



白皮书

思科 Meraki 自动 VPN

2013 年 7 月

本白皮书介绍自动 VPN（第 3 层站点间 IPsec）功能，以及如何在思科 Meraki 安全设备之间部署该功能。

目录

简介	3
思科 MERAKI 解决方案	4
相关详细信息	8

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。

简介

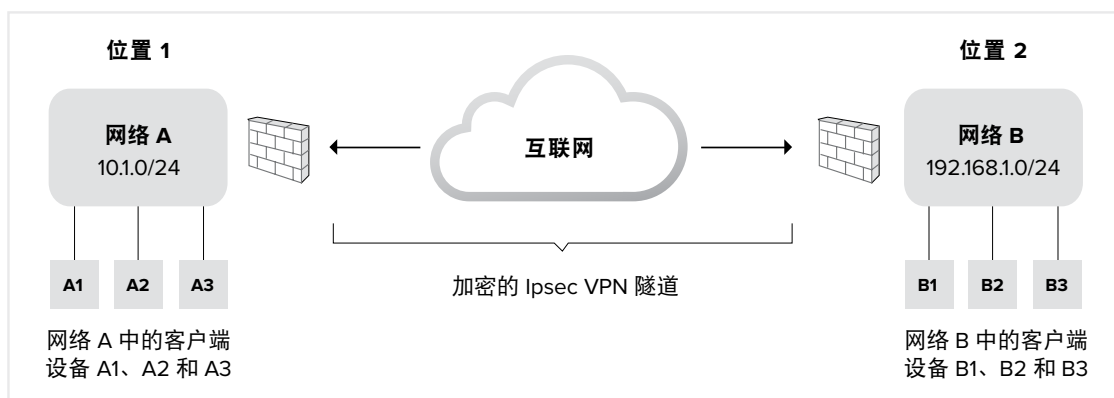
VPN 是什么？

希望为远程员工提供核心网络资源的虚拟现场访问权限或者希望将分支机构连接到核心网络的大多数组织都使用虚拟专用网 (VPN)。VPN 是加密隧道，可以通过不安全的公共基础设施（通常是互联网）进行安全、保密的数据传输。

站点间 VPN 是什么？

站点间 VPN 是一种最常用的 VPN 实施，在这种实施中，托管网络资源的一个位置通过 VPN 安全地连接到另一个位置（此处可能也托管着资源）；通常，这两个位置属于同一个组织。

下图显示的就是一个站点间 VPN：



站点间 VPN 部署在每个位置的安全设备/防火墙之间。位于这些防火墙之后的客户端设备（例如笔记本电脑或工作站）不需要安装软件或配置本地设置即可与对方站点发送或接收数据。

在**网络**站点间 VPN（也称为“分支到分支”）中，组织的各个网络全部都通过 VPN 彼此连接。在**中心辐射型**拓扑中，所有卫星分支机构网络（“分支”）通过 VPN 隧道连接回中心办公室（“中心”）；分支彼此间不会直接交换数据。

为什么 VPN 难以部署？

使用传统架构时，随着分布式站点数量的增加，多站点 VPN 的配置和管理复杂性之高令人望而却步。这是因为每个 VPN 隧道的两端都需要进行手动创建和调整，而且这些操作通常需要通过复杂的命令行界面来完成。这是一个既耗时又容易出错的过程：需要为每个隧道手动指定和配置两次变量，例如两个安全设备接口的 IP 地址、预共享密钥或证书、身份验证和加密协议、可导出的子网列表等。试想：如果主要广域网上行链路故障切换至 3G/4G 链路且 VPN 的外部 IP 地址变更，则需要为新地址重新确定上述所有设置才能恢复 VPN 功能。

