



Cisco 思科演示云dCloud系列培训

如何使用dCloud来做Meraki SD-WAN的演示

dCloud – 思科的演示云



**思科演示云将其产品解决方案架构的
软件和硬件虚拟化，让思科与合作伙
伴的销售团队在任何地方，任何时间
都可以做产品演示。**

什么是Cisco dCloud?

服务

思科, 合作伙伴, 客户

自服务, Managed Service

Instant(实时), Scheduled(预约), 企划书

Demo, Lab, 沙盘, POV, Events

可定制化, 保持, 共享

创建content

平台

5 个数据中心

云, 基础架构, 自动化, 用户 UI

管理员Admin, 开发工具

Cisco on Cisco

内容

超过250 offerings, 所有的架构

预配置有文档提供

虚拟机, 硬件, 用户设备, licensing

认证, 可信

可选的终端

Operations 和技术支持

24x5* chat, email, web, phone

Self help, event support, metrics

Cisco dCloud – 使用小技巧



- **请随时给我们反馈**
- **共享给你的客户**
- 定制化保存
- 和技术支持联系来Extend sessions
- 超过5个sessions可使用Event scheduling
- 多种 RDP连接的方式
- 将本地应用和云服务加入demo
- 使用多个数据中心来 capacity/redundancy

dCloud 满足你的要求

<http://dcloud.cisco.com>

As Easy As...



- 思科员工和合作伙伴
- 完整脚本
- 定制化, 本地化, 共享
- 可选的终端 (BYOD)
- 可使用你自己的设备



dCloud
Data Centers

US East
US West
EMEAR
APJ
GC

As Complete As...



- Virtual desktops
- Local clients on laptops
- Room based configuration
- 可添加你本地的服务器
- 多种使用案例

Meraki SD-WAN的演示

- **现在就让我们的企业网的专家 Tom一起开始吧：**
 - 转去dcloud.cisco.com
 - 使用CCO帐户SSO登陆
 - 选择大中华区GC数据中心
 - 马上就跟随**Tom**开始学习吧，你可以随时提问题



MERAKI SOFTWARE-DEFINED WAN

Simple, Secure, Optimized Connectivity



2018 Dec

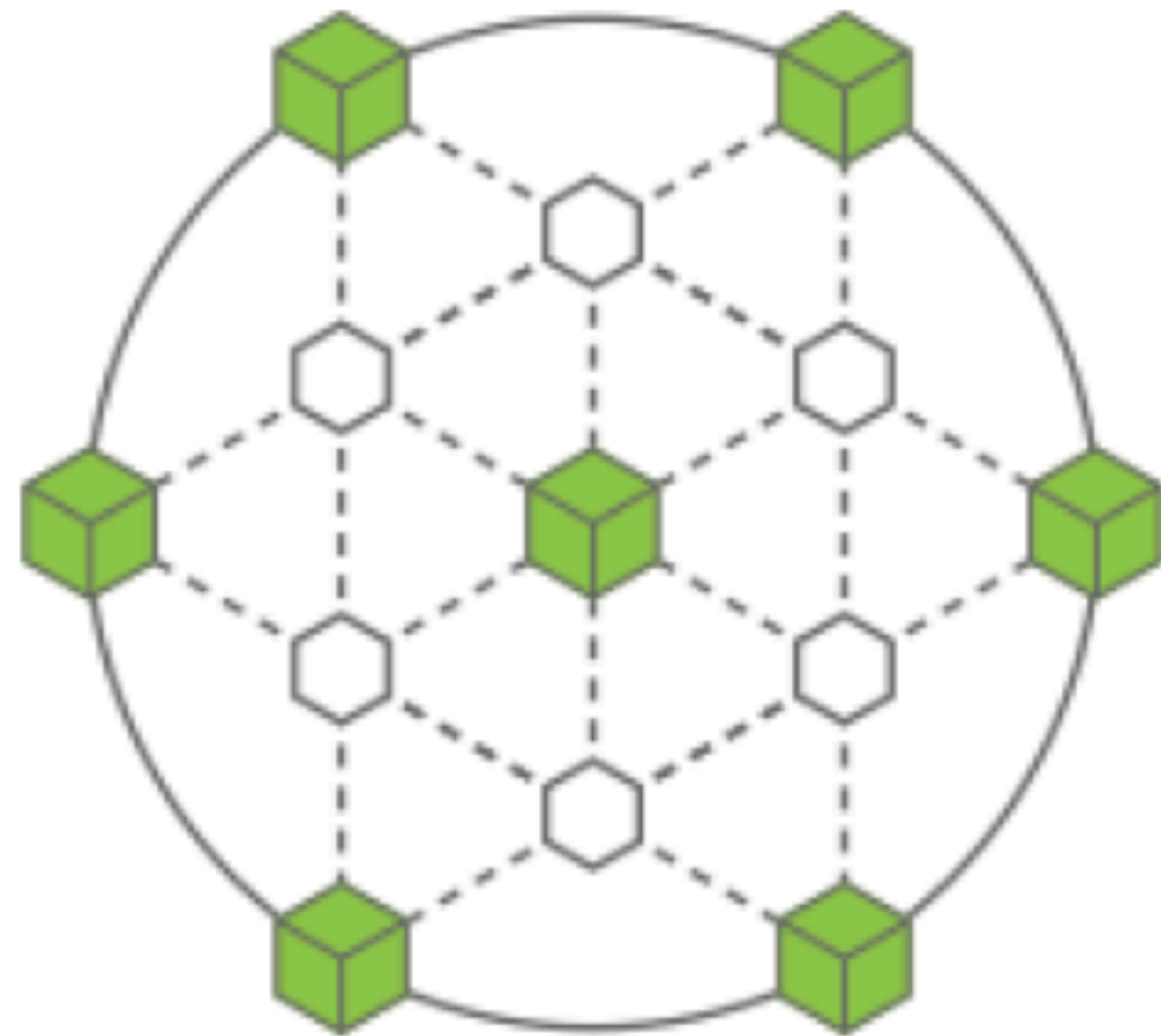
透过简化强大的技术

能让人才专注于他们真正的使命

Simplifying powerful technology to free
passionate people to focus on their mission

TECHNOLOGY THAT SIMPLY WORKS

关于 Meraki



完整的SaaS IT管理解决方案

无线、交换、安全、SD-WAN、智能网络洞察、终端设备管理、和安全监控摄像头

整合硬件、软件、和基于云技术的SaaS服务

SaaS IT管理领导品牌

思科成长最快的产品线之一

35万+

全球客户

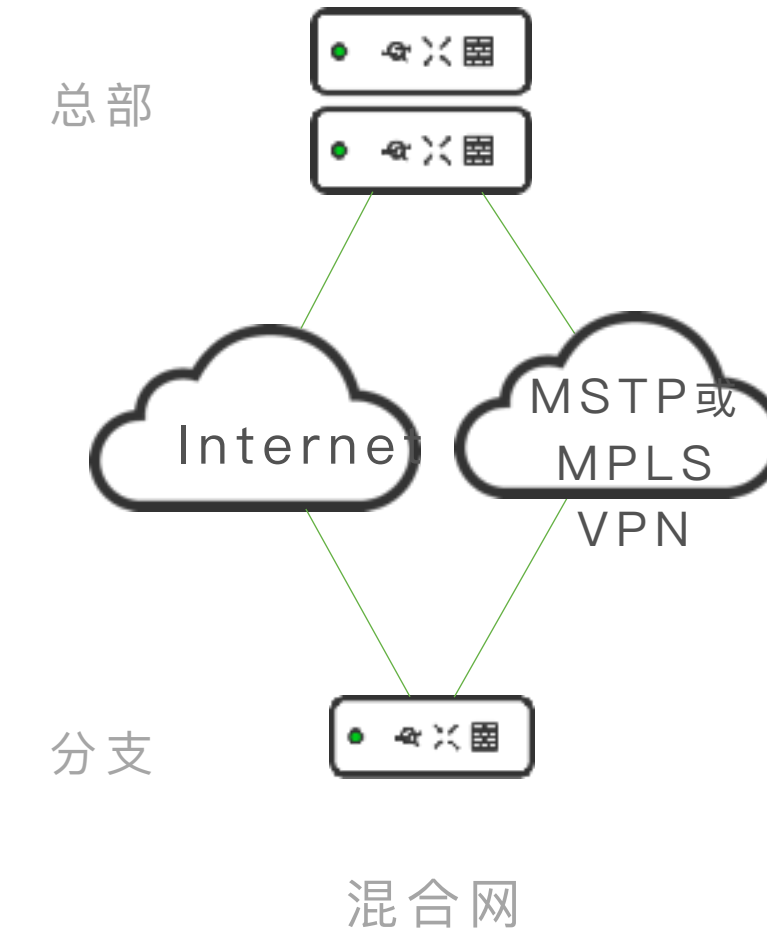
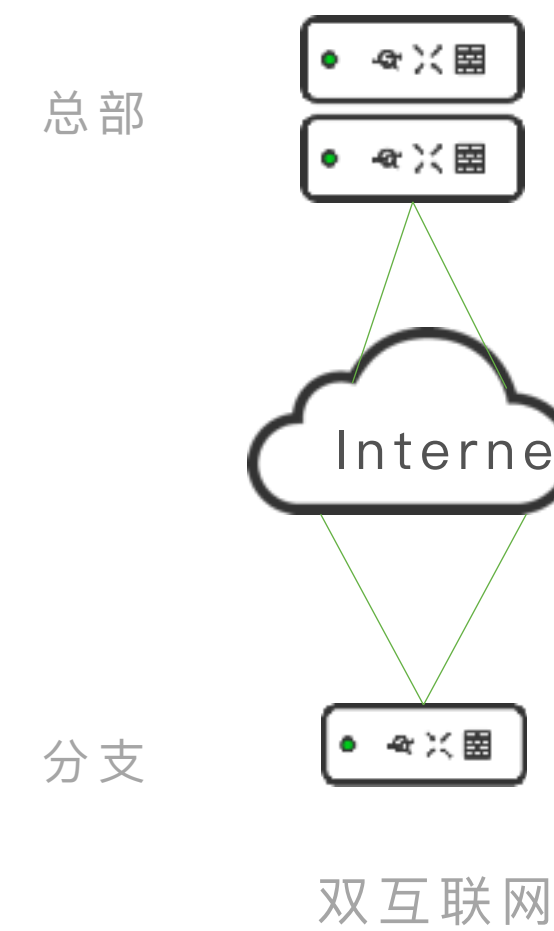
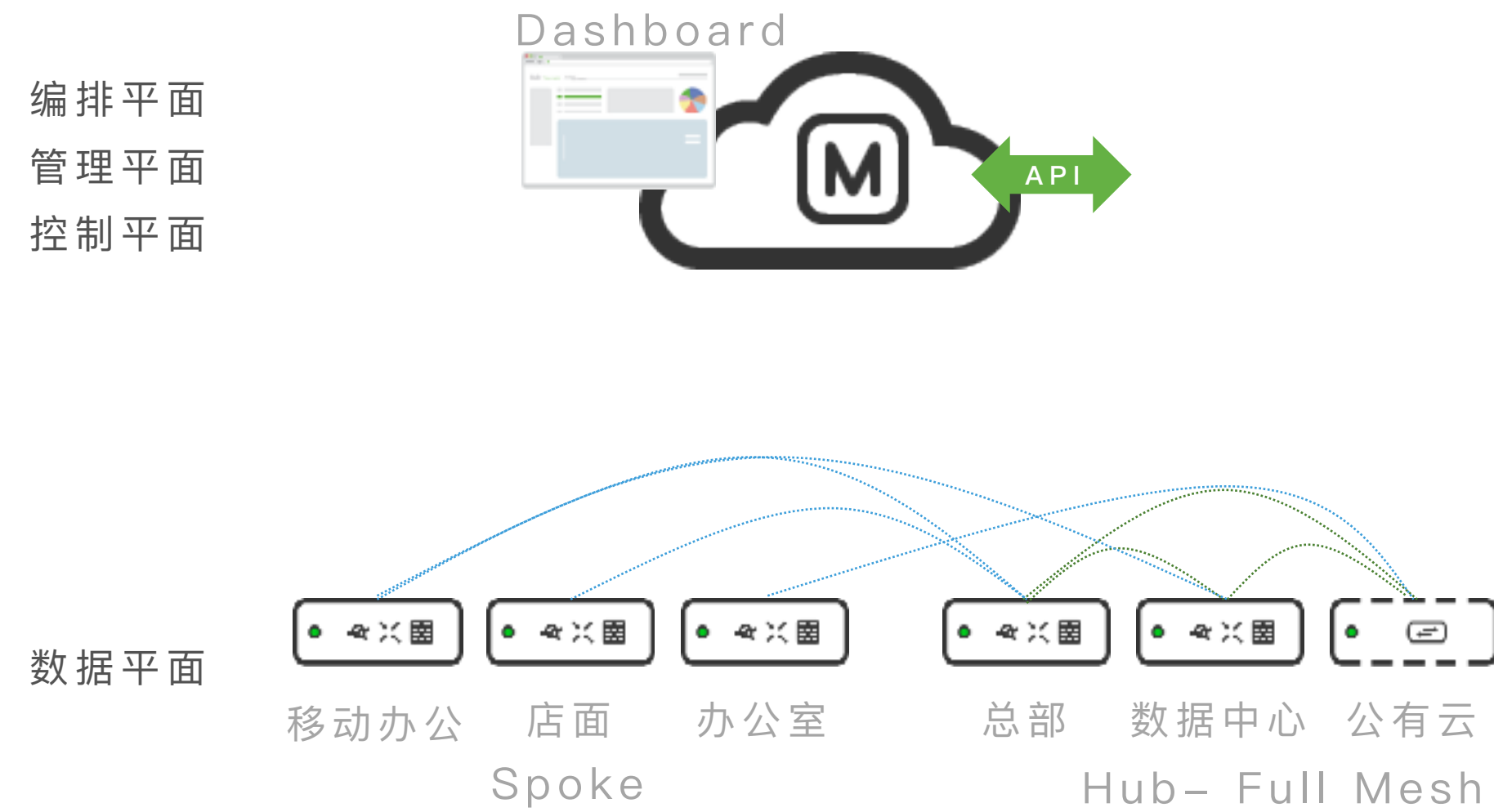
65万+

MX 路由器在线

14,900+

SD-WAN 客户

Meraki SD-WAN



Overlay

Auto VPN

应用于
互联网与混合网

Path Control

路径控制

负载均衡
基于应用的PBR
动态路径选择

应用于
互联网流量和VPN流量

Visibility and Traffic Control

可视化与流控

应用和线路可视化
基于每个用户每个应用的流控

Security

安全

L3 & L7 Firewall

Snort IPS/IDS
Content-Filter
Geo-IP Based
Firewall

Auto VPN

Auto VPN 的特色



Meraki Auto VPN

仅需Cisco Meraki Dashboard上的两次点击，即可在任何广域网连线，配置 site-to-site 三层 IPsec VPN。

自动配置VPN参数

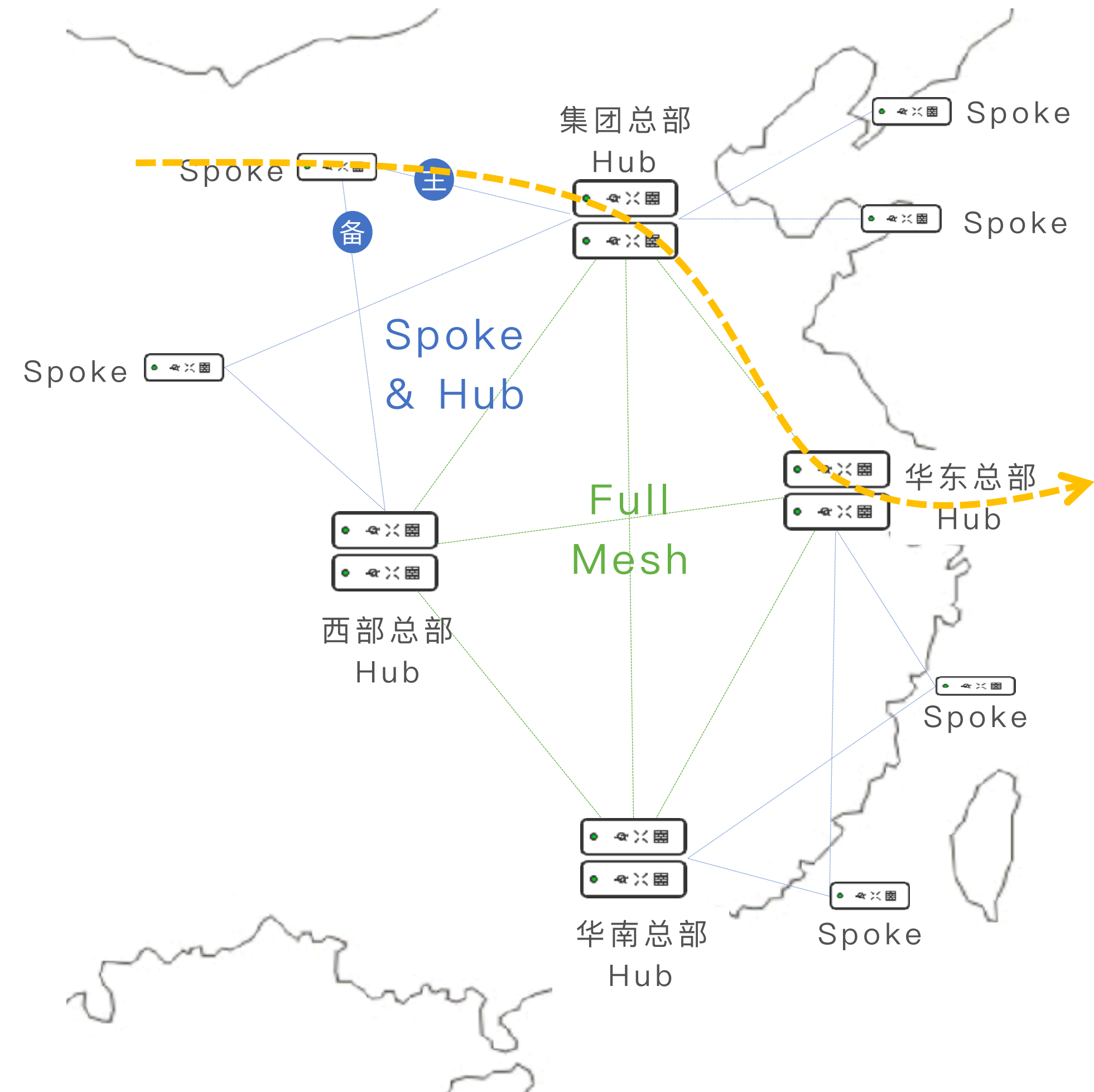
Cisco Meraki dashboard 能够在一个组织里的MX路由器之间，自动协商VPN路由、认证方式、加密协议、加密密钥，以创建hub-and-spoke和mesh VPN 拓扑。

