现代网络架构 PCI DSS 合规范围确定和网络分割措施实施探讨

作者：atsec 陈谨运

2024 年 11 月

关键词：支付安全、PCI DSS、持卡人数据、合规范围确定、网络分割

atsec information security

Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.cn

目录

1 引言

支付卡行业数据安全标准 （PCI DSS：Payment Card Industry Data Security Standard） 的制定旨在鼓励和加强支付账户数据（Account Data）的安全，并促进全球广泛采用一致的数据安全措施。PCI DSS 提供了旨在保护账户数据（Account Data）的技术和操作要求的基线。

随着组织采用更加先进，且更具优势的现代网络架构搭建持卡人数据环境（CDE: Cardholder Data Environment），支付账户数据（Account Data）的安全变得至关重要。采用现代网络架构虽然为组织提供了很大的优势，但它也增加 PCI DSS 范围确定和网络分割的复杂性，并对维护安全环境带来了挑战。其中一个非常关键的挑战是如何确保组织维持有效的网络分割控制措施。

本文档主要探讨云环境和现代网络架构的分割控制，并为有关组织提供如何将传统网络安全原则适用于具有动态性和分布式特性的现代网络架构环境的建议，以支持组织更好的符合 PCI DSS 标准要求。

本文的研讨基于 PCI DSS 标准，然而相关措施实施的信息安全建设思路也可以作为最佳实践用于产业内其他相关标准或者法规的安全建设和合规评估。

2 PCI DSS 合规范围确定

PCI DSS 适用于所有存储、处理或传输持卡人数据（CHD：Cardholder Data）和/或敏感验证数据（SAD：Sensitive Authentication Data），或可能影响持卡人数据环境（CDE）安全性的实体，包括但不限于商户、处理商、收单机构、发卡机构和其他服务提供商。PCI DSS 的要求适用于以下场景：

- 由以下内容组成的持卡人数据环境（CDE）：
  - 存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）的系统组件、人员和流程，和
  - 可能不存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）的系统组件，但它们可以不受限制地连接到那些存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）的系统组件。
- 可能影响持卡人数据环境（CDE）安全的系统组件、人员和流程。

根据上述描述，我们可知 PCI DSS 的要求适用于系统组件（技术实现）、人员和流程。人员和流程比较容易进行明确。在实际 PCI DSS 合规过程中，确定合规范围内的系统组件需要实体和合格的安全评估员（QSA：Qualified Security Assessor）投入大量的工作。通常是实体负责定义 PCI DSS 合规范围系统组件，并由 QSA 验证系统组件是否满足 PCI DSS 范围确定的要求。详细的 PCI DSS 合规范围确定可参考 PCI 标准委员会（PCI SSC：PCI Security Standards Council）提供的指导文件《Guidance for PCI DSS Scoping and Segmentation》。以下是 PCI DSS 合规过程中确定系统组件范围的注意事项：