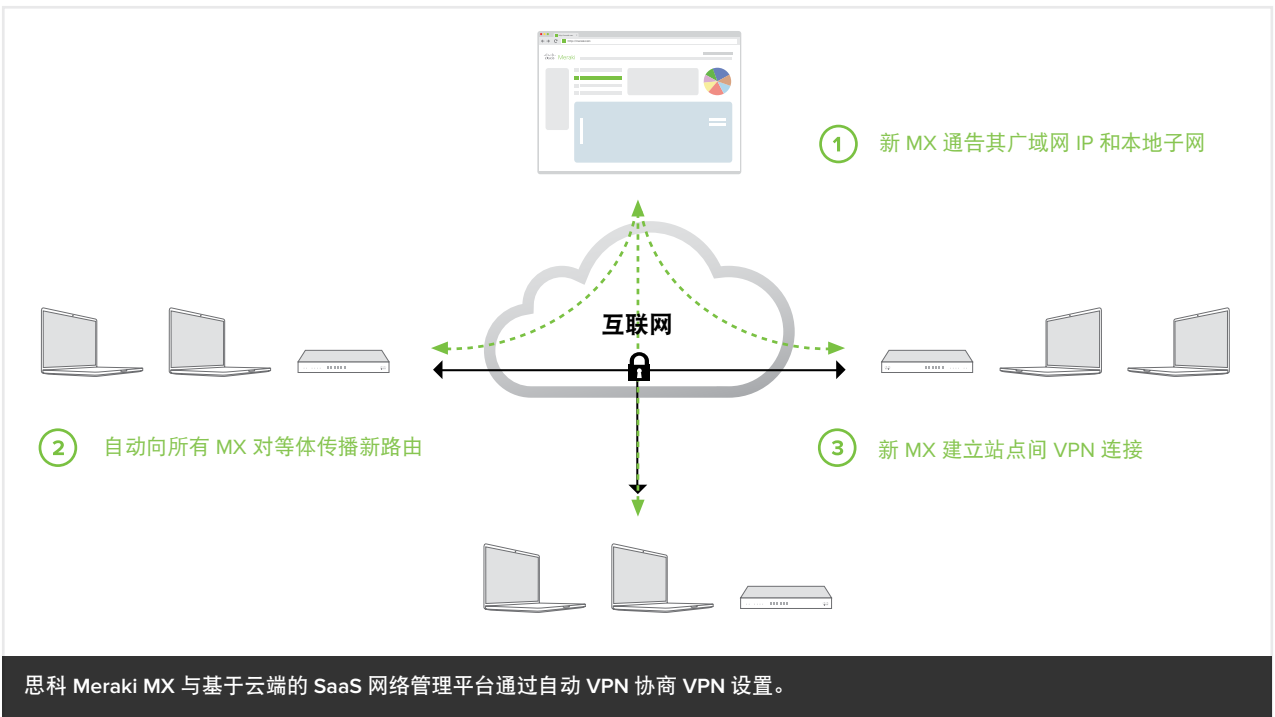
思科 MERAKI 解决方案

自动 VPN：快速轻松的设置

思科 Meraki MX 是一款基于云的安全设备，具有完全集成的网络和安全功能，例如企业级状态防火墙、深入的第 7 层应用可视性与可控性、广域网优化、符合 CIPA 标准的内容过滤等。此外，所有 MX 型号都支持自动 VPN 功能，只需在思科 Meraki 控制面板中点击两次即可配置站点间第 3 层 IPsec VPN，将一项耗时的工作压缩到仅仅几分钟之内。

要启用自动 VPN，思科基于云端的 SaaS 网络管理平台将用作组织中的 MX 之间的唯一代理，协商 VPN 路由、身份验证和加密协议，而密钥会自动交换。其过程如下所示：