内建冗余机制

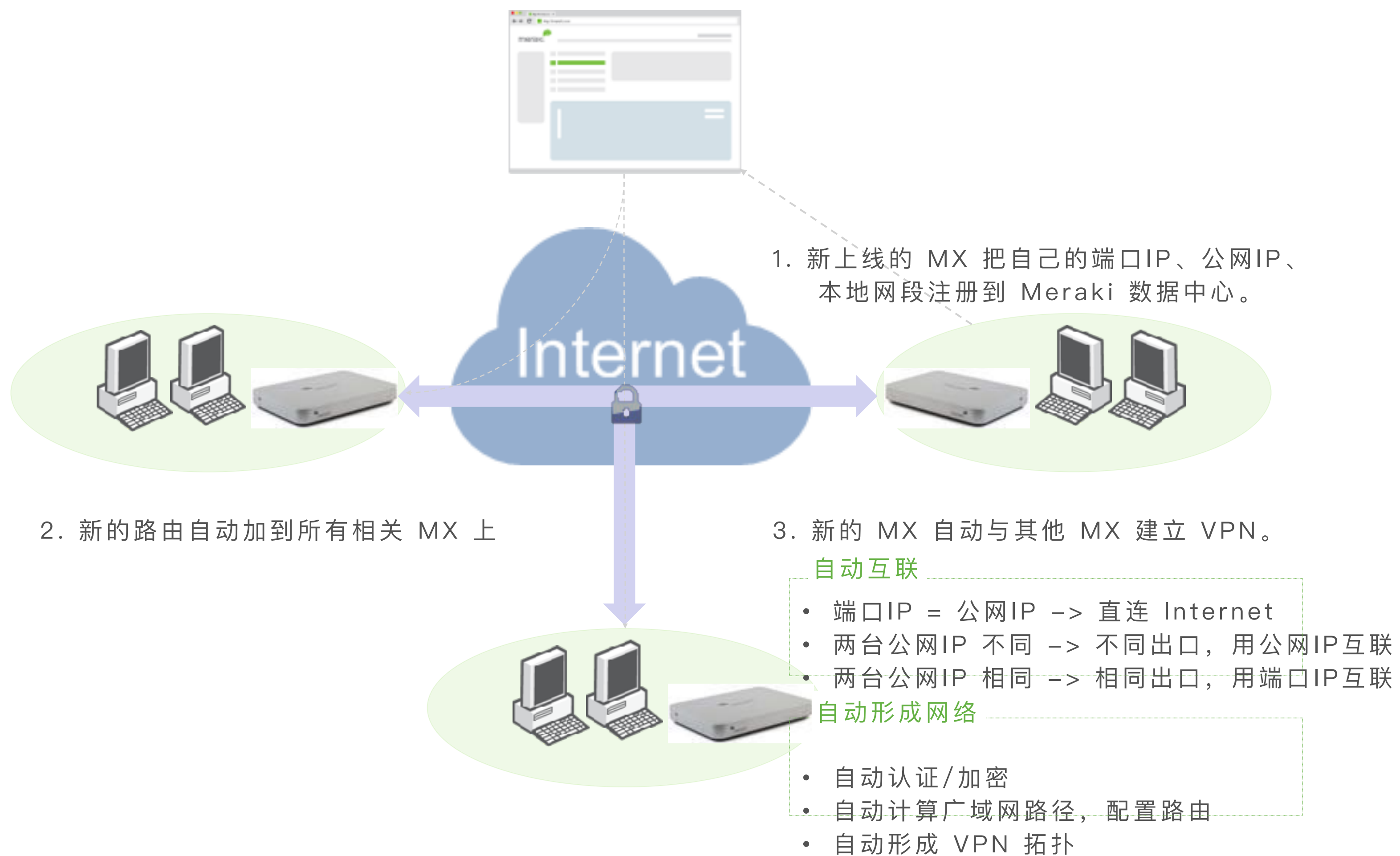
MX路由器拥有两个上行端口，在主要连线中断时，能够自动重新协商VPN通道，以自行修复连线。

Auto VPN 的架构

- Auto VPN 拓扑
 - Hub 站点自动形成 Full Mesh 拓扑
 - Spoke 站点需选择Hub，形成 Spoke-and-Hub 拓扑
(不需配置对端IP、ACL、密码、Tunnel IP、路由、IP SLA...)
- Auto VPN 路由
 - 每个站点只需勾选要使用VPN的网段，全网即可自动通告路由，无需配置VPN内的路由协议。
 - Spoke可以连接到多个Hub，并排列Hub的优先顺序
- Auto VPN 其他功能
 - NAT 穿越
 - 支持与第三方设备建立IPSec VPN（但不支持SDWAN功能）



Auto VPN 编排



VPN注册表

Subnet	Uplink IP	Public IP
10.0.1.0/24	10.1.1.1	184.23.135.1
10.0.2.0/24	10.1.1.2	184.23.135.2
10.0.3.0/24	10.1.1.3	184.23.135.3

Auto VPN 的配置

1. 选择 Hub 或 Spoke

站点间 VPN

类型 ⓘ

- 关闭
请勿加入站点间 VPN。
- 集线器（网状）
使用所有集线器和相关的分支建立 VPN 隧道。
- 分支
使用所选的集线器建立 VPN 隧道。

集线器 ⓘ

#	名称	Default route	行动
1	DATACENTER-NA-VPN_Concentrator	<input type="checkbox"/>	⇅ X
2	BRANCH-LON - appliance	<input type="checkbox"/>	⇅ X

2. 选择需要与VPN互通的本地网络

VPN 设置

本地网络

名称	子网	使用 VPN
Infrastructure	172.16.1.0/24	yes
Associates	172.16.50.0/24	no
Corp-Data	172.16.10.0/24	yes
Voice	172.16.20.0/24	yes
Wireless Infrastructure	172.16.5.0/24	yes

选择 yes 的网段就可以与其他站点互通

按住十字键可以调整优先顺序

Path Control

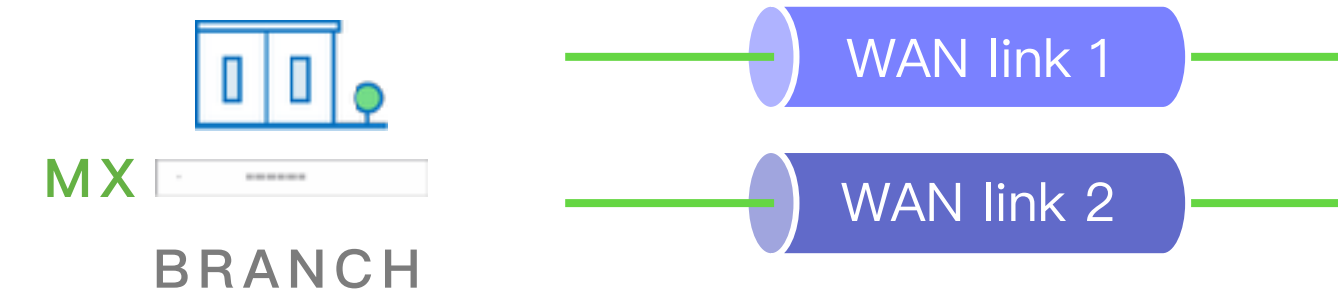
路径控制



路径控制

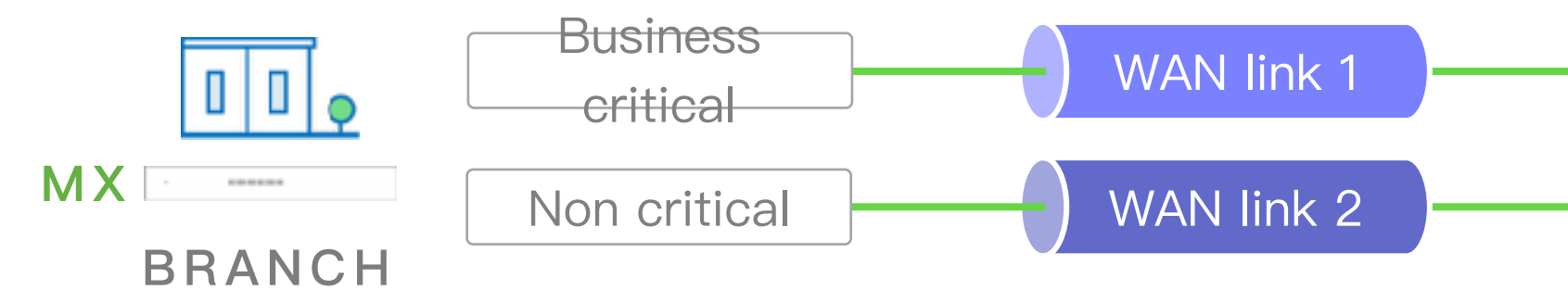
Dual active VPN

在两条上行线路上，对VPN流量进行负载均衡



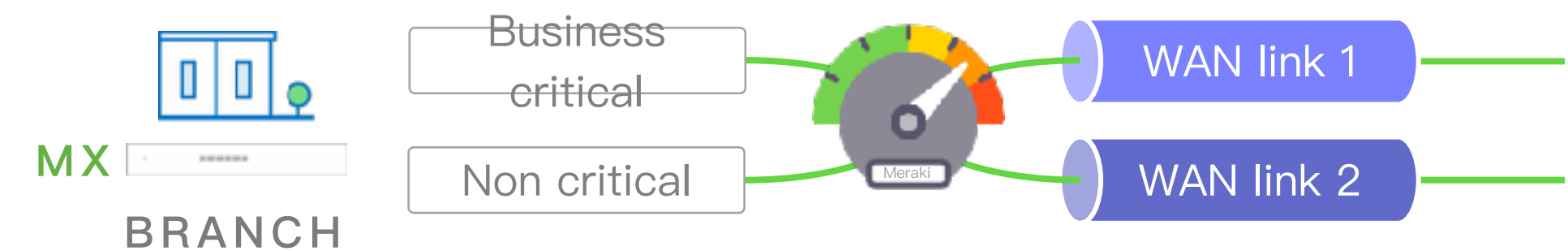
Policy-based Routing (PbR)

基于协议、端口、来源与目的地址、或应用类型，选择流量的首选路径



Dynamic path selection

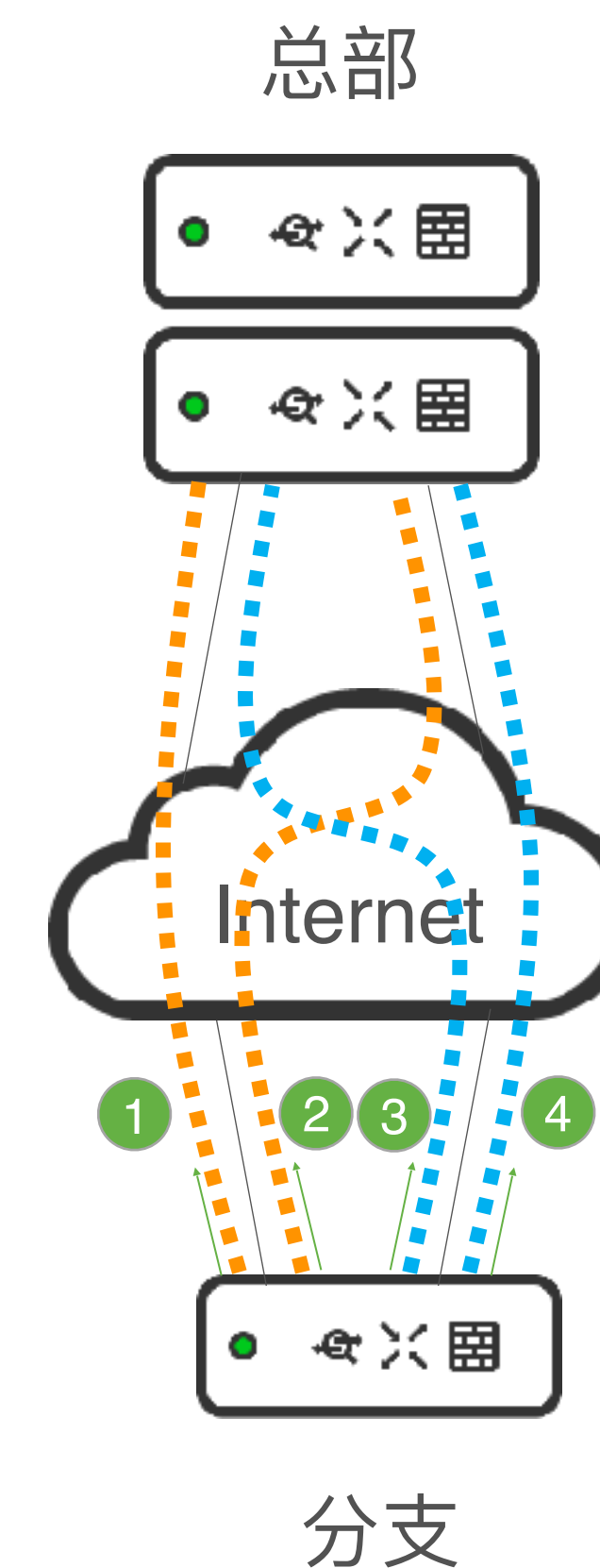
基于实时性能，自动使用最优VPN通道来传送流量



Auto VPN tunnels

广域网性能探针

- 每个上行端口，向所有路径发送探测包
 - 如右图，MX #2 发送 4 个探测包
 - 收到探测包的 MX #1 也会回复 4 个探测包
- 探测包：100 byte UDP (基于protobuf) 没有 DSCP 标示
- 缺省探测包发送间隔：1 或 10 秒
- 使用最后 6 个样本计算：平均时延、掉包、抖动
- 所有路径都会分别计算这些性能统计信息 (每台MX最多4条路径)



路径控制的配置 — Internet 流量

上行链路选择

全局首选项

主上行链路

负载均衡

WAN 1

启用

流量将按照以上指定的比例遍布在两个上行链路中。
到 Meraki 云的管理流量将使用主上行链路。

已禁用

所有互联网流量将使用主上行链路，除非主上行链路被上行链路首选项覆盖或出现故障。

只需一次点击，即可启用负载均衡！

流首选项

Internet 流量

协议	信息来源	源端口	目的地	目标端口	首选上行链路	行动
TCP	Any	Any	1.2.3.4	Any	WAN 1	⇄ X
UDP	10.1.1.0	Any	Any	Any	WAN 2	⇄ X

[添加首选项](#)



依据来源IP端口、目的IP端口，指定Internet流量出口

路径控制的配置 — VPN 流量

1. 定义性能

名称	最大延迟时间 (毫秒)	最大抖动时间 (毫秒)	最大丢失率 (%)	行动
My Probe 1	150	30	3	X

[创建新的自定义性能类别...](#)

2. 选择应用

流量过滤器

所有业务管理 x 魔兽世界 x 第3层 tcp from Any to cisco.com x 添加 +

3. 配置策略

流量过滤器

所有业务管理 x 魔兽世界 x 第3层 tcp from Any to cisco.com x 添加 +

策略

首选上行链路: WAN 2

在以下情况下进行故障转移:

性能不佳
上行链路关闭

性能等级: My Probe 1

三种路径控制

1. 负载均衡
2. 策略路由PBR: WAN1/WAN2 + 上行链路关闭
3. 动态路径选择: WAN1/WAN2 + 性能不佳 / VoIP

路径控制 — 路径决策:单臂架构

• 单臂架构路径决策

1. MX-DC向MX-Spoke发出第一个包

本地端口决策：无（因为只有一个物理端口）

对端端口决策：第一个包随机选择（round robin）— WAN2

2. MX-Spoke基于策略路由/动态路由选择，决定走WAN1

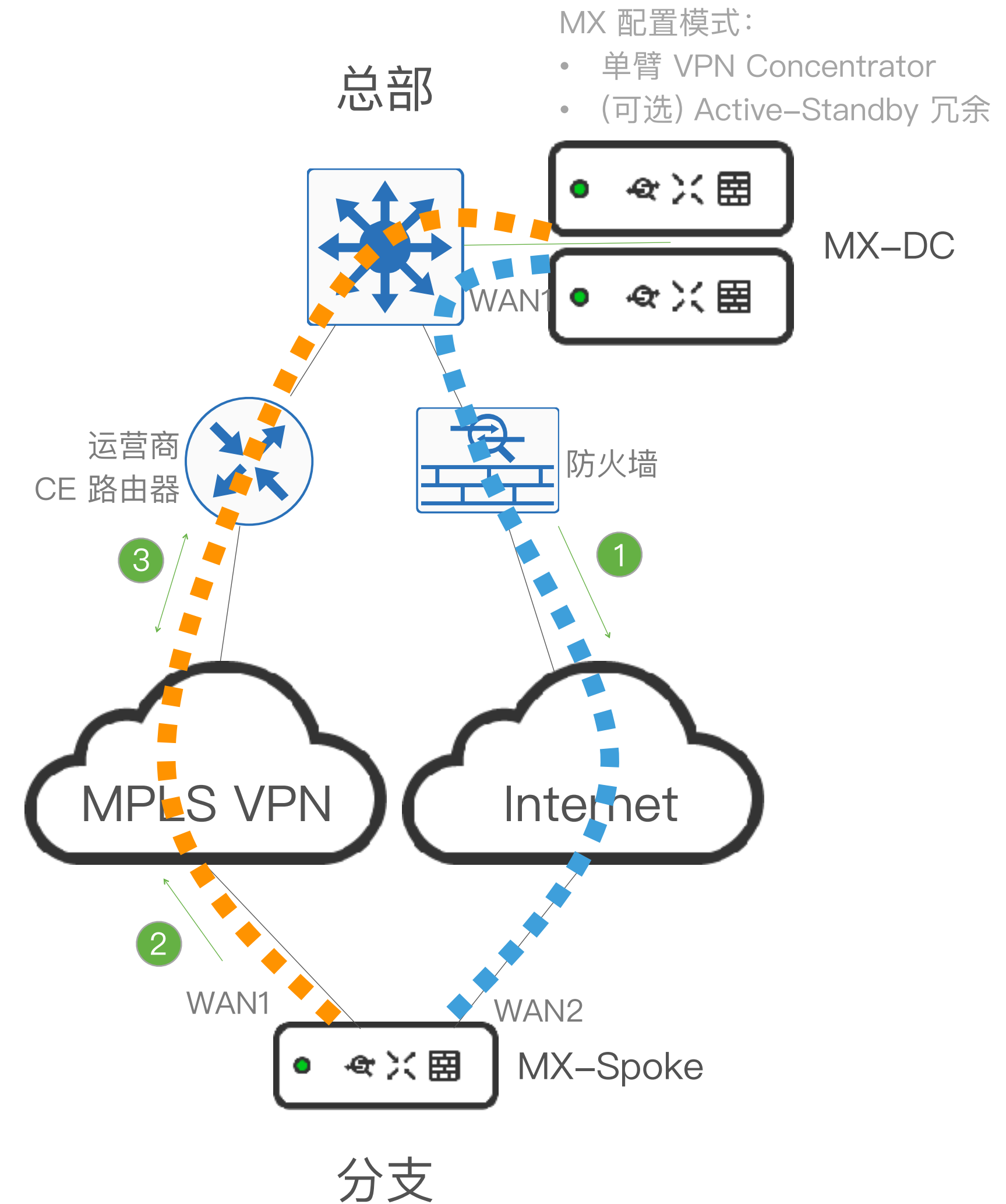
本地端口决策：基于策略路由/动态路由选择 — WAN1

对端端口决策：无（因为只有一个物理端口）

3. MX-DC学习到MX-Spoke的决定，使用MX-Spoked的WAN1

本地端口决策：无（因为只有一个物理端口）

对端端口决策：MX-DC学习到的对端端口 — WAN1



路径控制 — 路径决策:双网架构

• 双网架构路径决策

1. MX-Spoke向MX-DC发出第一个包

本地端口决策：基于MX-Spoke策略路由/动态路由选择-WAN1

对端端口决策：第一个包随机选择 (round robin) — WAN2

2. MX-DC基于策略路由/动态路由选择，决定走WAN1

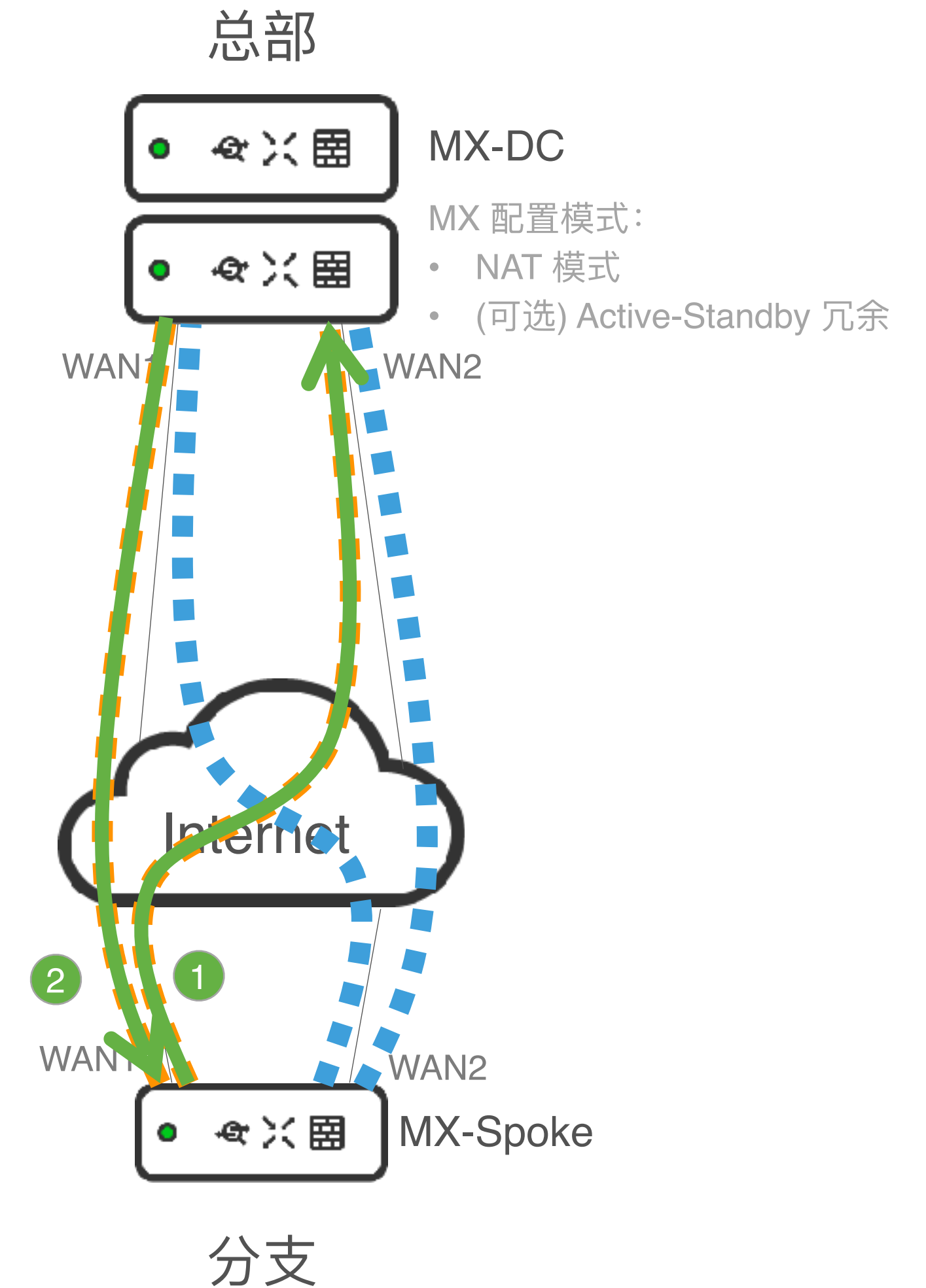
本地端口决策：基于MX-DC策略路由/动态路由选择-WAN1

对端端口决策：MX-DC学习到包是从MX-Spoke WAN1来的 — WAN1

3. MX-Spoke学习到MX-DC的决定，发向MX-DC的WAN1

本地端口决策：基于MX-Spoke策略路由/动态路由选择 — WAN1

对端端口决策：MX-Spoke学习到包是从MX-DC WAN1来的 — WAN1



Visibility and Traffic Control

可视化与流控



可视化 — 线路状态总表

需要 MI License
中国控制面板尚未开放

站点间VPN品质

SD-WAN路由器 > VPN状态 > 点击条状图

WAN Health **DCTA** 过去 2 小时

上行链路状态	网络名称	上行链路类型	ISP	可用性	总用量	用量	损耗	Average Latency	Jitter	受影响的应用	Signal (dBm)
● 良好	Meraki London - Finsbury - appliance	primary	Unknown	● 8	↑ 1.70 GB, ↓ 1.39 GB	↑ 242.05 kB/sec, ↓ 197.44 kB/sec	0.00%	294.75 ms	1.50 ms	-	-
● 就绪	Meraki London - Finsbury - appliance	secondary	Unknown	● 1	↑ 552.86 MB, ↓ 1.01 GB	↑ 78.75 kB/sec, ↓ 143.32 kB/sec	0.02%	322.17 ms	0.42 ms	-	-
● 就绪	Meraki Sydney - appliance	secondary	Unknown	● 0	↑ 1.52 GB, ↓ 7.41 GB	↑ 214.21 kB/sec, ↓ 1.04 MB/sec	0.00%	1.53 ms	0.60 ms	-	-
● 就绪	Meraki Sydney - appliance	primary	antclockwise.net.au	● 0	↑ 13.10 GB, ↓ 47.58 GB	↑ 1.04 MB/sec, ↓ 6.69 MB/sec	0.00%	0.49 ms	0.45 ms	-	-
● 就绪	Meraki San Francisco - Security	secondary	monkeybrains.net	● 0	↑ 142.40 MB, ↓ 1.39 GB	↑ 19.94 kB/sec, ↓ 194.61 kB/sec	0.00%	147.77 ms	0.88 ms	-	-
● 就绪	Meraki San Francisco - Security	primary	sonic.net	● 0	↑ 65.15 GB, ↓ 27.57 GB	↑ 9.26 MB/sec, ↓ 3.86 MB/sec	0.01%	160.13 ms	1.32 ms	-	-
● 就绪	Meraki London - Bishopsgate - appliance	primary	Unknown	● 0	↑ 596.26 MB, ↓ 1.29 GB	↑ 84.94 kB/sec, ↓ 183.66 kB/sec	61.08%	0.84 ms	6.75 ms	-	-
● 就绪	Meraki London - Bishopsgate - appliance	secondary	oncolt.com	● 0	↑ 19.12 MB, ↓ 476.54 MB	↑ 2.72 kB/sec, ↓ 67.68 kB/sec	100.00%	0.00 ms	0.00 ms	-	-

选择列

选中可添加客户端，拖动列可重新排序。

- 总用量
- Signal (dBm)
- 用量
- 损耗
- Average Latency
- Jitter
- Available Goodput
- 受影响的应用
- 可用性

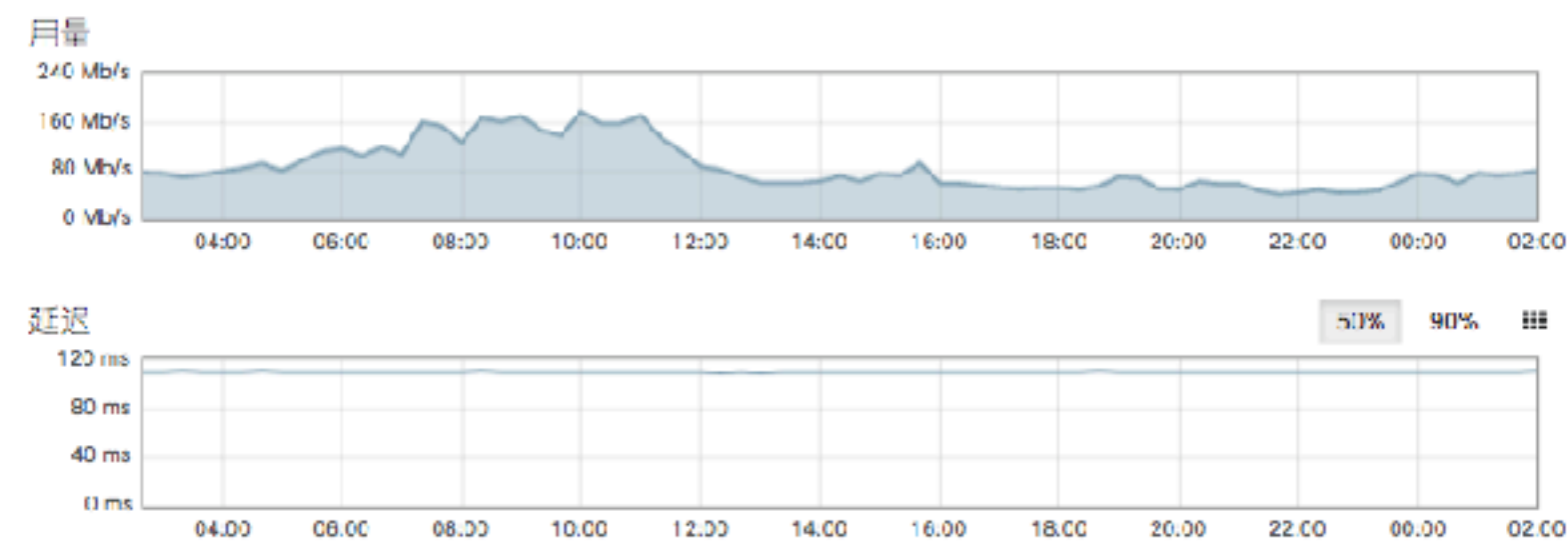
- Basic Information**
- 上行链路状态
- Basic information**
- 网络名称
- 上行链路类型
- ISP
- Network Tags

可视化 — 线路带宽利用率

站点间VPN带宽利用率

组织 > VPN状态

VPN 状态 过去一天

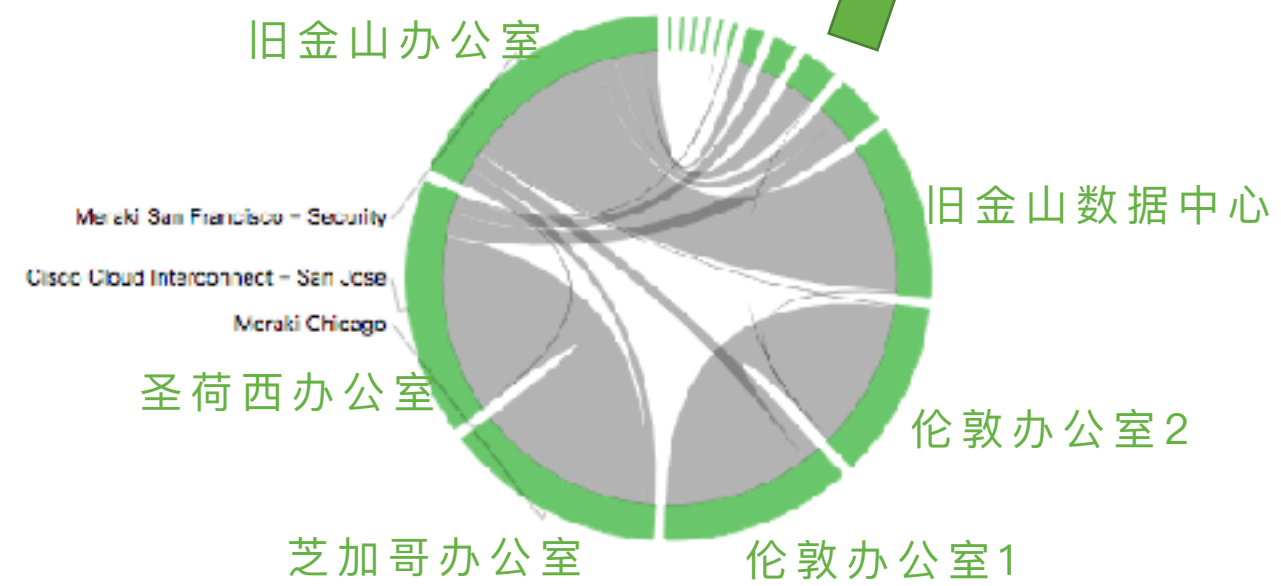


网络 搜索

下载

状态	说明	用量*	延迟 (50%)	延迟 (90%)	对等点	子网	连接
●	Meraki San Francisco - Security	177.15 G3	98 ms	140 ms	15	111	██████████
●	Cisco Cloud Interconnect - San Jose	150.66 G3	112 ms	160 ms	9	16	██████████
●	Meraki Chicago	135.42 G3	72 ms	94 ms	3	3	██████████
●	Meraki London - Bishopsgate	113.72 G3	7 ms	135 ms	3	6	██████████
●	Meraki London - Finsbury	110.48 G3	123 ms	192 ms	12	89	██████████
●	Meraki San Francisco - Data Center	103.75 G3	124 ms	144 ms	2	5	██████████
●	Meraki Sydney	30.80 G3	175 ms	320 ms	3	4	██████████
●	Meraki AWS - US West Oregon	21.62 G3	50 ms	147 ms	2	0	██████████
●	Meraki Tokyo	12.89 G3	137 ms	185 ms	3	3	██████████
●	Meraki Sydney - Data Center	9.44 G3	125 ms	145 ms	1	4	██████████
●	Meraki San Jose	1.32 G3	9 ms	139 ms	3	2	██████████
●	Teleworker - Christopher Buckley	242.0 MB	5 ms	9 ms	1	1	██████████
●	z- Meraki San Francisco GCI	107.6 MB	45 ms	139 ms	3	2	██████████

分析：主要流量分成三大块：旧金山办公室到数据中心、圣荷西到芝加哥、伦敦两个办公室之间

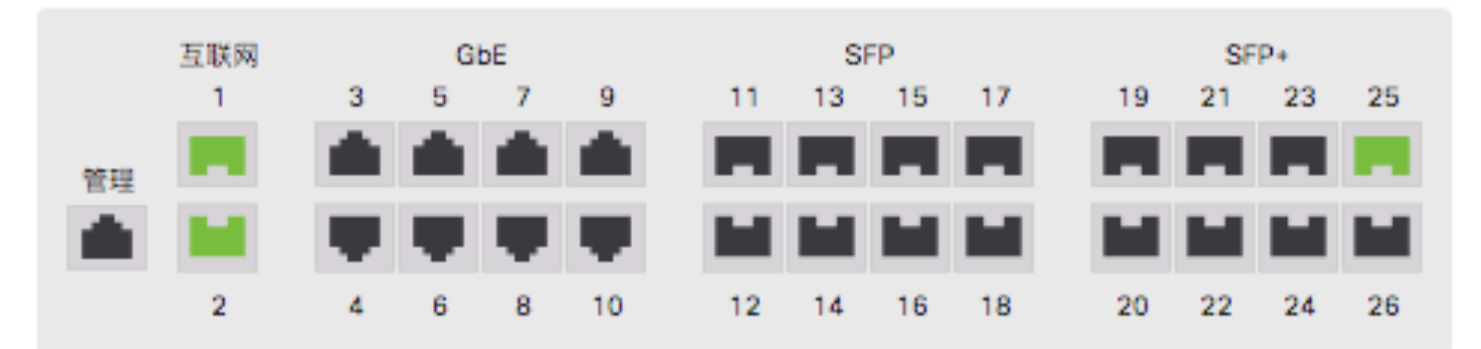


站点带宽利用率

SD-WAN路由器 > 设备状态

实时数据

端口

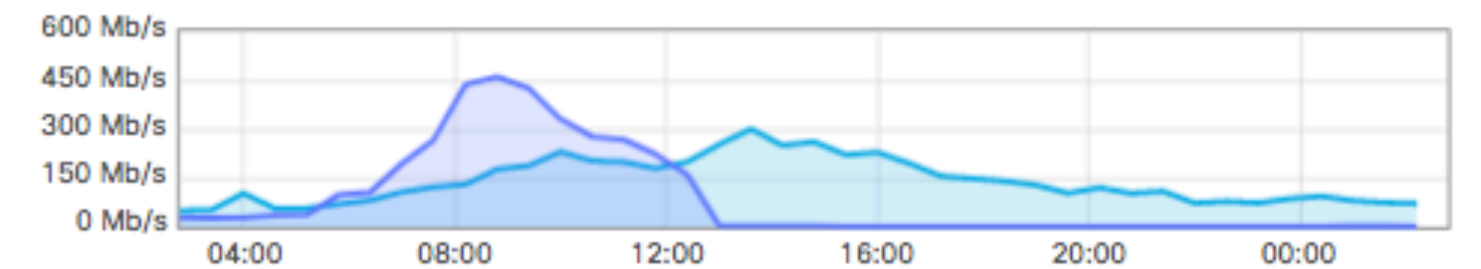


历史数据 过去一天

连接



网络利用率



可视化 — 线路品质

站点间VPN品质

SD-WAN路由器 > VPN状态 > 点击条状图

Meraki旧金山 - 安全



Meraki London -
Bishopsgate - appliance

自定义策略类别

名称	新订时间 (毫秒)	抖动时间 (毫秒)	丢失率 (%)
Citrix	150	30	5

VPN 路由选项

Use the uplink that's best for VoIP traffic.
any from 172.16.42.0/22:any to any:any

Use the uplink that's best for VoIP traffic.
any from 172.16.44.0/21:any to any:any

Modify VPN flow preferences on the [traffic shaping page](#).



