



TECHDOCS

ION 9000 硬件参考

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2020-2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

September 3, 2021

Table of Contents

| | |
|---------------------------|-----------|
| 准备工作..... | 5 |
| 防篡改声明..... | 6 |
| 第三方组件支持..... | 7 |
| 产品安全警告..... | 8 |
| ION 9000 概述..... | 11 |
| ION 9000..... | 12 |
| ION 9000 端口..... | 13 |
| ION 9000 前面板及 LED..... | 14 |
| ION 9000 规格..... | 15 |
| ION 设备合规声明..... | 17 |
| ION 9000 安装包组件..... | 18 |
| 开启 ION 9000..... | 19 |
| 关闭 ION 9000..... | 19 |
| 重新启动 ION 9000..... | 19 |
| 安装 ION 9000..... | 21 |
| 机架式安装 ION 9000..... | 22 |
| 在虚拟路径内配置下安装 ION 9000..... | 27 |
| 配置控制器端口..... | 27 |
| 配置对等端口..... | 28 |
| 配置 Internet 端口..... | 28 |
| 在高可用性环境下安装 ION 9000..... | 30 |

准备工作

安装或维修 Palo Alto Networks® 新一代防火墙或设备前，必须了解以下主题。以下主题适用于所有 Palo Alto Networks 防火墙和设备，另有说明的除外。

- [防篡改声明](#)
- [第三方组件支持](#)
- [产品安全警告](#)

防篡改声明

为确保从 **Palo Alto Networks** 购买的产品未在装运时被篡改，请在收到产品后验证以下内容：

- 在您订购产品时，通过电子方式提供给您跟踪编号与在包装盒或包装箱上实际标记的跟踪编号一致。
- 不得破坏用于密封包装盒或包装箱的防篡改胶带的完整性。
- 不得破坏防火墙或设备上保修标签的完整性。

第三方组件支持

必须先阅读 [Palo Alto Networks 第三方组件支持](#) 声明，然后才能考虑安装第三方硬件。

产品安全警告

安装或维修 Palo Alto Networks 硬件之前，必须先阅读并了解以下警告，避免造成您自己和他人受伤或死亡，以及损坏您的硬件。此外，您还必须阅读硬件参考指南中列出的警告信息，了解可能存在的危险。



带基于激光的光学接口的所有 Palo Alto Networks 产品均满足 21 CFR 1040.10 和 1040.11 要求。

以下安全警告适用于所有 Palo Alto Networks 防火墙和设备，硬件型号特别指定的除外。

- 如果 Palo Alto Networks 防火墙或设备的硬件组件存在裸露电路，在安装或维修时，必须戴上防静电防电带。搬运组件之前，务必让腕带上的金属触点接触到您的皮肤，且腕带的另一端接地。

法语翻译：Lorsque vous installez ou que vous intervenez sur un composant matériel de pare-feu ou de dispositif Palo Alto Networks qui présente des circuits exposés, veillez à porter un bracelet antistatique. Avant de manipuler le composant, vérifiez que le contact métallique du bracelet antistatique est en contact avec votre peau et que l'autre extrémité du bracelet est raccordée à la terre.

- 使用接地屏蔽以太网电缆（如果适用）确保经销商符合电磁兼容性 (EMC) 标准。

法语翻译：Des câbles Ethernet blindés reliés à la terre doivent être utilisés pour garantir la conformité de l'organisme aux émissions électromagnétiques (CEM).

- （仅限 ION 7000 和 ION 9000）建议至少需要两个人来执行较重防火墙的拆包、搬运和重新放置等操作。
- 不得连接超出防火墙或设备输入范围的电源电压。有关电气范围的详细信息，请参阅防火墙或设备电气规格。

法语翻译：Veillez à ce que la tension d'alimentation ne dépasse pas la plage d'entrée du pare-feu ou du dispositif. Pour plus d'informations sur la mesure électrique, consulter la rubrique des caractéristiques électriques dans la documentation de votre matériel de pare-feu ou votre dispositif.

- WAN 和 LAN 以太网端口适用于与其他本地设备以太网端口互连。这些端口不是为直接连接到公共交换电话网络 (PSTN) 端口或接口而设计的。此外，铜基 WAN 端口、LAN 端口和铜基模块化收发器不适用于连接到户外电信 (OSP) 布线网络。
- （仅限具有可维修电池的设备）更换电池的型号必须与原电池相同，否则，更换电池可能发生爆炸。废弃电池须遵循当地法规进行处理。

法语译文：Ne remplacez pas la batterie par une batterie de type non adapté, cette dernière risquerait d'exploser. Mettez au rebut les batteries usagées conformément aux instructions.