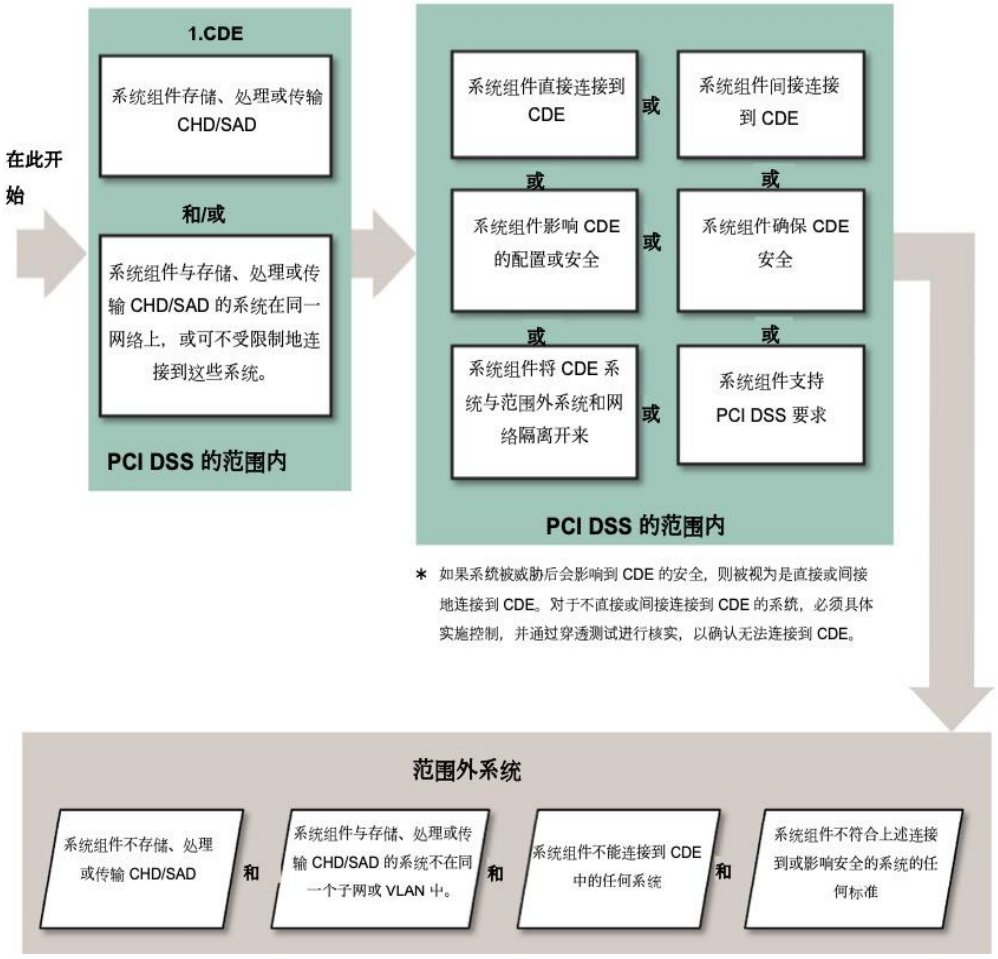

图 1：PCI DSS 确定系统组件范围的注意事项（图片源自 PCI DSS 标准 V4.0.1）

下表包含上图各类别系统组件的详细信息：

系统类别	描述	范围和适用性
持卡人数据环境	■ 系统组件存储、处理或传输	**这些系统：**

（CDE）系统	CHD/SAD。 ■ 系统组件位于同一网段上，例如，与存储、处理或传输 CHD/SAD 的系统位于同一子网或 VLAN 中。	■ 在 PCI DSS 的范围内。 ■ 必须进行评估，以确定每项 PCI DSS 要求的适用性。
连接到和/或影响安全的系统	■ 系统组件位于不同的网络（或子网或 VLAN）上，但可以连接或访问 CDE（例如通过内部网络连接）。 ■ 系统组件可以通过另一个系统连接到或访问 CDE，例如通过连接到提供对 CDE 访问的跳转服务器。 ■ 系统组件可能会影响 CDE 的配置或安全性，也可能影响 CHD/SAD 的处理方式，例如 web 重定向服务器或名称解析服务器。 ■ 系统组件为 CDE 提供安全服务，例如网络流量过滤、补丁分发或身份验证管理。 ■ 系统组件支持 PCI DSS 要求，例如时间服务器和审计日志存储服务器。 ■ 系统组件将 CDE 从范围外的系统和网络中分割出来，例如配置为阻止来自不可信网络的流量的防火墙。	**这些系统：** ■ 在 PCI DSS 的范围内。即使连接仅限于特定系统上的特定端口或服务，这些系统也包含在范围内，以验证适用的安全控制措施是否到位。 ■ 必须进行评估，以确定每项 PCI DSS 要求的适用性。 ■ 不得在 CDE 系统和范围外系统之间提供访问路径。
范围外系统	■ 系统组件不存储、处理或传输 CHD/SAD。 和 ■ 系统组件与存储、处理或传输 CHD 的系统不在同一网段或同一子网或 VLAN 中。 和 ■ 系统组件无法连接或访问 CDE 中的任何系统。 和 ■ 系统组件不能访问 CDE，也不能通过范围内系统影响 CDE 的安全控制。 和 ■ 系统组件不符合上述连接到或影响安全的系统的任何标准。	**这些系统：** ■ 不在 PCI DSS 的范围内；因此不需要 PCI DSS 控制。 ■ 无法访问任何 CDE 系统；如果有任何访问权限，则系统在范围内。 ■ 被视为不受信任（或“公共”）的系统（无法保证该部分系统已得到适当的保护）。 ■ 如果与已连接或影响安全的系统位于同一网络（或子网或 VLAN）上，或以其他方式与其相连，则必须实施控制措施，以防止范围外的系统通过范围内的系统访问 CDE。这些控制措施必须至少每年验证一次。

PCI DSS 标准中针对“系统组件”提出了如下的定义。系统组件包括网络设备、服务器、计算设备、虚拟组件、云组件和软件。系统组件的示例包括但不限于以下内容：

- 存储、处理或传输账户数据（Account Data）的系统（例如，支付终端、授权系统、清算系统、支付中间件系统、支付后台系统、购物车和店面系统、支付网关/交换系统、欺诈监控系统）。
- 提供安全服务的系统（例如，验证服务器、访问控制服务器、安全信息和事件管理（SIEM）系统、物理安全系统（例如，标记访问或 CCTV）、多因素验证系统、反恶意软件系统）。
- 分割控制系统（例如，内部网络安全控制）。
- 可能影响账户数据（Account Data）或持卡人数据环境（CDE）安全的系统（例如，名称解析或电子商务（网络）重定向服务器）。
- 虚拟化组件，例如虚拟机、虚拟交换机/路由器、虚拟设备、虚拟应用程序/桌面和虚拟机监视器。

- 云基础设施和组件，包括外部和内部，并包括容器或图像的实例、虚拟私有云、基于云的身份和访问管理、驻留在内部或云中的 CDE、带有容器化应用程序的服务网格以及容器协调工具。
- 网络组件，包括但不限于网络安全控制、交换机、路由器、VoIP 网络设备、无线接入点、网络设备和其他安全设备。
- 服务器类型，包括但不限于 Web、应用程序、数据库、身份验证、邮件、代理、网络时间协议（NTP）和域名解析系统（DNS）。
- 终端用户设备，例如计算机、笔记本、工作站、管理工作站、平板电脑和移动设备。
- 打印机，以及扫描、打印和传真的多功能设备。
- 任何格式的存储账户数据（Account Data）（例如，纸质文件、数据文件、音频文件、图像和视频记录）。
- 应用程序、软件和软件组件、无服务器应用程序，包括所有购买的、订阅的（例如，软件即服务）、订制和定制软件，包括内部和外部（例如，互联网）应用程序。
- 实施软件配置管理的工具、代码库和系统，或用于将对象部署到 CDE 或可能影响 CDE 的系统。

对于实体未分割的网络，我们通常称该网络为扁平网络。在 PCI DSS 合规过程中，实体整个扁平网络涉及的系统组件均需要纳入 PCI DSS 的评估范围。实体可以通过一些物理或逻辑方法来实现将持卡人数据环境（CDE）与实体网络的其余部分进行恰当的分割。在达到被分割的系统组件如被威胁也不会影响 CDE 的安全的前提下，被分割的系统组件可以不纳入 PCI DSS 的评估范围。需要明确的是，针对合规范围的分割并不是 PCI DSS 的要求，但是通过分割可以减少 PCI DSS 评估的范围；降低 PCI DSS 评估的成本；降低实施和维护 PCI DSS 控制的成本和难度；降低实体账户数据（Account Data）的泄漏风险。

