技术摘要

用于动态隔离的策略实施防火墙

随着企业网络成为数字转型的催化剂，连接变得无处不在，需要新的强制策略和网络安全解决方案来应对传统网络和安全方法的挑战。企业有线和无线网络的边界在持续改变，除了员工、客户和访客，现在物联网设备也加入到这一网络中。使用基于 IP 地址的访问控制策略和物理网络配置的传统防御模式（例如防火墙）已不再适用。

策略实施防火墙 (PEF)

一些新的网络攻击特意被设计为从网络内部发起，以绕开传统的安全防御。它们有时会在网络中滞留几周甚至几个月，只是为了在不经意间窃取数据、对数据进行加密，或者破坏 IT 资源。与此同时，IT 部门对应用层缺乏可视性，也会影响到网络应用性能和最终用户体验。

作为无线和有线网络的领导者，Aruba 率先使用了全面的边缘网络安全，其中包括高强度加密和基于身份的策略实施防火墙 (PEF) 解决方案。Aruba 策略实施防火墙是 ArubaOS 和 InstantOS 内置的一项成熟技术，并且稳定运行在**全球超过 400 万台设备上**。它是业界唯一的面向用户和设备的防火墙，提供“零信任”接入边界。

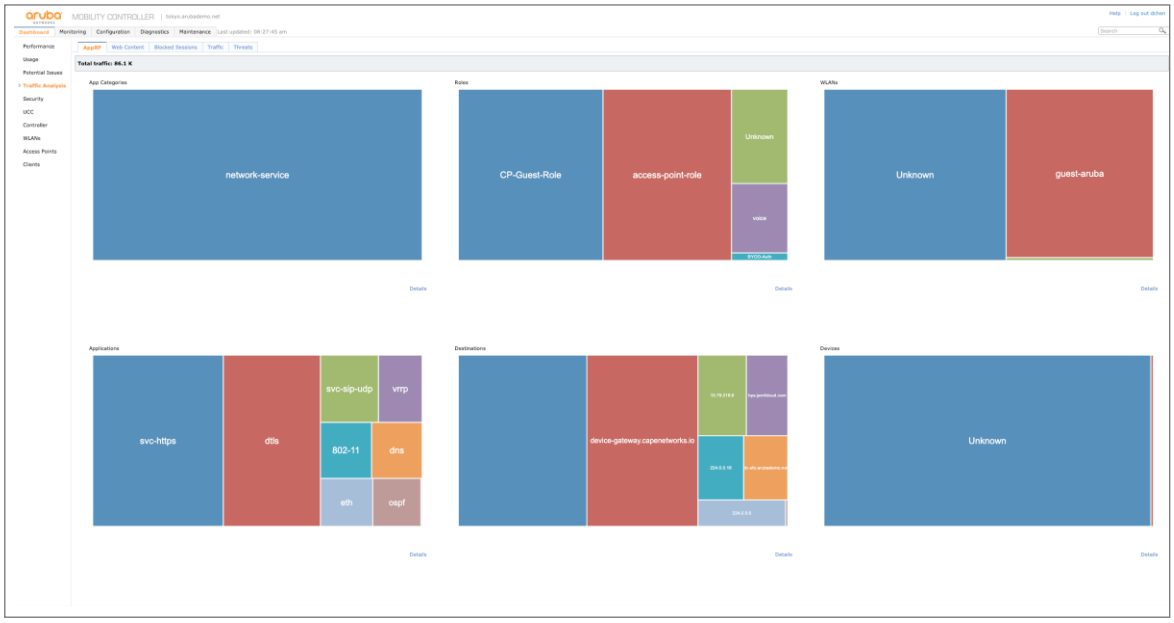
利用 VLAN 和 IP 进行控制的传统防火墙策略通常在用户或设备接入到网络中之后才可能被触发，这为高级攻击提供了可乘之机。相反，Aruba 面向用户和应用的策略实施防火墙，通过识别用户身份、流量属性和其他安全上下文来在终端发起初始连接时就进行有效的访问控制，因此可以填补这一漏洞。这一点很重要，因为攻击者连接到一个完全开放网络的每一秒钟，都可能会释放数千个恶意报文来骗取用户凭据、传播恶意软件或者进行其他破坏性活动。