- I/O 端口仅适用于构建内部连接，不适用于构建 OSP（外部设备）连接或任何受外部电压浪涌事件影响的网络连接。

•



（具有两个或多个电源的所有 Palo Alto Networks 设备）

小心：电击危险

从电源输入端断开所有电源线（交流或直流），让硬件完全断电。

法语译文：(Tous les appareils Palo Alto Networks avec au moins deux sources d'alimentation) Débranchez tous les cordons d'alimentation (c.a. ou c.c.) des entrées d'alimentation et mettez le matériel hors tension.

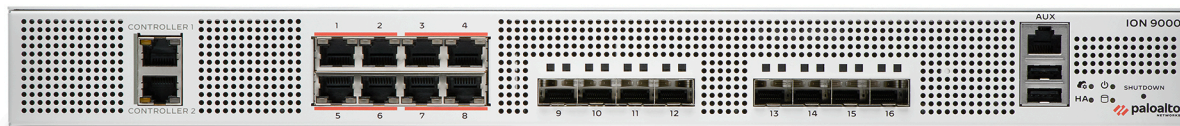
ION 9000 概述

了解 Prisma SD-WAN Instant-On Network (ION) 9000 并规划部署。

- [ION 9000](#)
- [ION 9000 端口](#)
- [ION 9000 前面板及 LED](#)
- [ION 9000 规格](#)
- [ION 设备合规声明](#)
- [ION 9000 安装包组件](#)
- [开启 ION 9000](#)

ION 9000

Prisma SD-WAN ION 9000 专为数据中心设计，可让您跨分支机构和数据中心创建安全的 SD-WAN 架构。它设计为在数据中心以无缝方式进行安装，具体方法是将其与使用传统标准路由协议的相邻数据中心设备进行对等。在“路径外”模型中部署 ION 9000 可支持弹性无干扰横向扩展以及高可用性 (HA)。

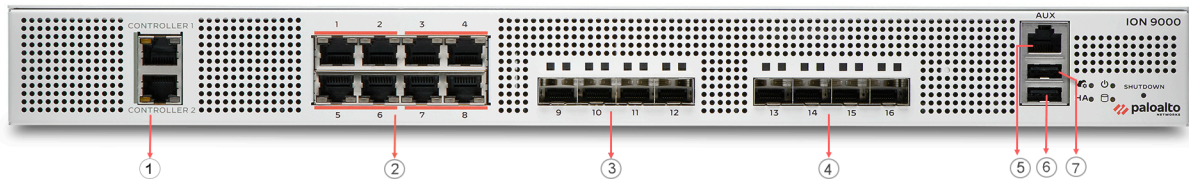


ION 9000 :

- 建立到数据中心网络的连接并交换路由信息。
- 终止所有已部署 Prisma SD-WAN 分支机构站点的虚拟专用网络 (VPN)。
- 维护路径对称性，并确保为应用程序使用最佳路径。
- 支持应用程序服务级协议 (SLA) 以及与分支机构 ION 设备相结合的路径选择。

ION 9000 端口

ION 9000 上端口的用途如下：



| 项目 | 端口 | 说明 |
|-------|-------------|--|
| 1 | 控制器端口 | ION 设备使用此端口与 Prisma SD-WAN 控制器通信。默认情况下，控制器端口支持 DHCP。 |
| 2 | 无法连线端口/绕过对端 | 4 对 - 端口 1/2、3/4、5/6、7/8。 |
| 3 | SFP+ 端口 | 端口 9 - 12 仅支持 10G SFP+。 |
| 4 | SFP+ 端口 | 端口 13 - 16 支持 1G SFP 和 10G SFP+ |
| 5 | AUX 端口 | 此端口用于离线访问和配置未安装的系统。AUX 端口速度为 115200 位/秒 |
| 6 和 7 | USB 端口 | 这些端口保留以供将来使用。 |

ION 9000 前面板及 LED

ION 9000 LED 指示以下内容：

| 图标 | 说明 |
|--|---|
| 显示电源状态  | 绿灯 — 开启电源。  黑灯 — 电源关闭。  |
| 显示控制器连接状态  | 蓝灯 — 已连接。  无灯 — 未连接。 |
| 显示磁盘状态  | 橙色灯（闪烁） — 显示磁盘活动。  |
| HA LED  | 熄灭 — 未配置。 绿色常亮 — 活动且已连接备份。  绿色（闪烁） — 活动，无备份。  红色常亮 — 待机。  红色（闪烁） — 故障。  |