站点上行线路品质

SD-WAN路由器 > 设备状态 > 上行链路

实时数据

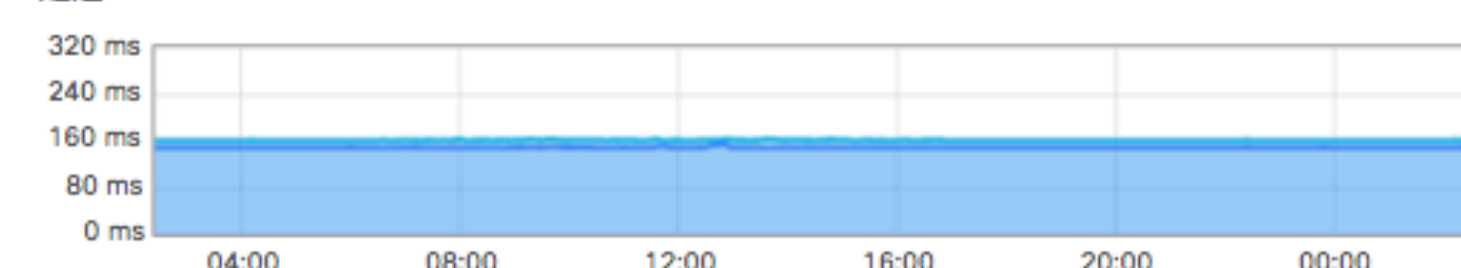
上行链路流量



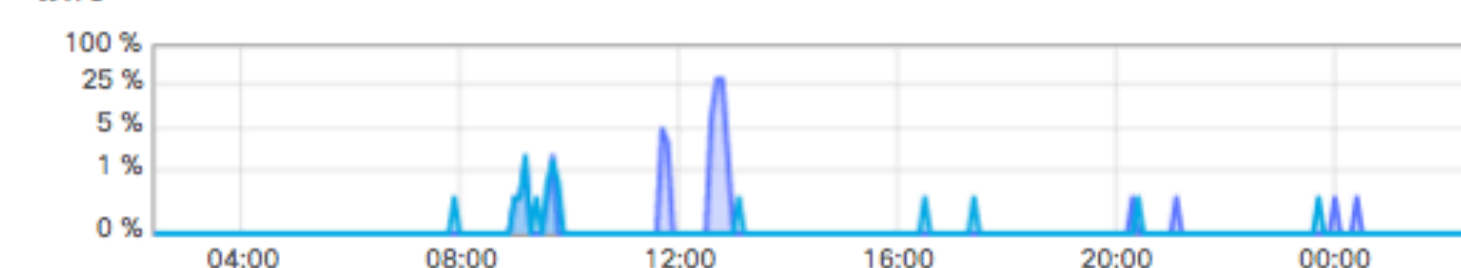
历史数据 过去一天

连接至 122.202.8.147

延迟



损耗



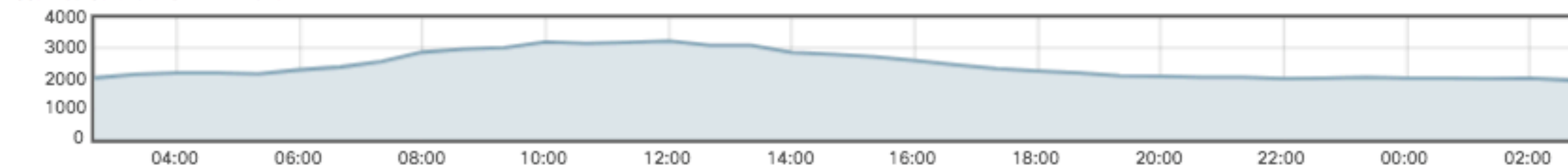
可视化 - 应用流量

站点应用流量

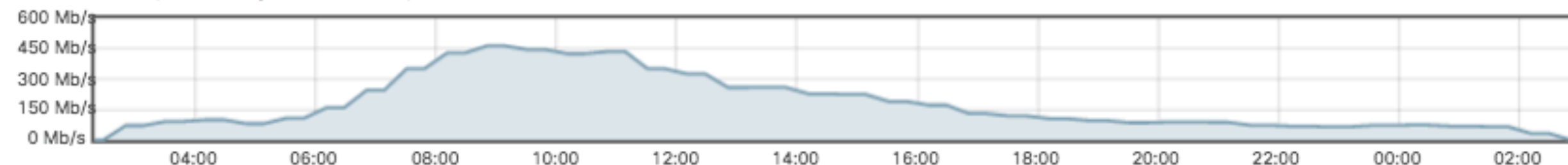
全网 > 流量分析

流量分析 过去一天 ▾

客户端计数 大约 4460 个唯一 clients



用量 1.9 TB (↓ 1.08 TB, ↑ 843.67 GB)



应用	目的地	国家/地区	协议	端口	% 使用比例	用量 ↑	已发送	已接收	流	活动时间 ⓘ	客户端数量
Meraki HTTPS	-	-	-	-	26.1%	508.92 GB	390.93 GB	117.99 GB	290895	6.7 months	1196
WebEx	-	-	-	-	6.5%	126.06 GB	20.28 GB	105.78 GB	45425	22 days	583
Microsoft OneDrive	-	-	-	-	5.3%	102.32 GB	100.63 GB	1.70 GB	42	4.7 days	16
iCloud	-	-	-	-	4.8%	93.75 GB	3.19 GB	90.56 GB	27250	10 days	429
Web based email	smtp.foxit.com	US	TCP	443	2.8%	53.94 GB	28.59 GB	25.36 GB	102213	2.9 months	687
YouTube	-	-	-	-	2.4%	46.99 GB	774.4 MB	46.24 GB	13351	8 days	436
Google HTTPS	-	-	-	-	2.3%	44.45 GB	18.12 GB	26.33 GB	72306	4.4 months	1117
Gmail	-	-	-	-	1.5%	28.70 GB	2.10 GB	26.60 GB	36384	9.4 weeks	893
Miscellaneous secure web	smtp.yix.com.cn	US	TCP	443	1.1%	20.84 GB	190.6 MB	20.65 GB	10	13 hours	5
iTunes	-	-	-	-	1.0%	19.79 GB	254.5 MB	19.54 GB	3845	16 hours	111
Netflix	-	-	-	-	1.0%	19.07 GB	362.8 MB	18.71 GB	596	32 hours	31
Facebook	-	-	-	-	0.9%	17.90 GB	681.5 MB	17.23 GB	7590	13 days	563
Miscellaneous secure web	smtp12.gdt.hcyn.com	US	TCP	443	0.9%	17.03 GB	328.7 MB	16.70 GB	43	30 hours	15
Miscellaneous secure web	smtp17.dzwd.com	US	TCP	443	0.8%	16.14 GB	5.53 GB	10.60 GB	25432	28 days	179
salesforce.com	-	-	-	-	0.7%	14.56 GB	3.63 GB	10.93 GB	139874	60 days	634

15 项结果/页

将报告下载为 CSV

* 排除流量不足总网络流量 0.1% 的目的地

用户流量分析

全网 > 客户端 > 点击要分析的客户端名称

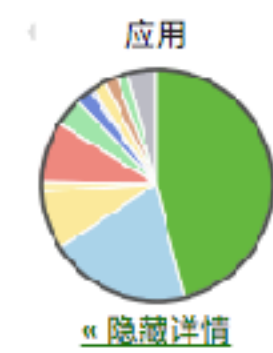
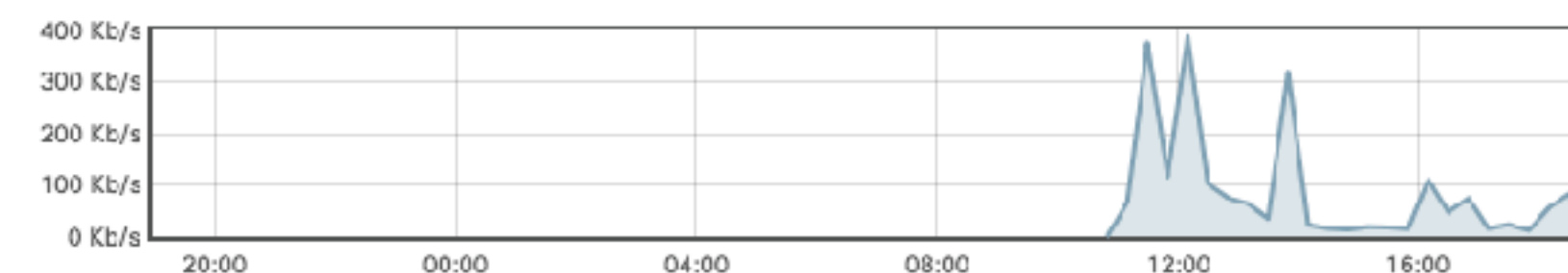
客户端: Yijen-Wang-MBP

状态: 相关的 Nov 22 11:12
 SSID: blizzard
 无线接入点: AP3 (topology)
 启动: N/A
 信号: 47dB (channel 36)
 用户: yijwang (802.1X登录)
 设备类型: Apple Mac OS X 10.13
 功能: 802.11ac - 2.4 and 5 GHz, Fastlane capable [详细信息](#)
[事件日志](#) | [数据包捕获](#) | [添加注释](#)



用量 过去一天 ▾

302.3 MB (+245.2 MB, +57 MB)



目的地	协议	端口	% 使用比例	用量 ↑	已发送	已接收	流	活动时间
Meraki HTTPS	-	-	19.9%	61.0 MB	4.7 MB	56.3 MB	166	3.6 hours
smtp.yix.com.cn	TCP	443	13.5%	41.4 MB	1006 KB	40.4 MB	1	2 minutes
smtp.dzwd.com	TCP	443	10.5%	32.4 MB	765 KB	31.8 MB	8	3 minutes
Facebook	-	-	8.0%	24.7 MB	1.9 MB	22.8 MB	47	2.2 hours
smtp.hcyn.com	TCP	443	7.3%	22.5 MB	12.3 MB	10.1 MB	141	3.8 hours
Google HTTPS	-	-	3.7%	11.3 MB	2.7 MB	8.5 MB	140	6.2 hours
smtp.yix.com.cn	TCP	443	2.3%	6.9 MB	1.2 MB	5.7 MB	71	14 minutes
WebEx	-	-	1.8%	5.4 MB	777 KB	4.6 MB	249	4.5 hours
smtp12.gdt.hcyn.com	TCP	443	1.5%	4.7 MB	84 KB	4.7 MB	1	60 seconds
smtp.dzwd.com	TCP	443	1.2%	3.8 MB	3.5 MB	344 KB	8	54 minutes
smtp17.dzwd.com	TCP	443	1.2%	3.6 MB	625 KB	3.0 MB	7	60 seconds
smtp.yix.com.cn	TCP	443	1.1%	3.3 MB	50 KB	3.2 MB	1	60 seconds
Google Drive	-	-	0.9%	2.8 MB	1.4 MB	1.4 MB	9	4.3 hours

可视化 — 应用品质

需要 MI License
中国控制面板尚未开放

应用服务品质

洞察 > 点选地点

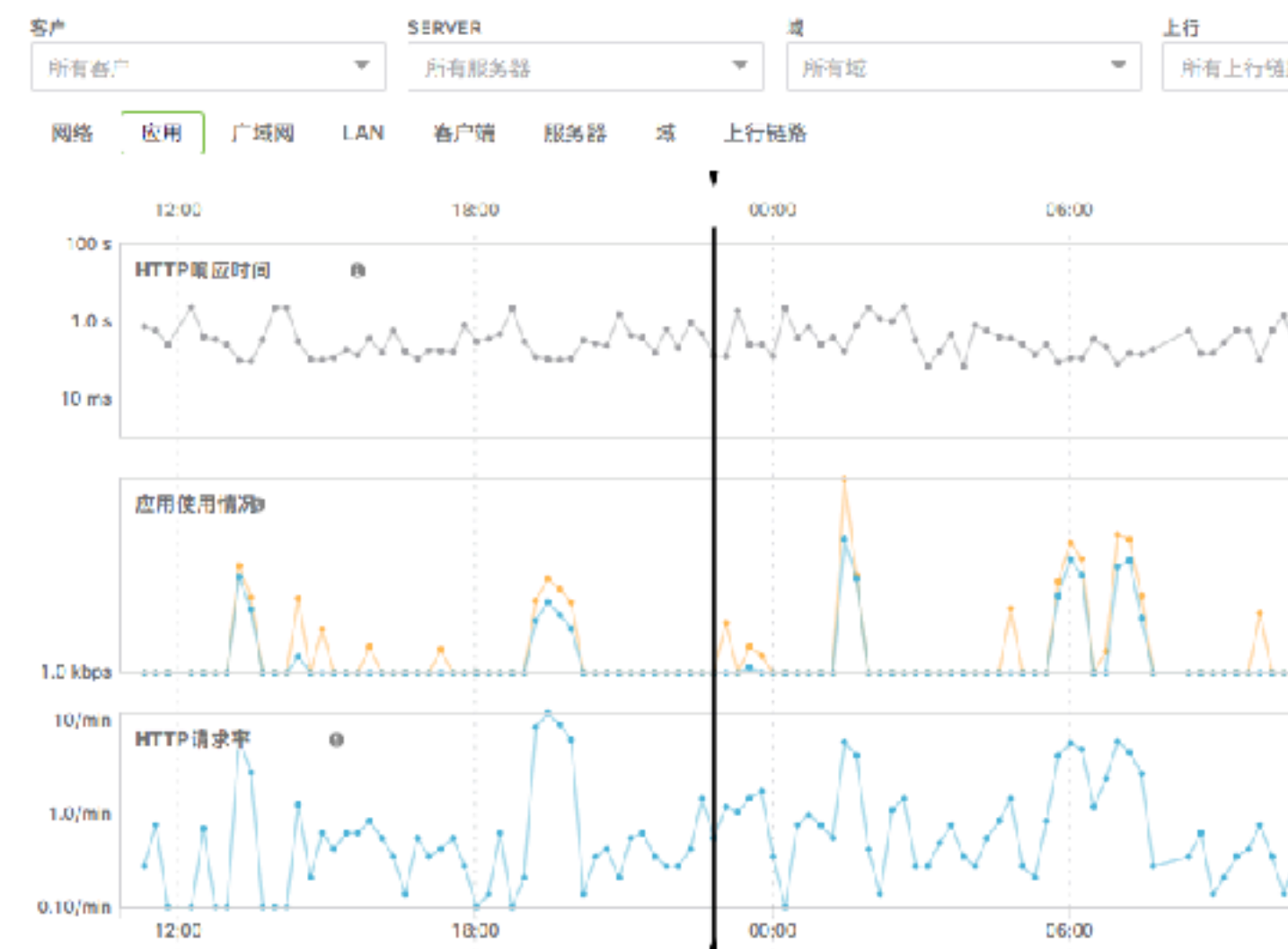
Web App Health for Meraki San Francisco - Security 过去2小时



应用服务品质

洞察 > 点选应用服务

WEB APP HEALTH > MFRANKLIN - 安全
Windows Office365 过去一天



WEB APP HEALTH > MFRANKLIN - 安全
Windows Office365 过去一天



使用应用服务仪表板，实时监控企业关键服务。

- 网络监控：综合得分、网络使用量、延迟
- 应用监控：HTTP响应时间、带宽使用量、HTTP请求率
- 广域网监控：WAN Goodput、掉包、延迟

- 局域网监控：LAN Goodput、掉包、延迟
- 其他：客户端得分、服务器得分、域得分、上行线路得分等...

流量控制

限速 — 针对每个用户

SD-WAN路由器 > SD-WAN和流量整形

全局带宽限制

每客户端限制

50 Mbps

[详细信息](#)

启用 SpeedBurst ⓘ

整形 — 默认规则

SD-WAN路由器 > SD-WAN和流量整形

启用默认流量整形规则 ⌵

Traffic Type	DSCP tag
SIP (Voice)	46 (EF - Expedited Forwarding, Voice)
All Advertising, All Software Updates, All Online Backups	10 (AF11 - High Throughput, Latency Insensitive, Low Drop)
WebEx, Skype	34 (AF41 - Multimedia Conferencing, Low Drop)
All Video & Music	18 (AF21 - Low Latency Data, Low Drop)

整形 — 自定义针对每个用户和每个应用的流控

SD-WAN路由器 > SD-WAN和流量整形

规则 1 ⊕ ✕

定义

此规则将在与以下任何表达式匹配的流量上强制实施。

带宽限制

优先级

DSCP 标记

[添加新整形规则](#)

添加 +

自定义表达式

通告

博客

商业管理

数据库和云服务

邮件

文件共享

游戏

卫生保健

新闻

在线备份

Peer-to-peer (P2P)

生产率

远程监控和管理

自定义表达式

添加表达式

主机名 ⓘ

google.com

CIDR/IP 范围

192.1.0.0

192.1.0.0/16

端口 ⓘ

80

9090

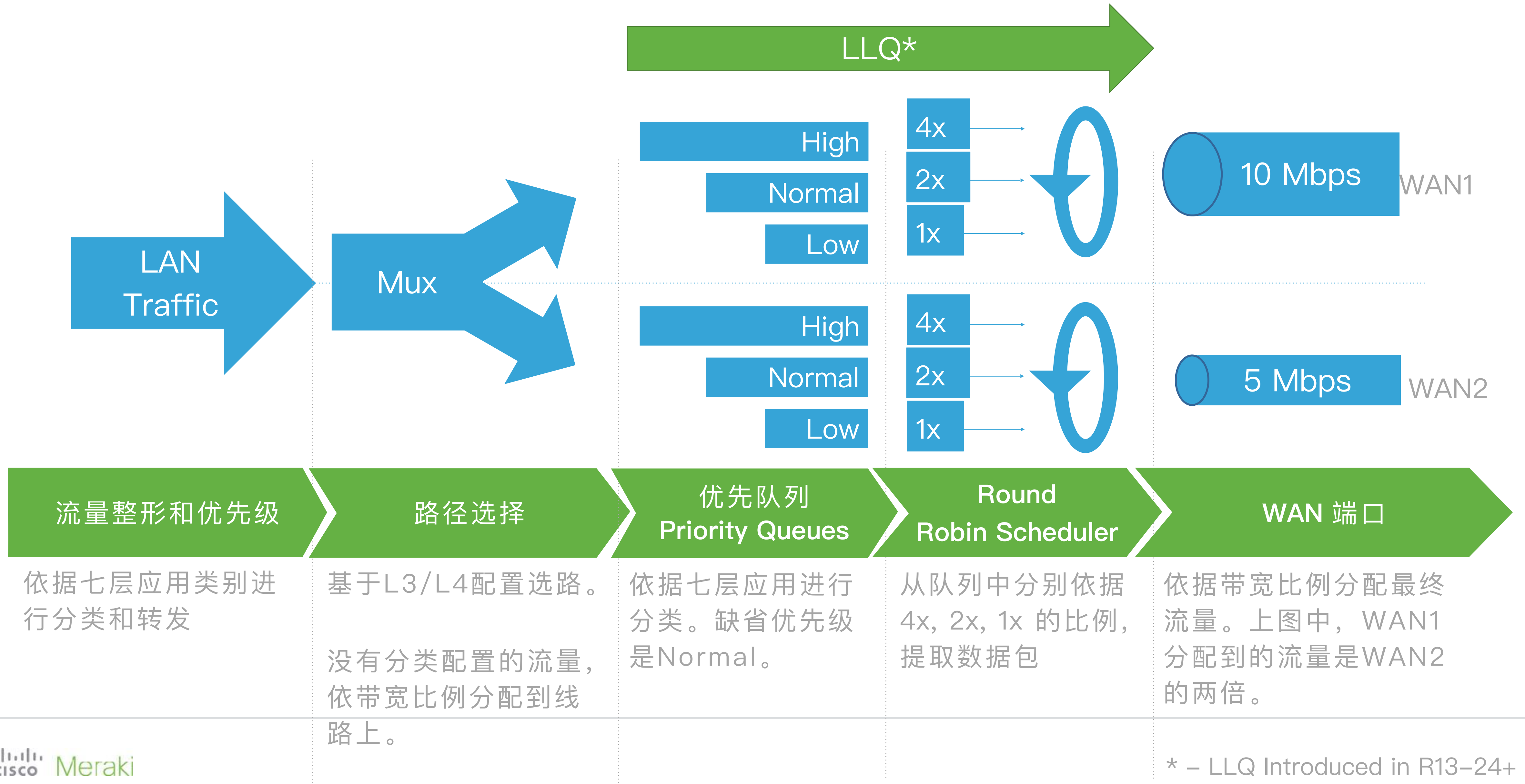
自定义网络和端口

10.1.0.0/16:80

本地网络 ⓘ

本地网络: 192.168.0.0/16

流量控制

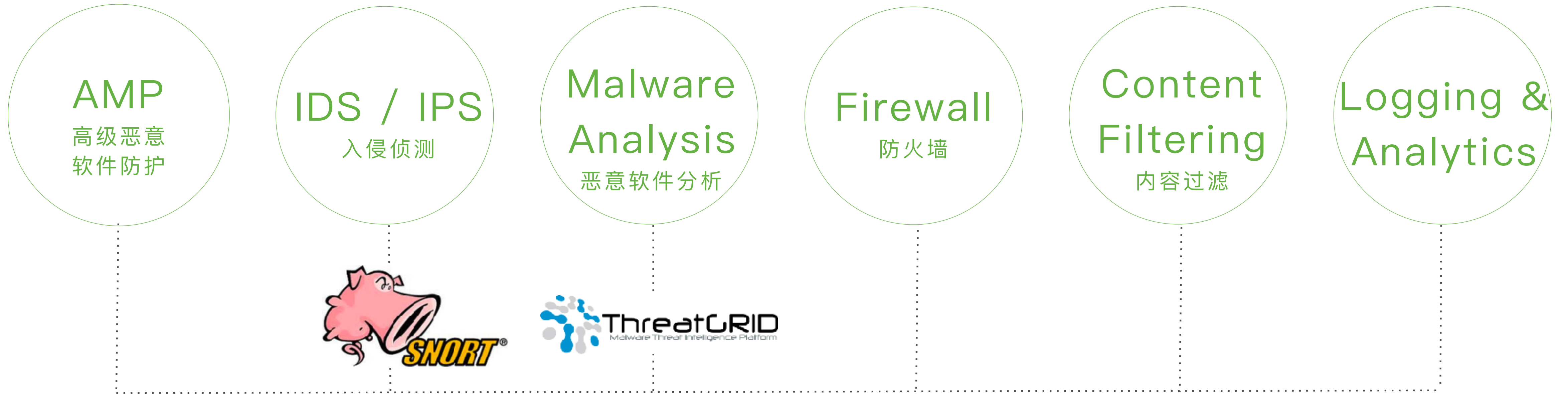


Security

安全



Meraki MX 安全功能



安全 — 组织安全纵览

安全中心

组织 > 安全中心

追溯性恶意软件检测 1

接收时间	威胁名称	受影响的客户端
Nov 13 19:25:12	Setup.zip	1

一段时间内发生的事件



受影响最大的网络

网络	活动
Z - San Francisco - Lab and Guest	11634
Meraki San Francisco - Security	4213
Meraki Sydney	4162
Meraki London - Finsbury	1945
Z - Chicago VanBuren - Lab and Guest	3
Cisco Cloud Interconnect - San Jose	3

