由服务器可用矩阵(SAM)和ASR确定。索引将匹配目标IP地址的目标列表存储在该区域中的最佳出口/入口点(EIP)中。另外，作为CIDR IP块或其他类型的符号映射到区域的国家IP地址表可以帮助确定最佳出口点。

[0114] 对于来自目的地S10-502、朝向起源地(Origin)C 10-002方向的流量，第一个EIP 10-320、10-322、10-334、10-326或10-328是GVN和互联网及其他网络(如LAN)、主干网、或其他之间的初始边界。SPI防火墙可以位于GVN后面的初始入口点，标明第一个外围。在下一个SRV_AP或其他SRV_AP(例如SRV_AP 10-102,10-104,10-204和10-206)，可以定位尾随的DPI防火墙的第二个周边。如果他们想要在第10-CP00段，客户端还可以在自己的网络中运行入站SPI或DPI防火墙。

[0115] 对于来自起源地C10-002、通过EPD 10-108、朝目的地Dest.S 10-502方向的流量，第一个SPI/DPI防火墙可以沿着路径10-CP00位于起源地C10-002和EPD 10-108之间。防火墙的第二个周边可以位于SRV_AP(如10-102,10-104,10-204和10-106)上，用以保护出站流量。

[0116] 对于来自互联网的流量，云的可扩展性是非常重要的，因为它可以通过扩展资源分配来处理分布式多通道流量的峰值负载。当活动相对平静时，可以提供最少的资源。资源的可扩展性对于互联网出站流量来说并不重要。在大多数情况下，LAN网络将具有比网络上行链路更大的带宽。由于在网络管理员的控制下的LAN/DMZ/网络中的威胁的性质，可扩展性不太重要。

[0117] 图18示出了基于云的防火墙负载平衡器连接的基于云的防火墙提供的可扩展性的防火墙的拓扑和相应布局。该图与图10相似，通过一系列通过GVN或其他类型的网络路径的路径，在业务流中额外安装各种SPI和DPI基于云的防火墙。

[0118] 状态包检测防火墙(SPI)是流量流经的设备。深度包检测防火墙(DPI)设备可以被

流经或分析克隆的流量副本，为DPI功能提供选项作为尾随指示器。如果检测到有害的流量，一旦识别出来就可以被阻止。设备之间通信的好处是，DPI防火墙识别的流量不良信息可能会被SPI消息传递到SPI防火墙。

[0119] 图11示出了状态包检测(SPI)防火墙和深度包检测(DPI)防火墙之间的通信。该图示出了从端点设备(EPD)11-100到互联网11-002经由路径TUN 11-0到第一接入点服务器(SRV_AP)11-302到路由器到云防火墙负载平衡器(CFW LB)设备11-144LB，然后通过TUN 11-6到SRV_AP 11-304。从SRV_AP 11-304流量通过出口进入点(EIP)11-E2将GVN流出到互联网11-002。

[0120] EIP 11-E2是扩展LAN到GVN和互联网11-002之间云端的边缘。EIP可以连接到开放式互联网或组织的基于云的资产，该资产包括服务器、存储阵列和其他设备。它也可以是一个混合的公共-私有云的链接，如云端的DMZ或外围网络。

[0121] 通过SRV_AP 11-302的流量可以将流量或克隆流量转移到重复流中，并通过路径TUN 11-2传递到云负载平衡器11-142LB。克隆的流量流提供了时间和资源-诸如DPI等昂贵的检测操作的拖尾结果，而不会阻碍流量的流动。从互联网11-002返回到EPD 11-100的流量通过EIP 11-E2进入GVN的反向路径。

[0122] 对于基于互联网的流量，第一个周边是CFW 11-144LB，它通过路径11-CPSPO和11-CPSP2将数据包发送到状态包检测防火墙FW(SPI)11-SPO-PRO，其中包11-SPO-H的报头被检查。SPI防火墙提供快速流量通信，并且需要比DPI防火墙相对较低的资源。

[0123] 第二个周边为CFW 11-142LB，这是深度数据包检测防火墙FW(DPI)11-DPO-PRO可以检查一个或多个组合数据包的有效载荷11-DPO-P的位置。DPI防火墙提供更深入的分析。如果有效载荷显示问题，则可以注意来自标题的源、目标和其他信息。

[0124] 因此，SPI防火墙和DPI防火墙之间的通信非常有用。FW(SPI)11-SPO-PRO可以通过路径11-APFW-SP将实时检测的信息发送到云防火墙负载平衡器CFW 11-142LB，以提醒其通过标题检测检测到的任何威胁。除了共享检测到的违规报头(headers)之外，当向CFW 11-142LB和11-DPO-PRO传送信息时，还将包括有效载荷11-SPO-P。FW(DPI)11-DPO-PRO可以通过路径11-APFW-DP向云防火墙负载平衡器CFW-11144LB发送信息，以提醒其通过有效载荷检测检测到的任何威胁。它共享的信息也可以来自报头11-DPO-H，以便11-144LB和/或11-SPO-PRO的SPI防火墙检测操作可以将违规标题添加到其流量违例者列表中。

[0125] 图12示出了由全局虚拟网络(GVN)启用的云端的多计数器防火墙(MPFW)。GVN隧道12-TUNO在端点设备(EPD)12-100和靠近EPD12-100的接入点服务器(SRV_AP)12-300之间的互联网的顶部(OTT)上。

[0126] 在该示例实施例中指示的三个周边是12-M1，其表示客户端位置与其到互联网的链接之间的边界，12-M2是在紧邻SRV_AP 12-300的数据中心的云端的边界，12-M3则是与SRV_AP 12-300相同数据中心的另一个边界，或者位于紧邻SRV_AP 12-302的另一个位置，该位置可能在另一个区域。

[0127] 隧道12-TUN2类似于12-TUNO，但二者在一个方面是不同的，因为它连接可移动的个人端点设备(PEPD)12-130，并因此通过公共接入无线或有线连接到SRV_AP 12-300或其他网络集成到GVN中。PEPD12-130可能不如EPD 12-100那么强大，从而将处理操作转移到SRV_AP，如图14所示。

[0128] 每个SRV_AP 12-300和SRV_AP 12-302可以表示一个或多个SRV_AP设备,EPD 12-100和/或EPD 12-130可以经由一个或多个隧道同时连接。

[0129] 在该示例实施例中描述了三种类型的防火墙。本地防火墙FW本地12-442是防火墙的一个示例,客户端可以使用防火墙来保护其局域网(LAN)免受基于互联网的威胁。这通常位于EPD 12-100和LAN 12-000之间。本地防火墙本地12-442可能提供IP地址和端口阻塞、转发等功能。其他两种类型的防火墙如图所示是位于12-M3处的FW SPI12-446,其提供状态包检测(SPI),以及位于12-M2处的FW DPI 12-444,其提供深度包检测(DPI)。

[0130] SPI与DPI之间的差异与性能与可见性全面性的权衡有关。SPI检查数据包的报头,以查找格式不正确的信息或模式,或者将IP地址或端口或其他已知威胁列表中的信息与当前的数据包流相匹配。DPI作为其名称意味着更深入地查看整个数据包,并且在多部分多数据包传输的情况下,将会查看一系列数据包的编译,以便深入了解正在传输的数据。

[0131] 所有防火墙都可以配置为调查和应用规则到入站和出站流量,并提供其他相关功能。在许多情况下,使用诸如FW 12-442等传统防火墙,管理员必须选择SPI的效率与DPI的彻底性、资源和时间密集型要求。

[0132] GVN提供了在云端的各个点分发两种类型的数据包检测的机会。此外,GVN允许分布式防火墙彼此锁定操作,而不会阻碍流量的流动。

[0133] 通过将FW SPI 12-446定位在12-M3,通过EIP远程12-310与互联网12-302最接近的边缘,可以阻止来自已知源IP地址或识别的恶意头的大量攻击流量。交流从SRV_AP 12-302通过12-T10和12-T12返回到FW SPI 12-446。FW SPI 12-446可以是CFW负载平衡器(见图11),其具有足够的可用资源。12-M3的SRV_AP可以在具有大带宽(BW)容量的多源骨干网上。因此,在第一个周边,可以抓住攻击,保护GVN内的带宽。

[0134] 在下一个周边12-M2,FW DPI 12-444可以使所有业务流量通过或仅通过来自SRV_AP 12-300的12-T20接收克隆的业务副本,并且它可能会或不会通过12-T22返回业务。关键是DPI功能可以是拖尾指示器,允许某些流量通过但分析和记录结果。该FW DPI 12-444也可以是CFW,根据需要负载平衡,可根据需要提供可用的资源,以便在需要时应对大规模事件,而无需个人客户端在正常时间内管理或承担维护基础设施的成本负担。

[0135] 来自FW SPI 12-446和FW DPI 12-444的信息可以通过内部通信路径12-P6共享,内部通信路径12-P6可以由GVN的NAPIM通过GVN隧道、GVN反向信道或其他一个或多个通信通路运载。每个FW机制还与GVN的中央控制服务器(SRV_CNTRL)12-200共享信息。该信息可以中继到世界各地的其他FW SPI和FW DPI,以便可以在数据库或其他信息索引中提供攻击向量、源、有效载荷和其他相关信息,以便SPI和DPI FW可以具有参考反对。由于全球信息分配提供了一个附加的安全网,这样可以提高规模效率。

[0136] 在客户端LAN和云端捕获违规流量可保护客户端的最后一英里互联网连接免受不必要的流量饱和。将流量卸载到可扩展的CFW也为客户带来许多优势。

[0137] FW本地12-442可以是独立设备、在EPD 12-100内部运行的软件应用(APP)或其他类型的FW设备。FW SPI 12-446和FW DPI 12-444设备和相关设备(例如负载平衡器,云防火墙或其他设备)可以定制或者可以由其他供应商提供架构。这些设备必须能够接收和转发流量,识别威胁,最重要的是能够传达其威胁结果,并从其他设备接收威胁配置文件和其他信息。

[0138] 随着威胁数据的积累，可以对内容、模式、攻击向量和其他收集到的信息进行分析。该分析提供了一个将启发式分析应用于新的潜在威胁的基础。

[0139] 这些只能通过由安全隧道和通信路径连接的相关设备组成的GVN或类似网络的安全网络优化(SNO)服务来实现。

[0140] 图14示出了支持个人端点设备的云端的多边界防火墙(MPFW)。该图与图12相似，但是显示了便携设备，其将从移动位置钩入GVN，并且14-M1边界是个人区域网络PAN 14-010与GVN之间的边缘。

[0141] 该图显示了个人终端设备(PEPD)14-130的拓扑，其中一些连接和其它功能分布在云端。该图进一步描述了分布到云端的防火墙操作以及代表本地设备(如个人端点设备(PEPD)14-130)在云端执行的其他操作。在PEDP 14-130是比端点设备(EPD)更低功能和更便携的设备的地方，它仍然可以利用由GVN提供的个人区域网络连接优化，包括高级智能路由(ASR)、多边界防火墙等等。

[0142] 说明的关键点在于个人设备将对于处理能力的需求扩展到云端。驻留在PEPD上的模块包括用于处理器CPU 106、存储器RAM 108和网络接口NIC 102的硬件组件。操作系统是用于为系统软件系统SW 112和连接172模块提供平台的最小O/S110。该基本配置足以允许PEPD14-130在其与接入点服务器SRV_AP 14-300之间构建隧道14-TUN2。

[0143] SRV_AP 14-300硬件组件的组件部分用于处理器CPU 306、存储器RAM 308和网络接口NIC 302。操作系统O/S 310是比O/S110更为广泛的安装。O/S 310为系统软件系统SW312提供平台，并为SRV_AP14-300提供连接372模块。高级智能路由(ASR)350模块和其他模块370向SRV_AP 14-300和连接的PEPD-14-130提供功能。

[0144] PEPD 14-130可以依赖于隧道14-TUN2，能够承载流量，实现基于云的ASR、FW和其他操作功能。

[0145] 图15示出了GVN中自动化设备和防火墙协作和信息交换所需的模块。

[0146] EPD 100是端点设备。SRV_AP 300是位于目标目的地区域中的接入点服务器。SRV_CNTRL 200是可由EPD和SRV_AP以及可能支持图形目的地机制的其他设备访问的中央服务器。

[0147] 每个设备EPD 100，SRV_AP 200和SRV_CNTRL 300以列表、文件、数据库表和记录的形式以及其他方式将关于自身的信息存储在本地信息库中。该存储库还包含有关对等设备关系，存储日志以及其他相关操作信息的信息。SRV_CNTRL 200还具有额外的存储功能，其作用是向与其相关的其他设备和/或与其连接的对等设备提供信息，以评估当前状况，并提供集中控制式指导，如发布的服务器可用性列表和其他功能。中立的API机制(NAPIM)可以在设备和它们连接的对等体之间发送信息，也可以用于更新API本身。

[0148] SRV_CNTRL 200上的数据库充当用于其自身以及其他设备的集中式存储库的信息库。在许多地方，可以有许多不同的SRV_CNTRL200服务器作为多主机。每个数据库可以存储包括隧道信息、对等信息、交通信息、缓存信息和其他信息的某些信息。安全性和其他方面由每个设备独立管理，包括心跳功能、触发脚本和其他机制。

[0149] 该图另外分别示出了接入点服务器(SRV_AP)300、中央控制服务器(SRV_CNTRL)200和终点设备(EPD)100上的防火墙管理器D344、D244、D144。SRV_AP 300的FW管理器D344通过路径15-PA2与SRV_CNTRL200上的FW管理器D244进行通信。通过路径15-PA1向EPD的

100FW管理器D144提供信息，以从SRV_CNTRL 200的FW管理器D244接收信息。

[0150] 防火墙之间的命令和控制通信以及报告信息传输SPI 15-SPO-PRO和DPI 15-DPO-PRO分别通过路径15-BA44和15-BA42。

[0151] 在各种设备上的数据库B344、B244和D144中的FW信息的存储允许威胁是已知的，并且还可以考虑通过GVN的流量的路由决定。例如，在一个区域的主动攻击饱和骨干网的情况下，这可能对通过该路由的业务的加权具有不利影响，并且通过较不拥塞的路径的业务的影响来接收路由优先级。

[0152] 图16示出了GVN中设备到设备的信息交换。流量通过路径16-CP144从局域网(LAN)16-002到防火墙(FW)16-144设备，然后通过路径16-CP100从终端设备(EPD)16-100传输。EPD在互联网16-000至SRV_AP 16-302之间建立了隧道TUN 16-0(OTT)。

[0153] 包含有关EPD 16-100的信息的数据阵列16-144100通过路径16-APSP4和16-AP100共享给FW 16-144。包含关于FW 16-144的信息的数据阵列16-100144通过路径16-APSP4和16-AP144被共享给EPD16-100。在此示例中，EPD信息数组仅可通过LAN端口使用，而不能通过打开的WAN端口从外部获得。它可以通过TUN 16-0在GVN中的其他可信设备可用。

[0154] 关键在于说明一种设备自动识别自身到相关设备的方法，包括其硬件规格、软件版本、当前操作状态和其他相关信息等信息。

[0155] 图17示出了多边界防火墙与GVN中的其他系统的集成。信息战的行为总是发生。无论是民族国家、企业玩家、黑客还是其他角色，这些攻击是无情的，根据趋势，威胁正在增加。利用这里描述的拓扑，存在将由被动防火墙或其他这样的监控中间设备检测到的实时攻击的信息整合到由安全提供商公司或组织聚合和报告的互联网上的可能性。不论攻击的性质入侵、网络钓鱼攻击、企图窃取知识产权、DDoS攻击或其他已知或未知的威胁，关键是要保护网络。

[0156] 图17显示各种设备之间的请求/响应(REQ/RESP)API循环。这些信息循环可以共享诸如CFW-DPI 17-142LB或CFW-SPI 17-144LB之类的云防火墙学习关于流经SRV_CNTRL 17-200的流量的信息。信息循环可以通过将信息从SRV_CNTRL 17-200传递到云防火墙(如CFW-DPI 17-142LB或CFW-SPI 17-144LB)来共享其他地区的攻击信息。此外，存储在SRV_CNTRL 17-200上的数据库Db 17-B200中的信息还可以包含启发式模式、已知威胁的签名以及要共享的全球互联网监视源的信息。也可以通过路径17-GUI-AJAX，通过客户端17-018上的图形用户界面(GUI)，从EPD 17-100上的托管实例获得可见性。

[0157] 这种信息交换拓扑的灵活性还允许性能监控，用于基于云的可扩展使用防火墙资源的计费模块、系统管理和其他目的。

[0158] 图20类似于图18，并且示出了用于向终端设备(EPD)20-100和互联网20-002的信息流的设备的拓扑和连接性。

[0159] 流量从互联网20-002到出口入口点(EIP)20-E2，进入接入点服务器(SRV_AP)20-304，然后通过隧道TUN 20-6到云防火墙负载平衡器CFW 20-144LB。该负载平衡器在FW(SPI)20-SPO-PRO上分配状态数据包检测(SPI)防火墙资源。该SPI防火墙检查流经它的数据包的标题20-SPO-H信息。FW(SPI)20-SPO-PRO检测到的威胁信息存储在本地数据库Db 20-BS中，并通过通信路径20-APSP4共享给中央控制服务器(SRV_CNTRL)200。该信息存储在SRV_CNTRL的数据库Db B200上。在其他SPI防火墙上检测到的威胁信息通过通信路径20-

APSP4从SRV_CNTRL 200共享到FW(SPI)20-SPO-PRO。

[0160] CFW 20-144LB允许的流量通过TUN 20-4流向SRV_AP 20-302。在SRV_20-302,流量有两个选择-它可以直接通过TUN 20-0流向EPD,并将数据流的克隆副本通过TUN 20-2传输到云防火墙负载平衡器CFW 20-142LB。或者可以将非克隆流程转移到云防火墙负载平衡器CFW 20-142LB进行过滤和分析。

[0161] 该云防火墙负载平衡器CFW 20-142LB在FW(DPI)20-DPO-PRO上分配深度数据包检测(DPI)防火墙资源。该DPI防火墙检查流经它的一个或多个组合数据包的有效载荷20-DPO-P信息。由FW(DSPI)20-DPO-PRO检测到的威胁信息存储在数据库Db 20-BD中,并且还经由通信路径20-APDP4共享到中央控制服务器(SRV_CNTRL)200。该信息存储在SRV_CNTRL的数据库Db B200上。关于在其他DPI防火墙上检测到的威胁的信息通过通信路径20-APDP4从SRV_CNTRL 200共享到FW(DPI)20-DPO-PRO。

[0162] 如果允许,则网络流量然后通过TUN 20-0从SRV_AP 20-302流向EPD 20-100。

[0163] SPI和DPI云防火墙负载平衡器可以了解系统性威胁、远程区域的威胁、以及通过与SRV_CNTRL 200的通信获取各种其他信息,或者在某些情况下,它们可以通过直接路径(例如20-CPSPDP)相互通信。

[0164] 图21示出了基于图20的拓扑或类似的拓扑的多边界防火墙算法,其中存在用于各种类型的防火墙操作的多个周边。

[0165] Db FW威胁21-D122可以存储在每个设备上和/或传送到中央控制服务器(SRV_CNTRL),以备将来访问和使用。SPI操作在一个周边。DPI操作在相同的周边或另一个周边。SPI和DPI防火墙可以相互通信威胁,并基于已知的威胁,可以采取适当的步骤。

[0166] 在这个例子中,流量从21-000开始。如果检测到威胁,则会记录和分享威胁信息,并将违规的流量在21-944处进行黑洞(blackholed)处理。在21-900处,流量被视为干净的流量。

[0167] 图22示出了诸如云防火墙CFW 444和云防火墙负载平衡器设备CFW LB 440等防火墙设备的软件体系结构的逻辑视图、以及相关设备的堆栈中央控制服务器(SRV_CNTRL)200、接入点服务器(SRV_AP)300和端点设备(EPD)100。如图所示,软件和硬件可以分布在网络设备内并跨越不同的电路板、处理器、网络接口卡、存储器和存储器。

[0168] 设备的软件体系结构彼此非常相似,每个设备在其操作中的作用不同,还有一些不同的模块。

[0169] 每个设备的最低级别是存储器(RAM)S106,S206,S306,S406和处理器(CPU)S102,S202,S302,S402和网络接口(NIC)S108,S208,S308,S408。所有这些都在硬件级别。操作系统(O/S)S110,S210,S310,S410可以是LINUX系统或诸如Debian等的等效系统。操作系统的描述包括用于路由、托管、通信和其他系统级操作软件的数据包和配置。

[0170] 中央控制服务器(SRV_CNTRL)200,接入点服务器(SRV_AP)300和端点设备(EPD)包括全局虚拟网络(GVN)操作系统的系统软件层S112,S212,S312。在这里操作为定制命令、系统模块、管理器和其他组成部分,以及GVN的其他组件。GVN的每种类型的设备可以具有系统软件层的这些部分中的一些或全部或者取决于它们的角色的不同部分。

[0171] 数据库模块Db 120,220,320和托管模块122,222和322被配置在该示例实施例中,用于GVN的中性API机制(NAPIM)、图形用户界面(GUI)和其他服务器端脚本托管站点的监

听、发送、处理、存储，检索和其他相关的基础级操作。数据库120，220.202(Db)模块可以是MySQL或等效的，例如MariaDb和托管模块122，222和322可以是Apache和PHP脚本或其他类型的托管语言。命令行脚本也可以用Bash，C，PHP，Pearl，Python或其他语言编写。

[0172] 计费模块可以协作和共享信息，例如由消费模型计费的隧道流量消耗的数据量。计费模块ACC 132 232 332在EPD 100上操作，并且SRV_AP 300具有对应的计费模块。两者都可以通提供财务信息给汇报屏幕、付款表格、电子邮件报表和其他由GVN产生的财务数据。

[0173] SRV_CNTRL 200具有处理计费信息、隧道管理器信息和可由GVN内的各种设备使用的其他数据的存储库管理器238。存储库管理器238还通过GVN的中性API机制(NAPIM)来处理对等体信息、凭证和连接到其他API对等体的各个设备的其它信息的协调。

[0174] EPD 100具有API模块130，SRV_CNTRL具有API模块230，并且SRV_AP 300具有API模块330。为了简化说明该示例实施例，仅每个设备已经表达了一个API模块。实际上，根据GVN中的功能，设备可能具有组合的客户端和服务器角色。

[0175] SRV_CNTRL 200上的缓存管理器管理分布在GVN的许多设备上的各种链接缓存的主索引。EPD100上的压缩引擎136和SRV_AP 300上的336管理对存储在文件、DB表或流传输数据中的数据的压缩和解压缩。

[0176] EPD100上的高级智能路由(ASR)150模块通过GVN的路由处理从EPD 100到目的地的最佳出口点的路由。

[0177] SRV_AP 300上的远程读取机器人(Remote Fetcher BOT)311是地理目的地机制(Geo-D)的核心组成部分。

[0178] SRV_CNTRL 200上的DNS管理器254管理可以在各种GVN设备(例如EPD 100上的DNS154)上确定(seed)DNS服务器的主DNS索引。

[0179] SRV_CNTRL 200上的Logger管理器通过API调用将设备共享的本地日志和日志管理到知识库(Repository)。在该示例性实施例中的记录管理器增加了记录操作事件，API动作和事务的功能，并且记录器还具有用于GVN操作的各个方面的其他角色和过程。

[0180] EPD100上的本地缓存152和SRV_AP 300上的本地缓存352在本地缓存数据。

[0181] GVN管理器272在SRV_CNTRL 200上操作以控制在SRV_CNTRL200和GVN的其他设备上的系统的各种组件的操作。

[0182] 在SRV_AP 300上的EPD 100和354上的本地DNS服务器和缓存154允许缓存DNS查找以用于快速、本地检索。可以完全刷新DNS 154和354，清除单个项目或设置为在一定时间段之后删除的检索查找的超时。

[0183] 在EPD100上是作为Geo-D的组件的内容传送代理(CDA)158。SRV_AP 300是内容提取代理(CPA)358，也是Geo-D的组件。通过使用从远程地区设置(seeding)的DNS 354，CPA358与SRV_300上的BOT 311一起从该远程地区提取内容。CPA 358使用隧道、高速缓存和GVN的其他改进来将获取的内容发送到CDA 158。

[0184] EPD100和SRV_AP300上的连接管理器(未示出)管理在设备和其他设备到设备通信路径之间的隧道。SRV_CNTRL 200的压缩管理器在本地管理压缩，并且还与SRV_AP 300上的EPD 100，336上的压缩引擎136以及GVN的其他设备进行协调。使用ASR 150，Geo-D和其他元素对EPD坐标进行路由，用以管理流量路由。

