



白皮书

# 第 7 层可视性与可控性

2013 年 2 月

本文档重点介绍 Meraki 自学习第 7 层流量分析引擎的基础知识及其帮助实现的丰富可视性和直观管理。

# 目录

|                 |    |
|-----------------|----|
| 1 简介            | 3  |
| 2 Meraki 流量整形技术 | 5  |
| 3 管理和控制         | 8  |
| 4 与典型解决方案的比较    | 10 |
| 5 结论            | 11 |

版权所有

© 2013 思科系统公司。保留所有权利

商标

Meraki® 是思科系统公司的注册商标。

# 1 简介

## 应用可视性的价值

企业工作效率对互联网访问的日益依赖让企业期望实现高性能和无处不在的连接。同时，自带设备 (BYOD) 和云计算的趋势也导致企业网络中使用的设备和应用数量快速激增。这些因素可能会给传统网络带来压力，并造成网络性能瓶颈等问题。在成本受限、带宽容量有限并且期望为关键应用提供最低服务质量 (QoS) 的情况下，提供高性能和应用优化常常被视为重要的应对手段。满足这些要求对预算和时间有限的 IT 部门可能是一个不小的挑战。

有两个因素对于应对这些挑战至关重要：一者是清楚地洞察网络性能，一者是有能力实施优化网络性能的网络策略。网络管理员必须具备对网络使用情况的彻底了解，不仅是了解带宽方面的使用情况，还要了解所有的层，甚至包括应用层的使用情况。了解访问特定应用的设备和用户以及在每个应用上所花的时间和流经的流量可以提供宝贵的情景信息，从而了解用户行为并更快地设计有效的网络策略。最后，支持创建和应用灵活的策略集的内置工具集可以确保 IT 管理员按照应用信息采取措施，从而帮助实现最佳网络性能。

应用可视性有一种新用法，那就是利用此数据通过交互式营销活动和具有针对性的体验来提高客户参与度。了解应用、用户和所花时间的流动可以帮助零售店或热点运营商的营销部门回答那个老生常谈的问题：“我的用户正在干什么？”这种级别的可视性及其提供的切实可行的数据也是网络基础设施中需要应用层可视性的另一个原因。

## 应用可视性的价值（续）

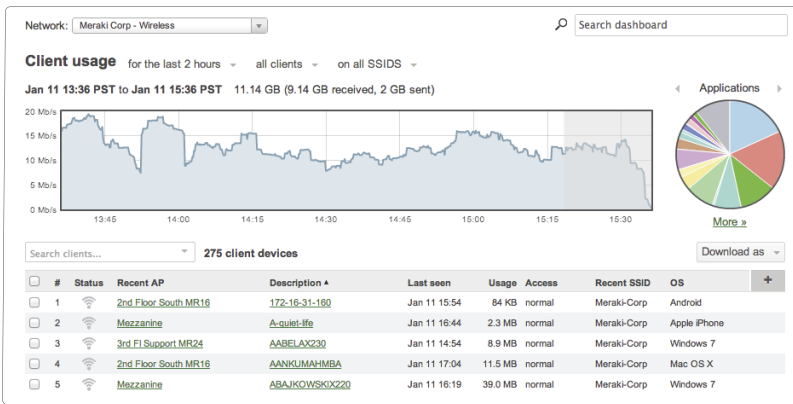
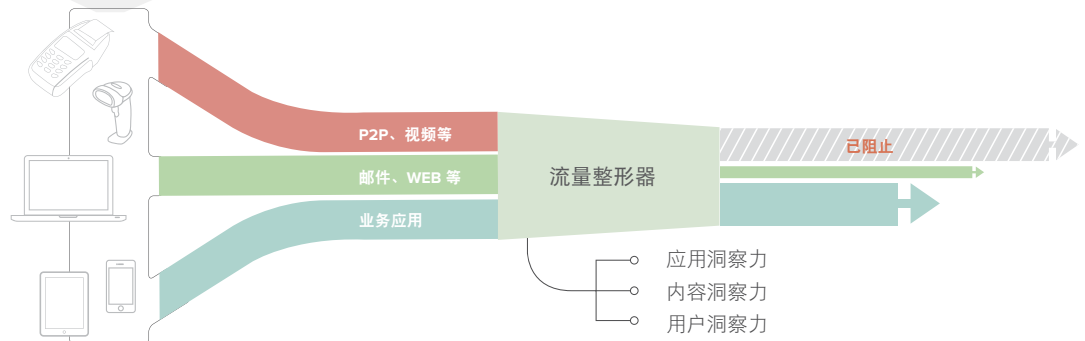