排名靠前的威胁源



受影响最大的客户端

客户端	网络	受影响最小	活动
lab-mx-00180e439ce9 Meraki Network OS	Z - San Francisco - Lab and Guest	Nov 7 0:01:11	11565
64.102.14.232	Meraki San Francisco - Security	Nov 14 3:30:16	3942
Cisco - Alpha ABB GW 1	Meraki London - Finsbury	Nov 22 0:03:13	293
mihint-6tt26gh	Meraki London - Finsbury	Nov 21 22:15:12	285
SEP5EB7F2954A42	Meraki Sydney	Nov 23 0:37:26	257

最常见的威胁

威胁	出现次数
PUA-OTHER CPUMiner-Multi cryptocurrency mining pool connection attempt	11566
POLICY-OTHER Adobe ColdFusion admin interface access attempt	2358
SQL 1 = 1 - possible sql injection attempt	1076
SERVER-APACHE Apache Struts remote code execution attempt	805
SERVER-APACHE Apache Struts remote code execution attempt	763
SERVER-WEBAPP Java XML deserialization remote code execution attempt	726
SERVER-APACHE Apache Struts remote code execution attempt - POST parameter	483
OS-WINDOWS Microsoft Windows SMB-DS Trans Max Param OS-WINDOWS attempt	406
SERVER-WEBAPP Apache Struts remote code execution attempt	305
SERVER-WEBAPP JBoss web console access attempt	303

安全 — NGFW防火墙

三层防火墙

SD-WAN路由器 > 防火墙

第3层

入站规则

#	策略	协议	信息来源	源端口	目的地	目标端口	备注	点击数	行动
	允许	Any	Any	Any	Any	Any	默认规则	0	

[添加规则](#)

出站规则

#	策略	协议	信息来源	源端口	目的地	目标端口	备注	点击数	行动
	允许	Any	Any	Any	Any	Any	默认规则	0	

[添加规则](#)

蜂窝网故障转移规则

#	策略	协议	信息来源	源端口	目的地	目标端口	备注	行动
	允许	Any	Any	Any	Any	Any	默认规则	

[添加规则](#)

路由器服务

服务	允许的远程 IP
ICMP ping	Any
Web (本地状态&配置)	None
SNMP	None

IP源地址伪造保护

模式

阻止

4G LTE 带宽有限，如果正常线路中断，转移到备用的4G LTE时，可以限制一些较不重要的流量。

WAN port上的服务，应该只对真正有需要的IP开启。

七层防火墙

SD-WAN路由器 > 防火墙

第7层

防火墙规则

#	策略	应用	行动
1	Deny	HTTP hostname...	e.g. "example.com"

添加一个第

- Blogging
- Email
- File sharing
- Gaming
- News
- Online backup
- Peer-to-peer (P2P)
- Social web & photo sharing
- Sports
- Video & music
- VoIP & video conferencing
- Web file sharing
- Software & anti-virus updates
- Security
- Productivity
- Remote monitoring & management
- Business management
- Health care
- Web payments
- Databases & cloud services
- Advertising
-
- HTTP hostname...
- Port...
- Remote IP range...
- Remote IP range & port...

- 可以为不同部门的员工、访客、外部承包商、和不同类型的设备，配置不同的组策略。
 - 组策略中包含：可连网时间表、可用带宽、三层和七层防火墙、流量整形等规则。
- 组策略

名称	影响	带宽
一般员工	0 客户端	2.00 Mb/s 上行, 下行
访客	0 客户端	1.00 Mb/s (上行, 下行)
研发部	0 客户端	SSID默认

安全 — Geo-IP 防火墙

需要 SEC License
中国控制面板即将开放

Geo-IP 防火墙

SD-WAN 路由器 > 防火墙

第 7 层

防火墙规则

#	策略	应用	行动
1	Deny	Countries...	

[添加一个第 7 层防火墙规则](#)

✓ 流量去往/来自
流量非去往/来自

- 阿富汗
- 奥兰群岛
- 阿尔巴尼亚
- 阿尔及利亚
- 美属萨摩亚
- 安道尔
- 安哥拉
- 安圭拉
- 南极洲
- 安提瓜和巴布达

安全 — 入侵侦测

需要 SEC License
中国控制面板即将开放

类别过滤

SD-WAN路由器 > 内容过滤

入侵检测和预防

模式 ⓘ

预防

预防: 侦测 + 告警 + 阻挡

检测: 侦测 + 告警

规则集 ⓘ

平衡

连接: 包含过去2年CVSS得分10的规则

平衡: 包含过去2年CVSS得分9以上的规则

安全: 包含过去3年CVSS得分8以上的规则

已列入白名单的规则 ⓘ

MALWARE-OTHER self-signed SSL certificate with default Int...

[Whitelist an IDS rule](#)

- 所有WAN、LAN之间与不同VLAN之间的流量都会检查。



实例：勒索病毒

WannaCry Snort

Security Center last month

snort_rule: 42329-42332 Search events Filter 75 matching events

Summary Events

[Win.Trojan.Eternalblue WnCRY variant](#)

Rule ID	Whitelist	Links
42329-42332	Off	dns.google.com



侦测到 Eternalblue 变种WannaCry勒索病毒

Meraki MX 封锁该病毒



Summary		Events				
Time	Type	Source	Destination	Disposition	Action	Details
May 31 10:20:42	IDS Alert	WEB-SERVER1	5.188.10.245:60904		Blocked	MALWARE-CNC Win.Trojan.Eternalblue WannaCRY variant

安全 — 内容过滤

需要 SEC License
中国控制面板即将开放

类别过滤

SD-WAN路由器 > 内容过滤

类别过滤

屏蔽的网站类别

URL 类别列表大小 ⓘ

包含40亿条URL
↓

Choose content categories to block

- 堕胎
- 滥用药物
- 成人和色情
- 酒精和烟草
- 拍卖
- 僵尸网络
- 欺骗 (学术)
- 计算机和互联网信息
- 计算机和互联网安全
- 已确认的垃圾邮件源

URL 拦截 (黑白名单)

SD-WAN路由器 > 内容过滤

URL 拦截

[了解 URL 拦截的工作原理](#)

已屏蔽的 URL 图案

(每行输入一个模式)

列入白名单的 URL 方案

(每行输入一个模式)

白名单优先于黑名单
↑

HTTPS 请求也可能被屏蔽。由于 HTTPS 请求中的 URL 已进行加密，因此仅将执行域检查
↓

安全 — AMP高级恶意软件防护

需要 SEC License
中国控制面板尚未开放

类别过滤

SD-WAN路由器 > 内容过滤

高级恶意软件防护 (AMP)

模式 📘 启用 ⌵

已列入白名单的 URL 📘

URL	备注
<input type="text"/>	<input type="text"/>

[添加已列入白名单的 URL](#)

已列入白名单的文件

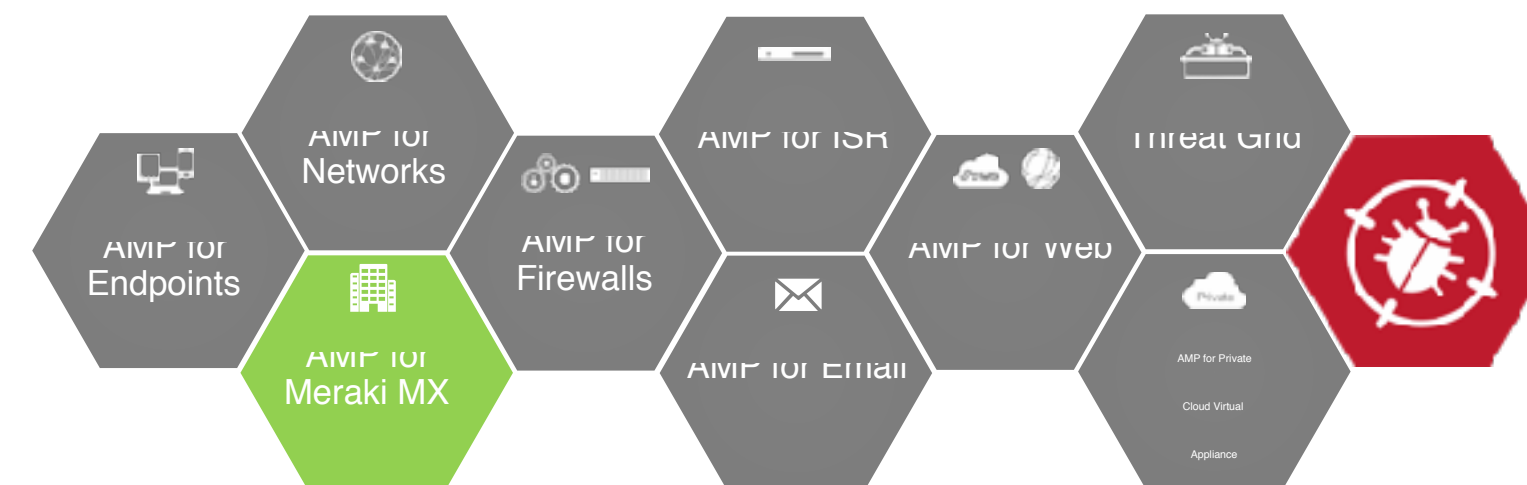
SHA256	备注
<input type="text"/>	<input type="text"/>

[添加已列入白名单的文件](#)

• 支持的文件类型

- MS OLE2 (.doc, .xls, .ppt)
- MS Cabinet (Microsoft compression type)
- MS EXE
- ELF (Linux executable)
- Mach-O/Unibin (OSX executable)
- DMG (Apple Disk Image)
- Java (class/bytecode, jar, serialization)
- PDF
- ZIP (regular and spanned)*
- EICAR (standardized test file)
- SWF (shockwave flash 6, 13, and uncompressed)

* 包含 XML-based Microsoft Office 文件 (.docx, .xlsx, etc...)