[0185] SDB100、SDB200和SDB300中的数据库表的结构对于设备操作是等效的，而每个数据表的数据表特定于设备类型，每个设备都具有身份特定的设备。在SRV_CNTRL 200上，存储库数据库SDB202是存储所有设备的唯一信息的位置，并且存储库管理器238可以使用该信息来将API凭据、隧道信息或其他信息传送到设备。

[0186] 存储在每个设备数据库中的是关于设备本身及其对等伙伴、事务列表和队列数据以及其他信息的身份和API对等体信息。所描述的方法和数据库除了描述之外还有其他用途，但是为了简化说明，本示例仅涵盖了一些核心功能元素示例。

[0187] 云防火墙CFW 444包括基本防火墙软件S414，以及通用规则DPI、SPI、启发式扫描和其他功能S444。云防火墙负载平衡器设备CFW LB440包括防火墙平衡器软件S448，其可根据需要管理云端防火墙的流量和资源分配。

[0188] 除了终点设备(EPD)100之外，还可以使用接入点服务器(SRV_AP)300和中央控制服务器(SRV_CNTRL)200的第三方设备，只要它们具有能够通信加配置的凭证和其他信息以促进与其他设备的通信。在每个设备下面是可能在该设备的堆栈内运行的一些可能的组件，然而一些其他组件可以同时运行，这里没有描述。这些组件可以包括EPD100下的FW连接(Connectivity)S148，SRV_AP 300下的FW连接S348以及SRV_CNTRL 200下的FW管理器S244。连接和管理器模块用于与CFW444和CFW LB 440进行交互。管理器模块进行正在进行的FW分析并与全系统和地理位置不同的CFW和CFW LB设备通信有关已知的威胁。

[0189] 防火墙负载平衡器CFW LB 440到防火墙CFW 444的通信可以通过FW每个设备上的连接模块S434。这些连接模块可以处理数据流通道以及数据流的信息流、所检测的威胁和其他信息。

[0190] 设备到设备的通信可以通过API S130在EPD100上通过API S330上的中立API机制(参见国际专利申请PCT/IB 16/00110)，在SRV_AP 300上通过API S330，在SRV_CNTRL 200上通过APIS230和CFW_LB 440通过API S430。

[0191] 图23示出了经由中央控制服务器(SRV_CNTRL)23-200从防火墙(FW)到全局虚拟网络(GVN)中的各种设备的信息流。它还包括存储在本地设备中的信息相对于数据库(DB)表中的防火墙信息的性质，例如DB23-110上的23-4100，DB 23-300上的23-4300，23-2300上的23-4200，210以及在FW设备23-140上的23-4140中的日志。

[0192] 信息通过API请求23-P140REQ/23-P140RESP或等效的设备到设备信息共享从FW设备23-140报告给SRV_CNTRL 23-200。也可以通过路径23-P102，23-P302，23-P502或其他设备的其他路径从单个设备上向SRV_CNTRL报告。

[0193] SRV_CNTRL 23-200可以通过路径23-P100，23-P300，23-P500或其他直接路径向设备广播和/或发布FW相关信息。FW信息还可以通过来自设备23-260的请求/响应路径23-P260REQ和23-P260RESP的API呼叫提供。

[0194] 标志可以指示诸如“在该设备上检测到”，“在另一设备上检测到”等信息的来源，以及诸如“基于LAN的攻击到外部”，“基于WAN的攻击”，“来自野外的攻击“等等。

[0195] 存储的信息还可以包括签名、通过启发式分析已知和预测的结构、IP地址、病毒和/或恶意软件的代码模式和/或其他有害载荷、有问题的流量的行为特征、传播模式等。

[0196] SRV_CNTRL 23-200还可以利用算法分析信息，并根据威胁寿命、第一次和最后一次检测的时间、规模和攻击范围等来评估严重性，并确定历史和任何趋势。此分析考虑到主

动威胁、过去的威胁、威胁之间的关系(例如,网络钓鱼攻击如何导致打开网络到其他攻击的妥协)、互联网/网络当前的条件来分配威胁级别和其他指标来衡量攻击的强度。在相对安静的时间,FW可能更容许,导致更快的操作。在相对活跃的时期,FW可能更具限制性和分析性,导致潜在的较慢的吞吐和操作。

[0197] SRV_CNTRL23-200将FW信息保留在存储库存储库中,用于编目威胁类型、报告历史记录和包括威胁信息更新发布的记录设备交互。

[0198] 图24是描述用于分析流过防火墙、防火墙负载平衡器和/或通过防火墙阵列的流量的算法的流程图。对于流经的流量,第一步是评估是否存在当前正在发现的主动威胁24-100。这受到当前威胁状态24-140的影响,该状态是防火墙活动的滚动指标。

[0199] 如果没有检测到威胁并且当前的威胁状态正常,则FW规则应用于流量24-220,允许通过24-300。它仍然处于被动威胁模式24-524,然后在下一个启动FW周期24-000重新启动。

[0200] 如果检测到威胁,则通过路径24-P200流量流动,并且通过路径24-P210检查威胁图案24-210的列表。如果被认可,则是黑洞或隔离。违规流量记录在24-240。一旦当前威胁在24-534处理,防火墙将设置为主动威胁模式24-554,然后返回到开始FW周期24-000。

[0201] 如果威胁不被识别,则在在24-250处使用启发式威胁检测进行检查。如果没有检测到威胁,则通过24-P314进行跟踪,以在24-314处处理为假阳性。模式升级到主动威胁模式24-554,下一个周期从24-000开始。

[0202] 图25示出了处理和处理威胁的系统堆栈中的各个层。内存最低级别为内存25-102、25-202、25-302,以及CPU 25-106、CPU 25-206、CPU 25-306。该系统是从最底层构建的。

[0203] 设备的增量锁定是基于威胁的性质以及堆栈的深度。例如,安全应用(Secure-APP)25-140,25-240和25-340安全层保护该层以上的应用模块。这些管理某些模块的操作,但不必要影响深层逻辑。安全系统(Secure-Sys)25-124,25-224和25-324保护系统软件层,用于数据库操作,DNS,日志记录,缓存,托管和其他功能。安全操作系统(Secure-O/S)25-114,25-214和25-314保护操作系统免受威胁。安全硬件(Secure-HW)25-104,25-204和25-304保护硬件系统的物理层免受威胁,包括驱动程序文件,闪存指令集和其他系统。

[0204] 锁定层的层数越低,系统的功能越少。

[0205] 图26示出了在从HFS文件存储26-010检索系统文件26-110的引导过程中自动解密加密卷的方法。在引导启动过程26-100中的一个时刻,从HFS文件存储26-010检索密钥文件26-210。此密钥26-A由加密卷解锁模块26-200使用。加密卷解锁后,可以使用26-300。

[0206] 将密钥存储到HFS文件存储卷26-010上的加密卷有一个明显的缺点。因为这是黑客入侵系统,使用未加密的密钥来解锁安全卷。另一个威胁是那些采取物理驱动,并试图解密卷以窃取有价值的客户端数据和/或逆向工程系统访问存储在加密卷中的软件。

[0207] 图27示出了如何基于特定于该设备的多个因素来为设备一致地计算唯一用户标识(UUID)。硬件(HW)UUID 27-100(如CPU序列号,CPU型号,网络接口卡(NIC)的MAC地址等)通常对每个设备都是唯一的。硬件(HW)DMI编码27-200可以使用DMI值烧录,如序列号,版本号或其他DMI数据。也可以使用硬盘驱动器(HDD)或固态驱动器(SSD)27-300的唯一卷ID。还可以使用某些O/S的UUID27-500,这是构建系统所独有的。UUID和密钥作为存储在本地数据

库27-600中的身份表中的值也可以用作设备的身份的一部分。

[0208] 在应用程序级别,可以使用密钥文件、证书和其他标识符27-800形式的UUID来为设备本身生成特定的UUID。

[0209] 可以计算、使用和验证各种设备UUID,以确保设备的整体操作的真实性。各种因素的组合在难以接近设备的情况下难以接近不可能的欺骗。

[0210] 图28示出了安全引导机构的模块。端点设备(EPD)28-100与安全引导服务器(SRV_SB)28-500联系,并通过安全引导服务器拒绝的API-2A1-2A5呈现虚假数据包。然后,SRV_SB使用一系列挑战向EPD查询。成功通过一系列测试后,EPD上的安全引导管理器28-150允许通过SRV_SB上的安全引导侦听器28-552构建安全隧道TUN 28-100500。将设备证书28-138呈现给SRV_SB,以由安全启动管理器(Secure Boot Manager)28-550对存储在数据库28-B500或HFS存储28-H500中的值进行验证。

[0211] 通过所有的测试,是密钥和凭证管理器28-536发布的EPD 28-100上的加密卷的密钥,并通过TUN 28-100500安全地将该密钥传送到EPD 28-100。通过服务器可用性机制28-222,可通过API查询向中央控制服务器(SRV_CNTRL)28-200提供可用的SRV_SB服务器列表。

[0212] 图29示出了后通道机构的细节。端点设备(EPD)29-100接收可通过API调用API-29A1-29A2与中央控制服务器(SRV CNTRL)29-200连接的后向通道服务器(SRV_BC)的列表。服务器可用性29-220列表提供了EPD可以连接的当前可用的SRV_BC。该图显示了通过TUN 29-100500至SRV_BC029-500的三个并发连接,通过TUN 29-100502至SRV_BC2 29-502,以及通过TUN 29-100506至SRV_BC629-506。

[0213] 一旦安全性被BC安全性29-540,29-542和29-546清除,EPD 29-100上的后通道客户端29-510通过后向通道管理器29-510,29-512和29-516进行同时连接。这些设备还可以通过API调用,例如通过API-29A1-29A2或SRV_BC0通过API-29A2-29A50通过API-29A1-29A2或SRV BTR到SRV_CNTRL的API调用。

[0214] 有关在EPD和SRV_BC之间建立隧道的对等体对、凭证、认证、密钥和其他信息的信息可以通过这些API调用传递给SRV_CNTRL。此外,具有健康关系的已知对等体之间的状态消息可以通过API直接发送,例如通过API-29A1-29A52从EPD 29-100到SRV_BC2 29-502。

[0215] 这个例子是一个EPD同时连接到许多SRV_BC。主动隧道的目标是使得能够始终向命令行界面(CLI)登录到EPD的路径,而不管EPD是否在开放的互联网和/或网络上被发现。

[0216] 图30示出了许多端点设备(EPD)30-100,30-102和30-106与后向通道服务器(SRV_BC0)30-500之间的连接。当EPD启动连接到SRV_BC0 30-500上的登录空间时,登录的实例是EPD 30-100的系统安全隔离实例30-510,EPD 30-102的30-512,和30-516分别为EPD 30-106。每个孤立的实例都像一个系统监视器,其中登录的用户只能被限制为限制其动作、权利、权限以及其他方式在主机系统上的能力的有限命令。

[0217] 所以从EPD到SRV_BC0 30-500,除了保持两者之间的连接之外,还有很少的事可以做。但是,另一方面,客户端30-000可以登录到SRV_BC0,且在具有某些权限的情况下,可以有权访问一个或多个孤立的实例。从那里可以将隧道上的SSH反向登录到EPD 30-100上的远程命令行界面CLI30-110或EPD 30-102上的CLI 30-112或EPD 30-106上的CLI 30-116。这允许客户端30-000在其登录权限范围内执行管理任务、远程执行、运行测试和进行其他操作。客户端可以是人或自动设备。

[0218] 后渠道的优点是在EPD不可达时提供接入。由于隧道TUN 30-100500、30-102500和30-106500的性质，它们对丢包、抖动和其他因素的容忍度远高于其他形式的隧道和/或通信路径。因此，在网络不稳定的情况下，后台通道可以访问诊断和补救问题，否则这些问题将难以解决。

[0219] 图31示出了使用对于每一行唯一的旋转和计算的密钥将加密数据写入数据库的一行中的选定字段。

[0220] 此流程图需要连接到数据库，创建一行并获取相应的自动增量整数ROW_ID值。然后利用加密过程，随后使用一系列密钥、密钥调节器、行内的字段和其他因素来处理要加密的值。用于加密数据行的相同因子可用于解密。

[0221]

表格 1：具有旋转键的数据库和加密字段中的可变数据

#	用户_ID	密钥_Adj	ENC_A	ENC_B	Open_A	创建时间	Flag	Mod_Time
658	1	AA	S#&*S	A(*SD*	开放数据	1459164978	1	3/28/16 11:36:18
659	51	BT	DS*WS%	(*%SK	更开放	1459164978	0	3/28/16 11:36:18
660	2	DA	3#&SX&	#*&S&	开放数据	1459164979	1	3/28/16 11:36:19
661	1	HC	S#*(S(AZ	W#E*&	更开放	1459164979	2	3/28/16 11:36:19
662	36	QP	Va($#*A3	A7!D(#	数据	1459164980	1	3/28/16 11:36:20
663	1	AC	D#(sa01	S@!A*9	可读	1459164988	0	3/28/16 11:36:28

[0222] 上表中的每个水平行都有两个加密字段[ENC_A]和[ENC_B]。每个字段的关键是基于多个因素，基于一些开放字段[用户_ID]，[密钥_Adj]和[创建时间]，以及其他因素，如基本系统密钥，根据以下计算：

[0223] $密钥_{待计算}$＝用户$_{ID}$+基础$_{Key}$+密钥$_{Adjustor}$+时间$_{创建}$+其他$_{因素}$

[0224] 即使相同的用户ID在完全相同的第二个时间为ENC_A和ENC_B输入相同的值，则值将不同，因为行ID#的自动递增整数值(例如，在行号658、661、663处，[用户_ID]＝1)是关键计算的一部分。上面示例中的[密钥_Adj]或键调节器字段是两位数的alpha值，但可以是存储在该行中的其他数据。他们的关键点是，如果数据库的SQL被盗，从计算和时间的角度来说，破解是昂贵的。若破解这些值，整个代码库、SQL和环境都必须被窃取并被复制。

[0225] 图32示出了从单个行中使用键、键调节器和使用框架来计算键的其他因素的数据解密。

[0226] 图33示出当客户端33-000从端点设备(EPD)33-100请求的图形用户界面(GUI)内容和请求内容被存储在锁定的卷33-114内时，会发生什么。404错误处理程序33-144抛出并捕获未找到的404错误。在33-120处，产生到简化的内容的跳转。该内容存储在锁定卷外部，

该锁定卷可以是存储在开放HFS文件存储33-220中的文件或来自开放DB 33-210的数据库内容或两者的组合。

[0227] 如果安全卷被锁定，则只有安全卷之外的内容才可用。然而，如果安全卷被解锁，则安全内容33-120可以被使用，该安全内容33-120可以来自于安全DB 33-210或是存储在安全HFS文件存储33-220中的文件或两者的组合。

[0228] 所提供内容中的Javascript脚本也可以轮询EPD 33-100以检查安全卷的状态。如果它被锁定并已被解锁，则可以跳转到安全的内容。相反，如果卷被解锁并突然被锁定，则内容可以恢复到安全卷之外的内容。

[0229] 本公开不受本文描述的具体实施例的限制。实际上，除了本文所描述的那些之外，本公开的其他各种实施例和修改对于本领域普通技术人员来说将从前述描述和附图中变得显而易见。因此，这样的其他实施例和修改旨在落入本公开的范围内。此外，尽管本文已经在至少一个特定实施方式的至少一个特定实施方案的上下文中针对至少一个特定目的描述了本公开，但是本领域普通技术人员将认识到其可用性不限于此，并且本公开可以在任何数量的环境中有益地实现用于任何数量的目的。因此，下面阐述的权利要求应当考虑到本文所述的本公开的全部宽度和精神来解释。

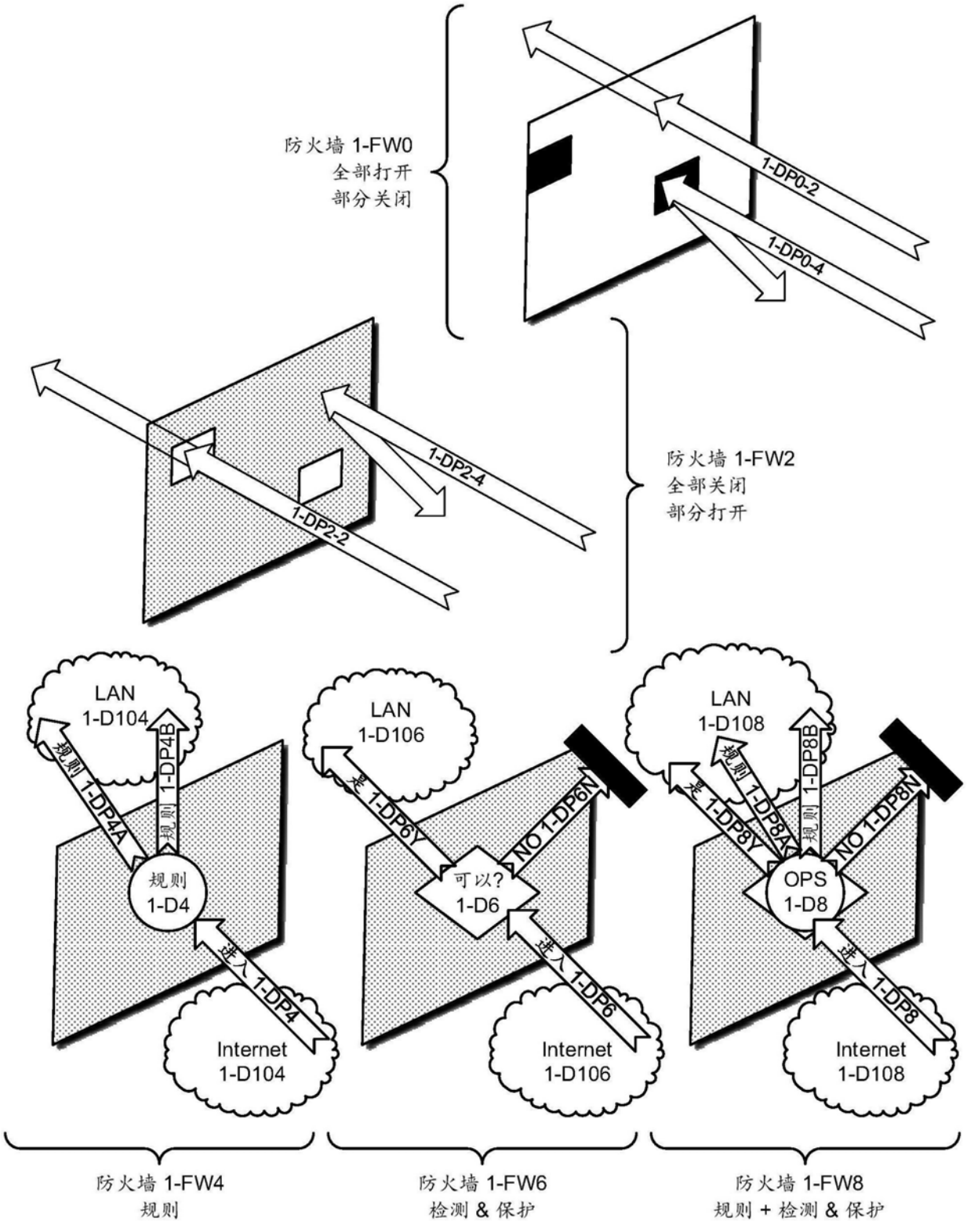

防火墙 1-FW0
全部打开
部分关闭
1-DP0-2
1-DP0-4
防火墙 1-FW2
全部关闭
部分打开
1-DP2-4
1-DP2-2
LAN
1-D104
规则 1-DP4A
规则 1-DP4B
规则
1-D4
进入 1-DP4
Internet
1-D104
LAN
1-D106
是 1-DP6Y
NO 1-DP6N
可以?
1-D6
进入 1-DP6
Internet
1-D106
LAN
1-D108
是 1-DP8Y
规则 1-DP8A
规则 1-DP8B
NO 1-DP8N
OPS
1-D8
进入 1-DP8
Internet
1-D108
防火墙 1-FW4
规则
防火墙 1-FW6
检测 & 保护
防火墙 1-FW8
规则 + 检测 & 保护