图 1  
流量分析和整形引擎



从端口和协议层直到应用层（例如 Facebook 和 YouTube），Meraki 独有的流量分析引擎可以跨网络栈的所有层提供可视性。此外，Meraki 的最新增强功能（2013 年发布）包括逐数据流对每个用户和每个应用所花的时间等参数进行深入的统计分析；这提供了有关用户行为的宝贵情景信息，而不是对网络中受到访问的所有应用进行无秩序的累积汇总。最后，Meraki 能够创建并按组应用第 7 层应用防火墙和流量规则，这为网络管理员根据提供的分析数据来自定义和优化网络提供了丰富的工具箱。Meraki 的无线 (MR)、交换 (MS) 和安全 (MX) 产品系列均提供第 7 层流量分析功能，Meraki 的 MR 和 MX 产品系列提供流量整形功能。本文将详细介绍这种创新功能。

## 2 Meraki 流量整形技术

### 深度数据包检测和流量签名

为了提供丰富的流量分析功能，Meraki 无线、交换和安全产品逐数据流对网络中的流量执行深度数据包检测 (DPI)。然后，从所有边缘终端将此分析实时上传到基于云端的 SaaS 网络管理平台进行统计汇总。详细信息通过可自定义的网络和时间格式在 Meraki 控制面板中向网络管理员提供。Meraki 的功能包括分析 IP 地址、主机名和端口范围等各种元素，这种分析与每个流量流的行为分析相结合。这有助于更深入地分类流量，不再局限于基于端口或 IP 的分类；其示例包括点对点 (P2P) 文件共享，以及因不断添加服务器而无法只使用 IP 地址来进行跟踪的社交游戏网站。

Meraki 几年来检测的数千种流量模式让其得以创建一个流量签名数据库，可用于识别应用级网络流量。由于 IP 地址和端口范围不断更改，点对点流量历来都非常难以确定，因此识别点对点流量成为特别具有挑战性的任务；Meraki 通过仔细分析 BT 流量流创建启发式签名，识别众多转瞬即逝的 IP 地址之间持续时间短暂的 TCP 会话，从而对 P2P 流量进行分类。类似的启发式技术可在没有任何具体识别信息的情况下运用于各种应用；这些启发式技术比较 Meraki 的流量签名库，并在基于云端的 SaaS 网络管理平台中维护，可以根据发现的新流量模式及其分析结果快速进行更新。此外，网络管理员还能使用主机名、IP 地址范围和端口创建自定义签名，因此可以跟踪发往特定目的地的流量。例如，管理员可以创建签名来跟踪员工访问本地 Web 或邮件服务器等活动。

### 精细分析

新的应用、协议和流量模式不断涌现。虽然提供包罗万象的流量签名可能是极具吸引力的降低复杂性的方法，但是对于“其他 Web”等流量签名，管理员通常需要更深的精细度和更详细的明细，了解哪些 IP 地址或主机名受到访问。