ION 9000 规格

Prisma SD-WAN ION 9000 设备规格如下：

| 设备规格 | 说明 |
|---------------|---|
| 网络中的位置 | 大型和远程分支机构数据中心。 |
| I/O | |
| 控制器端口 | 2 个 10/100/1000 RJ-45 |
| WAN/LAN/互联网端口 | <ul style="list-style-type: none"> 8 个 10 千兆位以太网 SFP+ 端口 9 -12 仅支持 10G SFP+，端口 13 -16 支持 1G SFP 和 10G SFP+ 8x10 x 10/100/1000 RJ45 端口对 1/2、3/4、5/6 和 7/8 具有适合在分支机构设备模式下使用的可编程内联无法连线功能 |
| 吞吐量 | |
| 加密 IP 吞吐量 | 测量使用 1400 字节数据包 - 15 Gbps (DC) 8 Gbps (分支机构) |
| 电源和机械 | |
| 类型/瓦数 | 1+1 热插拔冗余 PSU 450W，交流 |
| 电源输入 | 交流 100-240V @50-60Hz 6-3A |
| 风扇制冷 | 4 个热插拔冷却风扇，气流从前部流向后部。 |
| 认证 | |
| 认证 | IEC60950-1, cULus, FCC 和 CE, A 类 |
| 环境 | |
| 工作温度 | 0°C 到 40°C (32°F 到 104°F) |
| 存放温度 | -40°C 到 70°C (-40°F 到 158°F) |
| 工作湿度 | 5% 至 90% (非冷凝) |
| 存放湿度 | 5% 至 95% (非冷凝) |

| 设备规格 | 说明 |
|----------------|--|
| 物理 | |
| 1RU 标准 4 柱机架空间 | 推荐： |
| 重量 | 21.38 磅 |
| 尺寸（深 x 宽 x 高） | 19.69 英寸 X 17.24 英寸 X 1.73 英寸 |
| 物理网络连接 | 单个千兆位以太网铜缆端口（带 DHCP），以及两个或多个用于其他功能的千兆位端口或万兆位端口。 |
| BGP 对端 | 第 2 层连接到两个正在彼此加入任何动态路由协议（BGP、OSPF、EIGRP）的不同网络设备。 |
| Internet 连接 | 常用于连接 Prisma 控制器。该连接可以是公司数据中心，利用 MPLS 网络建立的专用连接，也可以是通过本地宽带连接提供的公共 Internet 连接。 |

ION 设备合规声明

ION 9000 安装包组件

ION 9000 安装套件包含用于安装设备的以下部件和工具：

- 2 个 19 英寸 1RU 机架式安装滑轨，内置快速连接方孔适配器。
- 2 个 安装支架，附带配套螺丝。
- 2 个 19 英寸滑锁支架，附带配套螺丝。
- 2 根红色 Cat.5E 交叉/反转以太网电缆。
- 1 根灰色 Cat.5E 直通以太网电缆。
- 2 根电源线 — 规格取决于国家/地区。
- 1 把螺丝刀。
- 1 根 USB 到 Cat5/RJ-45 串行电缆。
- 2 个滑锁支耳。
- 定位销。

开启 ION 9000

将电缆连接到 ION 设备并将设备电缆插入交流电源插座。打开电源后，设备处于开机状态，电源指示灯变为绿色。

设备通电后，[通过 SSH 登录 ION 设备](#)并使用控制台分配静态 IP 地址。

关闭 ION 9000

通过以下方式关闭 ION 9000：



请勿通过拉电源线突然关闭 ION 设备。

- [使用设备工具包命令关闭](#)

运行设备工具包命令 `debug shutdown` 以关闭设备。



在执行命令之前，确保可实际接触设备以将其重新打开。

- [使用电源开关关闭](#)

按下电源开关 5 次（按住 1 秒钟，然后松开）可关闭设备。

- [使用 Python 脚本关闭](#)

使用脚本顺利关闭单个 ION 设备或多个 ION 设备。

首先，生成一个 API 令牌并将其添加到 `cloudgenix_settings.py`，然后执行命令 `./shutdown.py --serial <20-019291-9468>`。要关闭多台设备，请添加 ION 设备的序列号，如下所示：

```
./shutdown.py --serial 20-019291-9468 ./shutdown.py --serial  
20-019291-9469 ./shutdown.py --serial 20-019291-9470
```

重新启动 ION 9000

按电源开关 3 或 4 次可重新启动 ION 9000。

安装 ION 9000

在以下模式下部署 Prisma SD-WAN ION 9000：

- [机架式安装 ION 9000](#)
- [在虚拟路径内配置下安装 ION 9000](#)
- [在高可用性环境下安装 ION 9000](#)