图1

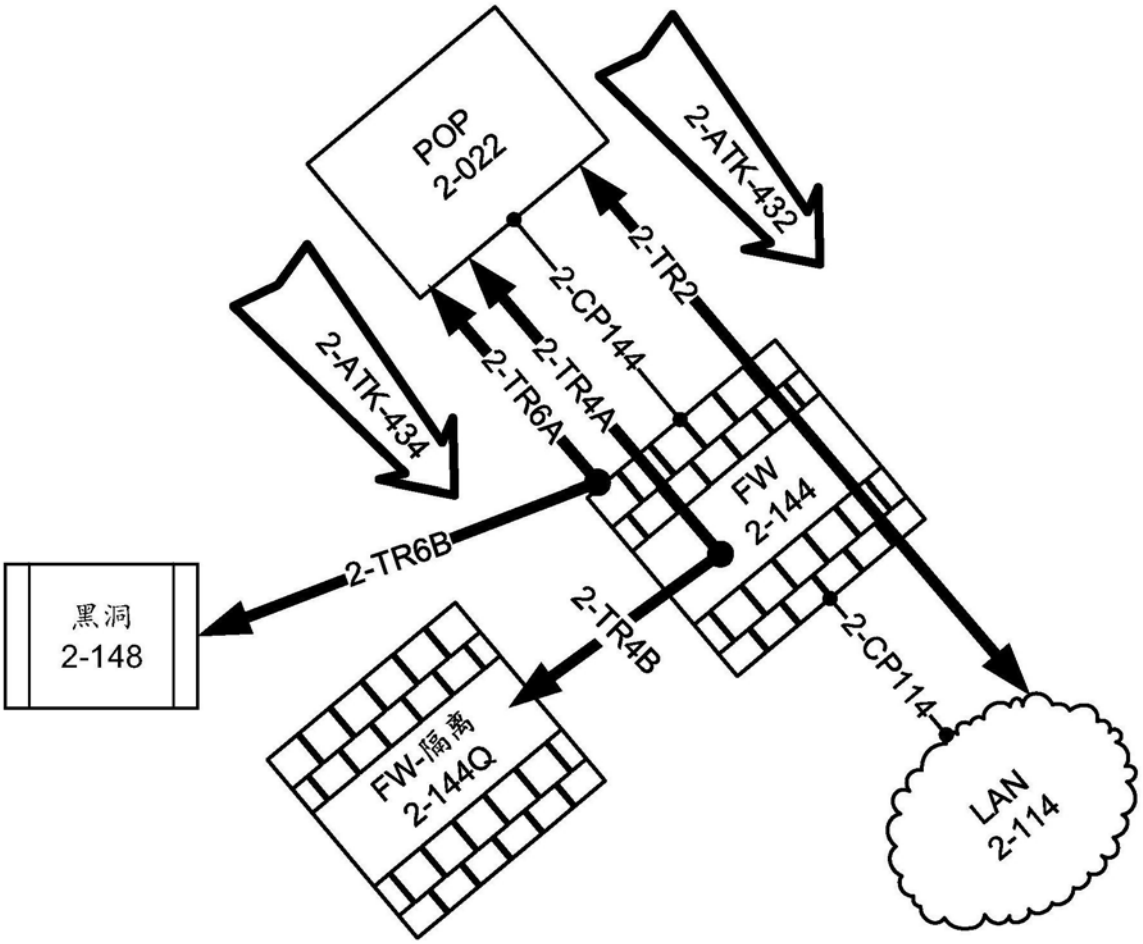

POP
2-022
2-ATK-432
2-ATK-434
2-TR2
2-CP144
2-TR4A
2-TR6A
FW
2-144
2-TR6B
黑洞
2-148
2-TR4B
2-CP114
FW-隔离
2-144Q
LAN
2-114

图2

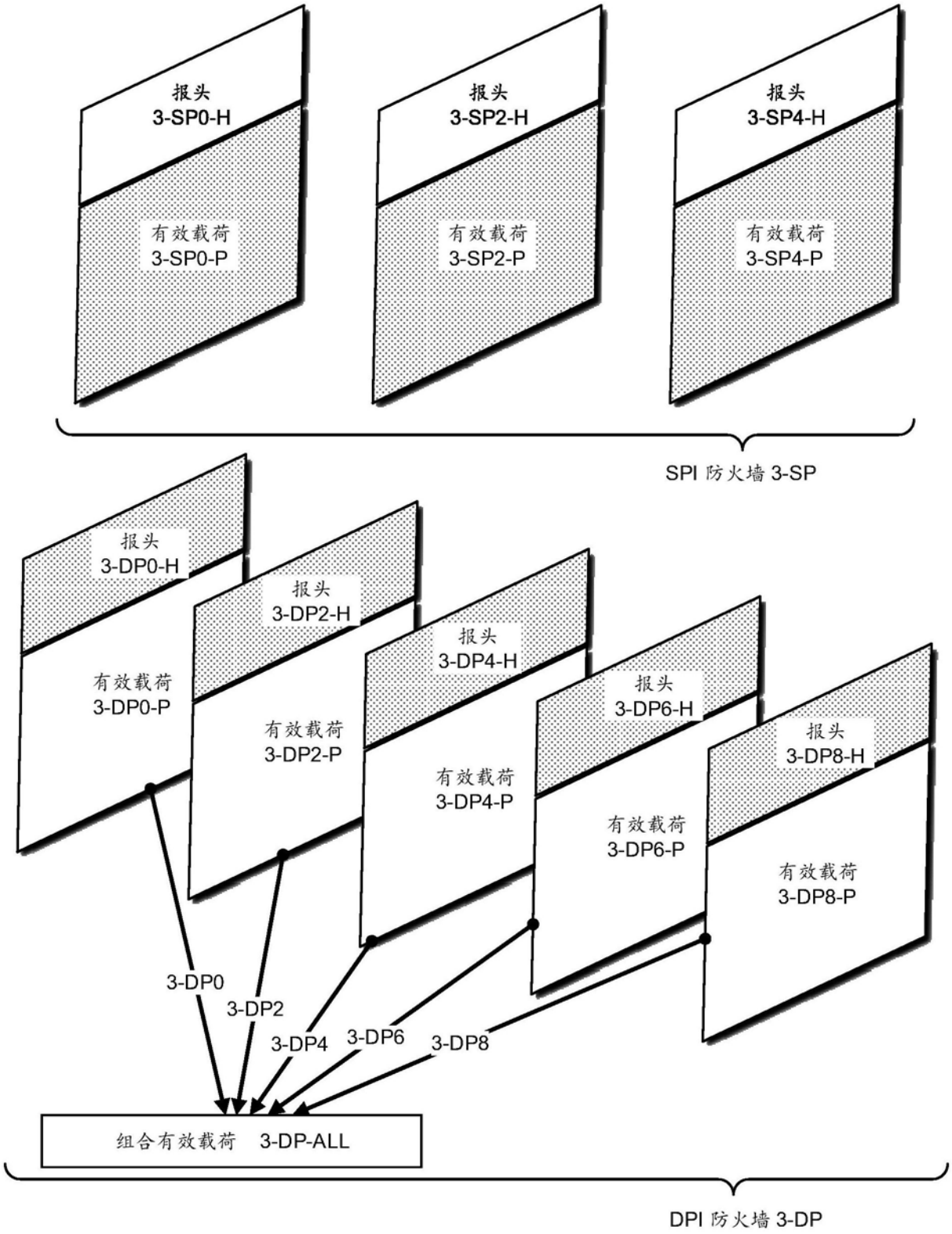

报头
3-SP0-H
有效载荷
3-SP0-P
报头
3-SP2-H
有效载荷
3-SP2-P
报头
3-SP4-H
有效载荷
3-SP4-P
SPI 防火墙 3-SP
报头
3-DP0-H
有效载荷
3-DP0-P
报头
3-DP2-H
有效载荷
3-DP2-P
报头
3-DP4-H
有效载荷
3-DP4-P
报头
3-DP6-H
有效载荷
3-DP6-P
报头
3-DP8-H
有效载荷
3-DP8-P
3-DP0
3-DP2
3-DP4
3-DP6
3-DP8
组合有效载荷 3-DP-ALL
DPI 防火墙 3-DP

图3

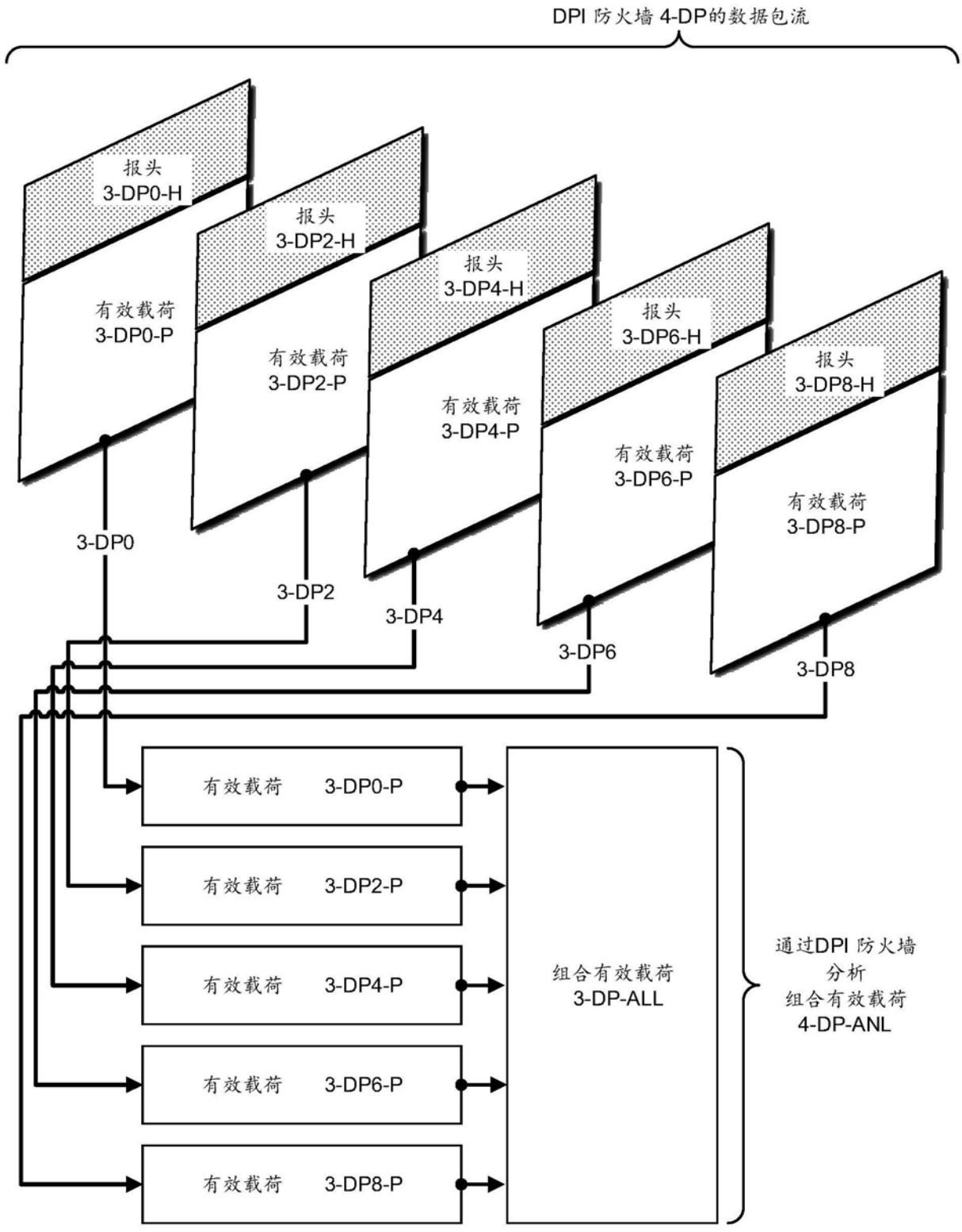

DPI 防火墙 4-DP的数据包流
报头
3-DP0-H
有效载荷
3-DP0-P
报头
3-DP2-H
有效载荷
3-DP2-P
报头
3-DP4-H
有效载荷
3-DP4-P
报头
3-DP6-H
有效载荷
3-DP6-P
报头
3-DP8-H
有效载荷
3-DP8-P
3-DP0
3-DP2
3-DP4
3-DP6
3-DP8
有效载荷 3-DP0-P
有效载荷 3-DP2-P
有效载荷 3-DP4-P
有效载荷 3-DP6-P
有效载荷 3-DP8-P
组合有效载荷
3-DP-ALL
通过DPI 防火墙
分析
组合有效载荷
4-DP-ANL

图4

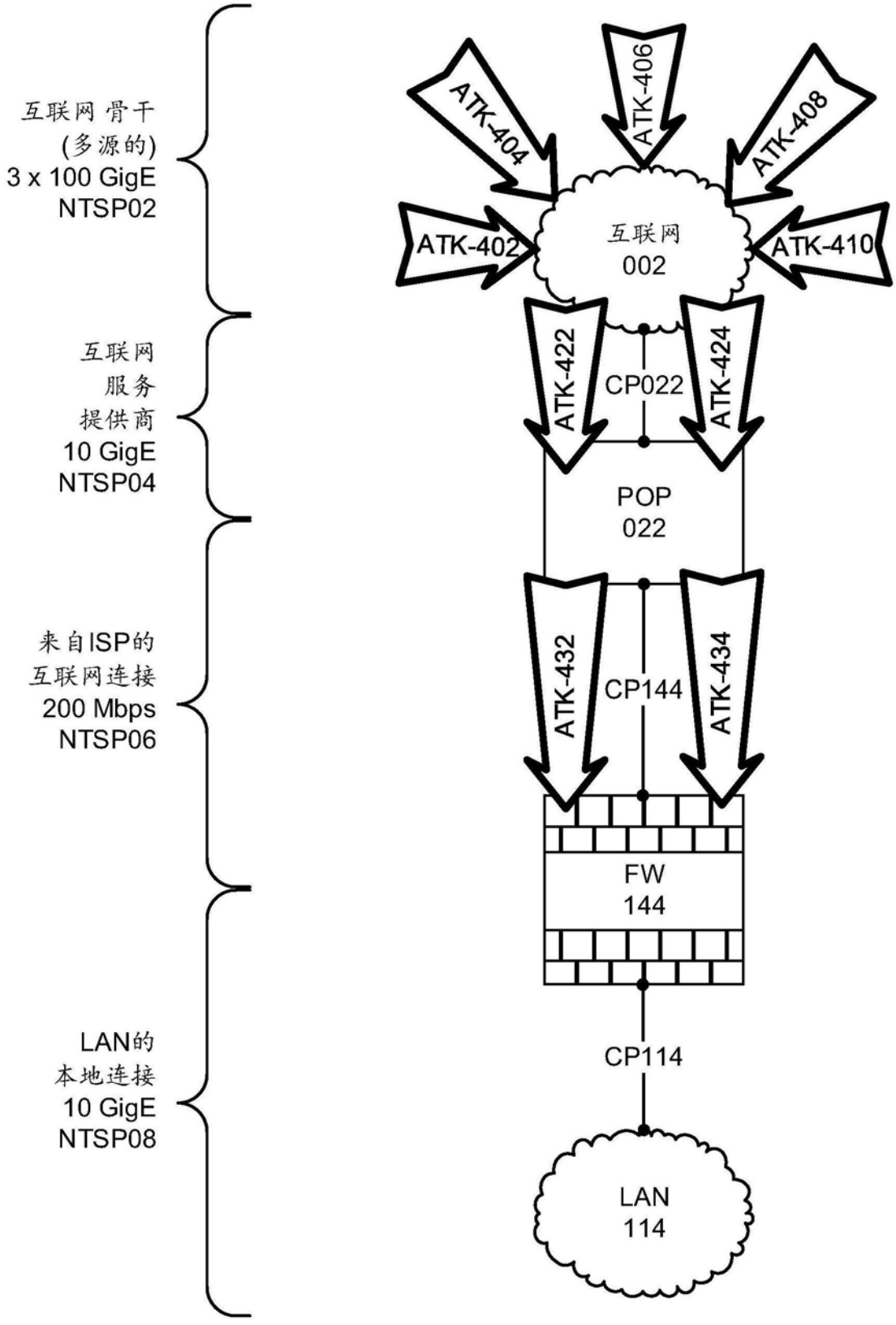

互联网 骨干
(多源的)
3 x 100 GigE
NTSP02
互联网
服务
提供商
10 GigE
NTSP04
来自ISP的
互联网连接
200 Mbps
NTSP06
LAN的
本地连接
10 GigE
NTSP08
ATK-404
ATK-406
ATK-408
ATK-402
互联网
002
ATK-410
ATK-422
CP022
ATK-424
POP
022
ATK-432
CP144
ATK-434
FW
144
CP114
LAN
114

图5

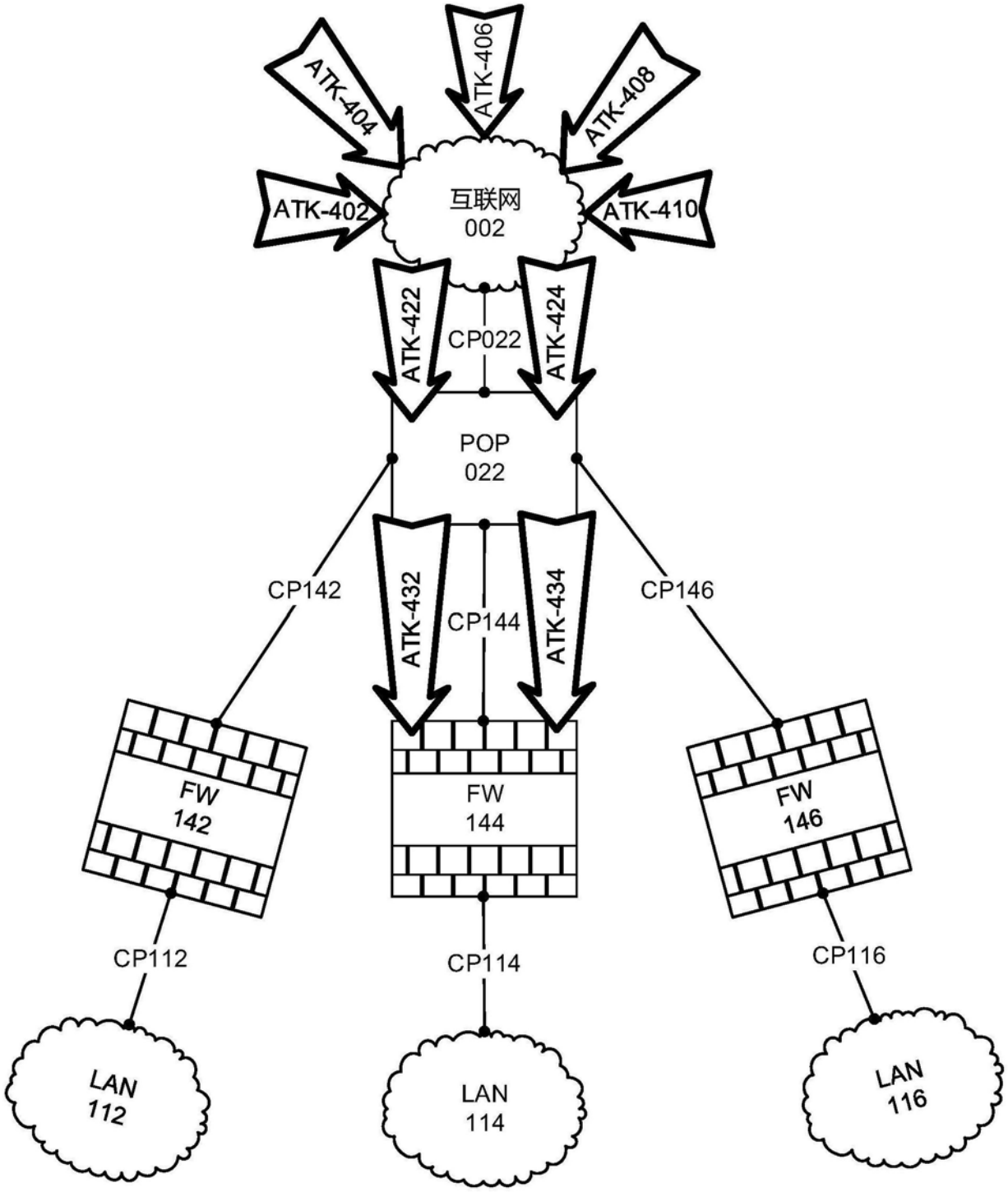

ATK-404
ATK-406
ATK-408
ATK-402
互联网
002
ATK-410
ATK-422
CP022
ATK-424
POP
022
CP142
ATK-432
CP144
ATK-434
CP146
FW
142
FW
144
FW
146
CP112
CP114
CP116
LAN
112
LAN
114
LAN
116

图6

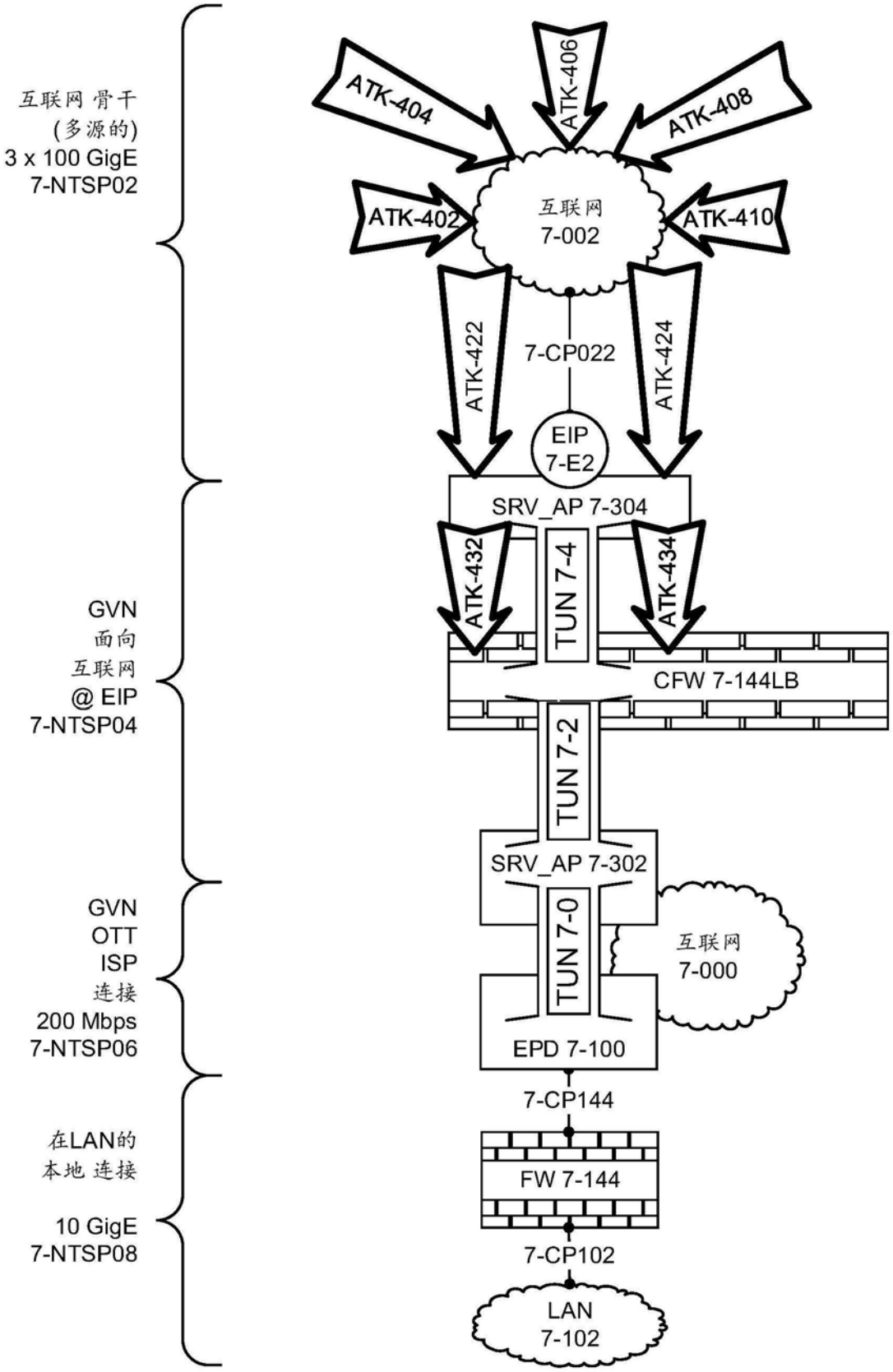

互联网 骨干
(多源的)
3 x 100 GigE
7-NTSP02
GVN
面向
互联网
@ EIP
7-NTSP04
GVN
OTT
ISP
连接
200 Mbps
7-NTSP06
在LAN的
本地 连接
10 GigE
7-NTSP08
ATK-404
ATK-406
ATK-408
ATK-402
ATK-410
互联网
7-002
ATK-422
7-CP022
ATK-424
EIP
7-E2
SRV_AP 7-304
ATK-432
TUN 7-4
ATK-434
CFW 7-144LB
TUN 7-2
SRV_AP 7-302
TUN 7-0
互联网
7-000
EPD 7-100
7-CP144
FW 7-144
7-CP102
LAN
7-102

图7

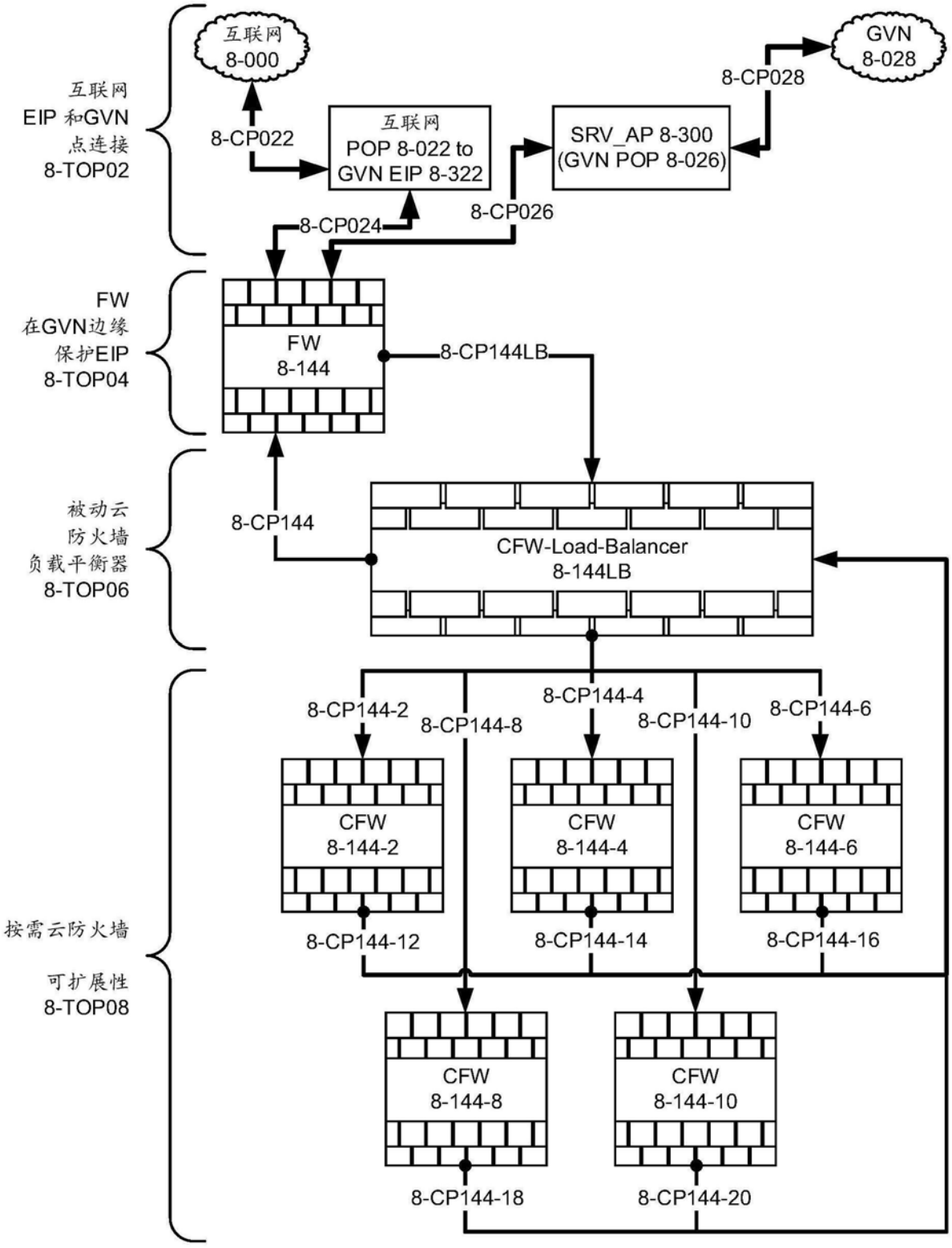

互联网
8-000
GVN
8-028
8-CP028
互联网
EIP 和GVN
点连接
8-TOP02
8-CP022
互联网
POP 8-022 to
GVN EIP 8-322
SRV_AP 8-300
(GVN POP 8-026)
8-CP026
8-CP024
FW
在GVN边缘
保护EIP
8-TOP04
FW
8-144
8-CP144LB
被动云
防火墙
负载平衡器
8-TOP06
8-CP144
CFW-Load-Balancer
8-144LB
8-CP144-2
8-CP144-8
8-CP144-4
8-CP144-10
8-CP144-6
CFW
8-144-2
CFW
8-144-4
CFW
8-144-6
8-CP144-12
8-CP144-14
8-CP144-16
按需云防火墙
可扩展性
8-TOP08
CFW
8-144-8
CFW
8-144-10
8-CP144-18
8-CP144-20