图 2  
显示 Web 流量明细的 Meraki 控制面板屏幕截图

| Destination                        | Protocol | Port | % Usage | Usage    | Sent     | Received | # clients | Active time per client |
|------------------------------------|----------|------|---------|----------|----------|----------|-----------|------------------------|
| mail.google.com                    | TCP      | 443  | 20.6%   | 17.77 GB | 7.70 GB  | 10.08 GB | 222       | 29 hours               |
| na4.salesforce.com                 | TCP      | 443  | 4.6%    | 3.99 GB  | 914.0 MB | 3.10 GB  | 167       | 9 hours                |
| mops.geckoboard.com                | TCP      | 443  | <0.1%   | 18.3 MB  | 9.6 MB   | 8.8 MB   | 1         | 6.9 hours              |
| docs.google.com                    | TCP      | 443  | 1.8%    | 1.58 GB  | 997.4 MB | 616.6 MB | 192       | 6.5 hours              |
| 0.drive.google.com                 | TCP      | 443  | <0.1%   | 22.2 MB  | 18.7 MB  | 3.5 MB   | 6         | 6.5 hours              |
| zcd-01.s3-external-1.amazonaws.com | TCP      | 443  | 1.3%    | 1.11 GB  | 17.2 MB  | 1.09 GB  | 1         | 5.1 hours              |
| www.google.com                     | TCP      | 443  | 1.2%    | 1.05 GB  | 425.8 MB | 648.5 MB | 214       | 3.9 hours              |
| d1t1fzb7fr.app02-17.join.me        | TCP      | 443  | 0.4%    | 385.5 MB | 9.6 MB   | 375.9 MB | 1         | 3.9 hours              |

对提供更深入可视性的需要促进了新分类方案的开发，该方案支持根据主机名和 IP 地址动态创建签名。例如，mail.company.com 的签名可提供对唯一流量流的可视性，而“Dropbox”等类别的精细的主机名和 IP 地址明细可以对访问此应用的特定 IP 地址和主机名进行更深入的检测。这种明细对“非 Web TCP”等范围广泛的大类特别有用，可以提供此类别中受到访问的所有网站的详细明细。这种新的学习引擎支持根据流量模式动态创建流量签名，并可为希望了解用户正在做什么的管理员提供更深入的可视性。

## 以线速执行深度数据包检测

Meraki 产品在充分考虑流量分析等丰富功能的前提下精心选择功能强大的硬件组件，利用这些硬件组件以线速执行流量分析检测和分类，确保在与众多其他可用功能配合使用时不会降低性能。例如，Meraki 的 MX 安全设备可以同时运行流量整形和与网状 VPN 拓扑中数十个其他站点的自动 VPN（全部以线速执行），在此同时还可传输数百 MB 的流量。想要紧密集成硬件与软件以实现性能优化，需要仔细选择和设计芯片组件。

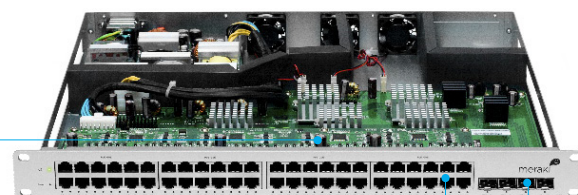


图 3  
高度优化的硬件和软件集成  
可实现线速处理

- 增强的 CPU：第 3-7 层防火墙和流量整形
- 3x3 MIMO，双频 802.11，3 空间流，最高 900 Mbps

## 集成的基于云端的 SaaS 网络管理平台管理

Meraki 的硬件产品和基于云端的 SaaS 网络管理平台通过高度压缩的 1 kbps 管理隧道保持严密的反馈环路，其中包括流量分析和配置信息（例如网络设置）。除了将流量签名从基于云端的 SaaS 网络管理平台推送到边缘并将流量流数据推送回基于云端的 SaaS 网络管理平台外，其他情景信息是逐数据流发送的，包括用户和应用，以及花在每个应用或网站上的每用户平均时间和总用户时间。