以下是分割对 PCI DSS 合规范围的影响示意图。

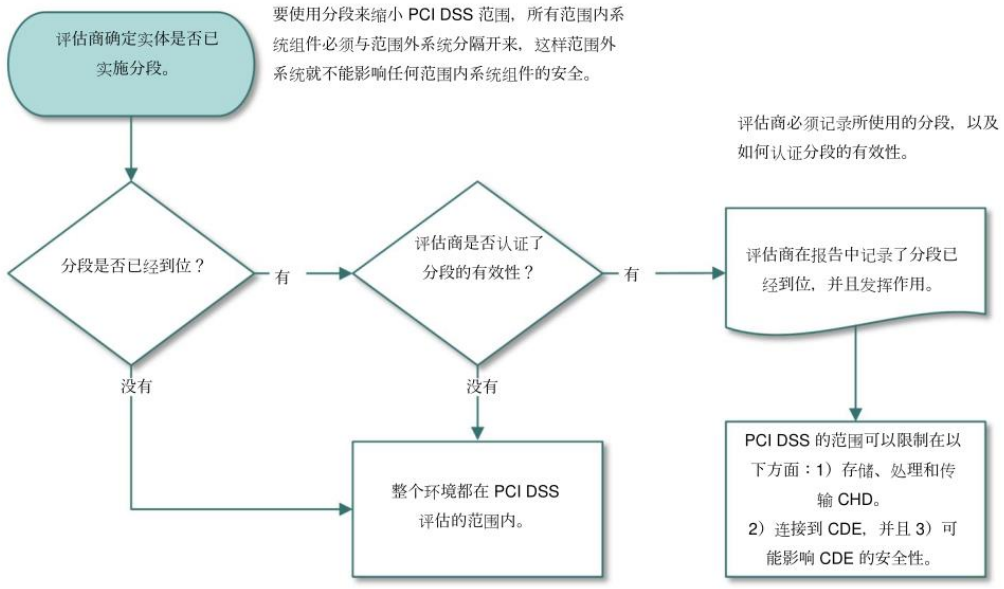

图 2：分割对 PCI DSS 合规范围的影响示意图（图片源自 PCI DSS 标准 V4.0.1）

3 现代网络架构的范围确定和分割措施实施

网络分割是一种基本的安全措施，它通过隔离系统和网络，以尽量减少事件的影响，并更容易限制未经授权的访问。网络分割允许根据系统的安全需求实施安全控制，最终将 PCI DSS 的合规范围缩减到实体持卡人数据环境（CDE），连接到持卡人数据环境（CDE）和可能影响持卡人数据环境（CDE）安全的必要系统组件和流程。

传统的采用防火墙，路由器，交换机，负载均衡构建的网络架构通常遵循基于边界的安全模型，其中明确定义的网络边界充当主要防线。然而随着技术的发展，越来越多的实体会采用包括云、虚拟化和容器化等使组织能够快速扩展资源，采用微服务架构，并利用无服务器计算的技术。这些技术的引入都会导致网络拓扑的变化。网络边界不再局限于传统的物理边界，而可能跨越多个云服务提供商（CSP：Cloud Service Provider）的区域（Regions）、可用区（Availability Zones）、虚拟私有云（VPC：Virtual Private Cloud）甚至混合环境。随着新技术的演进和实现，衍生了基于不同技术体现的网络架构，当前主流的现代网络架构主要包括如下类型：

- 云环境和多云环境（Multi-Cloud Environments）架构。
- 零信任（Zero Trust）架构。
- 混合持卡人数据环境（Hybrid Cardholder Data Environments）架构。
- 网络虚拟化技术（Network Virtualization Technologies）架构。
- 软件部署（Software Deployment）架构。

现代网络架构的动态特性和不断发展的网络拓扑结构在实现和维护稳定的网络分割方面提出了独特的挑战。为了支持这一快速的技术发展，安全策略必须不断提升。传统的网络安全控制（NSC：Network Security Controls）已不能在不同环境之间无缝转换，这导致安全策略需要从根本上转向以身份和访问管理（IAM：Identity and Access Management）为中心的策略，而这一转变也导致了零信任架构模型的发展。零信任架构模型的运行假设是：无论用户或系统在网络中的位置如何，都无法固有地信任它们。安全控制是根据系统组件身份、设备状态和其他情境因素实施的。零信任与云计算原则非常相似，云计算原则侧重于细粒度的访问控制和对每笔交易或通信的验证，而不受网络边界的限制。

下面，笔者将探讨采用云环境、零信任，以及混合网络架构的实体如何在 PCI DSS 合规过程中确定合规范围，且通过实施有效的分割措施，从而缩减 PCI DSS 的合规范围。

3.1 云环境和多云环境架构

当一个实体的云基础设施依赖于一个或多个不同的 CSP 时，实体 PCI DSS 合规的范围被成为云环境。根据依赖的 CSP 的数量不同，实体 PCI DSS 合规的范围也可能被称为单一云环境或者多云环境。在 PCI DSS 合规过程中，单一云环境和多云环境本质上是一样的，只是多云环境可能需要额外考虑不同 CSP 之间互联和数据传输的安全保护的问题。为了便于读者进行全面的了解，下面我们将以共有云的多云环境架构作为探讨重点。

3.1.1 多云环境架构 PCI DSS 合规范围确定

在多云环境中，CSP 通常会为机构提供基础架构即服务（IaaS：Infrastructure as a Service），平台即服务（PaaS：Platform as a Service）和软件即服务（SaaS：Software as a Service）类型的云服务。PCI SSC 发布的《PCI SSC Cloud Computing Guidelines》中针对不同类型的云服务进行了定义。以下是来自上述文档的截图。