Meraki MX 是思科安全架构中的一环

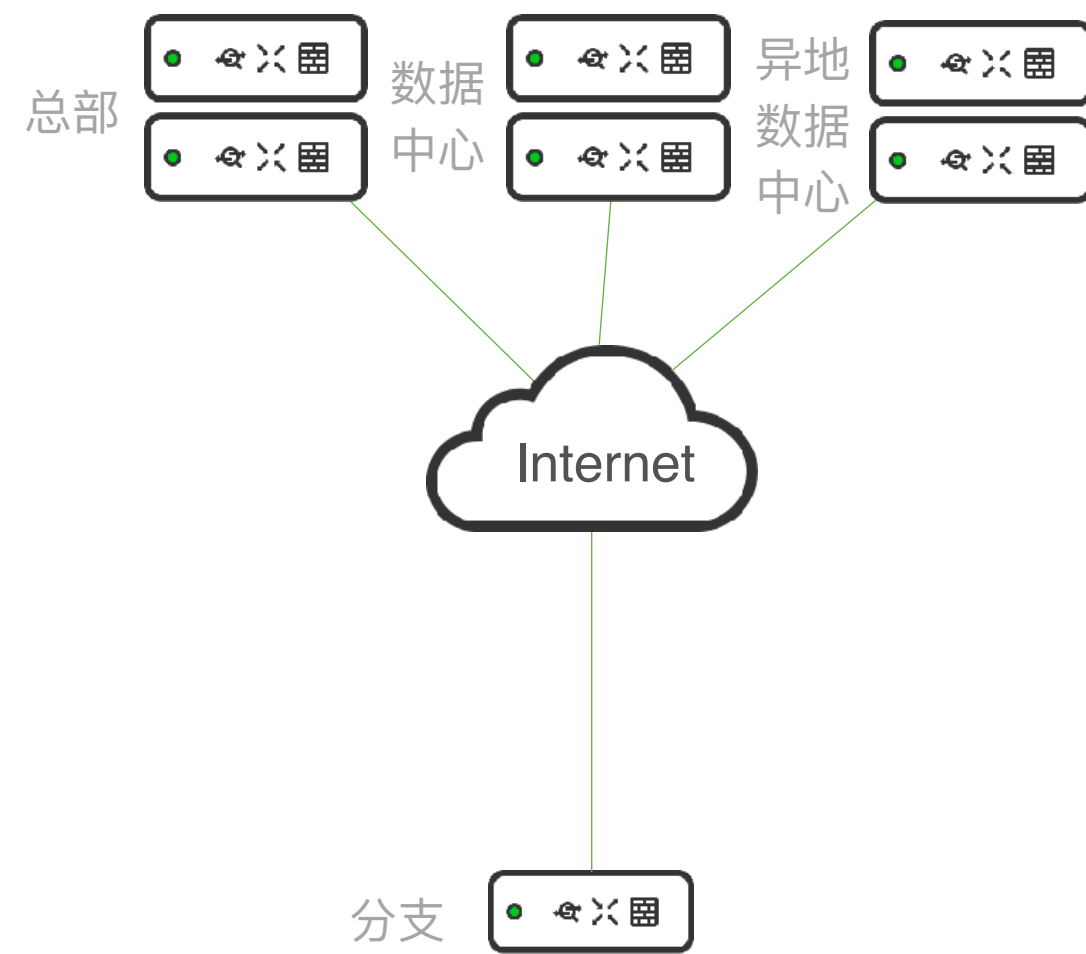
SD-WAN Design

网络设计

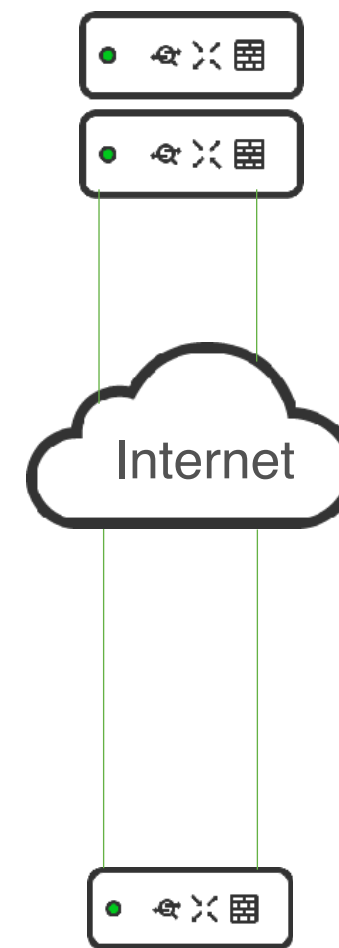
高可用性

High Availability and Redundancy

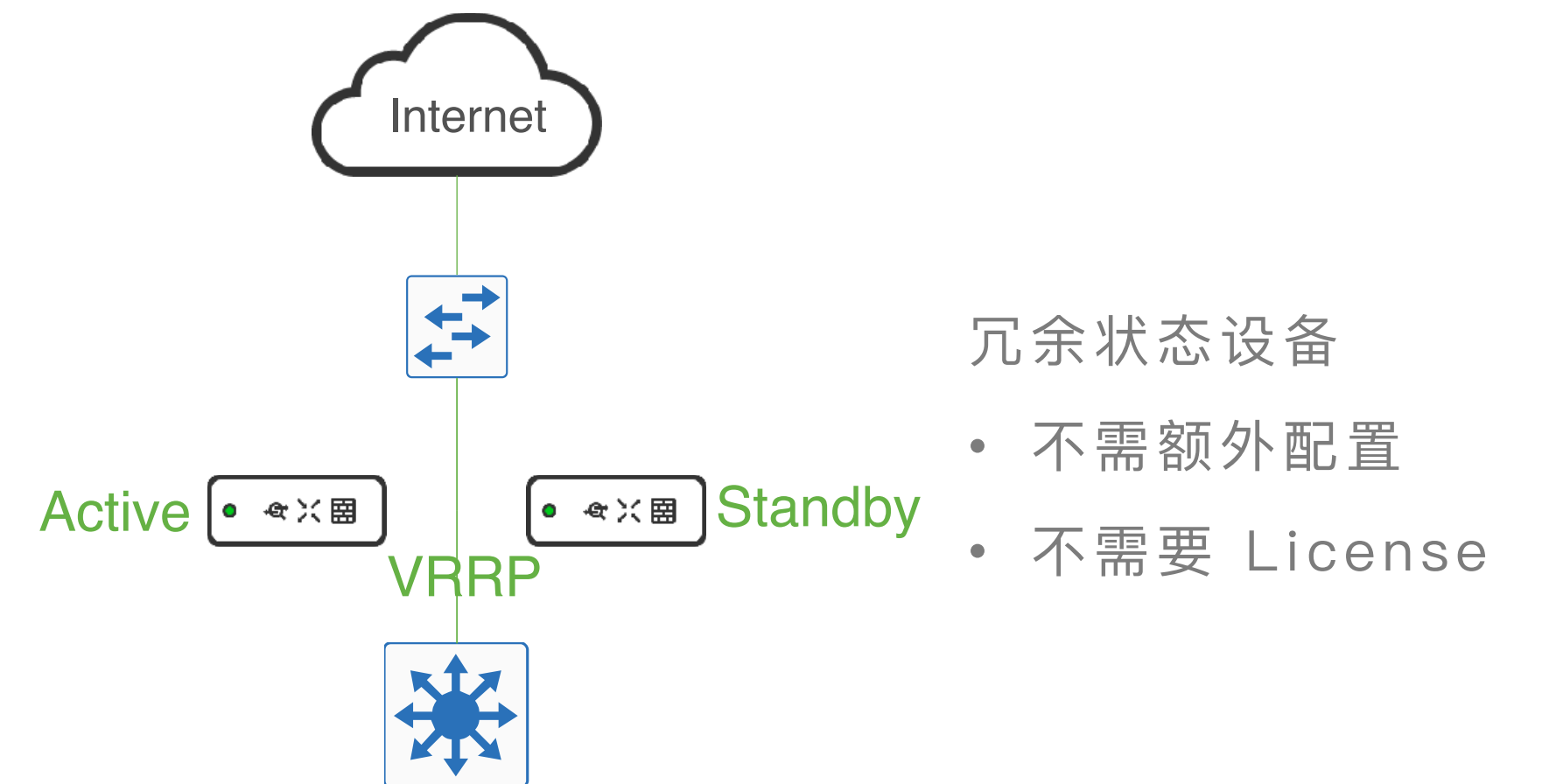
站点冗余



线路冗余



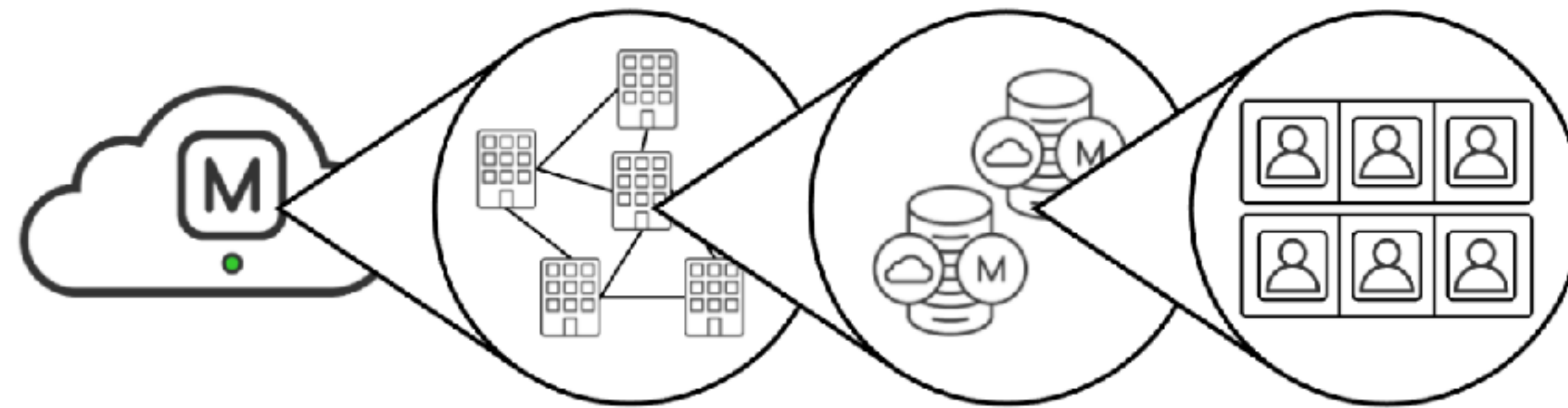
设备冗余



高可用性

High Availability and Redundancy

控制平面冗余 (99.99%)



Meraki SaaS 系统

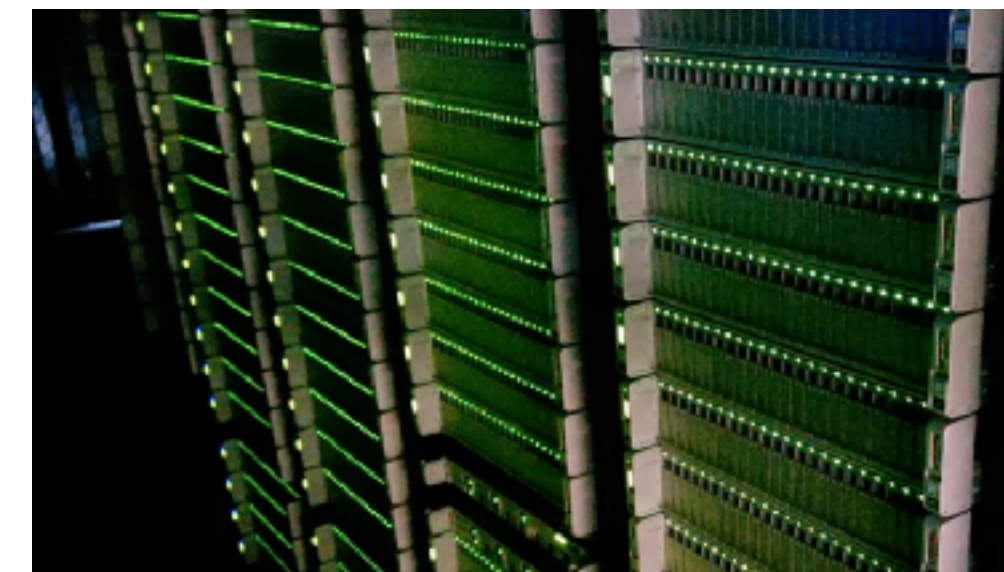
冗余数据中心

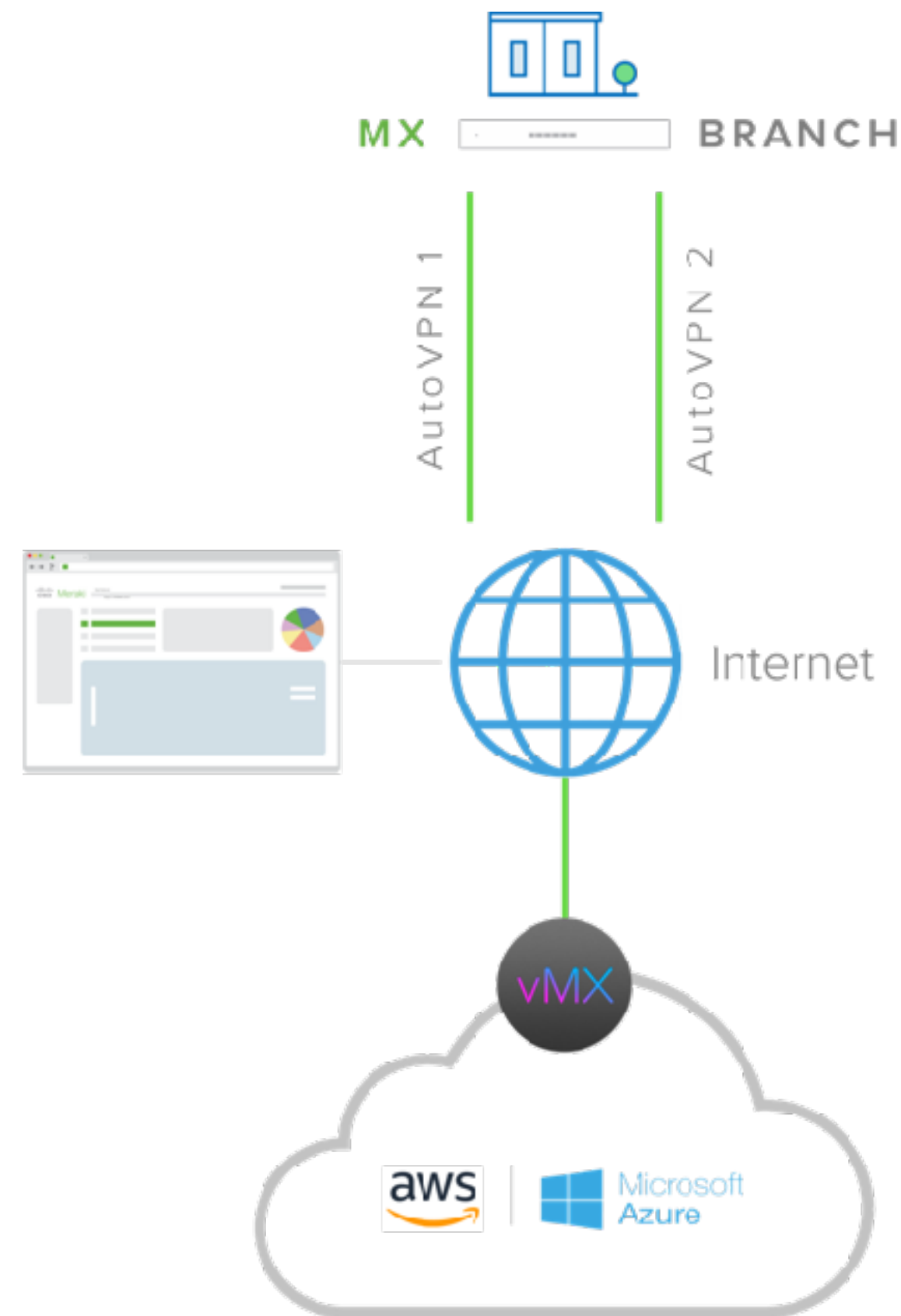
冗余服务器

客户组织隔离



Region	Data Center 1	Data Center 2
North and South America	USA	USA
Europe	Germany	Germany
Asia	Australia	Southeast Asia
China	China	China





- 藉由与虚拟化的 vMX 之间建立 site-to-site AutoVPN 把 MX 部署延伸到 AWS 或 Microsoft Azure 上的IT环境。
- 使用与实体 MX 相同的方式，在 vMX 启用 SD-WAN，以优化连往 AWS 或 Microsoft Azure 上 IT 服务的路径选择。
- 在控制面板上，管理部署为 AWS EC2 instance 或 Azure VM 的 vMX 就像管理实体 MX 一样
- 高达 500Mbps 的 VPN 性能
- 只需购买 License