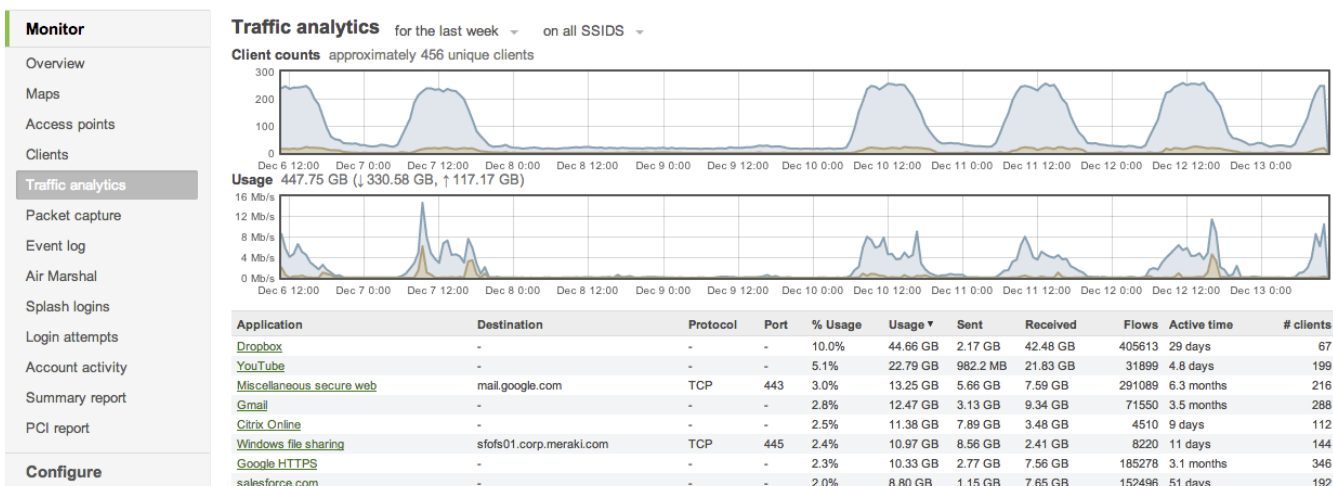


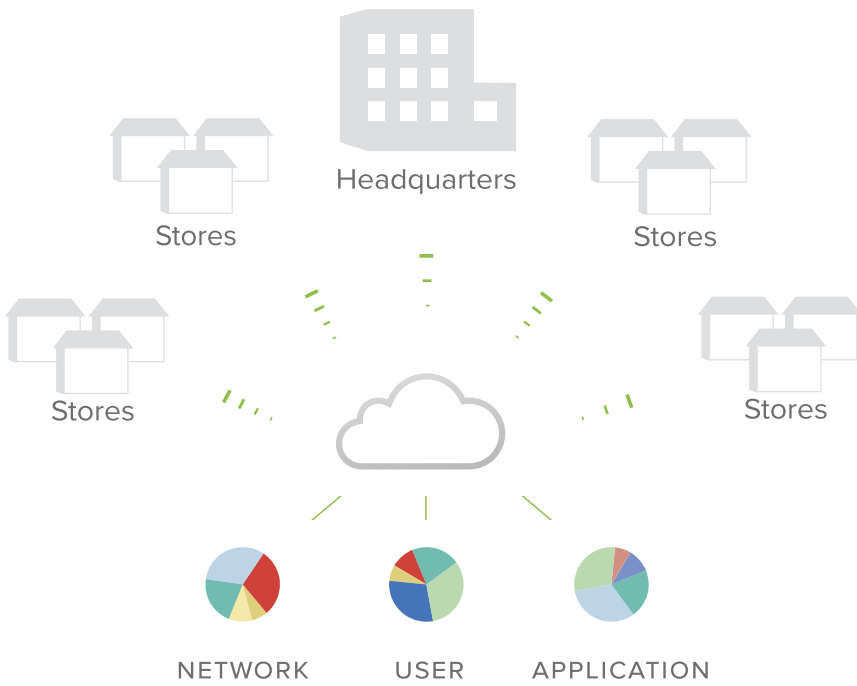
- 48 个 1 GbE 端口，802.3af/802.3at PoE/PoE+
- 增强的 CPU/内存基于云端的 SaaS 网络管理平台管理
- 内置 4 个 10 GbE SFP+ 端口，用于核心连接/堆叠



- 增强的 CPU：第 3-7 层防火墙和流量整形
- 用于内容过滤的额外内存

图 4  
基于云的管理和报告





**图 5**  
基于云端的 SaaS 网络管理平台架构促进大规模流量分析

基于云端的 SaaS 网络管理平台利用分布式数据中心架构的处理功能来汇聚和显示每个网络、每个 SSID 或每个用户在可自定义的一段时间内的流量分析数据。通过数据汇聚功能，可以跨多个地理位置显示流量信息的合并视图。汇总摘要报告提供每天、每周或每月的视图，包括排名靠前的设备、用户和应用的数据。可以将网络配置为包含一个或多个站点以获得所需的报告结构。Meraki 的网络标记引擎允许向多个网络分配特定标记（例如，为一组 100 个星巴克网络分配标记“星巴克”），因此可以对大规模部署中的网络进行层次化分类和报告。