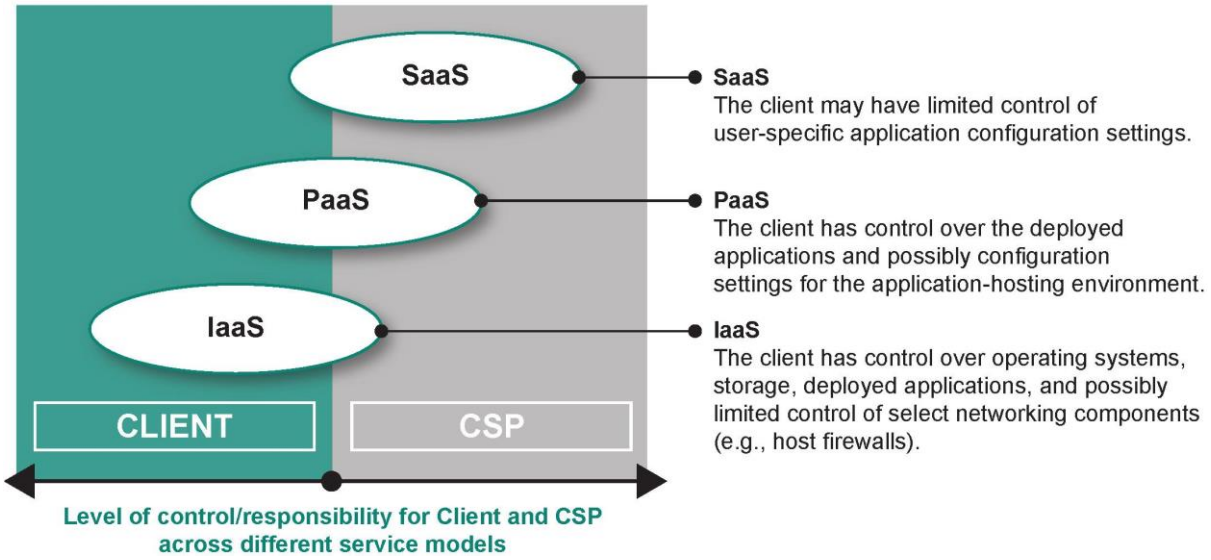

图 3：机构和 CSP 针对不同类别云服务的控制/责任矩阵（图片源自 PCI SSC Cloud Computing Guidelines）

针对机构采用多云环境进行 PCI DSS 合规的场景，我们在确定机构合规范围时需要考虑如下内容：

- 明确合规范围涉及哪些 CSP。
- 明确系统组件部署的区域（Regions）、可用区（Availability Zones）、VPCs。
- 识别机构使用的云服务资源，并对不同云服务资源根据《PCI SSC Cloud Computing Guidelines》进行分类，以确定使用的云服务属于类型（如 IaaS，PaaS 或者是 SaaS）。
- 识别持卡人数据环境（CDE）的系统组件（存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）的系统组件。如支付相关应用/服务器，数据库服务/服务器）。
- 识别不受限制地连接到持卡人数据环境（CDE）的系统组件（如与持卡人数据环境（CDE）系统组件同一网段的系统组件）。
- 识别可能影响持卡人数据环境（CDE）安全的系统组件。
- 识别为持卡人数据环境（CDE）提供安全服务的系统组件。
- 识别面向公网提供服务的域名和负载均衡实例。
- 识别从机构多云环境连接到外部机构且涉及账户数据（Account Data）传输的链路流经的系统组件（如 NAT）。
- 识别从机构办公环境/系统运维管理员远程访问持卡人数据环境（CDE）的链路或者系统组件。
- 判断机构所使用的 VPCs 内部是否属于扁平网络。如 VPCs 使用了网络隔离技术，需要判断隔离技术是否能达到有效的网络分割效果；如机构采用扁平网络，或者网络分割不能符合 PCI DSS 分割的要求，则需要考虑将机构所有多云环境的系统组件纳入 PCI DSS 合规范围。
- 如实体使用容器化的云服务（如 K8S，kubernetes）或者 Serverless 云服务（如 AWS Fargate），需要查阅 CSP 提供的合规责任矩阵，确认底层操作系统的合规职责责任归属。

3.1.2 多云环境架构有效的分割技术

实施多云设计的组织在实施分割控制之前，应该首先考虑如何将这些环境互连。为了在各种云环境中实现 PCI DSS 范围内和范围外系统之间的适当分割，每个实体都应该实施一个整体连接策略，然后配置分割控制以细化其持卡人数据环境（CDE）的范围。客户对互联互通的一些选择包括：

- 站点到站点 VPN：此连接选项可以通过使用 CSP 管理的服务和 CSP 计算机平台内的客户或提供商管理的基础设施来实现。
- 专线：客户和 CSP 可以合作实现环境之间的专用链接，从而在多个云环境之间建立私有的直接连接。

- 在公共互联网上公开 IP：可以通过 NAT 配置或 CSP 配置让已部署或管理的系统组件访问公共互联网，并使用访问控制列表（ACL）来控制允许或拒绝的流量。

3.1.2.1 网络层分割

当 CSP 之间通过站点到站点 VPN 或专线建立连接时，机构在其 CSP 之间创建的私有连接，可以使用私有 IP 空间。这并不能单独实现 PCI DSS 范围内和范围外系统之间的充分分割。由于大子网通常配置为互连，这些子网可能包含可以不适用 PCI DSS 要求的系统，因此应实施额外的分割措施，将这些系统从评估范围中删除。机构可以使用云管理服务（如安全组，云防火墙），或供应商开源或定制解决方案来实施网络安全控制（NSC）。他们可以配置防火墙规则、网络 ACL、网络策略或其他网络安全技术来控制网络流量，以实现网络或应用层系统之间的网络分割。这种细分网络分割的目标是确保 PCI DSS 合规范围外的系统组件无法访问 PCI DSS 合规范围内的系统组件或账户数据（Account Data），并且不会影响持卡人数据环境（CDE）的安全性。