- 1. MX 向思科基于云端的 SaaS 网络管理平台通告自己的广域网 IP 地址和任何活动的 NAT 穿越 UDP 端口。**设备到基于云端的 SaaS 网络管理平台的通信会加密两次：通过 Meraki 专有加密算法加密一次，使用 SSL 再加密一次。
- 2. 思科基于云端的 SaaS 网络管理平台收到 MX 通告和公共 IP 地址。**控制面板从 MX 收到广域网 IP 和 NAT 穿越信息，以及它们的公共 IP 地址（如果 MX 位于 NAT 设备之后，则该地址与其广域网 IP 不同）。
- 3. 基于云端的 SaaS 网络管理平台维护一个用于跟踪组织中所有 MX 的动态表。**对组织中的每台 MX，它都会跟踪其广域网 IP 地址、公共 IP 地址、NAT 穿越端口和本地子网。当新的 MX 联机时，其信息会添加到此表中。
- 4. 选择适当的 IP 地址。**对每台 MX，基于云端的 SaaS 网络管理平台决定使用其广域网 IP 还是公共 IP 地址来建立安全的 VPN 隧道。它会尽可能使用 MX 的广域网 IP 地址；这可以在对等 MX 之间提供较短的 VPN 路径（例如，当多个 VPN 对等体通过 MPLS 连接到主数据中心并在那里连接到外部的互联网时）。
- 5. 协商 VPN 隧道。**思科基于云端的 SaaS 网络管理平台已经知道每台 MX 的 VLAN 和子网信息，现在是用于创建隧道的 IP 地址。基于云端的 SaaS 网络管理平台与 MX 确定 16 个字符的预共享密钥（每个组织一个密钥），并建立一个 128 位 AES 加密的 IPsec 隧道。通过 VPN 导出 IT 管理员在控制面板中指定的本地子网。
- 6. 将 VPN 路由从控制面板推送至 MX。**最后，控制面板会将 VPN 对等体信息（例如导出的子网、隧道 IP 信息）动态推送至每台 MX。每台 MX 将此信息存储在单独的静态路由表中。



自动 VPN 以这种独特的智能方式利用基于云端的 SaaS 网络管理平台，意味着 IT 管理员在站点间设置 VPN 隧道所需的手动配置和时间都更少，在此过程中引入人为错误的机会也就更少。

内置和可配置的站点间 VPN 冗余

无法使用 VPN 功能会让员工无法查收邮件、访问文件共享、安全地发送数据或使用 VoIP 电话等，让工作效率猛地陷入停滞。为了防止这种情况，自动 VPN 功能利用基于云端的 SaaS 网络管理平台来提供内置冗余。例如，如果您的 MX 有两条互联网上行链路，当为 VPN 流量服务的主上行链路发生故障时，另一条上行链路将进入主用状态，该链路的所有站点间 VPN 隧道将立即通过基于云端的 SaaS 网络管理平台重新协商。这意味着，当主用链路故障切换至备用链路（比如切换至 3G/4G 上行链路，导致 MX 公共 VPN IP 地址更改）时，自动 VPN 将自行修复。自行修复适用于自动 VPN 可用的网格和中心辐射型 VPN 拓扑。

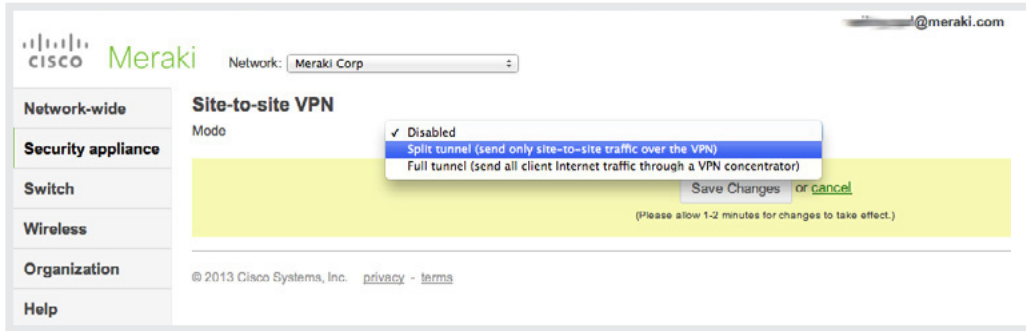
此外，如果要防止整个安全设备发生故障的罕见情况，您可以将一台 Meraki MX 安全设备配置为主 VPN 集中器，并将一台辅助的已启动（“热”）MX 准备好，随时可在第一台 MX 发生故障时接管。