假设一个部署有数千个分散在不同地理位置的终端设备和数万个需要访问的唯一应用，传统数据库需要数小时按每个用户或每个应用提供查询。基于云端的 SaaS 网络管理平台架构采用经过高度优化、专为不受限制的可扩展性而设计的软件栈（类似于 Google 和 Facebook 的架构设计）。它不依赖传统数据库，而是以内部开发的专有数据库促进快速的实时搜索。这种独有的数据库在支撑庞大数据集的同时，还能够在区区几秒钟内而不是几分钟内搜索和轮询数据。

### 借助数据增强用户体验

流量分析和精细的用户级数据还能促进超出网络性能优化范畴的决策。零售业、酒店业乃至企业的营销部门可以使用此数据就如何吸引客户并更有效地与其互动做出决策。Meraki 的外部强制网络门户 (EXCAP) API 可用于打造量身定制的客户自行激活体验，而且可以根据人口统计学或个体级的趋势来塑造和定制这些体验（例如，“我的购物者用 Facebook 用得很多，所以我应该将 Facebook 登录与我的启动服务器相关联”）。有广告预算的营销部门还可以使用此数据分析用户在哪些网站进行交易，并可选择在这些网站上做广告来帮助跟踪他们自己的广告战略并最大限度地发挥其效果。

最后，所有流量分析信息都是完全可选的，而且在 Meraki MR 无线产品系列中，还可以配置一组策略让特定用户或组退出精细的主机名级可视性。这些功能旨在为 IT 管理员设计隐私政策提供更大的灵活性。

# 3 管理和控制

与应用级可视性配合使用的是提供强大管理的 Meraki 流量整形引擎，它可以基于用户和网络组为 QoS 和优先排序创建并应用时间和情景感知策略。Meraki 的流量整形引擎包括限制性策略（例如应用防火墙或应用限制）和建设性策略（允许特定的应用类别忽略带宽限制并使用 PCP 和 DSCP 标记等工具跨网络层设置予以优先处理的优先级）。在 Meraki 的无线产品系列中，可以通过 Meraki 控制面板使用各种变量或通过与 RADIUS 服务器的集成使用 RADIUS 属性，创建并应用这些策略。可以在一个或多个用户或用户组中应用策略，也可以按网络或时间应用策略。

流量和组策略与 Meraki 的流量分析功能配合使用，有助于按每个用户或每个网络对应用和带宽使用进行有效的分类和优先排序。其示例包括在学校环境中创建具有不同带宽限制和视频流量防火墙的两个不同 SSID（例如“教师”和“学生”），在企业环境中的一个“企业”SSID 中分隔普通员工与高管。

### 策略变量

1. 第 7 层防火墙/流量整形
2. 第 3 层防火墙
3. 带宽限制
4. 在第 2 层/第 3 层中使用 PCP/DSCP 标记确定优先顺序

### 应用变量

1. 按个别用户或用户组
2. 按设备类型
3. 按 SSID（可用性可基于时间）

### 应用方法

1. 手动，通过 Meraki 控制面板中的客户端搜索
2. 自动，通过设备指纹识别
3. 通过 802.1x / RADIUS 服务器使用过滤器 ID 或其他 RADIUS 属性