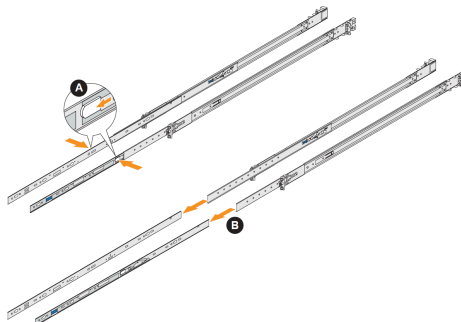
机架式安装 ION 9000

将 ION 9000 机架安装在带方孔的标准 19 英寸机架上：

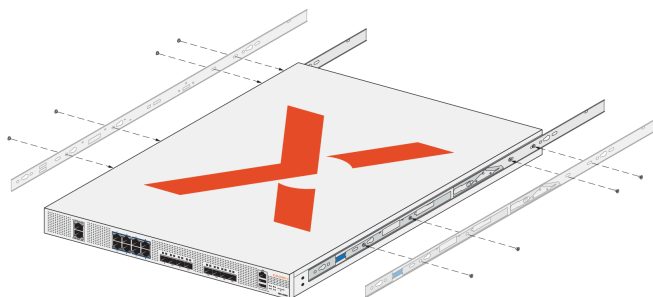
STEP 1 | 将机架式安装支架连接到 ION 9000

1. 打开安装包并找到滑轨。
2. 向外拉伸支架，并向前滑动支架释放按钮，以便将其完全从滑轨中退出，然后从滑轨上拆下机箱安装支架。

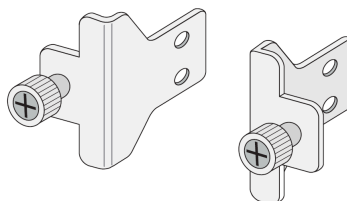
ION 9000 使用机箱安装支架连接两侧滑轨，从而安装在机架上。



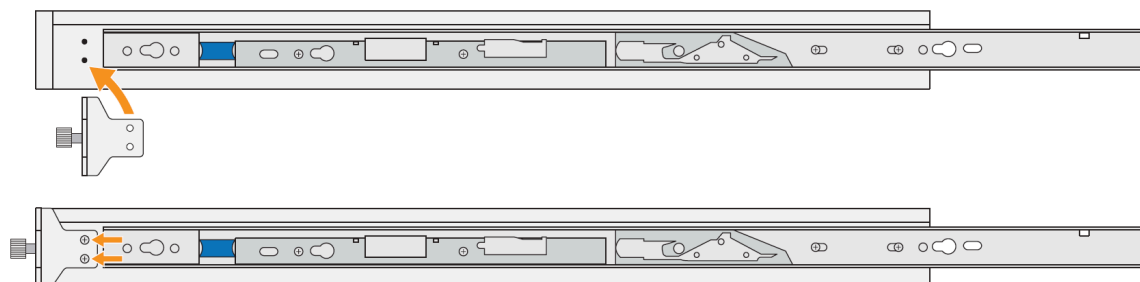
3. 将安装支架连接到 ION 9000 两侧。

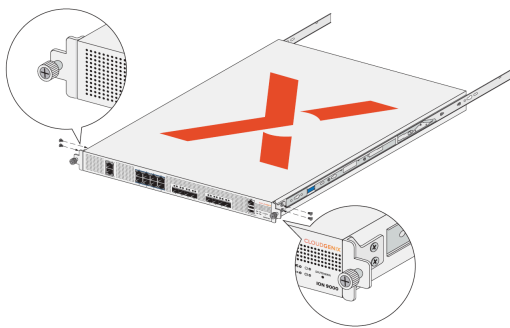


4. 从 ION 9000 配套工具包中找到滑锁支耳。



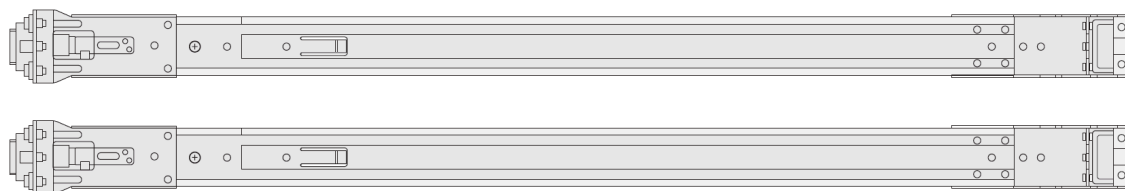
将滑锁支耳连接到 ION 9000 前端，从而在机架上锁定设备。



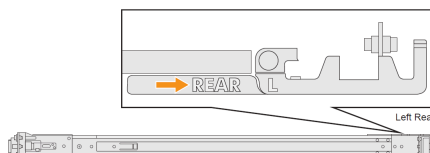


STEP 2 | 将滑轨连接到标准 19 英寸机架

1. 选择一个 1-RU 插槽，以便将滑轨插入机架。