图8

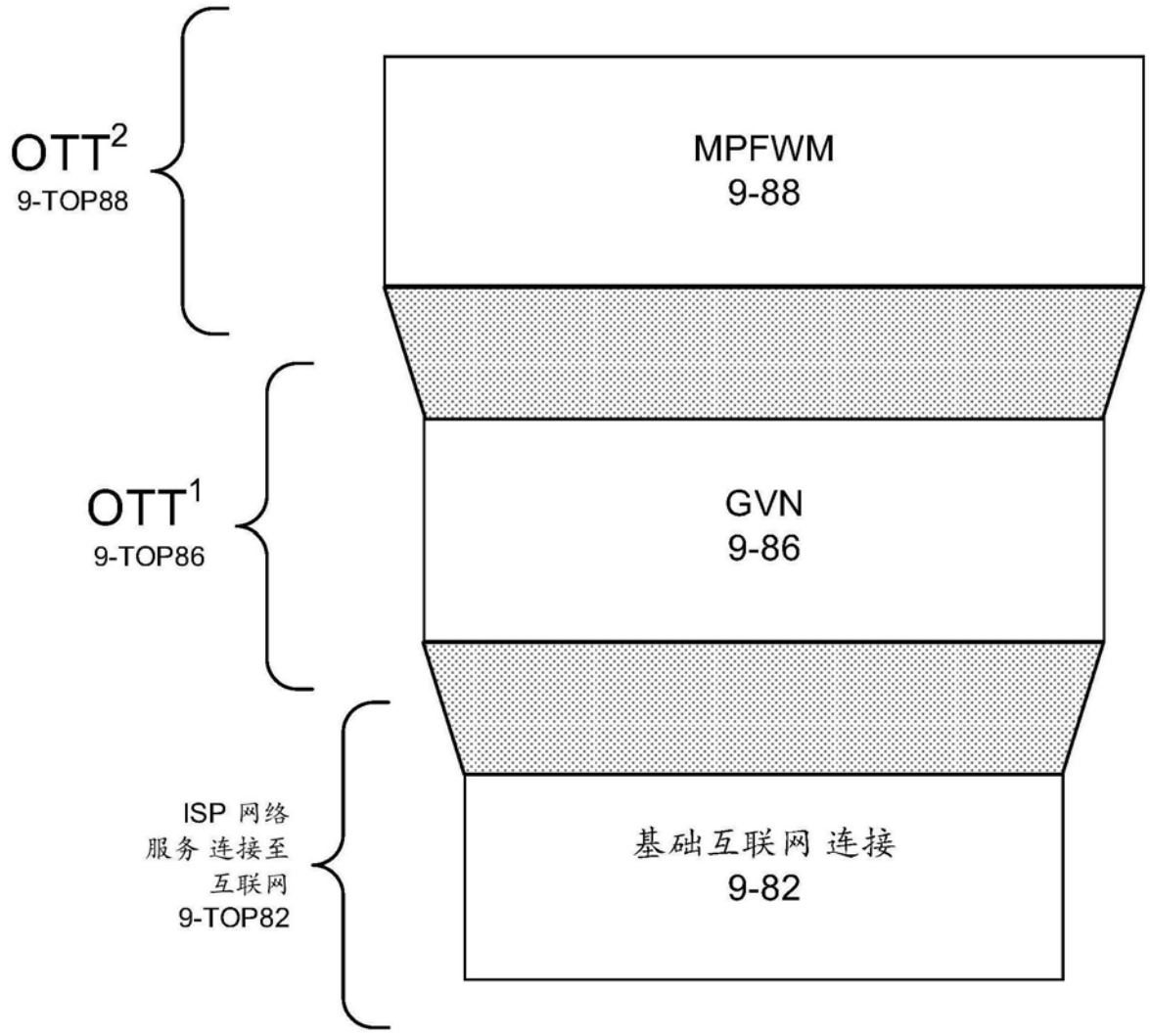

OTT2
9-TOP88
MPFWM
9-88
OTT1
9-TOP86
GVN
9-86
ISP 网络
服务 连接至
互联网
9-TOP82
基础互联网 连接
9-82

图9

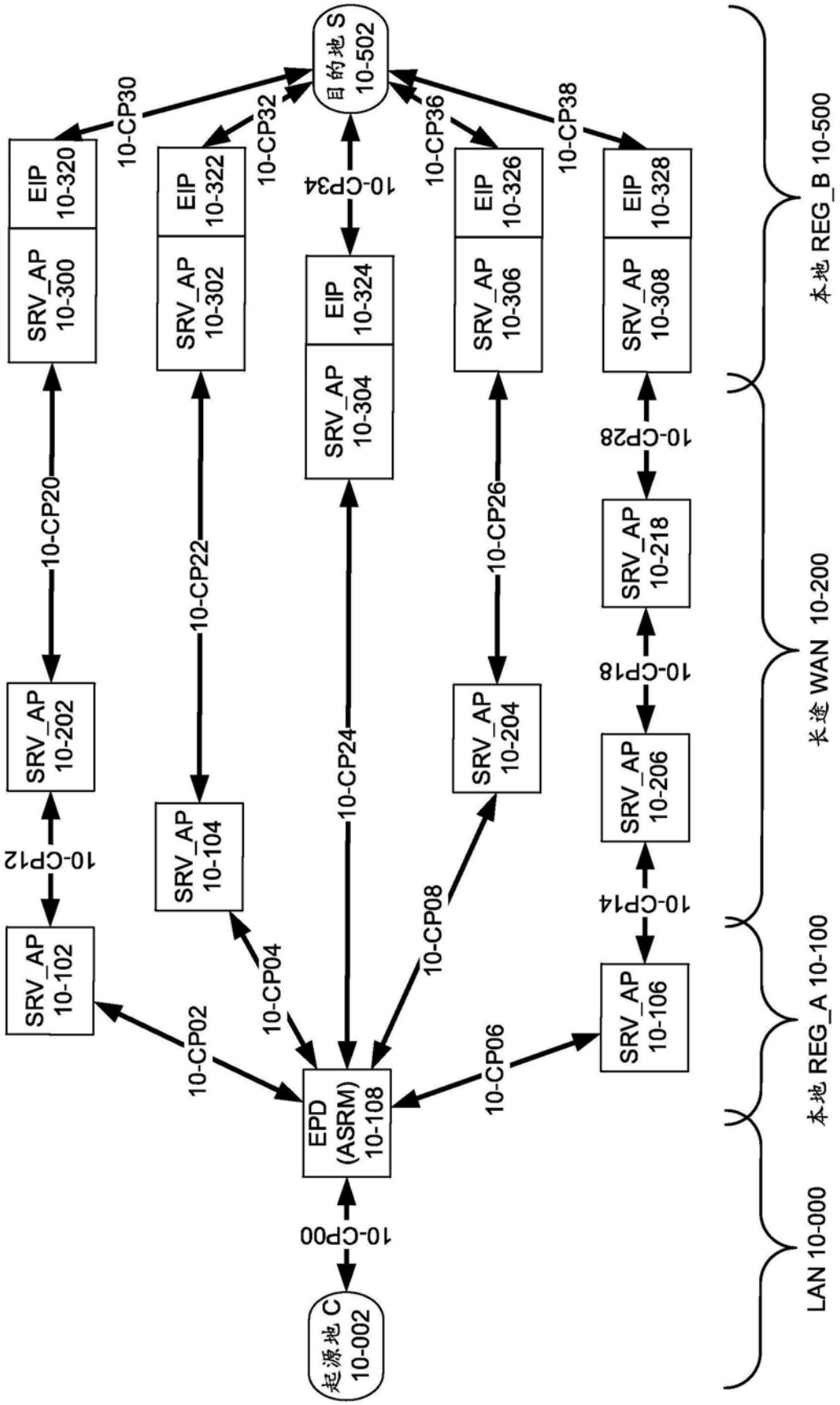

目的地 S
10-502
起源地 C
10-002
EPD
(ASRM)
10-108
SRV_AP
10-102
SRV_AP
10-104
SRV_AP
10-106
SRV_AP
10-202
SRV_AP
10-204
SRV_AP
10-206
SRV_AP
10-218
SRV_AP
10-300
SRV_AP
10-302
SRV_AP
10-304
SRV_AP
10-306
SRV_AP
10-308
EIP
10-320
EIP
10-322
EIP
10-324
EIP
10-326
EIP
10-328
10-CP00
10-CP02
10-CP04
10-CP06
10-CP08
10-CP12
10-CP14
10-CP18
10-CP20
10-CP22
10-CP24
10-CP26
10-CP28
10-CP30
10-CP32
10-CP34
10-CP36
10-CP38
LAN 10-000
本地 REG_A 10-100
长途 WAN 10-200
本地 REG_B 10-500

图10

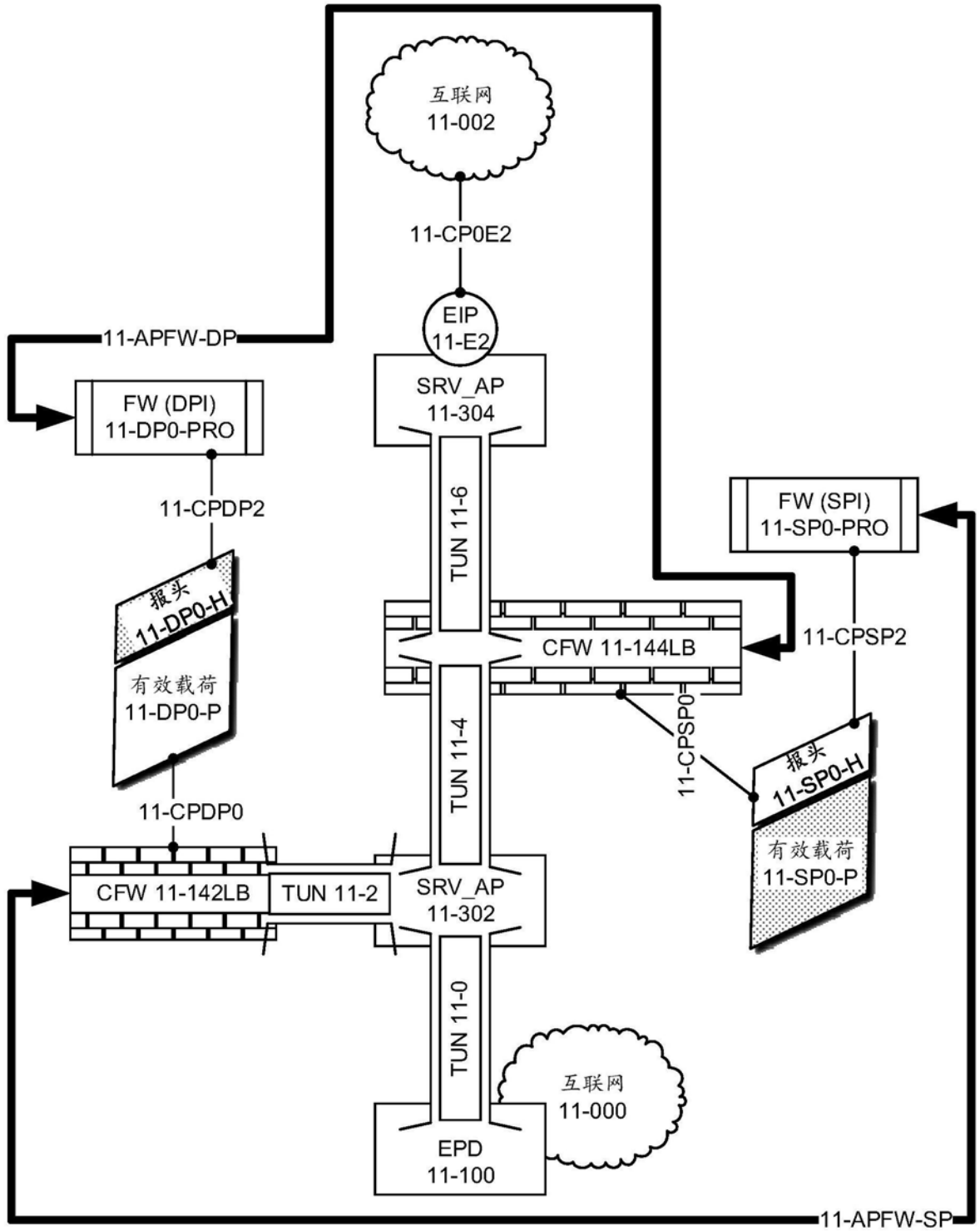

互联网
11-002
11-CP0E2
EIP
11-E2
11-APFW-DP
FW (DPI)
11-DP0-PRO
SRV_AP
11-304
TUN 11-6
FW (SPI)
11-SP0-PRO
11-CPDP2
报头
11-DP0-H
有效载荷
11-DP0-P
CFW 11-144LB
11-CPSP2
TUN 11-4
11-CPSP0
报头
11-SP0-H
有效载荷
11-SP0-P
11-CPDP0
CFW 11-142LB
TUN 11-2
SRV_AP
11-302
TUN 11-0
互联网
11-000
EPD
11-100
11-APFW-SP

图11

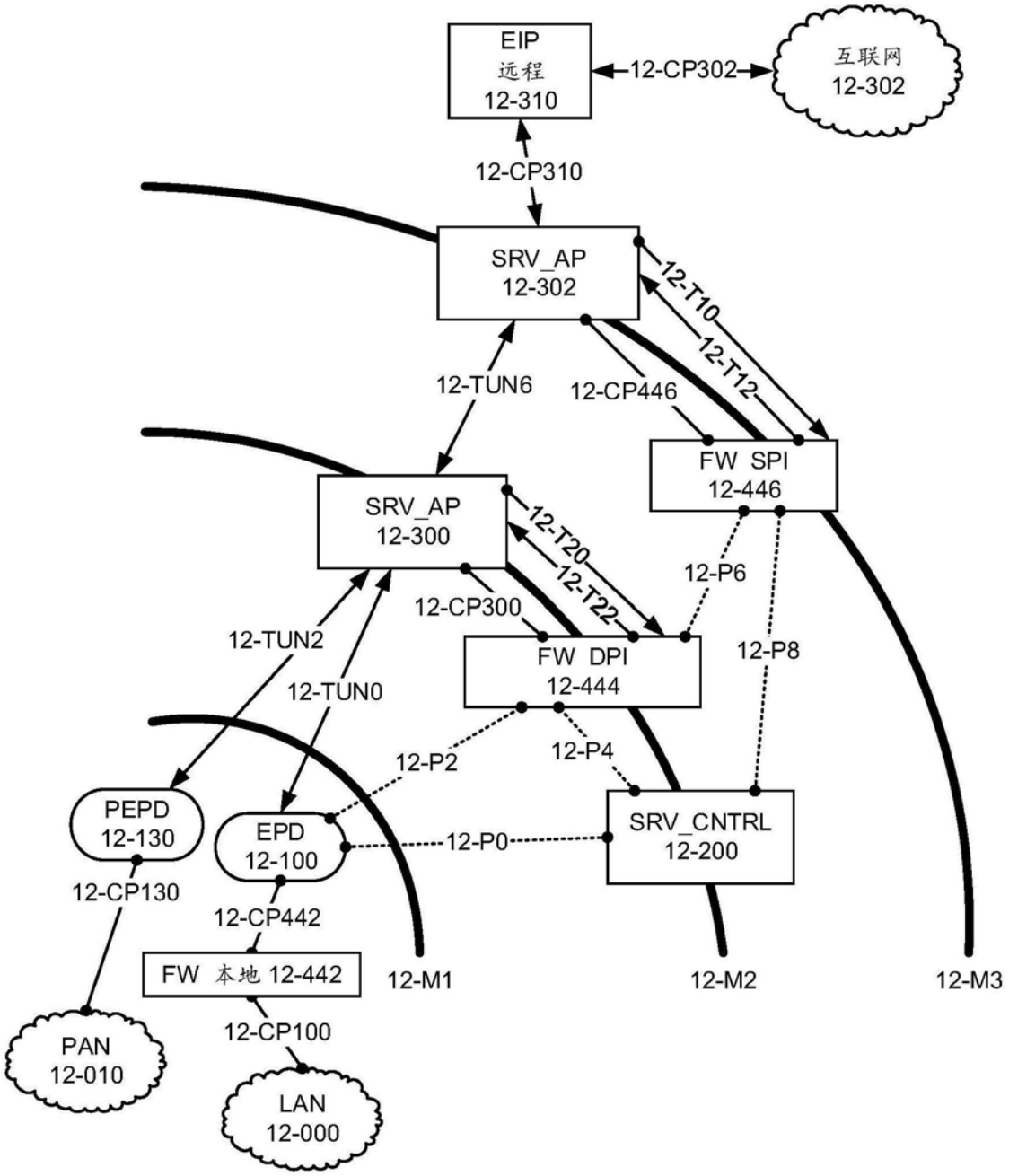

EIP
远程
12-310
12-CP302
互联网
12-302
12-CP310
SRV_AP
12-302
12-T10
12-T12
12-TUN6
12-CP446
FW SPI
12-446
SRV_AP
12-300
12-T20
12-T22
12-P6
12-CP300
12-TUN2
12-TUN0
FW DPI
12-444
12-P8
12-P2
12-P4
PEPD
12-130
EPD
12-100
12-P0
SRV_CNTRL
12-200
12-CP130
12-CP442
FW 本地 12-442
12-M1
12-M2
12-M3
PAN
12-010
12-CP100
LAN
12-000

图12

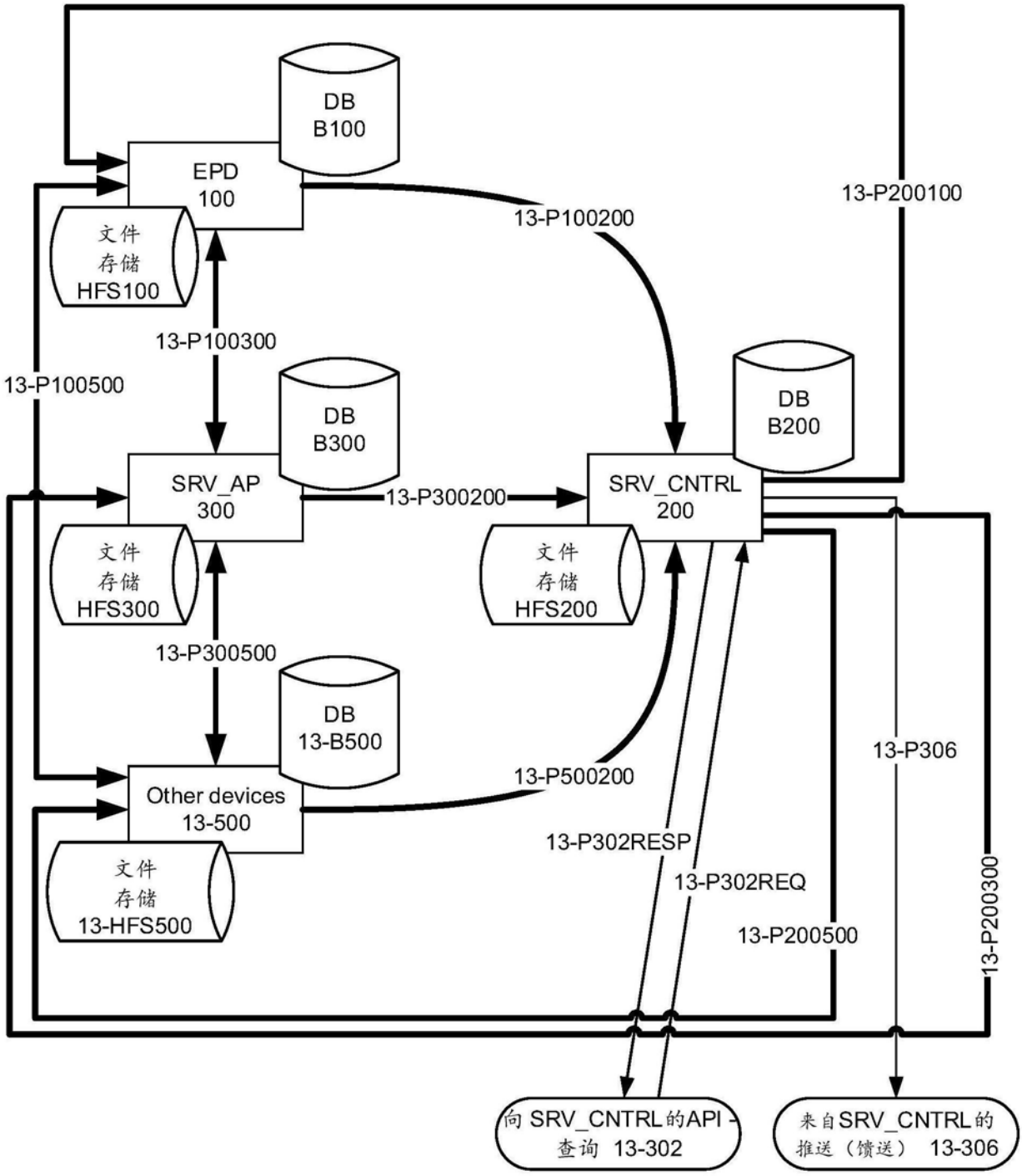

DB
B100
EPD
100
文件
存储
HFS100
13-P100200
13-P200100
13-P100300
13-P100500
DB
B300
DB
B200
SRV_AP
300
13-P300200
SRV_CNTRL
200
文件
存储
HFS300
文件
存储
HFS200
13-P300500
DB
13-B500
13-P306
13-P500200
Other devices
13-500
13-P302RESP
13-P302REQ
文件
存储
13-HFS500
13-P200500
13-P200300
向 SRV_CNTRL的API -
查询 13-302
来自SRV_CNTRL的
推送（馈送） 13-306