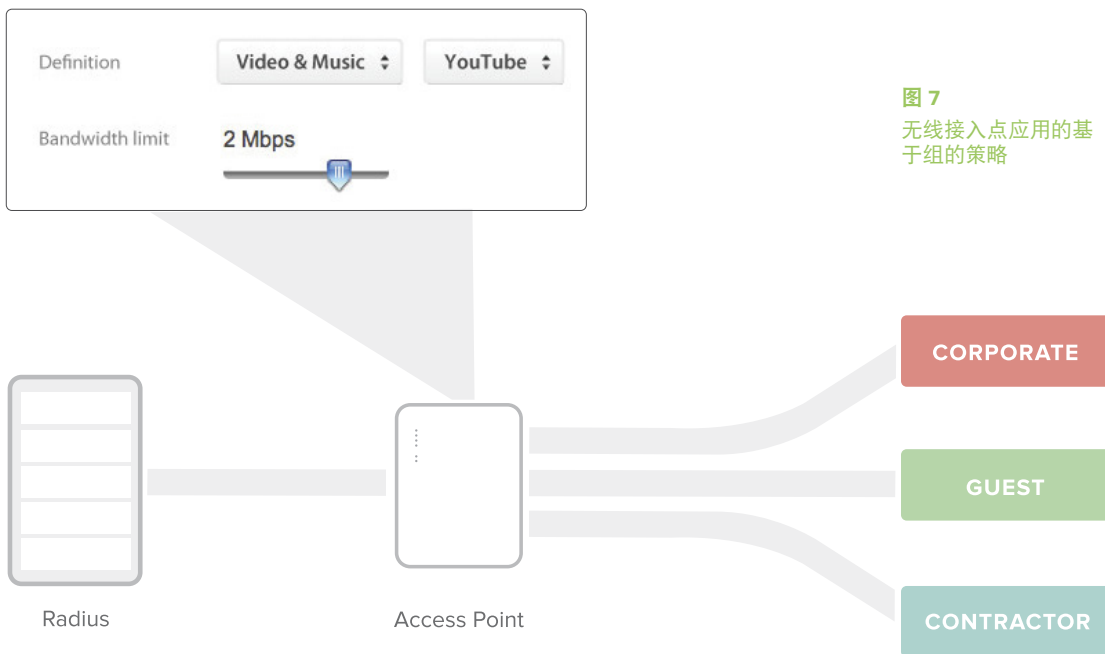


图 7  
无线接入点应用的基于组的策略



## 使用不同的流量规则创建组策略

| Monitor                    | Group policies                    |                           |                      |                 |              |                     |                     |         |
|----------------------------|-----------------------------------|---------------------------|----------------------|-----------------|--------------|---------------------|---------------------|---------|
| Configure                  | Name                              | Affecting                 | Bandwidth            | VLAN            | Splash       | Traffic             | Hostname visibility | Actions |
| SSIDs                      | <a href="#">Contractor</a>        | <a href="#">0 clients</a> | Unlimited            | Do not tag VLAN | SSID default | 3 rules applied     | SSID default        | Clone X |
| Access control             | <a href="#">Accounting_Staff</a>  | <a href="#">1 clients</a> | 5.00 Mb/s up, down   | SSID default    | SSID default | Do not use firewall | SSID default        | Clone X |
| Firewall & traffic shaping | <a href="#">iPad - Guests</a>     | <a href="#">1 clients</a> | Unlimited            | Do not tag VLAN | SSID default | 4 rules applied     | SSID default        | Clone X |
| Users                      | <a href="#">iPad - employees</a>  | <a href="#">1 clients</a> | 500.00 Kb/s up, down | SSID default    | SSID default | SSID default        | SSID default        | Clone X |
| Splash page                | <a href="#">Bandwidth Abusers</a> | <a href="#">0 clients</a> | 250.00 Kb/s up, down | SSID default    | SSID default | 3 rules applied     | SSID default        | Clone X |
| SSID availability          |                                   |                           |                      |                 |              |                     |                     |         |
| Network-wide settings      |                                   |                           |                      |                 |              |                     |                     |         |
| <b>Group policies</b>      |                                   |                           |                      |                 |              |                     |                     |         |
| Radio settings             |                                   |                           |                      |                 |              |                     |                     |         |

## 将策略应用到用户组

Apply policy: Clear Authorization 3rd fl 155 matches in 692 Add c

- Normal
- Whitelisted (no bandwidth limits or splash pages)
- Blocked (no access allowed)
- Group policy**
  - ipad guests
  - Accounting Staff
  - ipad - employees
  - Bandwidth Abusers
  - ipad - Guests
  - Exempt from Traffic Analysis
  - Throttle Video & Music**
  - Block major shopping websites
  - Executives - Prioritize All Traffic
  - Quarantine VLAN with Bandwidth Limits
  - Block BitTorrent & Gaming
  - Contractor
  - block facebook
  - ipad - BYOD

| Usage             | OS                 |
|-------------------|--------------------|
| 38.6 MB           | Apple iPhone       |
| 1 KB              | Mac OS X           |
| 132.0 MB          | Apple iPhone       |
| 144.1 MB          | Mac OS X           |
| 5.56 GB           | Mac OS X           |
| 7.0 MB            | Apple iPhone       |
| 1.80 GB           | Mac OS X           |
| 37.1 MB           | Mac OS X           |
| 1.02 GB           | Apple iPhone       |
| Bandwidth Abusers | 11.5 MB Apple iPad |
| 18.6 MB           | Apple iPhone       |
| 40.3 MB           | Apple iPhone       |
| 873.5 MB          | Mac OS X           |
| 4.2 MB            | Apple iOS          |