主要优势

- **集中式零信任接入：**减少初始网络连接和触发防火墙策略之间的时间差距
- **Cyber Catalyst℠ by Marsh：**通过 Aruba 策略实施防火墙降低风险，有助于企业从保险公司获得增强的网络保险条款
- **用户和应用防火墙：**基于角色的访问控制最大限度地减少了配置错误
- **不需要额外的硬件：**Aruba 策略实施防火墙运行在现有的 Aruba 网络基础设施上
- **极致的性能：**包括基于硬件加速的流量处理能力
- **自动化的自我学习：**提供关于网络和应用使用情况的深度洞察数据
- **可重复使用的策略库：**使管理员能够轻松创建有用、一致的策略
- **与连接方式无关：**角色跟随用户和设备，无论通过有线、无线或者远程方式接入网络
- **安全认证：**全方位验证

CYBER CATALYST℠ 指定解决方案

采用 Aruba 策略实施防火墙的组织可以实施零信任接入模型，通过识别身份、流量属性和其他安全上下文来集中控制初始连接时终端的访问权限。由于能够帮助组织动态实施基于角色的零信任安全策略，Aruba 策略实施防火墙凭借其有效降低风险的能力而被指定为“Cyber Catalyst℠”



ArubaOS 仪表盘视图：可识别 3000 多个应用

简单安全的网络访问

作为 Aruba 体验边缘解决方案的一个关键技术，Aruba策略实施防火墙也是实现Aruba动态隔离技术的基础，可简化并保护有线和无线网络的安全。通过基于用户和应用的控制能力，IT 不需要频繁添加和改变 VLAN、SSID 或 ACL，从而显著降低运维复杂性。

凭借 Aruba 策略实施防火墙 的应用可见性功能，网络管理员能够深入了解网络上运行的应用，以及谁在使用它们。WebCC 是一个基于订阅的附加功能，通过URL 过滤、IP 信誉评估和地理位置过滤来强化 Aruba 策略实施防火墙。

基于强认证和角色控制的零信任安全保护

首先，在网络登录过程中，通过与 Active Directory (AD)、RADIUS、LDAP、SQL 数据库、以及其它基于 LDAP 的身份存储或访客数据库的集成，验证每个用户或设备的身份。确定身份后，为终端分配角色。角色是不同权限的逻辑分组，包括应用访问权限和用户及设备间的互访权限。

将用户与角色相关联的价值在于，如果用户的安全上下文发生变化（例如，设备遭到破坏），只需分配新的、更具限制性的角色，就能够立即改变访问权限，而无需设备的网络参数进行重新配置。

在分配了用户或设备的角色后，系统会根据组织的网络安全政策来应用策略。这些策略在整个网络中始终跟随用户，并统一应用于无线、有线和 VPN 连接。如果设备没有在系统中注册过，也可以基于设备类型指纹应用默认策略（例如，“所有电视屏幕都可以访问 DNS、DHCP 和基于互联网的 HTTPS 服务，但不能访问内部资源”）。

当一个已经注册过的用户连接到受Aruba策略防火墙控制的接入网络时，就会被分配一个角色（例如“医院人力资源经理”），以及一组访问IT资源的权限。在这种情况下，每个用户都能获得最恰当的权限。例如，医院的IT管理员只能访问其工作所需的工具和网络服务：电子邮件、Microsoft Office 和员工记录，但不能访问患者医疗保健信息。如果用户终端受到侵害，Aruba 策略实施防火墙会自动为用户终端分配并应用新的角色（“潜在危害，发送至隔离区”）。

