Citrix SD-WAN 11.5

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Cloud Software Group 文档内容采用了机器翻译，仅供您参考。Cloud Software Group 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Cloud Software Group 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Cloud Software Group 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Cloud Software Group 不承担任何责任。

Contents

Citrix SD-WAN 的发行说明 11.5 版本

November 16, 2022

本发行说明文档介绍了 Citrix SD-WAN 11.5 的增强功能和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

SD-WAN 11.5 版本中提供的增强功能和更改。

其他

Citrix SD-WAN 11.5 版本规格

- Citrix SD-WAN 11.5.0 是有限可用性版本，仅针对特定的客户/生产部署推荐和支持。
- SD-WAN 11.5.0 版本不支持高级版 (AE)、高级版 (PE)、广域网优化部署。
- SD-WAN 11.5.0 仅支持 SD-WAN 平台模型和软件包中提到的平台。
- SD-WAN 11.5.0 不支持适用于本地的 Citrix SD-WAN Center 或 Citrix SD-WAN Orchestrator。
- Citrix 下载页面上没有 SD-WAN 11.5.0 固件。
- SD-WAN 11.5.0 版本只能通过 Citrix SD-WAN Orchestrator 服务提供，并且仅在选定的地理位置 POP 上提供。
- 在任何生产网络上部署 11.5.0 之前, 请确保获得 Citrix 产品管理/Citrix 支持部门所需的批准和指导。

[NSSDW-38486]

Citrix SD-WAN Orchestrator 服务取代 了 **SD-WAN** 配置编辑器：

从 Citrix SD-WAN 11.5 版本开始，SD-WAN 配置编辑器和 SD-WAN Center 被 Citrix SD-WAN Orchestrator 服务所取代。Citrix SD-WAN Orchestrator 服务支持当前通过 SD-WAN 配置编辑器完成的所有配置。有关 Citrix SD-WAN Orchestrator 服务的更多详细信息，请参阅 Citrix SD-WAN Orchestrator 服务。

[NSSDW-33528]

IPv6 支持:

从 Citrix SD-WAN 11.5.0 版本开始，Citrix SD-WAN 设备的以下数据平面功能支持 IPv6 地址：

- 应用程序路由
- Citrix Cloud 和网关服务优化
- 基于域名的应用程序分类
- 动态 PAC 文件定制
- 动态路由
- 防火墙默认值
- 多播
- Office 365 优化
- ppPoE
- 站点报告-路由协议
- VRRP

配置上面列出的功能后，如果禁用 IPv4 或 IPv6 协议，则这些功能将无法按预期工作。

[SDW-23397、NSSDW-29150、NSSDW-29152、NSSDW-29154、NSSDW-29155、NSSDW-29156、NSSDW-29468、NSSDW-1940、NSSDW-1995]

监控增强功能：

以下监控仪表板已得到增强，可在新的设备 UI 上使用：

- DNS 透明转发器
- 防火墙连接、防火墙过滤器、防火墙 NAT
- IGMP、IGMP 代理、IGMP 统计信息
- IKE、IPsec
- 多播组、多播组源、多播组目标
- PPPoE 会话
- VRRP

[NSSDW-33763]

平台和系统

参考资料-应用程序签名库

DPI 应用程序签名库已更新。

[NSSDW-38209]

已修复的问题

SD-WAN 11.5 版本中已解决的问题。

其他

某些 SD-WAN 设备的管理接口状态在 UI 的“以太网接口设置”页面上显示为“关闭”。当某些支持带内管理的设备提供带外使用选项时，会出现此问题。因此，设备使用带外管理接口来访问 SD-WAN Orchestrator 服务。

[NSSDW-37028]

已知问题

SD-WAN 11.5 版本中存在的问题。

如果在任何站点或 WAN 链路上更改配置时进行扩展部署，则路由引擎重新启动会导致 BGP 会话抖动。

[SDWANHELP-2594]

SD-WAN 设备意外崩溃。此问题发生在以下情况下：

- 在软件升级期间，IPv6 多播流量正在流动。
- IPv6 多播流量使用内部网 GRE 通道发出，并使用 MLDv2 代理配置通过虚拟路径复制到多个分支。

解决办法：在软件升级期间禁用 IPv6 多播流量，并在升级成功后启用。

[NSSDW-38495]

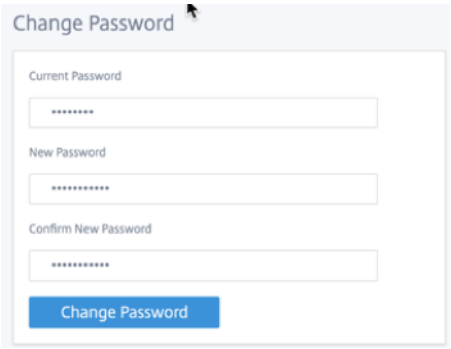
用于 **SD-WAN** 设备的新用户界面

September 2, 2022

为 SD-WAN 装置引入了新的用户界面 (UI)。新 UI 是使用最新 UI 技术构建的。新的 UI 设计提高了安全性，改进了外观和感觉，更高的性能、安全性和响应性。但新 UI 保留了旧 UI 中每个功能的流程和页面布局。

从 Citrix SD-WAN 11.4 开始，默认情况下，在配置为客户端的所有 Citrix SD-WAN 设备上启用新 UI。

> 注意
>
> - 将 Citrix SD-WAN 设备置备为 MCN 可将您重定向到旧版 UI。
> - 具有管理员角色的所有本地用户和远程管理员用户都可以访问新的用户界面。通过 RADIUS 或 TACACS+ 身份验证服务器对远程用户帐户进行身份验证。设 Provisioning SD-WAN 设备时，必须更改默认管理员用户帐户密码。默认密码是 SD-WAN 装置的序列号，必须在登录设备后首次更改。



为了向后兼容性，维护旧用户界面，不建议使用。可以使用 URL **https: // < ip-address >/cgi-bin/login.cgi** 访问旧用户界面。用户 管理员 的用户名和密码在两个（新/旧版）用户界面中保持不变，首次登录过程可以使用任一界面完成。新 UI 的未来版本将支持其他用户。

Citrix SD-WAN 新用户界面

新的用户界面可以使用谷歌浏览器（版本 81）、Mozilla 火狐浏览器、微软边缘（版本 81 +）和旧版微软边缘（44 版以上）浏览器访问。

> 注意
>
> 不支持微软 Internet Explorer、Apple Safari 和其他浏览器。

要访问新的 UI 页面，请执行以下操作：

1. 打开新的浏览器选项卡并导航到 **https: // < management-ip >** 以访问 SD-WAN 设备上的新 UI。如果您正在访问 IPv6 地址，请输入 `https://<[IPv6 address]>`。

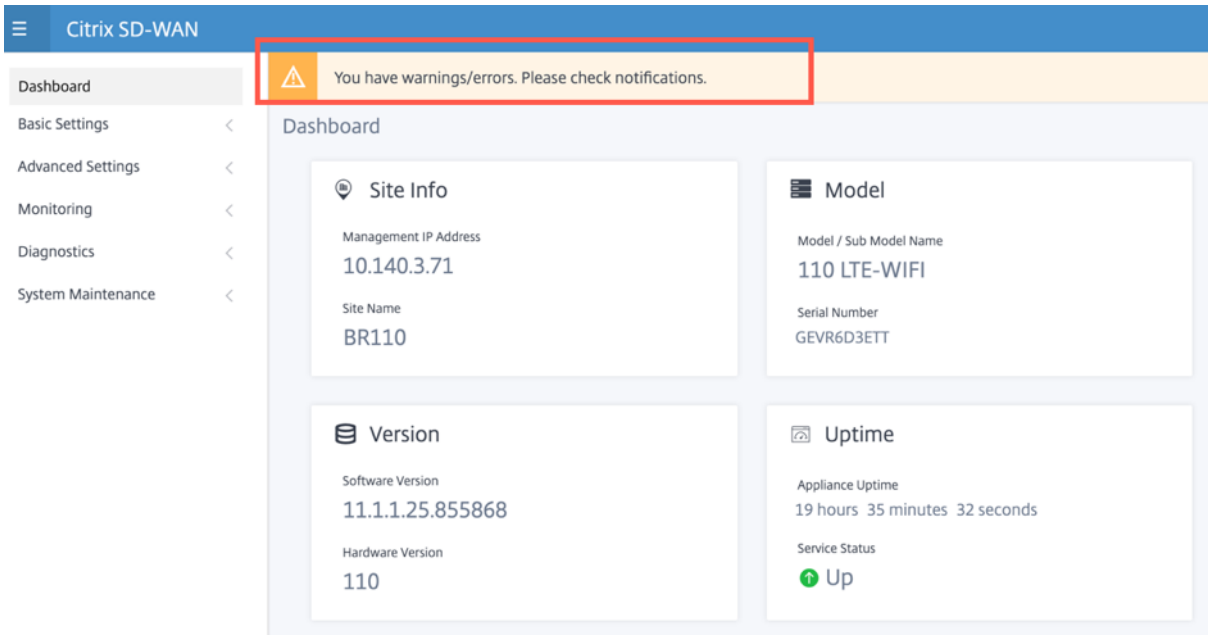
   示例：`https://[fd73:xxxx:yyyy:26::9]`

> 注意：
>
> 在启用带内管理的情况下，可以在中提供接口 IP 地址 ** < management-ip > 以访问新 UI。可以在启用用于 IP 服务的多个受信任接口上启用带内管理。您可以使用管理 IP 和带内虚拟 IP 访问 UI。

1. 提供用户名和密码。单击登录。

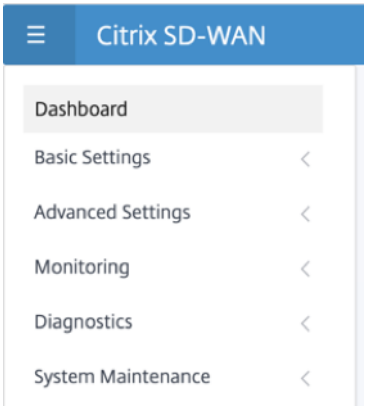
此时将显示 Citrix SD-WAN 用户界面页面。

成功登录后，您可以看到导航面板位于左侧。此外，如果有任何警告或错误，您可以在仪表板上看到通知横幅。



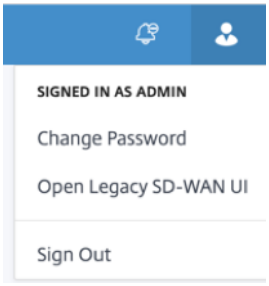
导航

左侧导航边栏可以隐藏或点击汉堡包图标可见。左上角的汉堡包图标提供指向仪表板、基本/高级 设置、监控和管理相关选项的链接。



菜单栏

右上角的用户菜单显示已登录用户详细信息。您可以通过单击“打开旧版 **SD-WAN UI**”选项，在新的浏览器选项卡中打开旧版 用户界面。单击任何通知的铃铛图标。

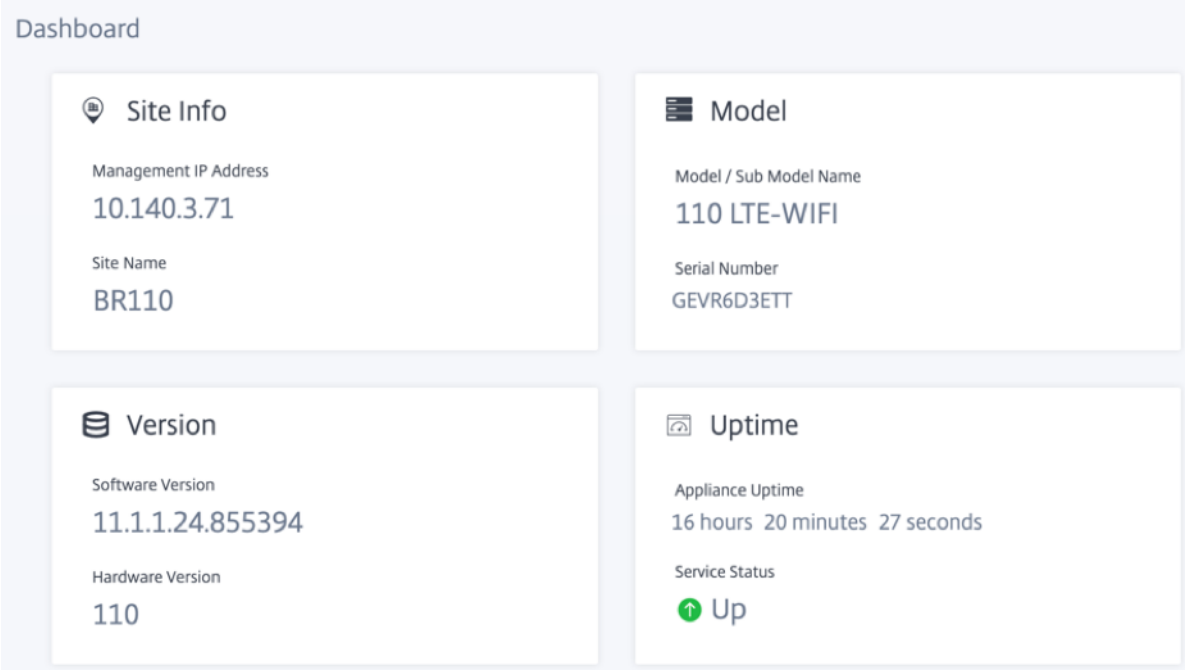


控制板

控制板 页面以磁贴视图的形式显示 SD-WAN 设备的以下基本信息：

- 站点—显示带 管理 **IP** 地址 和站 点名称的站点信息
- 型 号—显示 型号**/Sub** 型号 和 序列号
- 版本—显示 软件 和 硬 件版本
- 正常运行时 间-显示 设备正常运行时间、**Citrix** 虚拟 **WAN** 服务状态和 **Orchestrator** 连接
- 高可用性 -显示本地和对等设备 HA 状态以及上次 HA 更新接收时间。
- 按计费链接—显示已启用计量的链接的使用情况和账单详细信息。
- **Orchestrator** 连接 -显示设备与 Citrix SD-WAN Orchestrator 服务的连接状态。将显示以下状态信息：
  - 联机状态-指示设备与 Citrix SD-WAN Orchestrator 服务之间的连接状态。设备会定期向 Citrix SD-WAN Orchestrator 服务发送心跳信号，以将连接状态标识为好还是坏。

- 服务状态-指示设备对所有必需的 SD-WAN Orchestrator 服务（如下载、主页、日志记录、统计信息）的 https 可访问性。如果服务状态不好，则意味着连接已建立，但所有或部分服务都无法访问。此时将显示无法访问的服务名称。
- **DNS** 状态- 指示 FQDN DNS 解析状态。如果 DNS 状态不正确，则表示其中一个 FQDN 的 DNS 解析失败。将显示未解析的 FQDN 的名称。
- 本地网关状态-指示默认网关状态。对于带外连接，网关状态是通过 ping 默认网关来确定的。对于带内连接，网关状态是通过 ping 带内以太网接口 IP 地址来确定的。
- 通过连接-指示设备如何到达 Citrix SD-WAN Orchestrator 服务。通过带外（默认配置）或通过带内（如果配置了带内管理）。
- 失败原因：连接到 SD-WAN Orchestrator 服务时失败的原因。



基本设置

SD-WAN 设备 基本设置 包括以下实体配置。新 UI 提供了一个单独的页面，用于分别配置每个实体。

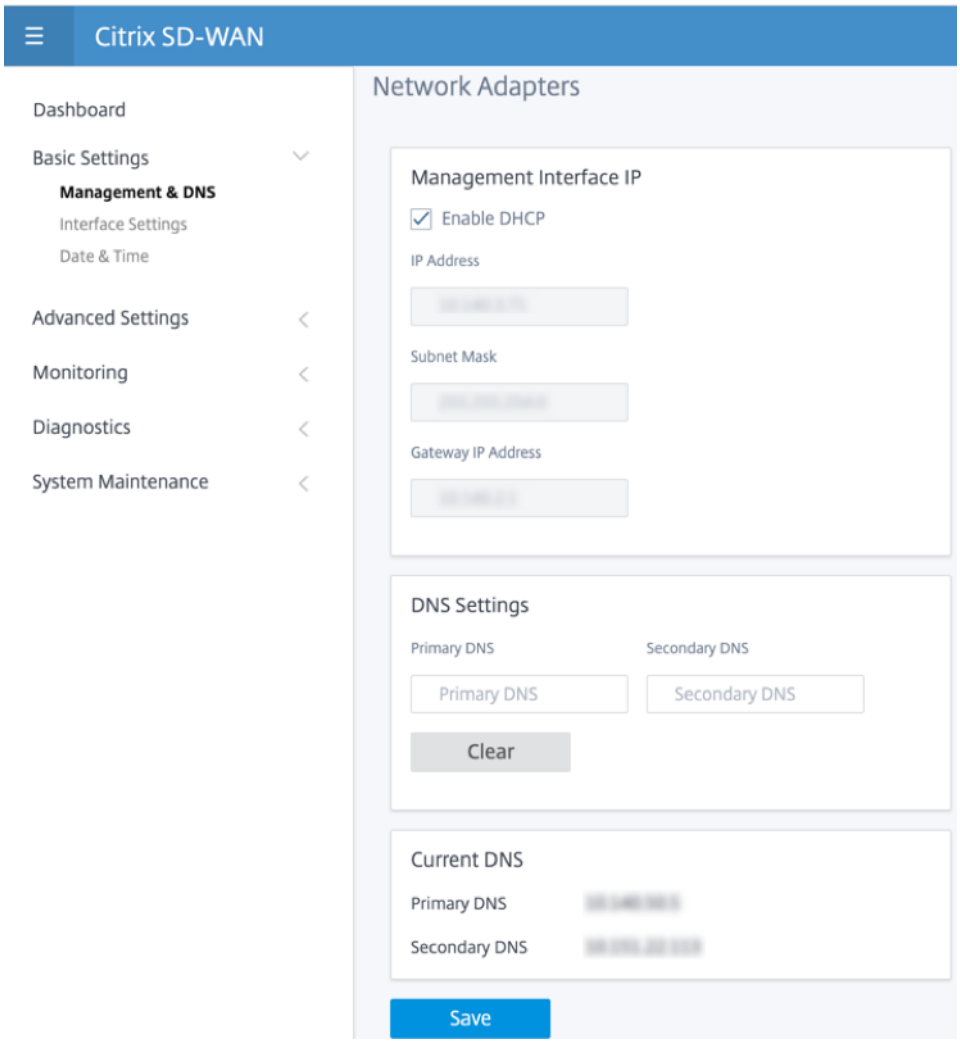
- 管理和 DNS
- 接口设置
- LACP LAG 组
- 日期和时间
- RADIUS 服务器
- TACACS+ 服务器

管理和 **DNS**

在 管理和 **DNS** 页面中，您可以配置管理接口 IP 地址和 DNS 设置。有关详细信息，请参阅 配置管理 IP 地址。

管理界面允许列表是有权访问管理界面的 IP 地址或 IP 域的批准列表。空列表允许从所有网络访问管理界面。您可以添加 IP 地址以确保管理 IP 地址只能由受信任的网络访问。

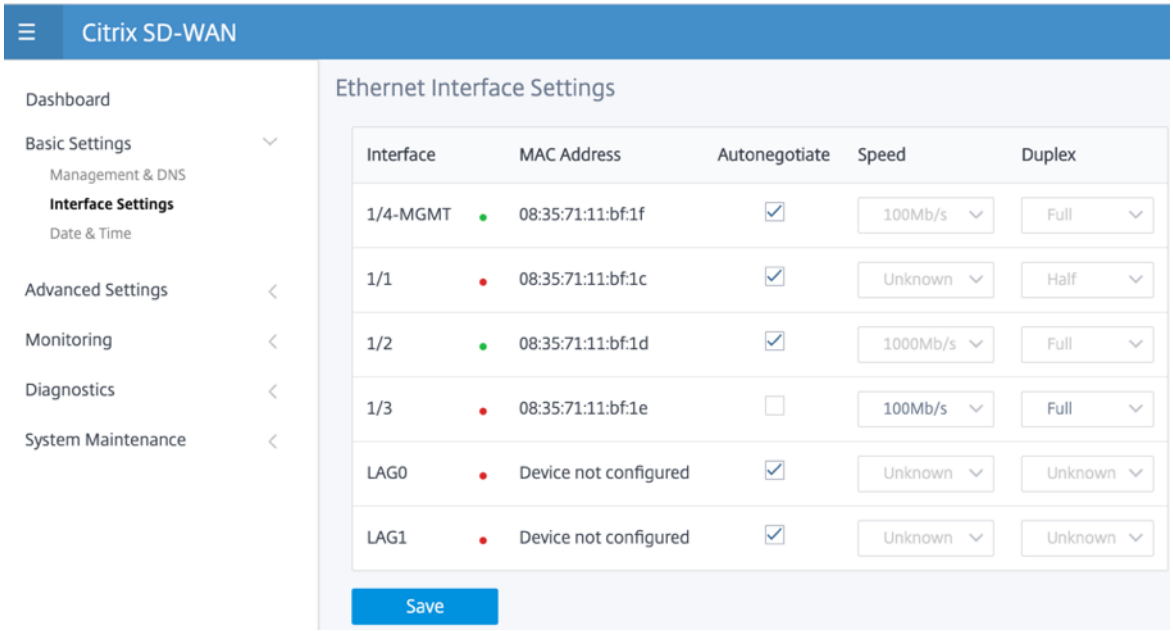
要在允许列表中添加或删除 IPv4 地址，必须仅使用 IPv4 地址访问 SD-WAN 设备管理界面。同样，要在允许列表中添加或删除 IPv6 地址，必须仅使用 IPv6 地址访问 SD-WAN 设备管理界面



输入要配置的设备的 **IP** 地址、子网掩码和网关 IP 地址。在 **DNS** 设置 部分下，提供主 DNS 服务器和辅助 DNS 服务器详细信息，然后单击 保存。

接口设置

接 口设置 页面显示以太网端口配置数据。关闭的端口在 MAC 地址上显示为红点。



LACP LAG 组

链路聚合组 (LAG) 功能允许您对 SD-WAN 设备上的两个或多个端口进行分组，以便作为单个端口一起工作。这可确保提高可用性、链路冗余性和增强性能。

之前，LAG 中只支持活动备份模式。从 Citrix SD-WAN 11.3 版本开始，支持基于 802.3AD 链路聚合控制协议 (LACP) 协议的协商。LACP 是标准协议，为 LAG 提供了更多功能。

在活动备份模式下，任何时候只有一个端口处于活动状态，其他端口处于备份模式。活动和备份支持依赖于数据平面开发工具包 (DPDK) 软件包来实现 LAG 功能。

使用 LACP，您可以同时通过所有端口发送流量。作为一项好处，您可以获得更多带宽以及链路冗余机制。LACP 实现支持 主动-主动 模式。现在，使用主动备份模式，您还可以从 SD-WAN UI 中选择完整的 LACP 主动-主动模式。

LAG 功能仅在以下 DPDK 支持的平台上可用：

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 2100 SE/PE
- Citrix SD-WAN 4100 和 5100 SE
- Citrix SD-WAN 6100 SE

> 注意
>
> VPX/VPXL 平台上不支持 LAG 功能。

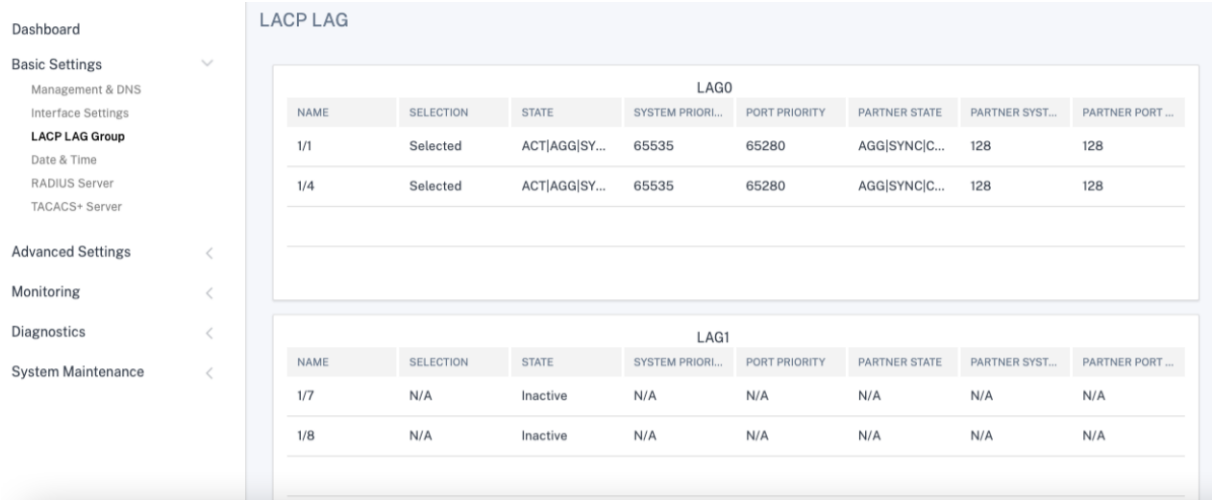
在 Citrix SD-WAN 设备上，最多可以创建 4 个 LAG，其中每个 LAG 中最多分组 4 个端口。

对于 Citrix SD-WAN 210 和 410 设备（最多 3 个 LAG）以及 Citrix SD-WAN 110 设备，最多可以创建 2 个 LAG。

您只能使用 旧版 UI 或 SD-WAN Orchestrator 创建 LAG。在新 UI 中，您只能查看创建的 LAG 的详细信息。

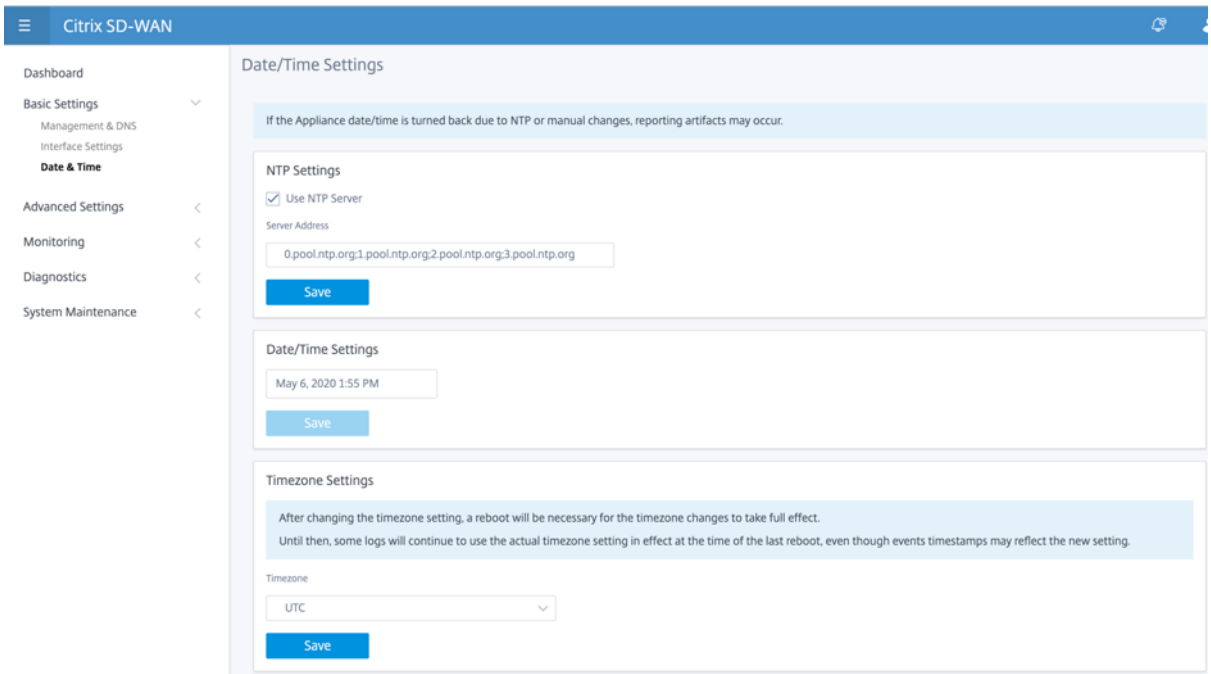
要查看 LAG 详细信息，请导航到 基本设置 > **LACP LAG** 组。

您可以查看 LACP LAG 详细信息，例如活动端口和伙伴端口的当前状态、系统和端口优先级详细信息。



日期和时间

在 日期和时间 设置页面中，您必须在设备上设置日期和时间。有关详细信息，请参阅 设置日期和时间。



RADIUS 服务器

您可以将 SD-WAN 设备配置为对一个或多个 RADIUS 服务器的用户访问进行身份验证。

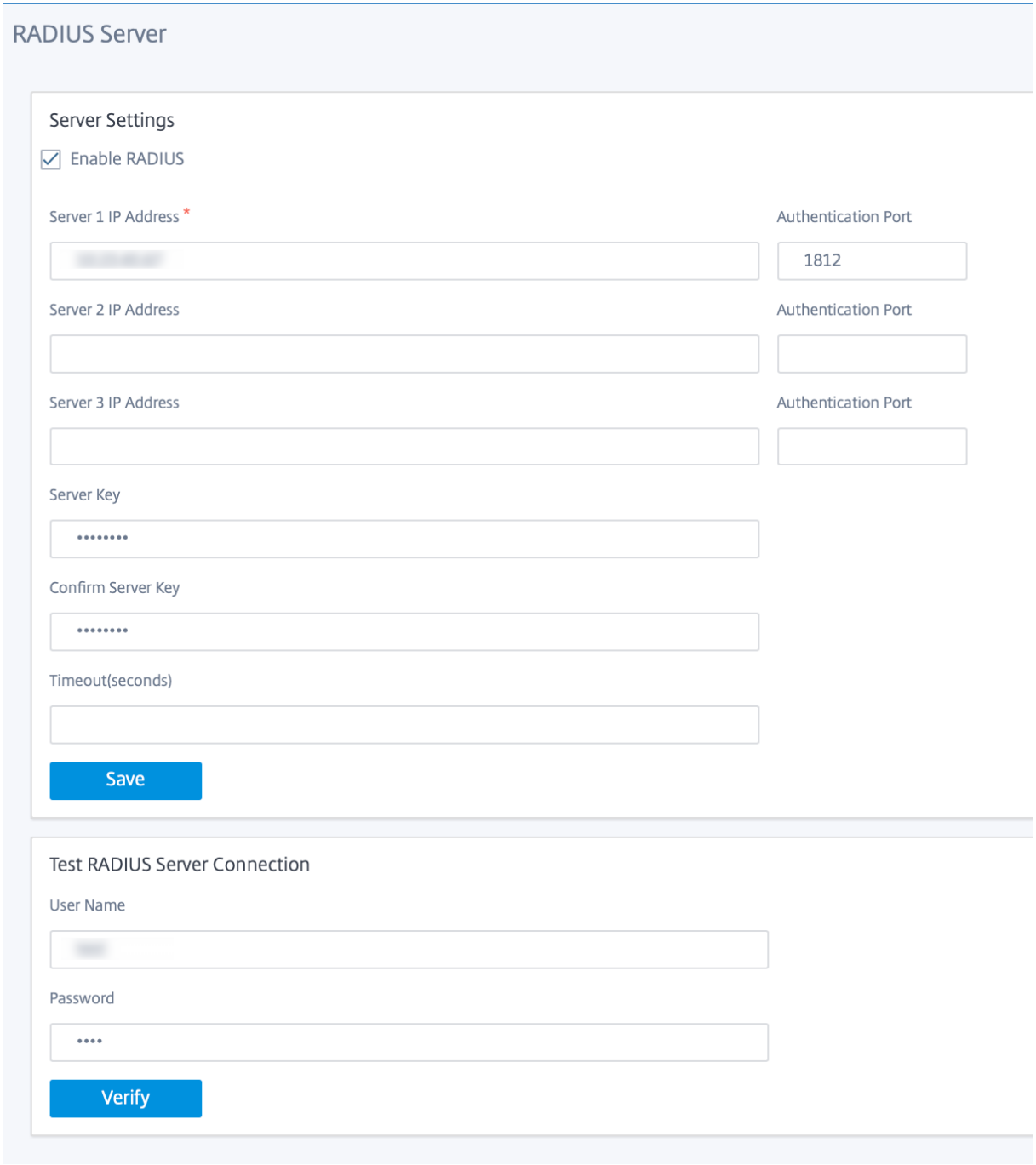
要配置 RADIUS 服务器：

1. 选中 启用 **RADIUS** 复选框。
2. 输入 服务器 **IP** 地址 和 身份验证端口。最多可以配置三个服务器 IP 地址。

   > 注意：
   >
   > 要配置 IPv6 地址，请确保 RADIUS 服务器还配置了 IPv6 地址。

3. 输入 服务器密钥 并确认。
4. 输入 超 时值（以秒为单位）。
5. 单击保存。

您还可以测试 RADIUS 服务器连接。输入 用户名 和 密码。单击 **Verify**（验证）。



TACACS+ 服务器

您可以配置 TACACS+ 服务器进行身份验证。与 RADIUS 身份验证类似，TACACS+ 使用私钥、IP 地址和端口号。默认端口号为 49。

要配置 TACACS+ 服务器，请执行以下操作：

1. 选中 启用 **TACACS+** 复选框。

2. 输入 服务器 **IP** 地址 和 身份验证端口。最多可以配置三个服务器 IP 地址。

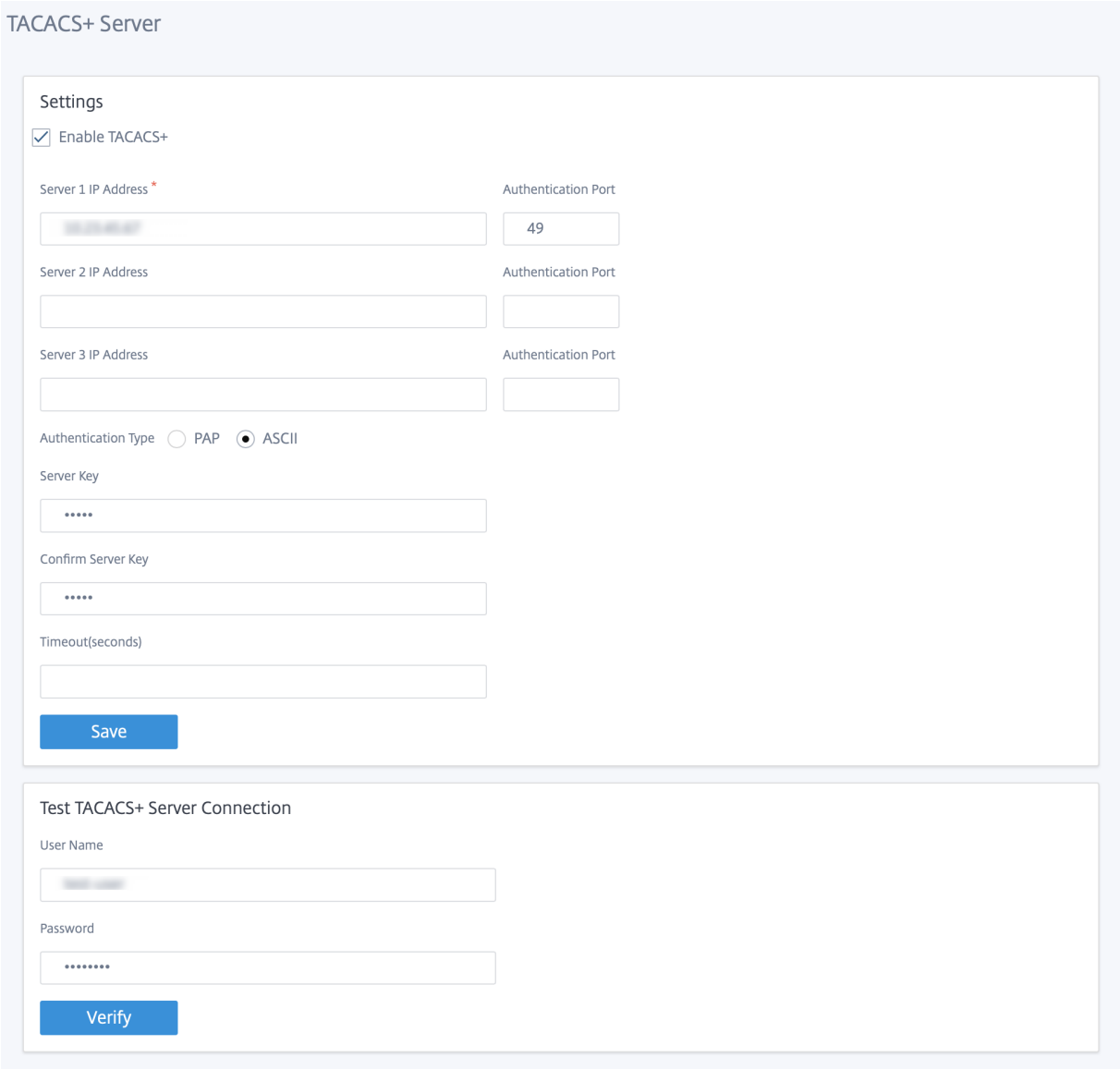
   > 注意：
   >
   > 要配置 IPv6 地址，请确保 TACACS+ 服务器还配置了 IPv6 地址。

3. 选择 **PAP** 或 **ASCII** 作为身份验证类型。

   - PAP：使用密码身份验证协议 (PAP) 通过向 TACACS+ 服务器分配强共享密钥来加强用户身份验证。
   - ASCII：使用 ASCII 字符集通过向 TACACS+ 服务器分配强共享密钥来加强用户身份验证。

4. 输入 服务器密钥 并确认。
5. 输入 超 时值（以秒为单位）。
6. 单击保存。

您还可以测试 TACACS+ 服务器连接。输入 用户名 和 密码。单击 **Verify**（验证）。



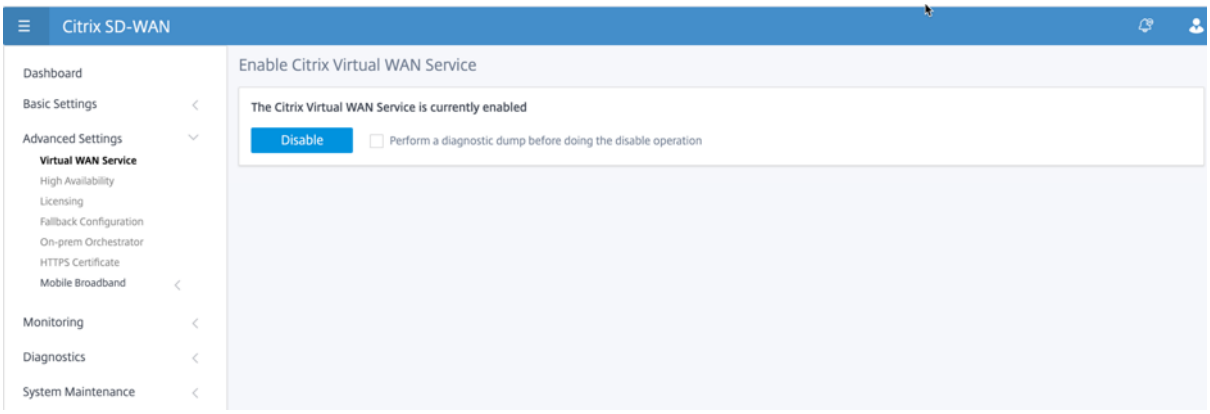
高级设置

SD-WAN 设备 高级设置 包括以下实体配置。

- Citrix 虚拟广域网服务
- 高可用性
- 移动宽带
- 许可
- 回退配置
- HTTPS 证书
- 本地管弦乐器

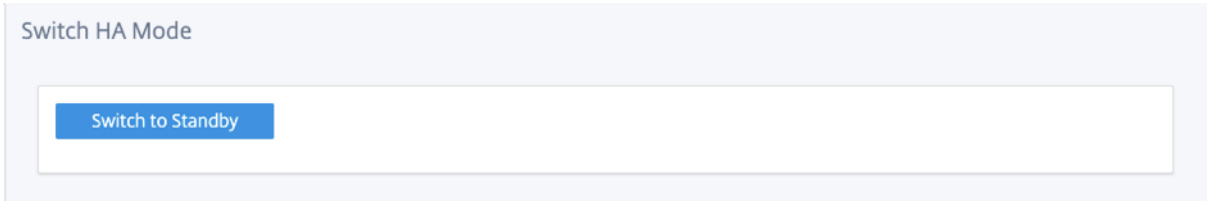
Citrix 虚拟广域网服务

Citrix 虚拟 **WAN** 服务 页面允许您启用/禁用 Citrix 虚拟 WAN 服务。有关详细信息，请参阅 配置虚拟 WAN 服务。



高可用性

在 高可用性 页面中，您可以在活动和备用状态之间切换 SD-WAN 高可用性 (HA) 设置。高可用性状态在仪表板中可用（如果配置了高可用性）。有关详细信息，请参阅 高可用性模式。



移动宽带

Citrix SD-WAN 设备（如 Citrix SD-WAN 210 SE LTE 和 110 LTE 无线网络设备）具有内置的 LTE 调制解调器。您还可以在以下 Citrix SD-WAN 装置上连接外部 3G/4G USB 调制解调器。

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 东南 LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE 无线网络 SE

CDC 以太网、MBIM 和 NCM 是支持的三种外部 USB 调制解调器类型。

有关使用旧版 GUI 配置 LTE 的详细信息，请参阅以下主题：

- 在 210 SE LTE 设备上配置 LTE 功能
- 在 110-LTE-WiFi 设备上配置 LTE 功能
- 配置外部 USB LTE 调制解调器

对于内置 LTE 调制解调器，请将 SIM 卡插入 Citrix SD-WAN 装置的 SIM 卡插槽中。将天线固定到 Citrix SD-WAN 装置。有关更多信息，请参阅 安装 LTE 天线 并打开设备电源。

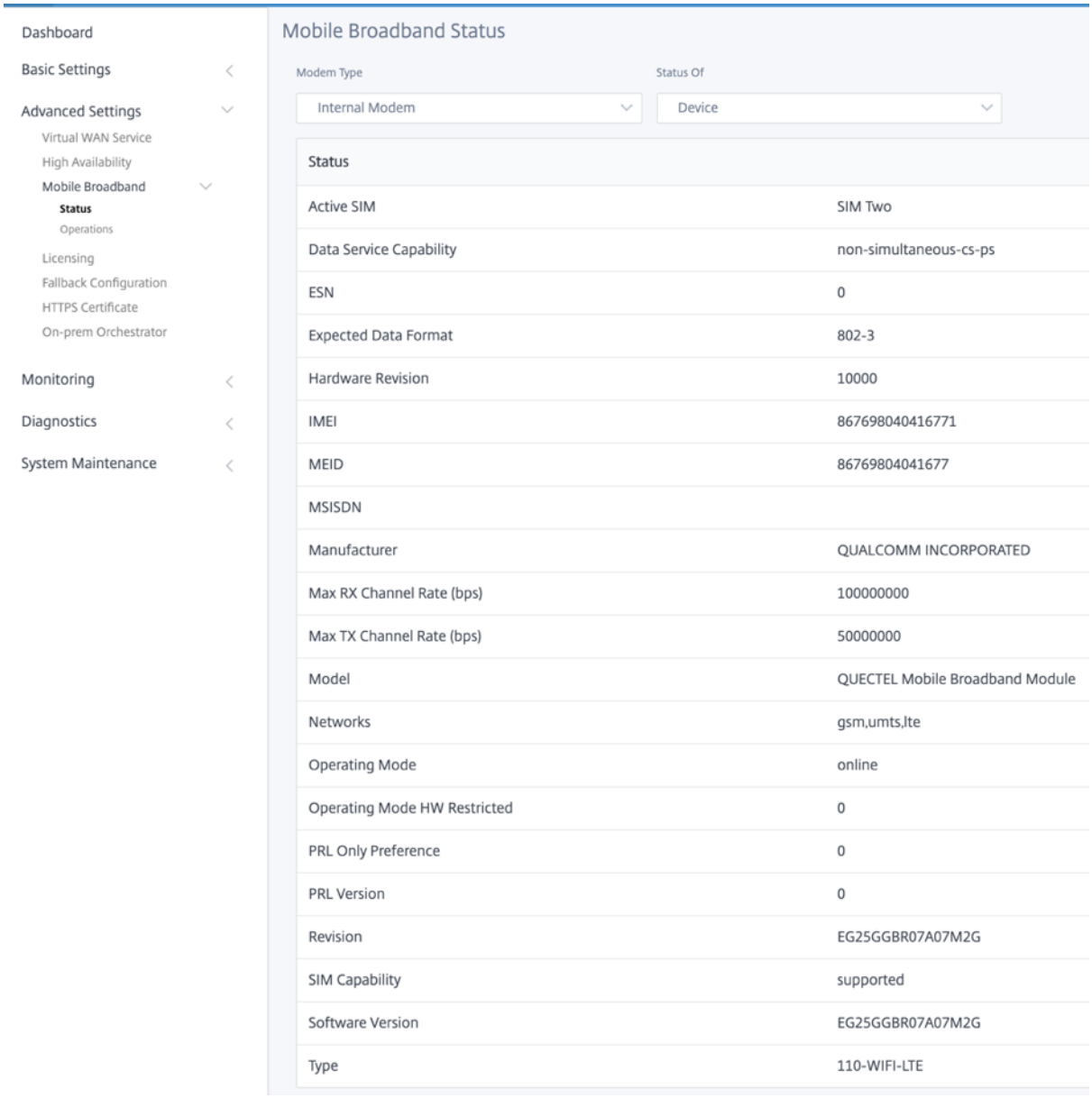
> 注意：
>
> Citrix SD-WAN 110-LTE-WiFi 设备具有两个标准 (2FF) SIM 插槽。要使用微型（3FF）和纳米（4FF）大小的 SIM 卡，请使用 SIM 适配器。将较小的 SIM 卡扣入适配器。您可以从 Citrix 获取适配器作为现场可更换单元 (FRU) 或从 SIM 提供程序获取适配器。仅在 Citrix SD-WAN 110-LTE-WiFi 设备上支持对内部 LTE 调制解调器进行热交换。

外部 LTE 调制解调器的配置：

- 使用支持的 USB LTE 转换器。支持的加密狗硬件型号是 Verizon USB730L 和 AT & T USB800。
- 确保将 SIM 卡插入 USB LTE 转换器。CDC 以太网 LTE 转换器预配置了静态 IP 地址，如果未插入 SIM 卡，则会干扰配置并导致连接故障或间歇性连接。
- 将 CDC 以太网 LTE 转换器插入 SD-WAN 设备之前，请将外部 USB 棒连接到 Windows /Linux 计算机，并确保 Internet 正常工作，使用正确的 APN 和移动数据漫游配置。确保 USB 加密狗的 连接模式 已从默认值“手动”更改为“自动”。