图13

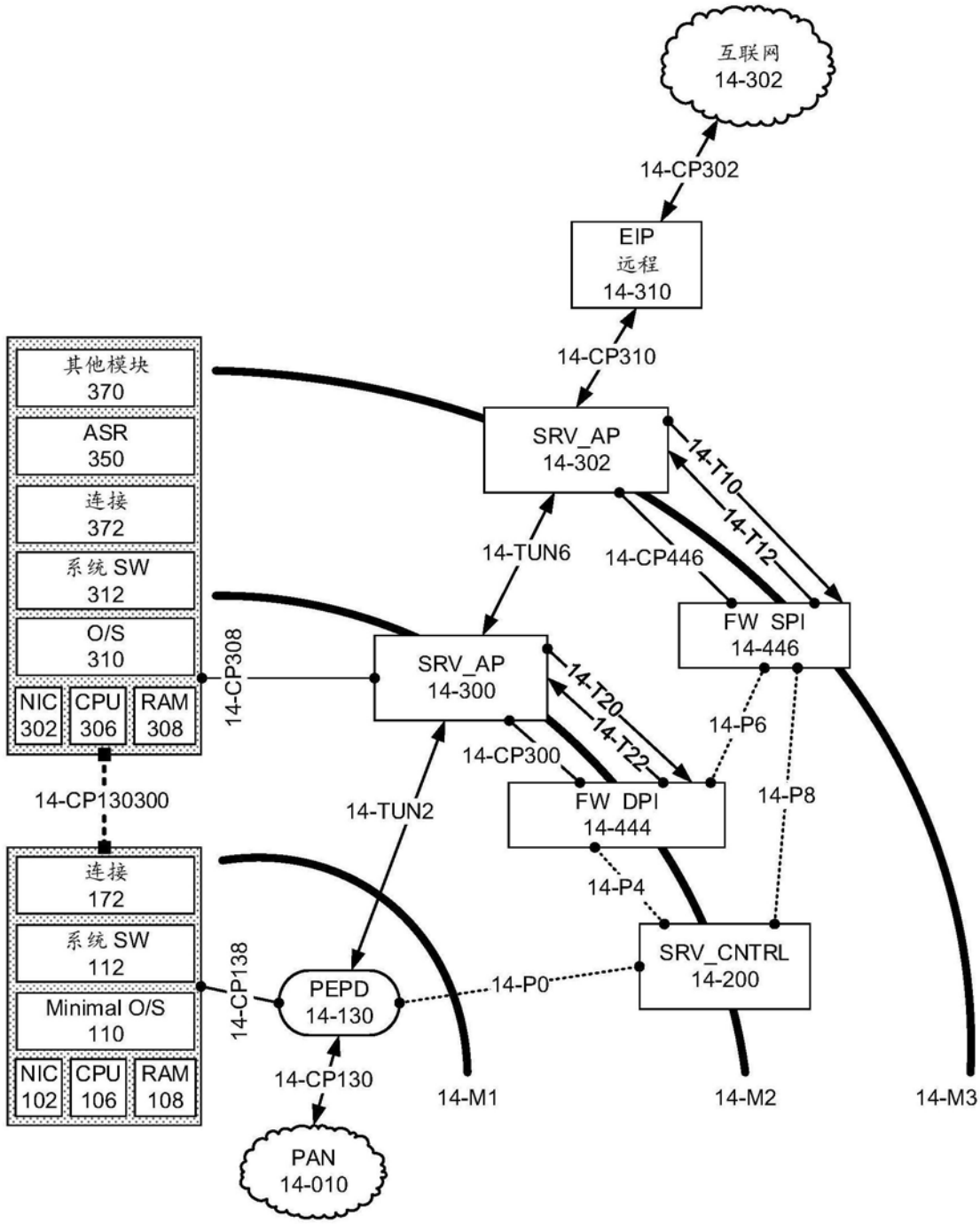

互联网
14-302
14-CP302
EIP
远程
14-310
14-CP310
其他模块
370
ASR
350
连接
372
系统 SW
312
O/S
310
NIC
302
CPU
306
RAM
308
14-CP308
SRV_AP
14-302
14-T10
14-T12
14-TUN6
14-CP446
FW SPI
14-446
SRV_AP
14-300
14-T20
14-T22
14-P6
14-CP300
14-CP130300
14-TUN2
FW DPI
14-444
14-P8
14-P4
连接
172
系统 SW
112
Minimal O/S
110
NIC
102
CPU
106
RAM
108
14-CP138
PEPD
14-130
14-P0
SRV_CNTRL
14-200
14-CP130
14-M1
14-M2
14-M3
PAN
14-010

图14

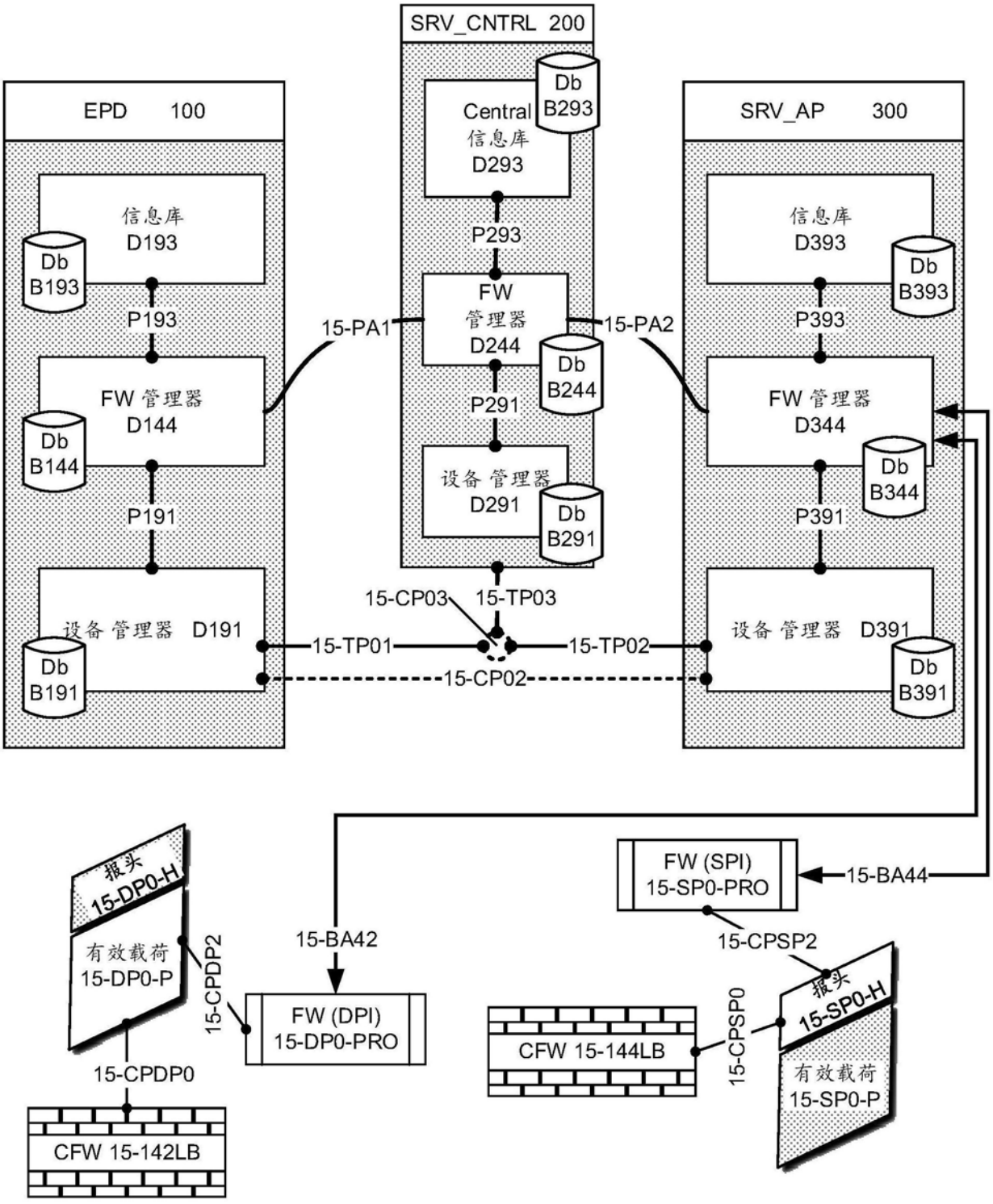

SRV_CNTRL 200
EPD 100
SRV_AP 300
Central 信息库 D293
Db B293
信息库 D193
Db B193
P193
FW 管理器 D144
Db B144
P191
设备 管理器 D191
Db B191
15-PA1
FW 管理器 D244
Db B244
P293
P291
设备 管理器 D291
Db B291
15-PA2
信息库 D393
Db B393
P393
FW 管理器 D344
Db B344
P391
设备 管理器 D391
Db B391
15-CP03
15-TP03
15-TP01
15-TP02
15-CP02
报头 15-DP0-H
有效载荷 15-DP0-P
15-CPDP2
15-CPDP0
CFW 15-142LB
15-BA42
FW (DPI) 15-DP0-PRO
FW (SPI) 15-SP0-PRO
15-BA44
15-CPSP2
CFW 15-144LB
15-CPSP0
报头 15-SP0-H
有效载荷 15-SP0-P

图15

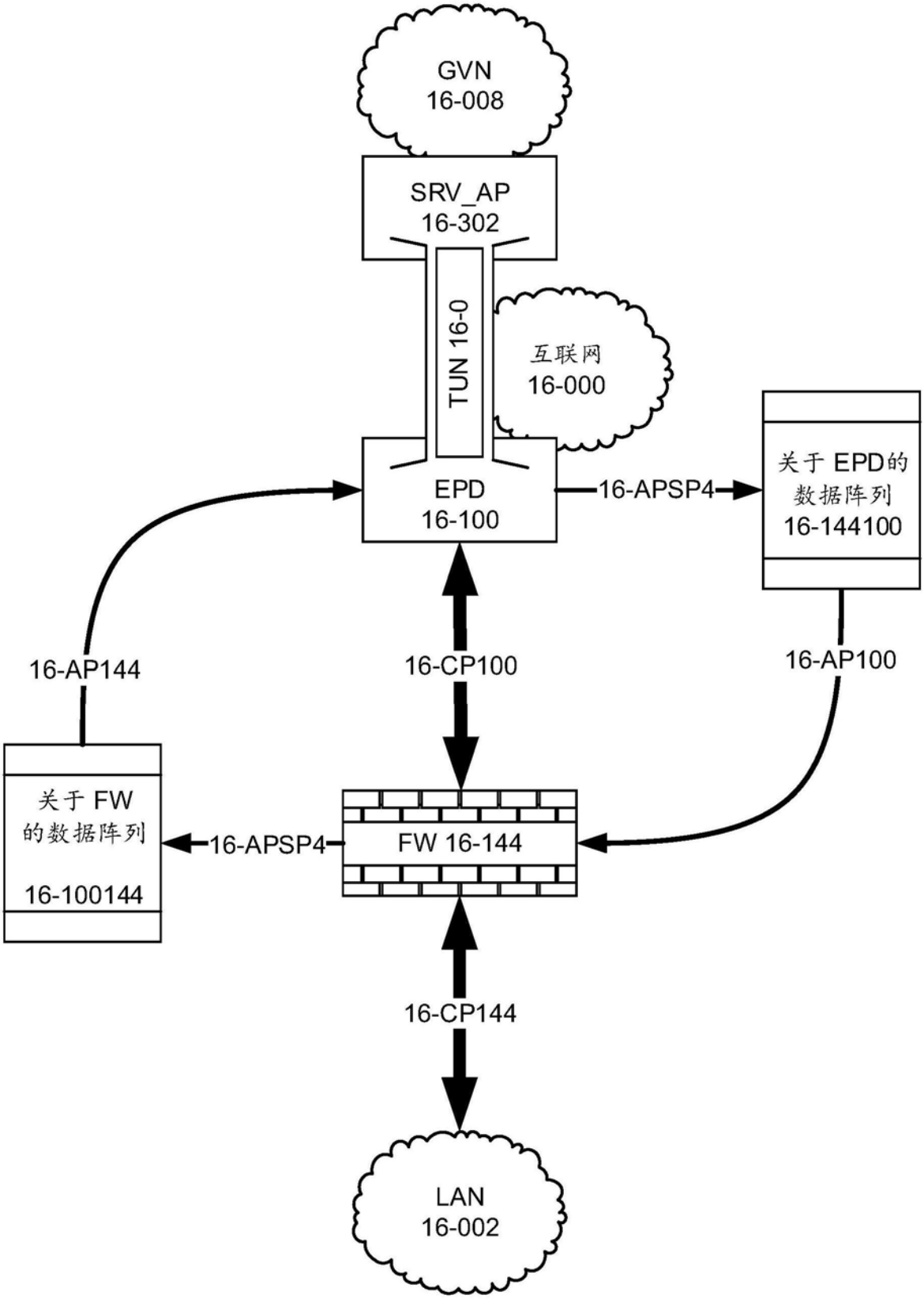

GVN
16-008
SRV_AP
16-302
TUN 16-0
互联网
16-000
EPD
16-100
16-APSP4
关于 EPD的
数据阵列
16-144100
16-AP144
16-CP100
16-AP100
关于 FW
的数据阵列
16-100144
16-APSP4
FW 16-144
16-CP144
LAN
16-002

图16

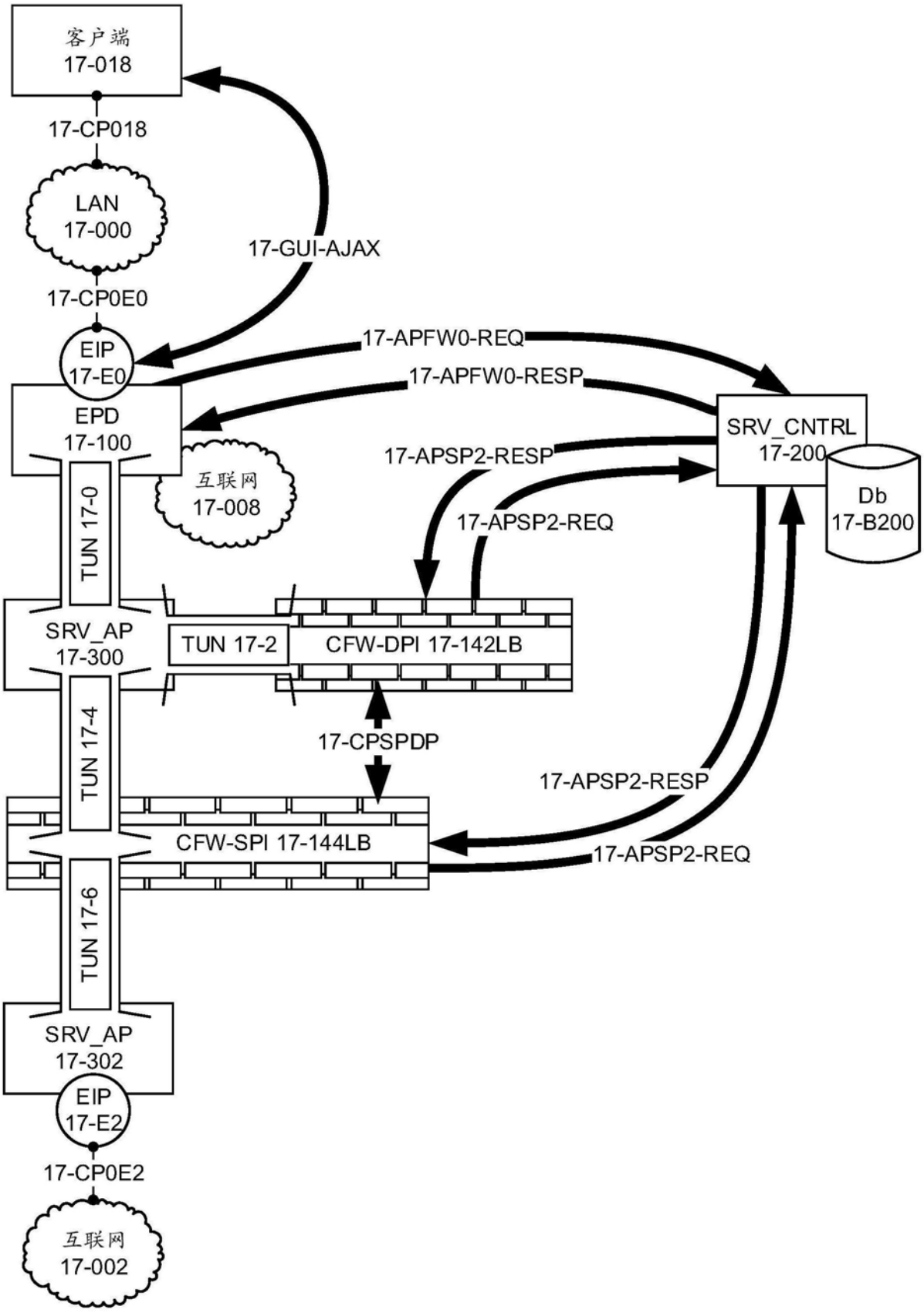

客户端
17-018
17-CP018
LAN
17-000
17-CP0E0
EIP
17-E0
17-GUI-AJAX
17-APFW0-REQ
17-APFW0-RESP
EPD
17-100
互联网
17-008
SRV_CNTRL
17-200
Db
17-B200
17-APSP2-RESP
17-APSP2-REQ
TUN 17-0
SRV_AP
17-300
TUN 17-2
CFW-DPI 17-142LB
17-CPSPDP
TUN 17-4
17-APSP2-RESP
CFW-SPI 17-144LB
17-APSP2-REQ
TUN 17-6
SRV_AP
17-302
EIP
17-E2
17-CP0E2
互联网
17-002

图17

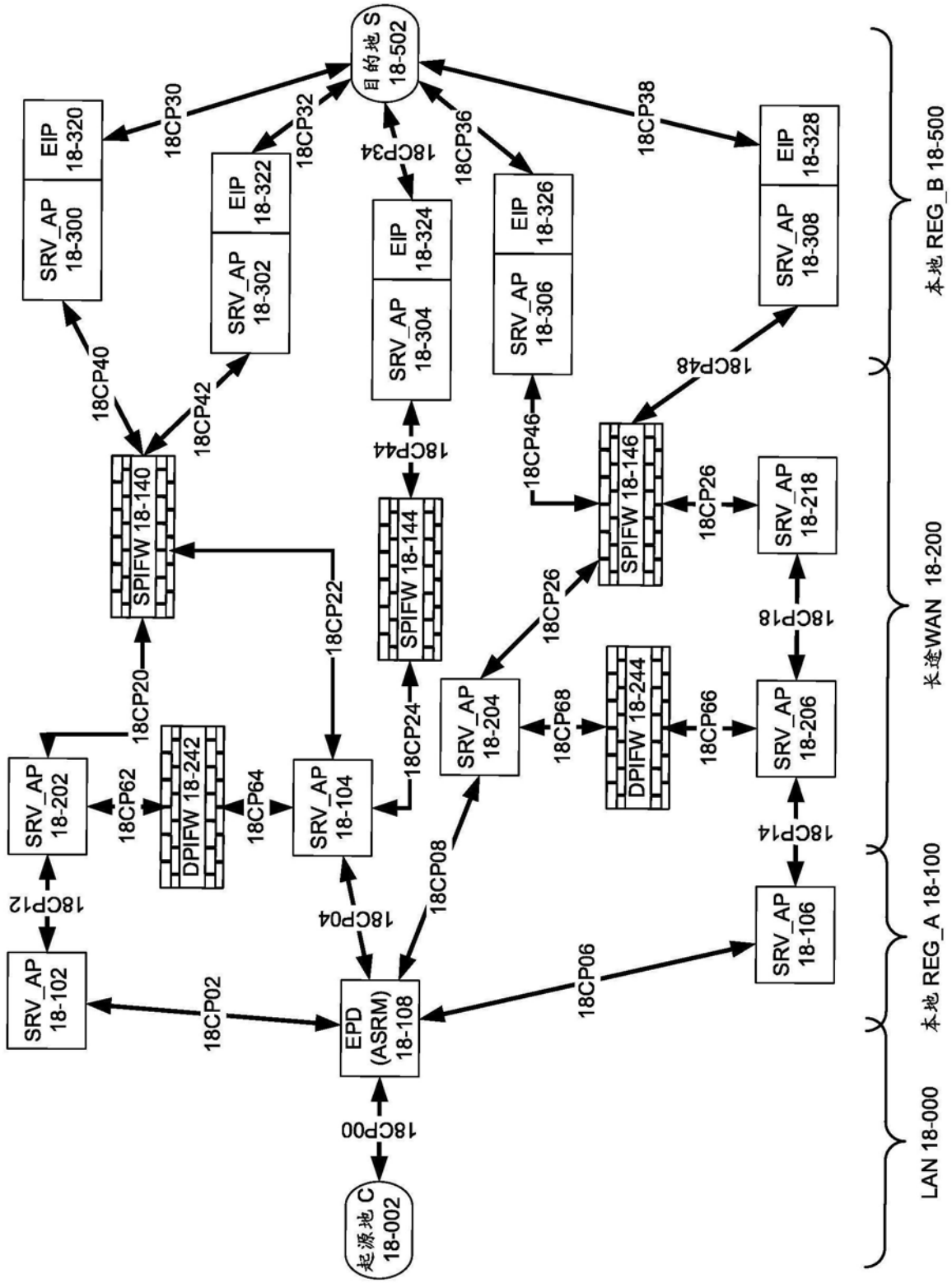

目的地 S
18-502
起源地 C
18-002
EPD (ASRM) 18-108
SRV_AP 18-102
SRV_AP 18-202
SRV_AP 18-104
SRV_AP 18-204
SRV_AP 18-106
SRV_AP 18-206
SRV_AP 18-218
SRV_AP 18-300
SRV_AP 18-302
SRV_AP 18-304
SRV_AP 18-306
SRV_AP 18-308
EIP 18-320
EIP 18-322
EIP 18-324
EIP 18-326
EIP 18-328
SPIFW 18-140
SPIFW 18-144
SPIFW 18-146
DPIFW 18-242
DPIFW 18-244
18CP00
18CP02
18CP04
18CP06
18CP08
18CP12
18CP14
18CP18
18CP20
18CP22
18CP24
18CP26
18CP30
18CP32
18CP34
18CP36
18CP38
18CP40
18CP42
18CP44
18CP46
18CP48
18CP62
18CP64
18CP66
18CP68
LAN 18-000
本地 REG_A 18-100
长途WAN 18-200
本地 REG_B 18-500

图18

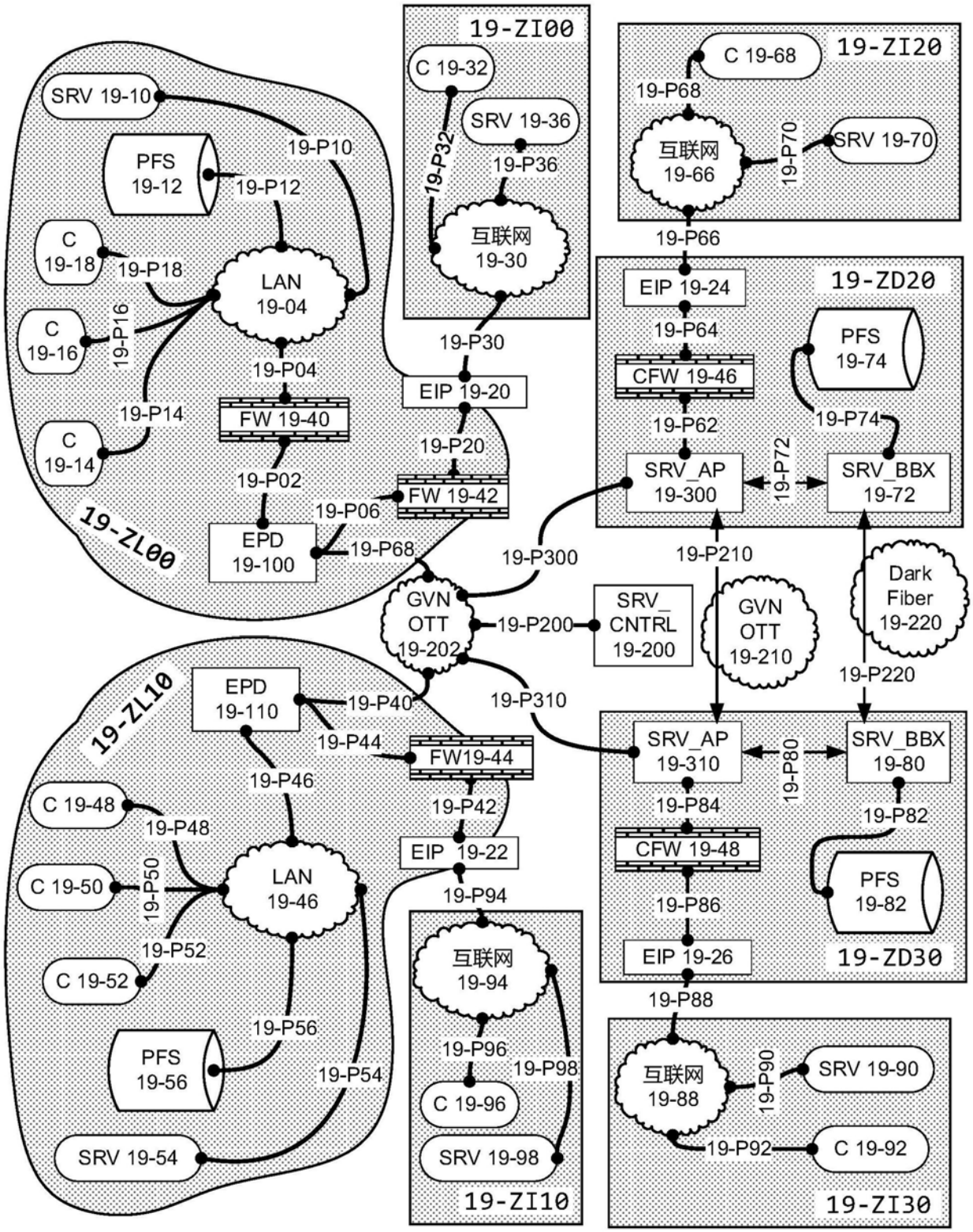

19-ZI00
C 19-32
SRV 19-36
19-P32
19-P36
互联网
19-30
19-P30
C 19-68
19-ZI20
19-P68
互联网
19-66
19-P70
SRV 19-70
19-P66
SRV 19-10
19-P10
PFS
19-12
19-P12
C
19-18
19-P18
LAN
19-04
C
19-16
19-P16
19-P14
C
19-14
19-P04
FW 19-40
19-P02
EPD
19-100
19-P06
19-P68
19-ZL00
EIP 19-20
19-P20
FW 19-42
EIP 19-24
19-ZD20
19-P64
CFW 19-46
PFS
19-74
19-P62
19-P74
SRV_AP
19-300
19-P72
SRV_BBX
19-72
19-P300
19-P210
Dark
Fiber
19-220
GVN
OTT
19-202
19-P200
SRV_
CNTRL
19-200
GVN
OTT
19-210
19-P220
19-P310
19-ZL10
EPD
19-110
19-P40
19-P44
FW19-44
19-P46
19-P42
C 19-48
19-P48
EIP 19-22
C 19-50
19-P50
LAN
19-46
19-P94
19-P52
C 19-52
19-P56
PFS
19-56
19-P54
SRV 19-54
互联网
19-94
19-P96
19-P98
C 19-96
SRV 19-98
19-ZI10
SRV_AP
19-310
19-P80
SRV_BBX
19-80
19-P84
19-P82
CFW 19-48
PFS
19-82
19-P86
EIP 19-26
19-ZD30
19-P88
互联网
19-88
19-P90
SRV 19-90
19-P92
C 19-92
19-ZI30

