



白皮书

VPN 集中器冗余

2013 年 1 月

本解决方案指南介绍如何部署一对“单臂”集中器模式的冗余 VPN 集中器。

目录

1 简介	3
2 高可用性概述	3
2.1 正常运行	
2.2 故障检测	
2.3 故障恢复至原来的主集中器	
2.4 故障恢复延迟	
3 支持的配置	4
3.1 前提条件	
3.2 连接“单臂”VPN集中器模式的MX	
3.3 路由配置	
4 配置集中器对	5
4.1 设置主（主用）集中器	
4.2 设置热备份（备用）集中器	
5 常见问题解答	6
6 结论	6

1. 简介

Meraki 自动 VPN 可以显著节省分布式网络的运营成本。本文概要介绍如何基于 VRRP 协议使用一对主/热备份 MX 实现高可用性 (HA)，从而最大限度缩短硬件出现故障时的停机时间。最开始，该高可用性对将限制为“单臂”VPN 集中器模式。将来的版本中将去除此限制。

2. 高可用性概述

2.1 正常运行

在正常运行期间，数据中心内有两台 MX 设备，都部署为“单臂”VPN 集中器。主用 VPN 集中器称为“主”集中器，备用集中器称为“热备份”集中器。每个集中器都有自己的 IP 地址，用于与基于云的集中管理服务交换管理流量。不过，集中器还共享一个“虚拟 IP 地址”。

2.1.1 虚拟 IP

虚拟 IP 地址 (VIP) 是主 VPN 集中器和热备份 VPN 集中器共享的 IP 地址。VPN 流量发送到 VIP 而非各集中器的物理 IP 地址。主集中器和热备份集中器使用 VRRP 协议进行同步，并选择主用集中器处理 VPN 流量。

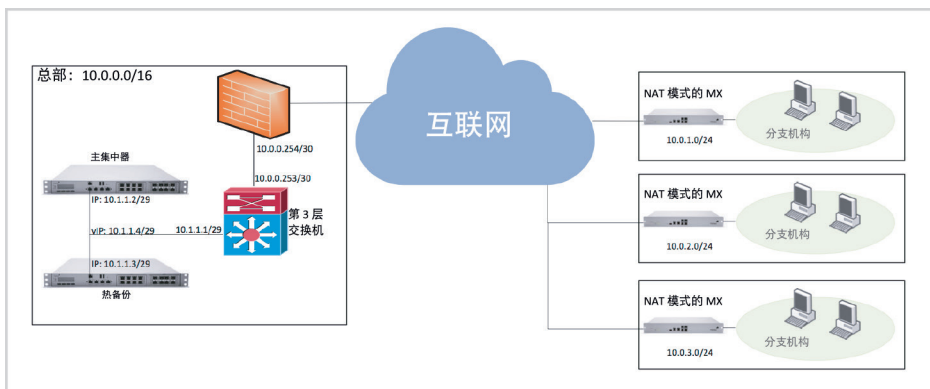


图 1: 数据中心内的冗余 VPN 集中器对。

2.2 故障检测

主/热备份集中器通过其连接的局域网使用 VRRP 协议共享运行状态信息。换言之，故障检测不需要依赖与互联网/Meraki 控制面板的连接。检测到故障时，热备份集中器将承担主集中器的角色，直到原来的主集中器重新上线。

2.3 故障恢复至原来的主集中器

原来的主 VPN 集中器重新上线并通过 VRRP 协议开始通告其运行状态后，热备份集中器会将 VPN 集中器功能交还原来的主集中器。

2.4 故障恢复延迟

从检测到故障到故障切换至热备份集中器并能开始处理 VPN 数据包，总时间通常不到 30 秒。

3. 支持的配置

冗余 VPN 集中器功能需要在总部或数据中心内配置“单臂”VPN 集中器模式的 MX 安全设备。

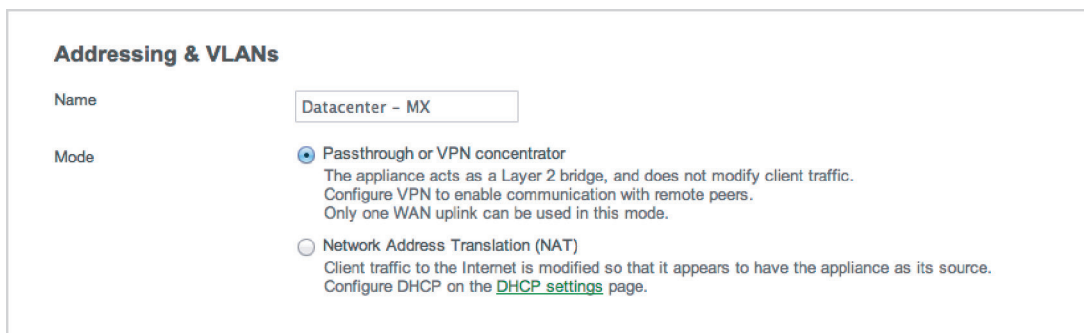


图 2: Meraki 控制面板中的直通或单臂 VPN 集中器模式选择器。

3.1 前提条件

- 每台 MX 设备都需要许可证（有关详细信息，请参阅常见问题解答部分）。
- 两台 MX 设备必须位于同一个第 2 层广播域中。
- 两台 MX 设备必须能够与基于云端的 SaaS 网络管理平台管理服务通信（即，有权访问互联网）。
- 两台 MX 设备必须按照“单臂”VPN 集中器连接。