因此，Aruba 策略实施防火墙省去了繁重、手动和容易出错的 VLAN 配置工作，同时提供了精细并且实时的强制策略。

此外，由于 Aruba 策略实施防火墙具有**第 7 层应用感知能力，可以通过深度数据包检测识别 3000 多种应用**。因此，还可以针对特定用户或设备、以及特定应用实施精细化的流量隔离策略，这种技术在基于 VLAN 的方法中完全无法实现。

丰富的应用可见性

基于深度数据包检测 (DPI)的丰富的应用可见性功能，可用于及时排查应用性能故障、制定全局策略和未来增长规划。

内置仪表盘为 IT 部门提供了简单、强大的移动应用使用情况和性能视图，可以根据用户角色、应用、网络和其他标准进行排序：

- **移动应用：**即使像 Box 这样的公司应用和像 Apple FaceTime 这样的个人应用运行在同一个移动设备上，也可轻松区分。
- **网络服务，例如 Apple AirPrint 和 AirPlay：**Aruba 优化了 IP 组播视频流量，自动区分服务优先级，并增加了策略控制。
- **基于 Web 的应用：**许多基于 Web 的应用使用同一个端口与客户端通信，并显示为 HTTP 流量。Aruba 的技术通过解析目的地址来识别独特的应用，例如 Facebook、Twitter、Box、WebEx 和数百个其他应用。
- **加密应用：**对于加密的流量，Aruba 使用试探法来寻找流量模式，并建立唯一的指纹来识别这些应用。

基于策略的流量管理和控制

Aruba 策略实施防火墙具有带宽流量控制优化功能。基于角色的策略可以限制特定用户或用户类别的最大允许带宽，防止超级用户独占网络资源。

同时，流量管理策略可以保证设备的最小带宽，以确保用户保持高工作效率。Aruba 策略实施防火墙还能够通过优化广播和组播流量改善应用性能。

对于 mDNS、ARP 和 NetBIOS 这类非常消耗空口带宽的协议，Aruba策略实施防火墙可以将其完全过滤，并限制于网络的特定部分。

此外，Aruba 策略实施防火墙还提供全面的在线威胁情报，实时保护用户和网络免受恶意文件和 URL 的攻击。策略可以基于 URL、IP 信誉和地理位置（WebCC 订阅）以及用户角色或设备上下文来实施。

服务质量控制

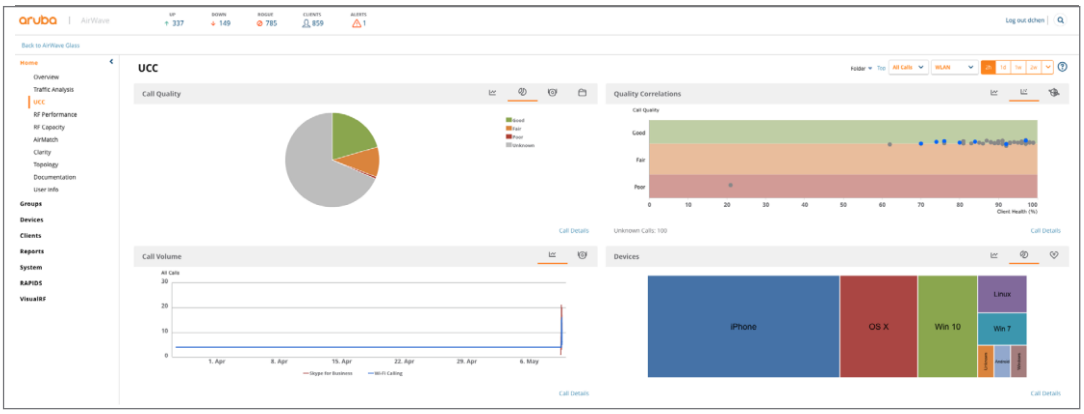
在识别移动应用并对其进行可视化之后，可以实施访问控制和 QoS 策略以保障企业应用相对于个人应用的优先级。在移动设备争抢 Wi-Fi 带宽的时候，Aruba 策略实施防火墙可以保障您最关心的应用性能。