> 注意
>
> - Citrix SD-WAN 设备一次只支持一个 USB LTE 转换器。如果插入了多个 USB 转换器，请拔下所有转换器，然后仅插入一个转换器。
> - Citrix SD-WAN 设备不支持 USB 调制解调器的用户名和密码。确保在安装过程中禁用了调制解调器上的用户名和密码功能。
> - 拔下或重新启动外部 MBM 转换器会影响内部 LTE 调制解调器数据会话。这是预期的行为。
> - 插入外部 LTE 调制解调器时，SD-WAN 设备需要大约 3 分钟才能识别它。

要查看移动宽带状态，请选择调制解调器类型。

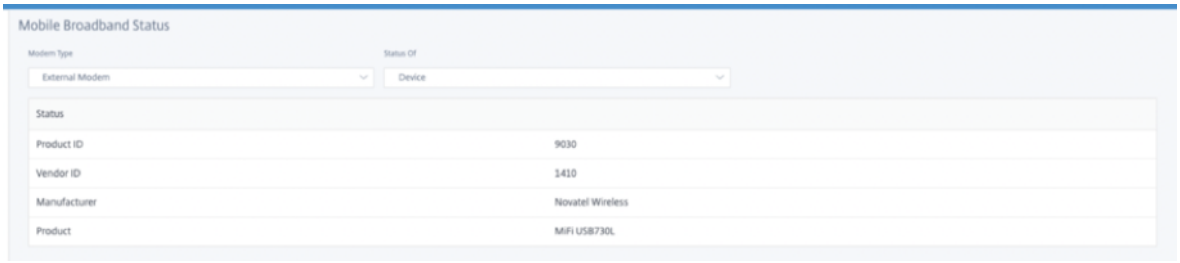


以下是一些有用的状态信息：

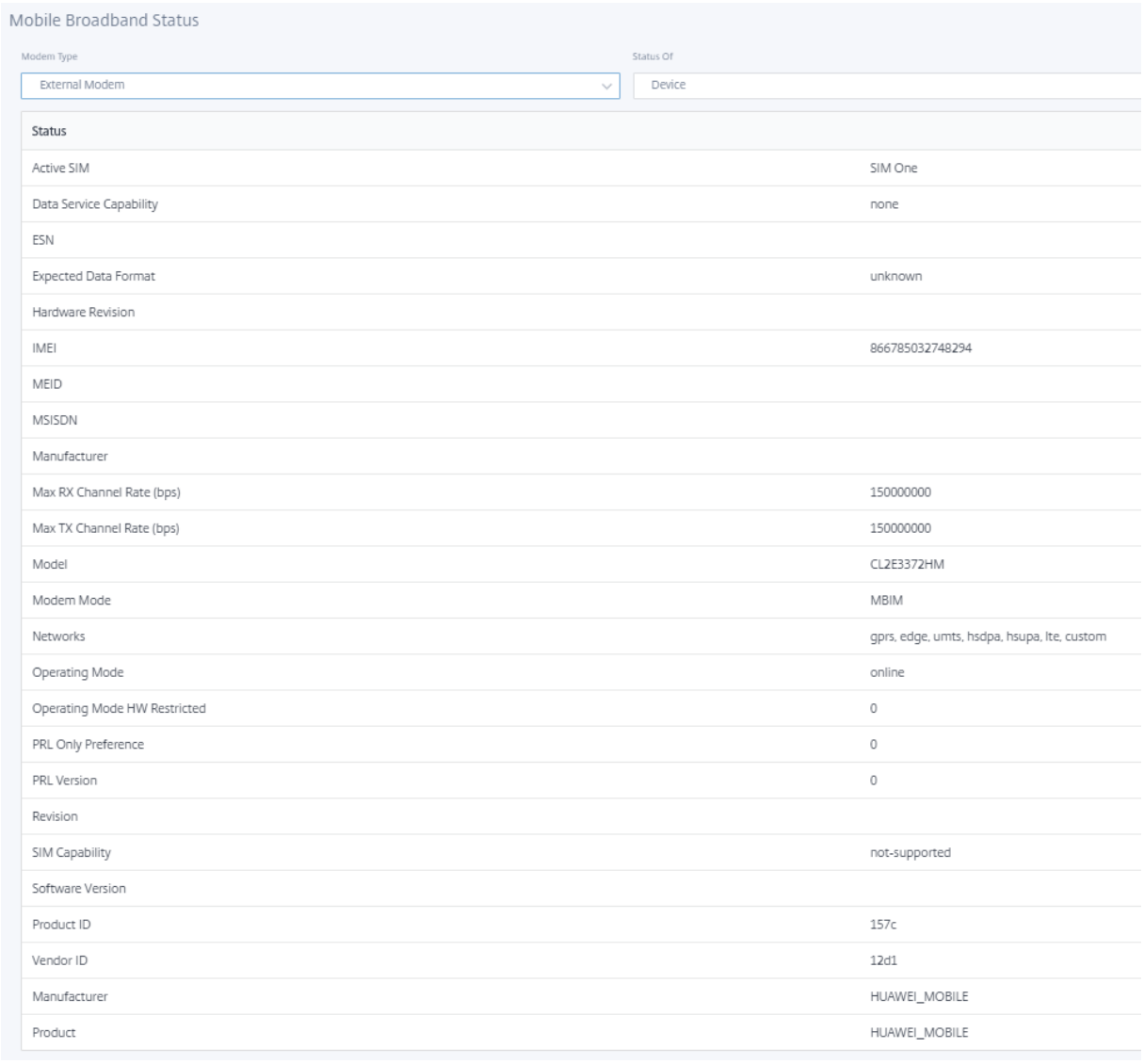
- 调制解调器类型：选择调制解调器类型为外部或内部内部调制解调器在 移动宽带 **>** 状态页面下显示状态。所有其他部分，例如 SIM 首选项、APN 设置、启用/禁用调制解调器、重启调制解调器和刷新 SIM 卡在 移动宽带 **>** 操作页面下提供。
- 活动 **SIM** 卡：在任何给定时间，只能有一个 SIM 卡处于活动状态。显示当前处于活动状态的 SIM 卡。
- 操作模式：显示调制解调器状态。
- **SIM** 功能：显示 SIM 卡是否受支持。
- 型号：显示移动宽带模块名称。

如果选择 外 部调制解调器，它将显示外部调制解调器的状态。但是，如果未配置外部调制解调器，则会显示警告消息，因为 此设备上未配置选定的调制解调器。

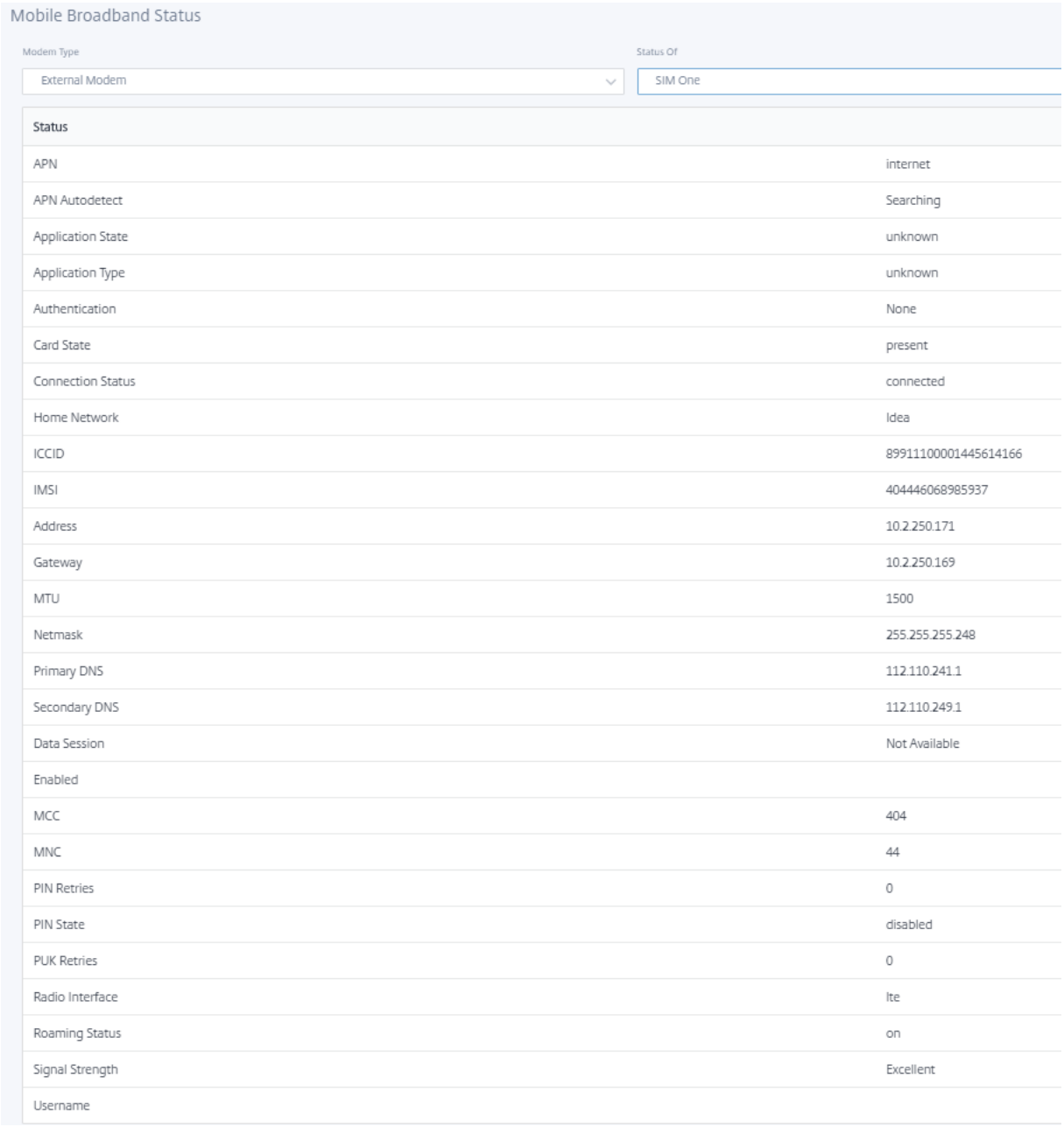
CDC 以太网外部调制解调器的设备详细信息。



MBIM 和 NCM 外部调制解调器的设备详细信息。调制解调器模式 字段显示外部转换器类型。



SIM 详细信息仅针对 MBIM 和 NCM 外部调制解调器显示。



移动宽带运营　内部和外部调制解调器支持的操作：

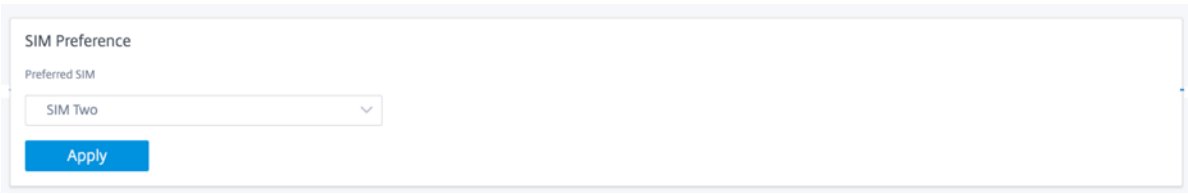
操作	调制解调器	外部调制解调器-CDC 以太网	外部调制解调器-MBIM 和 NCM
SIM 卡首选项	是-适用于支持双 SIM 卡的装置	否	否
SIM PIN	是	否	否
APN 设置	是	否	是

操作	调制解调器	外部调制解调器-CDC 以太网	外部调制解调器-MBIM 和 NCM
网络设置	是	否	否
漫游	是	否	否
管理固件	是	否	否
启用/禁用调制解调器	是	否	是
重启调制解调器	是	否	否
刷新 SIM 卡	是	否	否

SIM 卡首选项　您可以在 Citrix SD-WAN 110-LTE-WiFi 设备上插入双 SIM。在任何给定时间，只有一个 SIM 卡处于活动状态。选择 S **IM** 首选项：

- 首选 **SIM** 卡 **1**：如果插入了两张 SIM 卡，启动时 LTE 调制解调器将使用 SIM 卡 1（如果有）。LTE 调制解调器启动并运行时，它将使用当时可用的任何 SIM 卡（SIM 卡 1 或 SIM 卡 2），并将继续使用它，直到 SIM 处于活动状态。
- 首选 **SIM 2**：如果插入两个 SIM 卡，则在启动时 LTE 调制解调器使用 SIM Two（如果可用）。LTE 调制解调器启动并运行时，它将使用当时可用的任何 SIM 卡（SIM 卡 1 或 SIM 卡 2），并将继续使用它，直到 SIM 处于活动状态。
- **SIM** 卡 **1**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM 卡 1。SIM 卡 1 始终处于活动状态。
- **SIM Two**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM 卡二。SIM 卡二始终处于活动状态。

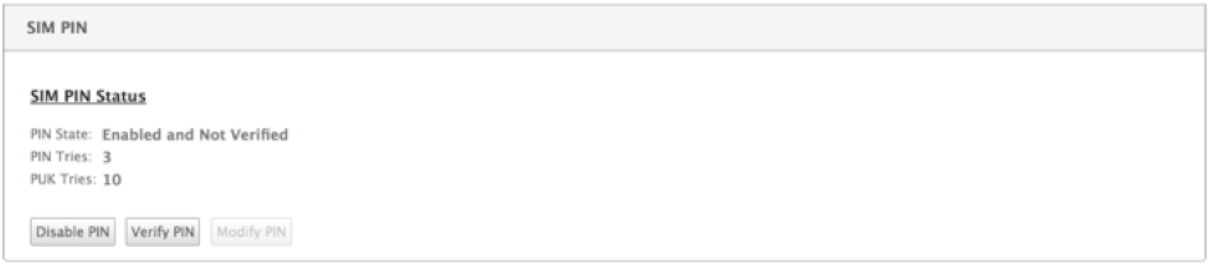
> 注意：
>
> Citrix SD-WAN 210-SE LTE Wi-Fi 设备不可用“SIM 首选项”选项，因为它只有一个 SIM 卡插槽。



SIM PIN

如果您插入了使用 PIN 锁定的 SIM 卡，则 SIM 卡状态为“已 启用”和“未验证”状态。在使用 SIM 卡进行验证之前，您无法使用 SIM PIN。您可以从运营商处获取 SIM PIN。

要执行 SIM PIN 操作，请导航到 高级设置 **>** 移动宽带 **>** 操作 **> SIM PIN** 状态。



您可以执行以下操作：

- 验证 **SIM PIN** 码：单击 验证。输入运营商提供的 SIM PIN，然后单击验证。状态更改为 已启用 和 已验证。
- 启用 **SIM PIN**：可以为禁用了 SIM PIN 的 SIM 卡启用 SIM PIN。Click **Enable**。输入运营商提供的 SIM PIN，然后单击启用。如果 SIM PIN 状态更改为已启用和未验证，则表示 PIN 未验证，在验证 PIN 之前，您无法执行任何 LTE 相关操作。单击 **Verify**（验证）。输入运营商提供的 SIM PIN，然后单击验证。
- 禁用 **SIM PIN**：您可以选择禁用已启用并验证 SIM PIN 的 SIM 卡的 SIM PIN 功能。单击禁用。输入 SIM PIN，然后单击禁用。
- 修改 **SIM PIN**：PIN 处于“已启用”和“已验证”状态后，您可以选择更改 PIN。单击 **Modify**（修改）。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 **Modify**（修改）。
- 解锁 **SIM** 卡 -如果您忘记了 SIM PIN 码，则可以使用从运营商处获得的 SIM PUK 重置 SIM PIN 码。要取消阻止 SIM 卡，请单击 取消阻止。输入从运营商处获取的 SIM PIN 和 SIM 卡 PUK，然后单击解除封锁。

  > 注意：
  >
  > 在解锁 SIM 卡的同时，SIM 卡会被永久阻止，PUK 尝试 10 次失败。请联系运营商以获取新的 SIM 卡。

APN 设置

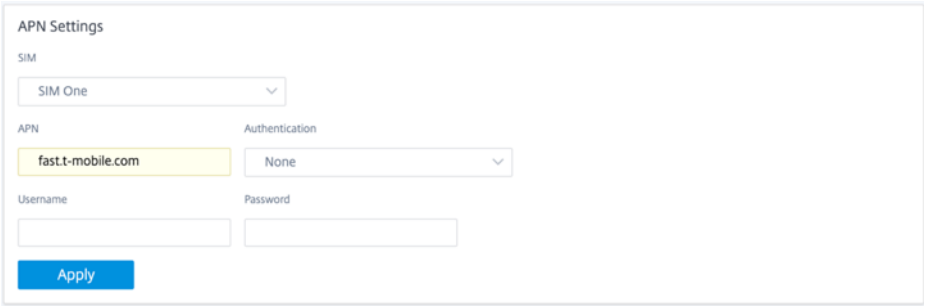
1. 要配置 APN 设置，请导航到 高级设置 **>** 移动宽带 **>** 操作 **>** 然后转到 **APN** 设置 部分。

   > 注意
   >
   > 从运营商处获取 APN 信息。

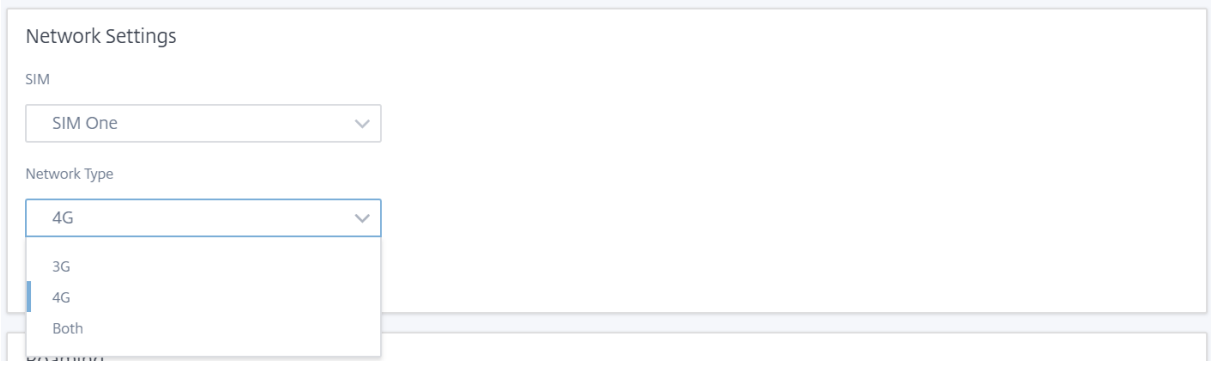
2. 选择 SIM 卡，输入运营商提供的 **APN**、用户名、密码 和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。

   > 注意
   >
   > 所有这些字段都是可选的。

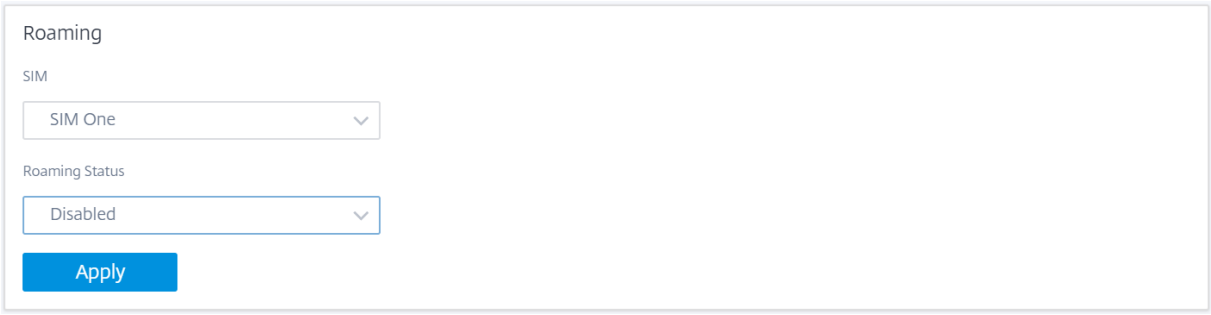
3. 单击应用。



网络设置　您可以在支持内部 LTE 调制解调器的 Citrix SD-WAN 装置上选择移动网络。支持的网络包括 3G、4G 或两者。



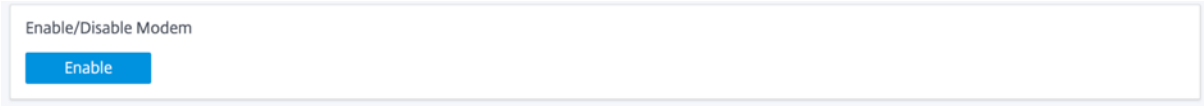
漫游　默认情况下，LTE 设备上启用漫游选项，您可以选择禁用它。



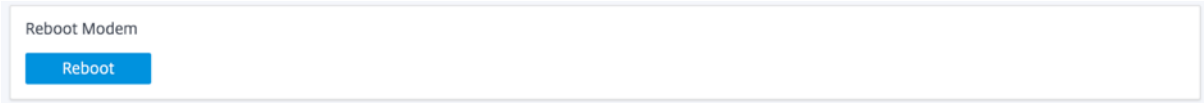
管理固件

每个启用 LTE 的装置都有一组可用的固件。您可以从现有的固件列表中选择或上载固件并应用它。如果您不确定要使用哪个固件，请选择 **AUTO-SIM** 选项。自动 SIM 选项允许 LTE 调制解调器根据插入的 SIM 卡选择最匹配的固件。

启用/禁用调制解调器　启用/禁用调制解调器，具体取决于您使用 LTE 功能的意图。默认情况下，LTE 调制解调器处于启用状态。

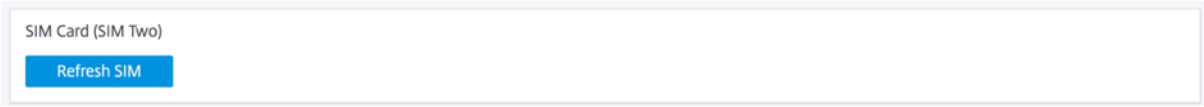


重启调制解调器　重新启动调制解调器。重新启动操作最多可能需要 7 分钟才能完成。



刷新 **SIM** 卡　如果 LTE-WiFi 调制解调器未正确检测到 SIM 卡，请使用 刷新 SIM 卡选项。

> 注意
>
> “刷新 SIM 卡”操作仅适用于活动的 SIM 卡。



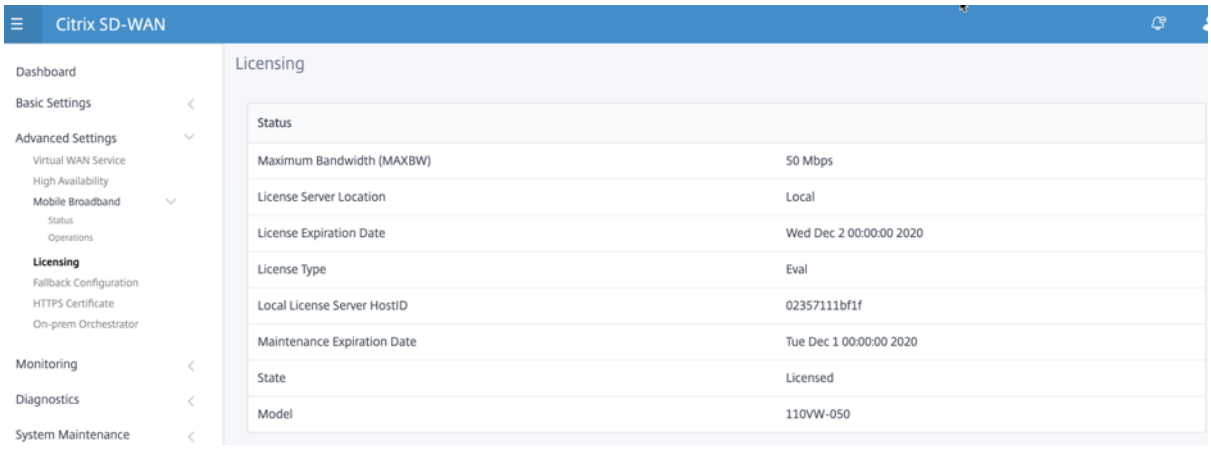
您可以使用 Citrix SD-WAN 中心远程查看和管理网络中的所有 LTE 站点。有关更多信息，请参阅 远程 LTE 站点管理。

有关 LTE 配置的更多信息，请参阅 在 110-LTE-WiFi 设备上 配 置 LTE 功能和在 210 SE LTE 设备上配置 LTE功能。

有关配置外部 LTE 调制解调器的信息，请参阅 配置外部 USB LTE 调制解调器

许可

许 可页面显示许可证详细信息，例如服务器位置、型号、许可证类型等。

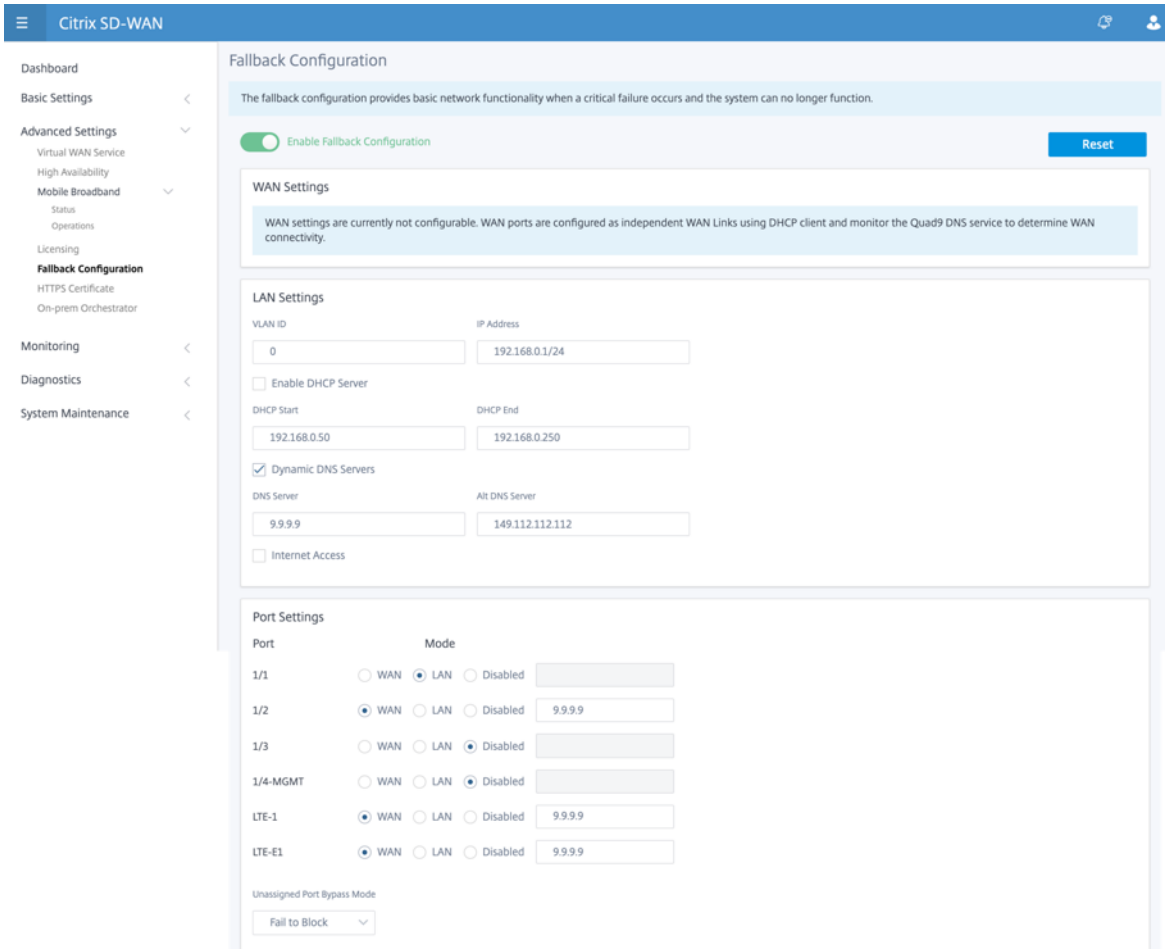


> 注意：
>
> 在安装和应用 SD-WAN Center 中的许可证时，请确保您的特定设备支持要启用的 SD-WAN 设备版本，并且可

> 用的软件版本正确。

默认/备用配置

“默认/回退配置”页显示存储的备用配置数据。如果禁用了回退配置，则可以通过打开启用 回退配置开关来启用 它。

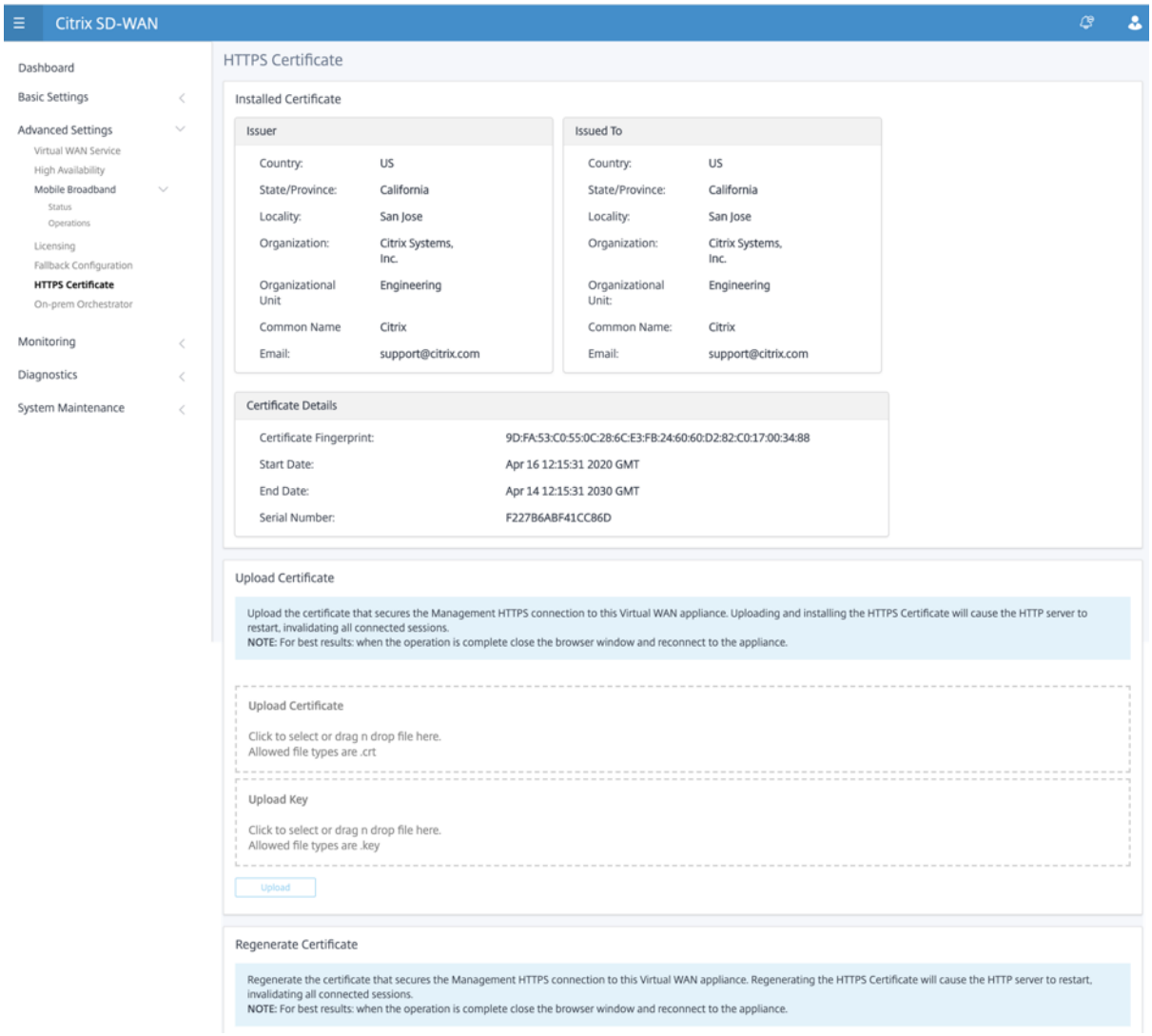


> 注意
>
> LTE 接口不能配置静态 IP 地址。

有关详细信息，请参阅 默认/回退配置。

HTTPS 证书

建立安全连接需要 HTTPS 证书。**HTTPS** 证书 页面显示已安装的 HTTPS 证书的详细信息。有关更多信息，请参阅 HTTPS 证书。



本地管弦乐器

Citrix 内部部署 SD-WAN Orchestrator 是 Citrix SD-WAN Orchestrator 服务的内部部署软件版本。Citrix On-PREM SD-WAN Orchestrator 为 Citrix 合作伙伴提供了一个单一窗格管理平台，通过适当的基于角色的访问控制集中管理多个客户。

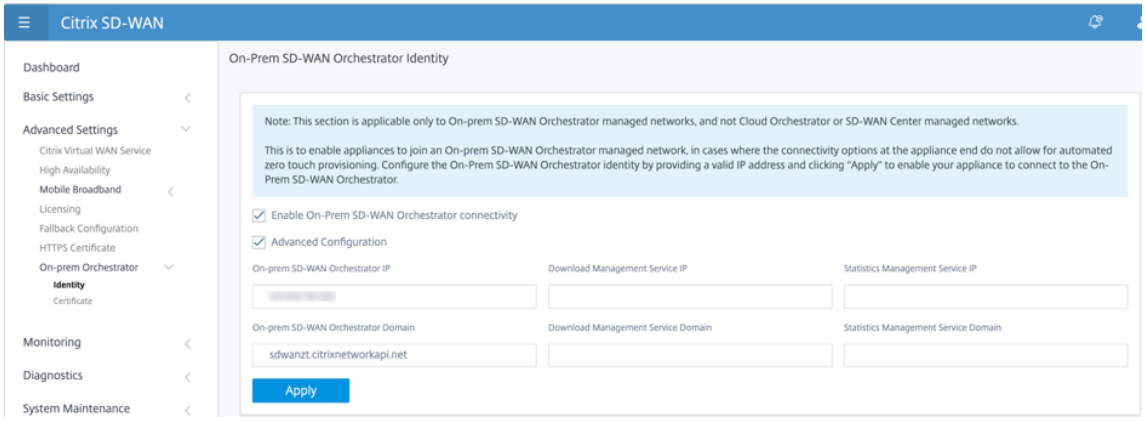
您可以通过启用 Orchestrator 连接并指定内部 PREM SD-WAN 协调器标识，在 Citrix SD-WAN 设备和 Citrix On-PREM SD-WAN 协调器之间建立连接。

> 注意
>
> - SD **-WAN** 设备上的本地 **SD-WAN Orchestrator** 配置 是 Citrix on-prem SD-WAN Orchestrator 的启用因素。SD-WAN 设备上的 Citrix 本地 SD-WAN Orchestrator 配置目前不可用。它的目标是将来的版本。

> • 如果在 SD-WAN 设 备上配置了 **SD-WAN** 设备上的本地 **SD-WAN Orchestrator** 配置，则零接触部署将不起作用。

要启用编排器连接：

1. 在设备 GUI 中，导航到 高级设置 **>** 本地 **Orchestrator >** 身份。
2. 选中 启用本地 **SD-WAN Orchestrator** 连接 复选框。



3. 输入内部部署 SD-WAN Orchestrator IP 地址或域或两者（IP 地址和域）以进行配置。

   如果客户只配置域，则必须确保在其本地 DNS 服务器中添加 DNS 记录，并且必须在 SD-WAN 设备上配置 DNS 服务器 IP 地址。要配置，请导航到 配置 **>** 网络适配器 **> IP** 地址。

   例如，如果内部 PREM SD-WAN Orchestrator 域配置为 citrix.com。，则必须在 DNS 服务器中为以下 FQDN 和内部部署 SD-WAN 编排器 IP 地址创建 DNS 记录：

   - download.citrix.com
   - sdwanzt.citrix.com
   - sdwan-home.citrix.com

   在高级配置的情况下：

   例如：如果本地 Orchestrator 域配置为 **citrix.com**，则下载管理服务域将配置为 **download.citrix**.com，并且统计管理服务域配置为 **statistics.citrix.com**。然后，您必须在 DNS 服务器中为下面的 FQDN 和相应的 IP 地址创建 DNS 记录：

   - download.citrix.com
   - sdwanzt.citrix.com
   - statistics.citrix.com

   On-Prem Orchestrator 可能支持正在运行的服务，如下载、独立服务器实例上的统计信息，以便为大型网络提供更好的可扩展性。您可以选择 高级配置并配置 下 载管理服务和统计管理 服务。

   选中“高级配置”复选框并提供以下详细信息：

- 下载管理服务 **IP/Domain**：提供有助于将 SD-WAN 软件和配置下载方面卸载的 IP 地址/域到独立的服务器实例，以便为大型网络提供更好的可扩展性。
- 统计管理服务 **IP/Domain**：提供有助于将 SD-WAN 统计信息的收集和管理从设备转移到独立服务器实例的 IP 地址/域，从而为大型网络提供更好的可扩展性。

4. 单击应用。

   要重新生成、下载和上传 SD-WAN 设备或本地 SD-WAN Orchestrator 证书，请导航到 高级设置 **>** 本地 **Orchestrator >** 证书。

   如果禁用了本地 Orchestrator 身份验证类型，设备可以通过无身份验证或单向身份验证模式或双向身份验证模式连接到本地 Orchestrator。

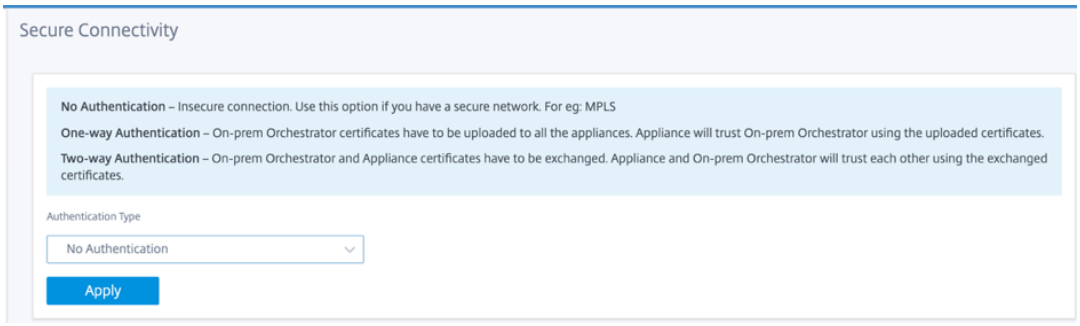
   如果启用了 Onprem Orchestrator 身份验证类型，则设备只能通过 双向身份验证连接到 Onprem Orchestrator。

   在将 on-prem Orchestrator 中的 身份验证类型 从启用状态禁用时，处于单向身份验证模式的现有设备将进入断开连接状态。客户必须将设备身份验证类型更改为双向身份验证，然后将 SD-WAN 设备证书上传到本地 PREM Orchestrator 才能连接。

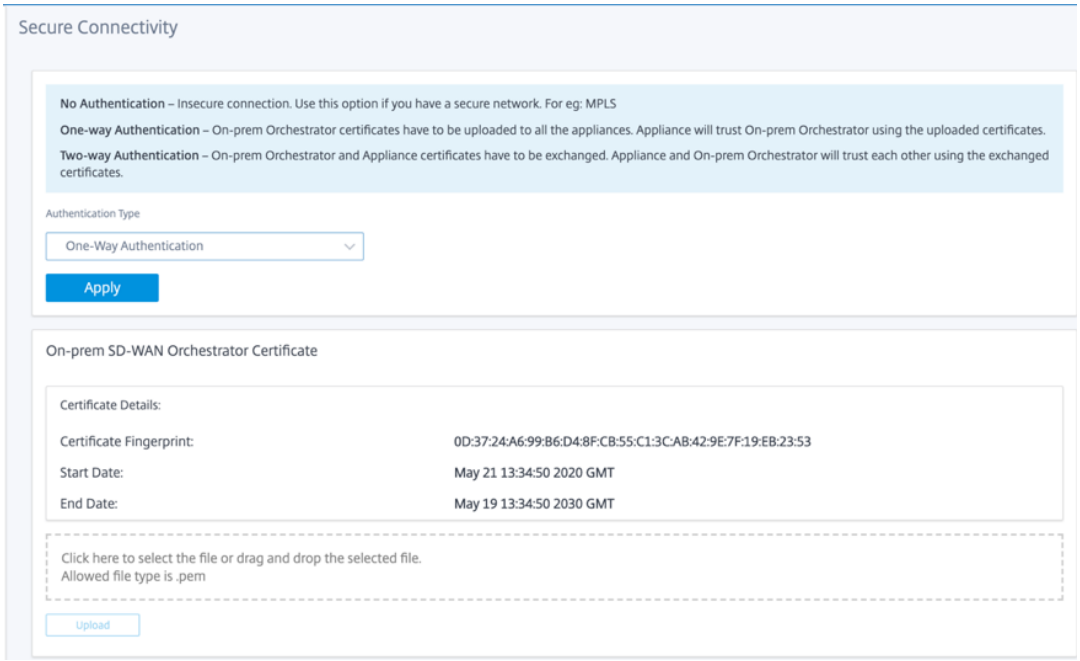
   > 注意
   >
   > - 生成的证书是 X509 自签名证书。
   > - 如果证书过期或破坏，客户必须重新生成证书。
   > - 证书的有效期为 10 年。
   > - 您可以查看证书详细信息，如指纹、开始日期和结束日期
   > - 客户必须确保在 On-PREM Orchestrator 和 SD-WAN 设备之间重新生成并交换证书，以避免设备与 ON-PREM 编排器的连接丢失。

5. 选择 身份验证类型。以下是 SD-WAN 设备和内部 PREM SD-WAN Orchestrator 连接之间支持的身份验证类型：

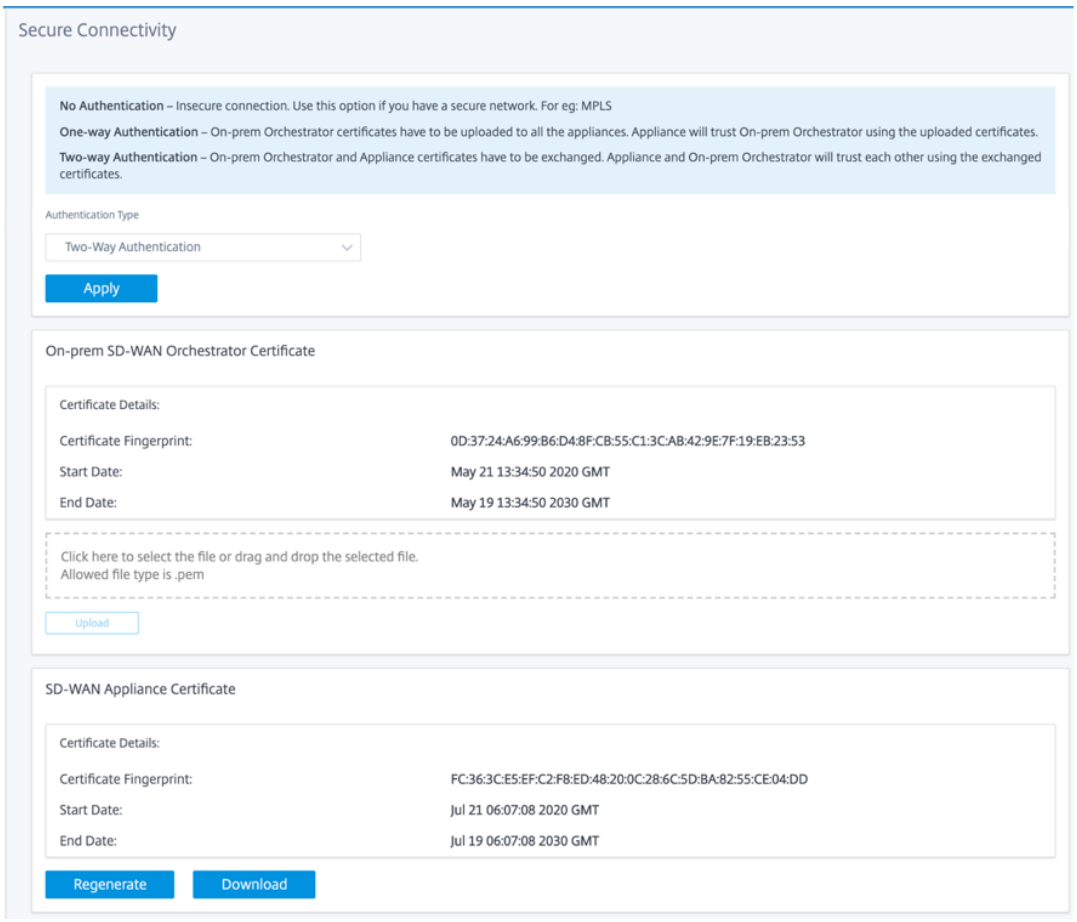
   - 无身份验证—在本地 SD-WAN Orchestrator 和 SD-WAN 设备之间不进行身份验证，也无需使用 SD-WAN 设备或本地 SD-WAN Orchestrator 证书。但是，如果您有一个安全的网络，如 MPLS，则可以使用此选项。

   - 单向身份验证—在选择单向身份验证类型时，必须上传本地 Orchestrator 证书。从本地业务编排器下载本地 PREM 业务流程，然后单击“上载”。SD-WAN 设备使用上传的证书信任本地 PREM 协调器。



- 双向身份验 证—必须彼此交换本地 Orchestrator 和设备证书。对于 双向身份验证，您必须在本地 Orchestrator 上重新生成、下载和上传 SD-WAN 设备证书。SD-WAN 设备和 On-PREM Orchestrator 使用交换的证书相互信任。



> 注意
>
> 建议仅使用单向身份验证或双向身份验证。如果没有身份验证，则必须选择安全 DNS 服务器。

要禁用本地 SD-WAN Orchestrator 连接，请清除 启用本地 **SD-WAN Orchestrator** 连接，然后单击 应用。要将本地 PREM 编排器托管网络转换为云编排器或 MCN 托管网络，您需要禁用内部 PREM SD-WAN Orchestrator 连接，并且必须执行配置重置。要重置配置，请导航到 配置 **>** 系统维护 **>** 配置重置。

升级和降级

- 将 SD-WAN 装置从 11.1.1/11.2.0/10.2.7 升级到 11.2.1 软件版本之后，您必须同时交换装置证书和本地编排器证书。
- 将 SD-WAN 设备从 11.2.1 降级到 11.1.1/11.2.0/10.2.7 软件版本后，必须在 Citrix SD-WAN 设备用户界面上再次应用身份设置。如果出现与本地 SD-WAN Orchestrator 配置或 SD-WAN 装置连接相关的问题，请禁用本 SD-WAN Orchestrator 连接，然后再次启用本地 SD-WAN 协调器连接。

必须禁用本 地 SD-WAN Orchestrator 身份验证类型 才能管理运行 10.2.7/11.1.1/11.2.0 软件版本的 SD-WAN 设备。

监视

在“华北事故”部分下，您可以查看地址解析协议 **(ARP)**、路由、以太网、以太网 **MAC** 统计信息以及 **DHCP** 客户端 **WAN** 链路、**SLAAC WAN** 链路、**DHCP** 服务器/中继、防火墙连接、流量和 **DNS** 统计信息。