对于在公共互联网上暴露的系统组件，机构负责在其 CSP 之间的入口和出口侧实施适当的访问控制。使用网络层分割时，客户应在网络边缘实施 NSC，其中包含处理或传输账户数据（Account Data）的系统组件，或可能影响账户数据（Account Data）安全性的系统。可以使用代理将内部系统暴露给公共互联网，并仅允许流量流向需要访问的备用 CSP 系统组件，从而控制流量。虽然这种通信可能发生在两个或多个 CSP 之间，但通信将穿越公共互联网，这被视为不受信任，因此受 PCI DSS 要求 4 以及要求 1 的约束，以确保在公开暴露的 PCI DSS 范围内的系统之间配置最小特权。

3.1.2.2 主机层或应用层分割

在多云环境中，无论连接类型如何，使用主机和应用程序层分割都有优势，因为它将有关 CSP 网络解决方案的细节抽象到主机或应用程序级别。基于主机的防火墙解决方案可以为运行范围内系统组件的特定系统提供一定程度的分割，而无需从范围中删除整个网络段。这提供了拥有更简单的网络架构的能力，其中分割控制接近存储、处理或传输账户数据（Account Data）的特定主机。分割控制可以应用于应用程序层，该应用程序层可能包含 API、微服务、容器和数据库，其中底层基础设施可能因各个 CSP 的部署而异。这种级别的分割通常通过软件定义网络、服务网格或其他提供策略引擎或控制平面的产品来实现，这些产品允许应用程序管理员配置哪些应用程序可以相互通信。可以在这种技术的基础上构建一个额外的审批层，以确保在允许生产环境中的系统之间进行额外通信之前对更改进行审查和验证。

3.1.3 多云环境架构分割有效性验证

验证分割控制有效性的渗透测试应包括 CSP 管理节点和机构系统之间的测试，以及共享基础设施上机构之间的测试以验证隔离效果。它应该考虑多云环境中的架构细微差别，例如无服务器组件、容器集群、Sidecar 或类似的代理设备，以及子网、路由表和安全组。

针对分割的渗透测试应考虑从构建和部署系统或其他开发管道到范围内环境的连接，还应明确考虑 CSP 控制台或原始云资源的其他管理如何影响环境的安全性。有了这些参数，预期分割边界的识别将变得更加清晰。

在多云环境中执行分割渗透测试时，应针对下面描述的每种潜在情况进行以下考虑：

测试类型	注意事项
在不同的虚拟私有云（VPC）内部和之间	分割测试不仅仅涉及使用端口扫描技术在范围内和范围外的 VPC 之间验证第 3 层访问控制列表（ACL）的存在。测试应考虑 VPC 是否以及如何相互连接，以及这些连接点是否可被利用。此外，测试应考虑组织如何更改其云资源（包括 VPC 配置），并评估是否有任何测试场景应模拟攻击控制台或类似的控制平面以更改 VPC 配置以击败分割控制。
使用同一 CSP 中的多个账户进行账户间连接	许多组织在给定的 CSP 中使用多个云资源账户（例如，CSP 客户可能有许多项目，每个项目都在自己的租户中运行）。在许多情况下，这些租户是组织范围的主账户的附属账户，可能会将资源部署到相同或相邻的 VPC 中。这些单独的账户可能有连接或交互的正当理由，分段测试应考虑这些账户之间的范围边界以及两者之间的连接是否可被利用。与其他分段测试一样，测试应考虑对控制平面（例如，主账户控制台）的攻击以更改

	配置以获取访问权限，或者攻击者建立具有新云资源的新账户并尝试与合法云资源交互的攻击。
跨越多个 CSP	使用多云环境的组织将在这些不同的 CSP 组件之间建立连接。这些可能涉及 WAN 连接、远程访问、公共网络连接或使用组合身份和访问管理（IAM）的链接。 渗透测试应考虑实施分割以隔离不同 CSP 中的组件以及分割通过特定定义的机制提供连接的场景，以确定渗透测试是否可以阻止或允许建立新的非预期连接。 此外，在使用联合用户账户集或其他权利的环境中进行测试时，应考虑针对授权过程的攻击是否允许以非预期或有害的方式进行跨 CSP 访问。

3.2 零信任架构

零信任（Zero Trust）架构旨在根据个人、设备和服务各自的分类，不断重新验证其对特定资源的真实性和授权。虽然采用“默认拒绝”的安全方法，但实施零信任（Zero Trust）架构可以应用超越传统网络安全控制的详细、严格的分割。