图 6  
在 Meraki 控制面板中  
创建并应用组策略

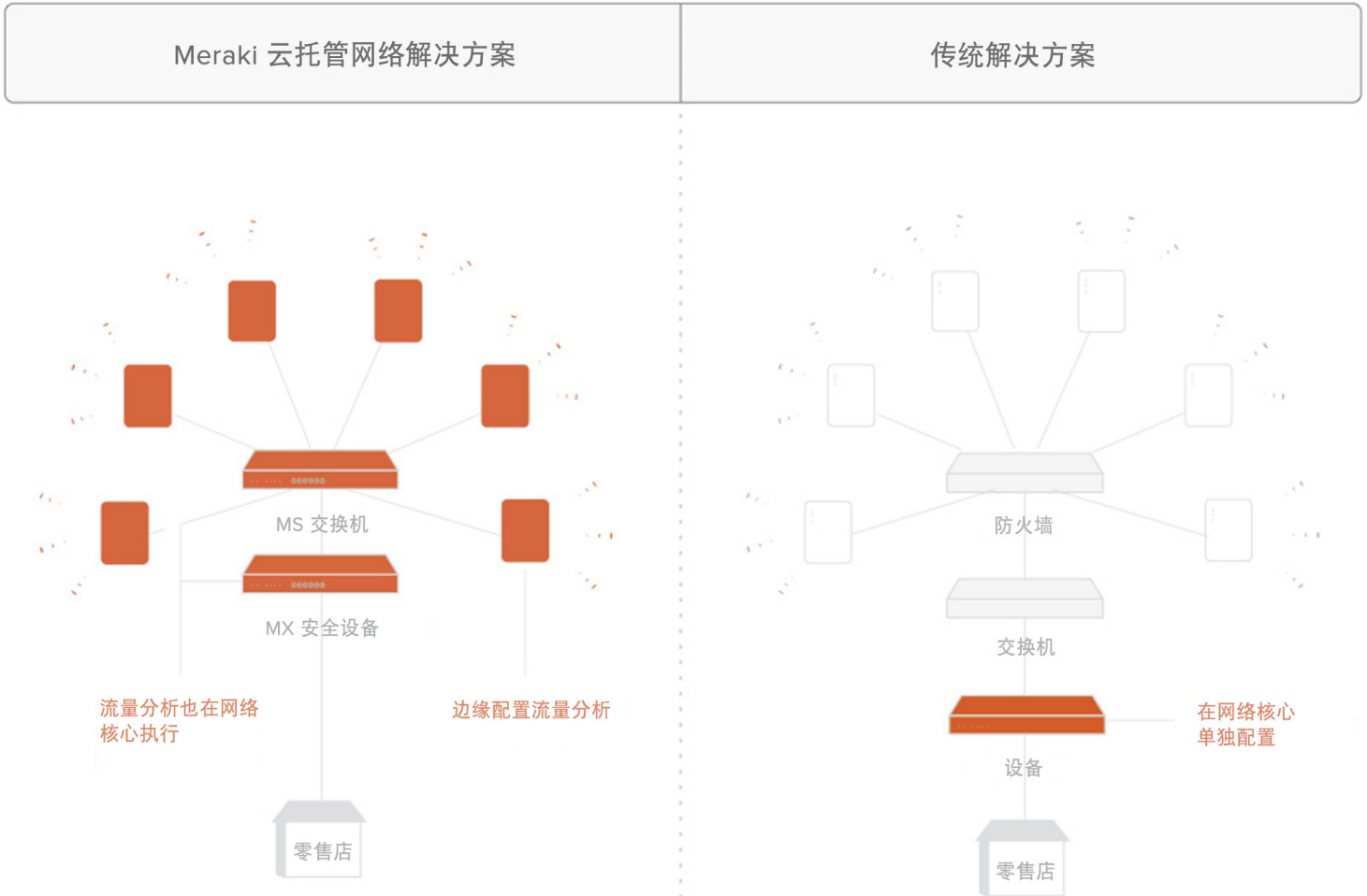
## 按设备类型应用策略

| Device type            | Actions |
|------------------------|---------|
| Android                | X       |
| BlackBerry             | X       |
| iPad                   | X       |
| iPhone                 | X       |
| Mac OS X               | X       |
| Windows                | X       |
| Other OS               | X       |
| Add group policy for   |         |
| Block all access until |         |

- built in policies
- whitelist
- blocked
- ipad guests
- Accounting Staff
- ipad - employees
- Bandwidth Abusers
- ipad - Guests
- Exempt from Traffic Analysis
- Throttle Video & Music
- Block major shopping websites
- Executives - Prioritize All Traffic
- Quarantine VLAN with Bandwidth Limits
- Block BitTorrent & Gaming**
- Contractor
- block facebook
- ipad - BYOD

## 4 与传统解决方案的比较

应用级可视性并不是一个新概念；有几家公司曾构建提供第 7 层可视性的解决方案，帮助管理员洞察网络性能。同样，也有一些工具可以提供创建并应用应用级防火墙和整形规则的功能。但是，Meraki 的方法在多个方面首开业界先河，包括跨有线和无线产品系列在边缘提供可扩展的处理能力，以及利用云数据库进行大数据处理和索引以便以可自定义的格式提供统计信息。这些优势使 Meraki 成为理想的流量可视性和策略管理解决方案。



