cisco Meraki

# MX 选型指南

2018 年 9 月

本技术文档就如何根据实际部署、行业标准基准和详细功能说明选择适当的思科 Meraki 安全设备提供指导。

# 概述

思科 Meraki MX 安全设备属于统一威胁管理 (UTM) 产品。
UTM 产品不仅外形坚固、易于部署，而且提供多种安全功能。
鉴于任意特定 MX 中可部署的安全功能的数量有所不同，设备性能将因使用案例而异。
选择哪个 MX 型号的产品才适当取决于使用案例和部署特征。

**本技术指南旨在帮助回答下列问题：**

- 如何确定哪个 MX 型号能够满足需求？
- 应该打开哪些功能？
- MX 型号相较于竞争产品的优势何在？

## 选择适当的硬件

思科 Meraki MX 产品有 8 个产品系列。下表概要列出了各个 MX 产品系列提供的硬件特性：

| | MX64(W) | MX65(W) | MX67(W/C) | MX68(W/CW) | MX84 | MX100 | MX250 | MX450 |
|---|---|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |  |  |
| **双广域网链路** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **3G/4G 故障切换** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **可提供内置 LTE 调制解调器型号** | | | ✓ | ✓ | | | | |
| **可提供内置无线功能** | ✓ | ✓ | ✓ | ✓ | | | | |
| **可提供内置 PoE+ 型号** | | ✓ | | ✓ | | | | |
| **硬盘驱动器** | | | | | 1TB | 1TB | 128GB (SSD) | 128GB (SSD) |
| **光纤连接** | | | | | SFP | SFP | SFP、SFP+ | SFP、SFP+ |
| **双电源** | | | | | | | ✓ | ✓ |
| **外形规格** | 桌面版 | 桌面版 | 桌面版 | 桌面版 | 1U | 1U | 1U | 1U |


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

# 网络性能基准

行业标准基准旨在帮助您将 MX 安全设备与其他供应商的防火墙进行比较。这些测试的假定前提是测试环境具备最佳的网络条件和理想的流量模式。当测量特定功能的最大吞吐量时，所有其他功能都会被禁用。生产网络中的实际结果视具体情况而定。

| | MX64/65 系列 | MX67/68 系列 | MX84 | MX100 | MX250 | MX250 |
|---|---|---|---|---|---|---|
| **启用所有安全功能时的最大吞吐量** | 200 Mbps | 300 Mbps | 320 Mbps | 650 Mbps | 2 Gbps | 4 Gbps |
| **直通模式下的最大状态（第 3 层）防火墙吞吐量** | 250 Mbps | 450 Mbps | 500 Mbps | 750 Mbps | 4 Gbps | 6 Gbps |
| **NAT 模式下的最大状态（第 3 层）防火墙吞吐量** | 200 Mbps | 450 Mbps | 500 Mbps | 750 Mbps | 4 Gbps | 6 Gbps |
| **最大 VPN 吞吐量** | 100 Mbps | 200 Mbps | 250 Mbps | 500 Mbps | 1 Gbps | 2 Gbps |
| **最大并发 VPN 隧道数**[1]（站点间或客户端 VPN） | 50 | 50 | 100 | 250 | 3000 | 5,000 |
| **建议的最大并发 VPN 隧道数**[2]（站点间或客户端 VPN） | 50 | 50 | 100 | 250 | 1000 | 1500 |
| **最大 AMP 吞吐量** | 250 Mbps | 300 Mbps | 500 Mbps | 750 Mbps | 2 Gbps | 4 Gbps |
| **最大 IDS 吞吐量** | 200 Mbps | 300 Mbps | 320 Mbps | 650 Mbps | 2 Gbps | 4 Gbps |

MX 的 SD-WAN 功能集包含双活 VPN，可在所有可用上行链路上的对等体之间创建 VPN 隧道，以便最高效地利用可用广域网带宽。因此，两个对等体之间的连接最多可以包含四个隧道，具体取决于每个站点的 MX 上行链路数量。这一点应该在做出 VPN 选型决策时予以考虑。