- **ARP**、路由、以太网和以太网 **MAC** 统计：您可以看到 ARP、路由、以太网和以太网 MAC 的统计信息。使用统计信息，您可以验证任何流量或接口错误。有关详细信息，请参阅 查看统计信息。
- **DHCP** 客户端 **WAN** 链接：DHCP 客户端 WAN 链接页面提供了学习 IP 的状态。您可以请求续订 IP，这会刷新租约时间。您还可以选择 发布续订，这将发布新的 IP 地址与新租约。有关更多详细信息，请参阅 监视 DHCP 客户端 WAN 链接。
- **SLAAC WAN** 链接：SLAAC WAN 链接页面提供了 SLAAC 分配给虚拟接口的 IPv6 地址的详细信息。您还可以选择“发布续订”以允许 SLAAC 向 IPv6 客户端分配新的 IP 地址或具有新租约的相同 IP 地址。
- **DHCP** 服务器/中继：您可以将 SD-WAN 设备用作 DHCP 服务器或 DHCP 中继代理。
  - DHCP 服务器功能允许与 SD-WAN 设备的 LAN/WAN 接口位于同一网络中的设备从 SD-WAN 设备获取其 IP 配置。
  - 通过 DHCP 中继功能，您的 SD-WAN 设备可以在 DHCP 客户端与服务器之间转发 DHCP 数据包。

  有关详细信息，请参阅 DHCP 服务器和 DHCP 中继。
- 防火墙连接：防火墙连接 页面提供防火墙连接统计信息。您可以查看防火墙策略如何对每个应用程序的流量进行操作。有关详细信息，请参阅查看防火墙统计信息。
- 流：流部分提供了查看虚拟 WAN 流信息的基本说明。有关详细信息，请参阅 查看流程信息。
- **DNS** 代理统计信息：此页提供有关已配置 DNS 代理的详细信息。单击 刷新 以获取当前数据。有关详细信息，请参阅 域名系统。

诊断

诊断 部分提供了测试和调查连接问题的选项。有关详细信息，请参阅 诊断。

> 注意：
>
> 对于 Citrix SD-WAN 110 设备，一次只能存在一个诊断程序包。对于 Citrix SD-WAN 210 装置，最多允许五个诊断程序包。

系统维护

使用“系统维护”部分执行维护活动。“系统维护”页包含以下选项：

- 删除文件：您可以删除日志文件、备份文件和存档数据库。从下拉菜单中选择要删除的文件，然后单击删除按钮。
- 重新启动系统：您可以重新启动虚拟 WAN 服务或重新启动系统。

- 本地变更管理：本 地更改管理 流程允许您将新的设备包上载到此单独的装置。
- 配置重置：您可以重置配置。此选项可清除此设备上的用户数据、日志、历史记录和本地配置数据。
- 恢复出厂设置：使用恢复出厂设置选项将 SD-WAN 设备重置为已发货的版本。

> 注意
>
> 所有这些功能已在现有的 SD-WAN 文档中详细说明。

不受支持的平台

新 UI 不支持以下 SD-WAN 设备：

- Citrix SD-WAN 1000 SE /PE
- Citrix SD-WAN 2000 SE /PE
- Citrix SD-WAN 4000 SE

Citrix SD-WAN 11.5 版本升级影响

September 2, 2022

- Citrix SD-WAN 11.5.0 是有限可用性版本，仅针对特定的客户/生产部署推荐和支持。
- SD-WAN 11.5.0 版本不支持高级版 (AE)、高级版 (PE)、广域网优化部署。
- SD-WAN 11.5.0 仅支持 SD-WAN 平台模型和软件包中提到的平台。
- SD-WAN 11.5.0 不支持适用于本地的 Citrix SD-WAN Center 或 Citrix SD-WAN Orchestrator。
- Citrix 下载页面上没有 SD-WAN 11.5.0 固件。
- SD-WAN 11.5.0 版本只能通过 Citrix SD-WAN Orchestrator 服务提供，并且仅在选定的地理位置 POP 上提供。
- 在任何生产网络上部署 11.5.0 之前, 请确保获得 Citrix 产品管理/Citrix 支持部门所需的批准和指导。

系统要求

September 2, 2022

硬件要求

设置 SD-WAN 设备中提供了安装 SD-WAN 设备的说明。

固件要求

虚拟广域网环境中的所有 Citrix SD-WAN 设备型号都需要运行相同的 Citrix SD-WAN 固件版本。

> 注意
>
> 运行早期软件版本的设备无法与运行 SD-WAN 版本 11.4 的设备建立虚拟路径连接。有关更多信息，请与 Citrix 支持团队联系。

软件要求

从 SD-WAN 11.5 版本开始，SD-WAN 设备许可通过 Citrix SD-WAN Orchestrator 服务进行管理。有关许可要求的详细信息，请参阅 许可。

浏览器要求

浏览器必须启用 cookie，并且已安装并启用了 JavaScript。

以下浏览器支持 SD-WAN 管理 Web 界面：

- 火狐火狐 49+
- Google Chrome 51+
- 微软边缘 13 +

支持的浏览器必须启用 Cookie，并且已安装和启用 JavaScript。

虚拟机管理程序

可以在以下虚拟机管理程序上配置 Citrix SD-WAN SE/PE VPX：

- VMware ESXi 服务器、5.5.0 或更高版本。
- Citrix Hypervisor 6.5 或更高版本。
- Microsoft Hyper-V 2012 R2 或更高版本。
- Linux KVM

云平台

可以在以下云平台上配置 Citrix SD-WAN SE/PE VPX：

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

SD-WAN 平台模型

September 26, 2023

以下是受支持的 SD-WAN 标准版硬件设备型号：

SD-WAN SE 平台模型	角色
110-SE/110-LTE-WiFi/110-WiFi-SE	小分支机器
210-SE/210-SE LTE	小分支机器
1100-SE	大型分支设备
2100-SE	大型分支设备
4100-SE	数据中心-主控制节点 (MCN) 设备
5100-SE	数据中心-主控制节点 (MCN) 设备
6100-SE	数据中心-主控制节点 (MCN) 设备

SD-WAN VPX 虚拟设备（SD-WAN VPX-SE）

以下是受支持的 SD-WAN VPX 虚拟设备 (VPX-SE) 型号：

SD-WAN VPX-SE 平台模型	角色
VPX 20-SE	MCN 或客户端设备，小分支机构
VPX 50-SE	MCN 或客户端设备，小分支机构
VPX 100-SE	MCN 或客户端设备，小分支机构
VPX 200-SE	MCN 或客户端设备，小分支机构
VPX 500-SE	MCN 或客户端设备，小分支机构
VPX 1000-SE	MCN 或客户端设备，小分支机构

有关更多信息，请参阅 Citrix SD-WAN 虚拟 VPX 标准版的 先决条件 。

升级路径

September 2, 2022

下表提供了从以前版本升级到的所有 Citrix SD-WAN 软件版本的详细信息。

SD-WAN	11.1	11.0	10.2	10.1	10	9.3.5	9.3.4	9.3	9.2
SD-WAN 11.0	✓								
SD-WAN 10.2	✓	✓							
SD-WAN 10.1	✓	✓	✓						
SD-WAN 10	✓	✓	✓	✓					
SD-WAN 9.3.5	✓	✓	✓	✓	✓				
SD-WAN 9.3.4	—	—	—	—	—	✓			
SD-WAN 9.3	—	—	—	—	—	✓	✓		
SD-WAN 9.2	—	—	—	—	—	✓	✓	✓	
SD-WAN 9.1	—	—	—	—	—	✓	✓	✓	✓

Citrix 升级指南中还提供了升级路径信息。

> 注意
>
> - 建议从 Citrix SD-WAN 9.3.x 版本升级到 10.2.8 的客户在升级到任何主要版本之前升级到 10.2.8。
> - 在执行软件升级时，请确保在激活之前完成对所有连接站点的转移。如果通过启用“忽略未完成”在暂存完成之前完成激活，则对于仍在进行过渡的站点，虚拟路径可能不会显示 MCN。要恢复网络，需要手动对这些站点执行本地更改管理。
> - 从 Citrix SD-WAN 11.0.0 版开始，SD-WAN 软件的底层操作系统/内核将升级到较新版本。它需要在升级过程中执行自动重新启动。因此，升级每台设备的预计时间大约增加 100 秒。此外，通过包括新的操作系统，传输到每个分支设备的升级包的大小将增加约 90 MB。

配置

September 26, 2023

安装 SD-WAN 软件和 许可证后，可以 配置 SD-WAN 设备设置以开始管理网络和部署。

初始设置

对于要添加到 SD-WAN 的每个设备，必须完成这些过程。因此，此过程将需要与网络中的站点管理员进行某些协调，以确保设备已准备就绪并准备在适当的时间进行部署。但是，配置和部署主控制节点 (MCN) 后，您可以随时向 SD-WAN

添加客户端设备（客户端节点）。

对于要添加到虚拟 WAN 的每个设备，您需要执行以下操作。

1. 设置 SD-WAN 设备硬件和要部署的任何 SD-WAN VPX 虚拟设备 (SD-WAN VPX-VW)。
2. 设置设备的管理 IP 地址并验证连接。
3. 设置设备上的日期和时间。
4. 将控制台会话 超时 阈值设置为高值或最大值。

   > 警告
   >
   > 如果控制台会话超时或您在保存配置之前注销管理 Web 界面，则任何未保存的配置更改都将丢失。然后，您必须重新登录到系统，并从头开始重复配置过程。因此，强烈建议您在创建或修改配置包或执行其他复杂任务时将控制台会话 超 时间隔设置为较高的值。

5. 在设备上上载并安装软件许可证文件。

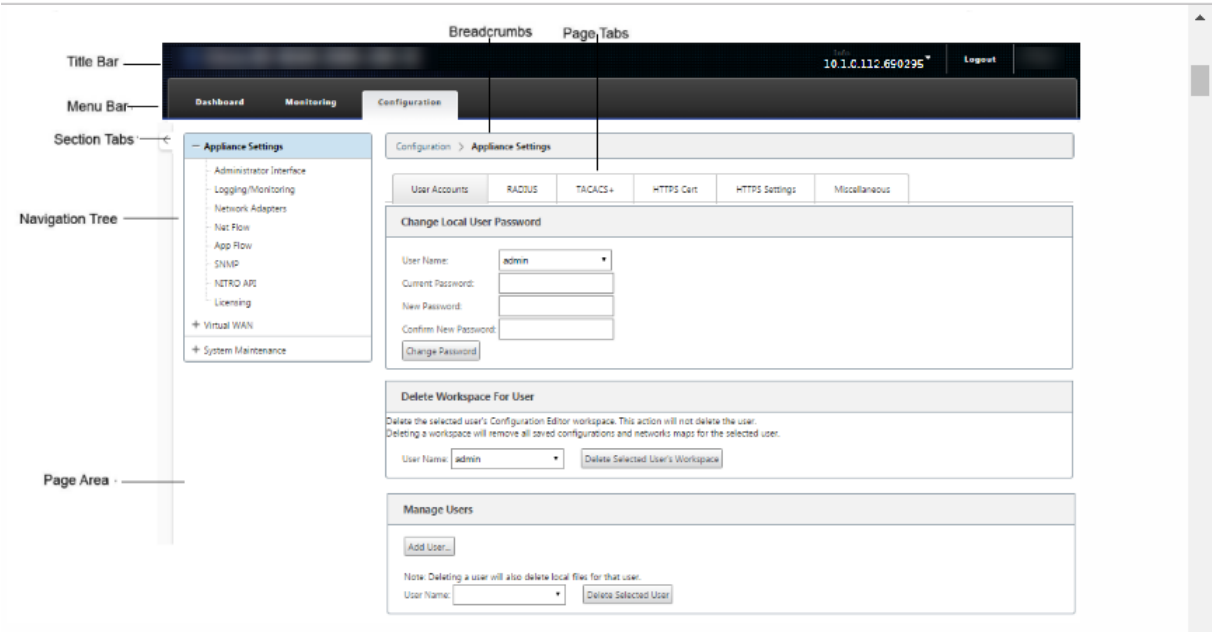
有关安装 SD-WAN 虚拟设备 (SD-WAN VPX) 的说明，请参阅以下部分：

- 关于 SD-WAN VPX。
- 在 ESXi 上安装和部署 SD-WAN VPX-SE。

Web 界面 (UI) 布局概述

本节提供基本导航说明和 SD-WAN Web 管理界面页层次结构的导航路由图。

基本导航　下图概述了 Web 管理界面的基本导航元素以及用于识别它们的术语。



基本导航元素如下所示：

- 标题栏—显示装置型号、装置的主机 IP 地址、装置上当前运行的软件包版本以及当前登录会话的用户名。标题栏还包含用于终止会话的 注销 按钮。
- 主菜单栏—这是每个管理 Web 界面屏幕上标题栏下方显示的栏。这包含用于显示所选部分的导航树和页面的部分选项卡。
- 部分选项 卡—部分选项卡位于页面顶部的主菜单栏中。这些是 Web 管理界面页面和窗体的顶级类别。每个部分都有自己的导航树，用于在该部分中导航页面层次结构。单击分区选项卡以显示该部分的导航树。
- 导航树—导航树位于主菜单栏下方的左窗格中。这将显示部分的导航树。单击分区选项卡以显示该部分的导航树。导航树提供以下显示和导航选项：
  - 单击部分选项卡以显示该部分的导航树和页面层次结构。
  - 单击树中某个分支旁边的 +（加号）以显示该分支主题的可用页面。
  - 单击页面名称可在页面区域中显示该页面。
  - 单击分支项目旁边的—（减号）以关闭分支。
- 面包屑—显示当前页面的导航路径。痕迹导航位于页面区域的顶部，正好位于主菜单栏下方。活动导航链接以蓝色字体显示。当前页面的名称以黑色粗体显示。
- 页面区域—这是所选页面的页面显示和工作区域。在导航树中选择一个项目以显示该项目的默认页面。
- 页面选项卡—某些页面包含用于显示该主题或配置表单的更多子页面的选项卡。它们位于页面区域的顶部，正好位于痕迹导航显示的下方。有时（与“更改管理”向导一样），选项卡位于页面区域的左窗格中，位于导航树和页面工作区之间。
- 调整页面区域大小—对于某些页面，您可以增大或缩小页面区域（或其部分）的宽度，以显示表格或表单中的更多字段。在这种情况下，页面区域窗格、窗体或表格的右边框上有一个灰色的垂直调整大小条。将光标滚到调整大小栏上，直到光标变为双向箭头。然后单击并向右或向左拖动条以增大或缩小区域宽度。

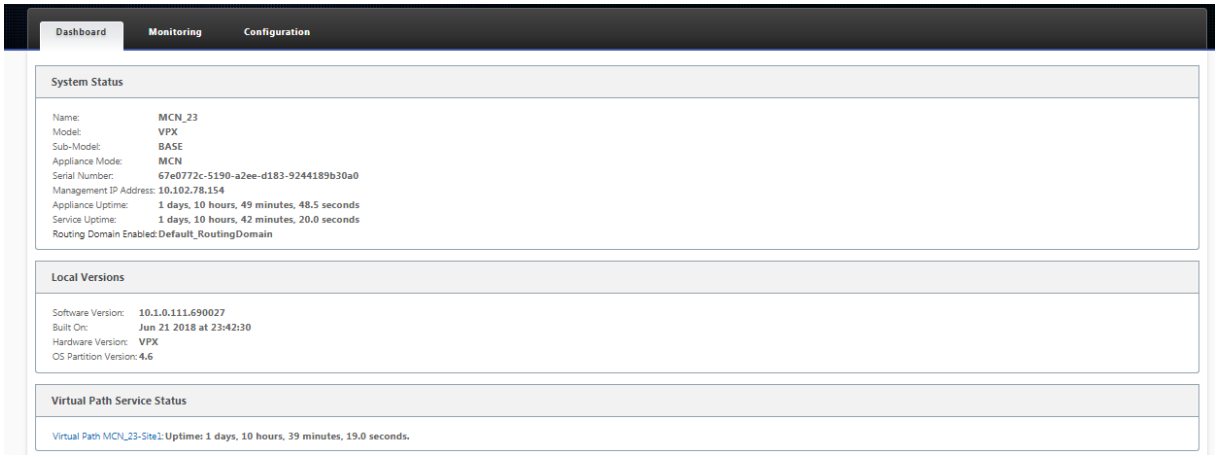
  如果调整大小栏不可用于某一页面，可以单击并拖动浏览器的右侧边缘以显示完整的页面。

Web 管理界面控制板　单击 控制板 部分选项卡以显示本地设备的基本信息。

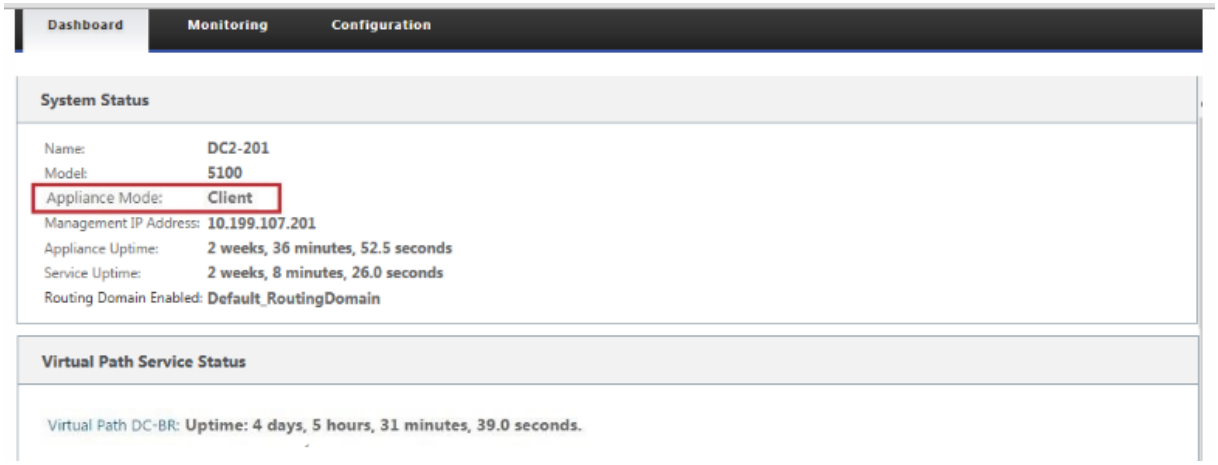
控制板 页面显示设备的以下基本信息：

- 系统状态
- 虚拟路径服务状态
- 本地设备软件包版本信息

下图显示了主控制节点 (MCN) 装置 仪表板 显示示例。



下图显示了客户端设备控制板显示示示例。



设置设备硬件

要设置 Citrix SD-WAN 设备硬件（物理设备），请执行以下操作：

1. 设置底盘。

   Citrix SD-WAN 设备可以安装在标准机架中。对于桌面安装，请将机箱放置在平坦的表面上。确保设备的侧面和背面至少有 2 英寸的间隙，以便适当通风。

2. 连接电源。

   a) 确保电源开关设置为关闭。
   b) 将电源线插入设备和交流插座。
   c) 按下设备前面的电源按钮。

3. 连接电源。

   a) 确保电源开关设置为关闭。

b) 将电源线插入设备和交流插座。
c) 按下设备前面的电源按钮。

4. 将设备管理端口连接到个人计算机。

您需要将设备连接到 PC，以准备完成下一步骤，设置设备的管理 IP 地址。

> 注意
>
> 连接设备之前，请确保 PC 上已启用以太网端口。使用以太网电缆将 SD-WAN 设备管理端口连接到个人计算机上的默认以太网端口。

SD-WAN VPX-SE 管理端口　SD-WAN VPX-SE 虚拟设备是虚拟机，因此没有物理管理端口。但是，如果在创建 VPX 虚拟机时没有为 SD-WAN VPX-SE 配置管理 IP 地址，则需要立即进行配置，如 配置 SD-WAN VPX-SE 的管理 IP 地址一节中所述。

SD-WAN VPX-SE 虚拟设备是虚拟机，因此没有物理管理端口。但是，如果在创建 VPX 虚拟机时没有为 SD-WAN VPX-SE 配置管理 IP 地址，则需要立即进行配置，如 配置 SD-WAN VPX-SE 的管理 IP 地址一节中所述。

配置管理 **IP** 地址

要启用对 SD-WAN 设备的远程访问，必须为该设备指定唯一的管理 IP 地址。为此，您必须首先将设备连接到 PC。然后，您可以在 PC 上打开浏览器并直接连接到设备上的管理 Web 界面，从而可以为该设备设置管理 IP 地址。每个设备的管理 IP 地址必须是唯一的。

Citrix SD-WAN 设备同时支持 IPv4 和 IPv6 协议。您可以配置 IPv4、IPv6 或两者（双堆栈）。当同时配置了 IPv4 和 IPv6 协议时，IPv4 协议优先于 IPv6 协议。

> 注意
>
> - 要在特定于功能的配置中配置 IPv4 或 IPv6 地址，请确保启用相同的协议并将其配置为管理接口协议。例如，如果要为 SMTP 服务器配置 IPv6 地址，请确保将 IPv6 地址配置为管理接口地址。
> - 不允许使用链路本地地址（以“fe80”开头的 IPv6 地址）。
> - 要配置 IPv6 地址，网络中必须有通告 IPv6 地址的路由器。

为硬件 SD-WAN 设备和 VPX 虚拟设备（Citrix SD-WAN VPX-SE）设置管理 IP 地址的过程不同。有关为每种类型的设备配置地址的说明，请参阅以下内容：

- **SD-WAN VPX** 虚拟设备—请参阅 [配置 SD-WAN VPX-SE 的管理 IP 地址和 SD-WAN VPX-SE 和 SD-WAN WANOP VPX 安装之间的区别] 部分。

要为硬件 SD-WAN 设备配置管理 IP 地址，请执行以下操作：

> 注意
>
> 必须对要添加到网络中的每个硬件设备重复以下过程。

1. 如果要配置硬件 SD-WAN 设备，请将设备物理连接到 PC。
   - 如果尚未这样做，请将以太网电缆的一端连接到设备上的管理端口，将另一端连接到 PC 上的默认以太网端口。

   > 注意
   >
   > 确保在用于连接到设备的 PC 上启用了以太网端口。

2. 记录您用于设置设备管理 IP 地址的电脑的当前以太网端口设置。

   在设置装置管理 IP 地址之前，必须更改 PC 上的以太网端口设置。请务必记录原始设置，以便在配置管理 IP 地址后还原它们。

3. 更改 PC 的 IP 地址。

   在电脑上，打开网络接口设置，并将电脑的 IP 地址更改为以下内容：
   - 192.168.100.50

4. 将电脑上的“子网掩码”设置更改为以下内容：
   - 255.255.0.0

5. 在电脑上，打开浏览器并输入设备的默认 IP 地址。在浏览器的地址行中输入以下 IP 地址：
   - 192.168.100.1

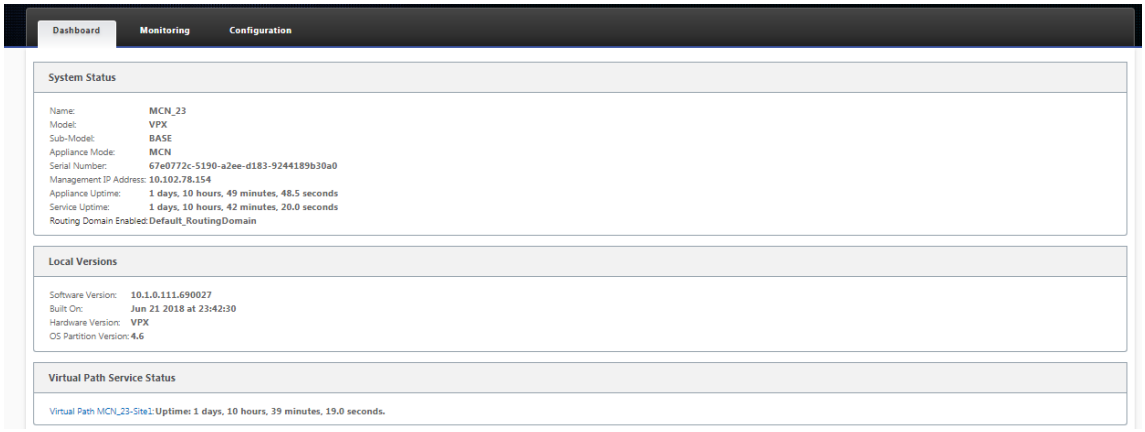
   > 注意
   >
   > 建议您在连接到 SD-WAN 设备时使用 Google Chrome 浏览器。
   >
   > 忽略管理 Web 界面的任何浏览器证书警告。

   这将在连接的设备上打开 SD-WAN 管理 Web 界面登录屏幕。

6. 输入管理员用户名和密码，然后单击 登录。
   - 默认管理员用户名：*admin*
   - 默认管理员密码：*password*

   > 注意
   >
   > 建议您更改默认密码。请务必在安全位置记录密码，因为密码恢复可能需要重置配置。

登录管理 Web 界面后，将显示 控制面板 页面，如下所示。



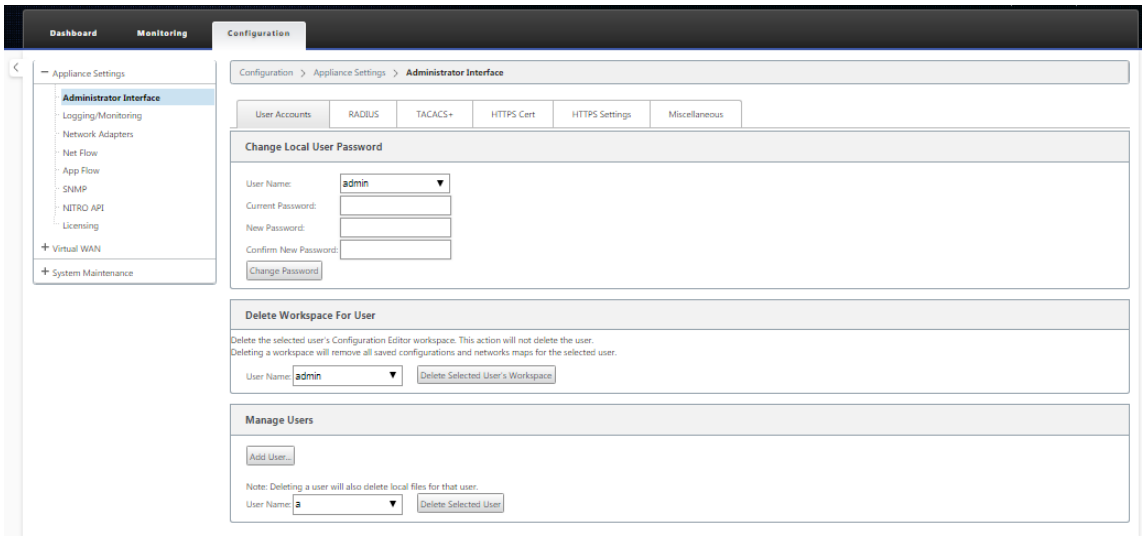
首次登录设备上的管理 Web 界面时，控制板 会显示警报图标（goldenrod 增量）和警报消息，指示已禁用 SD-WAN 服务，并且尚未安装许可证。目前，您可以忽略此警报。在您安装许可证并完成设备的配置和部署过程后，警报将得到解决。

7. 在主菜单栏中，选择“配置”部分选项卡。

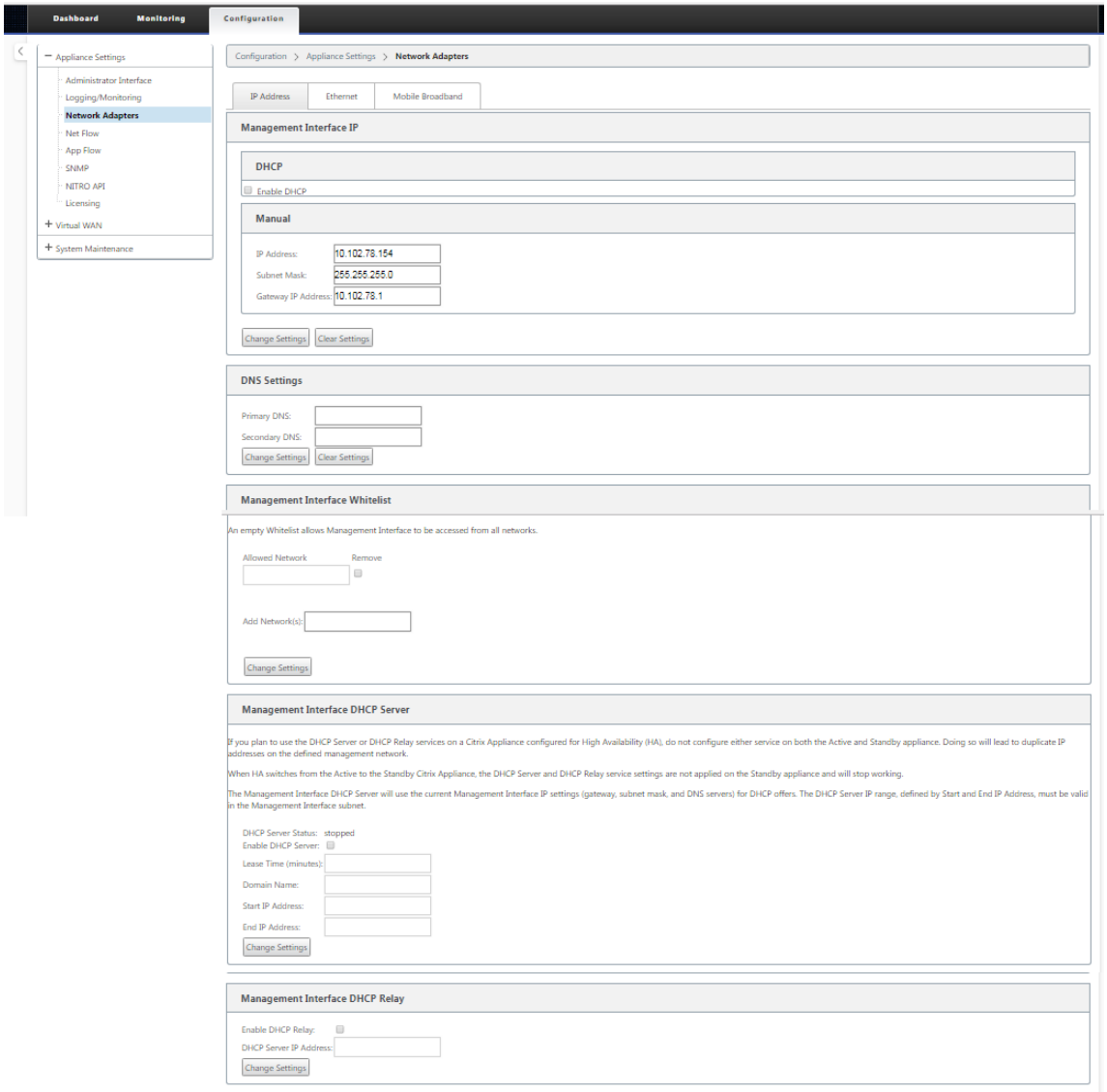
   这将在屏幕的左窗格中显示 配置 导航树。配置 导航树包含以下三个主要分支：

   - 设备设置
   - 虚拟广域网
   - 系统维护

   选择 配置 选项卡后，设备设置 分支会自动打开，默认情况下预选 管理员界 面 页面，如下图所示。



8. 在导航树的设备设置分支中，选择网络适配器。这将显示“网络适配器 设置”页面，其中默认情况下预选了“**IP** 地址”选项卡，如下图所示。



9. 在“IP 地址”选项卡中，启用以下选项之一：

   - **IPv4** 协议：要启用 IPv4 地址，请选中 启用 **IPv4** 复选框。动态主机控制协议 (DHCP) 为网络上的每台设备动态分配 IP 地址和其他网络配置参数。选择 启用 **DHCP** 以 动态分配 IP 地址。要手动配置 IP 地址，请提供以下详细信息：

     - IP 地址
     - 子网掩码
     - 网关 IP 地址

   - **IPv6** 协议：要启用 IPv6 地址，请选中 启用 **IPv6** 复选框。您可以手动配置 IPv6 地址，也可以启用 DHCP 或 SLAAC 自动分配 IP 地址。

     要手动配置，请提供以下详细信息：

     - IP 地址

- 前缀

要配置 SLAAC，请选中 **SLAAC** 复选框。SLAAC 自动为网络上的每台设备分配一个 IPv6 地址。SLAAC 使 IPv6 客户端能够使用本地可用信息和路由器通过邻居发现协议 (NDP) 公布的信息组合生成自己的地址。

要配置 DHCP，请选中 **DHCP** 复选框。要启用无状态 DHCP，请选中 **SLAAC** 和 **DHCP** 复选框。

- **IPv4** 和 **IPv6** 协议：选中 启用 **IPv6** 和 启用 **IPv4** 复选框以启用 IPv4 和 IPv6 协议。在这种情况下，SD-WAN 设备有一个 IPv4 管理 IP 地址和一个 IPv6 管理地址。

> 注意
>
> - 每个设备的管理 IP 地址必须是唯一的。
> - 只有在 管理界面中启用了 **IPv4** 协议时，“**IP** 地址” 选项卡上的 “管理接口 DHCP 服 务器” 和 “DHCP 中继” 部分才适用。
> - 当管理接口充当 DHCP 客户机时，DHCP 客户端消息中的主机名将作为选项 12 使用。从 Citrix SD-WAN 版本 11.2.3 起到 11.4.1 版，主机名被设置为 **sdwan**。从 Citrix SD-WAN 11.4.1 版起，主机名与站点名称相同。
>
> 如果第一次更改或配置站点名称，则在配置更新完成且虚拟 WAN 服务启动之前，DHCP 客户端消息中将使用旧站点名称或 **sdwan** 作为主机名。配置更新完成且虚拟 WAN 服务启动后，随后的 DHCP 客户端消息将使用新站点名称。

10. 单击 **Change Settings**（更改设置）。将显示一个确认对话框，提示您验证是否要更改这些设置。
11. 单击确定。
12. 将电脑上的网络接口设置更改回原始设置。

> 注意
>
> 更改电脑的 IP 地址会自动关闭与设备的连接，并终止管理 Web 界面上的登录会话。

13. 断开设备与 PC 的连接，并将设备连接到网络路由器或交换机。断开以太网电缆与 PC 的连接，但请勿将其与设备断开。将电缆的自由端连接到您的网络路由器或交换机。

    SD-WAN 设备现已连接到您的网络并可在您的网络上使用。

14. 测试连接。在连接到网络的 PC 上，打开浏览器，然后按以下格式输入为设备配置的管理 IP 地址：

    对于 IPv4 地址：`https://<IPv4 address>`

    示例：`https://10.10.2.3`

    对于 IPv6 地址：`https://<[IPv6 address]>`

    示例：`https://[fd73:xxxx:yyyy:26::9]`

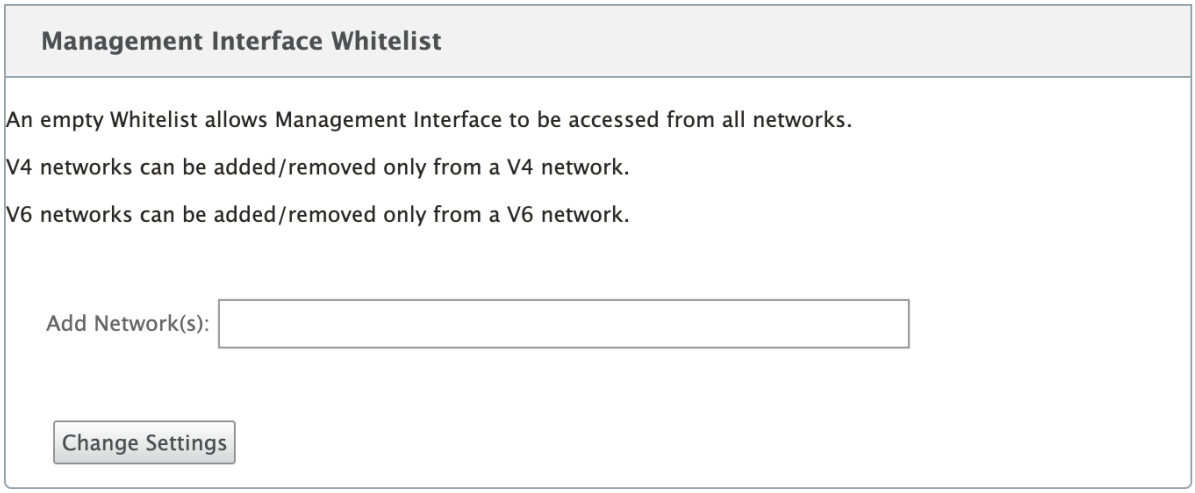
    如果连接成功，则会在配置的设备上显示 SD-WAN 管理 Web 界面的 登录 屏幕。

> 提示
>
> 验证连接后，请勿注销管理 Web 界面。您正在使用它来完成后续章节中概述的剩余任务。

您现在已设置 SD-WAN 设备的管理 IP 地址，并且可以从网络中的任何位置连接到该设备。

管理界面允许列表　允许列表是有权访问管理界面的 IP 地址或 IP 域的批准列表。空列表允许从所有网络访问管理界面。您可以添加 IP 地址以确保管理 IP 地址只能由受信任的网络访问。

要在允许列表中添加或删除 IPv4 地址，必须仅使用 IPv4 地址访问 SD-WAN 设备管理界面。同样，要在允许列表中添加或删除 IPv6 地址，必须仅使用 IPv6 地址访问 SD-WAN 设备管理界面。



设置日期和时间

在设备上安装 SD-WAN 软件许可证之前，必须在设备上设置日期和时间。

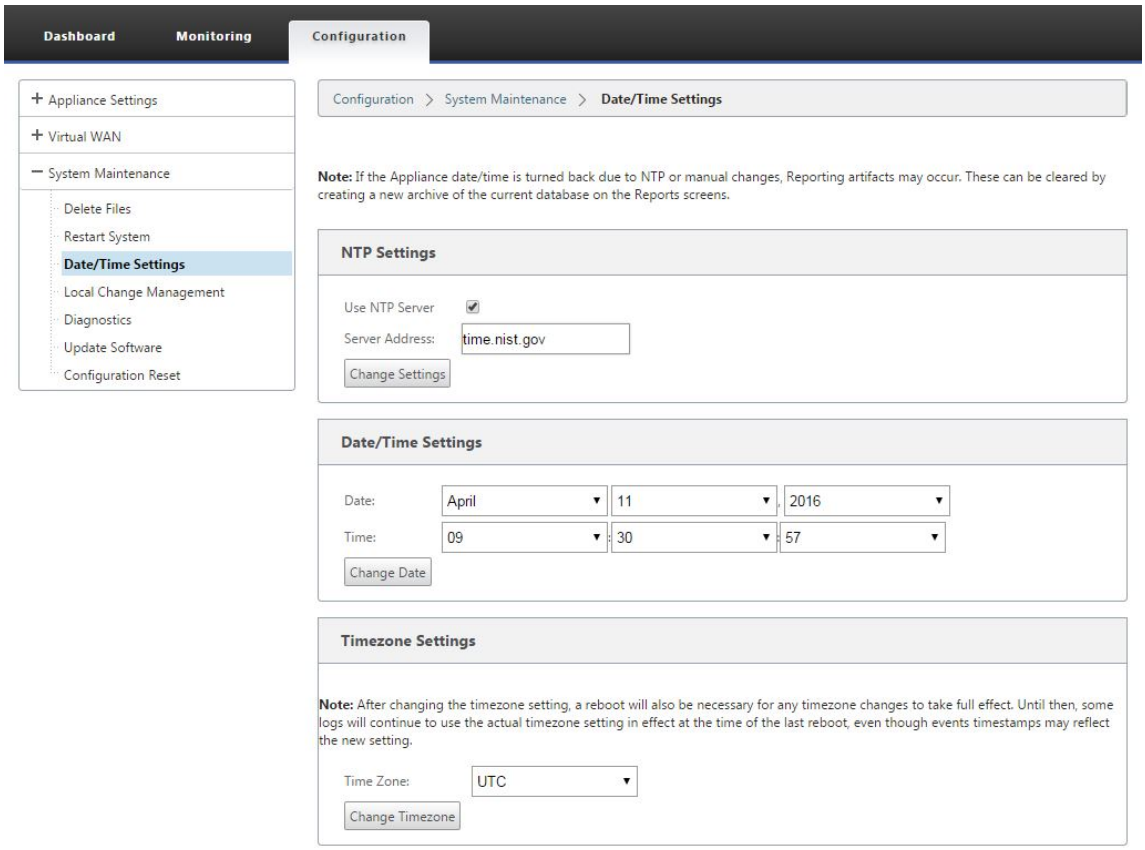
> 注意
>
> - 您必须为要添加到网络的每台设备重复此过程。
> - 如果手动或通过 NTP 服务器更改当前时间，并且新设置的时间超过会话超时计时器，则 UI 会话将被注销。

要设置日期和时间，请执行以下操作：

1. 登录到正在配置的设备上的管理 Web 界面。
2. 在主菜单栏中，选择“配置”选项卡。

   这将在屏幕的左窗格中显示 配置 导航树。
3. 在导航 树中打开系统维护分支。

4. 在 系统维护分支下，选择日期/时间设置。这将显示日期/时间设置页面，如下所示。



5. 从页面底部的时区字段下拉菜单中选择时区。

> 注意
>
> 如果您必须更改时区设置，则必须在设置日期和时间之前执行此操作，否则您的设置不会按输入的方式保留。

6. 单击 更改时区。此操作会更新时区并相应地重新计算当前日期和时间设置。如果您在此步骤之前设置了正确的日期和时间，则您的设置将不再正确。时区更新完成后，页面顶部将显示成功警报图标（绿色复选标记）和状态消息。

7. （可选）启用 NTP 服务器服务。

   a) 选择 使用 **NTP** 服务器。
   b) 在“服务器地址”字段中输入 服务器地址。
   c) 单击 **Change Settings**（更改设置）。
      更新完成时显示成功警报图标（绿色复选标记）和状态消息。

8. 从日期字段下拉菜单中选择月、日和年。
9. 从“时间”字段下拉菜单中选择小 时、分钟和秒。
10. 单击“更改日期”。

> 注意：
>
> 这将更新日期和时间设置，但不显示成功警报图标或状态消息。

下一步是将控制台会话 超时 阈值设置为最大值。此步骤是可选的，但建议使用。这样可以防止在处理配置时会话过早终止，这可能会导致工作丢失。以下部分提供了有关设置控制台会 话超时 值的说明。如果不想重置超时阈值，可以直接进入“上传和安装 SD-WAN 软件许可证文件”部分。

> 警告
>
> 如果控制台会话超时或您在保存配置之前注销管理 Web 界面，则所有未保存的配置更改都将丢失。重新登录系统，并从头开始重复配置过程。

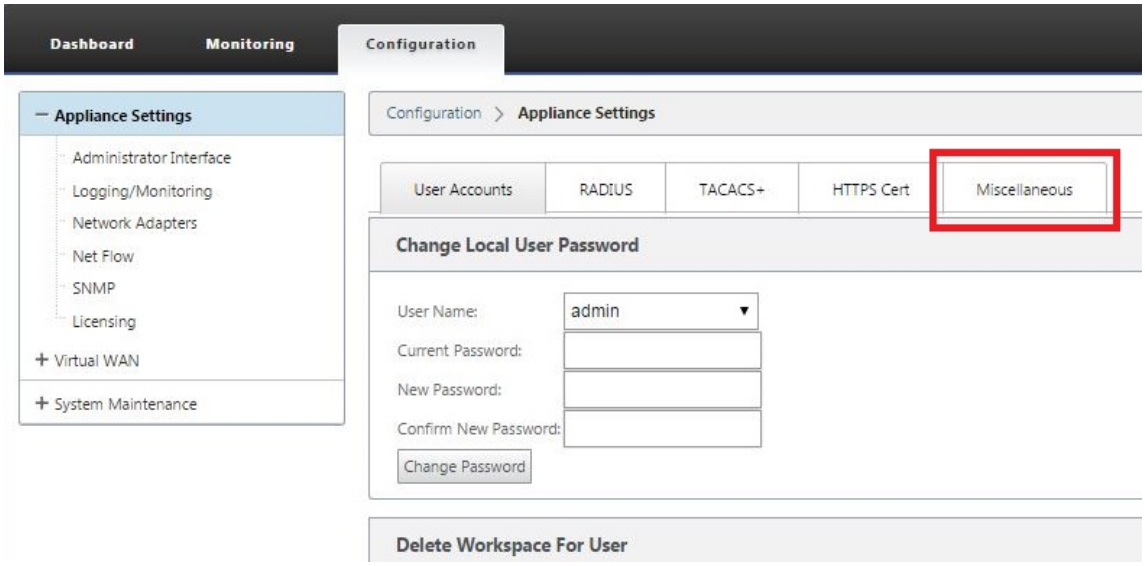
会话超时

如果控制台会话超时或您在保存配置之前注销管理 Web 界面，则所有未保存的配置更改都将丢失。然后，您必须重新登录到系统，并从头开始重复配置过程。因此，建议在创建或修改配置包或执行其他复杂任务时，将控制台会话 超 时间隔设置为较高的值。默认值为 60 分钟。最长时间为 9,999 分钟。出于安全原因，您应在完成这些任务后将其重置为较低的阈值。