通过优化 Apple AirPrint 和 AirPlay 等网络服务，Aruba策略实施防火墙会为 IP 组播视频流量自动分配优先级，并自动识别和优先处理 Apple FaceTime 和诸如 Microsoft Teams 或 Skype for Business 的加密语音和视频会话流量。

此外，常见的网络服务，例如 Pandora、Netflix、Google Drive、Citrix GoToMeeting、Salesforce.com 和 Dropbox，也可以根据用户、设备和位置获得恰当的优先级策略。

Aruba 策略实施防火墙可以对流量应用多种防火墙安全措施，包括允许、丢弃、日志或拒绝。数据包也可以打上 802.1p 或 DSCP 标记，根据优先级分配到多个队列中，并根据协议重定向到不同的目的地。

先进的语音和视频协议感知特性允许将恰当的 QoS 自动应用于控制协议和呼叫会话。



Aruba UCC 仪表盘视图

Aruba 策略实施防火墙确保将适当的优先级映射到相关的协议。例如，如果去往或来自用户的语音流量的相关 QoS 设置不一致，则该流量会被重新标记正确的优先级。

对于关键的统一通信 (UCC) 服务，了解呼叫状态和呼叫质量有助于实现更智能的 VoIP 管理。基于 AI 的智能，结合 Aruba 的 AirMatch 和 ClientMatch 射频优化技术，可以更好地规避对进行中的通话的干扰。

UCC 的最佳体验

通过内置的 UCC 仪表盘，Aruba 为各种 UCC 应用提供了关键通话质量指标的可视化，这些应用包括 Microsoft Teams、Microsoft Skype for Business、Apple FaceTime、Wi-Fi 通话、Jabber/Spark 和 SIP。

通过悬停和直接单击仪表盘，您可以获得详细的报告和故障排除信息，例如电话号码、通话质量、通话详细记录 (CDR) 和通话准入控制 (CAC)。

仪表盘包括：

- 通话质量和相关性 – 这些图表在 WLAN 选项卡下显示接入点到客户端的通话质量，在“端到端”选项卡下显示端到端质量，包括通话所基于的有线和无线线路。
- 通话量 – 此图显示基于 UCC 应用类型的通话总数。例如，SIP、Lync、SCCP、H.323、NOE、SVP、VOCERA 和 FaceTime。
- 设备 – 此图显示了按设备类型划分的语音会话。例如，iPhone、OS X、Win 10 等。

高性能流量处理

在 Aruba 策略实施防火墙中，策略执行不会以降低性能为代价，也不需要额外的外部硬件。

Aruba 移动控制器专为高速处理网络流量而设计，配有专用的网络控制、网络流量处理和加解密硬件。

因此可以实现高性能、低延迟的强制策略，并可扩展到数千个用户和数十万个活动会话。

外部认证和授权接口

Aruba 策略实施防火墙与授权和认证服务器整合扩展了对用户的细粒度控制。可以实现自动断开网络连接、重新分配用户角色和动态更新防火墙策略等控制。

这一功能通过两个 API 接口 实现 - IETF 标准 RFC 3576 或者基于 XML 的简单而灵活的 API。这两个 API 都允许外部系统对移动控制器进行用户和策略控制。

第三个接口是内置的系统日志处理器，它接受来自外部系统的系统日志消息，利用正则表达式对日志消息进行匹配，然后提供可配置的操作，例如更改用户角色或将用户列入黑名单。

缩短平均攻击响应时间

不再需要通过修改 VLAN 配置来实施控制，调整 IT 访问策略所需的资源就可以大大减少，并自动响应网络攻击。

借助 Aruba 策略实施防火墙的细粒度控制，可以有效抑制来自内部的网络攻击，即使这类攻击采用了合法凭证并且耐心地在整个网络中尝试横向扩展。如果用户或设备的角色具有一组有限的访问权限，那么攻击者也同样会受到角色和访问控制策略的限制。从而可以抑制攻击者在网络内部的横向扩展。