图19

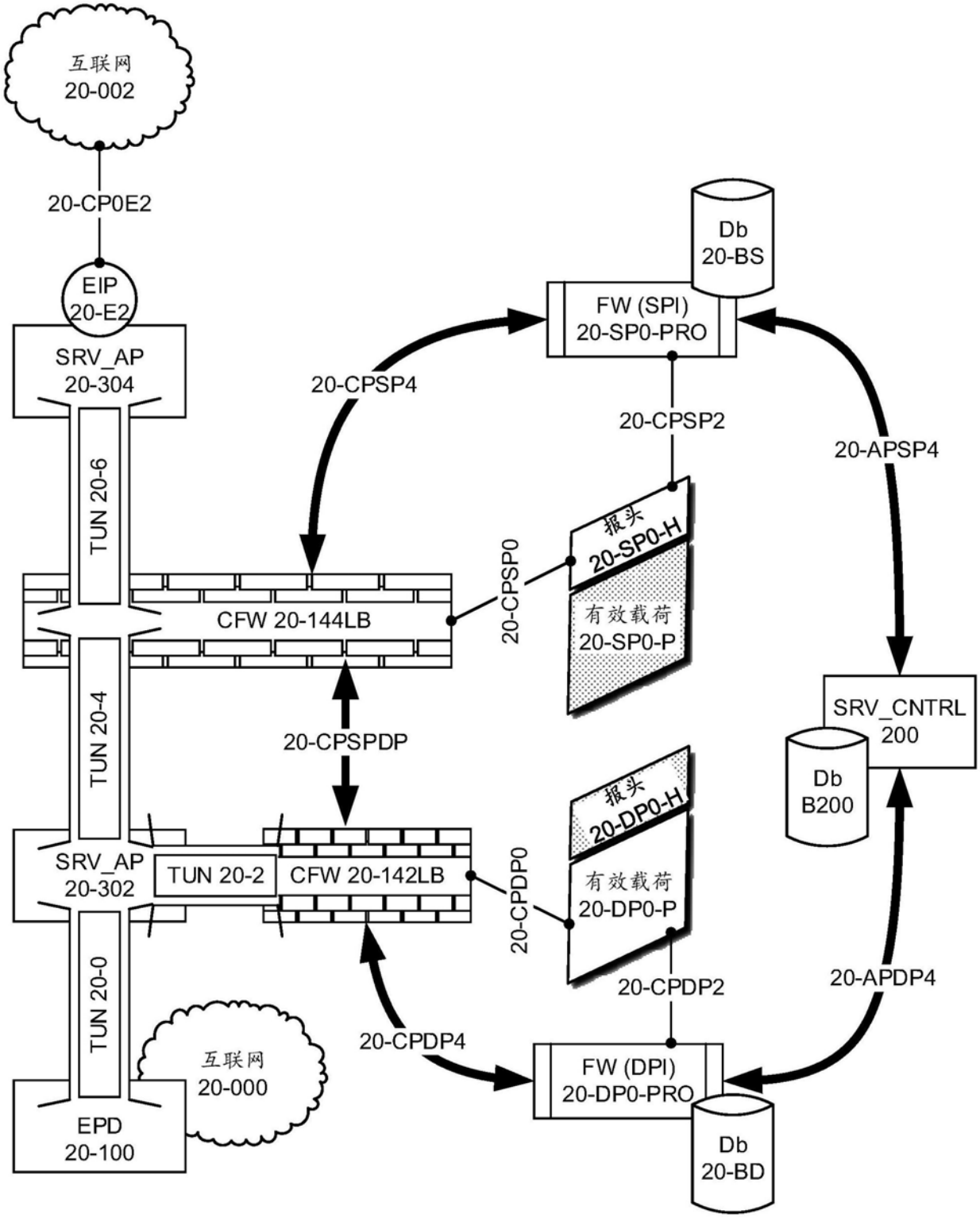

互联网
20-002
20-CP0E2
EIP
20-E2
SRV_AP
20-304
TUN 20-6
TUN 20-4
TUN 20-0
CFW 20-144LB
20-CPSP4
FW (SPI)
20-SP0-PRO
Db
20-BS
20-CPSP2
20-APSP4
报头
20-SP0-H
有效载荷
20-SP0-P
20-CPSP0
20-CPSPDP
SRV_CNTRL
200
Db
B200
SRV_AP
20-302
TUN 20-2
CFW 20-142LB
报头
20-DP0-H
有效载荷
20-DP0-P
20-CPDP0
20-CPDP2
20-APDP4
20-CPDP4
互联网
20-000
FW (DPI)
20-DP0-PRO
EPD
20-100
Db
20-BD

图20

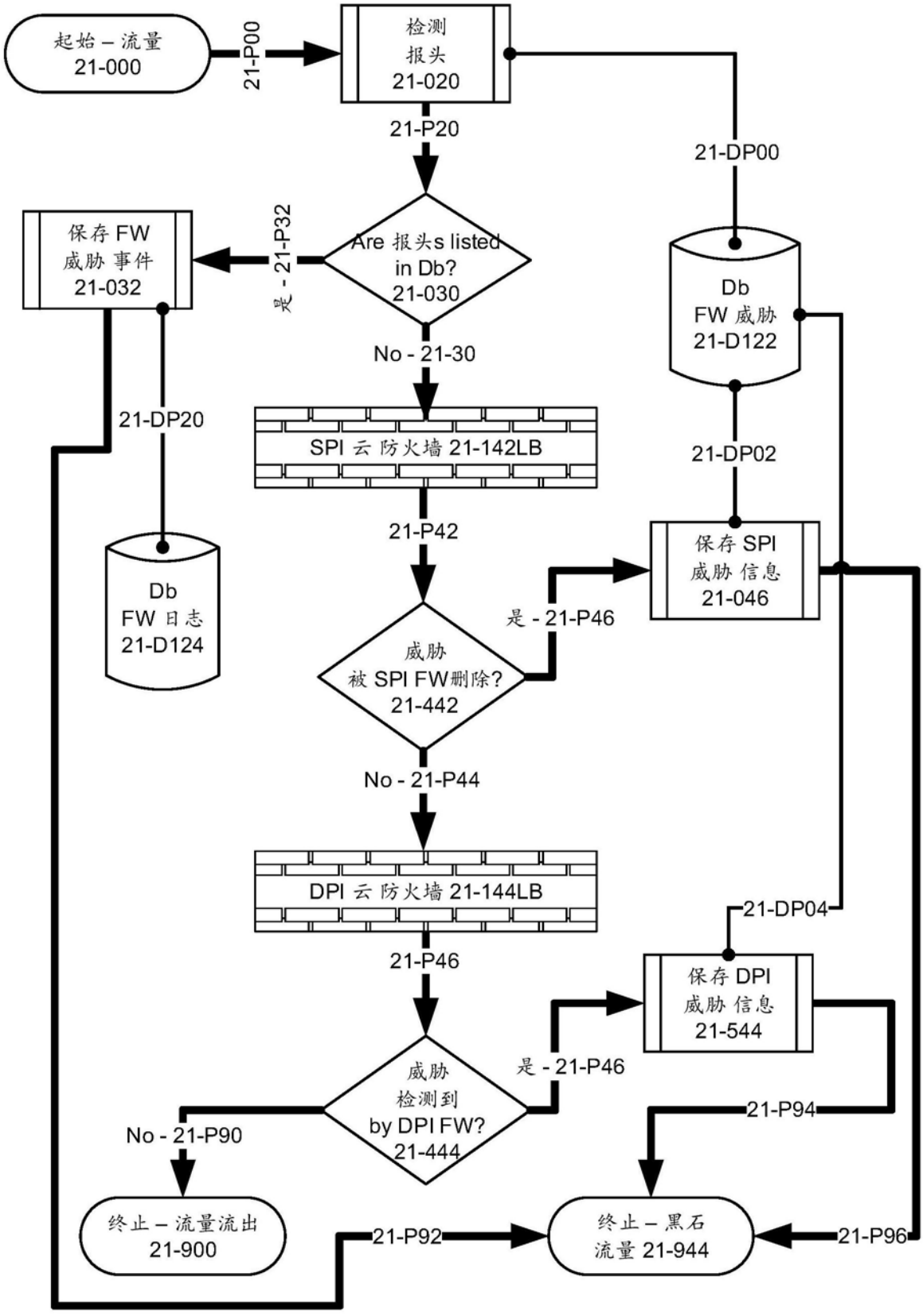

起始 – 流量
21-000
21-P00
检测
报头
21-020
21-P20
21-DP00
Are 报头s listed in Db?
21-030
是 - 21-P32
保存 FW
威胁 事件
21-032
No - 21-30
Db
FW 威胁
21-D122
21-DP20
SPI 云 防火墙 21-142LB
21-DP02
21-P42
保存 SPI
威胁 信息
21-046
Db
FW 日志
21-D124
威胁
被 SPI FW删除?
21-442
是 - 21-P46
No - 21-P44
DPI 云 防火墙 21-144LB
21-DP04
21-P46
保存 DPI
威胁 信息
21-544
威胁
检测到
by DPI FW?
21-444
是 - 21-P46
21-P94
No - 21-P90
终止 – 流量流出
21-900
21-P92
终止 – 黑石
流量 21-944
21-P96

图21

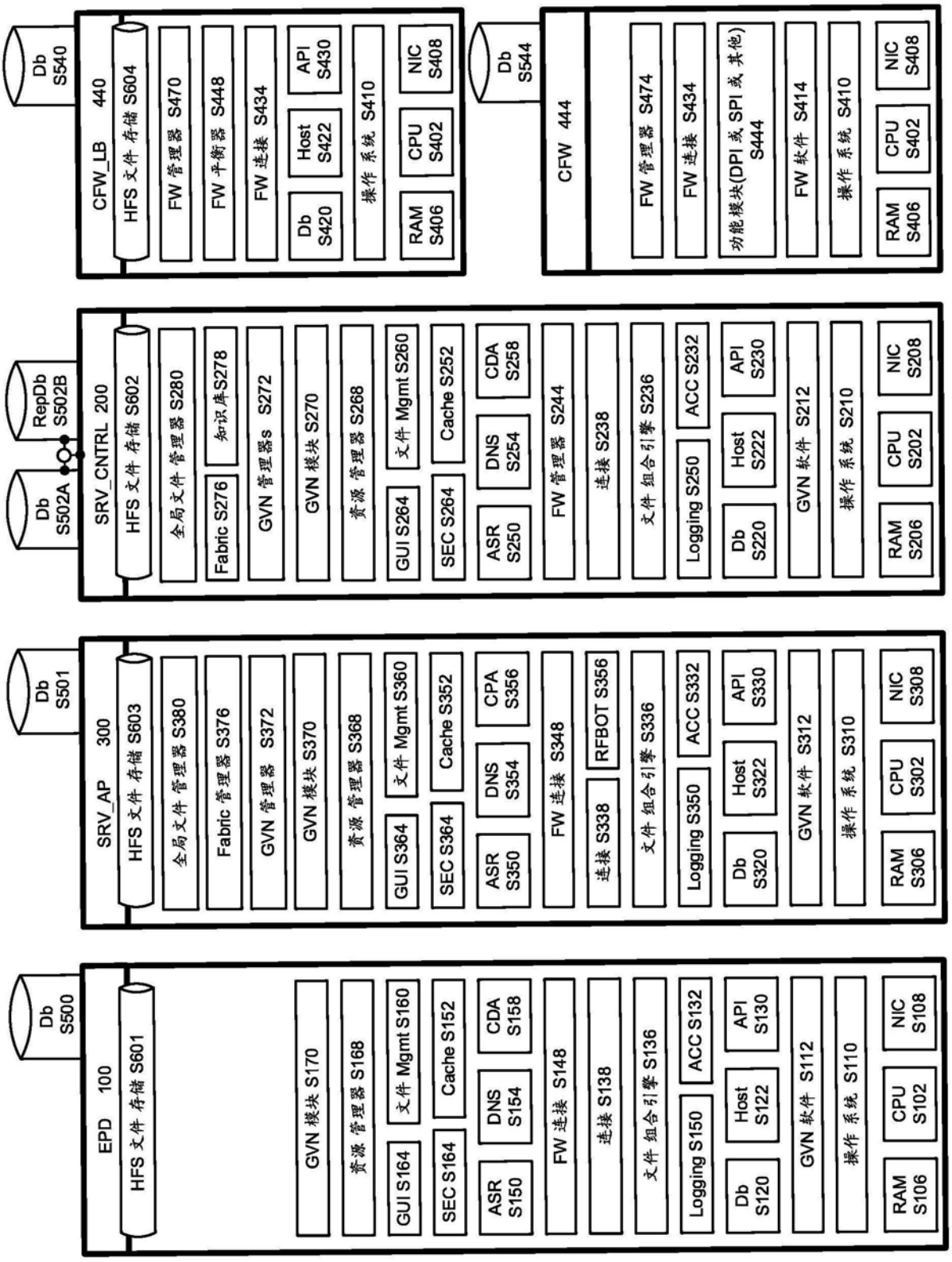

EPD 100
HFS 文件 存储 S601
Db S500
RAM S106
CPU S102
NIC S108
操作 系统 S110
GVN 软件 S112
Db S120
Host S122
API S130
Logging S150
ACC S132
文件 组合引擎 S136
连接 S138
FW 连接 S148
ASR S150
DNS S154
CDA S158
SEC S164
Cache S152
GUI S164
文件 Mgmt S160
资源 管理器 S168
GVN 模块 S170
SRV_AP 300
HFS 文件 存储 S603
Db S501
RAM S306
CPU S302
NIC S308
操作 系统 S310
GVN 软件 S312
Db S320
Host S322
API S330
Logging S350
ACC S332
文件 组合引擎 S336
连接 S338
RFBOT S356
FW 连接 S348
ASR S350
DNS S354
CPA S356
SEC S364
Cache S352
GUI S364
文件 Mgmt S360
资源 管理器 S368
GVN 模块 S370
GVN 管理器 S372
Fabric 管理器 S376
全局文件 管理器 S380
HFS 文件 存储 S603
SRV_CNTRL 200
HFS 文件 存储 S602
Db S502A
RepDb S502B
RAM S206
CPU S202
NIC S208
操作 系统 S210
GVN 软件 S212
Db S220
Host S222
API S230
Logging S250
ACC S232
文件 组合引擎 S236
连接 S238
FW 管理器 S244
ASR S250
DNS S254
CDA S258
SEC S264
Cache S252
GUI S264
文件 Mgmt S260
资源 管理器 S268
GVN 模块 S270
GVN 管理器s S272
Fabric S276
知识库S278
全局文件 管理器 S280
HFS 文件 存储 S602
CFW_LB 440
HFS 文件 存储 S604
Db S540
RAM S406
CPU S402
NIC S408
操作 系统 S410
FW 连接 S434
FW 平衡器 S448
FW 管理器 S470
Db S420
Host S422
API S430
CFW 444
Db S544
RAM S406
CPU S402
NIC S408
操作 系统 S410
FW 软件 S414
功能模块(DPI 或 SPI 或 其他) S444
FW 连接 S434
FW 管理器 S474

图22

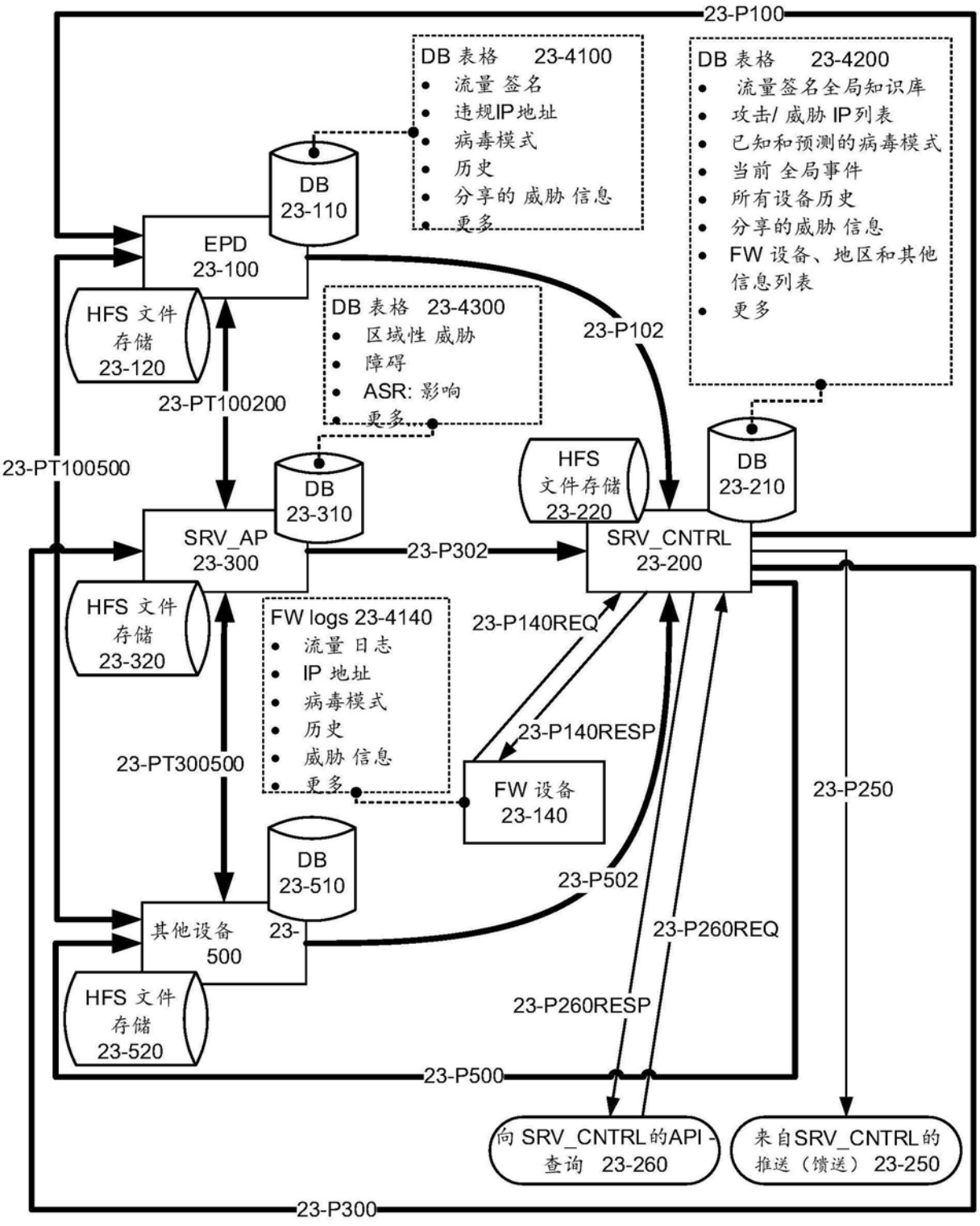

23-P100
DB 表格 23-4100
流量 签名
违规IP地址
病毒模式
历史
分享的 威胁 信息
更多
DB 表格 23-4200
流量签名全局知识库
攻击/ 威胁 IP列表
已知和预测的病毒模式
当前 全局事件
所有设备历史
分享的威胁 信息
FW 设备、地区和其他信息列表
更多
DB 23-110
EPD 23-100
HFS 文件存储 23-120
DB 表格 23-4300
区域性 威胁
障碍
ASR: 影响
更多
23-P102
23-PT100200
23-PT100500
DB 23-310
HFS 文件存储 23-220
DB 23-210
SRV_AP 23-300
23-P302
SRV_CNTRL 23-200
HFS 文件存储 23-320
FW logs 23-4140
流量 日志
IP 地址
病毒模式
历史
威胁 信息
更多
23-P140REQ
23-P140RESP
23-PT300500
FW 设备 23-140
23-P250
DB 23-510
23-P502
其他设备 23-500
23-P260REQ
HFS 文件存储 23-520
23-P260RESP
23-P500
向 SRV_CNTRL的API 查询 23-260
来自SRV_CNTRL的推送（馈送） 23-250
23-P300

图23

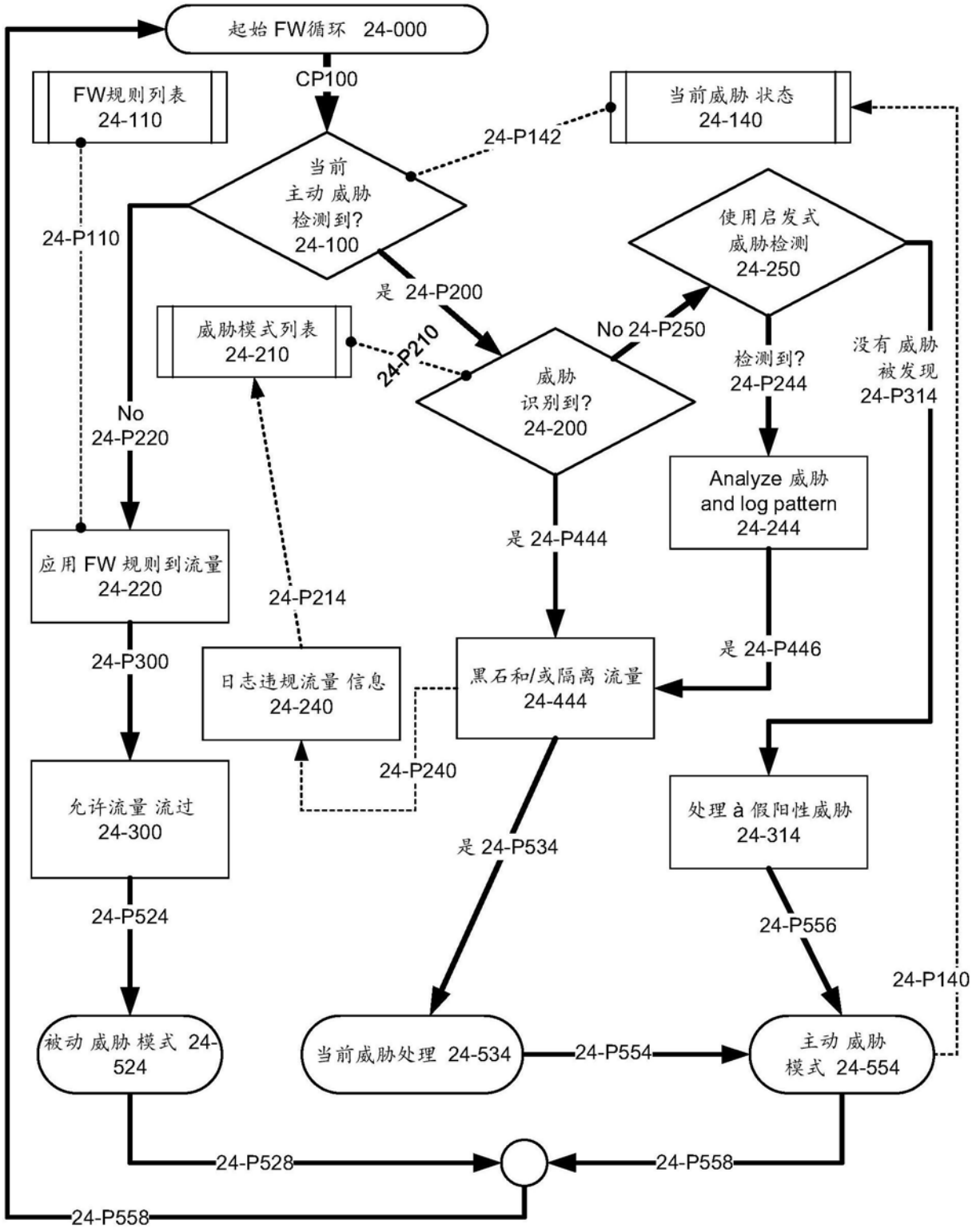

起始 FW循环 24-000
CP100
FW规则列表 24-110
当前威胁 状态 24-140
24-P142
当前 主动 威胁 检测到? 24-100
24-P110
是 24-P200
使用启发式 威胁检测 24-250
威胁模式列表 24-210
24-P210
No 24-P250
威胁 识别到? 24-200
检测到? 24-P244
没有 威胁 被发现 24-P314
No 24-P220
Analyze 威胁 and log pattern 24-244
是 24-P444
应用 FW 规则到流量 24-220
24-P214
是 24-P446
24-P300
日志违规流量 信息 24-240
黑石和/或隔离 流量 24-444
24-P240
允许流量 流过 24-300
处理 à 假阳性威胁 24-314
是 24-P534
24-P524
24-P556
24-P140
被动 威胁 模式 24-524
当前威胁处理 24-534
24-P554
主动 威胁 模式 24-554
24-P528
24-P558
24-P558