要重置控制台会话 超时 间隔，请执行以下操作：

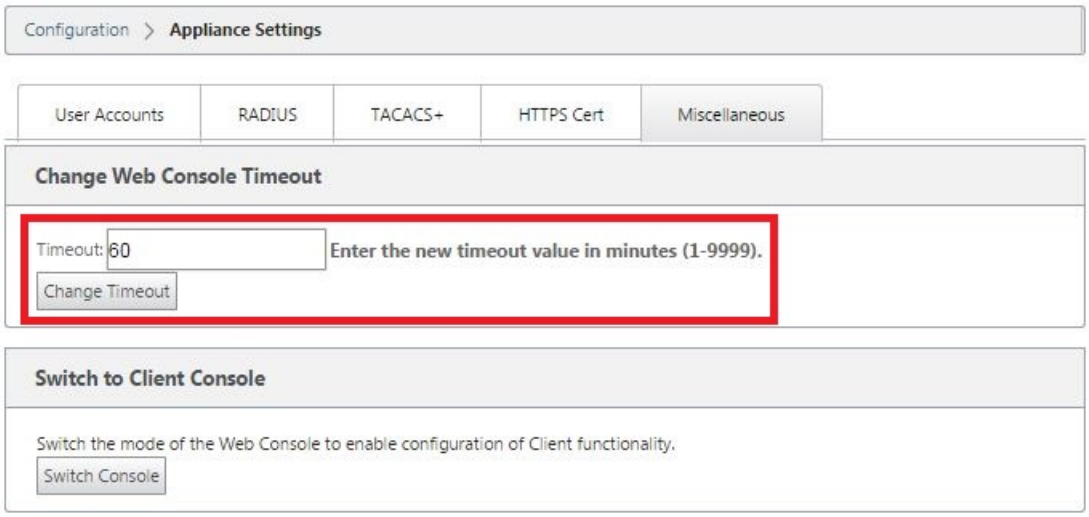
1. 选择“配置”选项卡，然后在导航树中选择“装置设 置”分支。

   这将显示“装置设置”页面，默认情况下会预先选择“用户帐户”选项卡。



2. 选择“其他”选项 卡（最右上角）。

   这将显示“其他”选项 卡页。



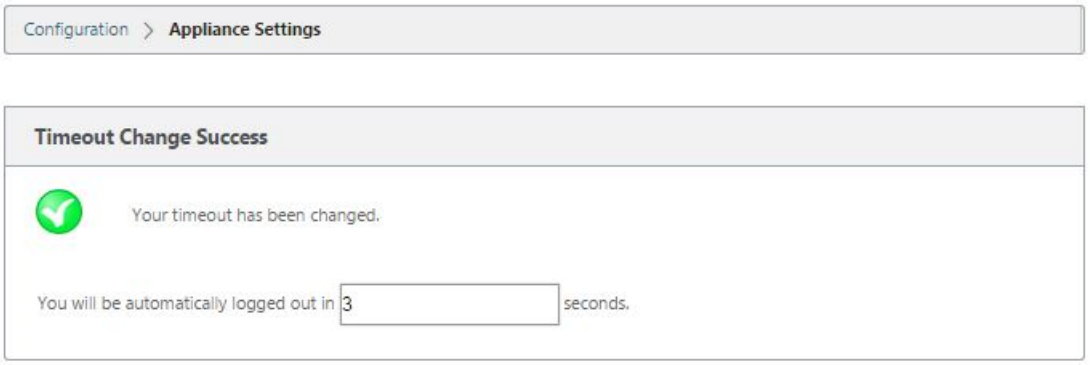
3. 输入控制台 超时 值。

   在 更改 **Web** 控制台超时部分的“超时”字段中，输入一个较高的值（以分钟为单位），最大值为 9999。默认值为 60，这对于初始配置会话来说太简短。

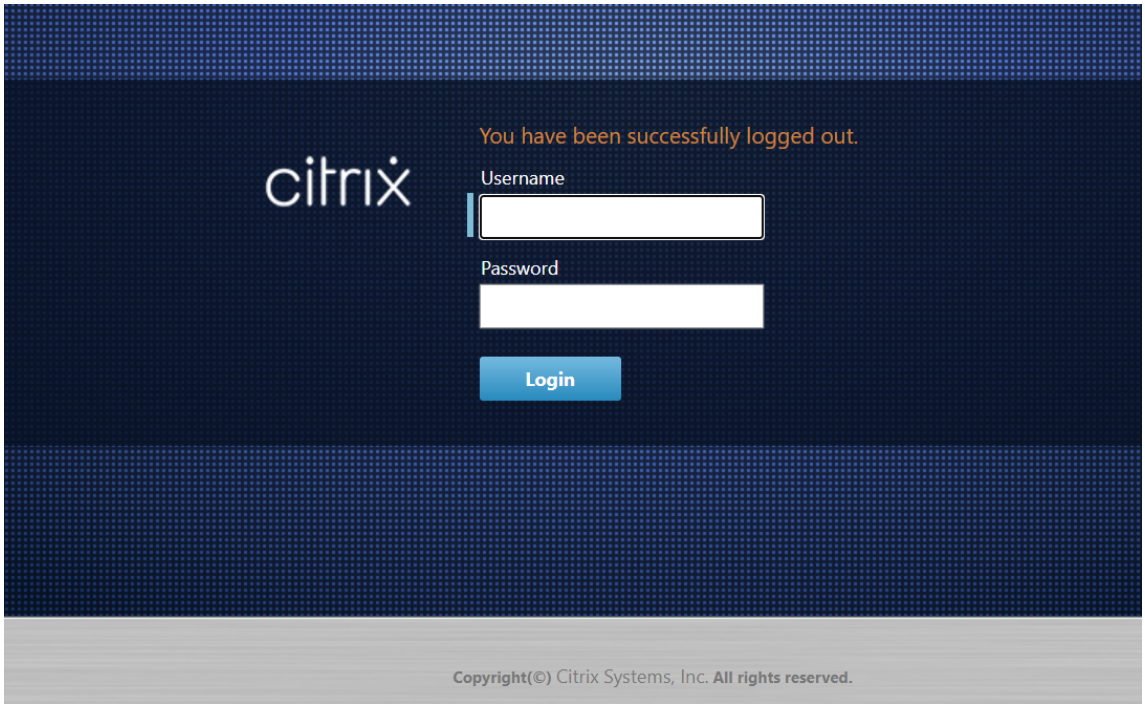
   > 注意
   >
   > 出于安全原因，请务必在完成配置和部署后将此值重置为较低的时间间隔。

4. 单击“更改超时”。

   这将重置会话 超时 间隔，并在操作完成时显示成功消息。



在短暂的间隔（几秒钟）后，会话将终止，并且您将自动注销管理 Web 界面。此时将显示登录页面。



5. 输入管理员用户名 (*admin*) 和密码 (密码)，然后单击 登录。

   下一步是在设备上上载并安装 SD-WAN 软件许可证文件。

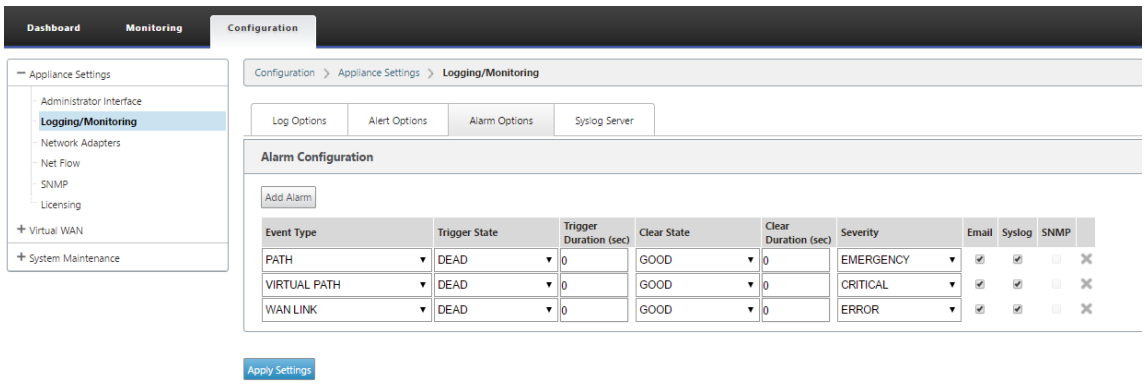
配置警报

现在，您可以配置 SD-WAN 设备，以根据网络和优先级识别警报条件，生成警报，并通过电子邮件、syslog 或 SNMP 陷阱接收通知。

警报是由事件类型、触发器状态、清除状态和严重性组成的已配置警报。

要配置警报设置，请执行以下操作：

1. 在 SD-WAN Web 管理界面中，导航到 配置 **>** 装置设置 > 日 志记录/监控，然后单击 警报选项。
2. 单击 添加警报以 添加新警报。



3. 为以下字段选择或输入值：

   - 事件类型：SD-WAN 设备可以为网络中的特定子系统或对象触发警报，这些子系统或对象称为事件类型。可用的事件类型包括 SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL 和 IPSEC_TUNNEL。
   - 触发器状态：触发事件类型警报的事件状态。可用的 触发状态 选项取决于所选事件类型。
   - 触发持续时间：以秒为单位的持续时间，这决定了设备触发警报的速度。输入 0 以接收即时警报，或者输入介于 15-7200 秒之间的值。如果在触发持续时间段内同一对象上发生更多事件，则不会触发警报。只有当事件持续时间超过 触发持续时间 时，才会触发更多警报。
   - 清除状态：触发警报后清除事件类型警报的事件状态。可用的清除状态选项取决于所选的触发器状态。
   - 清除持续时间：以秒为单位的持续时间，它决定了清除警报之前需要等待多长时间。输入 ‘0’ 即可立即清除警报，或输入 15-7200 秒之间的值。如果在指定时间内同一个对象上发生了另一个清除状态事件，则不会清除警报。
   - 严重性：用户定义的字段，用于确定警报的紧急程度。严重性显示在触发或清除警报时发送的警报以及触发的警报摘要中。
   - 电子邮件：事件类型的警报触发器和清除警报通过电子邮件发送。
   - **Syslog**：事件类型的警报触发器和清除警报通过 Syslog 发送。
   - **SNMP**：事件类型的警报触发器和清除警报通过 SNMP 陷阱发送。

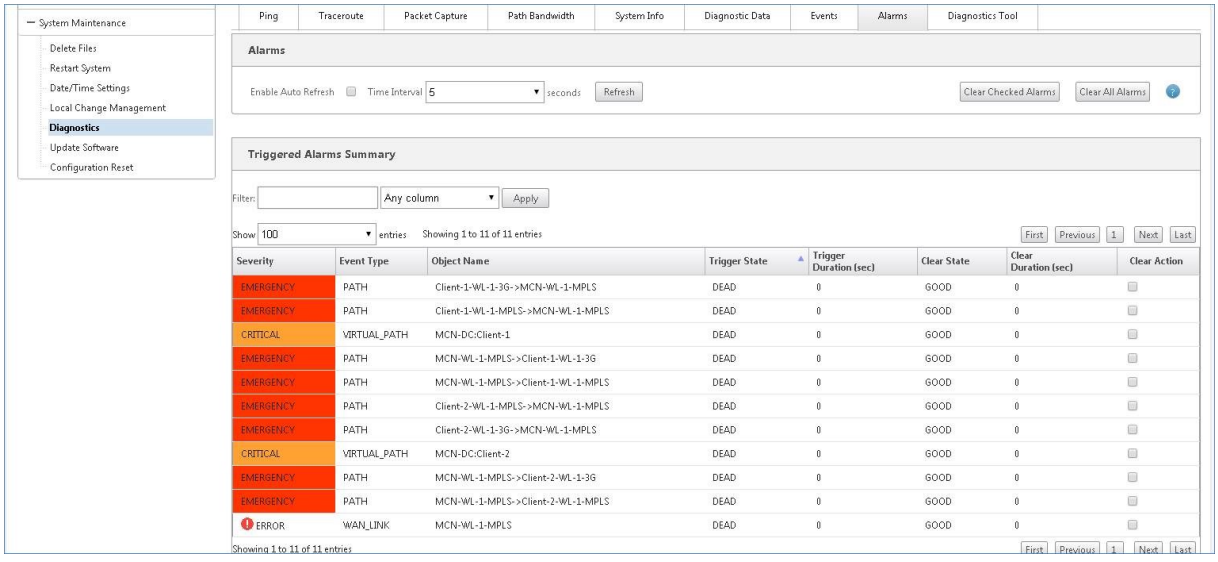
4. 根据需要继续添加警报。

5. 单击 应用设置。

查看触发的警报　要查看所有触发警报的摘要，请执行以下操作：

在 SD-WAN Web 管理界面中，导航到 配置 > 系统维护 **>** 诊断 > 警报。

将显示所有触发警报的列表。



清除触发警报　要手动清除触发的警报，请执行以下操作：

1. 在 SD-WAN Web 管理界面中，导航到 配置 > 系统维护 **>** 诊断 > 警报。
2. 在 清除操作 列中，选择要清除的警报。
3. 单击 清除选中的警报。或者，单击 清除所有警报 以清除所有警报。

设置主控制节点

SD-WAN 主控节点 **(MCN)** 是虚拟 WAN 中的头端设备。通常，这是部署在数据中心的虚拟 WAN 设备。MCN 用作初始系统配置和任何后续配置更改的分发点。此外，您可以通过 MCN 上的管理 Web 界面执行大多数升级过程。虚拟 WAN 中只能有一个活动的 MCN。

默认情况下，设备具有客户端的预先分配的角色。要将设备建立为 MCN，您必须首先添加并配置 MCN 站点，然后在指定的 MCN 设备上暂存并激活配置和相应的软件包。

从 Citrix SD-WAN 11.5 版本开始，您可以通过 Citrix SD-WAN Orchestrator 服务设置 MCN。有关更多信息，请参阅 部署 和 站点配置。

将客户端设备连接到您的网络

对于初始部署，或者如 果要将客户端节点添加到现有 SD-WAN，则下一步是分支站点管理员将客户端设备连接到各自分支站点的网络。这是为了向客户端上载和激活相应的 SD-WAN 设备包做准备。连接每个分支站点管理员以启动和协调这些过程。

要将站点设备连接到 SD-WAN，站点管理员应执行以下操作：

1. 如果尚未这样做，请设置客户端设备。

   对于要添加到 SD-WAN 的每个设备，请执行以下操作：

   a) 设置 SD-WAN 设备硬件和要部署的任何 SD-WAN VPX 虚拟设备 (SD-WAN VPX-SE)。
   b) 设置设备的管理 IP 地址并验证连接。
   c) 设置设备上的日期和时间。将控制台会话超时阈值设置为高值或最大值。
   d) 在设备上上载并安装软件许可证文件。

2. 将设备连接到分支站点 LAN。将以太网电缆的一端连接到 SD-WAN 设备上为 LAN 配置的端口。然后将电缆的另一端连接到 LAN 交换机。
3. 将设备连接到 WAN。将以太网电缆的一端连接到 SD-WAN 设备上为 WAN 配置的端口。然后将电缆的另一端连接到 WAN 路由器。

下一步是分支站点管理员在其各自的客户端上安装和激活相应的 SD-WAN 设备包。

访问 **shell** 命令

从 SD-WAN 11.4.1 版本开始，管理员帐户用户可以直接从 SD-WAN CLI 控制台运行 shell 命令，而无需提示输入 CBVWSSH 静态帐户的登录凭据。此功能可以删除 CBVWSSH 帐户的硬编码密码并使用更安全的方法替换它，从而增强了 SD-WAN 设备的安全性。要运行 shell 命令，请登录 SD-WAN CLI 控制台并键入 `shell`。

> 注意
>
> - 仅管理员帐户用户支持此功能。网络管理员、安全管理员或 Viewer 帐户用户不支持此功能。
> - 此功能仅用于故障排除目的。通过 `shell` 命令进行的任何特定于系统的更改都受 Citrix 监督。

升级　将 SD-WAN 设备升级到 11.4.1 版本时，默认管理员帐户的密码将与 CBVWSSH 帐户同步。每次编辑/更新管理员帐户时，CBVWSSH 帐户和默认管理员帐户之间的这种同步都会发生。

降级　将 SD-WAN 设备从 11.4.1 降级到旧版本时，您可以选择重置默认管理员帐户的密码。但是，新密码不会同步到 CBVWSSH 账户。因此，为了即使在降级后也能访问该 `shell` 命令，必须在降级设备之前记住当前密码。

使用云在 **OpenStack** 中部署 **Citrix SD-WAN** 标准版

现在，您可以在 OpenStack 环境中部署 Citrix SD-WAN 标准版 (SE)。为此，Citrix SD-WAN 映像必须支持配置驱动器功能。

> 注意
>
> 创建 Citrix 映像以支持配置驱动器功能。

配置驱动器功能支持以下参数配置，以便通过管理网络与 Citrix Orchestrator 建立通信：

- 管理 IPv4 地址
- 管理 Gateway
- Name-server1
- Name-server2
- 序列号- 用于身份验证，必须为新实例重复使用序列号。在云中传递的序列号必须覆盖 VPX 实例中自动生成的试用号。

> 注意
>
> - 要重复使用序列号，将在 SD-WAN 中合并一个 init 脚本，该脚本在 OpenStack 上运行，并在 /etc/default/系列中更改序列号。
> - Orchestrator 必须具有唯一的序列号和 SD-WAN 设备才能正常工作。

Cloudinit 脚本支持在 OpenStack 中使用配置驱动器进行 SD-WAN 部署的上下文化。

在上下文化过程中，基础结构使上下文可供虚拟机使用，虚拟机解释上下文。在上下文化中，虚拟机可以启动某些服务、创建用户或设置网络和配置参数。

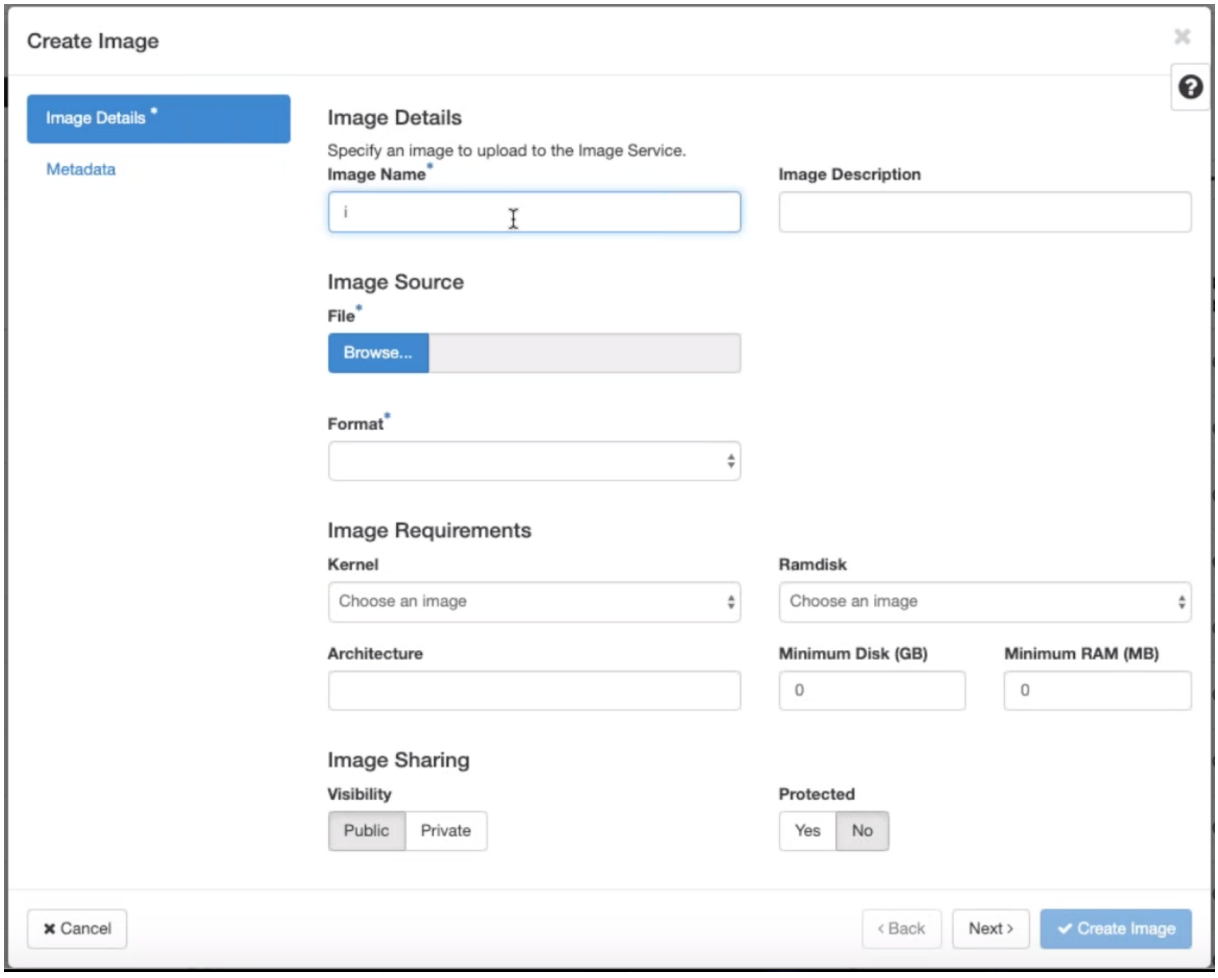
对于 OpenStack 中的 SD-WAN 实例，是用户提供的管理 IP、DNS 和序列号所需的输入。Cloudinit 脚本将解析这些输入并使用给定的信息置备实例。

在 OpenStack 云环境中启动实例时，Citrix SD-WAN 设备需要支持用户数据和 CloudInit 两种技术，以支持启动时实例的自动配置。

要在 OpenStack 环境中 Provisioning SD-WAN SE，请执行以下步骤：

必备条件

转到 图像，然后单击 创建映像。

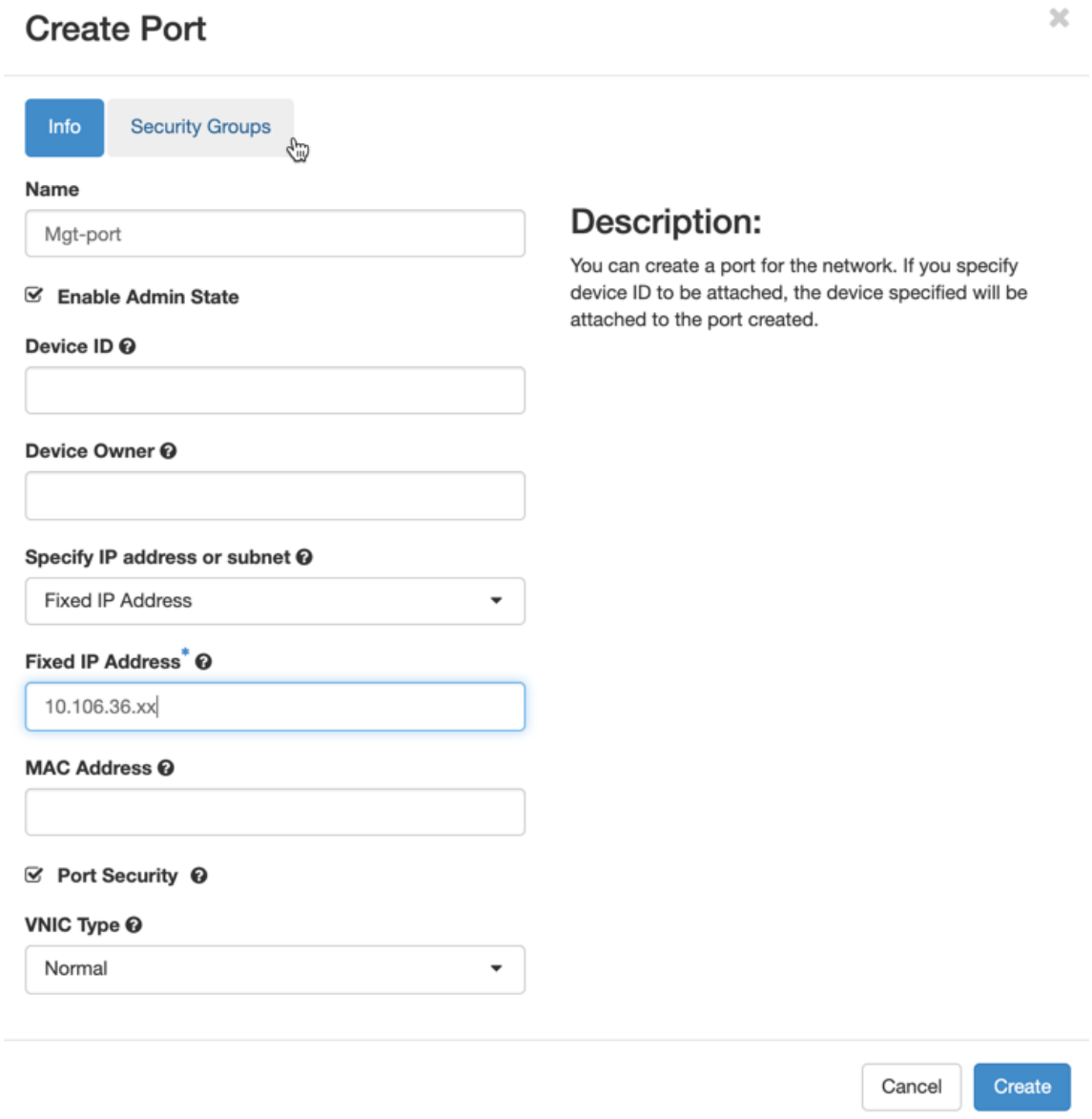


- 图片名称 -提供图像名称。
- 图片描述—添加图片描述。
- 文件 -从本地驱动器浏览 kvm.qcow2 映像文件并将其选中。
- 格式—从下拉列表中选择 QCOW2 —QEMU 模拟器磁盘格式。

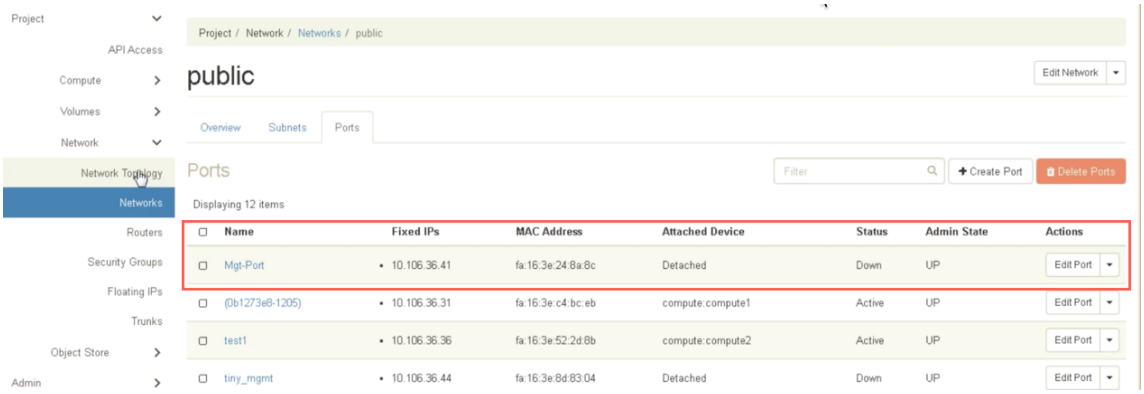
单击创建映像。

网络和网络端口都必须初始创建并预定义。要创建网络端口：

1. 选择 网络下的网络，然后转到端口 选项卡。
2. 单击 创建端口 并提供必要的详细信息，然后单击创建



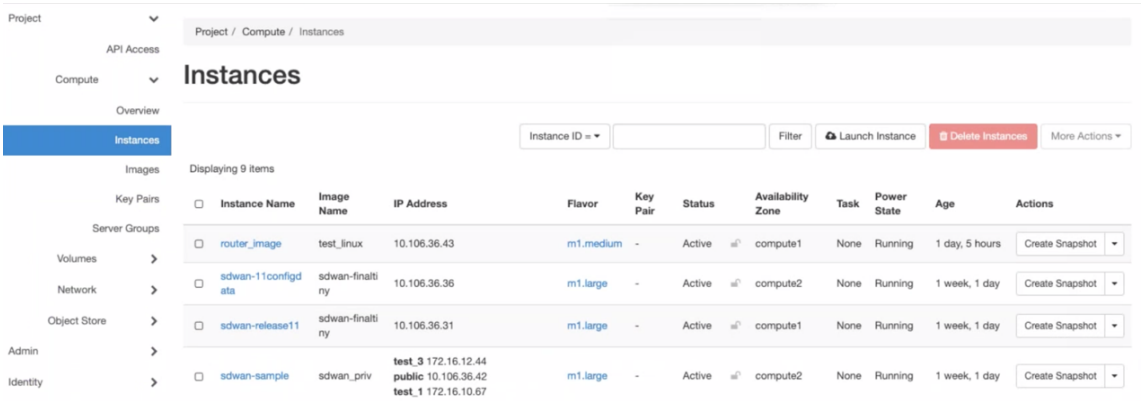
如果选择 固定 **IP** 地址，则必须为新端口提供子网 IP 地址。



端口已创建，因为它未连接到任何设备，当前状态显示为“已脱离”。

创建 OpenStack 实例以启用配置驱动器并传递用户数据。

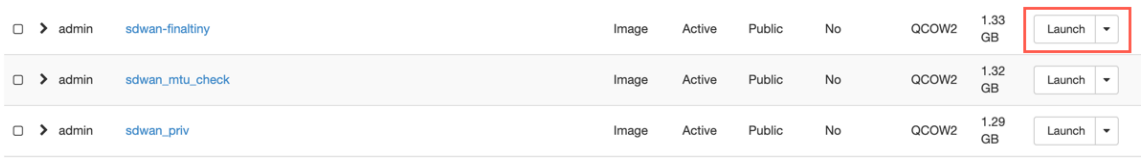
3. 登录 OpenStack 并配置实例。



4. 下载 **kvm.qcow2.gz** 文件并解压它。

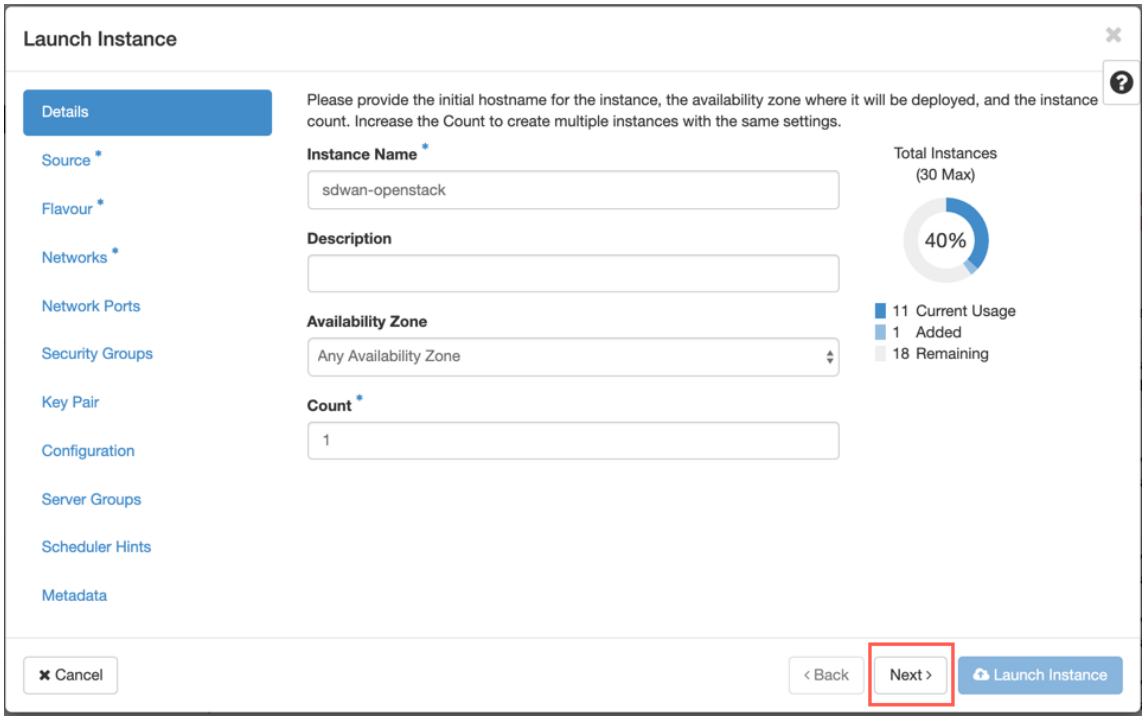
5. 转到 实例，然后单击 启动实例。

> 注意：
>
> 创建映像后，您可以返回 实例并单击启动实例，或者在映像屏幕中单击 启动。

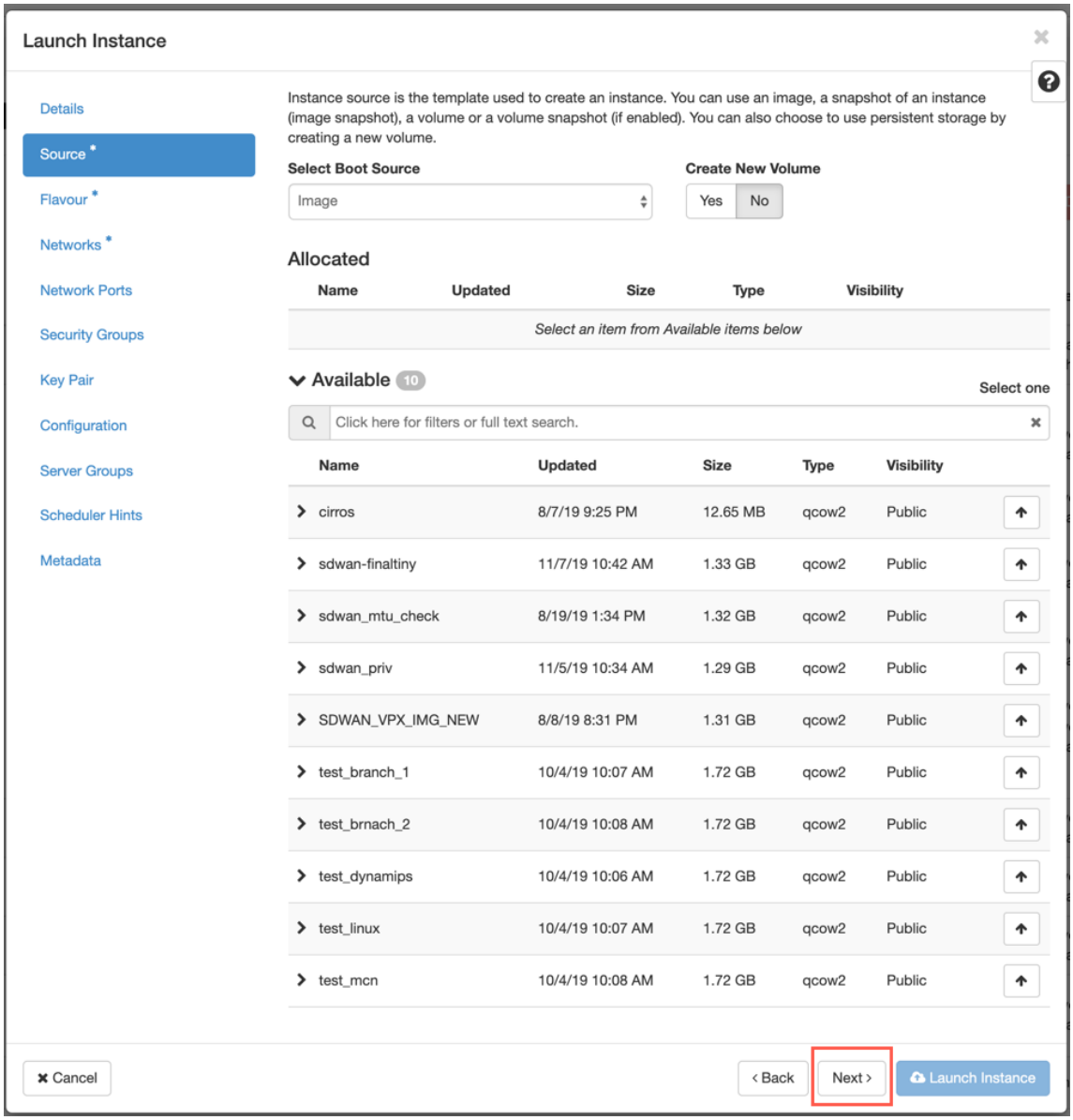


6. 在 详细 信息选项卡下，提供以下信息：

   - 实例名称—提供实例的主机名。
   - 描述—添加实例的描述。
   - 可用区—从下拉列表中选择要部署实例的可用区。
   - 计数—输入实例计数。您可以增加计数以创建具有相同设置的多个实例。单击下一步。



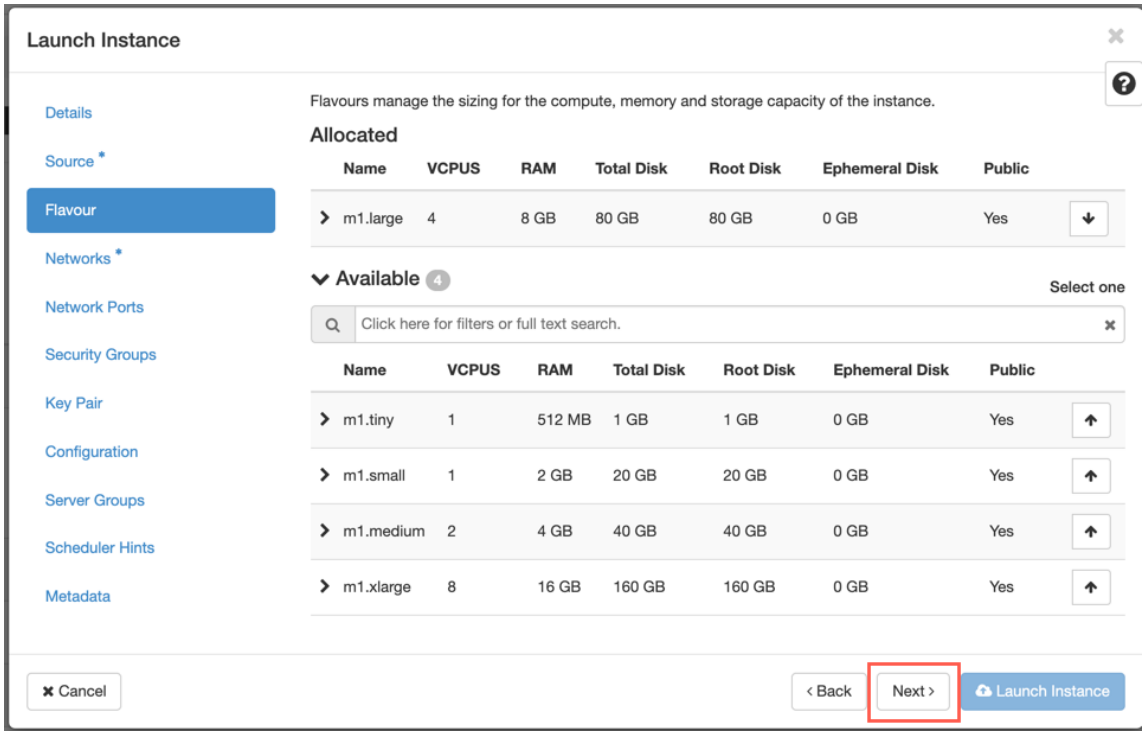
7. 在 源 选项卡中，在 创建新卷 下选择 否，然后单击下一步。实例源是用于创建实例的模板。



8. 为实例选择 **Flavour** ，然后单击下一步。您为实例选择的风格管理实例的计算、存储和内存容量。

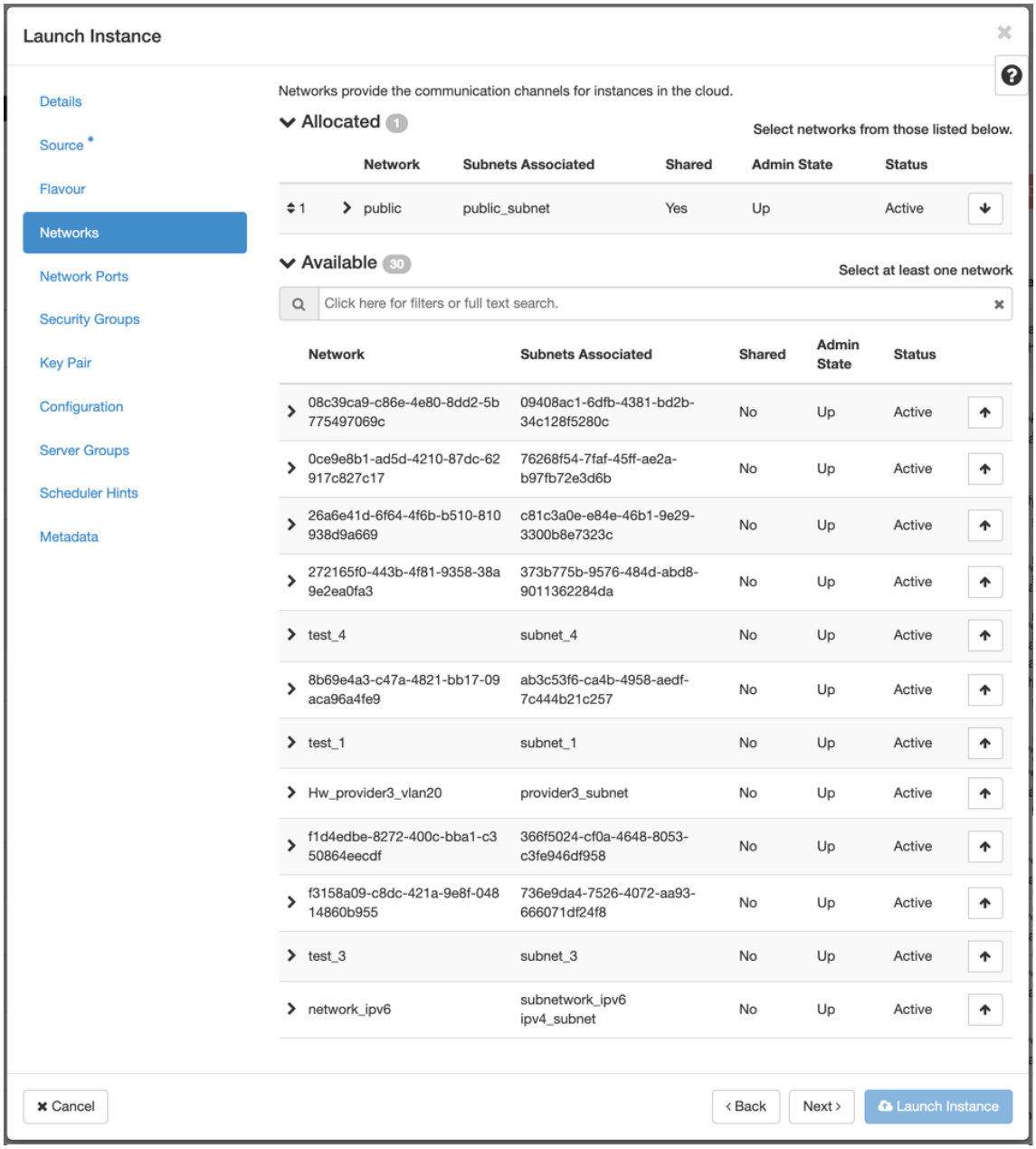
> 注意
>
> 您选择的风格必须有足够的资源来支持您尝试创建的实例类型。没有为您的实例提供足够资源的样式会在可用表中标识一个黄色警告图标。

管理员负责创建和管理风味。单击要分配的箭头（右侧）。



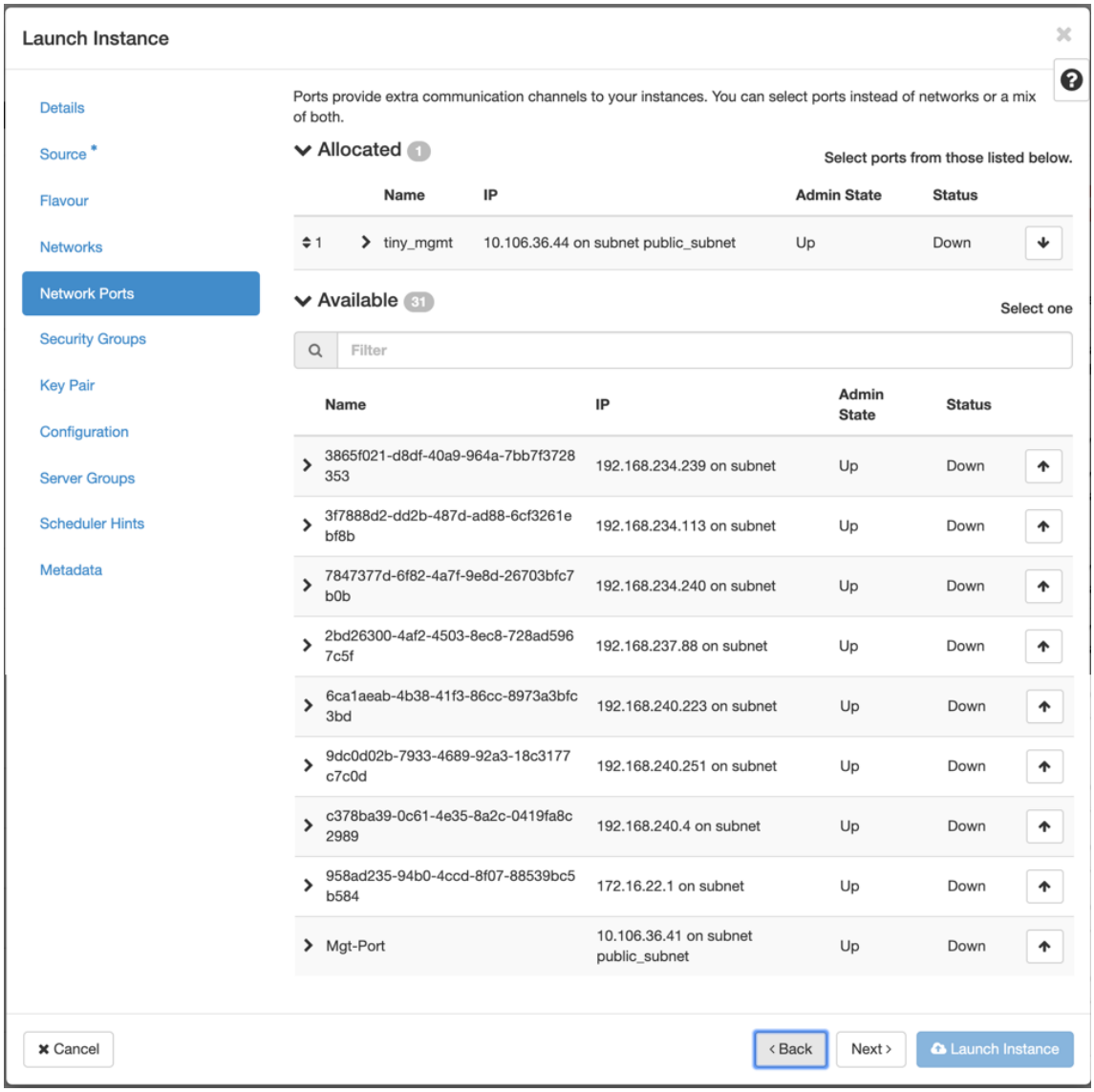
9. 选择网络，然后单击 下一步。网络为实例提供通信通道。

> 注意
>
> 管理员将创建提供商网络，并将这些网络映射到数据中心中的现有物理网络。同样，项目网络是由用户创建的，这些网络是完全隔离的，并且是项目特定的。



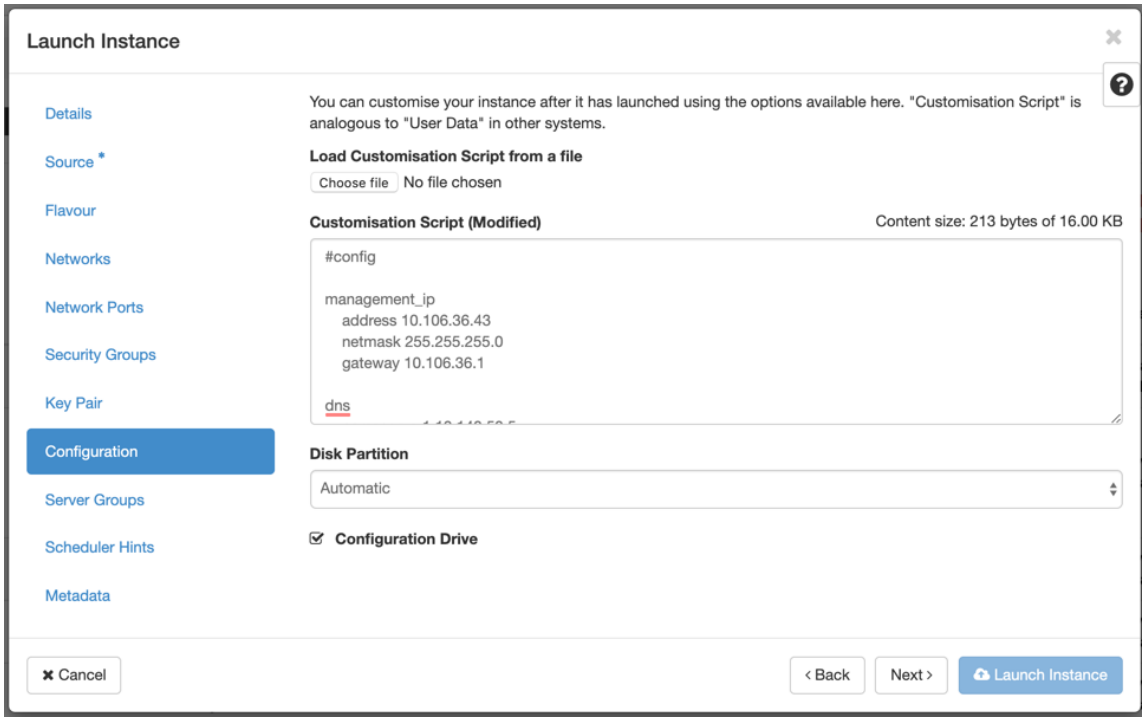
10. 为实例选择网络端口，然后单击 下一步。网络端口为实例提供额外的通信通道。