配置热备份非常简单：将两台 MX 都放在网络边界之内并配置为 VPN 集中器。为每台 MX 分配单独的 IP 地址使其可以与基于云端的 SaaS 网络管理平台通信，但它们也共享同一个虚拟 IP (vIP)。此公共虚拟地址将接收所有 VPN 流量，在默认情况下，主集中器将对该流量做出响应。但是，如果主 MX 发生故障，热备份设备可以立即介入处理 VPN 流量（故障检测和完整的故障切换所需时间不到 30 秒）。无需手动更改 IP 地址即可将流量定向至热备份设备，因为它与主 MX 共享 vIP。

如何配置思科 Meraki 自动 VPN

要在 MX 安全设备之间启用站点间 VPN，只需登录思科 Meraki 控制面板，然后导航至“配置”>“站点间 VPN”页面。

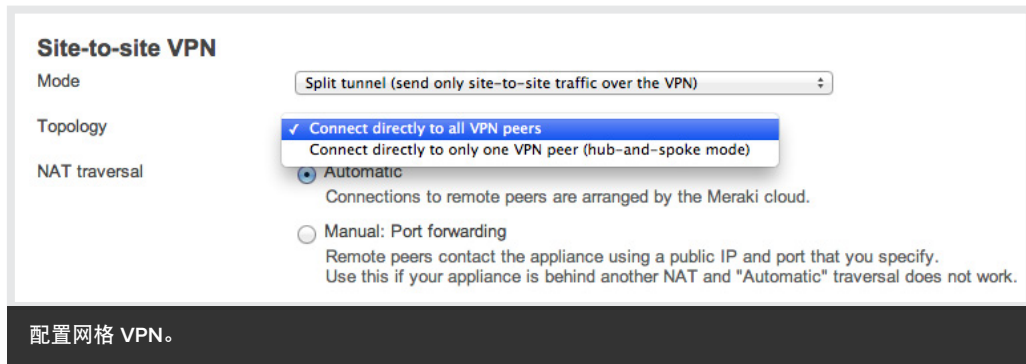
1. 通过选择您需要的是分割隧道 VPN 还是全隧道 VPN 来启用自动 VPN:



分割隧道模式只通过 VPN 发送站点间流量，将其他流量（例如直接互联网请求）定向至其最终目的地而无需通过安全 VPN 隧道。换言之，两个分支机构之间的邮件或文件服务器请求会经过分割隧道 VPN；用户查看网站（例如 www.nytimes.com）的请求不会经过。

全隧道模式通过安全 VPN 隧道定向所有流量。因此，即使是用户查看网页的请求也会被加密并通过 VPN 先发送到集中器。

2. 决定 VPN 拓扑是网格还是中心辐射型:



如果配置网格拓扑，请确保加入的每台 MX 都选择了“直接连接到所有对等体”选项。如果配置中心辐射型拓扑，请确保将中心 MX 配置为辐射状连接所有对等体，而将每个分支机构（“分支”）MX 配置为“仅直接连接到一个 VPN 对等体（中心辐射模式）”：