图24

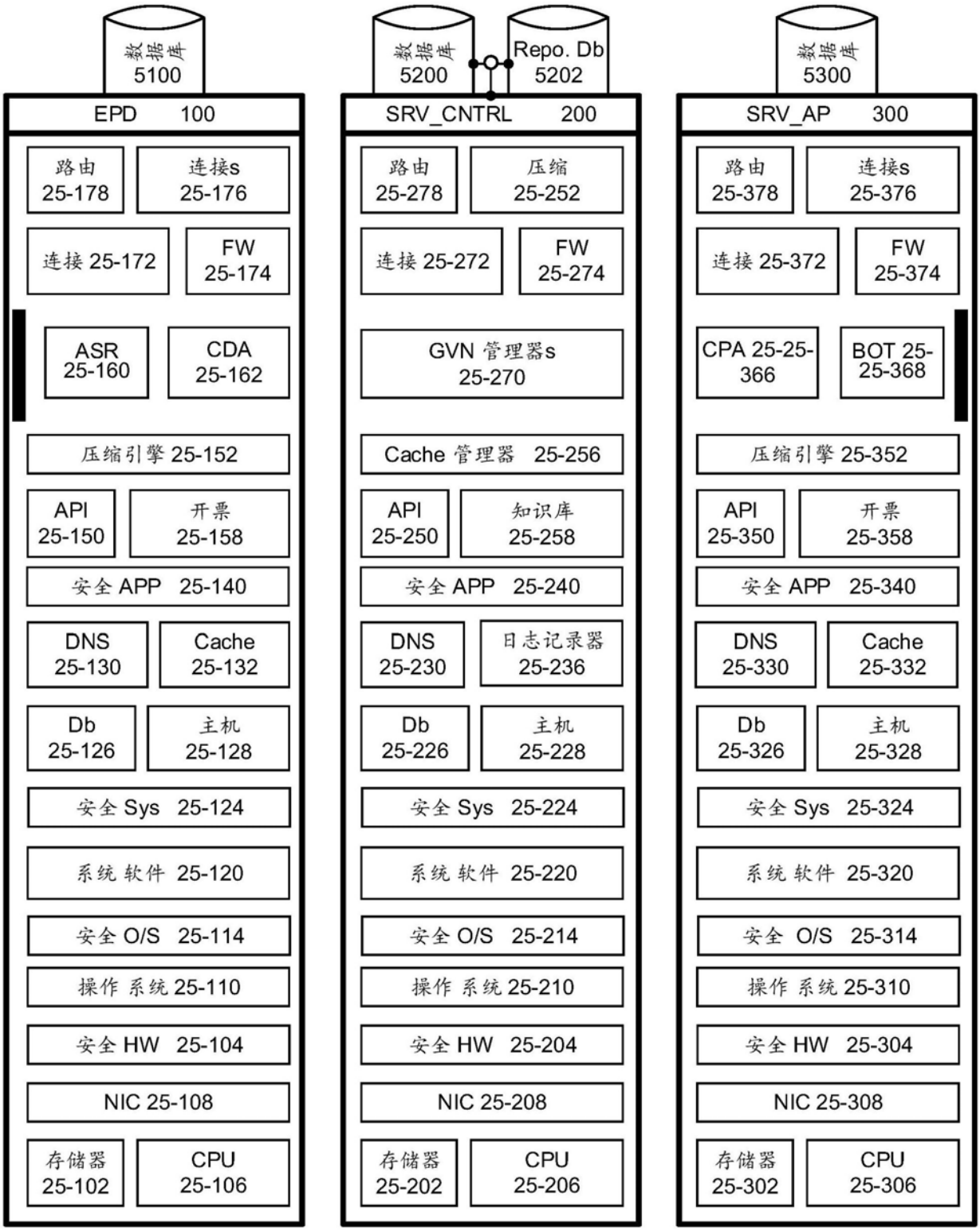

数据库 5100
EPD 100
路由 25-178
连接s 25-176
连接 25-172
FW 25-174
ASR 25-160
CDA 25-162
压缩引擎 25-152
API 25-150
开票 25-158
安全 APP 25-140
DNS 25-130
Cache 25-132
Db 25-126
主机 25-128
安全 Sys 25-124
系统 软件 25-120
安全 O/S 25-114
操作 系统 25-110
安全 HW 25-104
NIC 25-108
存储器 25-102
CPU 25-106
数据库 5200
Repo. Db 5202
SRV_CNTRL 200
路由 25-278
压缩 25-252
连接 25-272
FW 25-274
GVN 管理器s 25-270
Cache 管理器 25-256
API 25-250
知识库 25-258
安全 APP 25-240
DNS 25-230
日志记录器 25-236
Db 25-226
主机 25-228
安全 Sys 25-224
系统 软件 25-220
安全 O/S 25-214
操作 系统 25-210
安全 HW 25-204
NIC 25-208
存储器 25-202
CPU 25-206
数据库 5300
SRV_AP 300
路由 25-378
连接s 25-376
连接 25-372
FW 25-374
CPA 25-25-366
BOT 25-25-368
压缩引擎 25-352
API 25-350
开票 25-358
安全 APP 25-340
DNS 25-330
Cache 25-332
Db 25-326
主机 25-328
安全 Sys 25-324
系统 软件 25-320
安全 O/S 25-314
操作 系统 25-310
安全 HW 25-304
NIC 25-308
存储器 25-302
CPU 25-306

图25

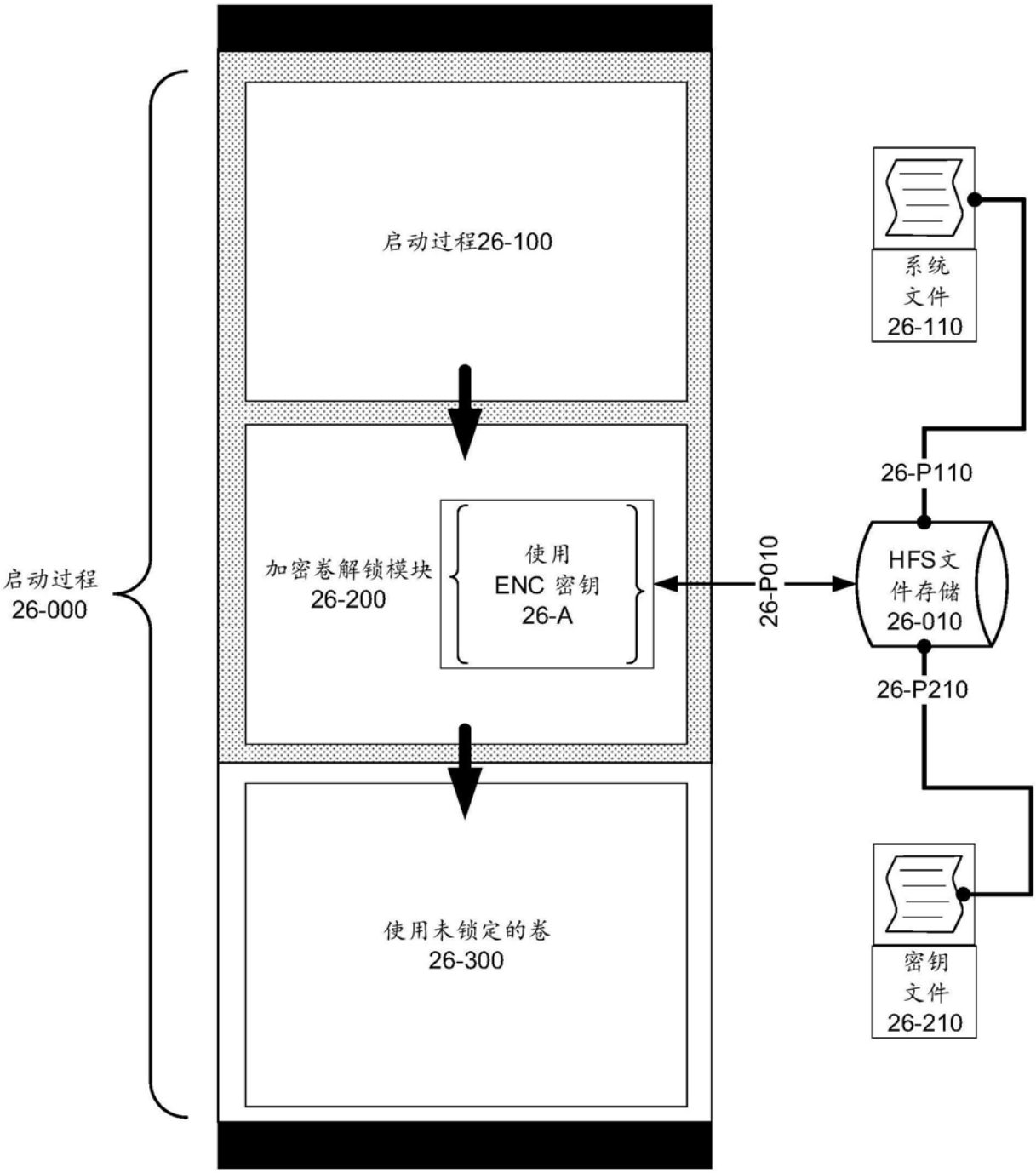

启动过程26-100
加密卷解锁模块
26-200
使用
ENC 密钥
26-A
使用未锁定的卷
26-300
启动过程
26-000
系统
文件
26-110
26-P110
HFS文
件存储
26-010
26-P010
26-P210
密钥
文件
26-210

图26

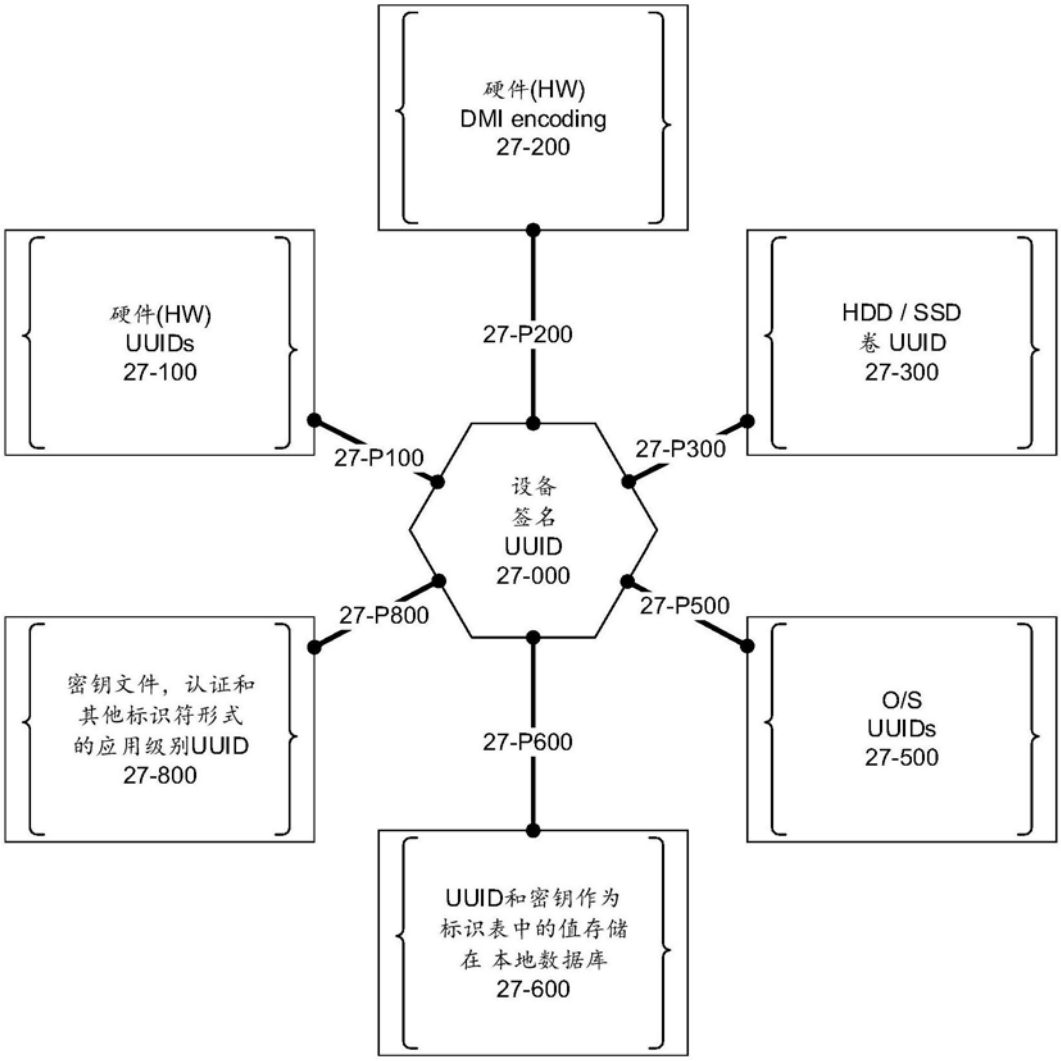

硬件(HW)
DMI encoding
27-200
硬件(HW)
UUIDs
27-100
27-P200
HDD / SSD
卷 UUID
27-300
27-P100
27-P300
设备
签名
UUID
27-000
27-P800
27-P500
密钥文件，认证和
其他标识符形式
的应用级别UUID
27-800
O/S
UUIDs
27-500
27-P600
UUID和密钥作为
标识表中的值存储
在 本地数据库
27-600

图27

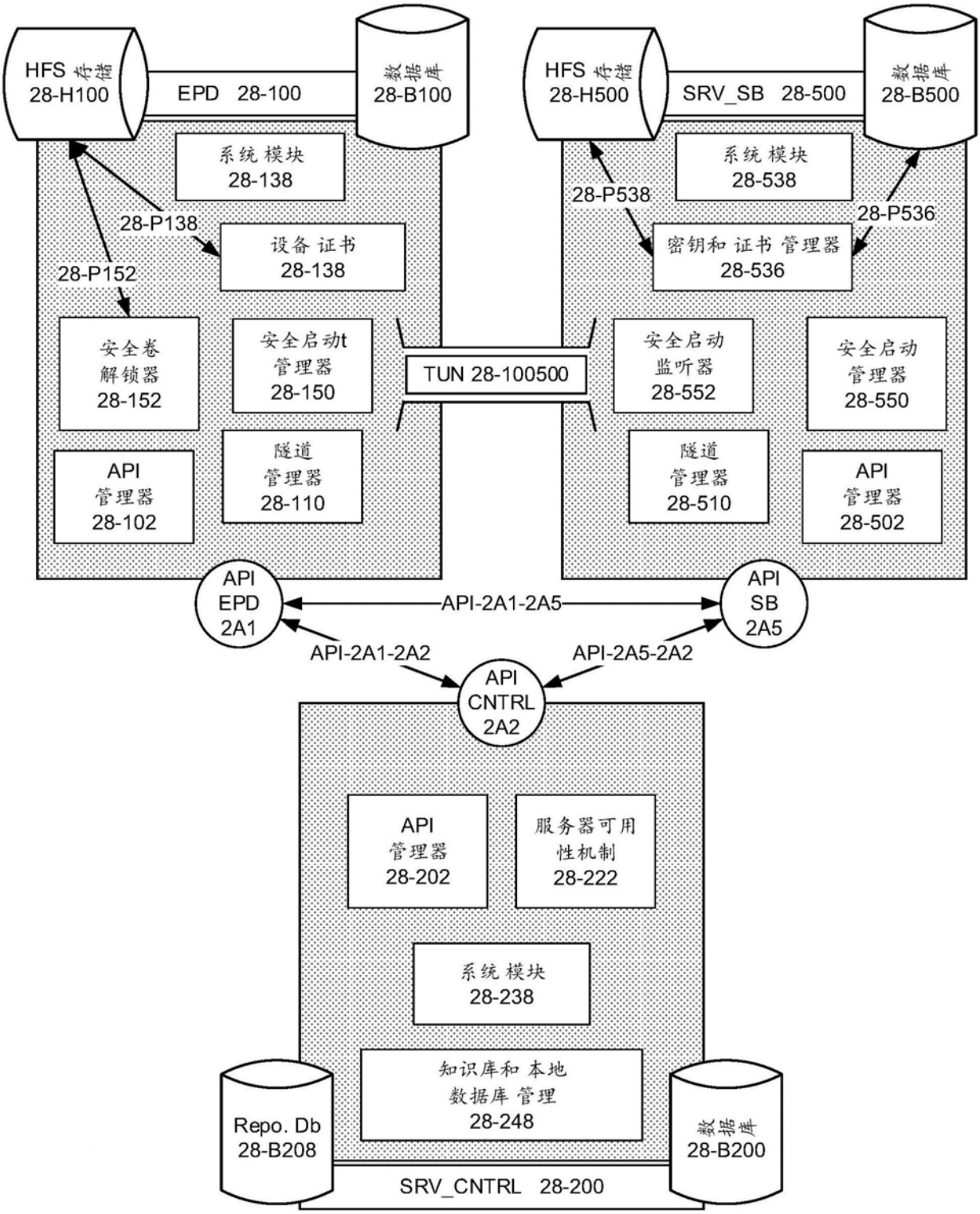

HFS 存储
28-H100
EPD 28-100
数据库
28-B100
HFS 存储
28-H500
SRV_SB 28-500
数据库
28-B500
系统模块
28-138
系统模块
28-538
28-P138
28-P538
28-P536
设备证书
28-138
密钥和证书管理器
28-536
28-P152
安全卷
解锁器
28-152
安全启动t
管理器
28-150
TUN 28-100500
安全启动
监听器
28-552
安全启动
管理器
28-550
API
管理器
28-102
隧道
管理器
28-110
隧道
管理器
28-510
API
管理器
28-502
API
EPD
2A1
API-2A1-2A5
API
SB
2A5
API-2A1-2A2
API-2A5-2A2
API
CNTRL
2A2
API
管理器
28-202
服务器可用
性机制
28-222
系统模块
28-238
知识库和本地
数据库管理
28-248
Repo. Db
28-B208
数据库
28-B200
SRV_CNTRL 28-200

图28

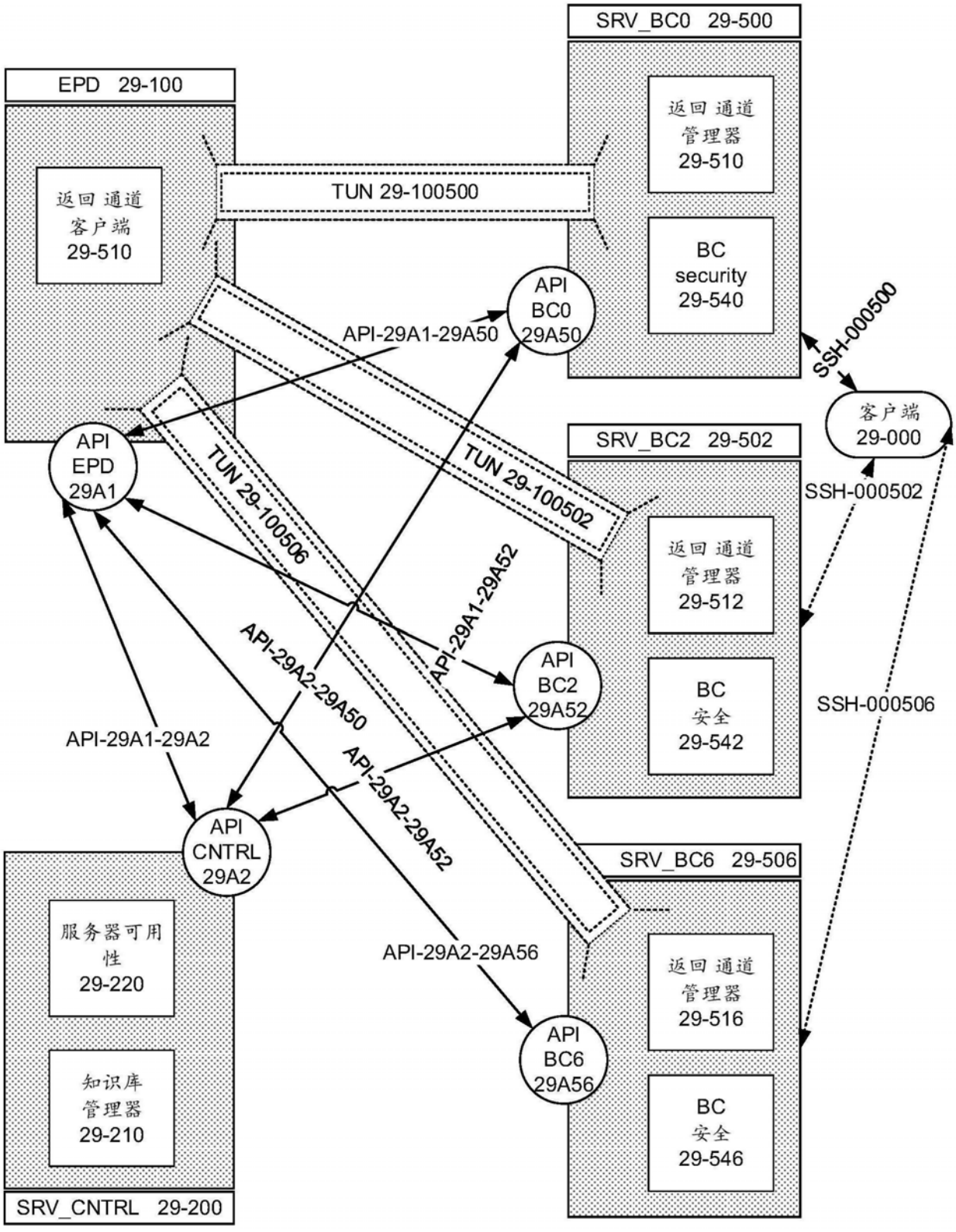

SRV_BC0 29-500
EPD 29-100
返回通道管理器 29-510
返回通道客户端 29-510
TUN 29-100500
BC security 29-540
API BC0 29A50
API-29A1-29A50
SSH-000500
客户端 29-000
API EPD 29A1
SRV_BC2 29-502
TUN 29-100502
TUN 29-100506
返回通道管理器 29-512
SSH-000502
API-29A1-29A52
API-29A2-29A50
API BC2 29A52
BC 安全 29-542
SSH-000506
API-29A1-29A2
API-29A2-29A52
API CNTRL 29A2
SRV_BC6 29-506
服务器可用性 29-220
API-29A2-29A56
返回通道管理器 29-516
知识库管理器 29-210
API BC6 29A56
BC 安全 29-546
SRV_CNTRL 29-200