> 注意
>
> 您可以选择端口而不是网络，也可以选择两者混合使用。



11. 转到 配置，然后单击 选择文件。选择 user_data 文件。您可以在 user_data 文件中查看 管理 **IP**、**DNS** 和 序列号 信息。

12. 启用 配置驱动器 复选框。通过启用配置驱动器，您可以将用户元数据放入映像中。



13. 单击 启动实例。

在 **210 SE LTE** 设备上配置 **LTE** 功能

September 2, 2022

您可以使用 LTE 连接将 Citrix SD-WAN 210-SE LTE 设备连接到您的网络。本主题提供有关配置移动宽带设置、为 LTE 配置数据中心和分支设备等的详细信息。有关 Citrix SD-WAN 210-SE LTE 硬件平台的更多信息，请参阅 Citrix SD-WAN 210 标准版设备。

> 注意
>
> LTE 连接取决于 SIM 运营商或服务提供商网络。有关如何在网络中配置和管理 LTE 站点的信息，请参阅 LTE 固件升级。

开始使 **Citrix SD-WAN 210-SE LTE**

1. 将 SIM 卡插入 Citrix SD-WAN 210-SE LTE 的 SIM 卡插槽中。

   > 注意：
   >
   > 仅支持标准或 2FF SIM 卡（15x25 毫米）。

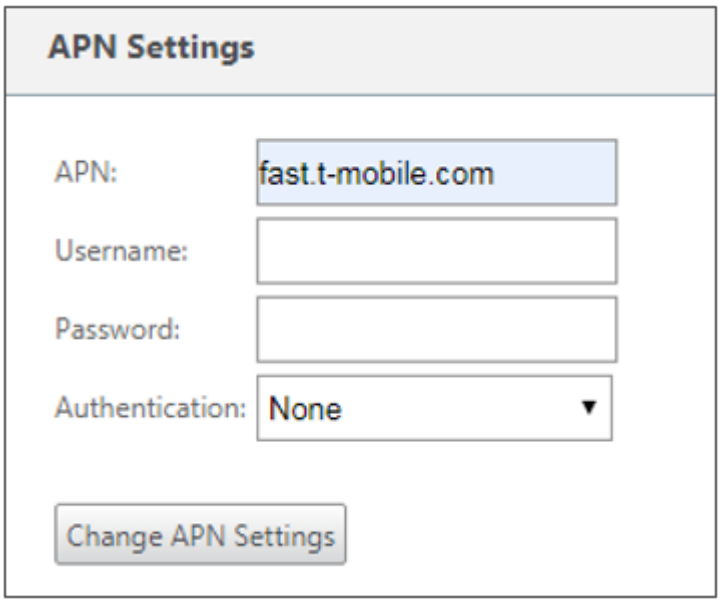
2. 将天线固定到 Citrix SD-WAN 210-SE LTE 设备上。有关更多信息，请参阅 安装 LTE 天线。

3. 打开设备的电源。

> 注意
>
> 如果您已将 SIM 卡插入已通电并已启动的装置，请导航至 配置 **>** 装置设置 **>** 网络适配器 **>** 移动宽带 **>** **SIM** 卡，然后单击 刷新 **SIM** 卡。

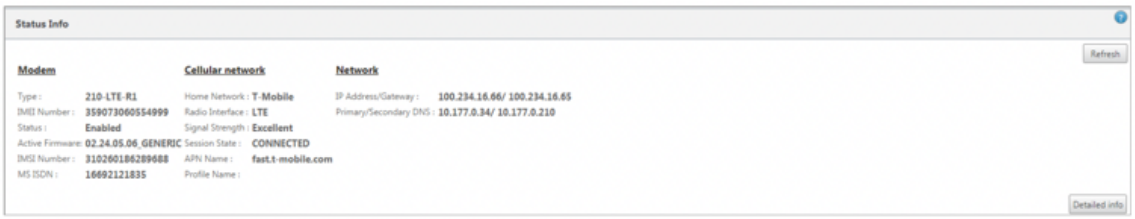
4. 配置 APN 设置。在 SD-WAN GUI 中，导航到 配置 **>** 设备设置 **>** 网络适配器 **>** 移动宽带 **>** **APN** 设置。

> 注意：
> 从承运人处获取 APN 信息。



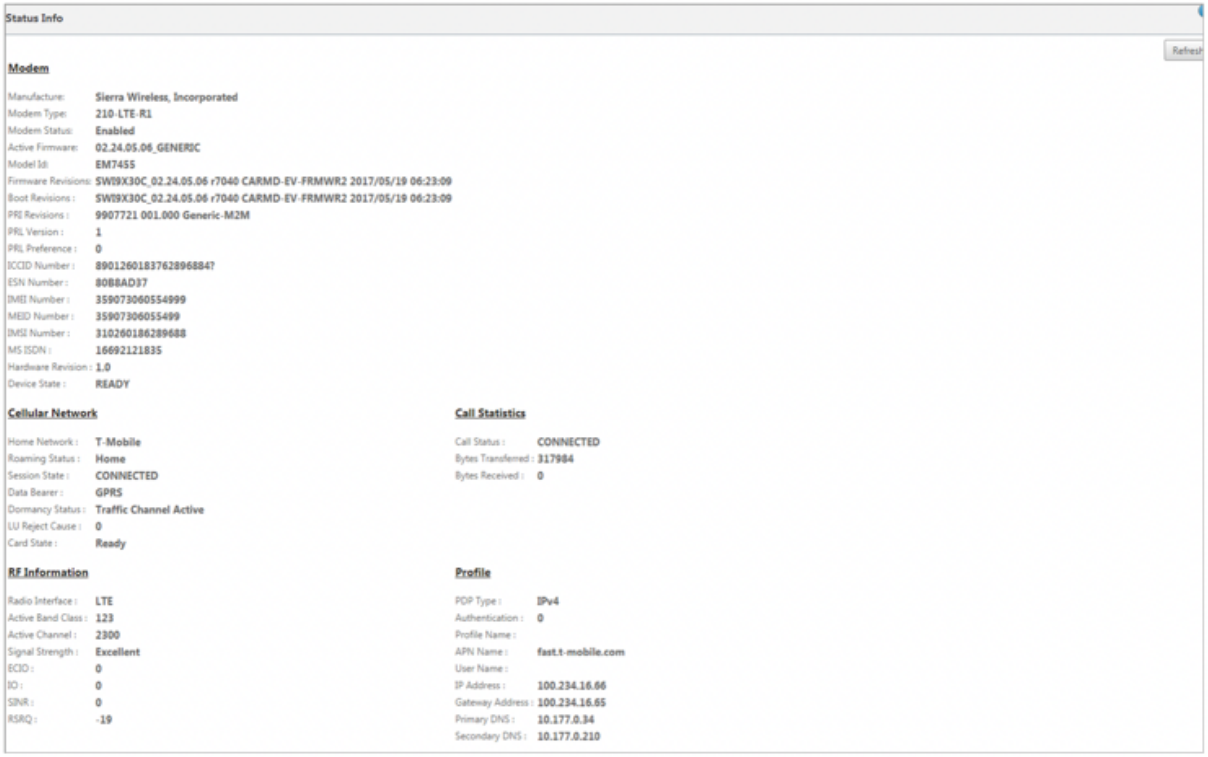
5. 输入承运人提供的 **APN**、用户名、密码 和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。
6. 单击 更改 **APN** 设置。
7. 在 SD-WAN 设备 GUI 中，导航到 配置 **>** 装置设置 **>** 网络适配器 **>** 移动宽带。

   您可以查看移动宽带设置状态信息。



以下是一些有用的状态信息：

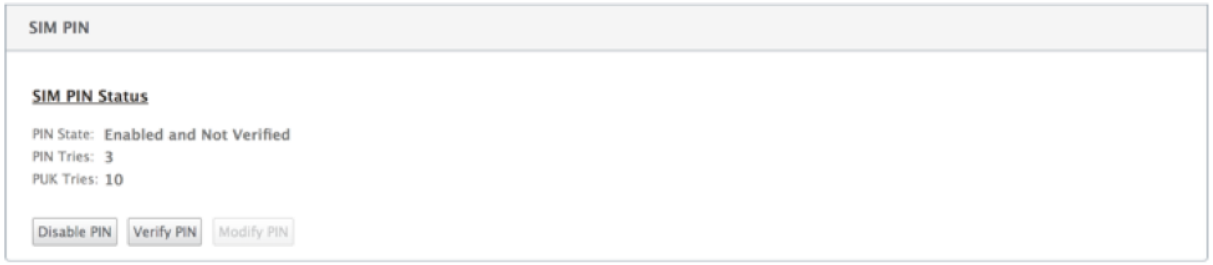
- 操作模式：显示调制解调器状态。
- 活动 **SIM** 卡：在任何给定时间，只能有一个 SIM 卡处于活动状态。显示当前处于活动状态的 SIM 卡。
- 卡状态：存在表示 SIM 卡已正确插入。
- 信号强度：信号强度的质量-优秀、良好、公平、差或无信号。
- 家庭网络：插入的 SIM 卡的运营商。
- **APN** 名称：LTE 调制解调器使用的接入点名称。
- 会话状态：已连接表示设备已加入网络。如果会话状态已 断开连接，请在启用数据计划时向运营商核实帐户是否已激活。



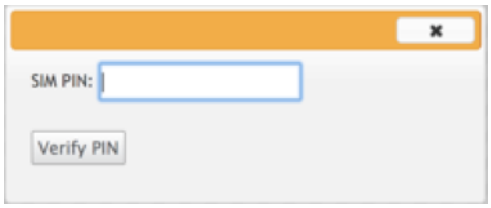
SIM PIN

如果您插入了使用 PIN 锁定的 SIM 卡，则 SIM 卡状态为“已启用”和“未验证”** 状态。在使用 SIM 卡进行验证之前，您无法使用 SIM PIN。您可以从运营商处获取 SIM PIN。

要执行 SIM PIN 操作，请导航到配置 **>** 设备设置 **>** 网络适配器 **>** 移动宽带 **> SIM PIN**。



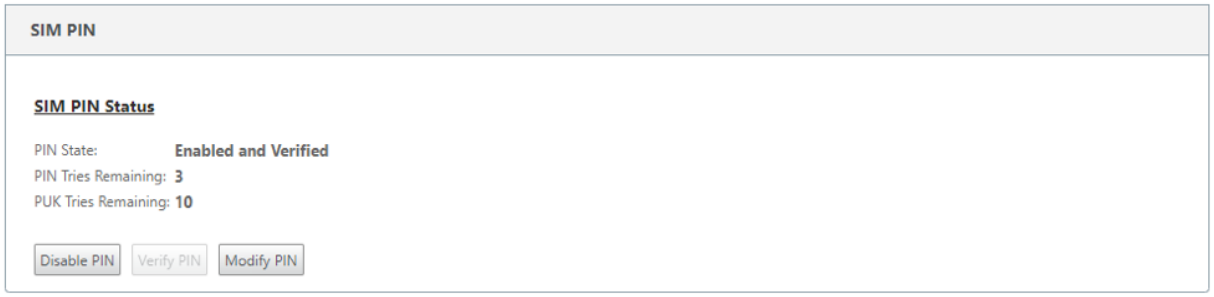
单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。

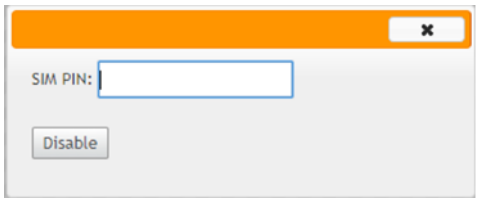


状态更改为 已启用 和 已验证。

禁用 **SIM PIN**

对于已启用和验证 SIM PIN 的 SIM 卡，您可以选择禁用 SIM 卡 PIN 功能。

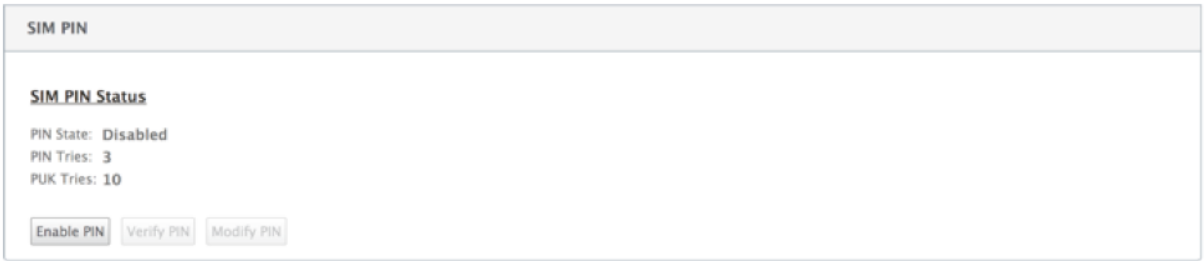




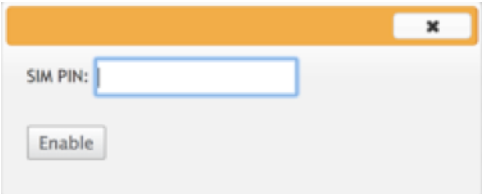
单击 禁用 **PIN**。输入 **SIM PIN**，然后单击禁用。

启用 **SIM PIN**

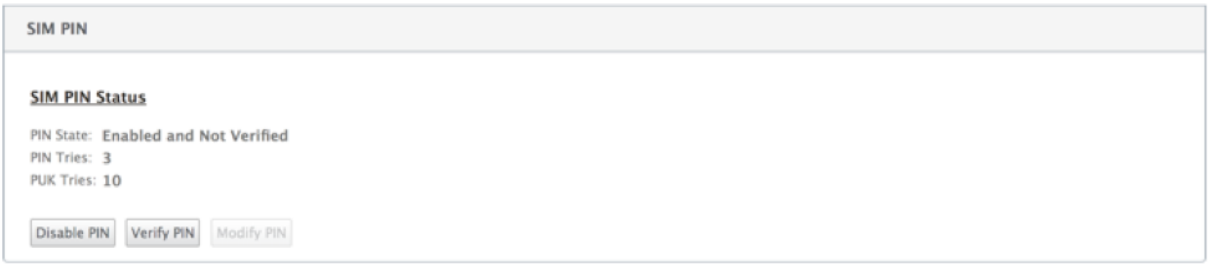
可以为禁用了 SIM PIN 的 SIM 启用 SIM PIN。



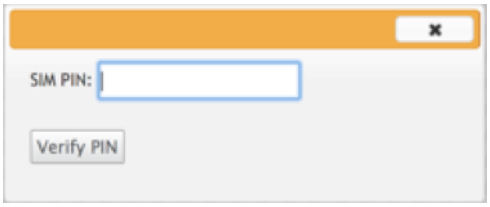
单击 启用 **PIN**。输入运营商提供的 SIM PIN，然后单击启用。



如果 SIM PIN 状态更改为已启用和未验证，则表示 PIN 未验证，在验证 PIN 之前，您无法执行任何 LTE 相关操作。

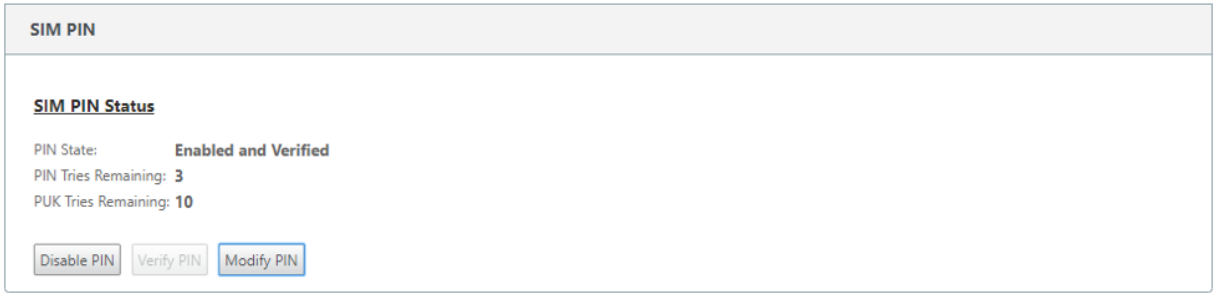


单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。

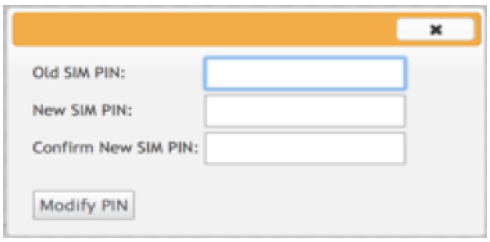


修改 **SIM PIN**

PIN 处于“已 启用”和“已验证”状态后，您可以选择更改 PIN。



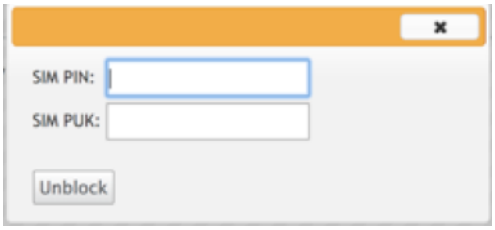
单击 修改 **PIN**。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 修改 **PIN**。



取消阻止 **SIM** 卡

如果您忘记了 SIM PIN，可以使用从运营商获得的 SIM PUK 重置 SIM PIN。

要取消阻止 SIM 卡，请单击 取消阻止。输入从运营商处获得的 **SIM PIN** 码和 **SIM PUK**，然后单击解锁。

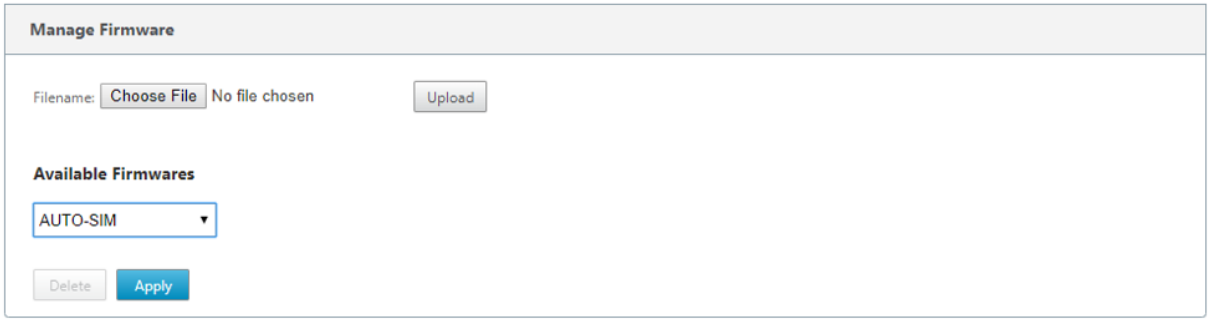


> 注意：
> SIM 卡被永久阻止，并且 10 次 PUK 尝试失败，同时解除阻止 SIM 卡。请联系运营商以获取新的 SIM 卡。

管理固件

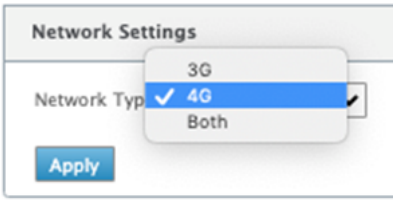
每个启用了 LTE 的设备都将拥有一组可用固件。您可以从现有的固件列表中选择或上载固件并应用它。

如果您不确定要使用哪个固件，请选择 AUTO-SIM 选项以允许 LTE 调制解调器根据插入的 SIM 卡选择最匹配的固件。



网络设置

您可以在支持内部 LTE 调制解调器的 Citrix SD-WAN 设备上选择移动网络。支持的网络包括 3G、4G 或两者。



漫游

默认情况下，LTE 设备上启用漫游选项，您可以选择禁用它。

启用/禁用调制解调器

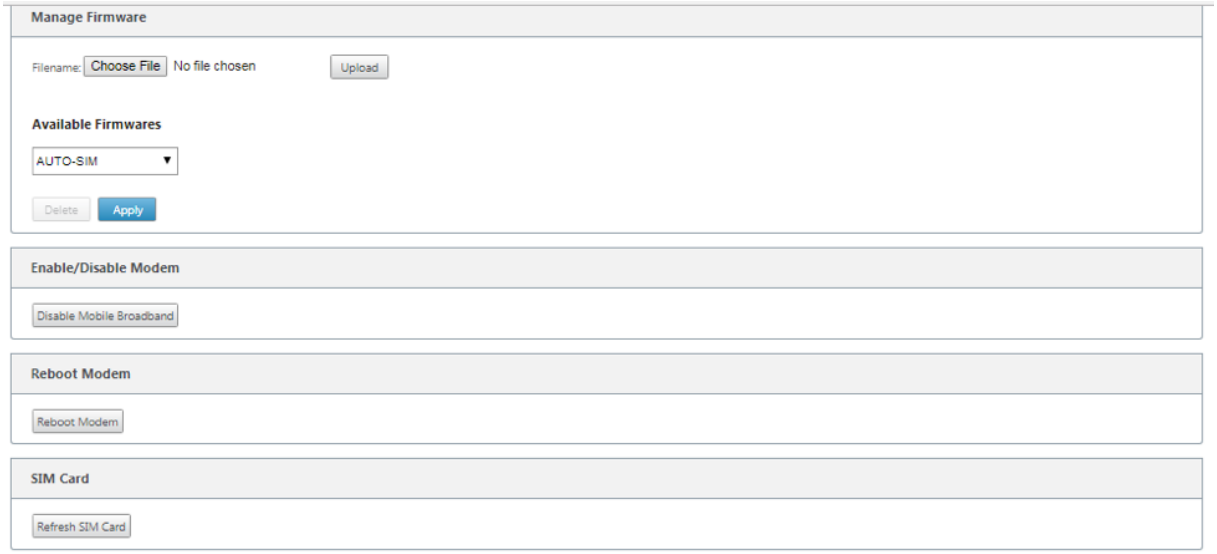
根据您使用 LTE 功能的意图启用/禁用调制解调器。默认情况下，LTE 调制解调器处于启用状态。

重启调制解调器

重新启动调制解调器。重新启动操作最多可能需要 3-5 分钟才能完成。

刷新 **SIM** 卡

当您热交换 SIM 卡以通过 210-SE LTE 调制解调器检测新 SIM 卡时，请使用此选项。



使用 **CLI** 配置 **LTE** 功能

使用 CLI 配置 210-SE LTE 调制解调器。

1. 登录到 Citrix SD-WAN 设备控制台。
2. 在提示符处，键入用户名和密码以获取 CLI 接口访问权限。
3. 在提示符处，键入命令 **lte**。键入 **>** 帮助。这将显示可用于配置的 LTE 命令列表。


```
site210>lte
lte>help
status                                      # Show status
show                                        # Show settings
disable                                     # Disable LTE modem
enable                                      # Enable LTE modem
apn <apn> [<user name> [<password> [<PAP|CHAP|PAPCHAP>]]]   # Set APN
sim-power <off|on|reset>                    # Off, on, reset SIM card power
sim-pin <show>                              # SIM card pin status
sim-pin <verify|disable|enable> <sim pin> # Verify/Disable/Enable SIM card PIN
sim-pin <modify> <old pin> <new pin>        # Modify SIM card PIN
sim-pin <unblock> <sim puk> <sim pin>       # Unblock SIM card PIN
reboot                                      # Reboot modem
ping                                        # Check if modem manager ready
list-fw                                     # List available firmware
apply-fw <fw>                               # Apply the specified firmware
```

下表列出了 **LTE** 命令描述。

命令	说明
帮助 {lte>help}	列出可用 LTE 命令和参数
状态 {lte> 状态}	显示 LTE 连接状态
显示 {lte>show}	显示 LTE 设置
禁用 {lte> 禁用}	禁用 LTE 调制解调器
启用 {lte> 启用}	启用 LTE 调制解调器
Apn {lte>apn}	配置 APN 设置信息
SIM-关闭电源、打开、重置 > {lte> sim-关机、打开、重置}	关闭 SIM 卡、打开 SIM 卡电源、刷新 SIM 卡
SIM PIN {lte>sim-pin}	关闭 SIM 卡、打开 SIM 卡电源、刷新 SIM 卡
Reboot {lte>reboot}	重新启动 LTE 调制解调器
Ping {lte>ping}	Ping LTE 调制解调器
列表-FW {lte>list-fw}	列出 R1 或 R2 LTE 调制解调器上可用的固件
Apply-fw {lte>apply-fw}	应用特定于运营商的固件

LTE 上的零接触部署

通过 LTE 实现零接触部署服务的先决条件

1. 为 210-SE LTE 设备安装天线和 SIM 卡。
2. 确保 SIM 卡具有激活的数据计划。
3. 确保管理端口未连接。
    - 如果管理端口已连接，请断开管理端口，然后重新启动设备。

- 如果在管理界面上配置了静态 IP 地址，则需要使用 DHCP 配置管理界面，应用配置，然后断开管理端口，然后重新启动设备。

4. 确保 210-SE 设备配置具有为 LTE 接口定义的 Internet 服务。

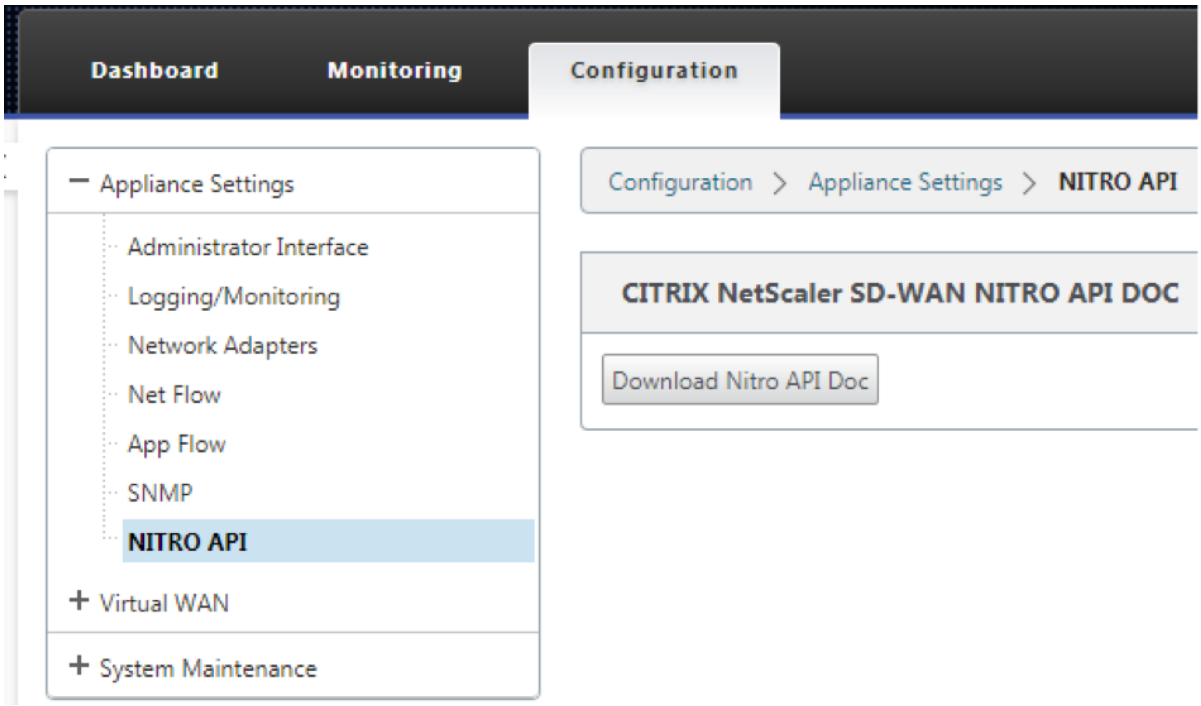
打开设备电源后，只有在管理端口未连接时，零接触部署服务才会使用 LTE 端口获取最新的 SD-WAN 软件和 SD-WAN 配置。

210-SE LTE 设备的零接触部署管理界面服务

连接管理端口并使用所有其他非 LTE 平台支持的标准 零接触部署程序 。

LTE REST API

有关 LTE REST API 的信息，请导航到 SD-WAN GUI，然后转到 配置 **>** 装置设置 **> NITRO API**。单击下载 **Nitro API** 文档。Citrix SD-WAN 11.0 中引入了用于 SIM PIN 功能的 REST API。



AT 命令

AT 命令有助于监控和排除 LTE 调制解调器的配置和状态。AT 是 **AtTension** 的缩写。由于每个命令行都以 **at** 开头，因此它们称为 AT 命令。支持 LTE 的 Citrix SD-WAN 平台型号支持运行 AT 命令。AT 命令是特定于调制解调器的，因此 AT 命令的列表因平台而异。

要运行 AT 命令，请执行以下步骤：

1. 登录到 Citrix SD-WAN 设备控制台。
2. 在提示符处，键入用户名和密码以获取 CLI 接口访问权限。
3. 在提示符下，键入 **LTE**。
4. 输入 **at** 然后输入 AT 命令。

以下是该命令的一个示例：

- 在 **at+cpin** —提供 SIM 卡状态信息。

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```

- **at at!gstatus** -提供 LTE 调制解调器状态信息。

```
lte> at at!gstatus?
Running at!gstatus? command
AT command state: success
  !GSTATUS:
  Current Time:  1279298                Temperature: 62
  Reset Counter: 1              Mode:        ONLINE
  System mode:   LTE            PS state:    Attached
  LTE band:      B5                     LTE bw:      10 MHz
  LTE Rx chan:   2559           LTE Tx chan: 20559
  LTE CA state:  NOT ASSIGNED
  EMM state:     Registered             Normal Service
  RRC state:     RRC Connected
  IMS reg state: Full Srv               IMS mode:    Normal
  PCC RxM RSSI:  -73            RSRP (dBm):  -112
  PCC RxD RSSI:  -73            RSRP (dBm):  -107
  Tx Power:      --             TAC:         1F00 (7936)
  RSRQ (dB):     -17.3          Cell ID:     00798912 (7964946)
  SINR (dB):      0.2
  OK
Success
```

- **at at!impref?** -提供调制解调器固件和网络载波信息。


```
lte> at at!impref?
Running at!impref? command
AT command state: success
  !IMPREF:
   preferred fw version:    00.00.00.00
   preferred carrier name:  AUTO-SIM
   preferred config name:   AUTO-SIM_000.000_000
   preferred subpri index:  000
   current fw version:      02.33.03.00
   current carrier name:    VERIZON
   current config name:     VERIZON_002.079_001
   current subpri index:    000
  OK
success
```

在 **110-LTE-WiFi** 设备上配置 **LTE** 功能

September 2, 2022

您可以使用 LTE 连接将 Citrix SD-WAN 110-LTE-WiFi 设备连接到您的网络。本主题提供有关配置移动宽带设置、为 LTE 配置数据中心和分支设备等的详细信息。有关 Citrix 110-LTE-WiFi 硬件平台的更多信息，请参阅 Citrix SD-WAN 110 标准版设备。

> 注意
>
> - LTE 连接取决于 SIM 运营商或服务提供商网络。
> - 有关如何配置和管理网络中的所有 LTE 站点的信息，请参阅 LTE 固件模板。

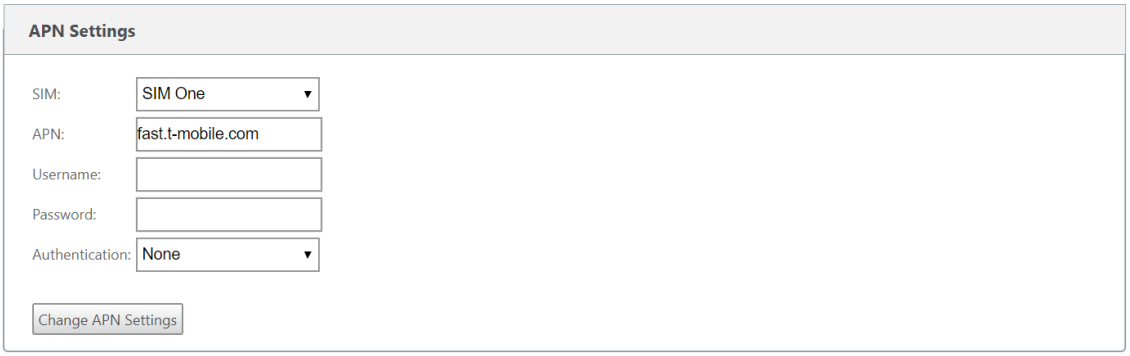
Citrix SD-WAN 110-LTE-无线上网入门

1. 打开设备电源，然后将 SIM 卡插入 Citrix SD-WAN 110-LTE-WiFi 设备的 SIM 卡插槽中。

   > 注意
   >
   > Citrix SD-WAN 110 轻型 WiFi 设备有两个标准 (2FF) SIM 卡插槽. 要使用微型（3FF）和纳米（4FF）大小的 SIM 卡，请使用 SIM 适配器。将较小的 SIM 卡扣入适配器。您可以从 Citrix 获取适配器作为现场可更换单元 (FRU) 或从 SIM 提供程序获取适配器。

2. 将天线固定到 Citrix SD-WAN 110 无线网络设备。有关更多信息，请参阅 安装 LTE 天线。
3. 打开设备的电源。
4. 配置 APN 设置。在 SD-WAN GUI 中，导航到 配置 **>** 设备设置 **>** 网络适配器 **>** 移动宽带 **> APN** 设置。

> 注意
>
> 从运营商处获取 APN 信息。

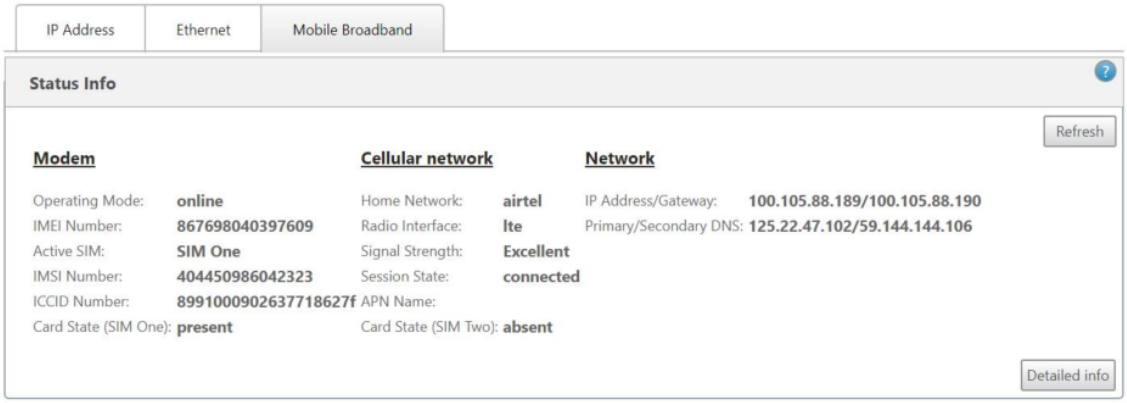


5. 选择 SIM 卡，输入运营商提供的 **APN**、用户名、密码和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。

   > 注意
   >
   > 所有这些字段都是可选的。

6. 单击 更改 **APN** 设置。
7. 在 SD-WAN 设备 GUI 中，导航到 配置 **>** 装置设置 > 网络适配器 > 移动宽带。

   您可以查看移动宽带设置状态信息。



以下是一些有用的状态信息：

- 操作模式：显示调制解调器状态。
- 活动 **SIM** 卡：在任何给定时间，只能有一个 SIM 卡处于活动状态。显示当前处于活动状态的 SIM 卡。
- 卡状态：存在表示 SIM 卡已正确插入。
- 信号强度：信号强度的质量-优秀、良好、公平、差或无信号。
- 家庭网络：插入的 SIM 卡的运营商。
- **APN** 名称：LTE 调制解调器使用的接入点名称。

- 会话状态：已连接表示设备已加入网络。如果会话状态已断开连接，请咨询运营商是否已激活帐户并启用数据计划。

SIM 卡首选项

您可以在 Citrix SD-WAN 110-LTE-WiFi 设备上插入两个 SIM 卡。在任何给定时间，只有一个 SIM 卡处于活动状态。选择 S **IM** 首选项：

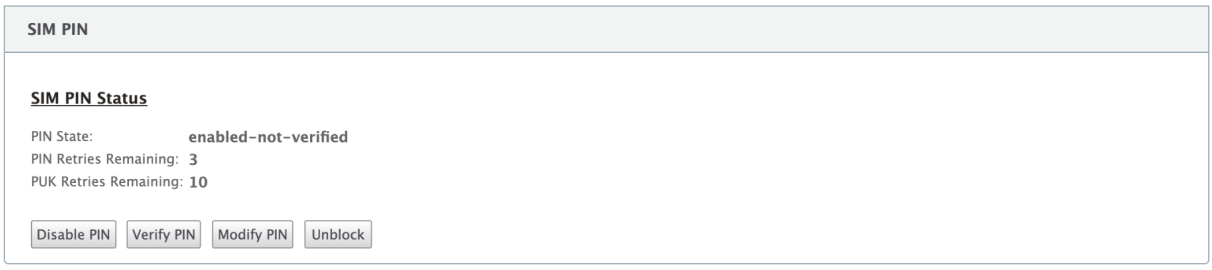
- 首选 **SIM** 卡 **1**：如果插入了两张 SIM 卡，则在启动时，LTE 调制解调器使用 SIM 卡 1（如果可用）。LTE 调制解调器启动并运行时，它将使用当时可用的 SIM 卡（SIM 卡 1 或 SIM 卡 2）。它会继续使用它，直到 SIM 处于活动状态。
- 首选 **SIM 2**：如果插入两个 SIM 卡，则在启动时 LTE 调制解调器使用 SIM Two（如果可用）。LTE 调制解调器启动并运行时，它将使用当时可用的 SIM 卡（SIM 卡 1 或 SIM 卡 2）。它会继续使用它，直到 SIM 处于活动状态。
- **SIM** 卡 **1**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM 卡 1。SIM 卡 1 始终处于活动状态。
- **SIM Two**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM 卡二。SIM 卡二始终处于活动状态。

SIM PIN

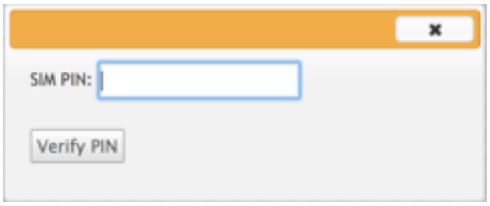
如果您插入了使用 PIN 锁定的 SIM 卡，则 SIM 卡状态为 启用未验证 状态。在使用 SIM 卡进行验证之前，您无法使用 SIM PIN。您可以从运营商处获取 SIM PIN。

> 注意
>
> SIM PIN 操作仅适用于活动的 SIM 卡。

要执行 SIM PIN 操作，请导航到配置 **>** 设备设置 **>** 网络适配器 **>** 移动宽带 **> SIM PIN**。



单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。

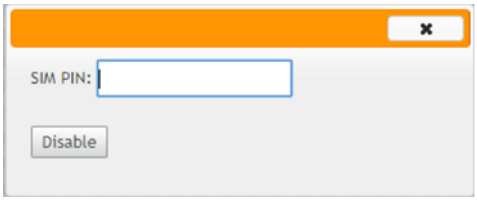


状态变为已 启用验证。

禁用 **SIM PIN**

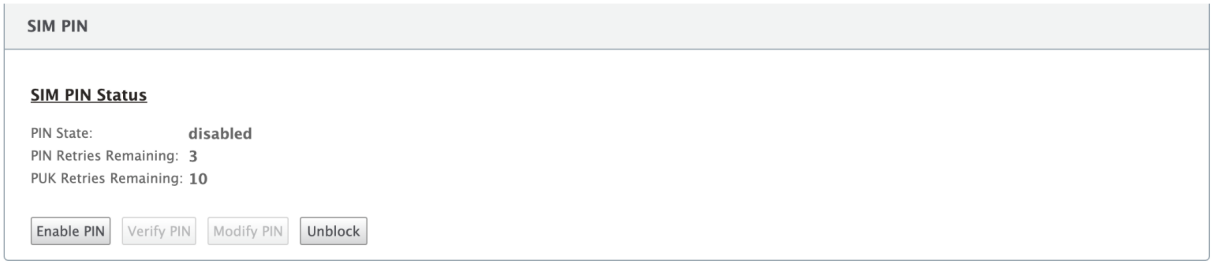
对于已启用和验证 SIM PIN 的 SIM 卡，您可以选择禁用 SIM 卡 PIN 功能。

单击 禁用 **PIN**。输入 **SIM PIN**，然后单击禁用。

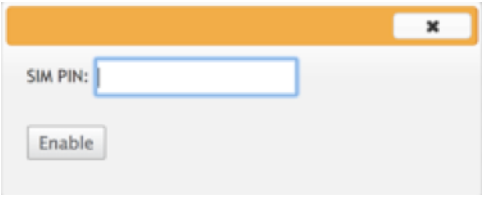


启用 **SIM PIN**

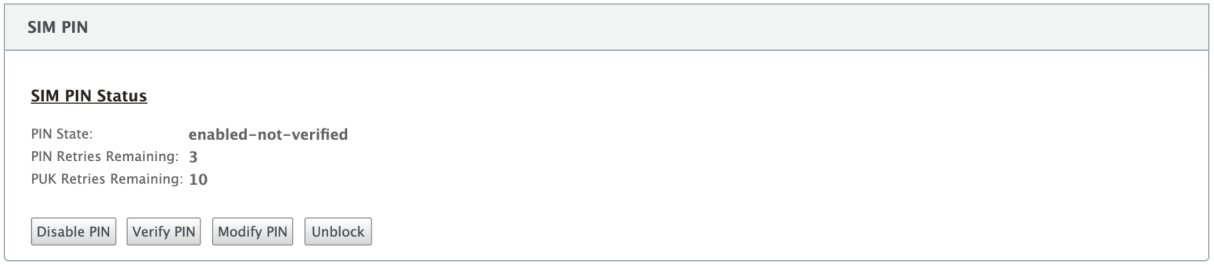
可以为禁用了 SIM PIN 的 SIM 启用 SIM PIN。



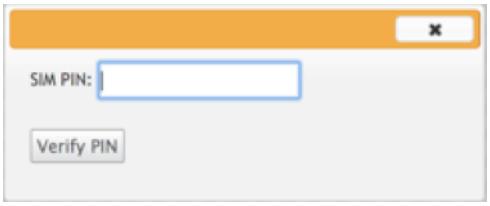
单击 启用 **PIN**。输入运营商提供的 SIM PIN，然后单击启用。



如果 SIM PIN 状态更改为 启用未验证，则表示 PIN 未经验证，并且在验证 PIN 之前您无法执行任何与 LTE 相关的操作。



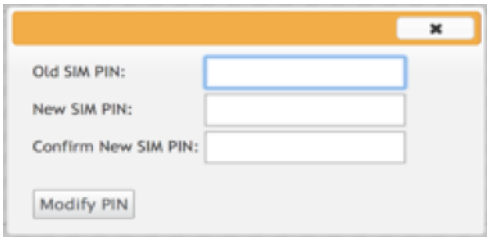
单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。



修改 **SIM PIN**

PIN 处于 启用验证 状态后，您可以选择更改 PIN。

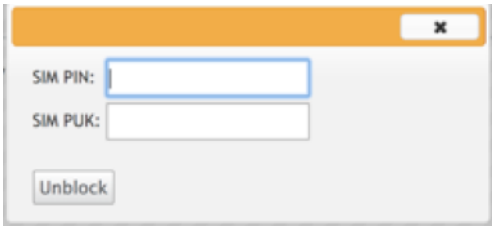
单击 修改 **PIN**。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 修改 **PIN**。