Site-to-site VPN

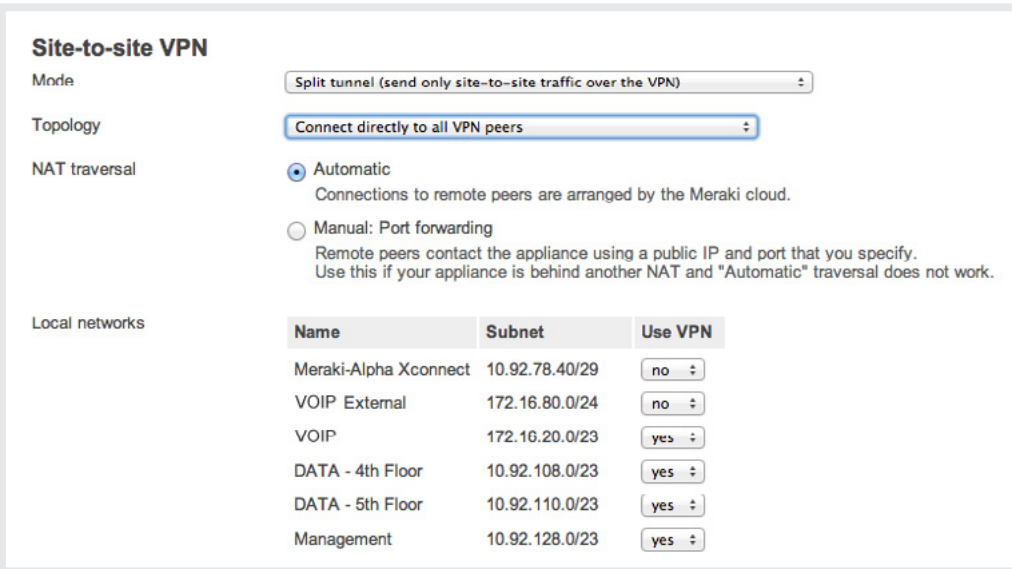
Mode: Split tunnel (send only site-to-site traffic over the VPN)

Topology: Connect directly to all VPN peers
 Connect directly to only one VPN peer (hub-and-spoke mode)

NAT traversal: Automatic
Connections to remote peers are arranged by the Meraki cloud.
 Manual: Port forwarding
Remote peers contact the appliance using a public IP and port that you specify. Use this if your appliance is behind another NAT and "Automatic" traversal does not work.

中心辐射型拓扑中配置的远程员工站点，通过隧道连接回“Meraki 公司设备”中心 MX。

3. 选择要通过 VPN 导出的子网（本地网络）：



Site-to-site VPN

Mode: Split tunnel (send only site-to-site traffic over the VPN)

Topology: Connect directly to all VPN peers

NAT traversal: Automatic
Connections to remote peers are arranged by the Meraki cloud.
 Manual: Port forwarding
Remote peers contact the appliance using a public IP and port that you specify. Use this if your appliance is behind another NAT and "Automatic" traversal does not work.

Local networks

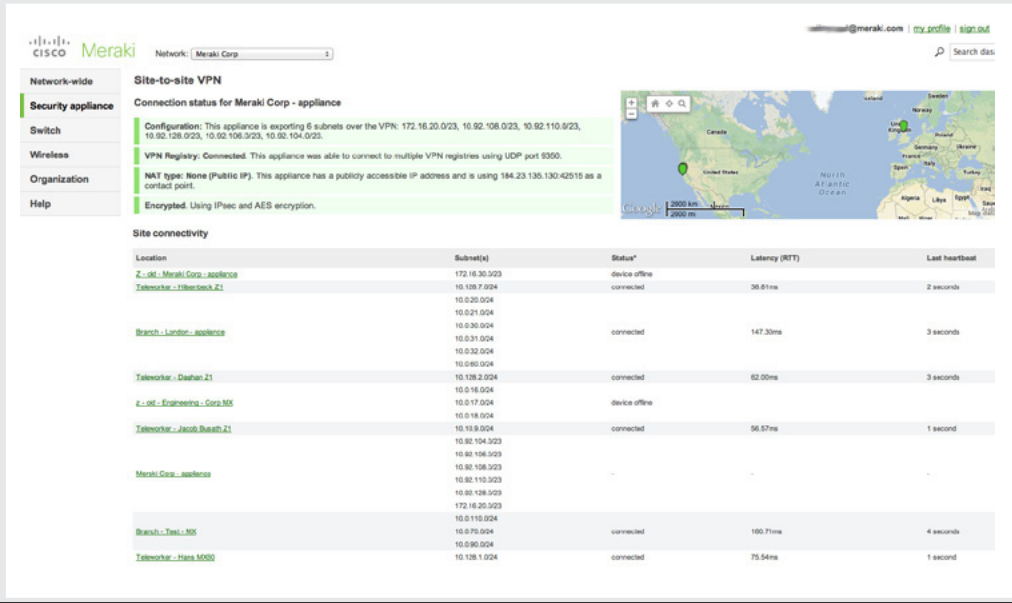
Name	Subnet	Use VPN
Meraki-Alpha Xconnect	10.92.78.40/29	no
VOIP External	172.16.80.0/24	no
VOIP	172.16.20.0/23	yes
DATA - 4th Floor	10.92.108.0/23	yes
DATA - 5th Floor	10.92.110.0/23	yes
Management	10.92.128.0/23	yes