SD-WAN Operations

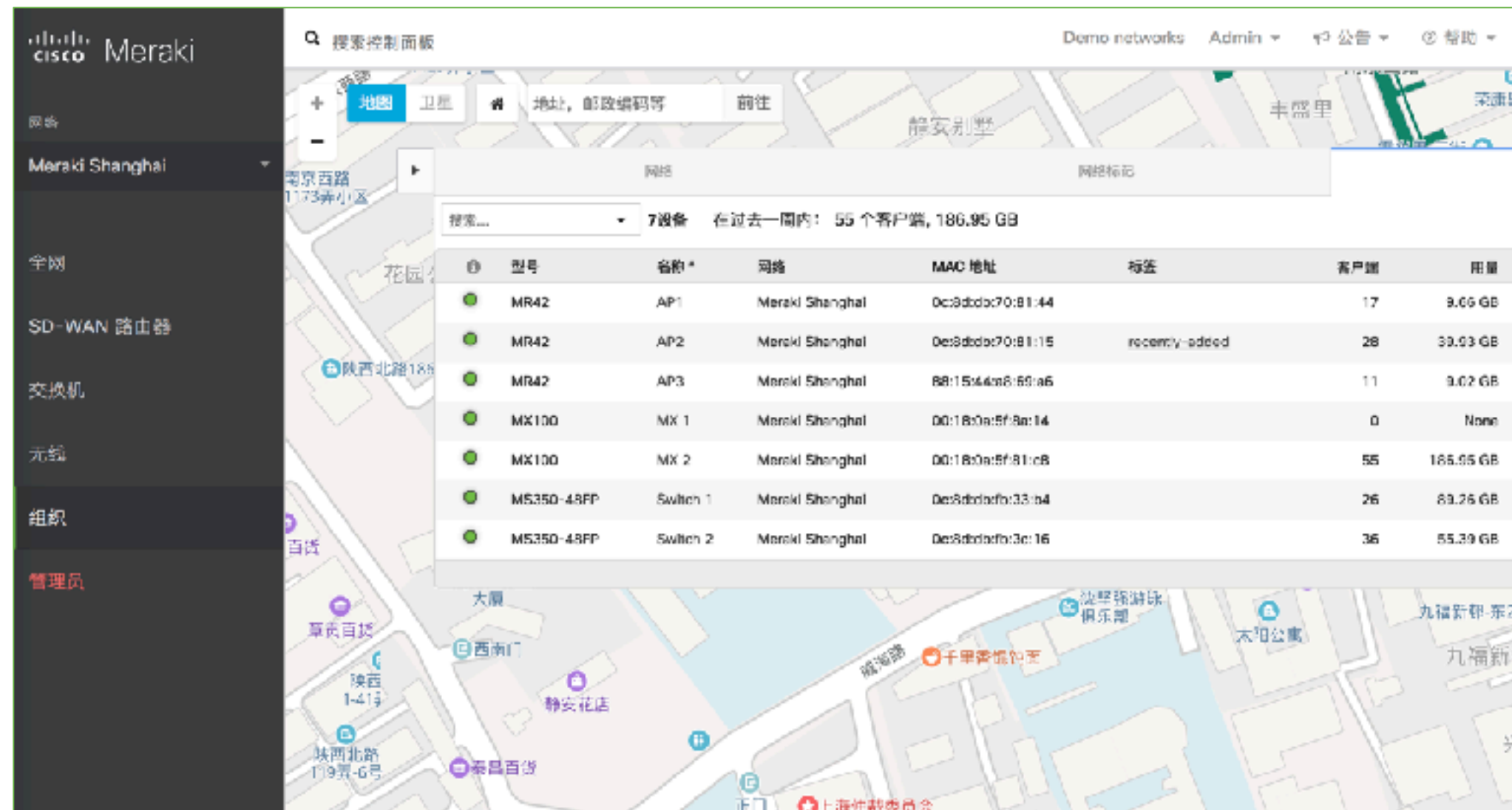
极简运维

简化管理和运维

Simplified Management and Operations

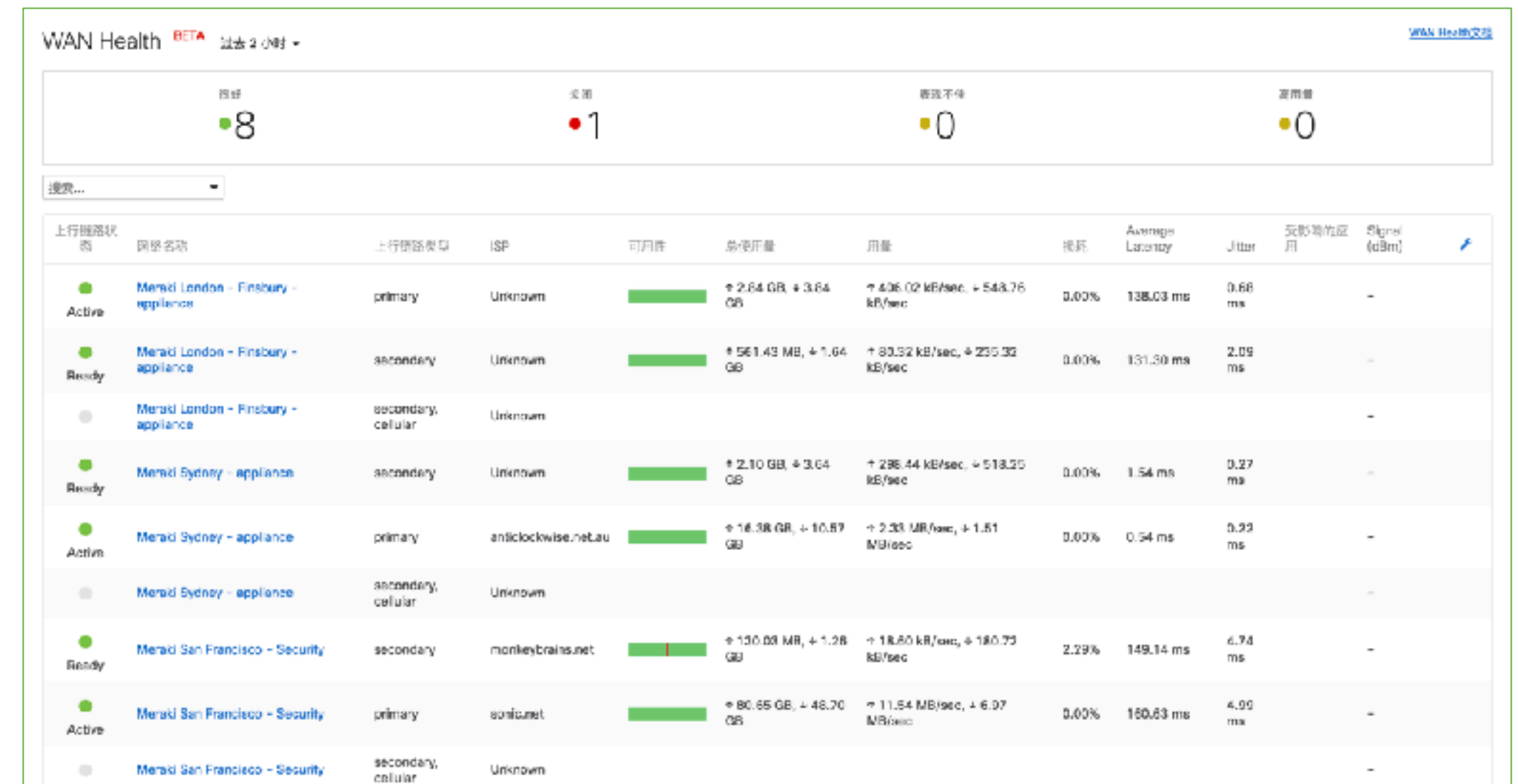
单一管理运维窗口

涵盖路由/安全、交换、无线



丰富的分析报表

涵盖广域网性能、无线信号、安全监控、用户接入等



API



NAT Log



Syslog



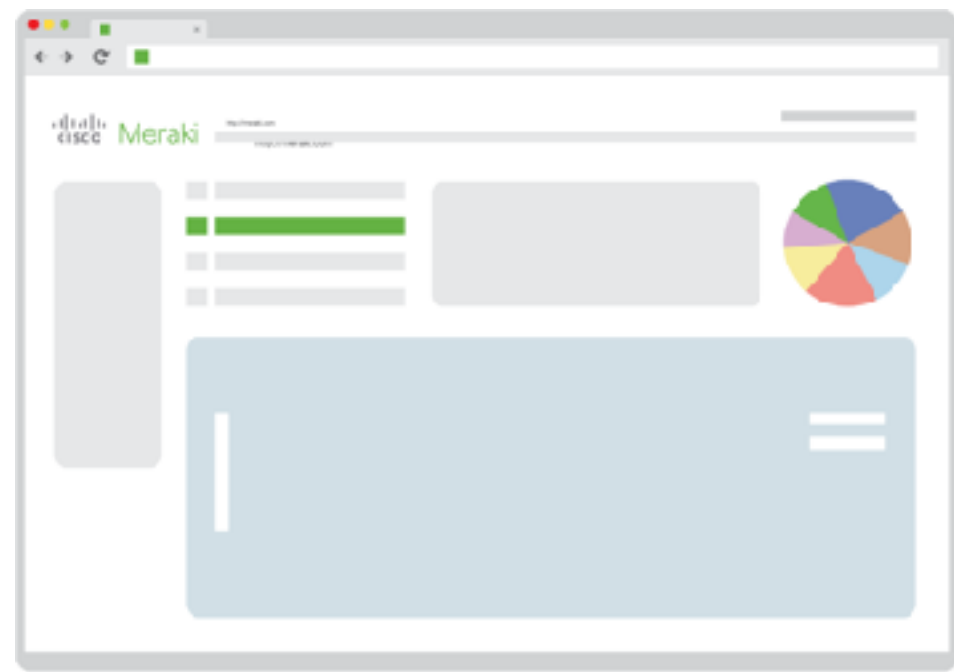
SNMP



NetFlow

零接触部署

Zero Touch Provisioning



仅需一次远程、
基于网页的配置
亦可使用配置模版
简化多站点部署

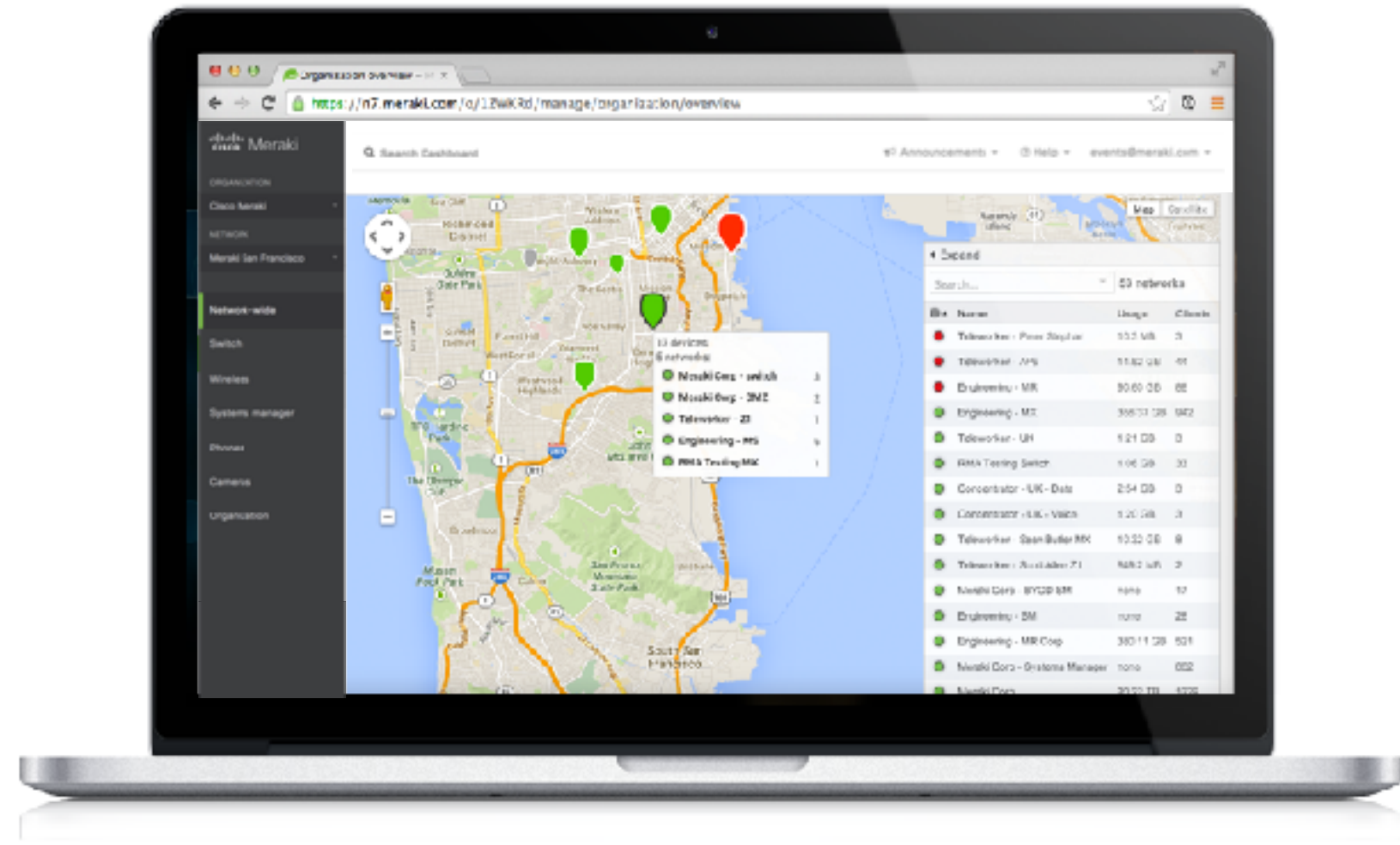


不需预先配置
不需现场配置



开箱后在所需位置
接上MX设备

集中管理 Centralized Management



管理性
MANAGEABILITY

扩展性
SCALABILITY

成本效率
SAVINGS

更完整：一整套完整的安装和管理解决方案

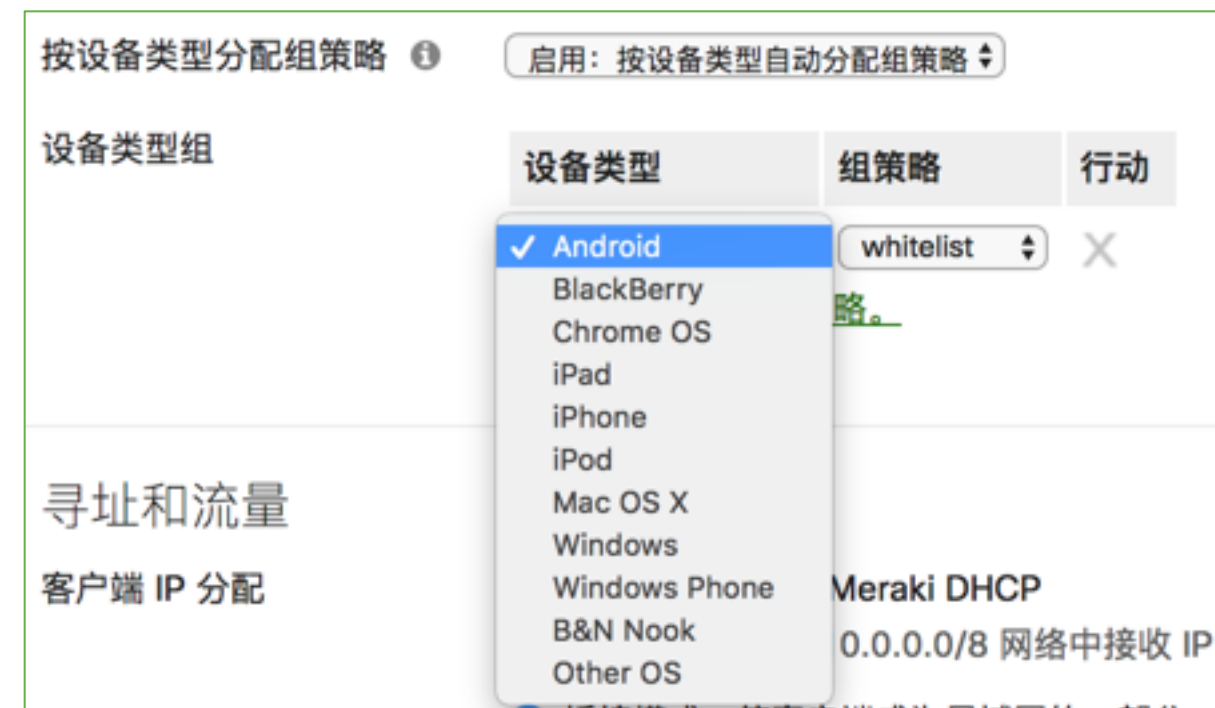
可持续：功能持续更新，并维持高度整合

可扩展：从小型分支支持到大型网络

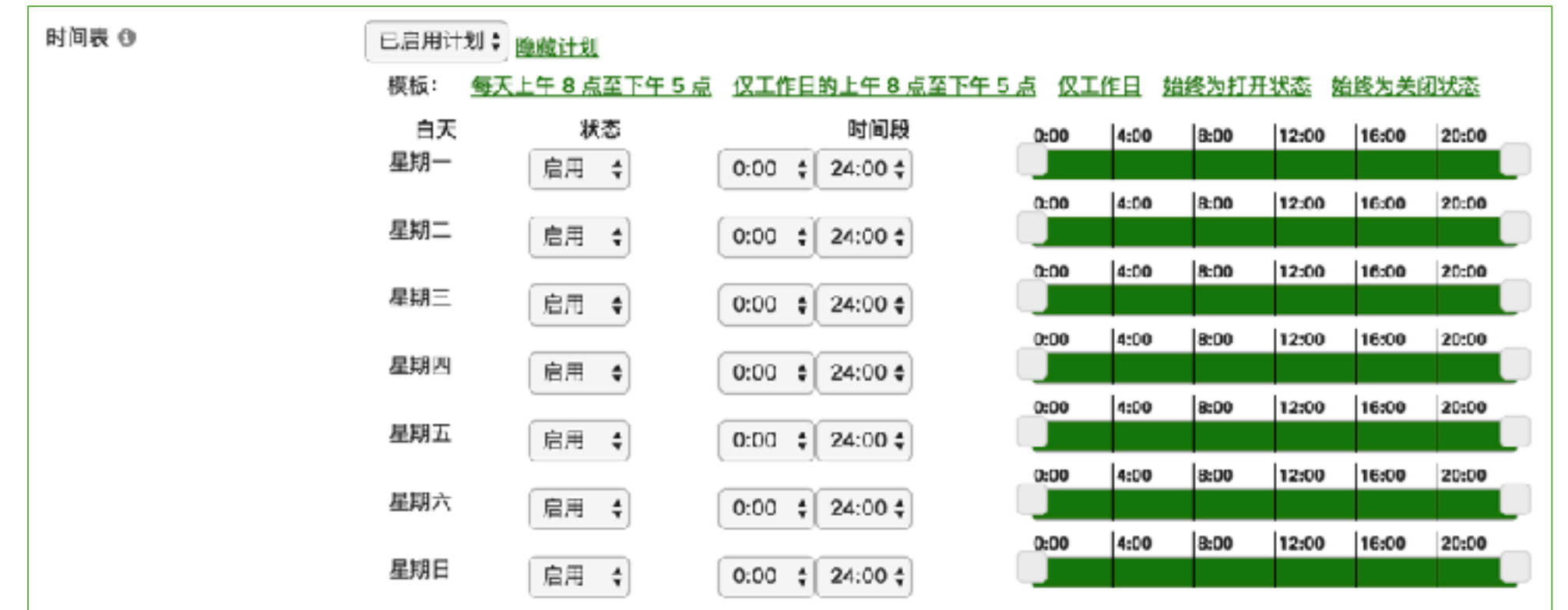
低成本：大幅降低运维成本

自动配置组策略

	MR无线	MX路由
依据客户	√	√
依据设备类型	√	
依据VLAN		√
依据RADIUS回复	√	



可用时间



流量整形



三层七层
防火墙

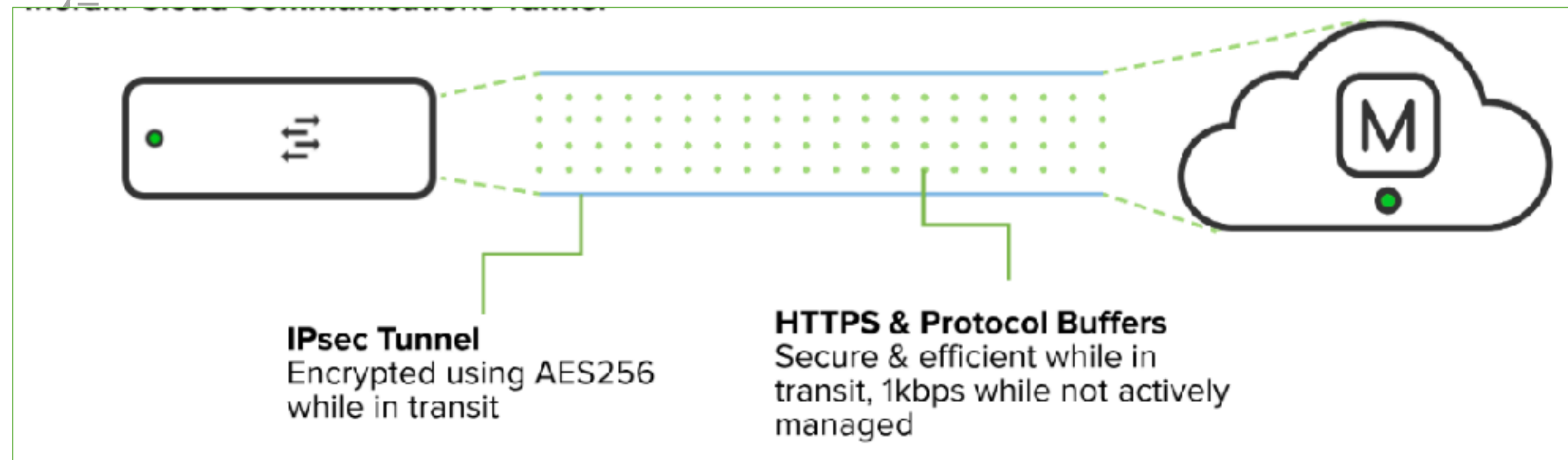


设备准入管理

Device Admission Control

固件 最新 Current version: MX 15.10
配置 过期 (changed 14 minutes ago)
从网络中删除设备...
© 2018 Cisco Systems, Inc. 隐私 - 条款 浙ICP备17050678号-1  浙公网安备3301020200

- 需手动加入设备(序列号或订单号, 设备才会被允许加入组织。
- 如设备损坏、被盗遗失, 将设备从网络中删除, 设备就无法连入组织的网络中。
- 设备与Meraki之间使用AES256加密通信



集中化软件升级

Centralized Software Upgrades

Firmware upgrades ^{BETA}

概述 计划更改 所有网络

最近的变化

计划更改

最新的固件版本

稳定

稳定的候选版本

Beta



MX 13.32
2018年3月29日发布
[发行说明](#)



MS 10.40
Released Oct 16, 2018
[发行说明](#)



MR 25.13
Released Oct 16, 2018
[发行说明](#)

Wireless firmware versions MR 25.13 changelog

New

- Added support for Device Name CCX in Site Survey Mode

Bug fixes

- Fixed an issue where guard interval is incorrectly set (MR16/MR66)
- A corner case causing APs to reboot (MR30H/MR33/MR42/MR52/MR53/MR74/MR84)
- Fixed an issue where an MR30H would not pass BPDU's from LAN ports, potentially leading to upstream network instability (MR30H)
- Removed duplicate timestamps from RADIUS accounting start packets (All MRs)
- Fixed an issue where RADIUS accounting packets were reporting incorrect Acct-Input / Acct-Output values
- Fixed an issue where ARP responses were not sent back over VPN tunnel to MX (All MRs)
- Fixed an issue where the BLE radio would stop beaconing and scanning (MR30H/MR33/MR74)

Known issues

- Condition under investigation that causes VoIP RTP packet loss (MR42/MR52/MR53)
- Condition under investigation causes 2.4GHz radios to become unresponsive (MR32/MR72)
- Condition under investigation causes radios to become unresponsive for 5 seconds in high density networks (MR34/MR32/MR72/MR26)


[<以前的版本 \(MR 25.12\)](#)

概述 计划更改 所有网络

所有网络

计划升级

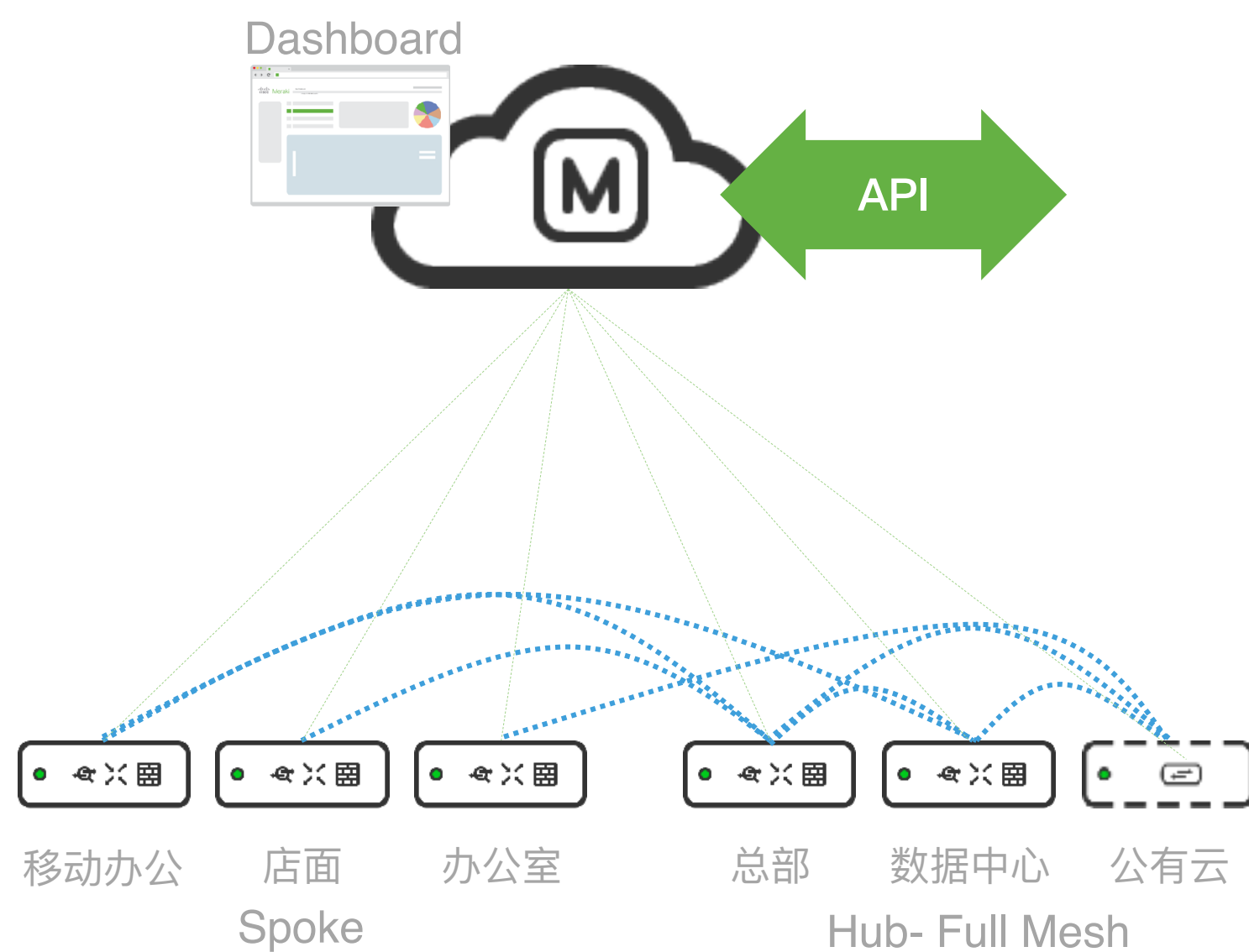
网络名称 设备类型 当前版本 固件状态 **0 networks selected**