取消阻止 **SIM** 卡

如果您忘记了 SIM 卡 PIN 码，您可以使用从运营商获得的 SIM PUK 重置 SIM 卡 PIN 码。

要取消阻止 SIM 卡，请单击 取消阻止。输入您选择的 **SIM** 卡 **PIN** 码。输入从运营商处获得的 **SIM PUK** ，然后单击解锁。



> 注意：
> SIM 卡被永久阻止，并且 10 次 PUK 尝试失败，同时解除阻止 SIM 卡。您需要联系运营商服务提供商以获取新的 SIM 卡。

网络设置

您可以在支持内部 LTE 调制解调器的 Citrix SD-WAN 设备上选择移动网络。支持的网络包括 3G、4G 或两者。

漫游

默认情况下，LTE 设备上启用漫游选项，您可以选择禁用它。

启用/禁用调制解调器

启用/禁用调制解调器，具体取决于您使用 LTE 功能的意图。默认情况下，LTE 调制解调器处于启用状态。

重启调制解调器

重新启动调制解调器。重新启动操作最多可能需要 7 分钟才能完成。

刷新 **SIM** 卡

如果 110-LTE-WiFi 调制解调器无法正确检测 SIM 卡，请使用此选项。

> 注意
>
> 刷新 SIM 卡操作仅适用于活动 SIM 卡。

使用 **CLI** 配置 **LTE** 功能

要使用 CLI 配置 110 轻型 WiFi 调制解调器，请执行以下操作：

1. 登录到 Citrix SD-WAN 设备控制台。
2. 在提示符处，键入用户名和密码以获取 CLI 接口访问权限。
3. 在提示符处，键入命令 **lte**。键入 **>** 帮助。这将显示可用于配置的 LTE 命令列表。

```
lte> help
Usage
    ?|help                                          # Print this message
    status [default|verbose]                        # Show status
    show                                            # Show configuration
    select [1|2] [1|2]                              # Show or choose modem and/or sim to work
    enable                                          # Enable the selected modem
    disable                                         # Disable the selected modem
    apn <apn> [<username> [<password> [<NONE|PAP|CHAP|PAPCHAP>]]]   # Set APN
    sim-prefer <prefer|use> <1|2>                   # Prefer to use or use SIM one or two
    sim-power <show|off|on|reset>                   # Show, off, on, reset SIM card power
    sim-pin <show>                                  # SIM card pin status
    sim-pin <verify|disable|enable> <sim pin>       # Verify/Disable/Enable SIM card PIN
    sim-pin <modify> <old pin> <new pin>            # Modify SIM card PIN
    sim-pin <unblock> <sim puk> <sim pin>           # Unblock SIM card PIN
    reboot                                          # Reboot modem
    list-fw                                         # List available firmware
    upload-fw <fw file>                             # Upload firmware file
    apply-fw <fw> [keep-AUTO-SIM]                   # Apply firmware
    delete-fw <fw>                                  # Delete firmware
    session <show|stop|start>                       # Show/stop/start data session
    exit|quit                                       # Exit LTE CLI
```

下表列出了 **LTE** 命令描述。

命令	说明
帮助 {lte>help}	列出可用 LTE 命令和参数
状态 {lte> 状态}	显示 LTE 连接状态
显示 {lte>show}	显示 LTE 设置
禁用 {lte> 禁用}	禁用 LTE 调制解调器
启用 {lte> 启用}	启用 LTE 调制解调器
Apn {lte>apn}	配置 APN 设置信息
SIM-关闭电源、打开、重置 > {lte> sim-关机、打开、重置}	关闭 SIM 卡电源、打开 SIM 卡电源、刷新 SIM 卡
Select [1|2] [1|2] {lte>select [1|2] [1|2]}	选择 LTE 调制解调器的 SIM 卡。
SIM 偏好 {lte> 简单-首选}	选择首选或要使用的 SIM 卡。
SIM PIN {lte>sim-pin}	SIM 密码相关操作

命令	说明
Reboot {lte>reboot}	重新启动 LTE 调制解调器

> 注意
>
> 110-LTE-WiFi 设备不支持与固件相关的操作。

LTE 上的零接触部署

SD-WAN 110 SE 设备支持通过管理端口和数据端口对 SD-WAN 设备进行第 0 天 Provisioning 和第 n 天管理

通过 LTE 启用零接触部署服务的先决条件：

1. 安装天线，打开设备电源，然后插入 SIM 卡。
2. 确保 SIM 卡具有激活的数据计划。
3. 确保未连接管理/数据端口。
    - 如果管理/数据端口已连接，请断开管理/数据端口的连接。
    - 如果在管理/数据接口上配置了静态 IP 地址，则必须使用 DHCP 配置管理/数据接口，应用配置，然后断开管理/数据端口的连接。
4. 确保 110-LTE-WiFi 设备配置具有为 LTE 接口定义的 Internet 服务。

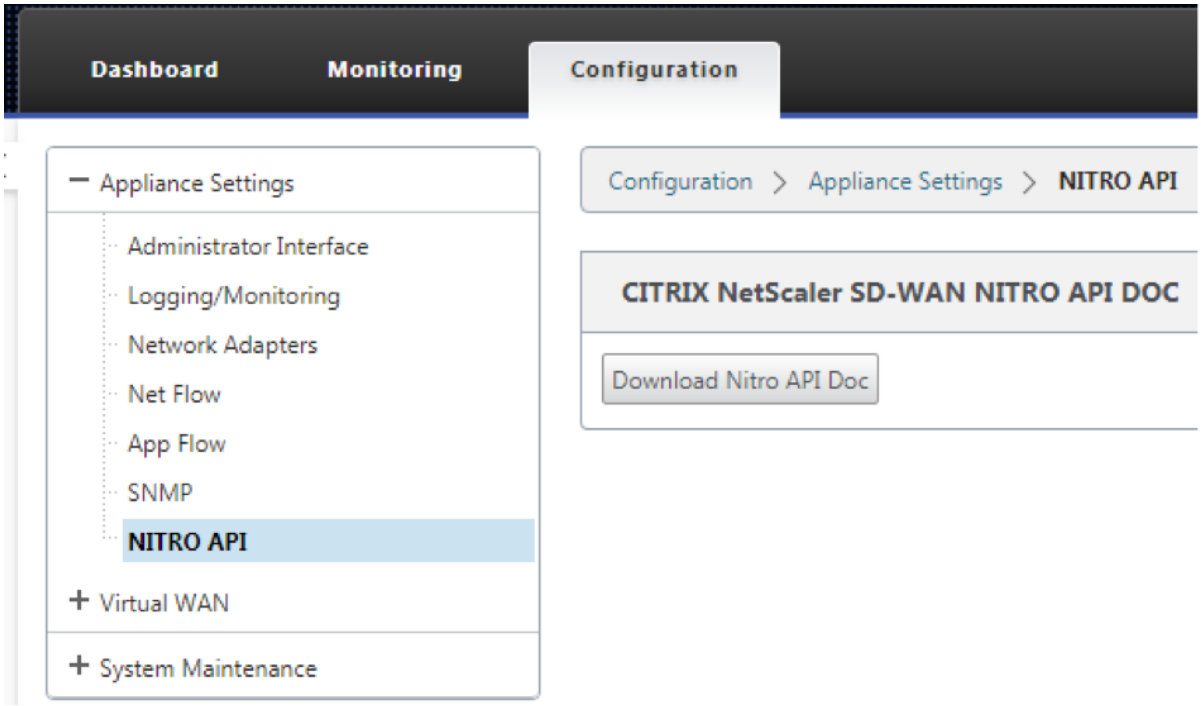
打开设备电源后，零接触部署服务将使用 LTE 端口获取最新的 SD-WAN 软件和 SD-WAN 配置。

通过管理/数据接口提供零接触部署服务，适用于 **110-SE LTE** 设备

将管理/数据端口连接到 Internet，并使用所有其他非 LTE 平台支持的标准 零接触部署程序 。

LTE REST API

有关 LTE REST API 的信息，请导航到 SD-WAN GUI，然后转到 配置 **>** 装置设置 **> NITRO API**。单击下载 **Nitro API** 文档。Citrix SD-WAN 11.0 中引入了用于 SIM PIN 功能的 REST API。



AT 命令

AT 命令有助于监控和排除 LTE 调制解调器的配置和状态。AT 是 **AtTension** 的缩写。由于每个命令行都以 **at** 开头，因此它们称为 AT 命令。支持 LTE 的 Citrix SD-WAN 平台型号支持运行 AT 命令。AT 命令是特定于调制解调器的，因此 AT 命令的列表因平台而异。

要运行 AT 命令，请执行以下步骤：

1. 登录到 Citrix SD-WAN 设备控制台。
2. 在提示符处，键入用户名和密码以获取 CLI 接口访问权限。
3. 在提示符下，键入 **LTE**。
4. 输入 **at** 然后输入 AT 命令。

以下是该命令的一个示例：

- 在 **at+cpin** —提供 SIM 卡状态信息。

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```


配置外部 **USB LTE** 调制解调器

September 2, 2022

您可以在某些 Citrix SD-WAN 设备上连接外部 3G/4G USB 调制解调器。这些设备使用 3G/4G 网络和其他连接来形成一个虚拟网络，以聚合带宽并提供弹性。如果其他接口出现连接故障，则通过 USB LTE 调制解调器自动重定向流量。以下设备支持外部 USB 调制解调器：

- Citrix SD-WAN 210 SE
- Citrix SD-WAN 210 东南 LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 Wi-Fi SE
- Citrix SD-WAN 110 LTE 无线网络 SE
- Citrix SD-WAN 1100 SE
- Citrix SD-WAN 2100 SE

Citrix SD-WAN 210 SE LTE 和 Citrix SD-WAN 110 LTE Wi-Fi SE 设备具有内置的 LTE 调制解调器。这些设备支持主动双 LTE。

CDC 以太网、MBIM 和 NCM 是支持的三种外部 USB 调制解调器类型。您可以在 MBIM 和 NCM USB 调制解调器上配置 **APN** 设置和启用/禁用调制解调器。CDC 以太网 USB 调制解调器不支持移动宽带操作。

> 注意
>
> 调制解调器类型为 MBIM 的外部 LTE 加密狗在 Citrix SD-WAN 2100 平台上无法正常工作。

连接 **USB** 调制解调器

根据无线运营商提供的指南启用和测试 USB 调制解调器。

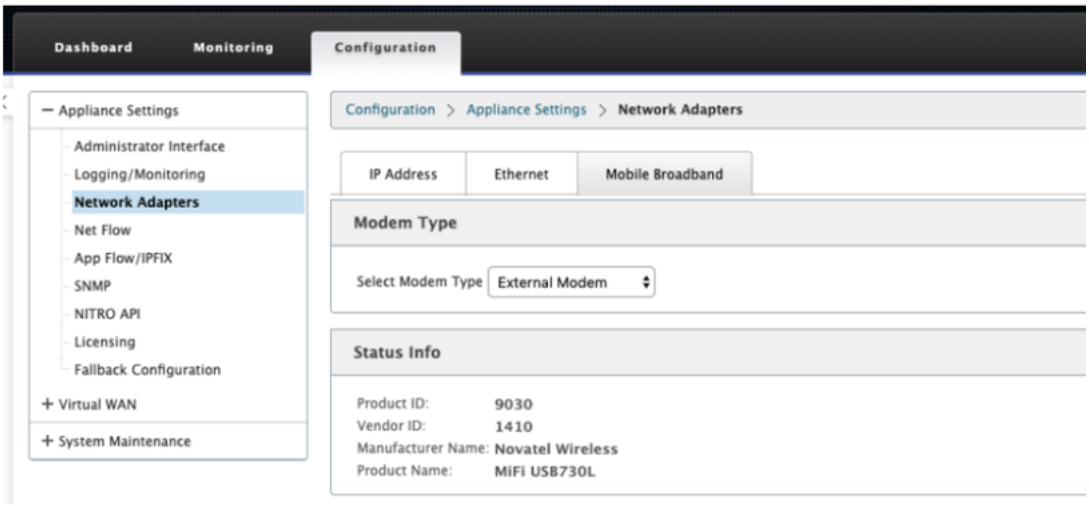
外部 LTE 调制解调器的配置：

- 使用支持的 USB LTE 转换器。支持的加密狗硬件型号是 Verizon USB730L 和 AT & T USB800。
- 确保将 SIM 卡插入 USB LTE 转换器。CDC 以太网 LTE 转换器预配置了静态 IP 地址，如果未插入 SIM 卡，则会干扰配置并导致连接故障或间歇性连接。
- 将 CDC 以太网 LTE 转换器插入 SD-WAN 设备之前，请将外部 USB 棒连接到 Windows /Linux 计算机，并确保 Internet 正常工作，使用正确的 APN 和移动数据漫游配置。确保 USB 加密狗的 连接模式 已从默认值“手动”更改为“自动”。

> 注意
>
> - Citrix SD-WAN 设备一次只支持一个 USB LTE 转换器。如果插入了多个 USB 转换器，请拔下所有转换器，然后仅插入一个转换器。
> - Citrix SD-WAN 设备不支持 USB 调制解调器的用户名和密码。确保在安装过程中禁用了调制解调器上的

> 用户名和密码功能。
> - 拔下或重新启动外部 MBM 转换器会影响内部 LTE 调制解调器数据会话。这是预期的行为。
> - 插入外部 LTE 调制解调器时，SD-WAN 设备需要大约 3 分钟才能识别它。

要查看外部调制解调器详细信息，请在设备 UI 中导航到 配置 > 装置设置 > 网络适配器 > 移动宽带。选择 外部调制解调器 作为调制解调器



> 注意：
>
> LTE USB 加密狗型号不显示在 状态信息 部分。

移动宽带运营

CDC 以太网和 MBIM /NCM 外部调制解调器支持的操作：

操作	外部调制解调器-CDC 以太网	外部调制解调器-MBIM 和 NCM
SIM 卡首选项	否	否
SIM PIN	否	否
APN 设置	否	是
网络设置	否	否
漫游	否	否
管理固件	否	否
启用/禁用调制解调器	否	是
重启调制解调器	否	否
刷新 SIM 卡	否	否

配置外部 **USB** 调制解调器

您可以通过 Citrix SD-WAN Orchestrator 服务使用外部 USB 调制解调器配置 LTE 站点。有关更多信息，请参阅 LTE 固件升级。

LTE 上的零接触部署

通过 USB LTE 调制解调器启用零接触部署服务的先决条件：

- 将 USB 调制解调器插入 Citrix SD-WAN 设备中。有关详细信息，请参阅 连接 USB 调制解调器。
- 确保 USB 调制解调器上的 SIM 卡具有激活的数据套餐。
- 确保未连接管理/数据端口。如果管理/数据端口已连接，请断开连接。
- 确保设备配置具有为 LTE 接口定义的 Internet 服务。

设备打开电源时，零接触部署服务使用 LTE-E1 端口获取最新的 SD-WAN 软件和配置。

有关通过 SD-WAN Orchestrator 服务进行零接触部署的信息，请参阅 零接触部署。

支持的 **USB** 调制解调器

以下调制解调器与 Citrix SD-WAN 设备兼容。

> 注意
>
> Citrix 不控制无线运营商固件更新。因此，不能保证新的调制解调器固件与 Citrix SD-WAN 软件的兼容性。客户控制调制解调器固件更新。Citrix 建议在将固件更新推送到整个网络之前，先在单个站点上测试固件更新。

地理区域	无线承运人/制造商	USB 调制解调器	支持调制解调器	接口
美国	Verizon	全局调制解调器 USB730L	cdc_ether	仅限 4G
美国	AT&T	AT&T 全局调制解调器 USB800	cdc_ether	仅限 4G

AT 命令

AT 命令有助于监控和排除 LTE 调制解调器的配置和状态。AT 是 **AtTension** 的缩写。由于每个命令行都以 **at** 开头，因此它们称为 AT 命令。支持 LTE 的 Citrix SD-WAN 平台型号支持运行 AT 命令。AT 命令是特定于调制解调器的，因此 AT 命令的列表因平台而异。

要运行 AT 命令，请执行以下步骤：

1. 登录到 Citrix SD-WAN 设备控制台。
2. 在提示符处，键入用户名和密码以获取 CLI 接口访问权限。
3. 在提示符下，键入 **LTE**。
4. 输入 **at** 然后输入 AT 命令。

以下是该命令的一个示例：

在 **at+cpin** —提供 SIM 卡状态信息。

```
lte> at at+cpin?
Running at+cpin? command
AT command state: success
  +CPIN: READY
  OK
success
```

部署

September 2, 2022

以下是使用 Citrix SD-WAN 设备实现的一些使用案例方案：

- 在网关模式下部署 SD-WAN
- 内联模式
- 在 PBR 模式下部署 SD-WAN（虚拟内联模式）
- 分支到分支通信的动态路径
- WAN 到 WAN 转发
- 构建 SD-WAN 网络
- 局域网分段路由
- 零接触部署
- 单一区域部署
- 多区域部署
- 高可用性

清单以及如何部署

September 2, 2022

强烈建议在开始安装之前，先阅读 Citrix 虚拟 WAN 部署规划指南。本文讨论基本的虚拟 WAN 概念和功能，并提供规划部署的指南。

准备部署

以下列表概述了部署 SD-WAN 标准版所涉及的步骤和过程。

要查看一些部署使用案例，请参阅 部署。

1. 收集 Citrix SD-WAN 部署信息。
2. 设置 Citrix SD-WAN 设备。
    - 对于要添加到 SD-WAN 部署的每个硬件设备，必须完成以下任务：
        - 设置设备硬件。
        - 设置设备的管理 IP 地址并验证连接。
        - 设置设备上的日期和时间。
        - （可选）将控制台会话 超时 间隔设置为高值或最大值。
3. 在设备上上载并安装软件许可证文件。

安装和配置清单

为要部署的每个 SD-WAN 站点收集以下信息：

- 产品的许可信息
- 要部署的每个设备所需的网络 IP 地址：
    - 管理 IP 地址
    - 虚拟 IP 地址
    - 站点名称
    - 设备名称（每个站点一个）
    - SD-WAN 设备型号（针对要部署的每个设备）
    - 部署模式（MCN 或客户端）

- 拓扑
- 网关 MPLS
- GRE 通道信息
- 路由
- VLAN
- 每个电路在每个站点的带宽

最佳做法

September 2, 2022

本文概述了 Citrix SD-WAN 解决方案的部署最佳做法。它为以下 Citrix SD-WAN 部署模式提供了一般指导、优势和使用案例。

边缘/网关模式

建议

以下是 网关 模式部署的建议：

1. 网关模式最适用于 SD-WAN 分支，其中路由器进行整合，客户已准备好允许 SD-WAN 作为终止连接的边缘设备。
2. 当从头开始构建项目时，可以通过严格的设计来呈现出色的网络架构。

> 注意：
>
> 网关模式可以在数据中心端用于存在某些基础设施中断的现有项目。

优点/使用案例

以下是网关模式部署的优势/使用案例：

1. 客户分支机构的路由器/防火墙/网络元素合并的最佳使用案例。
2. 通过 DHCP 进行简单、方便的局域网主机管理。
    - 允许 SD-WAN 成为下一跳，并为数据端口的所有 LAN 主机提供基于 DHCP 的 IP 地址。
3. 所有连接都在 SD-WAN 边缘/网关终止，管理变得简单。

4. SD-WAN 是边缘路由的焦点，可控制所有流量。决策是在边缘到突破、回传或覆盖（包括带宽/容量计算）上做出的。
5. 作为 LAN 主机的所有 LAN 子网主机都允许将 SD-WAN LAN VIP 用作下一跳。如果 SD-WAN LAN 连接到核心交换机，则可以运行动态路由以获得所有 LAN 子网的可见性。
6. 高可用性 (HA) 的极大灵活性-严格建议 Gateway 模式，以便站点以主动/备用模式运行。此外，它有助于防止 SD-WAN 设备出现故障时的流量黑洞。
    - 分支机构提供的交换机-并行高可用性可以在 Gateway 模式下工作。
    - 分支机构不可用的交换机—SD-WAN 也可以在 SD-WAN 边缘高可用性模式（失效到线高可用性模式）下运行，其中两个 SD-WAN 盒以菊花链形式连接，以便利用故障到线端口充当融合高可用性对。
7. 允许将 Internet 定义为 不受信任 的接口，这些接口会自动创建动态 NAT 以进行突破，并将连接源入 NAT，以便响应返回到 SD-WAN。
8. 不受信任 接口的安全考虑因素自然是隐含的，因为只允许 4980 上的 ICMP/ARP/UDP 控制数据包。

警告

以下是在网关模式下需要注意的信息：

- 谨慎的设计和网络架构 -网关模式可能需要仔细的设计和网络考虑因素，因为整个分支/边缘网络都在 SD-WAN 中。阻止什么，路由什么，如何连接 LAN，如何终止 WAN 等。
- 设备故障 - 边缘模式不能具有故障到线功能。当设备关闭时，整个分支都会关闭。
- 安全态势 -由于路由在边缘管理，因此防火墙、中断/回程等安全状况至关重要，必须与客户一起构思。
- 高可用性—故障到线的高可用性必须有一些端口可用性考虑因素，并且根据部署的不同，可能会变得难以设计。
    - SD-WAN 110 不是一个选项，因为它没有故障到线端口。

例如，如果您需要 2 条 WAN 链路才能运行，则需要 5 个端口，其中包括一个用于高可用性接口（包括 LAN 接口）的专用端口。

串联模式—故障到线/故障到模块

建议

以下是内联模式部署的建议：

1. 内联模式最适合那些不更改现有基础架构且 SD-WAN 与 LAN 网段透明地内联的分支机构。
2. 数据中心还可以采用内联故障到线或串联并行高可用性，因为确保数据中心工作负载不会因设备故障/崩溃而被遮蔽至关重要。

优势和使用案例

以下是内联模式部署的优势/使用案例：

1. 因此，保持 MPLS 路由器失效到线是一个可爱的功能。支持故障到线的设备能够在包装箱出现故障时无缝故障切换到底层基础架构。

    - 如果您的设备支持故障到线（SD-WAN 210 及更高版本），这允许在 SD-WAN 崩溃/关闭时将单个 SD-WAN 内联到硬件绕过 LAN 流量传送到客户边缘路由器。
    - 如果存在 MPLS 链路，能够自然扩展到客户的 LAN/Intranet，则故障到线桥对端口是最佳选择（支持故障到线路的对），因此，当设备崩溃或停机时，LAN 流量会绕过硬件到客户边缘路由器（仍然保持下一个跳）。

2. 网络很简单。
3. SD-WAN 可以通过串联模式查看所有流量，因此这是适当的带宽/容量计算的最佳情况。
4. 集成要求很少，因为您只需要 L2 网段的 IP。LAN 段是众所周知的，因为您有一个通向 LAN 接口的臂。如果您连接到核心交换机，您还可以运行动态路由以获得所有 LAN 子网的可见性。
5. 客户的期望是，SD-WAN 必须将其作为新的网络节点融入现有基础架构（没有其他任何变化）。
6. 代理 **ARP** —在内联模式下，如果网关关闭或者 SD-WAN 接口向下一跳停机，SD-WAN 将 ARP 请求代理到局域网下一跳是一种祝福。

    - 通常，在具有多个 WAN 连接 (MPLS/Internet) 的网桥对（故障到块或故障到线）的串联模式下，建议为将 LAN 主机连接到其下一跳 Gateway 的网桥对接口启用代理 ARP。
    - 出于任何原因，当下一跳 Gateway 闭或 SD-WAN 接口到下一跳时，SD-WAN 将充当 ARP 请求的代理，允许 LAN 主机仍然无缝地发送数据包，并使用剩余的 WAN 连接保持虚拟路径正常运行。

7. 高可用性—如果故障到线无法选择，则可以将设备置于并行高可用性（主动/备用的通用 LAN 和 WAN 接口）设备中以实现冗余。

    - 如果您的设备不支持故障到线（如 SD-WAN 110），则必须采用内联并行高可用性，以便在主设备出现故障时启动备用设备。

警告

以下是在内联模式下需要注意的信息：

- 管道网络与 SD-WAN（LAN 和 WAN 端）有两个臂，需要一些停机时间，因为网络必须用两个臂管道。
- 必须确保是否使用故障到线路，它位于 受信任 区域中的客户边缘路由器/防火墙的后面，以免安全性受到威胁。
- MPLS QoS 稍有改变，因为之前的 QoS 策略可能取决于源 IP 地址或基于 DSCP 的 DSCP，现在由于覆盖而被屏蔽。

- 必须注意重新调整 MPLS 路由器的用途，使其具有特定 DSCP 标签的经过精心设计的 SD-WAN 特定预留带宽，以便 SD-WAN 的 QoS 负责排定流量的优先级，并立即发送其他类的高优先级应用程序（但能够考虑整体带宽为 MPLS 路由器上的 SD-WAN 保留）。MPLS 队列是一种替代或 MPLS 在自动路径组上设置单个 DSCP，可以处理此问题。
- 如果客户边缘路由器上的链路终止时 Internet 接口是 可信 的，则要使用 Internet 服务，则必须编写独占动态 NAT 规则以启用从设备中断 Internet 。
- 如果 Internet 链路是唯一的 WAN 连接，并且仍然在客户边缘路由器上终止，则如果客户边缘路由器采取预防措施，通过其现有的底层基础架构引导数据包，则绕过这些连接仍然是可以的。
  - 必须适当谨慎地考虑到通过 Internet 连接的网桥对绕过 LAN 流量以及设备出现故障时的流动。由于这是一个敏感的企业 Intranet 流量，因此在发生故障的前夕，客户必须知道如何处理它。

虚拟内联/单手模式

建议

以下是虚拟内联模式部署的建议：

1. 虚拟内联模式是数据中心网络的最佳选择，因为 SD-WAN 网络管道可以在数据中心利用现有基础架构为其现有工作负载提供服务时并行处理。
2. SD-WAN 位于单臂接口中，通过 VIP 上的 SLA 跟踪进行管理。如果跟踪发生故障，流量将通过现有底层基础设施恢复路由。
3. 也可以在虚拟内联模式下部署分支，但是在内联/网关部署中更主要。

优势和使用案例

以下是虚拟内联模式部署的优势/用例：

1. 在数据中心网络 SD-WAN 的最简单和推荐方式。
   - 虚拟内联模式允许使用前端核心路由器对 SD-WAN 进行并行网络管道。
   - 虚拟内联模式允许我们轻松定义 PBRs 转移 LAN 流量必须通过 SD-WAN 并获得覆盖的好处。
2. 如果 SD-WAN 发生故障，则无缝故障切换到底层基础架构，并在正常情况下无缝转发到 SD-WAN 以获得覆盖优势。
3. 简单的 网络 和 集成 要求。虚拟内联式从前端路由器到 SD-WAN 的单臂接口。
4. 易于在 仅导入模式下 部署动态路由（不导出任何内容），以获得 LAN 子网的可见性，以便将其发送到远程 SD-WAN 对等设备。
5. 易于在路由器上定义 PBR（每个 WAN VIP 1），以指示如何选择物理。

警告

以下是在虚拟内联模式下需要注意的信息：

- 必须适当注意将定义的 WAN 链路的 SD-WAN 逻辑 VIP 明确地映射到正确的物理接口（否则，这可能会导致 WAN 指标评估和 WAN 路径选择中出现不良问题）。
- 要知道所有流量是通过 SD-WAN 还是仅通过特定流量转移，需要进行适当的设计考虑。
- 这意味着 SD-WAN 必须专门用于自身的一些带宽份额，这些带宽必须在接口上设置，以便 SD-WAN 的容量不会被其他非 SD-WAN 流量使用，从而导致不良后果。
  - 如果 SD-WAN 链路容量定义不正确，则可能会出现带宽记帐问题和拥塞问题。
- 如果设计不当，如果 SD-WAN 路由数据中心和分支 VIP 导出到前端，并且如果路由受到到 SD-WAN 的影响，叠加数据包开始循环并导致不良后果，则动态路由可能会导致一些问题。
- 动态路由必须得到适当管理，考虑到学习内容/宣传内容的所有潜在因素。
- 单臂物理接口有时可能会成为瓶颈。在这些线路中需要一些设计考虑因素，因为它既能满足上传/下载的需求，也可以充当 LAN 到 LAN，从 SD-WAN 到 LAN 的流量。
- 在设计过程中，局域网到 LAN 的流量过多可能是一个值得注意的问题。
- 如果未使用动态路由，则必须适当小心管理所有 LAN 子网，否则可能会导致不良路由问题。
- 如果在虚拟内联的 SD-WAN 上定义一些默认路由 (0.0.0.0/0)，以指向前端路由器，则存在潜在的路由环路问题。在这种情况下，如果虚拟路径出现故障，则来自数据中心 LAN 的任何流量（例如监控流量）都会循环回头端并回到 SD-WAN，导致不希望的路由问题（如果虚拟路径关闭，远程分支子网将变为可访问 否 导致默认路由为 HIT，这会导致循环问题）。

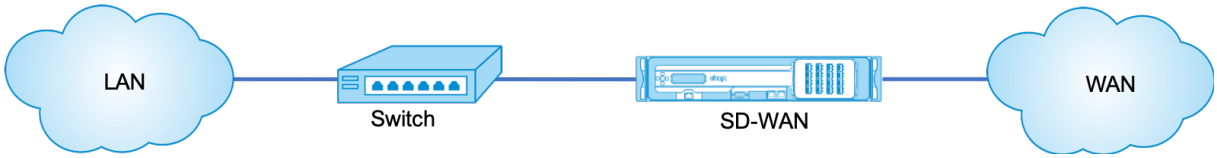
网关模式

September 2, 2022

Gateway 模式将 SD-WAN 设备置于路径中（双臂部署），并且需要对现有网络基础结构进行更改，以使 SD-WAN 设备成为该站点整个 LAN 网络的默认网关。Gateway mode used for new networks and router replacement. 网关模式允许 SD-WAN 设备：

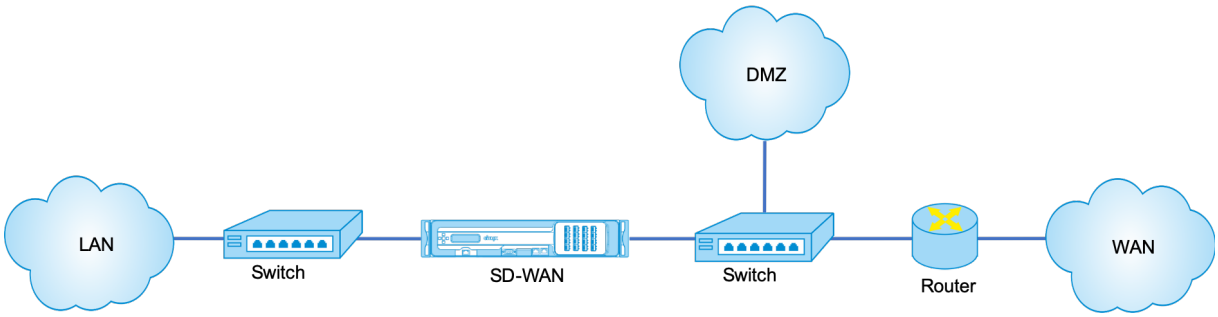
- 查看进出 WAN 的所有流量
- 执行本地路由

Citrix SD-WAN Orchestrator 服务支持网关部署模式。有关更多信息，请参阅 接口。



> 注意
>
> 在网关模式下部署的 SD-WAN 充当第 3 层设备，无法执行故障到线。所有涉及的接口都将被配置为 故障到阻止。如果设备出现故障，站点的默认 Gateway 也将出现故障，从而导致中断，直到还原设备和默认 Gateway 为止。

在 内联模式 下，SD-WAN 设备似乎是以太网桥。大多数 SD-WAN 设备型号都包括用于串联模式的 故障到线（以太网旁路）功能。如果电源发生故障，继电器会关闭，输入和输出端口通过电连接，从而允许以太网信号从一个端口传递到另一个端口。在故障到线模式下，SD-WAN 设备看起来像连接两个端口的交叉电缆。内联模式，用于集成到已经明确定义的网络中。

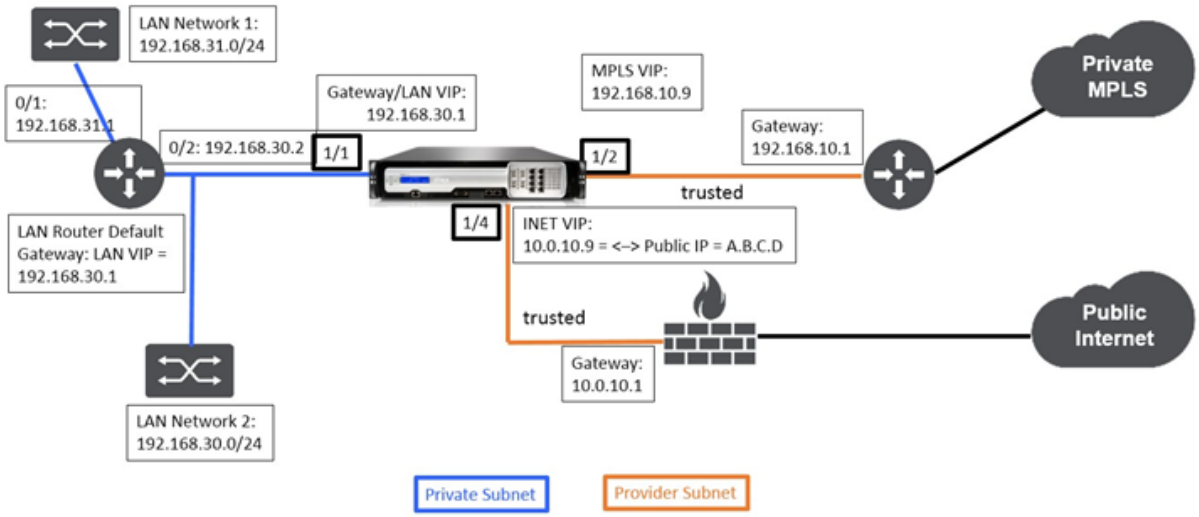


本文提供了在示例网络设置中在网关模式下配置 SD-WAN 设备的分步过程。还介绍了内联部署，以便分支端完成配置。如果删除了内联设备，网络可以继续运行，但如果删除网关设备，则会失去所有访问权限。

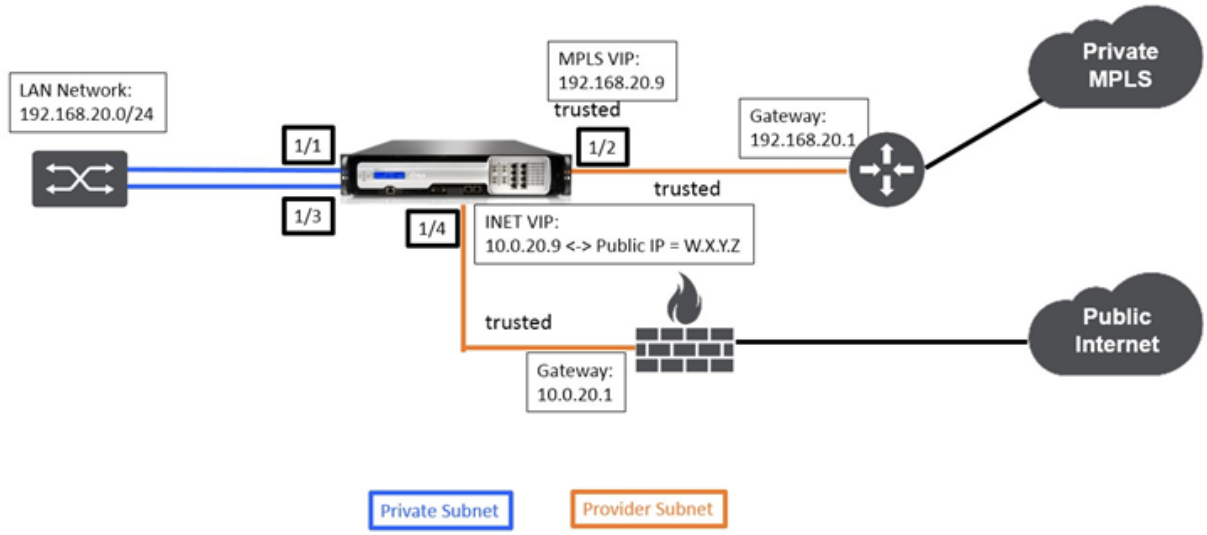
拓扑

下图描述了 SD-WAN 网络支持的拓扑。

Gateway 部署中的数据中心



内联部署中的分支



数据中心站点 **Gateway** 模式配置

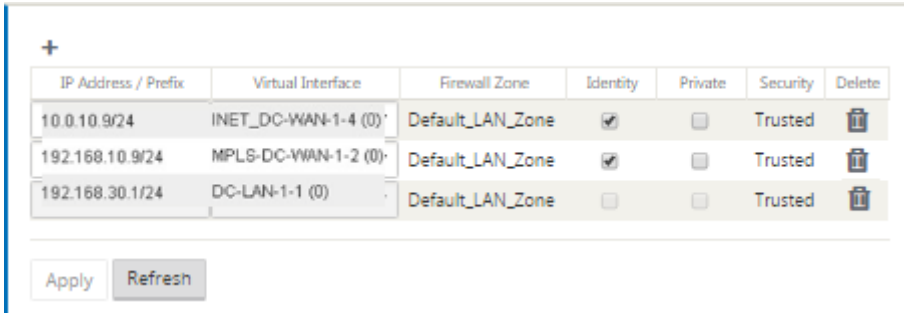
以下是配置数据中心站点网关部署的高级配置步骤：

1. 创建 DC 站点。
2. 基于连接的以太网接口填充接口组。
3. 为每个虚拟接口创建虚拟 IP 地址。
4. 使用 Internet 和 MPLS 链接基于物理速率而不是突发速度填充 WAN 链接。

5. 如果 LAN 基础结构中有更多子网，请填充路由。

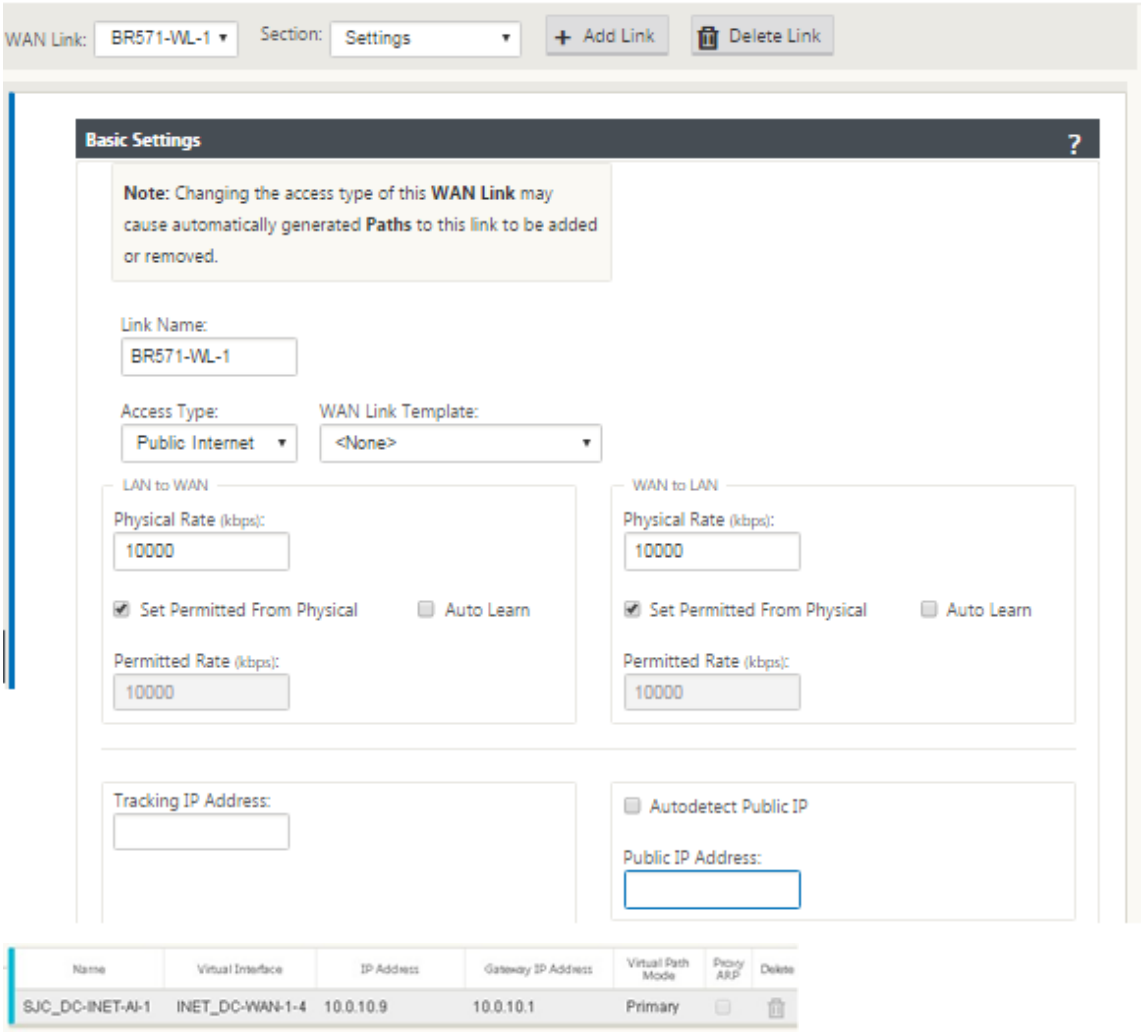
为每个虚拟接口创建虚拟 **IP (VIP)** 地址

1. 在适当的子网上为每个 WAN 链接创建 VIP。VIP 用于虚拟 WAN 环境中的两个 SD-WAN 设备之间的通信。
2. 创建一个虚拟 IP 地址，用作 LAN 网络的网关地址。



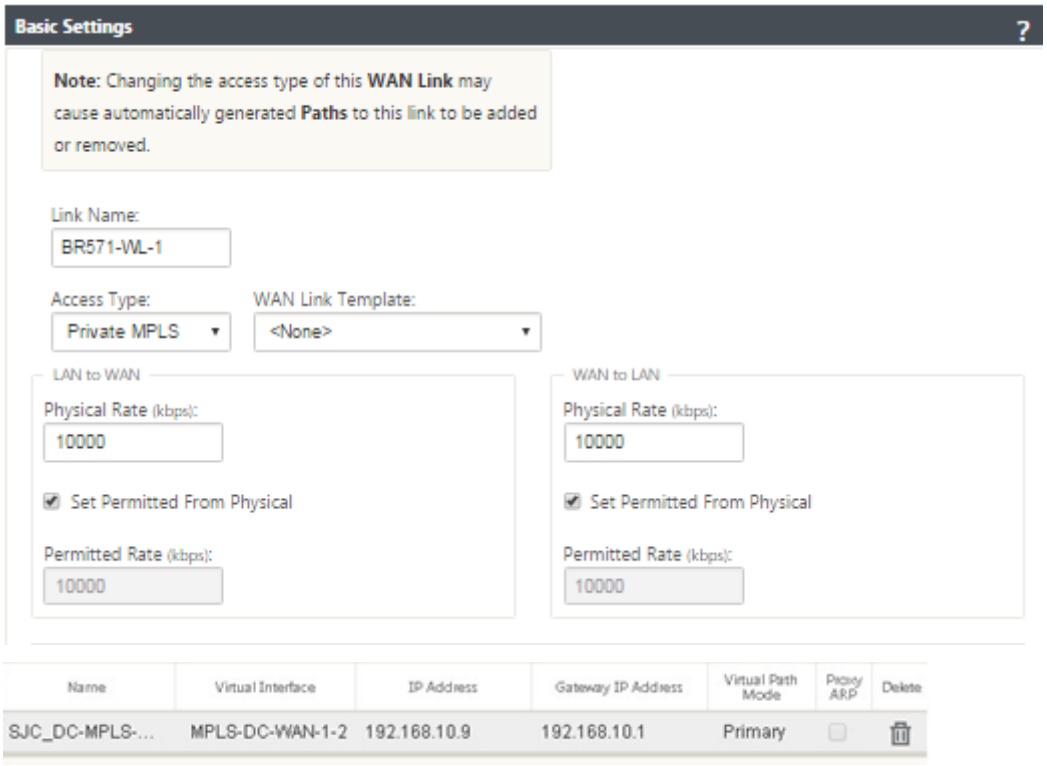
要使用 Internet 链路根据物理速率而不是突发速度填充 WAN 链路，请执行以下操作：

1. 导航到 **WAN** 链接，单击 **+** 添加链接 按钮为 Internet 链接添加 WAN 链接。
2. 填充 Internet 链接详细信息，包括提供的公有 IP 地址，如下所示。无法为配置为 MCN 的 SD-WAN 设备选择自动检测 公有 **IP**。
3. 从部分下拉菜单导航到 访问界面，然后单击 **+** 添加按钮以添 加特定于 Internet 链接的界面详细信息。
4. 填充 IP 和 Gateway 地址的访问接口，如下所示。



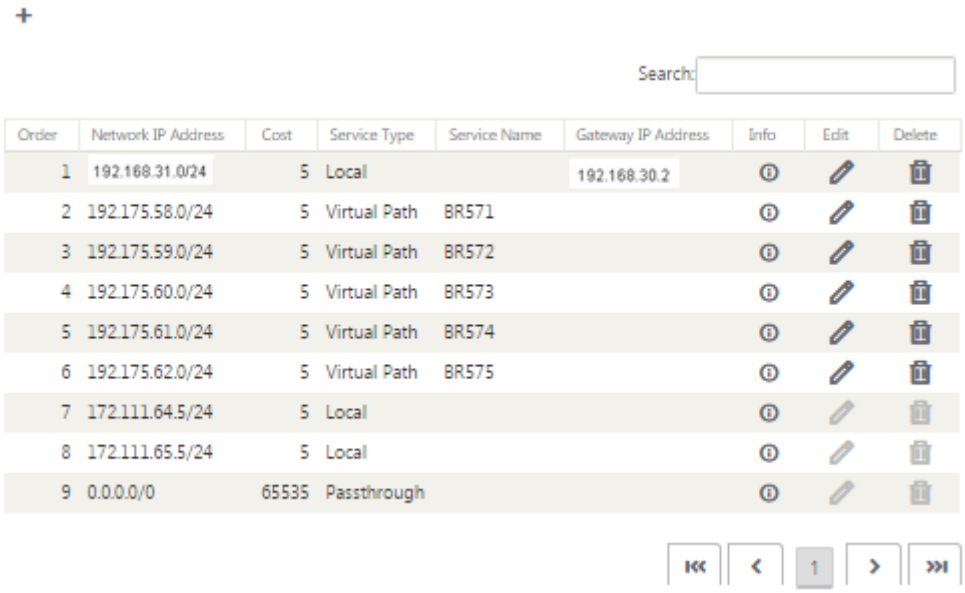
创建 **MPLS** 链接

1. 导航到 **WAN** 链接，单击 **+** 按钮为 MPLS 链接添加 WAN 链接。
2. 填充 MPLS 链接详细信息，如下所示。
3. 导航到 访问接口，单击 **+** 按钮添加特定于 MPLS 链接的接口详细信息。
4. 填充 IP 和 Gateway 地址的访问接口，如下所示。



填充路由

路由是基于上述配置自动创建的。上面显示的 DC LAN 拓扑示例有一个额外的 LAN 子网，即 **192.168.31.0/24**。需要为此子网创建路由。网关 IP 地址必须与直流 LAN VIP 位于同一子网中，如下所示。



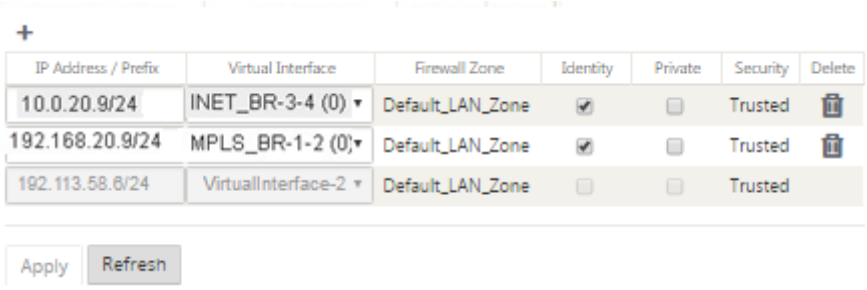
分支站点内联部署配置

以下是为内联部署配置分支站点的高级配置步骤：

1. 创建分支站点。
2. 基于连接的以太网接口填充接口组。
3. 为每个虚拟接口创建虚拟 IP 地址。
4. 使用 Internet 和 MPLS 链接基于物理速率而不是突发速度填充 WAN 链接。
5. 如果 LAN 基础结构中有更多子网，请填充路由。