Meraki 的应用层分析可以跨思科有线或无线产品系列在边缘执行，而传统解决方案需要在网络核心内的某个位置部署整合的专用设备。这种需要在中心位置部署设备的要求可能存在许多缺点，其中包括：(a) 需要专门搭建网络，以使所有流量流经此设备；(b) 构成单点故障；(c) 由于一台设备的 CPU 有限，造成可扩展性也有限。单独的设备还伴随着高成本，且通常基于终端授予许可，如果存在大量边缘设备（例如 1000 个无线接入点），则可能导致成本急剧上涨。而 Meraki 的流量分析功能包含在企业云许可证的成本中（最新的分析升级同样如此）。

其次，Meraki 能够利用其基于云端的 SaaS 网络管理平台的力量，根据可调整的变量快速汇聚、分析和自定义显示统计信息。其示例包括能够跨多个地理位置在单一视图中查看汇总统计信息，以及每个网络、每个用户和每个应用的明细，并能对查看的数据进行排序和自定义。利用 Meraki 快速增长的自定义数据库和地域分布广泛的数据中心，可以进行“大数据”处理，从而支持大规模合成和显示网络统计信息，而这在单一设备或企业托管架构中根本不可能实现。

最后，Meraki 的 MR 和 MX 无线和安全设备产品系列配备创建和应用自定义应用签名和流量整形策略的功能，支持根据感知的网络趋势优化网络。利用 Meraki 强大的设备指纹识别和实时客户端搜索功能，可以快速过滤策略并应用到自定义用户组。创建并应用策略之后，能否衡量策略在应用和网络使用方面的影响也非常重要。通过 Meraki 控制面板衡量策略更改的影响也非常直观，这种可视性便于快速调整策略，从而帮助管理员以传统企业设备不可能实现的方式跟踪和优化网络性能。

## 结论

超越简单的网络管理提供更高可视性能够让管理员了解其基础设施上的用户行为和网络使用情况。Meraki 的策略管理工具方便管理员创建应用感知防火墙和流量整形规则，用于优化网络性能并为最终用户提供高品质的体验。使用 Meraki，管理员现在可以指望在边缘接入层对应用层获得丰富的了解，从而全面了解用户行为。然后，他们可以利用灵活的策略工具包来创建特定应用策略并将其应用到每个用户。无论是传统 IT 员工还是营销部门，都可以使用 Meraki 的 MX、MS 和 MR 产品系列获得优化网络性能所需的可视性，并最终构建一个可扩展的应用感知型架构，在新的自带设备和云应用时代长存。