<input type="checkbox"/> 网络	设备类型	当前固件版本	固件状态	升级预定	上次升级时间	计划升级版本	
<input type="checkbox"/> Meraki Shanghai	Wireless	MR 25.12	Upgrade available	No	-	-	
<input type="checkbox"/> Meraki Shanghai	Switch	MS 10.35	Upgrade available	No	-	-	
<input type="checkbox"/> Meraki Shanghai	Security appliance	MX 15.10	On beta	No	September 22, 2018	-	

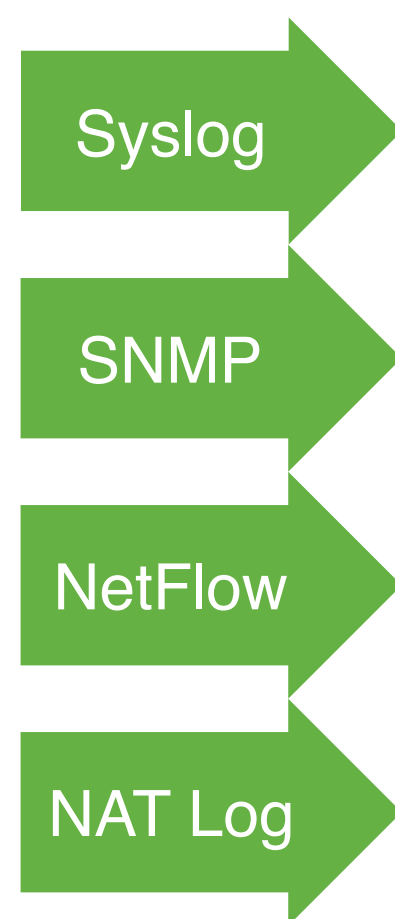
管理和可编程端口

Management and Programmatic Interfaces

编排平面
管理平面
控制平面



数据平面



控制面板 API 帮助

- [管理员](#)
- [警报设置](#)
- [分析](#)
- [蓝牙客户端](#)
- [摄像头](#)
- [客户安全事件](#)
- [客户端](#)
- [配置模板](#)
- [设备](#)
- [Firewalled services](#)
- [组策略](#)
- [HTTP servers](#)
- [MR L3防火墙](#)
- [MX L3防火墙](#)
- [MX VPN防火墙](#)
- [MX集线器防火墙](#)
- [Meraki auth用户](#)
- [网络](#)
- [加强组织管理](#)

客户端

- ▶ 列出设备的客户端（最多一个月以前）。以千字节为单位，返回每个客户端的使用量。如果设备是一台交换机，返回交换机端口；否则交换机端口字段为空。
- ▼ 返回与给定标识符关联的客户端，此端点将根据客户端ID或MAC或IP进行查找，具体取决于网络是否使用Track-by-IP。

HTTP 请求

```
GET /networks/{networkId}/clients/{id_or_mac_or_ip}
```

参数

-

请求示例

```
curl -L -H 'X-Cisco-Meraki-API-Key: <key>' -H 'Content-Type: application/json' -X GET 'https://api.meraki.cn/api/v0/networks/{networkId}/clients/{id
```

响应示例

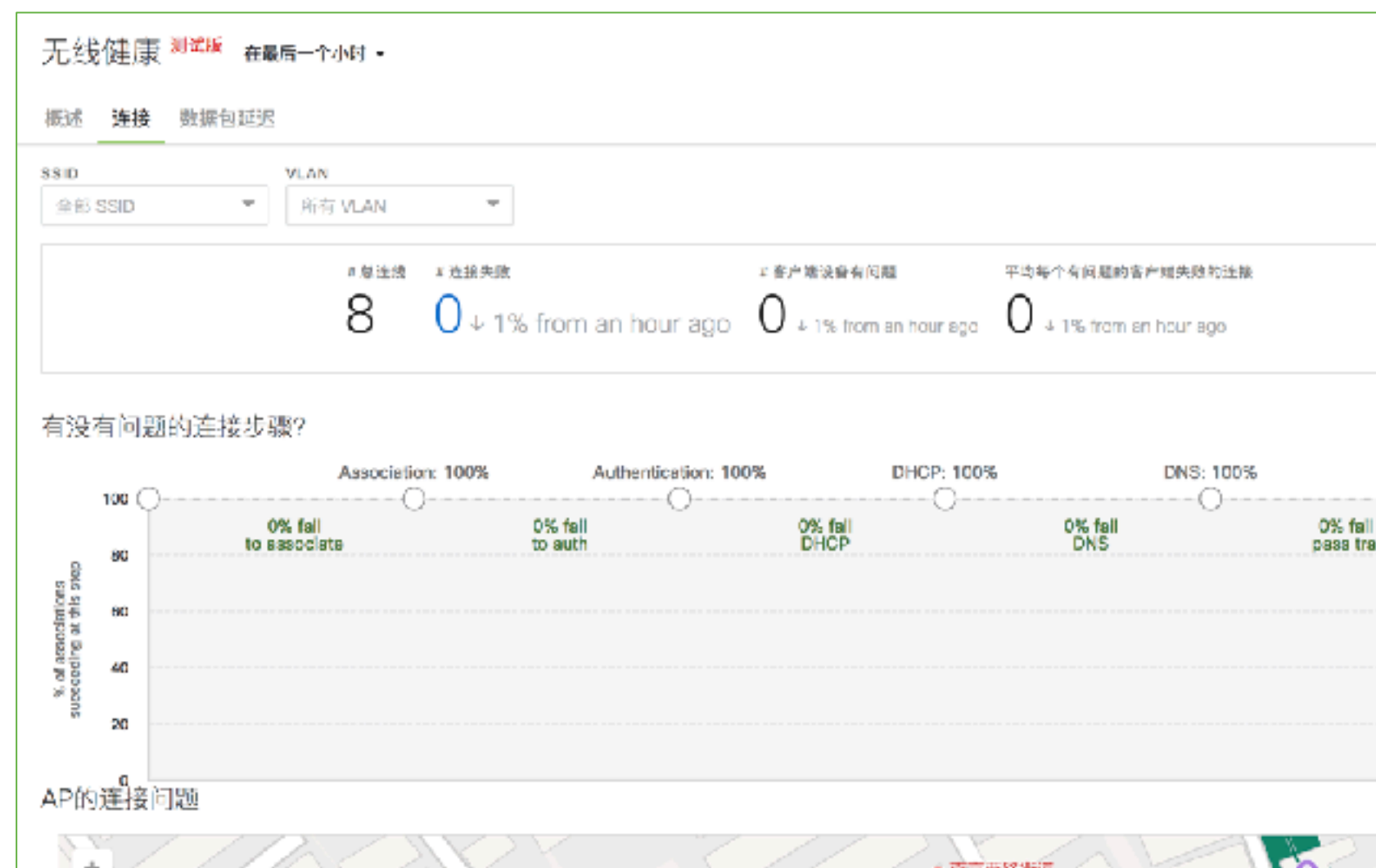
Successful HTTP Status: 200

```
{  
  "id": "k74272e",  
  "description": "Miles's phone",  
  "mdnsName": "Miles's phone",  
  "dhcpHostname": "MilesPhone",  
  "mac": "00:11:22:33:44:55",  
  "ip": "1.2.3.4",
```

故障排查

Troubleshooting

健康状况报表



排错工具

Ping: icmp.canireachthe.net | Ping 或 Ping appliance

重新启动设备: 重启设备

LED 闪烁: 运行

吞吐量: 运行

Traceroute: 上行链路 互联网 1 | icmp.canireachthe.net | 运行

MTR: icmp.canireachthe.net | 数字周期: 1 | 接口: 互联网 1 | 运行

DNS 查找: 主机名: canireachthe.net | DNS服务器: 9.9.9.9 | 运行

ARP 表: 运行

技术支持

Meraki Enterprise support hotline

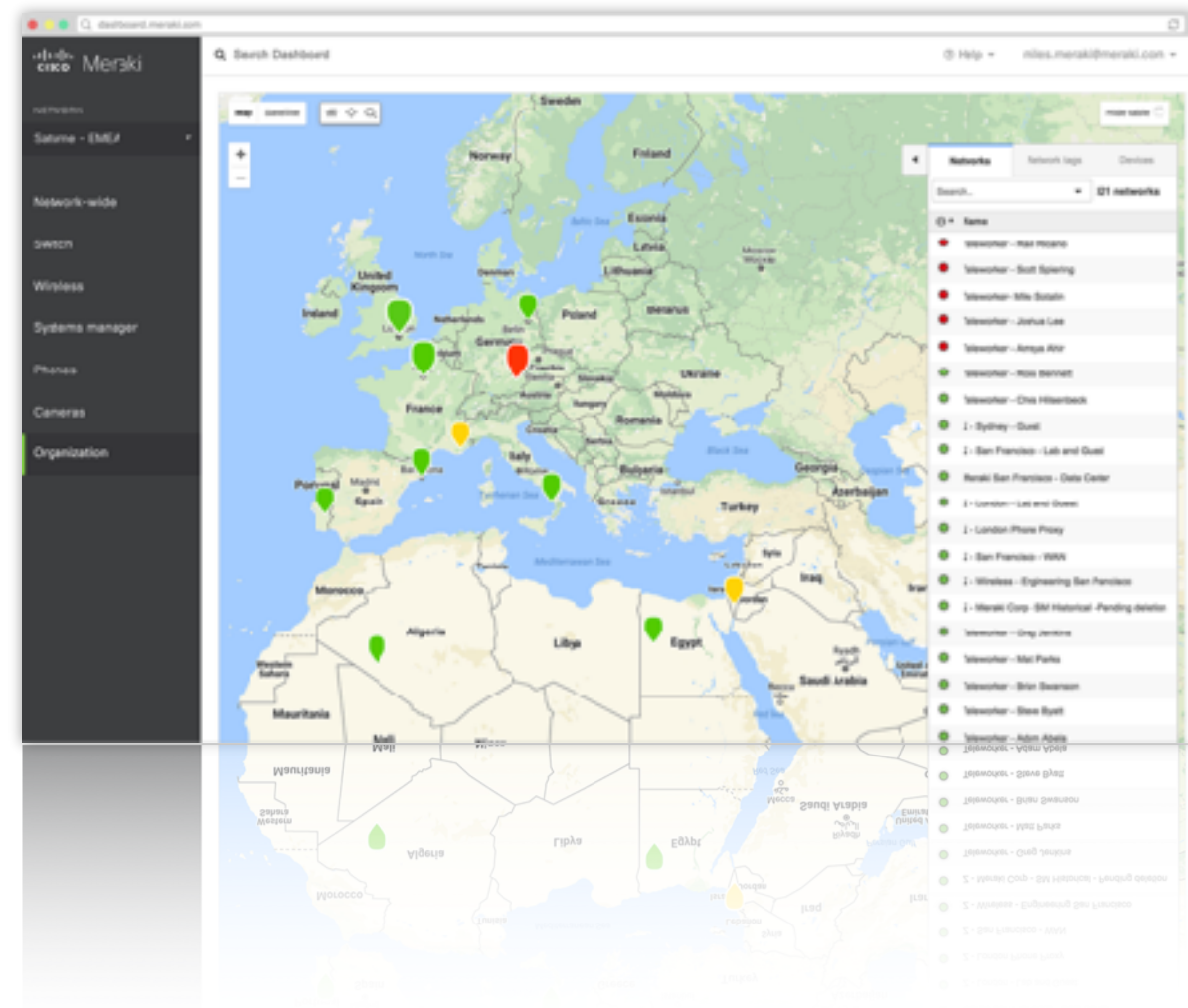
North America +1 415-937-6671
Europe +44 203 808 7003
Australia/Asia-Pacific +61 286078968

Argentina +54 1159844099
Brazil +55 6135500832
Chile +56 225 952 968
中国内地 ⓘ +86 400 605 7895

邮件支持

[提交案例](#)

全网SaaS IT管理



MR
无线 AP



MS
交换机



MX
SD-WAN 路由器



Systems
Manager*
统一终端管理



MI*
洞察

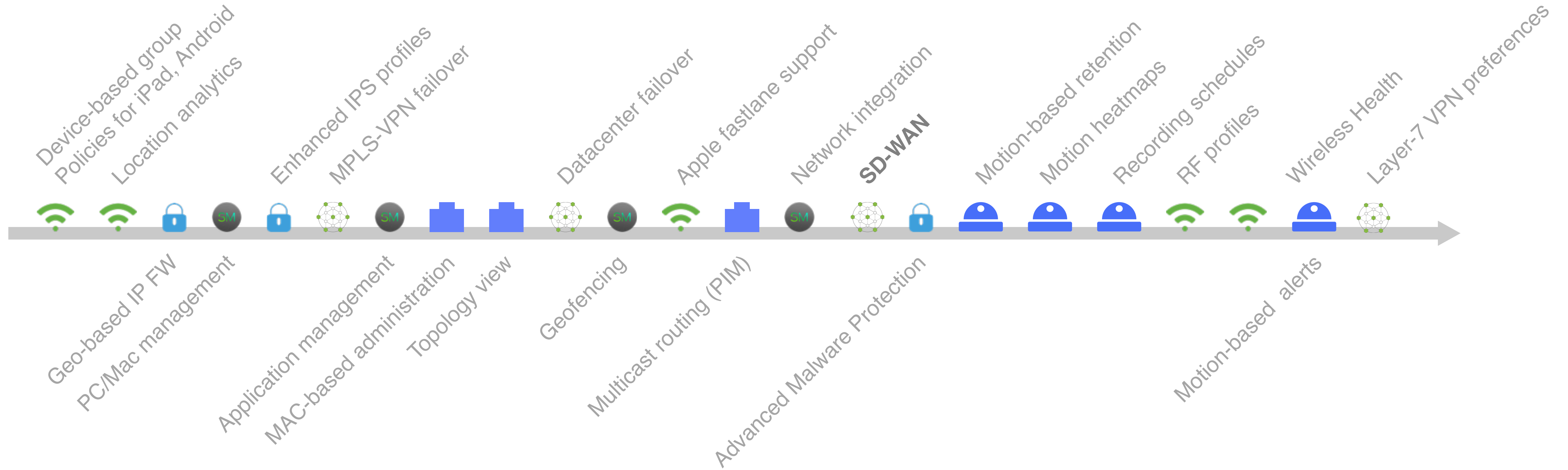


MV*
摄像头

* 尚未在中国开放

完整基于云技术的SaaS IT管理产品组合
单一管理窗口

投资保障



透过网站提供每季更新

精准的版本控制

SD-WAN Platform

硬件平台

Meraki MX 路由器

使用一个易于使用、易于扩充的平台，
以保障网络安全、连接世界。



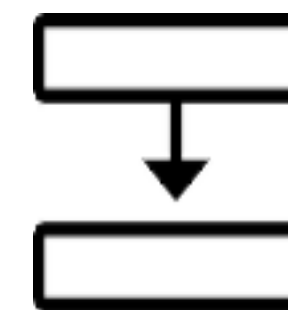
UTM 网络安全功能

下一代防火墙、入侵侦测、恶意软件防御、内容过滤、地理防火墙



连接功能

Site-to-Site VPN, SD-WAN, Non-Meraki Site-to-site VPN, Client VPN, 双上行端口、流量整形、易于扩充



冗余和备援

Warm Spare (HA), 上行线路冗余和负载均衡、3G/4G 无线备援

强悍的硬件平台

MX平台的硬件亮点

-  两个 WAN 端口
-  3G / 4G / LTE USB 作为唯一上行或备援线路
-  部分端口具备 PoE/PoE+ 功能
-  高可用性模式



MERAKI MX SD-WAN & SECURITY APPLIANCES

MX SD-WAN 路由器

Teleworker



Z3



Z3C

~5 users
802.11ac Wave 2 Wireless & PoE
FW throughput: 100 Mbps
CAT 3 LTE (**Z3C**)

Small Branch



MX64/65

~50 users
802.11ac Wireless* & PoE
FW throughput: 250 Mbps



MX67/68

~50 users
802.11ac Wave 2* & PoE
FW throughput: 450 Mbps



MX67C/68CW

~50 users
802.11ac Wave 2* & PoE
FW throughput: 450 Mbps
CAT 6 LTE

Medium Branch



MX84

~200 users
FW throughput: 500 Mbps



MX100

~500 users
FW throughput: 750 Mbps

Large Branch, Campus or Concentrator



MX250

~2,000 users
FW throughput: 4 Gbps



MX450

~10,000 users
FW throughput: 6 Gbps

Virtual



vMX100 for AWS & Azure

FW throughput: 750 Mbps
VPN & SD-WAN features

*Available with wireless models
(MX64W, MX65W, MX67W, MX68W, MX68CW)
Z3C not available in Japan, China

MX SD-WAN 路由器 小型分支系列



MX64/65

MX64W/65W

MX67/68

MX67W/68W

MX67C

MX68CW

Firewall Throughput	250 Mbps	250 Mbps	450 Mbps	450 Mbps	450 Mbps	450 Mbps
VPN Throughput	100 Mbps	100 Mbps	200 Mbps	200 Mbps	200 Mbps	200 Mbps
Wi-Fi	-	802.11ac	-	802.11ac Wave 2	-	802.11ac Wave 2
Embedded Cellular	-	-	-	-	CAT 6 LTE	CAT 6 LTE
Price	\$595/\$945	\$945/\$1,245	\$695/\$995	\$995/\$1,295	\$1,295	\$1,795

North America variant:

Bands 2, 4, 5, 12, 13, 17, and 29

Worldwide variant:

Bands 1, 3, 5, 7, 8, 20, 26, 28A, 28B, 34, 38, 39, 40, 41

Meraki 许可证



硬件

+



许可证

许可证

集中管理和全网范围的可视性与可控性

无缝的固件和安全更新

全天候企业支持和终身保修

1:1 比例的硬件和许可证

MX许可证



Enterprise License

完整的SD-WAN功能组

Site-to-site Auto VPN

企业分支路由

线路绑定和故障切换

应用流量控制

网页缓存

Client VPN

状态防火墙



Advanced Security License

所有Enterprise License的功能, 加上:

内容过滤

恶意软件防护 (AMP)

入侵侦测

基于地理位置的IP地址防火墙

[附注: HA模式下, 备机无需License]

Demo

Next Steps

下一步

开始销售Meraki SD-WAN



Meraki SD-WAN CVD

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_SD-WAN



Demo 资源

Meraki SD-WAN dCloud — Instant Demo

<https://dcloud.cisco.com>

找 Cisco Meraki SD-WAN v2, 有Cisco版和Partner版, 内容都一样, Cisco版用CCO登入, Parter版直接进入

Meraki Corp (Cisco Internal)

<https://dashboard.cisco.com>

思科员工使用CCO账号登入, 选择左上角 Meraki Corp, 目前悉尼和伦敦Finsbury办公室网络已启用SD-WAN



Meraki SD-WAN 销售工具 (Cisco Internal)

SalesConnect: <http://cs.co/meraki-sd-wan>

MerakiCorner: <http://cs.co/merakicorner>

Thank you



Meraki