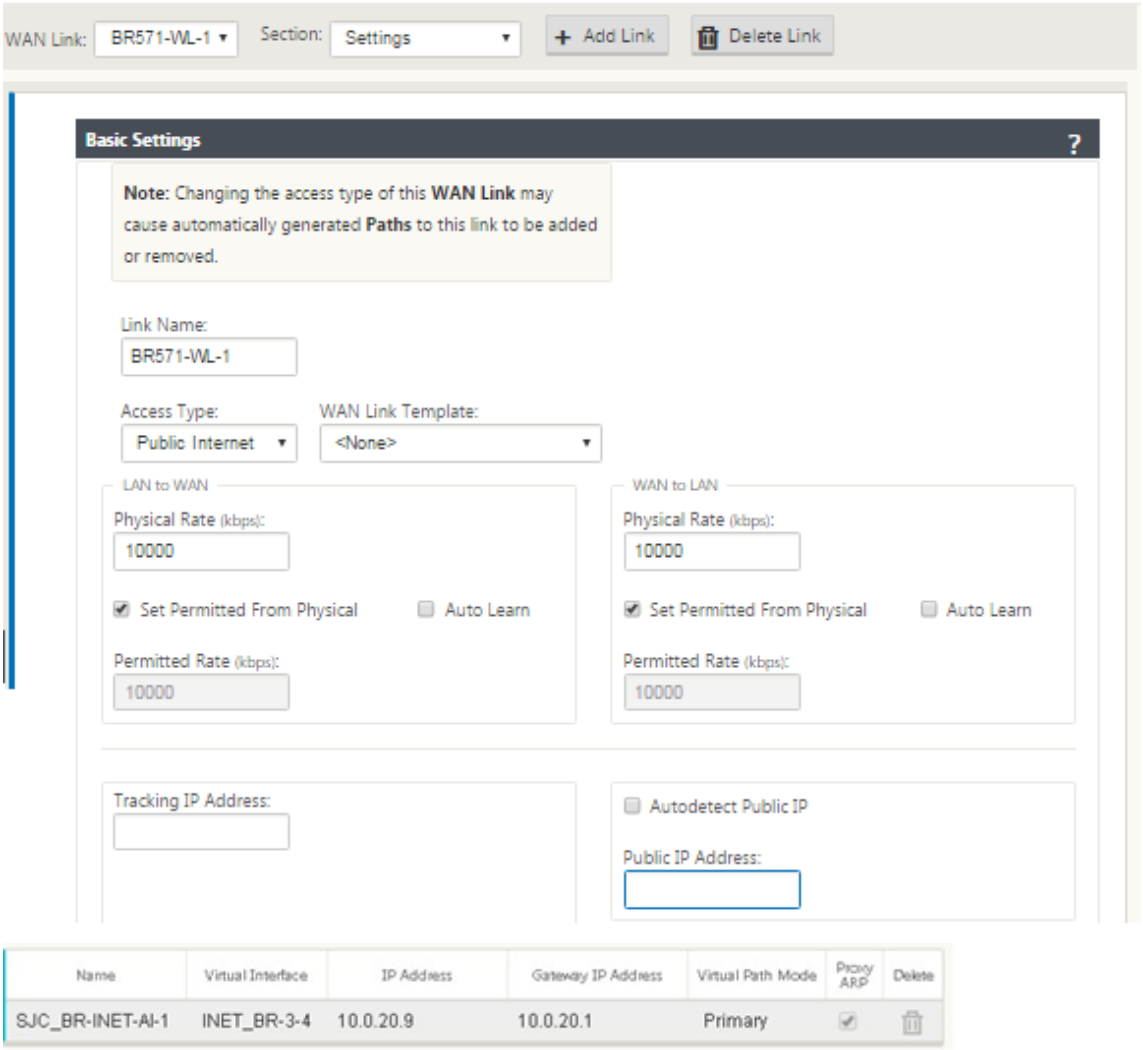
为每个虚拟接口创建虚拟 **IP (VIP)** 地址

1. 在相应的子网上为每个 WAN 链接创建一个虚拟 IP 地址。VIP 用于虚拟 WAN 环境中的两个 SD-WAN 设备之间的通信。



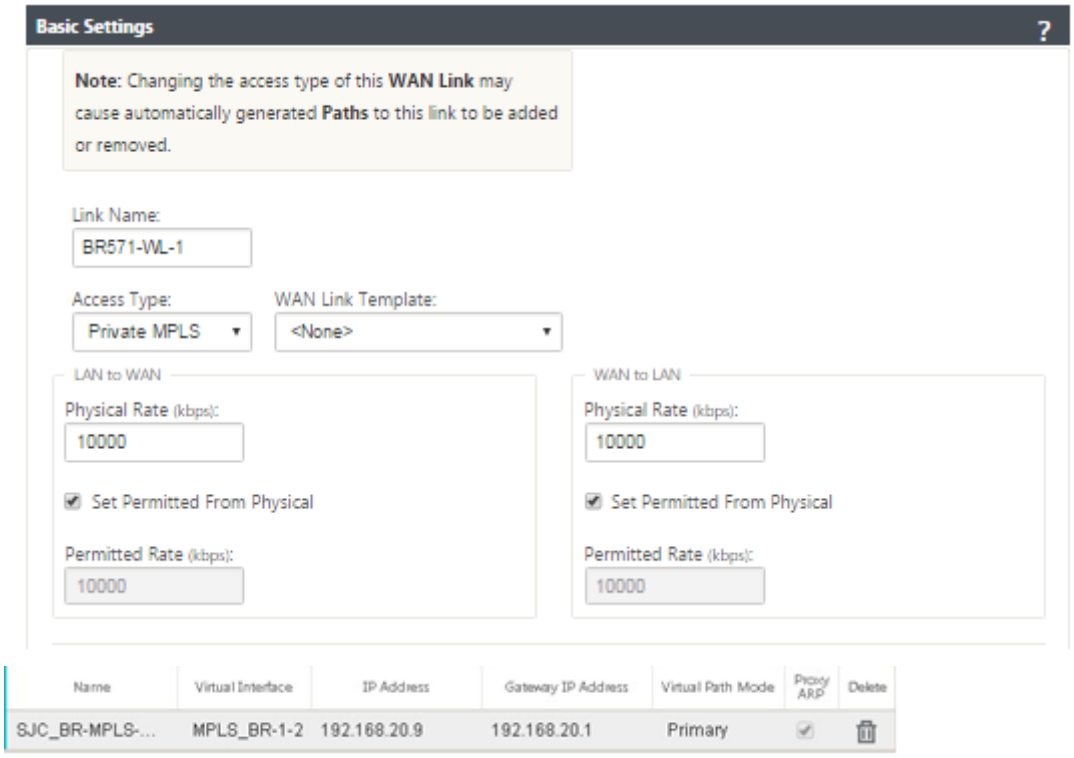
要使用 Internet 链路根据物理速率而不是突发速度填充 WAN 链路，请执行以下操作：

1. 导航到 **WAN** 链接，单击 **+** 按钮为 Internet 链接添加 WAN 链接。
2. 填充 Internet 链接详细信息，包括自动检测公有 IP 地址，如下所示。
3. 导航到 访问界面，单击 **+** 按钮以添加特定于 Internet 链接的界面详细信息。
4. 填充 IP 地址和 Gateway 的访问接口，如下所示。



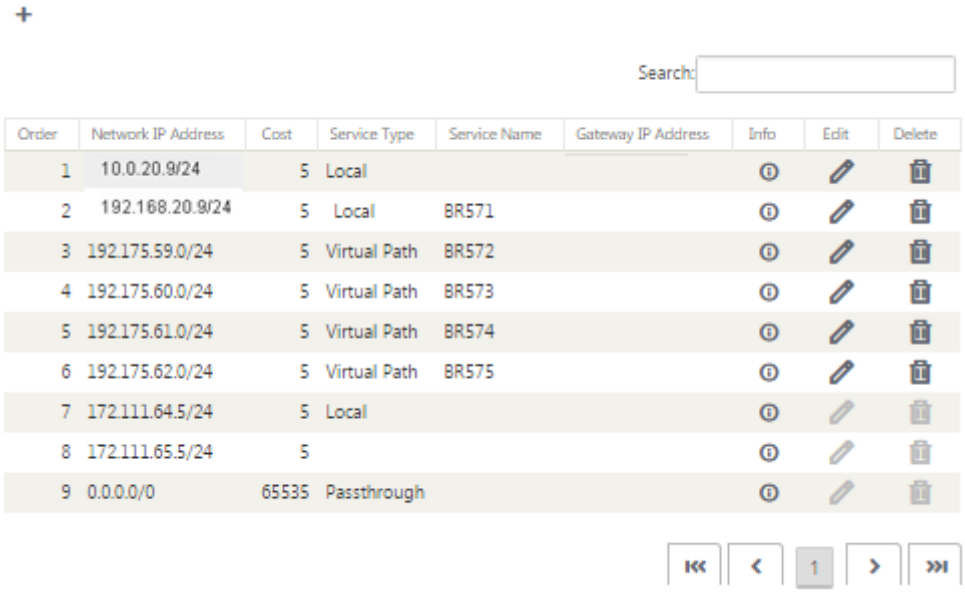
创建 **MPLS** 链接

1. 导航到 WAN 链接，单击 **+** 按钮为 MPLS 链接添加 WAN 链接。
2. 填充 MPLS 链接详细信息，如下所示。
3. 导航到访问接口，单击 **+** 按钮添加特定于 MPLS 链接的接口详细信息。
4. 填充 IP 地址和 Gateway 的访问接口，如下所示。



填充路径

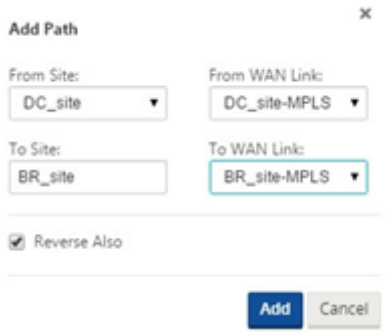
路由是基于上述配置自动创建的。如果有更多的子网特定于此远程分支机构，则需要添加特定的路由，以确定哪个 Gateway 将流量引导到达这些后端子网。



解决审计错误

完成 DC 站点和分支站点的配置后，系统将提醒您解决 DC 站点和 BR 站点上的审核错误。

默认情况下，系统会为定义为访问类型公共 Internet 的 WAN 链接生成路径。您需要使用自动路径组功能或手动启用具有专用 Internet 访问类型的 WAN 链接的路径。通过单击“添加”运算符（绿色矩形中），可以启用 MPLS 链接的路径。



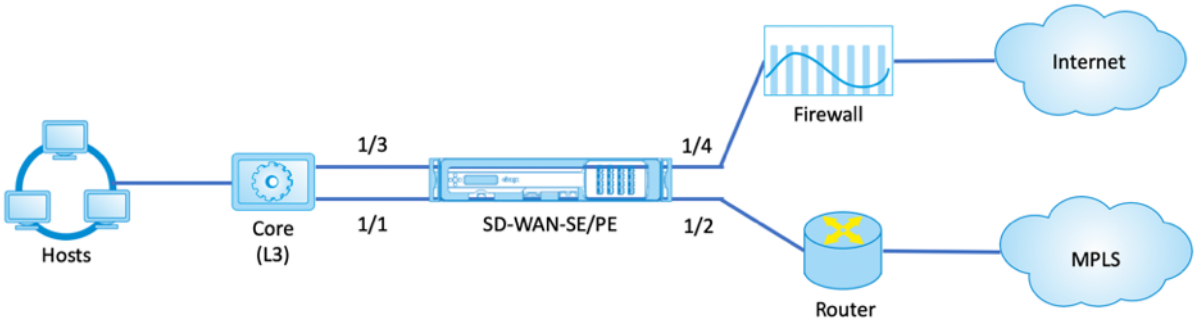
完成上述所有步骤后，继续 准备 SD-WAN 设备软件包。—>

内联模式

September 2, 2022

本文详细介绍了使用 内联部署 模式配置分支的详细信息。在此模式下，SD-WAN 设备似乎是以太网桥接。大多数 SD-WAN 设备型号都包括用于串联模式的 故障到线（以太网旁路）功能。如果电源发生故障，继电器会关闭，输入和输出端口通过电连接，从而允许以太网信号从一个端口传递到另一个端口。在故障到线模式下，SD-WAN 设备看起来像连接两个端口的交叉电缆。

在下图中，1/1 和 1/2 接口是硬件旁路对，将核心连接到边缘 MPLS 路由器的故障到线。1/3 和 1/4 接口也是硬件旁路对，并且会将核心连接到边缘防火墙的故障到线。有关基于 SD-WAN Orchestrator 服务的内联模式部署的更多信息，请参阅 接口。



虚拟内联模式

September 2, 2022

在虚拟内联模式下，路由器使用路由协议（如 PBR、OSPF 或 BGP）将传入和传出 WAN 流量重定向到设备，设备将处理的数据包转发回路由器。

以下文章介绍了配置两个 SD-WAN (SD-WAN SE) 设备的分步过程：

- 虚拟内联模式下的数据中心设备
- 在内联模式下分支设备
- 路由协议必须在核心交换机或路由器的上游配置。路由器必须监视 SD-WAN 设备的运行状况，以便在设备出现故障时可以绕过设备。
- 虚拟内联模式将 SD-WAN 设备置于物理路径之外（单臂部署），也就是说，在旁路模式设置为故障阻止 (FTB) 的情况下，仅使用单个以太网接口（例如：接口 1/5）。
  必须将 Citrix SD-WAN 设备配置为将流量传递到正确的 Gateway。用于虚拟路径的流量被定向到 SD-WAN 设备，然后封装并定向到相应的 WAN 链接。

收集信息

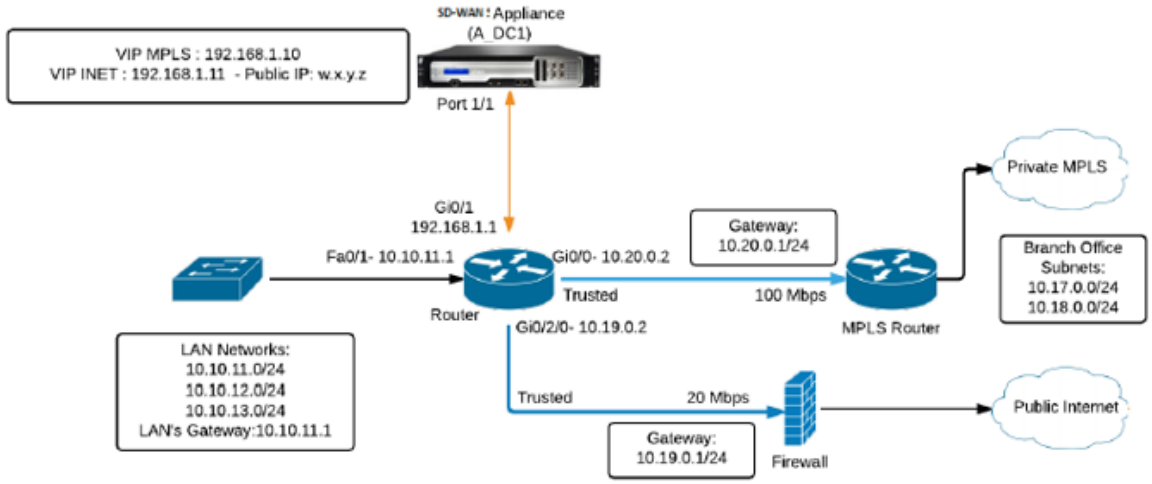
收集配置虚拟内联模式所需的以下信息：

- 本地和远程站点的准确网络图，包括：
  - 本地和远程 WAN 链接及其双向带宽、子网、每条链路、路由和 VLAN 中的虚拟 IP 地址和网关。
- 部署表

有关基于 SD-WAN Orchestrator 服务的虚拟内联模式部署的信息，请参阅 接口。

以下是示例网络逻辑示意图和部署表：

数据中心拓扑-虚拟内联模式



解决审计错误

完成数据中心和分支站点的配置后，系统将提醒您解决 DC 和 BR 站点上的审计错误。解决审计错误（如果有）。

构建 **SD-WAN** 网络

September 2, 2022

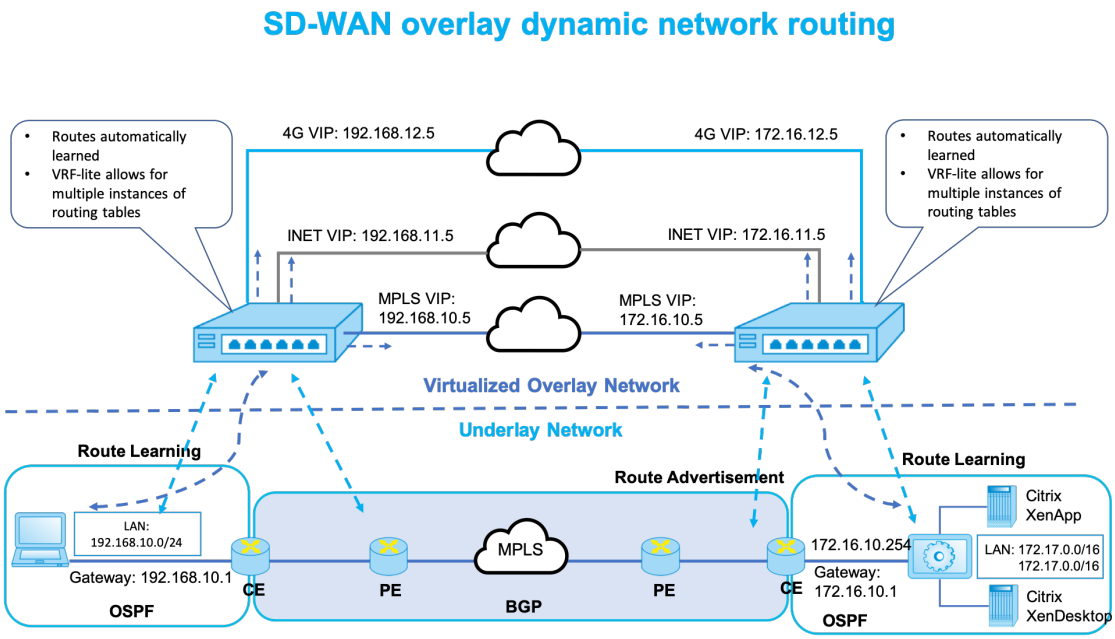
要在无需构建 SD-WAN 叠加路由表的情况下构建 SD-WAN 叠加网络，请执行以下操作：

1. 在两个 SD-WAN 设备之间跨每个 WAN 链接创建 WAN 路径通道。
2. 配置虚拟 IP 以表示每个 WAN 链接的终端节点。您可以通过当前 L3 网络建立加密的 WAN 路径。
3. 将 2、3 和 4 个 WAN 路径（物理链路）聚合到单个虚拟路径中，允许数据包利用 SD-WAN 叠加网络，而不是现有底层网络遍历 WAN，后者最不智能且成本最低。

SD-WAN 路由组件和网络拓扑

- 本地—子网驻留在此站点（通告到 SD-WAN 环境）
- 虚拟路径—通过虚拟路径发送到所选站点设备
- 内联网—没有 SD-WAN 设备的站点

- Internet -Internet 流量
- 直通—未触及的交通，在一个桥接接口出另一个
- 定义的默认路由 (0.0.0.0/0) - 用于未被 SD-WAN 叠加路由表捕获的直通流量，或在 MCN 上使用的直通流量指示客户端站点将所有流量转发回到 MCN 节点，以便进行 Internet 流量的回传。



高可用性

September 2, 2022

本主题介绍 SD-WAN 设备（标准版）支持的高可用性（高可用性）部署和配置。

Citrix SD-WAN 设备可以在高可用性配置中作为主动/备用角色中的一对设备进行部署。有三种高可用性部署模式：

- 并行在线高可用性
- 故障到线的高可用性
- 单臂高可用性

这些高可用性部署模式类似于虚拟路由器冗余协议 (VRRP)，并使用专有的 SD-WAN 协议。SD-WAN 网络中的客户端节点（客户端）和主控制节点 (MCN) 都可以在高可用性配置中进行部署。主设备和辅助设备必须是相同的平台型号。

在高可用性配置中，站点上的一个 SD-WAN 设备被指定为活动设备。备用设备监控活动设备。配置在两个设备之间进行镜像。如果备用设备在定义的时间段内失去与活动设备的连接，则备用设备将采用活动设备的标识并接管流量负载。根据部署模式，此快速故障转移对通过网络的应用程序流量的影响最小。

高可用性部署模式

单臂模式：

在单臂模式下，高可用性设备对位于数据路径之外。应用程序流量将重定向到具有基于策略的路由 (PBR) 的设备对。当网络中的单个插入点不可行或应对线失效的挑战时，可实现单臂模式。备用设备可以添加到与活动设备和路由器相同的 VLAN 或子网。

在单臂模式下，建议 SD-WAN 设备不驻留在数据网络子网中。虚拟路径流量不必遍历 PBR 并避免路由循环。SD-WAN 设备和路由器必须通过以太网端口或在同一 VLAN 中直接连接。

- **IP SLA** 监控回退：

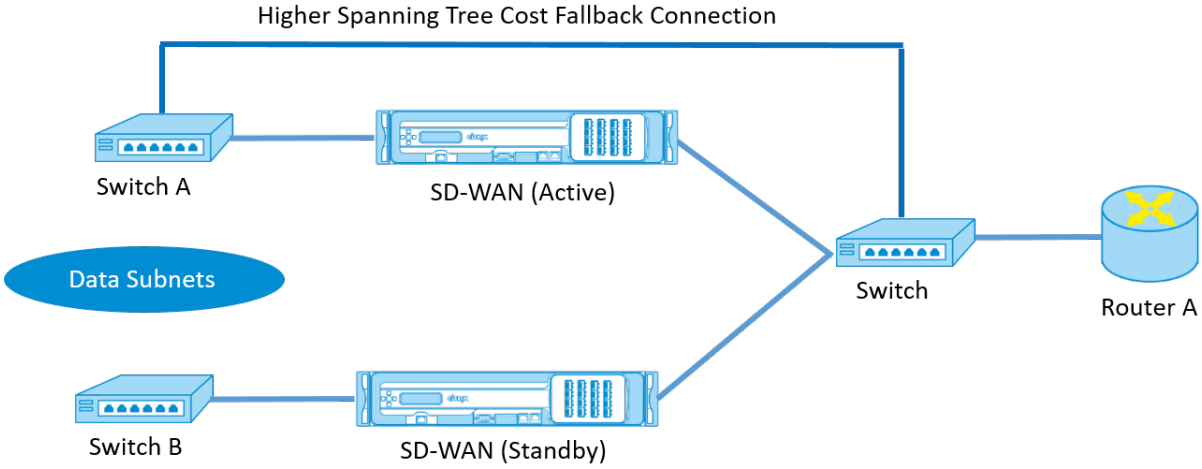
  只要 SD-WAN 设备之一处于活动状态，即使虚拟路径处于关闭状态，活动流量也会流动。SD-WAN 设备将流量重定向回路由器，作为内部网流量。但是，如果两个活动/备用 SD-WAN 设备都变为非活动状态，路由器会尝试将流量重定向到设备。如果下一台设备无法访问，则可以在路由器上配置 IP SLA 监视以禁用 PBR。它允许路由器回退以执行路由查找并适当转发数据包。

并行内联高可用性模式：

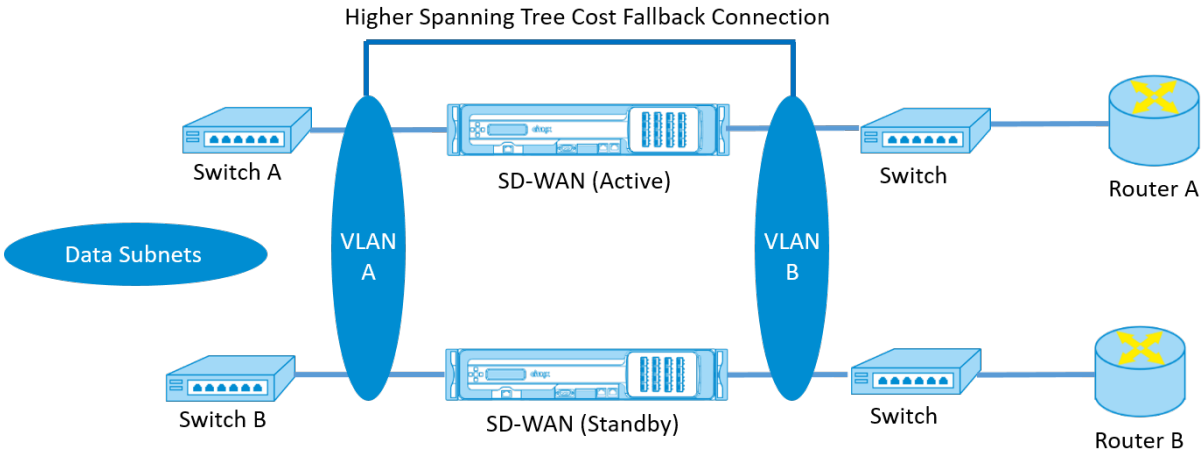
在并行内联高可用性模式下，SD-WAN 设备彼此并行部署，并与数据路径内联。只使用通过活动设备的一个路径。请注意，绕过接口组被配置为故障到块，以避免故障转移过程中的桥接环路。

可通过内联接口组或设备之间的直接连接来监视高可用性状态。外部跟踪可用于监视上游或下游网络基础设施的可达性。例如，如果需要，切换端口故障转换为直接更改高可用性状态。

如果主动和备用 SD-WAN 设备都被禁用或失败，则可以直接在交换机和路由器之间使用第三级路径。此路径的生成树成本必须高于 SD-WAN 路径，以便在正常条件下不使用。并行串联高可用性模式下的故障切换取决于配置的故障切换时间，默认故障切换时间为 1000 毫秒。但是，故障转移会对流量造成 3-5 秒的影响。在生成树重新收敛期间，回退到第三路径会影响流量。如果存在到其他 WAN 链接的路径外连接，则必须将两个设备连接到它们。



在更复杂的情况下，如果多个路由器可能正在使用 VRRP，建议使用非路由 VLAN，以确保在第 2 层可以访问 LAN 侧交换机和路由器。



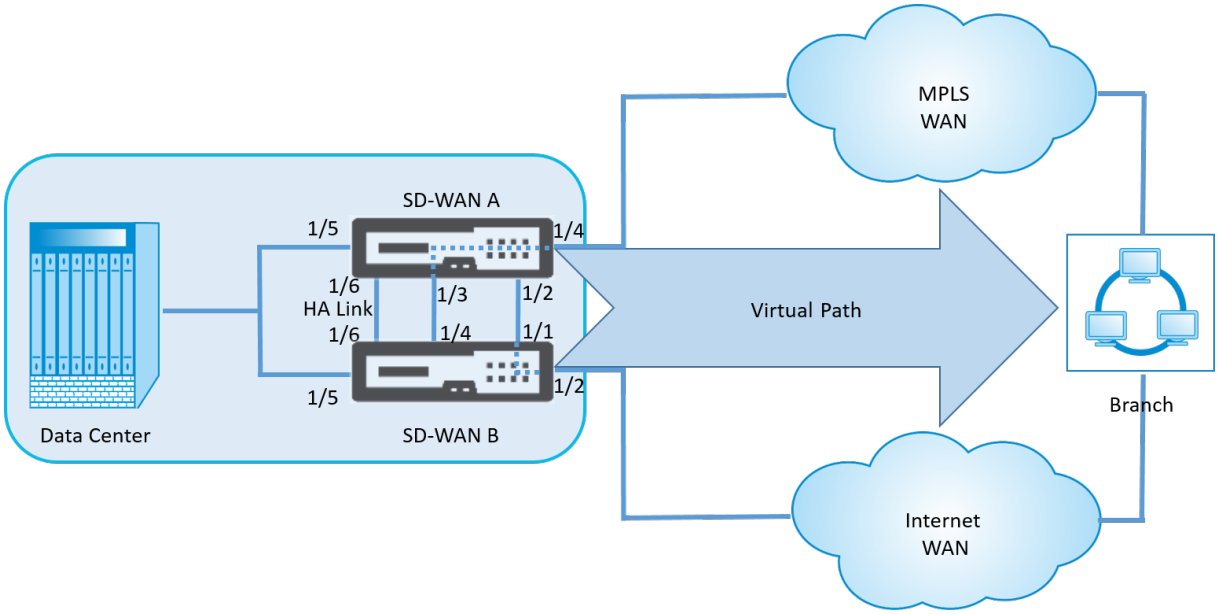
故障到线模式：

在故障到线模式下，SD-WAN 设备在相同的数据路径中内联。旁路接口组必须处于故障到线模式，备用设备处于直通或旁路状态。必须为高可用性接口组配置并使用单独端口上的两个设备之间的直接连接。

> 注意
>
> - 故障到线模式下的高可用性切换大约需要 10 到 12 秒钟，因为端口从故障到线模式恢复出现延迟。
> - 如果设备之间的高可用性连接失败，则两台设备都进入活动状态并导致服务中断。要减少服务中断，请分配多个高可用性连接，以便没有单点故障。
> - 在高可用性故障到线模式下，硬件设备对中必须使用单独的端口，以实现高可用性控制交换机制，从而帮助实现状态收敛。

由于 SD-WAN 设备从活动切换到待机时物理状态发生变化，故障转移可能导致部分连接丢失，具体取决于自动协商在以太网端口上所需的时间。

下图显示了故障到线部署的示例。



对于转发大量流量的数据中心或站点，建议使用 One-Arm 高可用性配置或并行内联高可用性配置，以最大限度地减少故障转移期间的干扰。

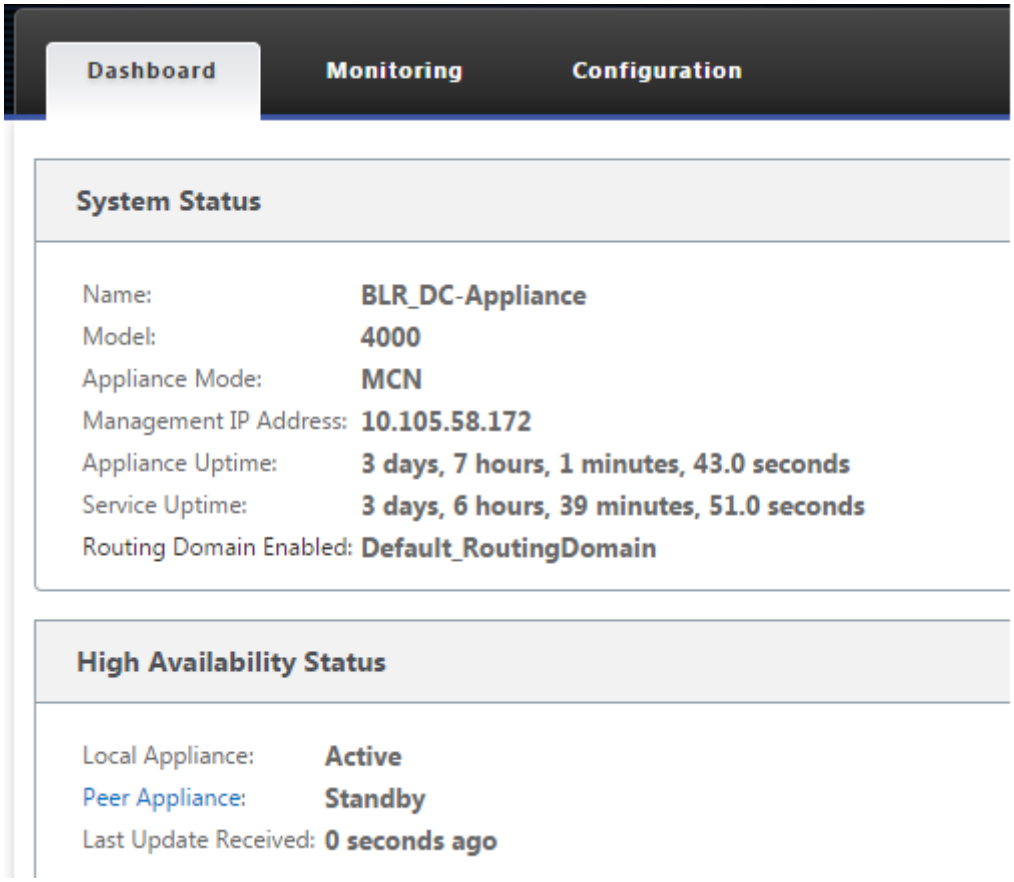
如果在故障转移期间可以接受最小的服务损失，则故障到线高可用性模式是更好的解决方案。故障到线高可用性模式可防止设备故障，并行内联高可用性可防止所有故障。在所有情况下，高可用性对于在系统故障期间保持 SD-WAN 网络的连续性都很有价值。

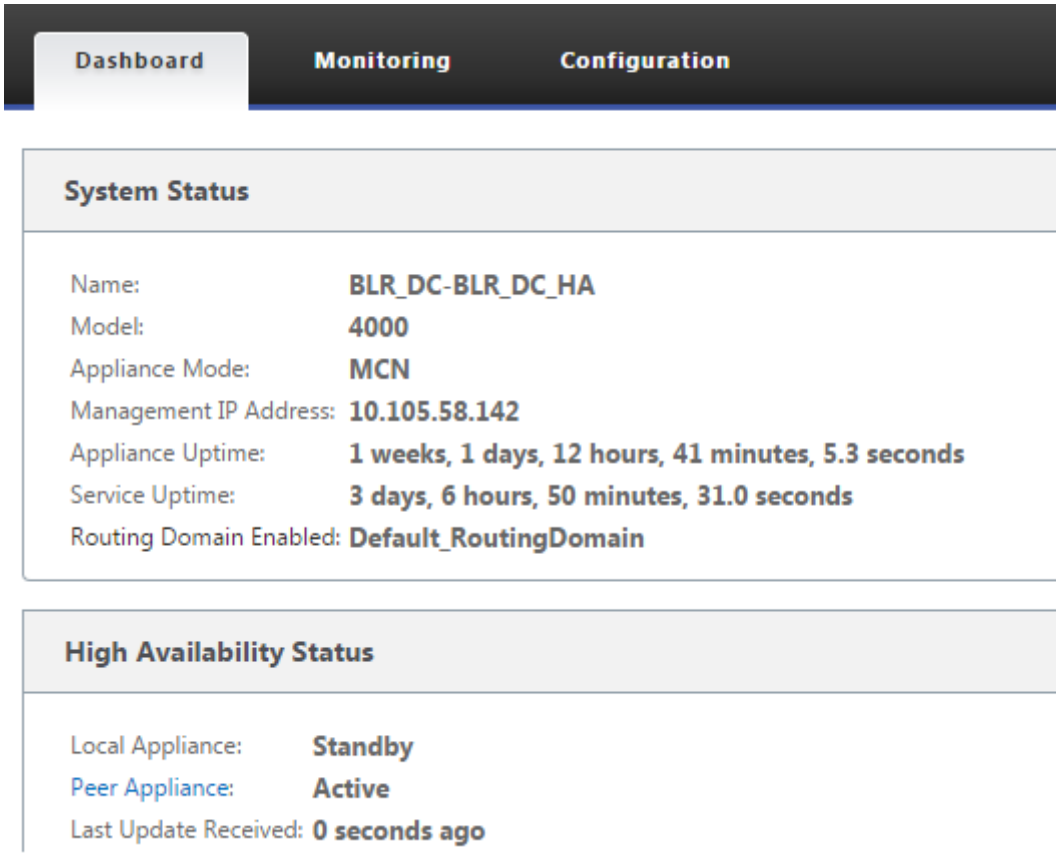
有关基于 SD-WAN Orchestrator 服务的高可用性部署的更多信息，请参阅 设备详细信息。

监视

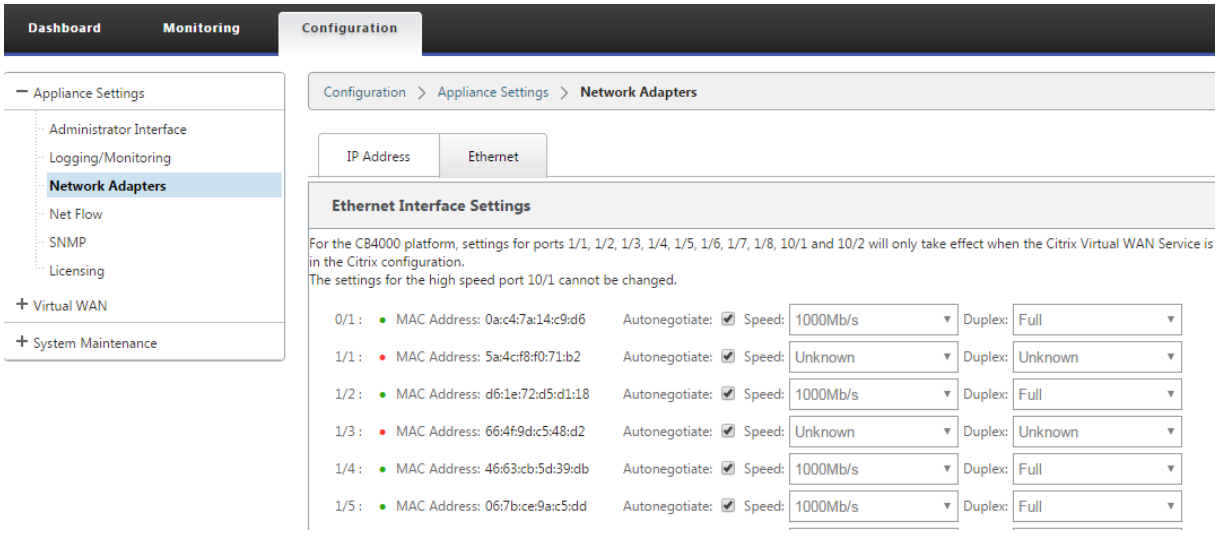
要监视高可用性配置，请执行以下操作：

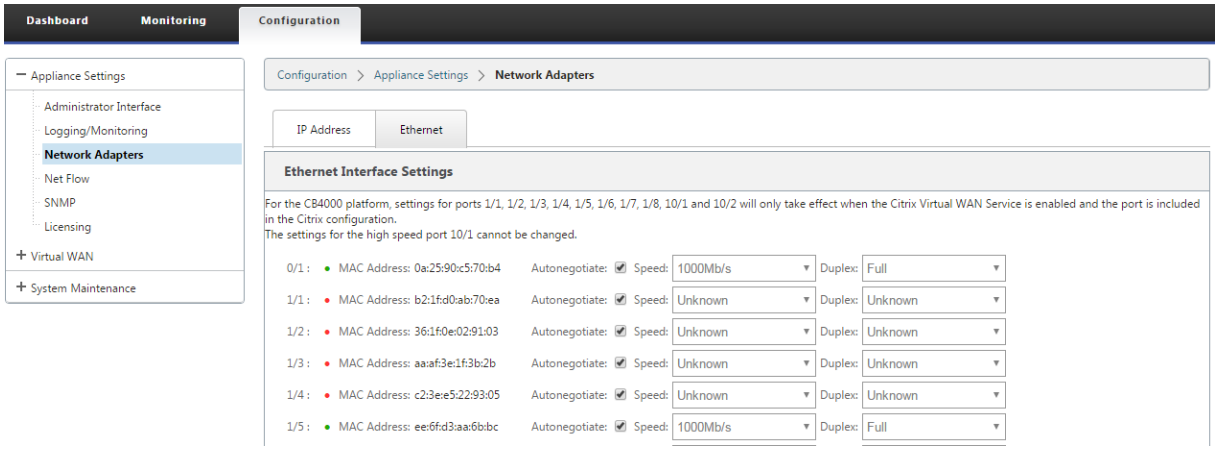
登录到已实现高可用性的活动和备用设备的 SD-WAN Web 管理界面。在 控制板 选项卡下查看高可用性状态。





有关活动和备用高可用性设备的网络适配器详细信息，请导航到 配置 > 设备设置 > 网络适配器 > 以太 网选项卡。





故障排除

在高可用性 (HA) 模式下配置 SD-WAN 设备时，请执行以下故障排除步骤：

1. 大脑分裂问题的主要原因是 HA 设备之间的通信问题。
    - 检查 SD-WAN 设备之间的连接是否存在问题（例如，两个 SD-WAN 设备上的端口都是启动还是关闭）。
    - 必须禁用其中一个 SD-WAN 设备上的 SD-WAN 服务，以确保只有一个 SD-WAN 设备处于活动状态。
2. 您可以验证登录到 **SDWAN_common.log** 文件中的与 HA 相关的日志。

    > 注意
    > 所有与 HA 相关的日志都使用关键词 **racp** 进行记录。

3. 您可以验证 **SDWAN_common.log** 文件中的端口相关事件（例如，启用 HA 的端口关闭或启用）。
4. 对于每次 HA 状态更改，都会记录一个 SD-WAN 事件。因此，如果日志被滚动，您可以验证事件日志以获取事件详细信息。

使用光纤 Y 电缆实现边缘模式高可用性

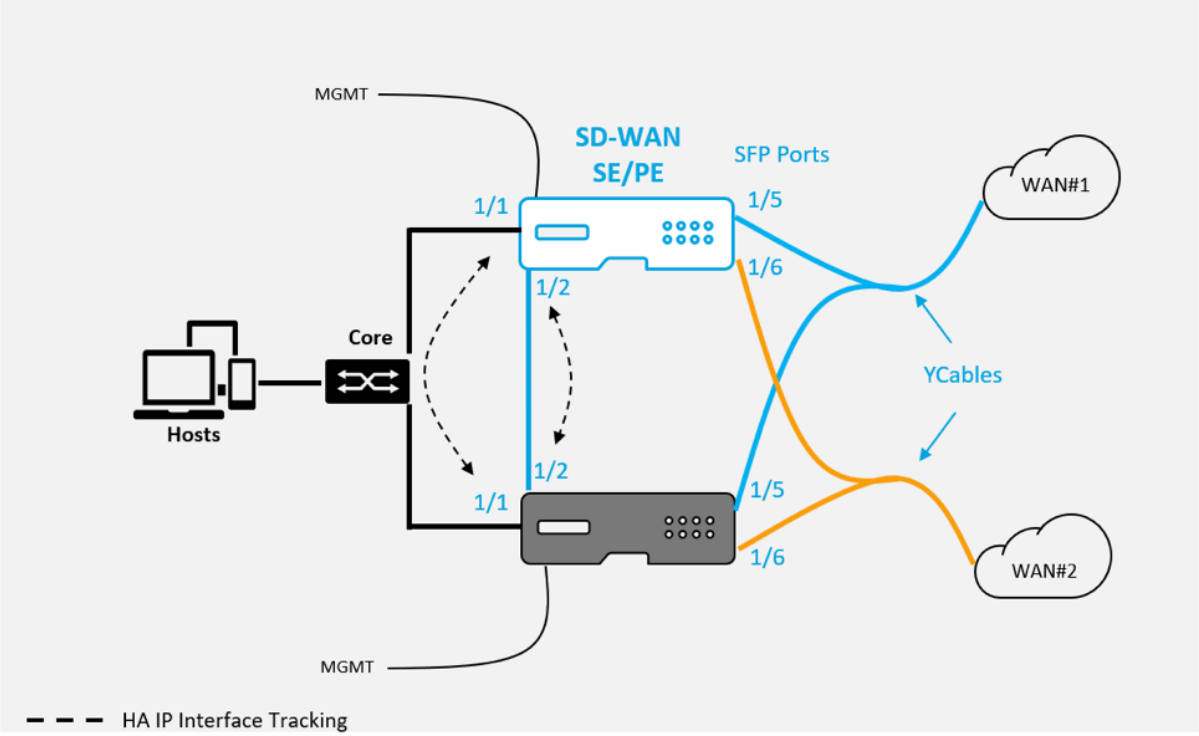
September 2, 2022

> 注意：在版本 10.2 第 2 版中，此功能仅适用于 1100 SE 设备。

以下过程描述了在边缘模式下部署的 1100 SE 设备上启用高可用性 (HA) 的步骤，其中 WAN 链路服务提供商的移交是光纤的。
1100 设备上的可用小型可插拔 (SFP) 端口可与光纤 Y 电缆一起使用，以实现边缘模式部署的高可用性功能。
在 1100 SE 设备上，分路器电缆分割端连接到配置为 HA 对的两台 1100 设备的光纤端口。

光纤 Y 型电缆有三端。一端连接到提供商的光纤切换，另一端连接到部署在高可用性对中的两台 1100 SE 设备上为该 WAN 链路配置的 SFP 端口。分离器电缆用于将一个传入信号分成多个信号。

有关基于 SD-WAN Orchestrator 服务的边缘模式高可用性部署的信息，请参阅 设备详细信息。



局限性：

- 不支持使用 Y 型电缆进行 HA 故障到线模式配置。
- 连接到 Y 型电缆的 SFP 不能用作 HA IP 接口跟踪。
- 软件版本 10.2.2 或更高版本，以及 11.0 或更高版本才能支持此部署。

零接触

September 2, 2022

> 注意
>
> 仅在选择 Citrix SD-WAN 设备时支持零接触部署服务：
>
> - SD-WAN 110 标准版
> - SD-WAN 210 Standard Edition
> - SD-WAN 1100 标准版
> - SD-WAN 2100 Standard Edition

- SD-WAN AWS VPX 实例

零接触部署云服务是 Citrix 运营和托管的基于云的服务，允许在 Citrix SD-WAN 网络中发现新设备，主要侧重于简化 Citrix SD-WAN 在分支机构或云服务办公室位置的部署过程。零接触部署云服务可通过公共 Internet 访问从网络中的任何点公开访问。零接触部署云服务可通过安全套接字层 (SSL) 协议进行访问。

零接触部署云服务安全地与后端 Citrix 服务进行通信，这些服务托管已购买支持零接触的设备（例如 2100-SE）的 Citrix 客户的存储标识。后端服务已到位，可以对任何零接触部署请求进行身份验证，从而正确验证客户帐户与 Citrix SD-WAN 设备序列号之间的关联。