选择“是”或“否”通过站点间 VPN 导出本地子网。

4. 点击控制面板中的“保存”

就这么简单！您现在已经配置了一个采用网格或中心辐射型拓扑的分割隧道 VPN 或全隧道 VPN。

如果要检查您的网络中所有 VPN 对等体 MX（或 Z1 远程员工网关设备，它也支持自动 VPN）的状态，从思科 Meraki 控制面板中的“监视工具” >> “VPN 状态”页面中即可轻松完成此操作。系统将显示每台 MX 或 Z1 的状态，及其导出的子网；每隔几秒钟，系统会检查一次每个对等体的延迟和连接，提供接近实时的视图。



The screenshot displays the Meraki VPN Status page for Meraki Corp. It includes a navigation menu on the left with options like Network-wide, Security appliance, Switch, Wireless, Organization, and Help. The main content area shows the 'Site-to-site VPN' connection status for Meraki Corp - appliance, including configuration details, VPN Registry status, NAT type, and encryption. A map shows the location of the appliance. Below the map is a table titled 'Site connectivity' with columns for Location, Subnet(s), Status*, Latency (RTT), and Last heartbeat.

Location	Subnet(s)	Status*	Latency (RTT)	Last heartbeat
Z_01_Meraki_Corp_appliance	172.16.20.0/23	device offline		
Teleworker - Hitechack Z1	10.128.7.0/24 10.0.20.0/24 10.0.21.0/24 10.0.30.0/24	connected	30.61ms	2 seconds
Branch - London - appliance	10.0.21.0/24 10.0.30.0/24 10.0.32.0/24 10.0.40.0/24	connected	147.30ms	3 seconds
Teleworker - Dasha Z1	10.128.2.0/24 10.0.18.0/24	connected	82.00ms	3 seconds
Z_01_Engineering - Corp MX	10.0.17.0/24 10.0.18.0/24	device offline		
Teleworker - Jacob Buech Z1	10.18.0/24 10.32.104.0/23 10.88.106.0/23	connected	56.57ms	1 second
Meraki_Corp_appliance	10.88.106.0/23 10.82.110.0/23 10.88.126.0/23 172.16.20.0/23			
Branch - Test_355	10.0.110.0/24 10.0.90.0/24	connected	180.71ms	4 seconds
Teleworker - Hans M500	10.128.1.0/24	connected	75.54ms	1 second

在思科 Meraki 控制面板中实时查看 VPN 状态。

相关详细信息

简而言之，思科 Meraki MX 让远程办公室之间的站点间 VPN 创建和维护过程变得简单而直观。我们将基于云端的 SaaS 网络管理平台用于自动 VPN 的独特方法还可以提供内置冗余以及从任何可访问互联网的位置管理 VPN 网络的能力。所有 MX 安全设备均配备自动 VPN 功能，无需另行付费。

所有思科 Meraki MX 型号均可进行免费评估 (meraki.cisco.com/eval)，其他相关信息请访问此处：

meraki.cisco.com/library (VPN 冗余白皮书和 MX 产品手册等)

meraki.cisco.com/blog (有关自动 VPN、MX 功能等的博客)

您也可以在 youtube.com 上搜索 MX 自动 VPN 视频