[1] 最大并发 VPN 隧道数基于实验室测试场景，无客户端流量通过 VPN 隧道传输。

[2] 建议的并发 VPN 隧道数基于实验室测试场景，有通过 VPN 隧道传输的客户端流量。


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

# 功能、优势和性能影响

UTM 产品提供了各种安全和网络功能。为了在最大限度地保障安全的同时避免不必要的性能降级，了解这些功能的优势并在各个功能之间进行权衡至关重要。

| | 优势 | 性能影响 | 建议 |
|---|---|---|---|
| **恶意软件防护** | 根据从思科 AMP 云收到的性质阻止基于 HTTP 的申请下载。 | 高 | 考虑禁用访客 VLAN 并使用防火墙规则隔离这些 VLAN。如果您在主机设备上运行面向终端的 AMP 等全面的恶意软件防护客户端，也应该考虑将其禁用。 |
| **IDS/IPS** | 针对可疑网络流量提供警报/防护 | 高 | 考虑在低带宽网络中不通过 VPN 发送 IDS/IPS 系统日志数据。 |
| **VPN** | 加密两个位置之间的流量并确保安全 | 中 | 使用拆分隧道 VPN 并在边缘部署安全服务。 |
| **Web 缓存** | 通过本地缓存加速访问 Web 内容 | 中 | 适于在低带宽网络中重复、频繁地访问大量多媒体内容。不建议在高带宽网络中使用。请注意，YouTube 不支持 Web 缓存。 |
| **内容过滤（最大流量生成站点）** | 使用本地下载的数据库进行基于类别的 URL 过滤 | 低 | 如果您优先考虑的是速度而非涵盖范围，请选择此选项。 |
| **内容过滤（完整列表）** | 使用 Brightcloud.com 上托管的完整数据库进行基于类别的 URL 过滤 | 中 | 如果您优先考虑的是 100% 涵盖和安全，请选择此选项。Web 浏览速度最初会稍微变慢，但随着缓存的 URL 类别越来越多，速度也会越来越快。 |
| **Web 安全搜索** | 打开 Google/Bing 安全搜索选项 | 低 | 必须与“禁用加密搜索”选项一起部署才能生效。 |
| **阻止加密搜索** | 禁用通过 HTTPS（端口 443）的 Google/Bing 搜索，允许执行 Web 安全搜索 | 低 | 必须与“Web 安全搜索”一起部署才能生效。需要修改 DNS 设置，否则还会中断 Google Apps。有关详细信息，请查看 Meraki 知识库。 |


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

# 有关客户端的建议

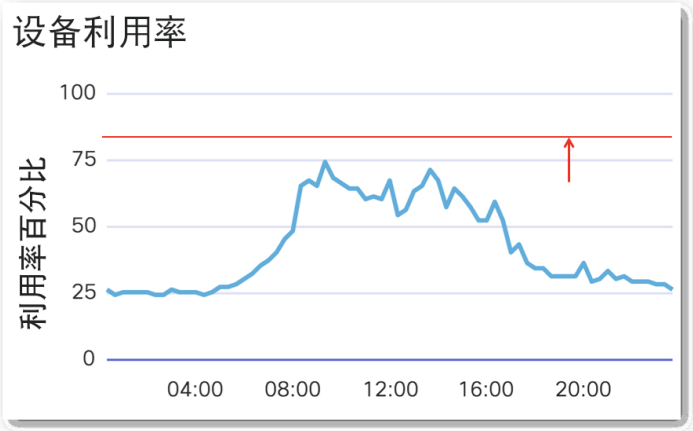
虽然对可以在 MX 安全设备下部署的客户端设备数量没有硬性限制，但在本文档中，所有已执行的测试均基于下表所示的客户端数量。如果超过这些客户端数量，可能会导致性能与本指南所含选型数据有所不同。

| 建议客户端设备数量 | | | | | | |
|---|---|---|---|---|---|---|
| | **MX64/65 系列** | **MX67/68 系列** | **MX84** | **MX100** | **MX250** | **MX450** |
| **建议客户端设备数量** | 50 | 50 | 200 | 500 | 2,000 | 10,000 |

# 内置 MX 设备利用率

本指南旨在帮助用户了解特定 MX 型号在启用某些功能时预期的利用率和负载水平。但是，为了准确地预测设备上的负载，必须在该设备的指定环境中和预期条件下对其进行测试。每一个网络中都存在大量可影响实际性能的变量，例如独特的流量组合和使用的功能。

MX 设备利用率工具可以帮助您更好地了解设备在不同时间的负载，并可用于评估利用率水平，以及是否需要更高端的设备或减少负载。如果 MX 设备在正常工作* 期间的利用率一直在 85% 以上，则应该考虑升级到吞吐量更高的型号或减少每台设备的负载。MX 设备利用率工具可以通过 API 使用，也可作为“摘要报告”页面中显示的图表使用。




## MX 设备利用率计算

向 Meraki 控制面板报告的设备利用率数据基于在一分钟时间内测量的负载平均值。返回的负载值是介于 1 到 100 之间的数值。值越低表示负载越低，值越高表示工作负载越繁重。目前，设备利用率值根据 MX 及其流量负载的 CPU 使用率计算。

由于取的是负载平均值，因此有可能出现发生瞬时负载高峰而利用率指标中反映不出来的情况。例如，一直显示为不到 85% 的设备负载仍有可能出现瞬时负载高峰。这些瞬时负载高峰可能会导致收到的超出设备转发容量的数据包被丢弃。

** 开启所有所需功能，连接预期数量的客户端，并且预期的流量组合流经设备。*


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

# 结论

虽然每个网络的流量模式都有独特之处，但本指南旨在重点介绍一些常见场景，帮助您为所在环境选择适当的思科 Meraki MX 产品。请考虑在选择防火墙时留出缓冲余地，为未来的增长做出规划（例如，如果您目前有 550 个用户，请选择支持 1000 个用户的 MX）。通过这种方式，您可以确保当额外的安全和网络功能可用时，即可继续启用这些功能。与此同时，鉴于 ISP 速度正在逐年增长，选择可为您提供长期服务的防火墙也非常重要。


Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com