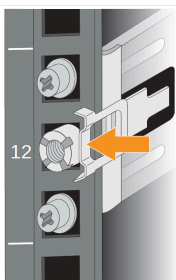
2. 将标有 REAR 的滑轨端与机架后侧对齐。



3. 将滑轨上的螺丝插入机架螺孔，确保金属扣将滑轨固定到机架柱上。



如果螺丝安装在滑轨上，请不要在插入机架前从滑轨上取下螺丝。



如果机架上带有带螺纹圆孔：

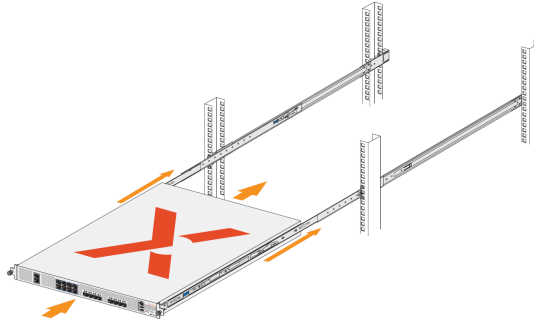
1. 使用机架式安装包中的定位销，将其穿过机架孔。
2. 将定位销穿过滑轨。
3. 将机箱安装支架连接到 ION 9000 两侧。
4. 将 ION 9000 滑入机架并确认已牢牢安装好设备。

如果机架上有无螺纹圆孔：

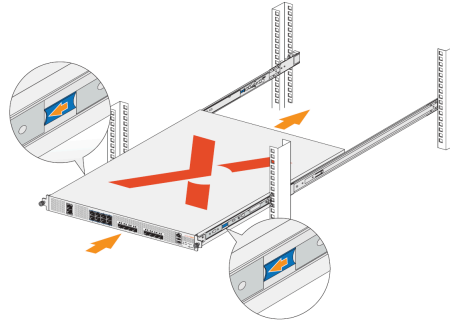
1. 在孔盘背后插入滑轨。
2. 使用安装包中的螺丝将滑轨固定到安装板。
3. 将机箱安装支架连接到 ION 9000 两侧。
4. 将 ION 9000 滑入机架并确认已牢牢安装好设备。
4. 在机架前侧，通过在机架上插入螺丝，将滑轨对齐到位。确保将紧固弹簧夹完全扣住，以便将滑轨牢牢固定到机架上。

STEP 3 | 将 ION 9000 滑入滑轨

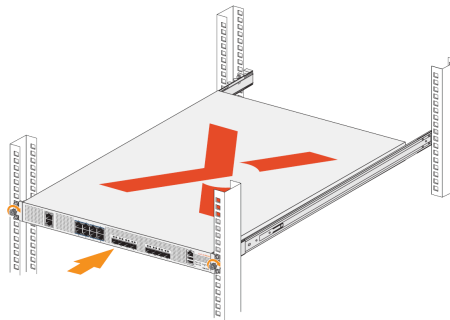
1. 将 ION 9000 上的安装支架与滑轨插槽对齐，并推入 ION 9000。