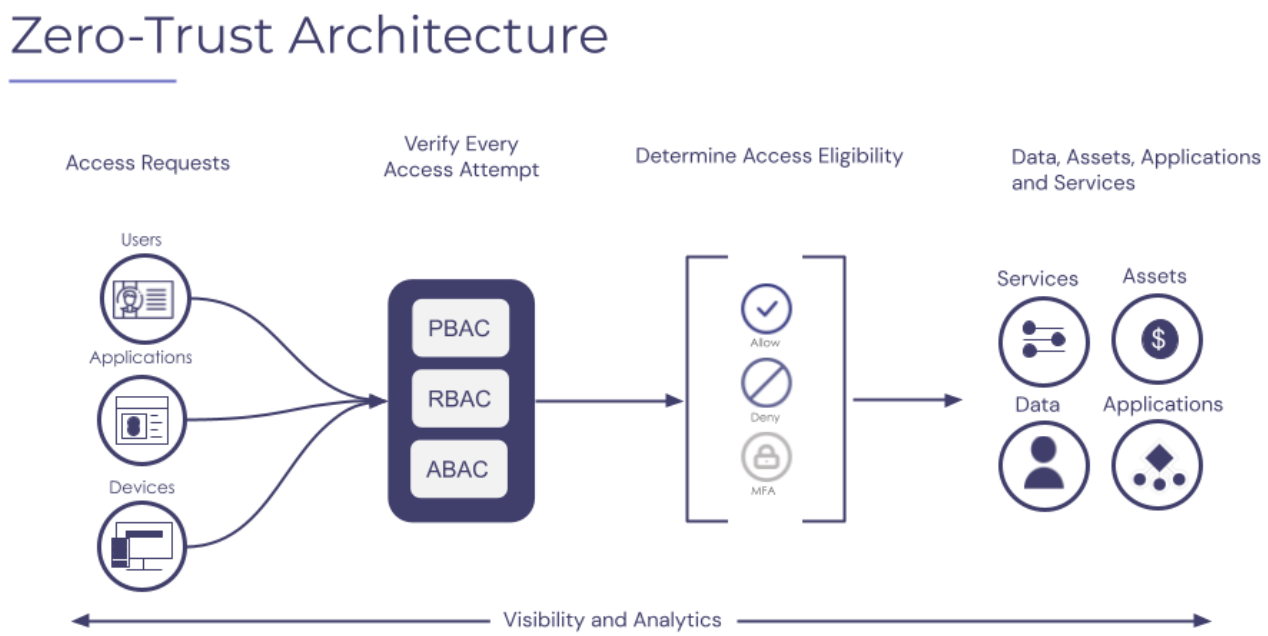

图 4：零信任架构示意图（图片源自 https://www.skyflow.com/post/what-is-zero-trust）

在传统架构中，持卡人数据环境（CDE）边界由包含存储、处理数据或传输数据的设备的网络段定义。范围内的所有设备也被视为在 PCI DSS 持卡人数据环境（CDE）范围。相比之下，零信任（Zero Trust）架构可以依赖于单个设备本身，并受软件定义的检查点的约束，这些检查点决定了哪些数据可以在组件之间传递。

3.2.1 零信任架构 PCI DSS 合规范围确定

零信任（Zero Trust）架构旨在通过精细的实时策略实施点保护托管资源。这些策略机制根据各种因素确定谁或什么可以查询资源。只有满足这些精细策略时，数据才能在主体和客体之间传递。边界甚至可以隔离资源内的各个进程。针对机构采用零信任（Zero Trust）架构进行 PCI DSS 合规的场景，我们在确定机构合规范围时需要考虑如下内容：

- 识别持卡人数据环境（CDE）的系统组件（存储、处理或传输持卡人数据 - CHD 和/或敏感验证数据 - SAD 的系统组件。如支付相关应用/服务器，数据库服务/服务器）。
- 识别不受限制地连接到持卡人数据环境（CDE）的系统组件（如与持卡人数据环境 - CDE 系统组件同一网段的系统组件）。

- 识别能连接到持卡人数据环境（CDE）并能访问账户数据（Account Data）的系统组件。
- 识别可能影响持卡人数据环境（CDE）安全的系统组件（如零信任 - Zero Trust 身份认证和权限控制系统）。
- 识别为持卡人数据环境（CDE）提供安全服务的系统组件。
- 识别面向公网提供服务的域名。
- 识别从机构零信任（Zero Trust）架构网络连接到外部机构且涉及账户数据（Account Data）传输的链路流经的系统组件。
- 识别从机构办公环境/系统运维管理员远程访问持卡人数据环境（CDE）的链路或者系统组件。

3.2.2 零信任架构有效的分割技术

在为传统网络架构实施 PCI DSS 分割时，环境边界通常部分由包含符合 PCI DSS 要求的系统组件的网络段定义，并由网络段边界上的设备（如防火墙或路由器）的实施支持。如果网络分割符合 PCI DSS 要求，则该段中的所有设备也都在范围内。相比之下，零信任（Zero Trust）架构下的环境范围由这些单个设备本身组成，受软件定义的检查点约束，这些检查点决定哪些数据可以在组件之间传递。在零信任（Zero Trust）架构环境中，这些边界与数据验证和检查点一样细化，甚至可能隔离设备内的各个进程。

零信任（Zero Trust）架构专注于设备本身，通过软件定义的检查点管理设备访问，这些检查点确定每个设备允许做什么以及每个设备可以访问哪些数据和资源。随着组织的零信任（Zero Trust）成熟度的提高，其零信任（Zero Trust）架构可以采用 PCI DSS 控制来补充其政策、流程和安全策略，以帮助实时确定是否允许用户、设备和服务访问持卡人数据环境（CDE）和连接/影响安全的环境中的资源。我们在构建零信任（Zero Trust）架构时，需要考虑如下的原则：

- 验证和认证：解释如何对所有访问敏感数据的用户、设备和应用程序实施认证机制。
- 受限访问：描述如何应用最小特权原则，确保用户和系统仅具有执行其角色所需的最小访问权限。
- 微隔离：详细说明如何使用网络分割将敏感数据与网络的其他部分隔离。这应包括网络图和策略。
- 监控：记录如何监控这些控制。示例包括实时监控网络流量、用户行为和访问模式。
- 加密：描述如何在存储和传输过程中使数据变得不可读。
- 日志记录和审计：定义日志记录配置和集中化，以支持组织如何识别和应对可疑行为。

3.2.3 零信任架构分割有效性验证

零信任（Zero Trust）和经典环境中的渗透测试都有一个共同的目标，即识别漏洞和验证防御的有效性。然而，零信任（Zero Trust）模型强调内部、每笔交易的验证，而不是传统的外围防御，这大大改变了渗透测试的计划和执行方式。考虑到零信任（Zero Trust）环境的独特性，这种转变需要一种更细致的方法。