3.2 连接“单臂”VPN 集中器模式的 MX

在单臂 VPN 集中器模式下，MX 对仅通过其各自的互联网端口连接。仅 VPN 流量被路由到 MX，而且入口和出口数据包通过同一个接口发送。

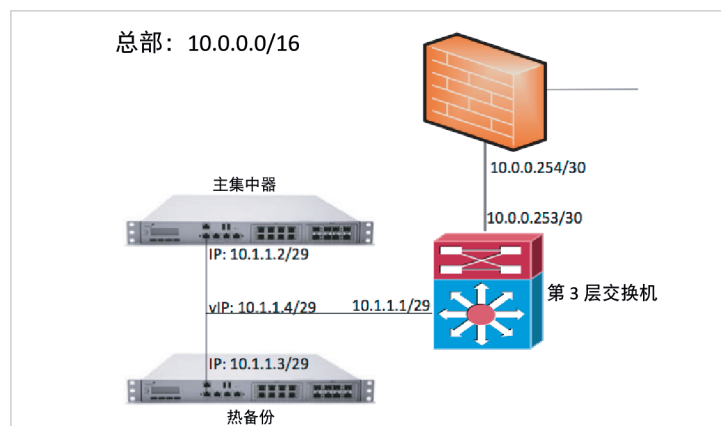


图 3: “单臂”VPN 集中器对

3.3 路由配置

要通过 VPN 隧道发送流量，必须在第 3 层交换机上添加新路由。以下是上面的网络图的思科 IOS 命令示例，假设 10.0.1.0/24、10.0.2.0/24 和 10.0.3.0/24 是分支机构网络的路由：

```
ip route 10.0.1.0 255.255.255.0 10.1.1.4
ip route 10.0.2.0 255.255.255.0 10.1.1.4
ip route 10.0.3.0 255.255.255.0 10.1.1.4
```

请注意，10.1.1.4 是主/热备份 MX 对的虚拟 IP (vIP)。有关为主/热备份对设置虚拟 IP 的信息，请参阅第 4.2 节。

4. 配置集中器对

4.1 设置主 (主用) 集中器

创建一个新网络，然后输入 MX 的序列号。请务必将该设备设置为直通或 VPN 集中器模式。

4.2 设置热备份 (备用) 集中器

1. 在控制面板中点击配置 > 热备份。
2. 输入热备份 MX 设备的序列号或订单编号。
3. 为主/热备份 MX 对分配虚拟 IP。

4.2.1 虚拟 IP 要求：

- 虚拟 IP 必须位于同一子网/VLAN 范围内。
- 虚拟 IP 必须是唯一的。具体而言，它不能与主集中器或热备份集中器的物理 IP 地址相同。

示例

在上例中 (请参阅图 1)，如果主集中器 IP 地址为 10.1.1.2/29，热备份集中器 IP 地址为 10.1.1.3/29，则 10.1.1.4/29 是有效的虚拟 IP 地址，因为它没有被任何其他设备使用。

The screenshot shows the Meraki dashboard interface. At the top left is the Meraki logo. The top right has links for 'my profile' and 'sign out'. Below the logo is a navigation sidebar with categories: Monitor, Configure (selected), and Organization. Under 'Configure', there are sub-items: Addressing & VLANs, DHCP, Firewall, Site-to-site VPN, Client VPN, Active Directory, Traffic shaping, Security filtering, Content filtering, Warm spare (highlighted), Alerts & administration, and Help. The main content area is titled 'Warm spare' and contains the following elements: a 'Network: Central DC' dropdown menu, a search bar labeled 'Search dashboard', a heading 'Warm spare' with a help icon, a paragraph 'To configure a warm spare, enter the serial number or order number of an appliance to add to this network.', an input field for 'Device serial or order number', a paragraph 'Enter the virtual IP to assign to the primary MX and warm spare.', an input field for 'Virtual IP', and an 'Add warm spare' button. At the bottom, there is a footer with copyright information '© 2012 Meraki, Inc.', links for 'privacy' and 'terms', login information 'Last login: about 1 month ago from 1.2.3.4 (San Francisco, CA)', and buttons for 'I wish this page would...' and 'make a wish'.

5. 常见问题解答

问 如果 MX 部署为 NAT 模式，如何设置 HA？

答 有关配置 NAT 模式高可用性的详细信息，请参阅[热备份文档](#)的 NAT 热备份部分。

问 两台 MX 必须是同一个型号吗？

答 虽然这不是强制要求，但建议采用相同型号。出于预算的原因，有些客户可能会选择使用性能/成本较低的 MX 作为辅助集中器。但是，确保辅助 MX 有足够的网络能力在故障切换期间处理 VPN/广域网优化流量非常重要。

问 热备份设备需要许可证吗？

答 不需要，运行热备份对只需要一个许可证。

问 系统检测到主设备的故障并故障切换至热备份设备需要多长时间？

答 故障切换时间通常不到 30 秒。

问 如果主设备重新上线，会发生什么情况？

答 它会立即承担主 VPN 集中器的功能。

问 现有连接（例如 VoIP 呼叫）会中断吗？

答 会，故障切换期间将出现短暂的中断，通常不到 30 秒。

问 可以将热备份设备放在灾难恢复 (DR) 辅助数据中心内吗？

答 只要两个数据中心都通过可以跨两个数据中心之间的单个子网/广播域的第 2 层连接进行连接，就可以将主设备和热备份设备放在位于不同地理位置的数据中心内。

6. 结论

MX 产品系列现在可使用行业标准的 VRRP 协议为大规模 VPN/广域网优化部署提供易于配置和完全自动化的冗余功能。其他文档和安装说明位于：<http://docs.meraki.com/mx>