关于多云防御

关于多云防御

多云防御 (MCD) 是一个全面的安全解决方案，包含两个主要组件： 多云防御控制器 和 多云防御网关。这些组件协作建立安全的多云环境

多云防御 目前支持 Amazon Web Services (AWS)、Azure、Google Cloud Platform (GCP) 和 Oracle OCI 云账户。这些平台的支持范围各不相同。

本质上， 多云防御提供了一个复杂且简化的安全框架，协调控制器协调、网关通信和优化的数据路径处理，以实现强大且高效的多云保护机制。

本文档面向对公共云网络和安全概念有基本了解并参与各种职能团队的从业人员，包括：

- 开发运营 (DevOps 和 DevSecOps)
- 安全运营中心 (SOC)
- 安全架构师信息
- 安全架构师云架构师

有关此产品组件的详细信息，请继续阅读。

多云防御 组件

多云防御 使用公共云和软件定义网络 (SDN) 中的通用原则，将控制平面和数据平面分离，转换为两个解决方案组件 - 多云防御控制器 和 多云防御网关。

多云防御控制器

多云防御控制器 是一种高度可靠且可扩展的集中式控制器，可提供管理和控制平面。它作为软件即服务 (SaaS) 运行，由 多云防御完全管理和维护。客户访问 Web 门户以利用 多云防御控制器，或者他们可以选择使用 多云防御 提供程序来将安全性实例化到 DevOps/DevSecOps 流程中。

多云防御网关

多云防御网关 是由 多云防御控制器以模式即服务 (PaaS) 形式部署到客户公共云账户的 多云防御 软件的自动扩展队列。这提供了高级内联安全保护，以防御外部攻击，防止出口数据泄露并防止攻击横向移动。 多云防御网关包括 TLS 解密、入侵检测和防御 (IDS/IPS)、Web 应用防火墙 (WAF)、防病毒过滤、防数据丢失 (DLP) 和 FQDN/URL 过滤功能。

多云防御 SaaS 控制器

多云防御 SaaS 控制器管理网关堆栈。配备各种微服务的控制器包括一个 API 服务器，用于协调 CSP LB 和网关实例。这可以通过在负载均衡器的“目标池”中添加和删除实例来实现动态扩展，由负载均衡器本身监控。

间通信

多云防御网关与 多云防御控制器进行持续通信，大约每 3 秒进行一次通信，传输运行状况和策略更新。这可以根据需要实现主动运行状况报告、网关更换和可扩展性调整。

优化网关实例

多云防御网关 实例在高度优化的软件上运行，并结合了单通道数据路径管道，以实现高效的流量处理和高级安全实施。每个网关实例包含三个核心进程：负责策略实施的“工作线程”进程、用于流量分配和会话管理的“分发器”进程，以及与控制器通信的“代理”进程。网关实例可以无缝过渡到“服务中”以实现“数据路径重启”，从而在不中断流量的情况下实现平稳更新。

高级安全配置文件

多云防御网关在单通道数据路径管道中实施精细的安全配置文件，以满足不断变化的流量需求。客户可以根据需要灵活地启用或禁用**高级安全配置文件**。管道的单通道架构不需要将流量分流到第三方引擎。例如，在管道内选择性地触发完整的 TLS 解密，确保高效处理，而无需进行不必要的数据传输。

本质上，多云防御提供了一个复杂且简化的安全框架，协调控制器协调、网关通信和优化的数据路径处理，以实现强大且高效的多云保护机制。

第三方产品支持和版本控制

多云防御 利用其他产品和功能。为实现最佳操作，请考虑使用列出的相应版本。

互联网浏览器

对于 多云防御 组件，我们支持并建议使用以下互联网浏览器：

表 *1:* 互联网浏览器支持

浏览器	支持
Chrome	是。 我们 **强烈** 推荐此浏览器。
Firefox	是。
边缘	是。
Safari	是。
Internet Explorer	是。

AWS 的实例元数据服务

实例元数据服务 (IMDS) 用于从 Amazon EC2 实例访问实例元数据。 多云防御控制器 版本 23.10 将 IMDSv2 设置为“ **必需** ”或“ **可选** ”，具体取决于相应的 多云防御网关版本。

我们 **强烈** 建议在“ **必需** ”模式下升级到专门支持 IMDSv2 的 多云防御网关 版本，以实现 Amazon EC2 实例的最佳安全性。

注释 多云防御控制器版本23.10强制将 多云防御网关 版本23.04及更高版本默认用于EC2实例的IMDSv2。

使用下表确定将在您的环境的 EC2 实例内设置哪个 IMDS 版本：

多云防御网关版本	需要的 **IMDS** 版本
23.08	IMDSv2（必需）
23.06	IMDSv2（必需）
23.04	IMDSv2（必需）
23.02	IMDSv1 IMDSv2（可选）
22.12	IMDSv1 IMDSv2（可选）

有关 IMDS 版本以及如何迁移到所选版本的更多信息，请参阅 AWS 文档。

多云防御 组件的推荐版本

我们建议您使用最新的升级和更新来更新增强功能和新功能，并修复漏洞。有关可用更新和升级以及每个软件包的详细信息，请参阅 思科多云防御版本说明。

支持的磁盘大小

考虑适当的网关版本的以下磁盘大小支持：

表 *2:* 每个网关版本的磁盘大小

网关版本	支持的磁盘大小
23.12 及更高版本	128GB
最高 23.10	256GB

服务通告

以下公告适用于 多云防御 产品和组件。如果您对这些问题有任何疑问或疑虑，请 联系支持 人员以获取更多信息。

基于 IP 的地理阻止

从 多云防御网关 版本 23.10 开始， 思科的出口和合同合规性 将对使用 多云防御 平台和组件的客户生效。在基于 IP 的地理阻止中实施以下行为：

- 对于识别为来自具有地理阻止功能的已批准区域的IP地址的查询，DNS服务将不会应用安全或内容过滤策略。报告功能也将被禁用。DNS 查询仍将收到有效的响应，并将被视为与来自世界其他地方的流量相同的服务级别。
- 漫游客户端同步和内部域列表应继续与控制面板同步，并提供预期行为（将内部域发送到内部 DNS 服务器）。在将来这种情况会得到改变。
- 为某个国家/地区完全实施基于 IP 的地理阻止后，Umbrella 控制面板和 API 访问也将被阻止。

高级策略设置

某些策略支持其他特性或功能。

入口策略中的 XFF 报头

请注意，入口策略支持 HTTP 数据包中的 X-Forwarded-For (XFF) 报头。XFF 是标准报头用于通过代理服务器识别连接至 Web 服务器客户端的源 IP 地址的常用方法。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。