2. 滑动支架两侧的支架释放按钮，将 ION 9000 滑入机架，直到锁定到位。



3. 使用滑锁支耳侧面的大头螺丝，将 ION 9000 固定到滑轨。



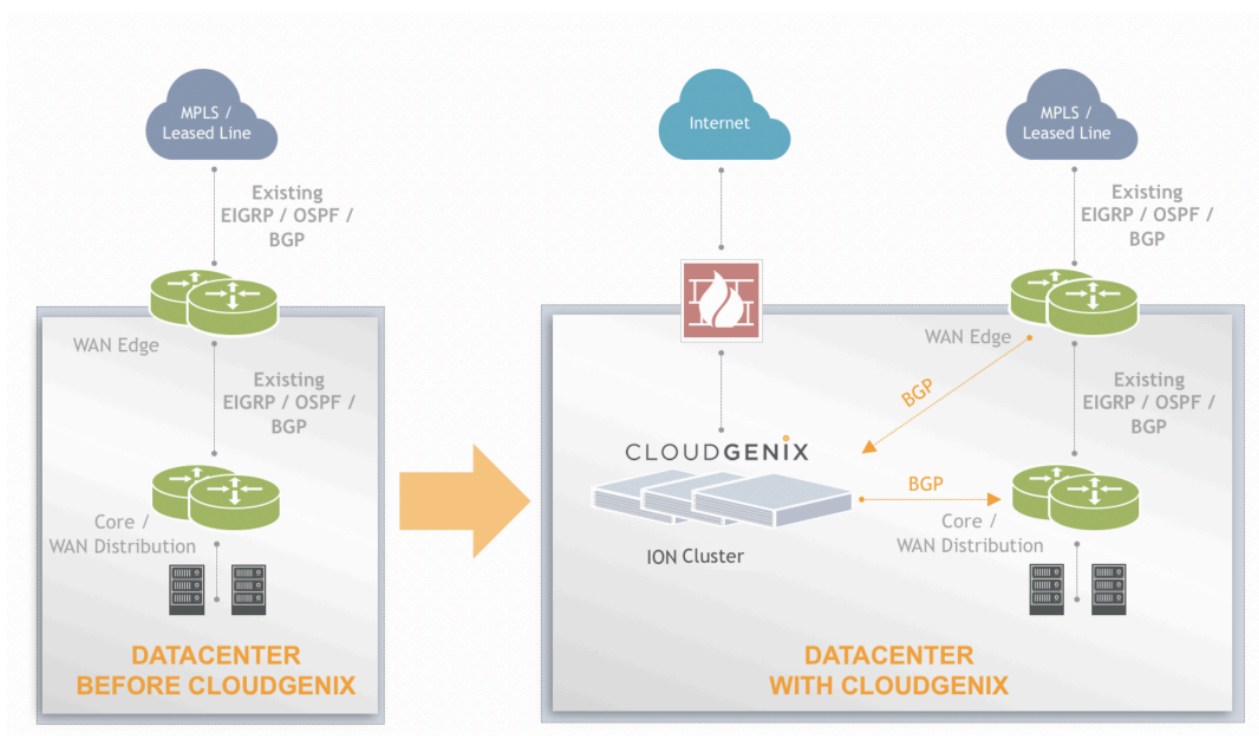
在虚拟路径内配置下安装 ION 9000

利用虚拟路径内配置，当 Prisma SD-WAN ION 9000 进入和退出数据中心时，可支持系统执行 SD-WAN 操作。

利用这种操作模式，ION 9000 集群可以：

- 使用传统网络路由协议为特定端点请求非常具体的流量。
- 只需对现有数据中心网络拓扑结构稍作更改，或完全不需要更改。
- 根据负载、站点数量和地理分布进行水平扩展。
- 如果发生故障，可以将流量无缝转发到另一个 ION 9000 或旧路由网络。

下图展示了 ION 9000 数据中心的虚拟路径内部署架构。



使用以下端口类型配置系统，以便在虚拟路径内配置下设置 ION 9000：

- 配置控制器端口
- 配置对等端口
- 配置 Internet 端口

配置控制器端口

Prisma SD-WAN ION 9000 使用控制器端口与 Prisma SD-WAN 控制器进行通信。默认情况下，控制器端口是为 DHCP 配置的。但是，如果要设置静态 IP，或者没有启用 DHCP 的网络，请访问控制台，并在控制器 1 上设置静态 IP。

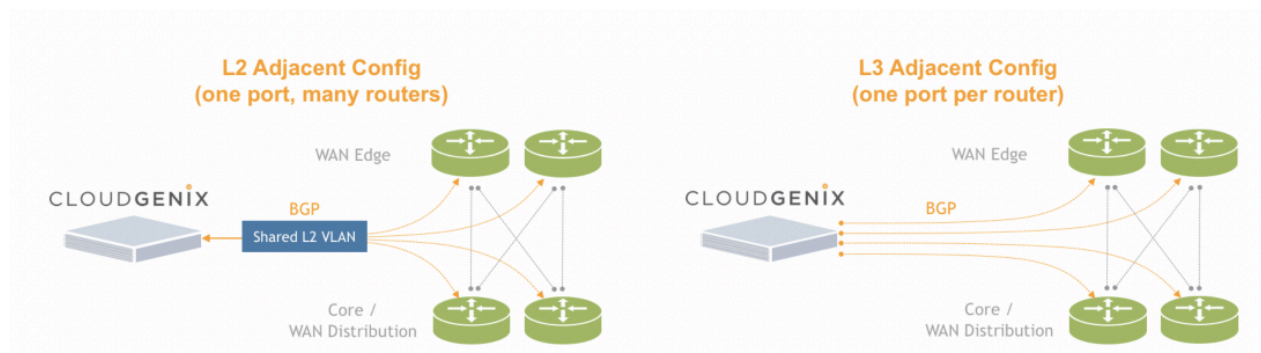
控制器 1 端口应连接至 1G 以太网铜缆端口，与客户端 PC 或笔记本电脑连接到公司网络的情况相似。确保在端口 443 上允许出站互联网访问权限，以便支持控制器端口与 Prisma SD-WAN 控制器服务之间的通信。