一旦检测到数据泄露或勒索软件等攻击，Aruba 策略实施防火墙可以通过修改用户角色来自动更新与用户或设备相关的权限。攻击响应可以包括降低网络带宽、流量隔离和彻底阻断等一系列操作。基于简单的 API 集成，攻击警报可以来自组织安全生态系统中的任何第三方安全产品。

与 CLEARPASS POLICY MANAGER 集成

Aruba 策略实施防火墙是一个独立的访问控制解决方案，同时也可以与 Aruba 的 ClearPass Policy Manager 无缝集成。ClearPass 可以为Aruba策略实施防火墙提供简化的身份验证和策略定制能力，从而实现中心化的身份认证和强制策略的大规模部署。ClearPass 的一个主要优点是，它可以把从独立办公室到整个跨国企业的认证、授权和访问控制功能无缝整合在一起。

ClearPass 还可以将策略、角色和攻击响应与 140 多个 Aruba 技术合作伙伴解决方案（从移动设备管理到服务台解决方案，例如 ServiceNow）集成在一起。

最高级别的安全认证

Aruba 策略实施防火墙 (PEF) 经过 NIAP 认可，符合共同标准和 DoDIN-APL。Aruba 策略实施防火墙也在 NATO 批准的产品清单上。

易于实施

为确保 IT 部门能够轻松实施和保护其环境，Aruba策略实施防火墙作为可选的Aruba控制器软件许可提供，并缺省包含在 Aruba Instant 无线接入点中。它还可以与 Aruba 网络交换机结合，用于动态隔离技术的应用，并且不需要额外的硬件。

总结

由于传统防火墙策略的实施都是基于 VLAN 的，并且只在设备接入网络后才能生效，因此 IT 团队难以跟上在网络连接刚刚开始时的中和攻击的步伐。Aruba 策略实施防火墙是唯一能够解决这一问题的访问控制解决方案，该解决方案基于用户或设备的身份和角色，而不管位置、连接方法或设备类型，在网络连接点提供零信任边界。

借助 Aruba 策略实施防火墙实施的精细访问权限，组织可以在检测到攻击时自动阻止或隔离端点，防止网络攻击的进一步扩散。

因为 Aruba 策略实施防火墙是基于现有 Aruba 网络基础设施上的软件解决方案实施的，所以不需要安装额外的硬件就可以确保只有经识别和授权的用户和设备连接到网络。

功能概述	
功能	**优势**
基于状态的第 4-7 层应用可见性	通过控制双向数据流，在网络边缘提供独特的可见性和安全性
性能零影响	不会降低控制器的流量处理性能
用户防火墙	根据用户身份、设备类型、应用或目的地设置基于角色的策略
UCC 仪表盘	查看通话质量指标，例如 MOS，以及 Teams 和 SIP 等 UCC 服务的健康状况
应用感知 QoS	使管理员能够区分应用流量的优先级并控制射频层行为
实时应用仪表盘	实时跟踪最常用应用、设备和目的地，以便进行网络监控或故障排除
可重复使用的策略库	使管理员能够轻松创建有用、一致的策略
历史数据收集	使用 AirWave 可以获得应用的长期使用情况并合理规划容量
ClearPass 和外部 RADIUS 集成	认证用户，允许第三方设备或 ClearPass 进行详细的设备识别和动态策略更新

Cyber Catalyst

在 Cyber Catalyst℠计划中，领先的网络保险公司评估并确认他们认为能有效降低网络风险的解决方案。参与的保险公司包括 Allianz、AXIS、AXA XL（AXA 的一个部门）、Beazley、CFC、Munich Re、Sompo International 和 Zurich North America。Microsoft 是该计划的技术顾问。

aruba
a Hewlett Packard Enterprise company

TB_PEF_090419 a00073442enw