零信任（Zero Trust）环境下渗透测试的关键考虑因素如下：

基于零信任（Zero Trust）架构的方法	渗透测试策略必须针对所实施的特定零信任（Zero Trust）架构模型进行定制。这涉及通过关注微隔离控制和信任边界的验证来确认细分工作的有效性。与以广泛的外围防御为主要重点的传统环境不同，零信任（Zero Trust）需要对内部交互和信任区的执行进行细致的测试。
防御验证	在零信任（Zero Trust）环境中，重点从外围测试转移到内部防御的稳健性。渗透测试人员必须专注于验证内部安全策略在检测和缓解来自外部和内部来源的威胁方面是否有效。这涉及对访问控制、身份验证机制以及在分割区域内遏制威胁的能力进行严格测试。
横向运动测试	在传统网络中，一旦进入，实体通常是隐式信任的，允许横向移动。然而，零信任（Zero Trust）不承担任何固有的信任。测试人员必须验证网络中的每个操作或步骤都需要正确的身份验证，并经过严格的验证。测试应确保微细分有效地限制或防止横向移动，从而降低攻击者在网络内传播的风险。

目标选择	零信任（Zero Trust）环境中渗透测试目标的选择是由信任边界的粒度驱动的。测试人员必须识别并关注根据定义的特征（如数据敏感性或用户角色）授予访问权限的单个环境元素。细粒度信任结构中的设备或系统需要进行个性化测试，不包括那些仅基于网络地址的可能已包含在传统测试中的设备。
渗透测试有效载荷	在零信任（Zero Trust）环境中，可能需要专门设计用于测试分割控制的有效载荷，以挑战通过数据标记方案实现的断言。有效载荷的设计应测试管理分割网络内数据访问和移动的策略的有效性。
策略测试	零信任（Zero Trust）在很大程度上依赖于明确和强制的网络访问策略。渗透测试人员必须严格测试这些策略，以确保它们是全面的，没有可利用的漏洞。这涉及测试网络各个部分的策略执行情况，确保访问控制既有效又与组织的安全态势保持一致。
行为分析测试	零信任（Zero Trust）网络通常将用户/实体行为分析（UEBA）作为其安全框架的一部分。渗透测试人员应评估这些系统在检测和响应异常行为方面的有效性。这包括测试 UEBA 识别偏离既定基线的能力及其与零信任（Zero Trust）环境中其他安全机制的集成。
持续验证	在零信任（Zero Trust）模型中，网络环境是动态的，策略可能经常变化，通过定期渗透测试进行持续验证至关重要。测试人员应制定一个持续评估的时间表，以确保分段控制随着时间的推移保持有效。
与安全运营部门的合作	渗透测试人员应与安全运营中心（SOC）密切合作，了解现有的监控和事件响应流程。测试应包括模拟真实世界攻击的场景，以验证检测和响应机制的有效性。
文件和报告	全面记录测试过程、结果和建议至关重要。这包括关于所识别的任何漏洞、其潜在影响和建议补救措施的详细报告。在零信任（Zero Trust）环境中，记录分段控制的有效性对于持续的安全管理和审计尤为重要。

3.3 混合架构

混合架构是指同时包含本地网络和基于云服务的环境。混合架构既保留了企业对关键数据和应用程序的本地控制，又能利用云计算的灵活性、可扩展性和成本效益等优势。该技术架构目前被很多机构广泛采用。因为本地网络和云环境采用了不同的技术体系，因此采用混合架构的机构在 PCI DSS 合规过程中会面临一些因技术体系不一致所带来的挑战。比较常见的问题是对于开发能力较弱的机构，不得不维护本地和云环境两套管理流程以满足本地环境和云环境的日常安全管理。承认并解决与混合架构相关的固有风险非常重要，包括：

- 数据传输风险：确保本地和云环境之间的数据传输安全，以减轻传输过程中未经授权访问的风险。
- 集成挑战：预测并解决在不同环境中集成安全控制的挑战，平衡一致性的需求和每个平台的独特特性。
- 合规一致性：确保安全措施在本地和云部署中始终符合 PCI DSS 要求。

3.3.1 混合架构 PCI DSS 合规范围确定

针对机构采用混合架构进行 PCI DSS 合规的场景，我们在确定机构合规范围时需要考虑如下内容：

- 明确合规范围涉及哪些 CSP 和哪些物理机房。
- 明确系统组件部署的物理环境和涉及 CSP 的区域（Regions）、可用区（Availability Zones）、VPCs 。
- 识别机构使用的云服务资源，并对不同云服务资源根据《PCI SSC Cloud Computing Guidelines》进行分类，以确定使用的云服务属于类型（如 IaaS，PaaS 或者是 SaaS）。
- 识别本地和云环境持卡人数据环境（CDE）的系统组件（存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）的系统组件。如支付相关应用/服务器，数据库服务/服务器）。

- 识别本地和云环境不受限制地连接到持卡人数据环境（CDE）的系统组件（如与持卡人数据环境（CDE）系统组件同一网段的系统组件）。
- 识别本地和云环境可能影响持卡人数据环境（CDE）安全的系统组件。
- 识别本地和云环境为持卡人数据环境（CDE）提供安全服务的系统组件。
- 识别本地和云环境面向公网提供服务的域名和负载均衡实例。
- 识别从机构本地或云环境连接到外部机构且涉及账户数据（Account Data）传输的链路流经的系统组件（如 NAT）。
- 识别从机构办公环境/系统运维管理员远程访问本地或云环境持卡人数据环境（CDE）的链路或者系统组件。
- 判断机构所使用的本地网络和 VPCs 内部是否属于扁平网络。如本地网络和 VPCs 使用了网络隔离技术，需要判断隔离技术是否能达到有效的网络分割效果；如机构采用扁平网络，或者网络分割不能符合 PCI DSS 分割的要求，则需要考虑将机构所有本地网络和云环境的系统组件纳入 PCI DSS 合规范围。

3.3.2 混合架构有效的分割技术

混合架构有效的分割技术与传统网络和云环境使用的分割技术一致。传统的网络分割技术由防火墙、交换机、路由器等硬件设备组成。这些物理组件可用于分离托管在同一个或多个虚拟机管理程序上的虚拟机，类似于在物理网络中对系统进行分割的方式。这将需要具有多个网络接口的虚拟机管理程序，并且其配置必须符合各种类型网络硬件的 PCI DSS 要求。针对传统网络一般采用如下方式进行有效的网络分割：