然后，在此端口建立连接并打开 ION 9000 电源后，ION 9000 会自动连接并注册到 Prisma SD-WAN 控制器。注册后即可在 Prisma SD-WAN 控制台中声明和配置 ION 9000。

配置对等端口

Prisma SD-WAN ION 9000 使用对等端口通过 BGP 与 WAN 边缘/核心或 WAN 分布路由器进行通信。每个路由器可能使用一个物理端口进行连接，或者通过共享第 2 层 VLAN，多个路由器也可以共享单个端口。

下图展示了 ION 9000 的对等端口拓扑结构。



根据路由器的数量、类型以及第 2 层或第 3 层配置的选择，需要的对等端口数量可能不同。但是，对于对等端口，可以使用任何非控制器端口。配置时可以设置和识别这些端口。

在配置前为对等端口预先布线：

1. 计划好对等配置所需要的 ION 9000 端口的类型和端口号。
2. 从 ION 9000 设备将端口连接到相应的路由器或交换机。
3. 记录 ION 端口号以及连接路由器/交换机的端口信息，以便将来参考。

以下是 HA 部署的各种方案：

- 具有互联网、MPLS 和第 3 层 LAN 交换机的分支机构 HA
- 具有互联网、MPLS 和第 2 层 LAN 交换机的分支机构 HA
- 具有双互联网和第 3 层 LAN 交换机的分支机构 HA
- 具有双互联网和第 2 层 LAN 交换机的分支机构 HA
- ION 设备的分支机构 HA，无旁路

配置 Internet 端口

Prisma SD-WAN ION 9000 使用互联网端口接收来自互联网的入站 VPN 连接。通常，ION 9000 设备为每个数据中心使用一个互联网端口，并且此端口必须能够从互联网接收流量。

该互联网端口必须明确允许从远程 ION 设备向 ION 9000 传输入站 UDP 4500 流量。此外，如果在 ION 9000 外部通过此端口使用了防火墙或 NAT，则需要从防火墙或 NAT 设备为 UDP 4500 配置端口转发或直通。

在配置前为互联网端口预先布线：

1. 计划好 VPN 配置所需要的 ION 9000 端口的类型和端口号。
2. 从 ION 9000 设备将端口连接到相应的设备。
3. 记录 ION 端口号以及连接设备端口信息，以便将来参考。