图29

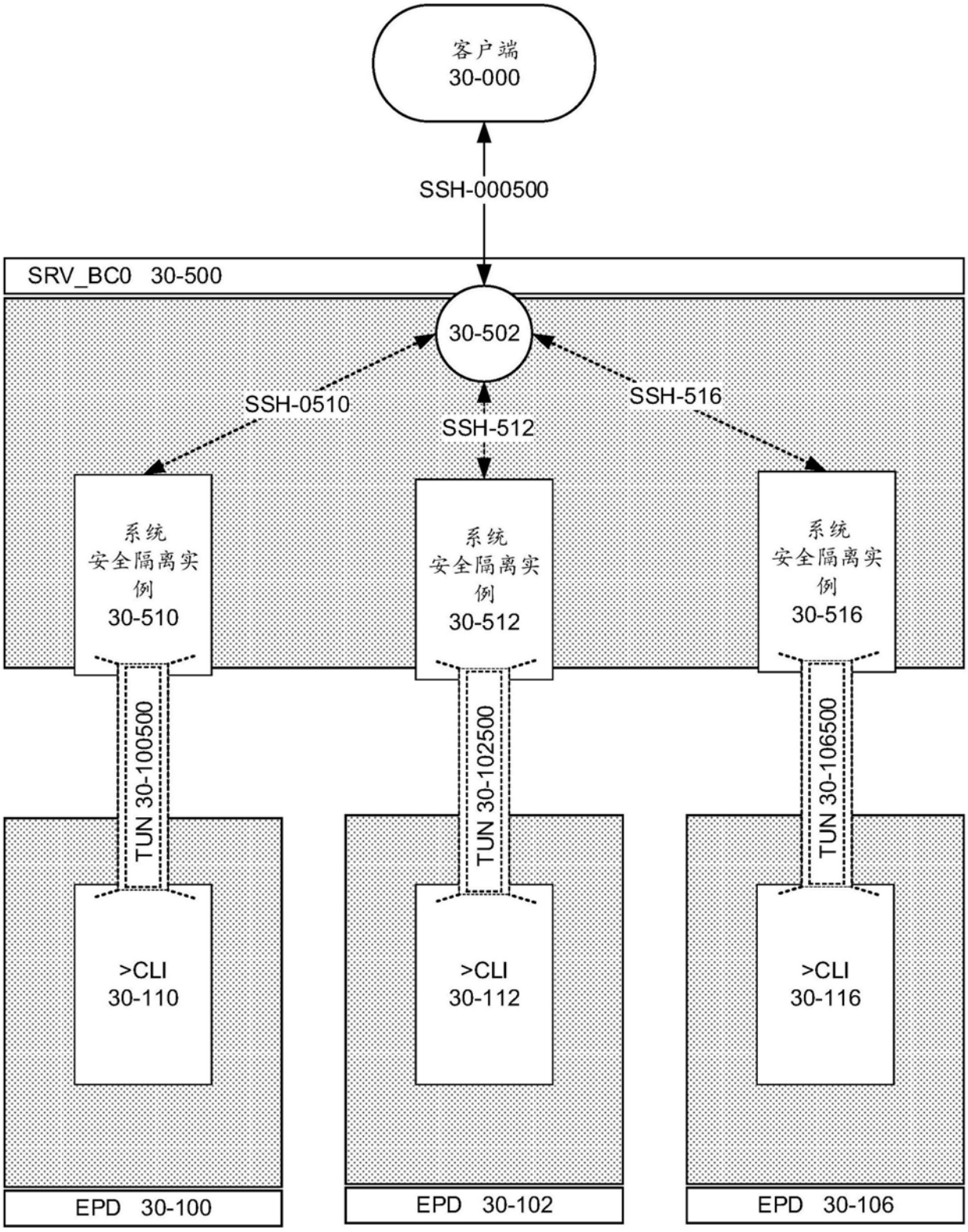

客户端
30-000
SSH-000500
SRV_BC0 30-500
30-502
SSH-0510
SSH-512
SSH-516
系统
安全隔离实
例
30-510
系统
安全隔离实
例
30-512
系统
安全隔离实
例
30-516
TUN 30-100500
TUN 30-102500
TUN 30-106500
>CLI
30-110
>CLI
30-112
>CLI
30-116
EPD 30-100
EPD 30-102
EPD 30-106

图30

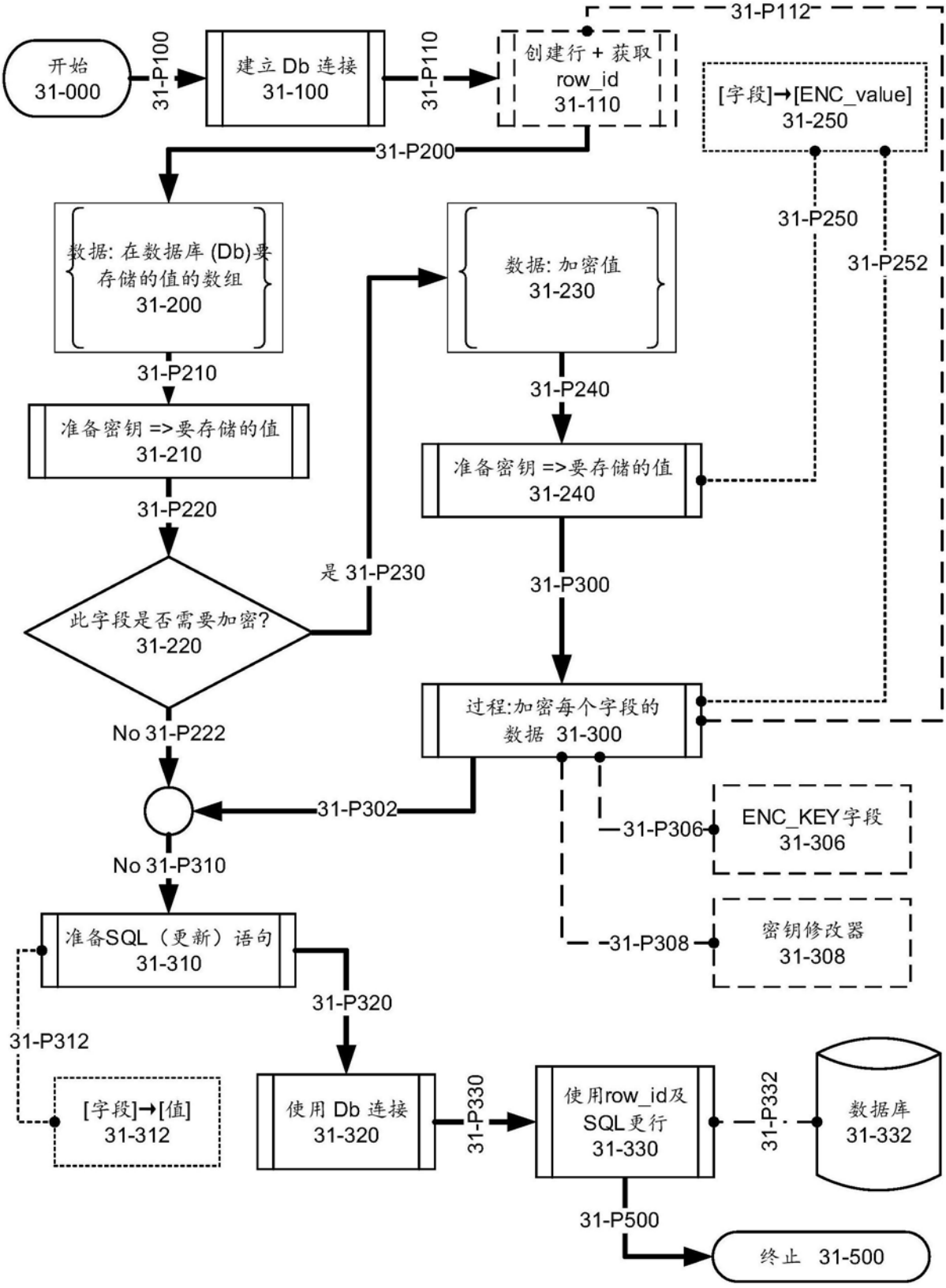

开始
31-000
31-P100
建立 Db 连接
31-100
31-P110
创建行 + 获取
row_id
31-110
31-P112
[字段]→[ENC_value]
31-250
31-P200
数据: 在数据库 (Db)要
存储的值的数组
31-200
数据: 加密值
31-230
31-P250
31-P252
31-P210
31-P240
准备密钥 =>要存储的值
31-210
准备密钥 =>要存储的值
31-240
31-P220
是 31-P230
31-P300
此字段是否需要加密?
31-220
过程:加密每个字段的
数据 31-300
No 31-P222
31-P302
31-P306
ENC_KEY字段
31-306
No 31-P310
31-P308
密钥修改器
31-308
准备SQL（更新）语句
31-310
31-P320
31-P312
[字段]→[值]
31-312
使用 Db 连接
31-320
31-P330
使用row_id及
SQL更行
31-330
31-P332
数据库
31-332
31-P500
终止 31-500

图31

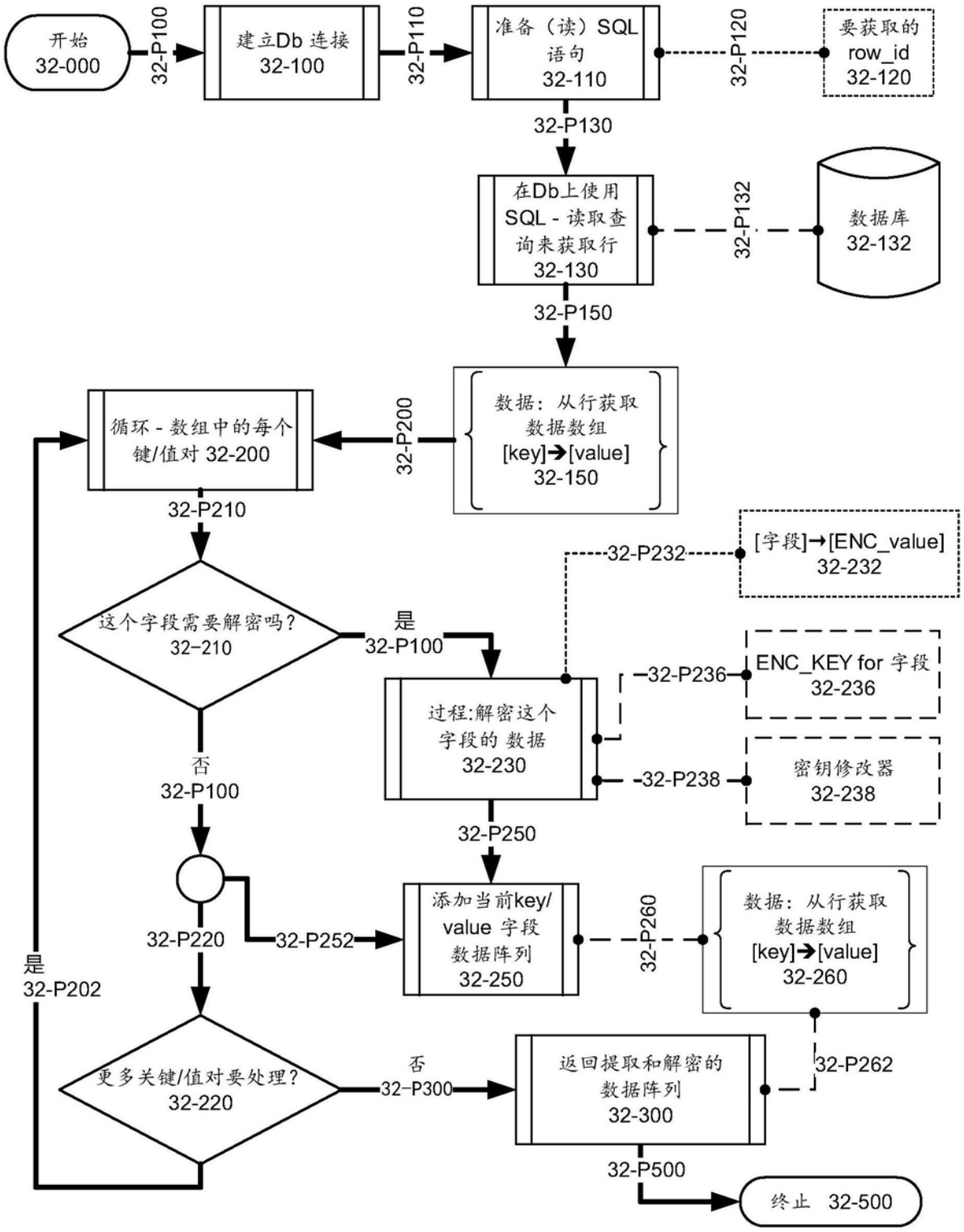

开始
32-000
32-P100
建立Db 连接
32-100
32-P110
准备（读）SQL
语句
32-110
32-P120
要获取的
row_id
32-120
32-P130
在Db上使用
SQL - 读取查
询来获取行
32-130
32-P132
数据库
32-132
32-P150
数据：从行获取
数据数组
[key]➔[value]
32-150
32-P200
循环 - 数组中的每个
键/值对 32-200
32-P210
这个字段需要解密吗?
32-210
是
32-P100
32-P232
[字段]➔[ENC_value]
32-232
32-P236
ENC_KEY for 字段
32-236
过程:解密这个
字段的 数据
32-230
32-P238
密钥修改器
32-238
否
32-P100
32-P250
32-P220
32-P252
添加当前key/
value 字段
数据阵列
32-250
32-P260
数据：从行获取
数据数组
[key]➔[value]
32-260
是
32-P202
更多关键/值对要处理?
32-220
否
32-P300
返回提取和解密的
数据阵列
32-300
32-P262
32-P500
终止 32-500

图32

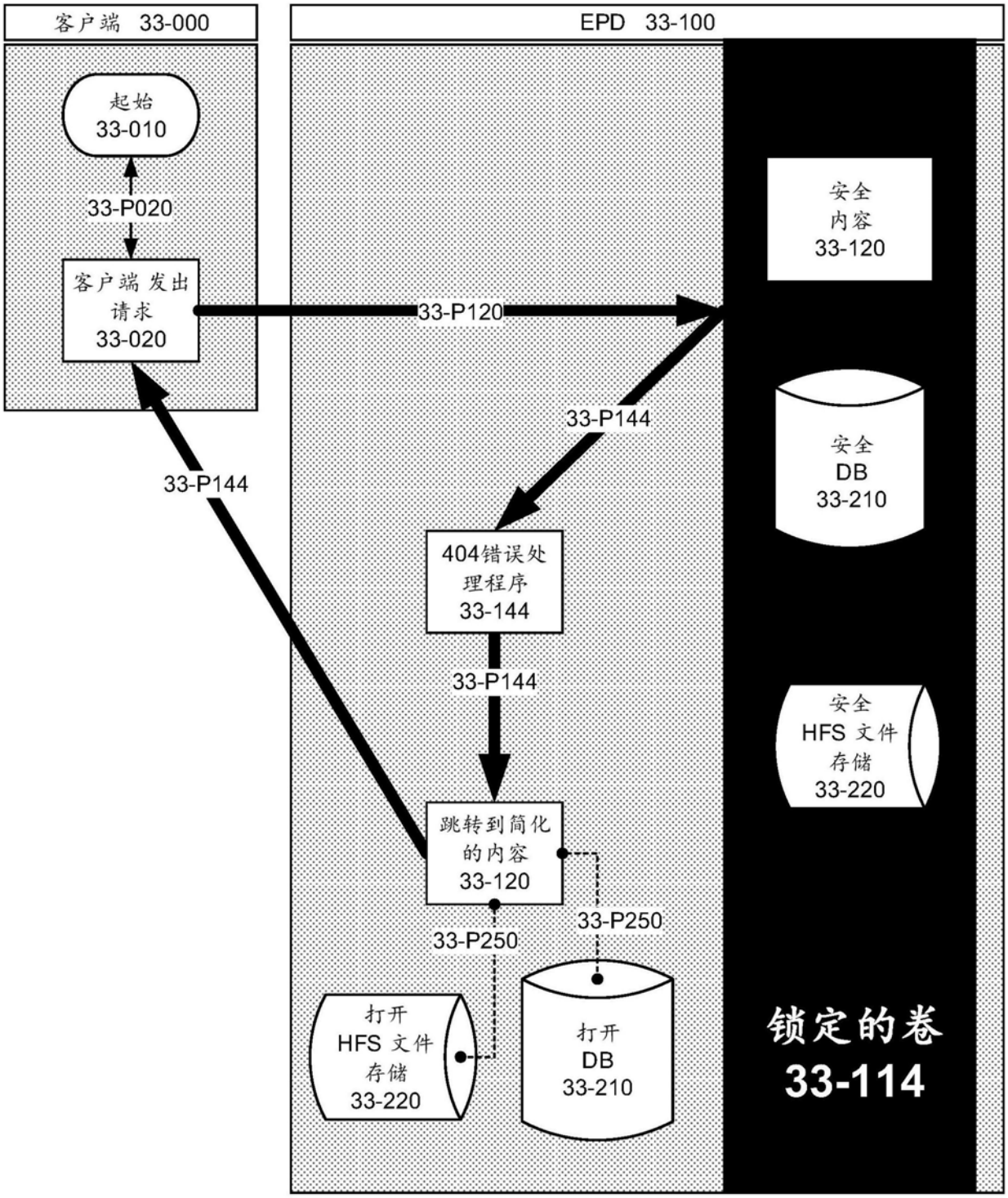

客户端 33-000
EPD 33-100
起始
33-010
33-P020
客户端 发出
请求
33-020
33-P120
安全
内容
33-120
安全
DB
33-210
33-P144
33-P144
404错误处
理程序
33-144
33-P144
安全
HFS 文件
存储
33-220
跳转到简化
的内容
33-120
33-P250
33-P250
打开
HFS 文件
存储
33-220
打开
DB
33-210
锁定的卷
33-114

图33

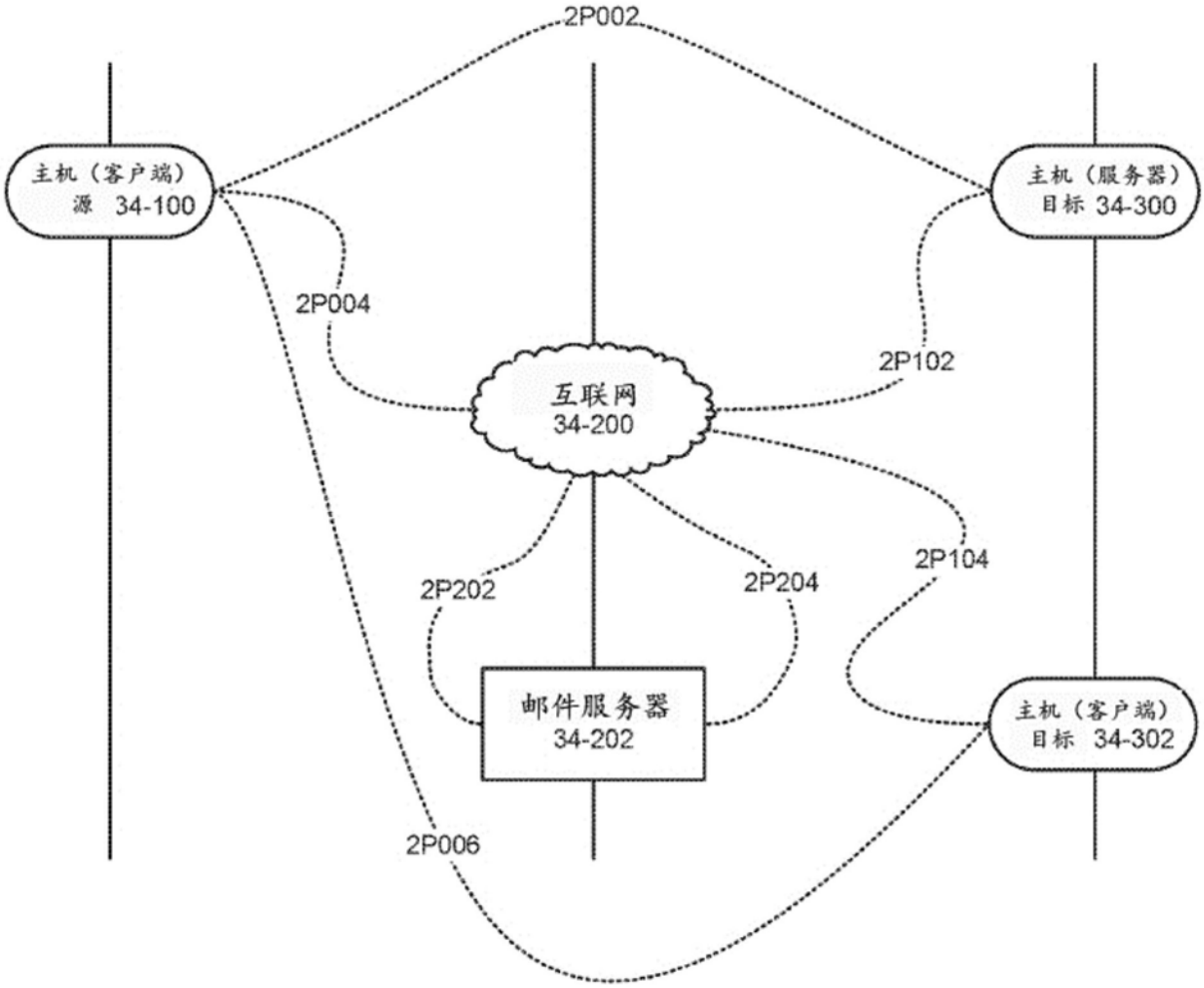

2P002
主机（客户端）
源 34-100
主机（服务器）
目标 34-300
2P004
2P102
互联网
34-200
2P104
2P202
2P204
邮件服务器
34-202
主机（客户端）
目标 34-302
2P006

图34

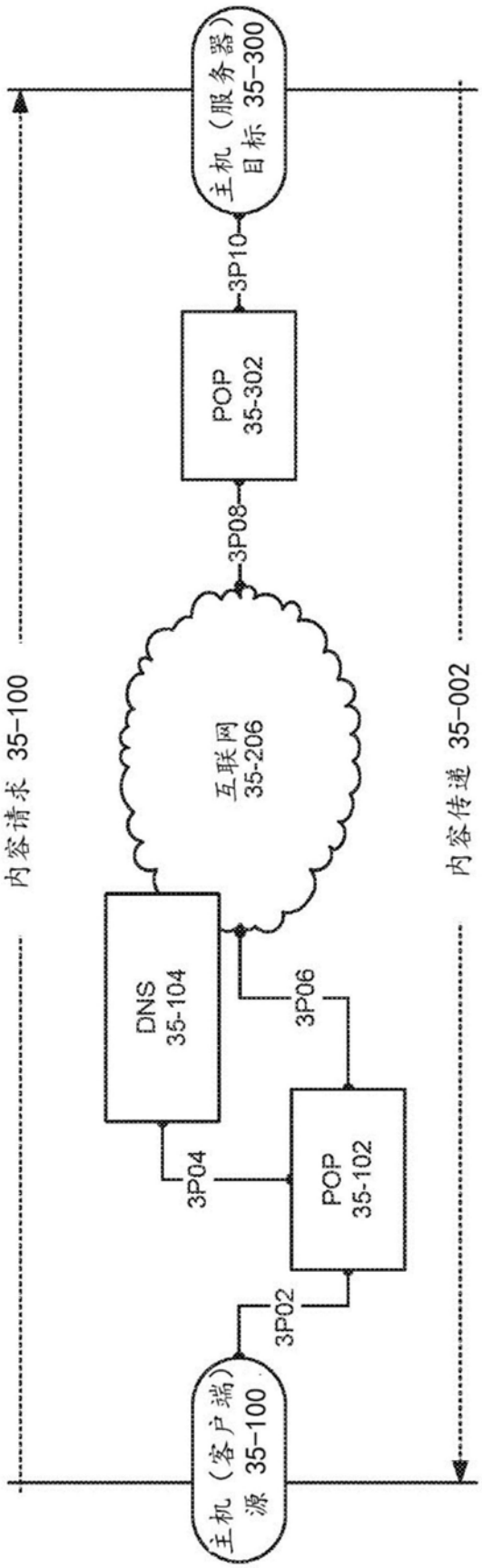

主机（客户端）
源 35-100
3P02
POP
35-102
3P04
DNS
35-104
3P06
互联网
35-206
3P08
POP
35-302
3P10
主机（服务器）
目标 35-300
内容请求 35-100
内容传递 35-002

图35