- 基础设施级别的防火墙和网络分割。
- 虚拟机管理程序和虚拟机级别的防火墙。
- 除防火墙外，还有 VLAN 标记或分区。
- 虚拟机管理程序级别、虚拟机级别或两者的入侵防御系统，用于检测和阻止不需要的流量。
- 虚拟机管理程序级别、虚拟机级别或两者的数据丢失防护工具。
- 控制以防止通过底层基础设施发生带外通信。

对于云环境可以参考本文 3.1.2 章节提及的方式进行有效的分割。为了更有效地管理 PCI DSS 范围，必须采用符合以下关键原则的战略细分方法：

- 识别关键细分边界：明确定义和识别本地和云环境之间的关键细分边界。了解账户数据（Account Data）的流动，并确保其通过安全渠道。
- 应用一致的控制：在本地和云组件之间保持安全控制的一致性。这包括访问控制、加密标准和监控机制。
- 设计动态可扩展性：分割策略应适应动态可扩展，允许在不损害安全性的情况下无缝集成新的云资源。

在这些环境中，建立强有力的控制对于有效的分割至关重要，以下控制尤为关键：

- 基于网络的控制：利用防火墙、VLAN 和入侵检测/防御系统来实施基于网络的分割控制。确保这些控制措施在本地和云网络中得到一致应用。
- 身份和访问管理（IAM）：实施 IAM 解决方案，统一跨本地和云平台的访问控制。这包括强大的身份验证机制和最小特权原则。
- 数据加密：对传输中和静止的数据应用强大的加密协议，在所有环境中保持一致的加密策略，以保护账户数据（Account Data）。
- 明确定义混合持卡人数据环境（CDE）中管理分割的角色和职责。为分割策略的每个方面分配所有权，涵盖本地和云组件。这可确保责任制并促进本地和云团队之间的有效沟通。

3.3.3 混合架构分割有效性验证

分割测试是验证访问控制有效性并确保持卡人数据环境（CDE）保持隔离和安全的关键过程。在集成了各种组件的混合架构中，以下提供了一种全面的方法来进行彻底的隔离测试。

范围定义	明确划分测试工作的范围，包括混合环境中在处理账户数据（Account Data）方面发挥作用的所有组件。这包括本地服务器、云实例、网络设备和任何中间组件。
测试场景	精心设计各种测试场景，模拟真实世界的条件和潜在的攻击媒介。考虑从内部和外部来源进行未经授权的访问尝试的情况。这应该包括测试本地和非本地组件之间的交互，确保数据传输安全进行，并始终如一地执行访问控制。 当 WAN 连接连接到这些环境时，考虑机构从本地到云组件的用例，反之亦然，以及 WAN 连接是否用于任何类型的访问控制。还要考虑攻击，例如从本地环境中欺骗客户端试图访问云资源，或者欺骗云资源对本地请求的响应以破坏分割控制。 当远程访问网关加入这些环境时，就像在传统的本地环境中一样，考虑攻击者如何绕过远程访问网关，例如直接攻击网关系统、攻击用户配置系统（如 Active Directory 或 IAM）或冒充特权用户以击败分段控制。
依赖关系映射	了解混合环境中不同组件之间的依赖关系。识别软件定义的网络、服务网格和在零信任（Zero Trust）架构之间的关键互连和交互。这种映射对于确保不会无意中绕过分割控制至关重要。
渗透测试	进行模拟复杂攻击的逼真渗透测试演习。这包括攻击者试图利用混合环境中的潜在配置错误或弱点来未经授权访问持卡人数据环境（CDE）的情况。
合规性验证	确保分割测试符合 PCI DSS 要求。验证访问控制和隔离实践是否符合行业标准和法规。
网络图和数据流	确保网络图和账户数据（Account Data）流图描绘了不同的环境，例如本地、云托管等。
文件和报告	记录分割测试过程，包括测试场景、方法、发现和补救措施。向利益相关者提供清晰简洁的报告，突出细分策略中的优势和改进领域。

4 结语

随着新技术的不断发展，必将会涌现越来越多各种不同类型的现代网络架构。在支付生态系统中实施现代网络架构需要应对复杂的安全、合规和运营挑战。

针对机构使用现代网络架构的场景，在确定其 PCI DSS 合规范围时，我们需要依据持卡人数据环境（CDE）系统， 连接到和/或影响安全的系统，范围外系统的判断准则（详情请参考第 2 章的内容）对系统组件进行范围确定。如机构采用了分割措施缩减其 PCI DSS 合规范围，对于分割措施需要进行全面的核查和验证，以确保分割措施的有效性。

信息安全合规的建设思路是相通且互相借鉴的。希望通过针对 PCI DSS 标准的探讨，对于产业内其他安全标准和/或法规的合规建设和进一步发展也有所帮助。

A 参考资料

[1] PCI DSS Scoping and Segmentation Guidance for Modern Network Architectures https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/PCI-DSS-Scoping-and-Segmentation-Guidance-for-Modern-Network-Architectures.pdf

[2] PCI SSC Cloud Computing Guidelines https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Virtualization%20and%20Cloud/PCI_SSC_Cloud_Guidelines_v3.pdf

[3] Guidance for Containers and Container Orchestration Tools https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Containers%20and%20Container%20Orchestration%20Tools/Guidance-for-Containers-and-Container-Ochestration-Tools-v1_0.pdf

[4] Guidance for PCI DSS Scoping and Segmentation https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf

[5] Third-Party Security Assurance https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/ThirdPartySecurityAssurance_March2016_FINAL.pdf

[6] Penetration Testing Guidance https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Penetration%20Testing/Penetration-Testing-Guidance-v1_1.pdf

[7] PCI DSS Virtualization Guidelines https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Virtualization%20and%20Cloud/Virtualization_InfoSupp_v2.pdf

[8] PCI SSC https://www.pcisecuritystandards.org/