在高可用性环境下安装 ION 9000

Prisma SD-WAN 在分支机构站点与数据中心集群之间提供了可水平扩展的高可用性 (HA) 解决方案。

STEP 1 | 添加第二个 ION 9000 到需要高可用性 (HA) 的数据中心。

STEP 2 | 通过同一端口将电缆连接至第二个 ION 9000。

STEP 3 | 在 Prisma SD-WAN 控制台上，声明 ION 设备并将其分配给数据中心。

STEP 4 | 配置 ION 设备，并确认它可以与核心和 WAN 边缘路由器通信。

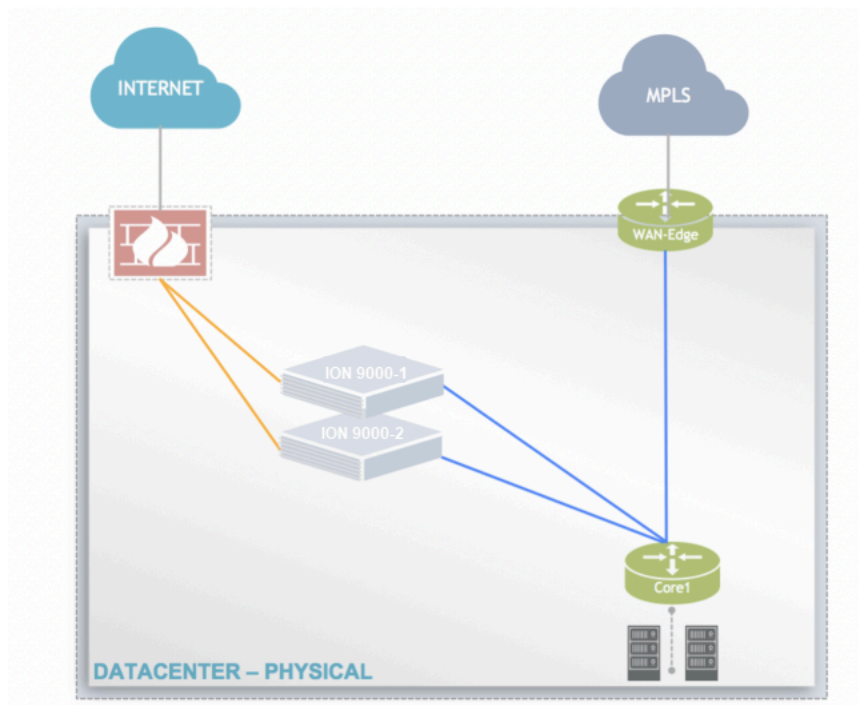
确保：

- 对于每个 ION 设备，控制器端口的 IP 地址是唯一的。请注意，控制器端口可以与第一个 ION 设备属于同一子网。
- 对于每个 ION 设备，核心和 WAN 边缘对等端口的 IP 地址都是唯一的，并且会为其对等地址分配一个 /29 或更大的子网块。
- 对于每个 ION 设备，互联网端口的 IP 地址都是唯一的。
- 最后，如果已配置 NAT，请确保对于每个 ION 设备，NAT IP 地址或 NAT 端口都是唯一的。

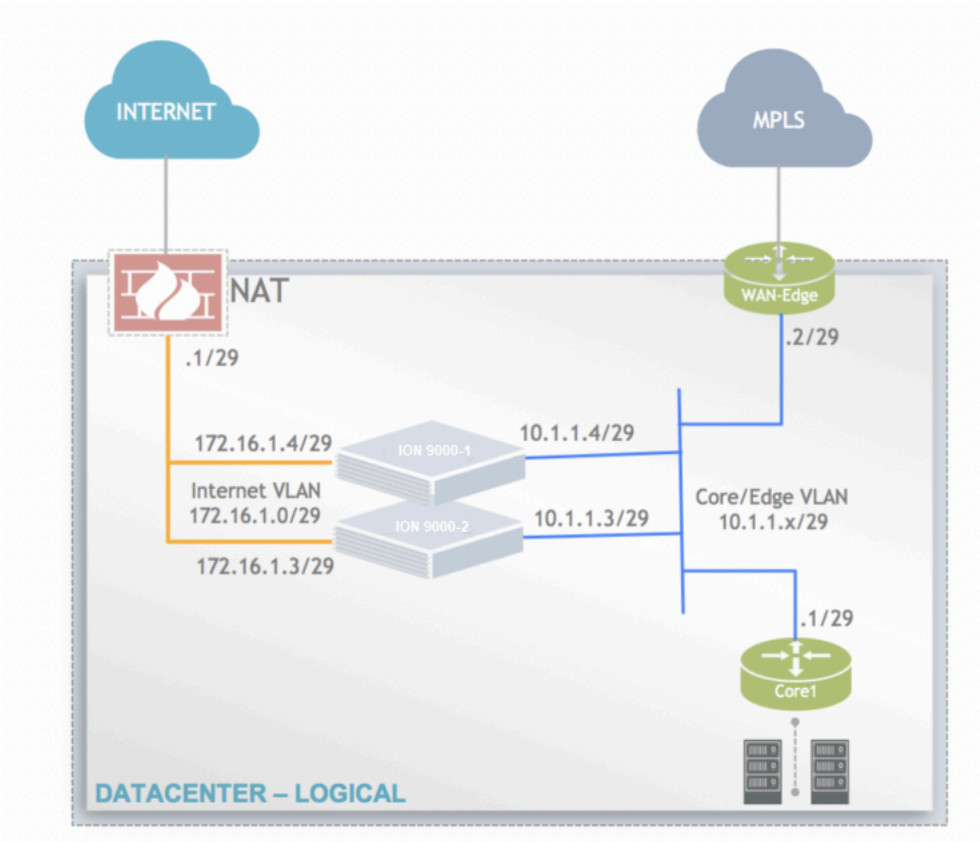
除 IP 地址外，第二个 ION 设备不需要其他配置。两个 ION 9000 设备都要与同一核心和 WAN 边缘路由器对等。第二个 ION 设备将继承与第一个设备一样的 BGP 配置。

下图展示了使用两个 ION 9000 设备的物理和逻辑连接示例。虽然该拓扑结构仅显示了一个核心路由器和一个 WAN 边缘路由器，但是，在有多多个路由器的环境中，您可以使用同一连接模型。

下图展示了 ION 9000 HA 的物理连接。



下图展示了 ION 9000 HA 的逻辑连接和 IP 地址。



下图展示了 ION 9000 HA 的 BGP 设置。