有关更多信息，请参阅 Citrix SD-WAN Orchestrator 服务 零接触部署 主题。

ZTD 高级架构和工作流程：

数据中心站点：

Citrix SD-WAN 管理员—具有 SD-WAN 环境管理权限的用户，主要责任如下：

- Citrix Cloud 登录为新站点节点部署启动零接触部署服务。

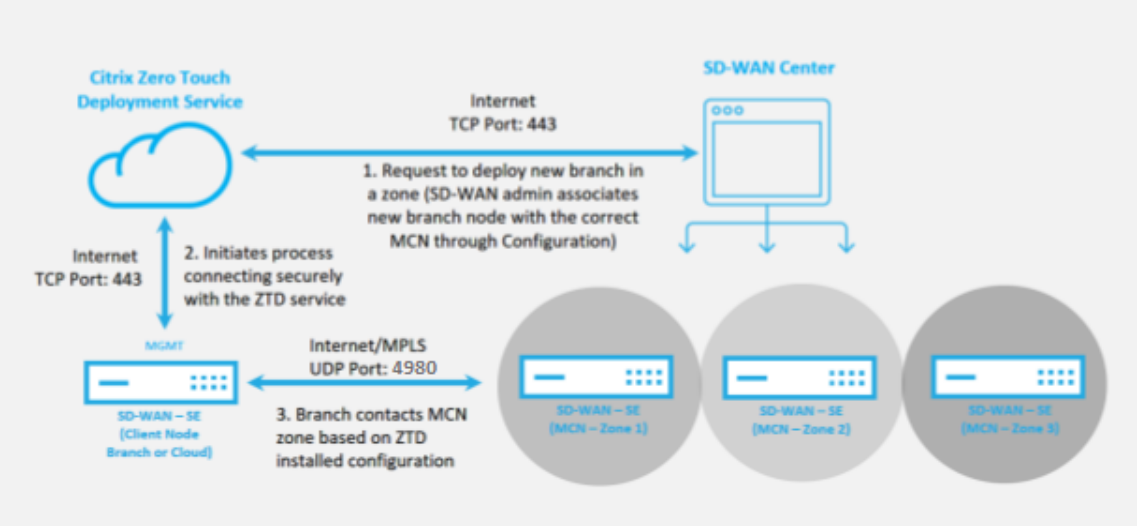
网络管理员—负责企业网络管理（DHCP、DNS、Internet 、防火墙等）的用户。

远程站点：

现场安装 人员—现场活动的本地联系人或雇用的安装人员，主要职责如下：

- 物理解压 Citrix SD-WAN 设备的包装。
- 重新映像非 ZTD 就绪设备。
  - 所需的：SD-WAN 1000-SE、2000-SE、1000-EE、2000-EE
  - 不需要：SD-WAN 410-SE、2100-SE
- 电源线的设备。
- 在管理界面（例如 MGMT 或 0/1）上连接设备以便连接 Internet 。
- 在数据接口（例如 AP.WAN、APB.WAN、APC.WAN、APC.WAN、0/2、0/3、0/5 等）上连接设备的电缆连接。

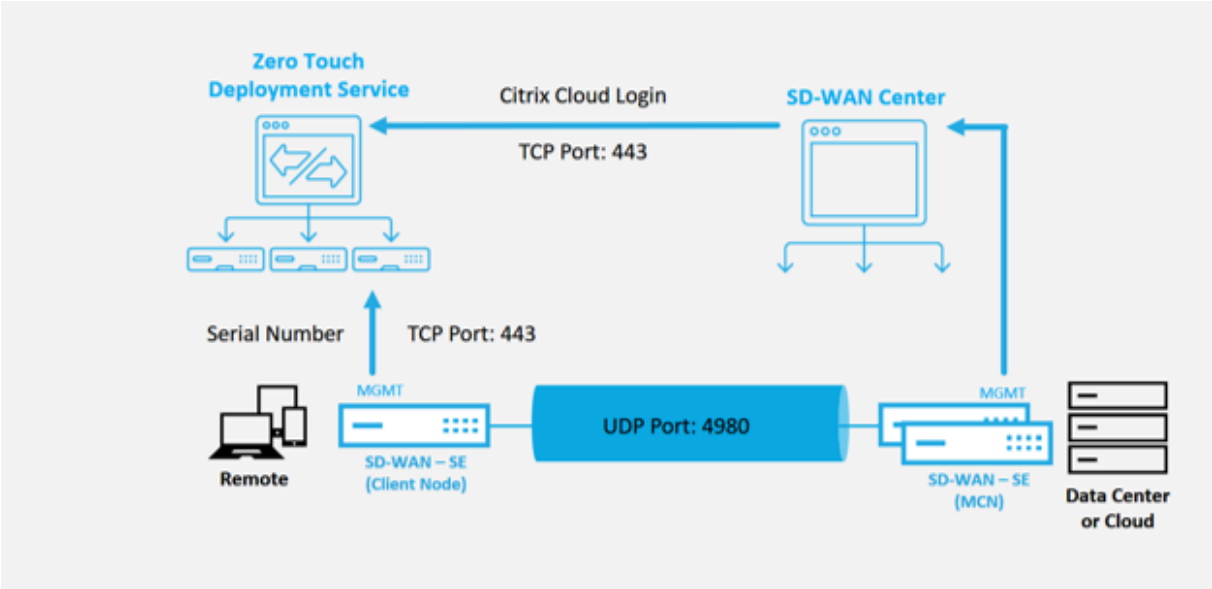
> 注意
>
> 每种型号的接口布局都有所不同，因此请参考有关识别数据和管理端口的文档。



需要满足以下必备条件，才能启动任何零接触部署服务：

- 主动运行 SD-WAN 提升到主控制节点 (MCN)。
- 在 https://onboarding.cloud.com 上创建的 Citrix Cloud Login 凭据（请参阅以下有关创建帐户的说明）。
- 通过端口 443 直接或通过代理服务器管理到 Internet 的网络连接（SD-WAN 设备）。
- （可选）至少有一个在客户端模式下在分支机构运行的主动运行的 SD-WAN 设备，并具有与 MCN 的有效虚拟路径连接，以帮助验证在现有底层网络中成功建立路径。

最后一个先决条件不是必需的，但允许 SD-WAN 管理员验证底层网络是否允许在任何新添加的站点完成零接触部署时建立虚拟路径。首先，这可以验证是否已针对 NAT 流量实施了适当的防火墙和路由策略，或者确认 UDP 端口 4980 能够成功穿透网络以到达 MCN。



零接触部署服务概述：

要使用零接触部署服务（或零接触部署云服务），管理员必须首先部署环境中的第一个 SD-WAN 设备。

正在运行的 SD-WAN 环境启动并向零接触部署服务中运行注册后，将通过创建 Citrix Cloud 帐户登录来完成。登录零接触服务可对与特定 SD-WAN 环境关联的客户 ID 进行身份验证。

当 SD-WAN 管理员使用零接触部署流程启动站点进行部署时，您可以选择通过预填充序列号并发起与现场安装人员的电子邮件通信以在现场开始预先验证用于零接触部署的设备活动。

现场安装程序会接收电子邮件通信，表明该站点已准备就绪，可以进行零接触部署，并且可以开始执行安装过程，以便在 MGMT 端口上启动并连接设备，以实现 DHCP IP 地址分配以及访问 Internet。此外，在任何 LAN 和 WAN 端口中连接布线。其他所有内容均由零接触部署服务启动，并使用激活 URL 监控进度。如果要安装的远程节点是云实例，打开激活 URL 时，将开始执行工作流以自动在指定的云环境中安装实例，本地安装程序不需要执行任何操作。

零接触部署云服务可自动执行以下操作：

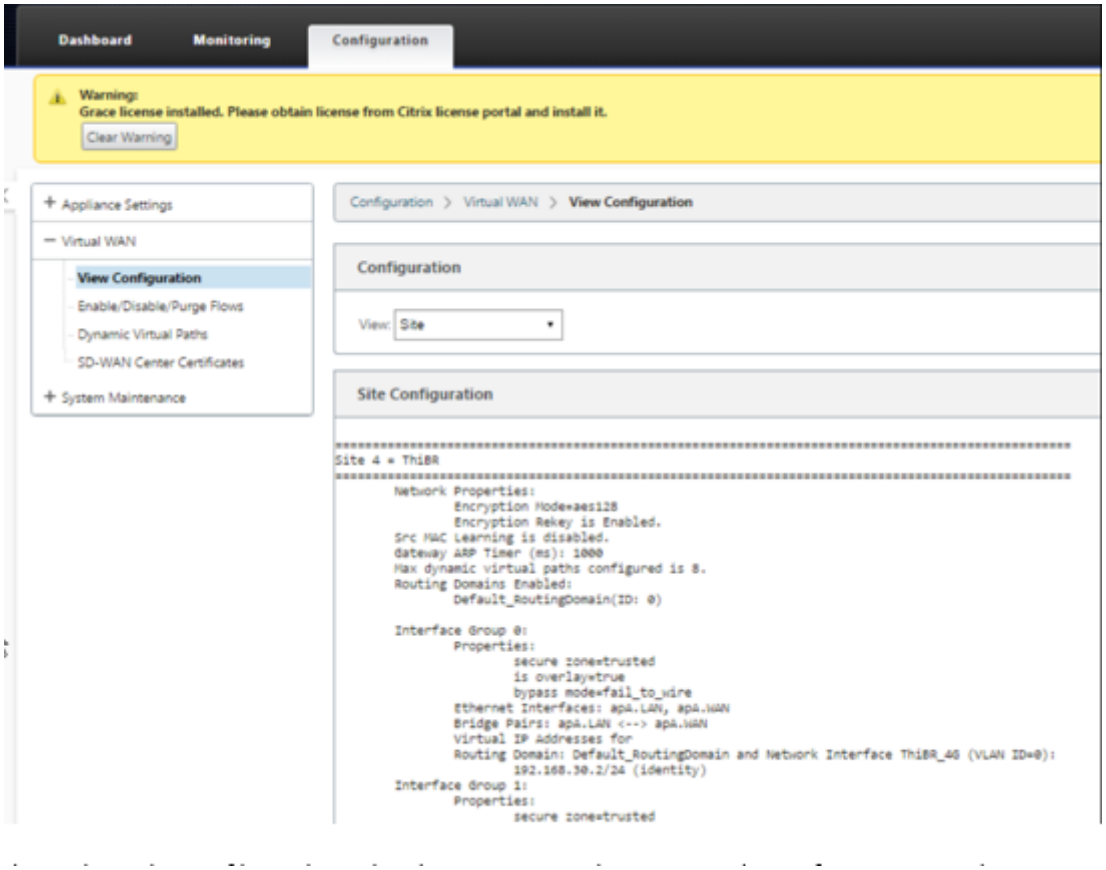
如果分支设备上有新功能，请下载并更新零接触部署代理。

- 通过验证序列号对分支设备进行身份验证。
- 将特定于目标设备的配置文件推送到分支设备。
- 在分支设备上安装配置文件。
- 将任何丢失的 SD-WAN 软件组件或所需更新推送到分支设备。
- 推送一个临时 10 Mbps 许可证文件，以确认与分支设备建立的虚拟路径。
- 在分支设备上启用 SD-WAN 服务。

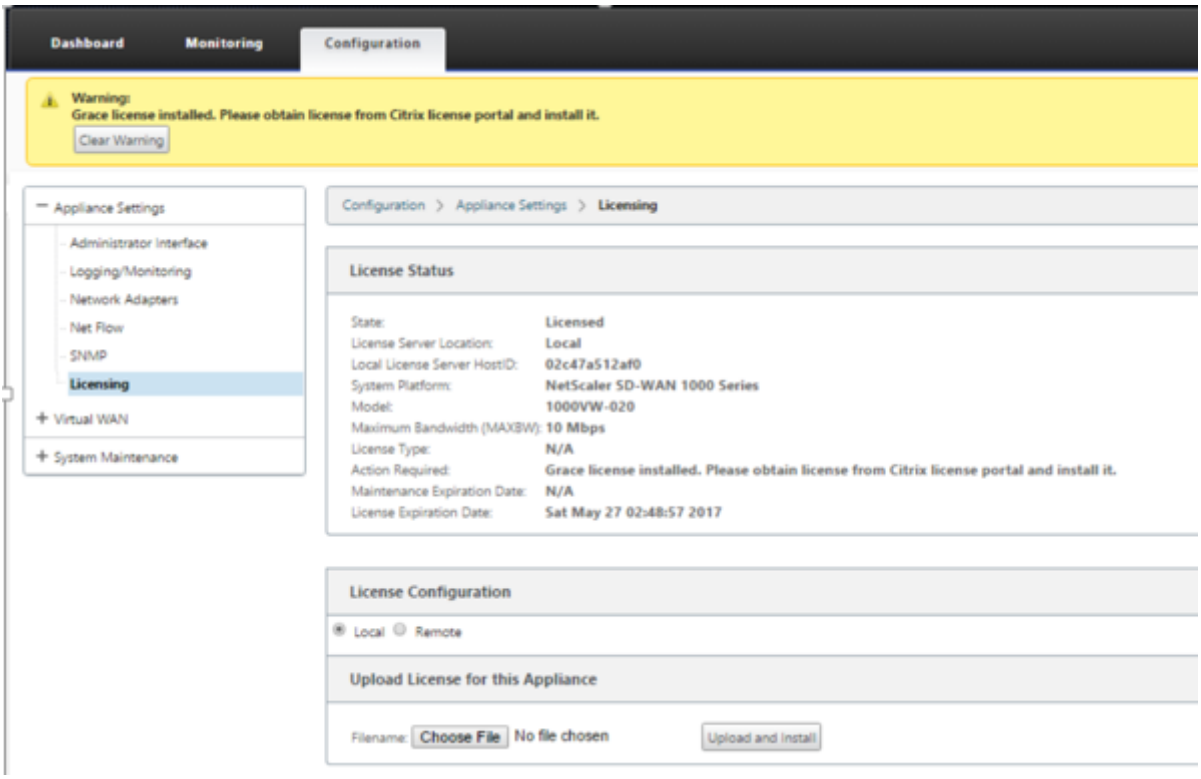
要在设备上安装永久性许可证文件，SD-WAN 管理员需要执行更多步骤。

> 注意：
>
> 在执行已具有与 MCN 中使用的设备软件相同版本的分支配置时，零接触部署过程将不会再次下载设备软件文件。此更改适用于出厂发货的新设备、设备重置为出厂默认值以及以管理方式重置配置。如果重置了配置，请选中 还原后重新启 动复选框以启动零接触部署过程。

可以使用配置 > 虚拟 **WAN**> 查看配置页面对设备配置进行验证。



可以使用配置 > 设备设置 > 许可页面将设备许可证文件更新为永久许可证。



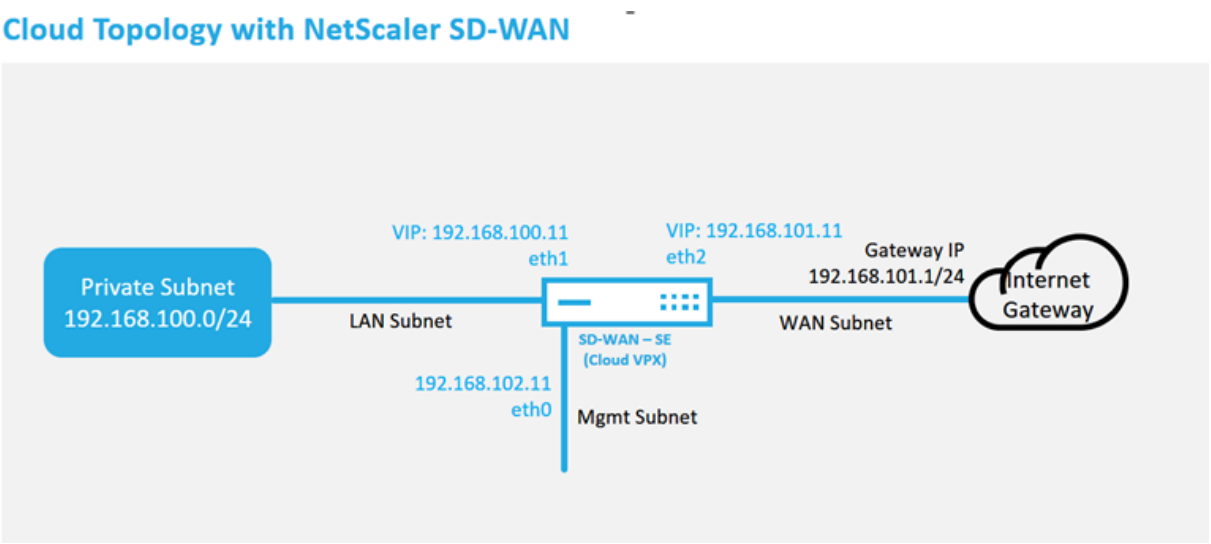
上传并安装永久许可证文件后，Grace 许可证警告横幅将消失，并且在许可证安装过程中，与远程站点的连接不会中断（不会丢弃零 ping）。

AWS

September 2, 2022

在 SD-WAN 版本 11.5 中，通过 SD-WAN Orchestrator 服务支持在 AWS 环境中进行零接触部署。

> 注意
>
> - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
> - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
> - SD-WAN VPX 的可用云模板目前很难获取 VPC 中可用子网的 #.#.#.#.11 IP 地址。



这是 SD-WAN 云部署站点的示例部署，Citrix SD-WAN 设备部署为此云网络中的单个 Internet WAN 链接提供服务的边缘设备。远程站点将能够利用连接到同一 Internet 网关的多个不同 Internet WAN 链路，从而提供从任何 SD-WAN 部署站点到云基础设施的弹性和聚合带宽连接。这样就可以提供经济高效且高度可靠的云连接。

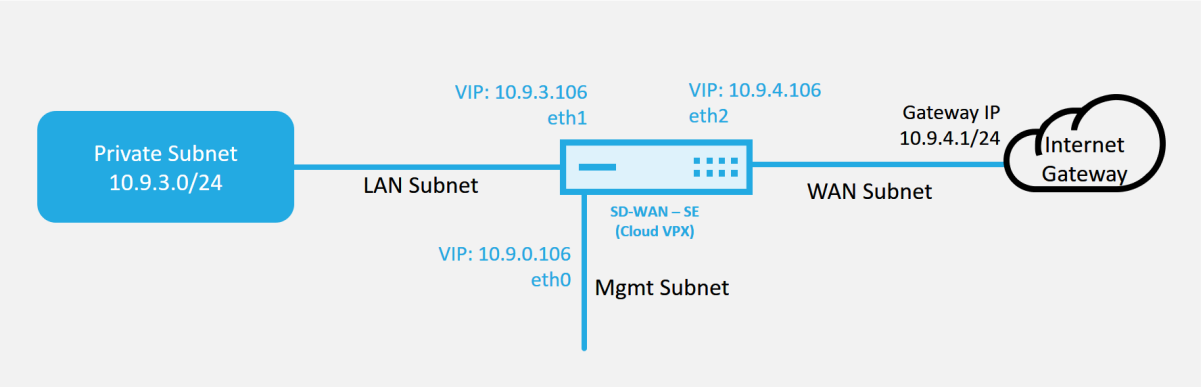
Azure

September 2, 2022

在 SD-WAN 版本 11.5 中，通过 SD-WAN Orchestrator 服务支持在 Azure 环境中进行零接触部署。

> 注意
>
> - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
> - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
> - 适用于 SD-WAN VPX 的 Azure 云模板当前被硬设置为获取 WAN 的 10.9.4.106 IP、适用于 LAN 的 10.9.3.106 IP 以及管理地址的 10.9.0.16 IP。针对零接触的 Azure 节点的 SD-WAN 配置必须与此布局匹配。
> - 配置中的 Azure 站点名称必须全小写且无特殊字符（例如 ztdazure）。

Azure Cloud Topology with NetScaler SD-WAN



这是 SD-WAN 云部署站点的示例部署，Citrix SD-WAN 设备作为边缘设备部署，为该云网络中的单个 Internet WAN 链接提供服务。远程站点将能够利用连接到同一 Internet 网关的多个不同 Internet WAN 链路，从而提供从任何 SD-WAN 部署站点到云基础设施的弹性和聚合带宽连接。这样就可以提供经济高效且高度可靠的云连接。

单区域部署

September 2, 2022

区域允许您定义具有分布式管理的网络层次结构。区域必须定义一个区域控制节点 (RCN)，该节点将接管网络控制节点 (MCN) 为其区域执行的功能。MCN 是默认区域的 Controller。片段之间不允许使用静态和动态虚拟路径。RCNS 管理区域之间的流量。SD-WAN 网络中的单区域部署可以支持小于 550 的网络站点。

有关通过 Citrix SD-WAN Orchestrator 服务进行单区域部署的更多信息，请参阅 区域。

多区域部署

September 2, 2022

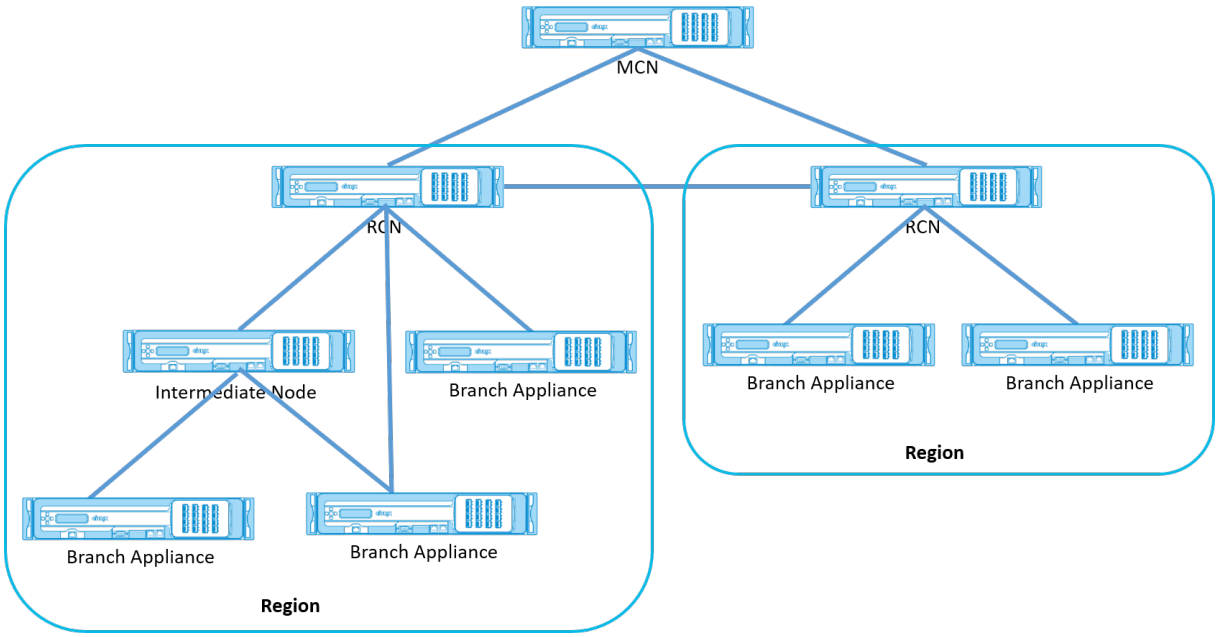
配置为主控节点 (MCN) 的 SD-WAN 设备支持多区域部署。MCN 管理多个区域控制节点 (RCN)。反过来，每个 RCN 管理多个客户端站点。MCN 还可用于直接管理某些客户端站点。

将 MCN 作为网络的控制节点，RCN 作为区域的控制节点，SD-WAN 可以管理多达 6000 个站点。

多区域部署使您能够将网络分割成区域并设置分层网络；例如分支机构（客户端）> RCN > MCN。

具有单个区域的 MCN 最多可配置 1000 个站点。您可以将现有站点保留在默认区域中，并添加具有 RCN 的新区域及其站点以进行多区域部署。

有关通过 Citrix SD-WAN Orchestrator 服务进行多区域部署的更多信息，请参阅 区域。



下表提供了配置主 MCN/RCN 所支持的平台列表。

> 注意
>
> 仅在 SD-WAN 编排器托管的网络中将 Citrix SD-WAN 210 SE 设备用作 MCN。

平台版本	小学/中学 MCN	小学/中学 RCN
110-SE	否	否
210-SE	是	是
1100-SE	是	是
VPX-SE、VPXL-SE	是	是
2100-SE、4100-SE、5100-SE、6100-SE	是	是

Citrix Virtual Apps and Desktops 工作负载配置指南

September 2, 2022

Citrix SD-WAN 是新一代 WAN Edge 解决方案，通过针对 SaaS、云和虚拟应用程序的灵活、自动化、安全的连接和性能加快数字化转型，从而确保始终在线的 Workspace 体验。

Citrix SD-WAN 是使用 Citrix Virtual Apps and Desktops 服务连接到云中 Citrix Virtual Apps and Desktops 工作负载的组织的推荐也是最佳方式。有关更多信息，请参阅 Citrix 博客。

本文档重点介绍如何配置 Citrix SD-WAN 以便连接到 Azure 上的 Citrix Virtual Apps and Desktops 工作负载。

优势

- 通过引导式工作流在 Citrix Virtual Apps and Desktops 中轻松设置 SD-WAN
- 通过先进的 SD-WAN 技术实现始终在线、高性能连接
- 跨所有连接（VDA 到 DC、用户到 VDA、VDA 到云、用户到云）的优势
- 与向数据中心回传流量相比，降低了延迟
- 流量管理以确保服务质量 (QoS)
  - 跨 HDX/ICA 流量流的 QoS（单端口多流 HDX 自动 QoS）
  - HDX 和其他流量之间的 QoS
  - HDX 用户之间的 QoS 公平性
  - 端到端服务质量
- 链路绑定提供更多带宽，实现更快的性能
- 高可用性，具有无缝链路故障切换和 Azure 上的 SD-WAN 冗余
- 优化的 VoIP 体验（数据包赛用于减少抖动和减少数据包丢失、QoS、本地突破以减少延迟）
- 与 Azure 快速路由相比，可节省大量成本，并且必须更快、更容易部署

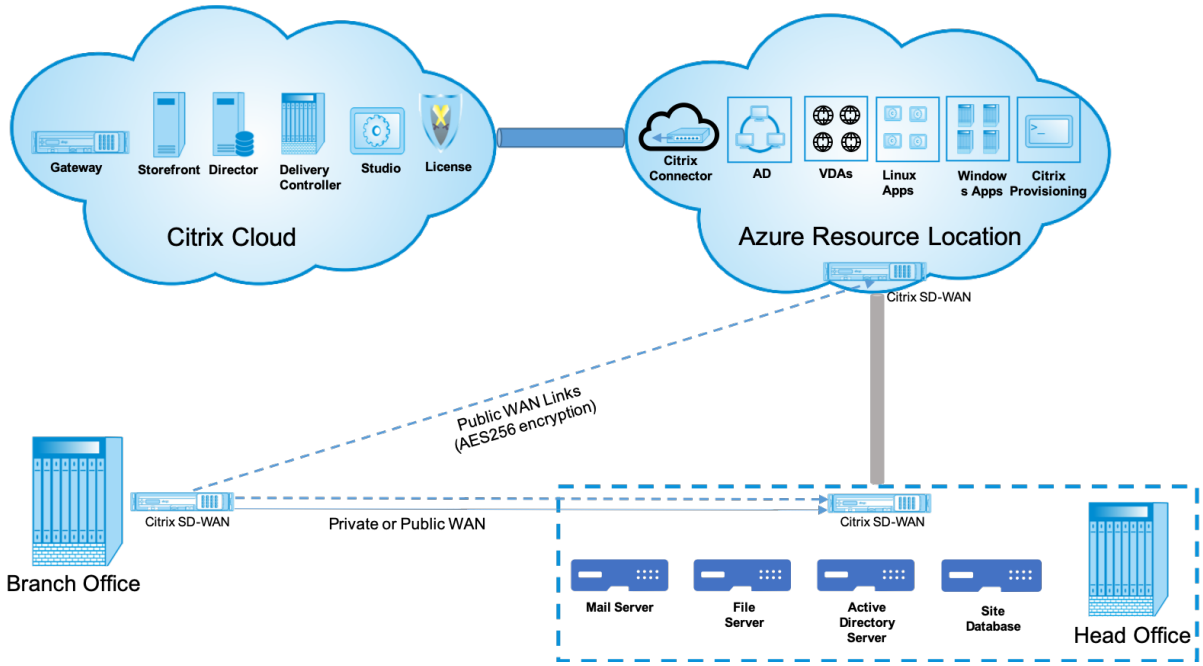
必备条件

遵守以下先决条件来评估和部署 Citrix Virtual Apps and Desktops 工作负载功能：

- 您必须拥有现有 SD-WAN 网络或构建新网络。
- 您必须订阅 Citrix Virtual Apps and Desktops 服务。
- 要使用 SD-WAN 功能（如多流 HDX AutoQoS 和深度可见性），必须为网络中的所有 SD-WAN 站点配置网络定位服务 (NLS)。
- 您必须在客户端终端节点所在的位置部署 DNS 服务器和 AD（通常位于数据中心环境中），或者可以使用 Azure Active Directory (AAD)。
- DNS 服务器必须能够解析内部（私有）和外部（公共）IP。

- 确保将 FQDN (sdwan-位.citrixnetworkapi.net) 添加到防火墙中允许的列表中。这是网络定位服务的 FQDN，对于通过 SD-WAN 虚拟路径发送流量至关重要。此外，如果您对将通配符列入白名单感到满意，更好的方法是将 *.citrixnetworkapi.net 添加到允许的列表中，因为这是其他 Citrix Cloud 服务（如零接触配置）的子域。
- 在 sdwan.cloud.com 注册，以使用 SD-WAN 编排器管理您的 SD-WAN 网络。SD-WAN Orchestrator 是一个基于 Citrix Cloud 的多租户管理平台，用于 Citrix SD-WAN。

部署体系结构



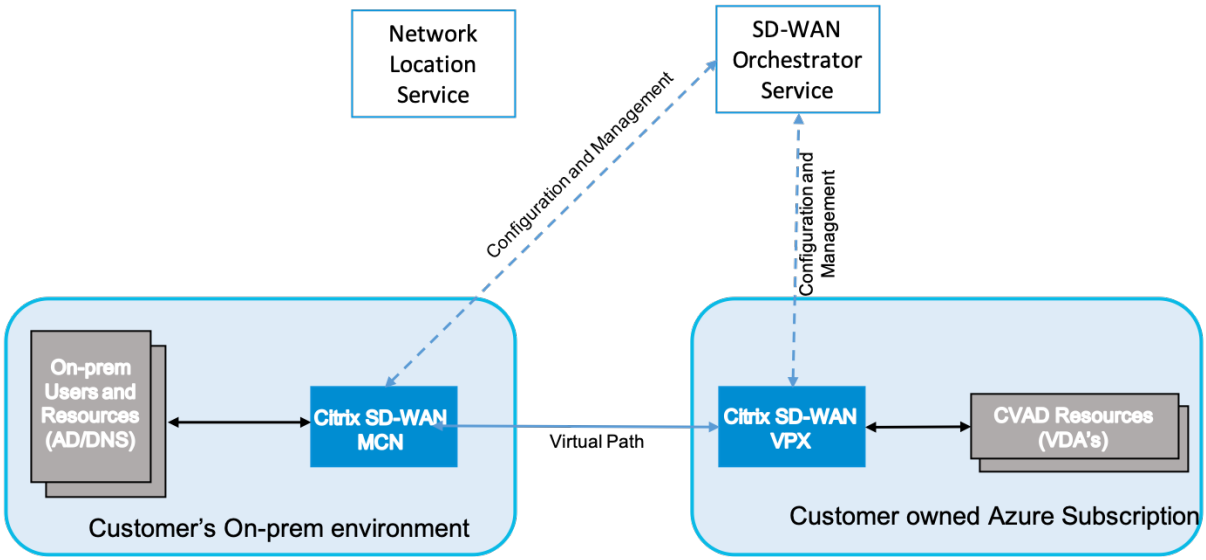
部署需要以下实体：

- 托管 SD-WAN 设备的本地位置，可以在分支模式下部署或作为 MCN （主控制节点）进行部署。分支模式或 MCN 包含客户端计算机、活动目录和 DNS。但是，您也可以选择使用 Azure 的 DNS 和 AD。在大多数情况下，本地位置充当数据中心并容纳 MCN。
- **Citrix Virtual Apps and Desktops** 云服务—Citrix Virtual Apps and Desktops 提供了虚拟化解决方案，使 IT 部门能够控制虚拟机、应用程序和安全性，同时为任何设备提供最终用户可以独立于设备的操作系统和界面使用应用程序和桌面。

  使用 Citrix Virtual Apps and Desktops 服务，您可以将安全的虚拟应用程序和桌面交付到任何设备，并将大部分产品安装、设置、配置、升级和监控保留给 Citrix。您负责在任何设备上交付最佳用户体验的同时维护对应用程序、策略和用户的完全控制。
- **Citrix** 连接器/云连接器 -您可以通过 Citrix Cloud Connector 将资源连接到服务，该连接器可作为 Citrix Cloud 和资源位置之间的通信渠道。借助 Cloud Connector，不需要诸如 VPN 或 IPsec 通道等任何复杂的网络连接或基础结构配置即可实现云管理。资源位置包含向您的订阅者交付应用程序和桌面的计算机及其他资源。

- **SD-WAN Orchestrator** —Citrix SD-WAN Orchestrator 是一项云托管的多租户管理服务，可供 自己 动手的企业和 Citrix 合作伙伴。Citrix 合作伙伴可以使用 SD-WAN Orchestrator 管理多个客户，通过单个窗格和适当的基于角色的访问控制来管理多个客户。
- 虚拟和物理 **SD-WAN** 设备—这在云 (VM) 和数据中心和分支机构（物理设备或虚拟机）的本地多个实例运行，以便在这些位置之间以及与公共 Internet 之间提供连接。Citrix Virtual Apps and Desktops 中的 SD-WAN 实例是通过 Azure Marketplace 配置这些实例而创建为单个或一组虚拟设备（在高可用性部署的情况下）。其他位置（DC 和分支机构）的 SD-WAN 设备由客户创建。所有这些 SD-WAN 设备都由 SD-WAN 管理员通过 SD-WAN 编排器进行管理（在配置和软件升级方面）。

部署和配置



在常见部署中，客户可以将 Citrix SD-WAN 设备（H/W 或 VPX）作为 MCN 部署在其 DC/大型办公室中。客户 DC 通常会托管内部部署用户和资源，如 AD 和 DNS 服务器。在某些情况下，客户可以使用 Azure Active Directory 服务 (AADS) 和 DNS，这两者都受到 Citrix SD-WAN 和 CMD 集成的支持。

在客户管理的 Azure 订阅中，客户需要部署 Citrix SD-WAN 虚拟设备和 VDA。SD-WAN 设备通过 SD-WAN Orchestrator 理。配置 SD-WAN 设备后，它将连接到现有的 Citrix SD-WAN 网络，并通过 SD-WAN Orchestrator 处理配置、可见性和管理等其他任务。

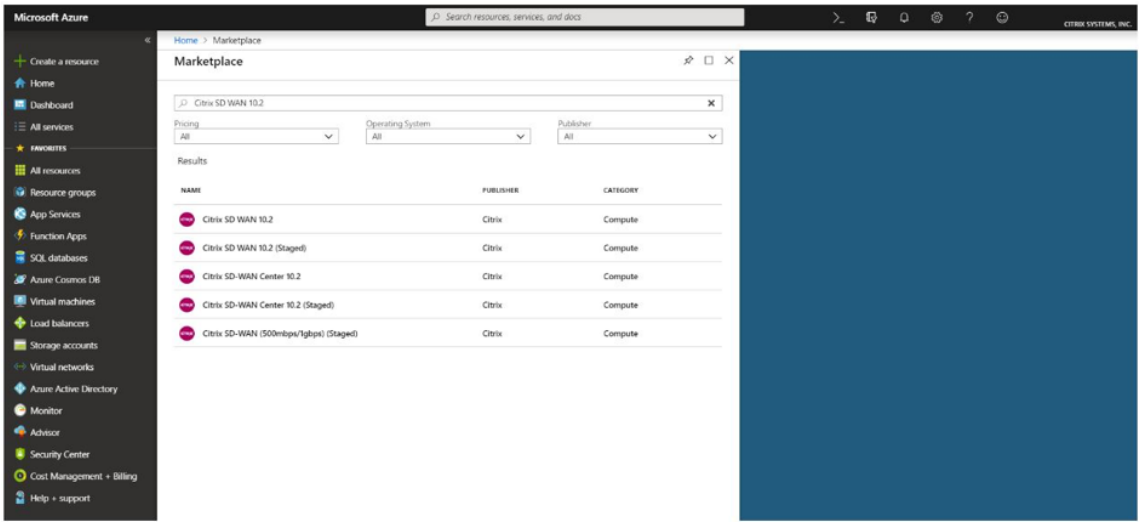
此集成的第三个组件是 网络定位服务 **(NLS)** ，允许内部用户绕过网关并直接连接到 VDA，从而减少内部网络流量的延迟。您可以手动配置 NLS，也可以通过 Citrix SD-WAN Orchestrator 进行配置。有关更多信息，请参阅 NLS。

配置

Citrix SD-WAN 虚拟机部署在指定区域内（根据客户的需要），并且可以通过 MPLS、Internet 或 4G/LTE 连接到多个分支机构位置。在虚拟网络 (VNET) 基础架构中，SD-WAN 标准版 (SE) 虚拟机以 Gateway 模式进行部署。VNET

具有通向 Azure Gateway 的路由。SD-WAN 实例有一条通向 Azure Gateway 的路由，用于 Internet 连接。此路由需要手动创建。

1. 在 Web 浏览器中，转到 Azure 门户。登录到微软 Azure 帐户并搜索 Citrix SD-WAN 标准版。
2. 在搜索结果中，选择 Citrix SD-WAN 标准版解决方案。在浏览描述并确保选择的解决方案正确无误后，单击 创建。

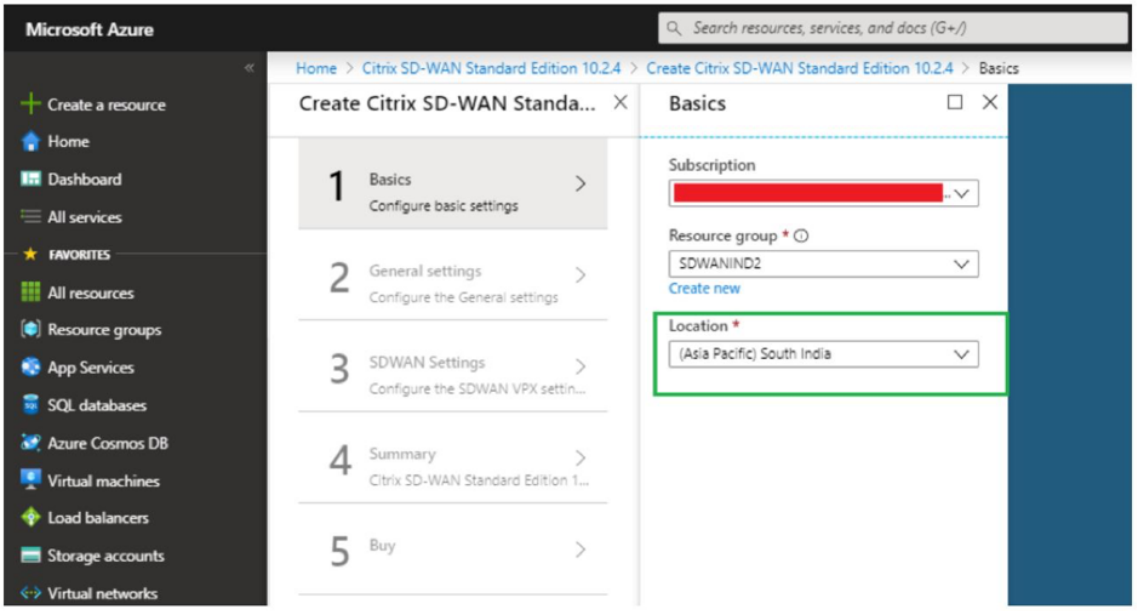


单击 创建后，将显示向导，提示创建虚拟机的必要详细信息。

3. 在 基本设置 页面中，选择要在其中部署 SD-WAN SE 解决方案的资源组。

   资源组是一个容器，用于保存 Azure 解决方案的相关资源。资源组可以包括解决方案的所有资源，或者仅包括要作为一个组管理的资源。根据您的部署情况，您可以决定如何为资源组分配资源。

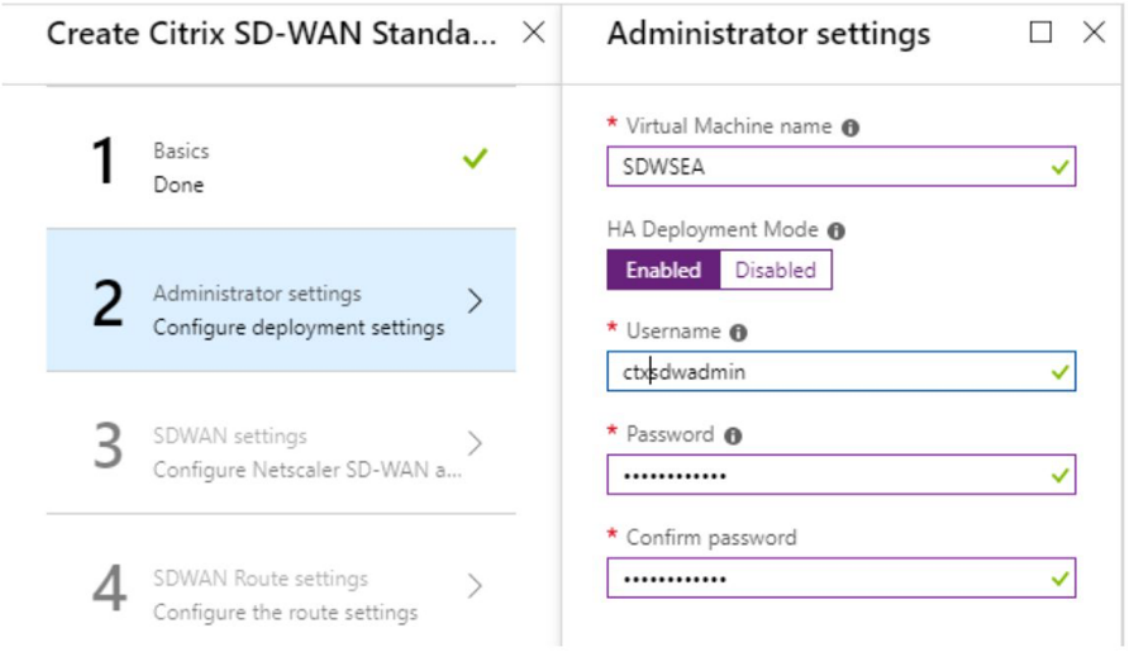
   对于 Citrix SD-WAN，建议您选择的资源组必须为空。同样，选择要在其中部署 SD-WAN 实例的 Azure 区域。该区域必须与部署 Citrix Virtual Apps and Desktops 资源的区域相同。



4. 在 管理员设置 页面下，提供虚拟机的名称。选择用户名和强密码。密码必须由大写字母和特殊字符组成，且必须超过九个字符。单击确定。

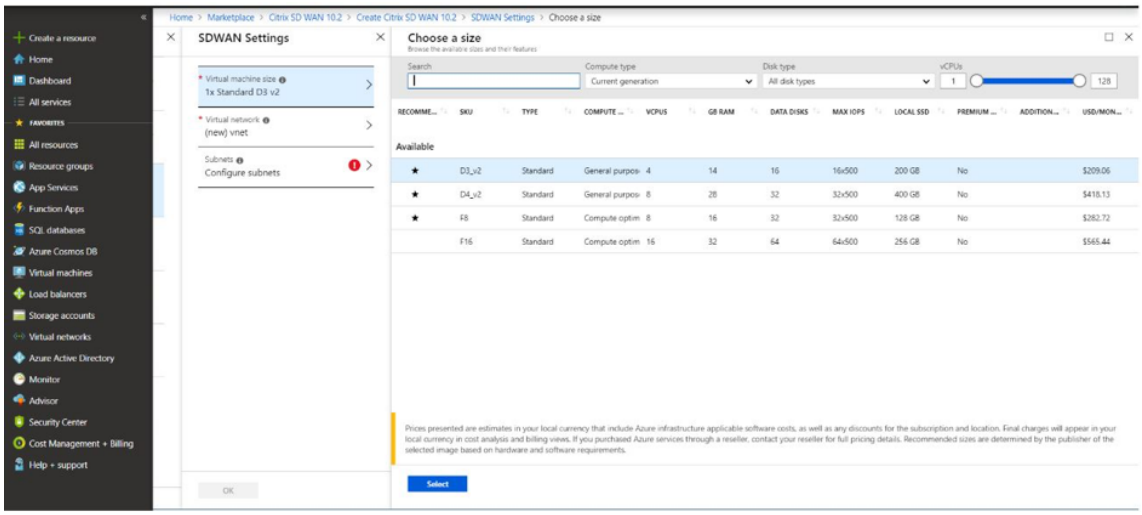
   以来宾用户身份登录到实例的管理界面需要此密码。要获得对实例的管理员访问权限，请使用 admin 作为用户名，并使用在 Provisioning 实例时创建的密码。如果您使用在 Provisioning 实例时创建的用户名，则可获得只读访问权限。此外，请在此处选择部署类型。

   如果要部署单个实例，请确保从 HA 部署模式选项中选择禁用，否则选择启用。对于生产网络，Citrix 始终建议以高可用性模式部署实例，因为它可以防止网络出现实例故障。

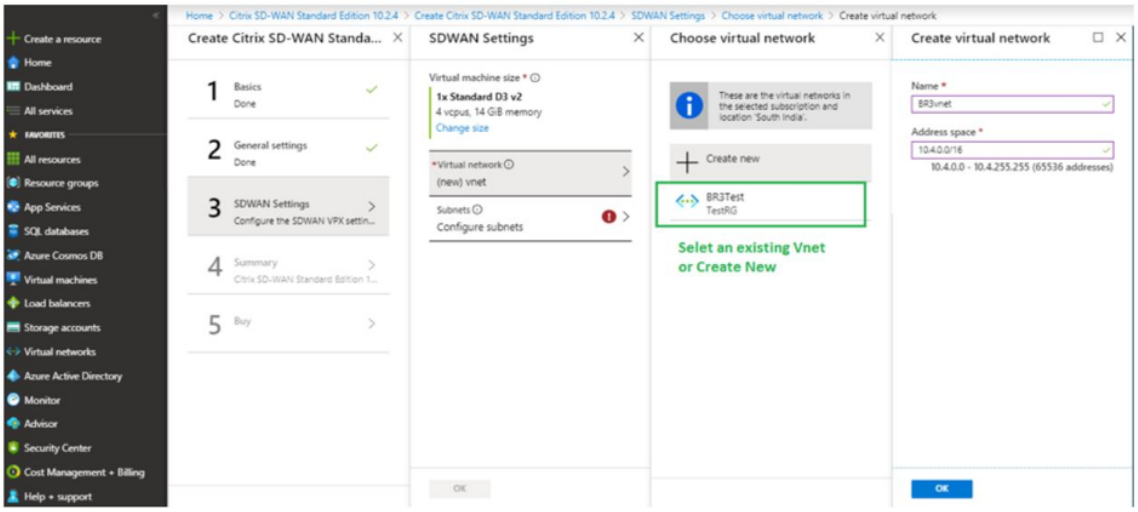


5. 在 **SD-WAN** 设置 页面下，选择要在其中运行映像的实例。根据您的要求选择以下实例类型：

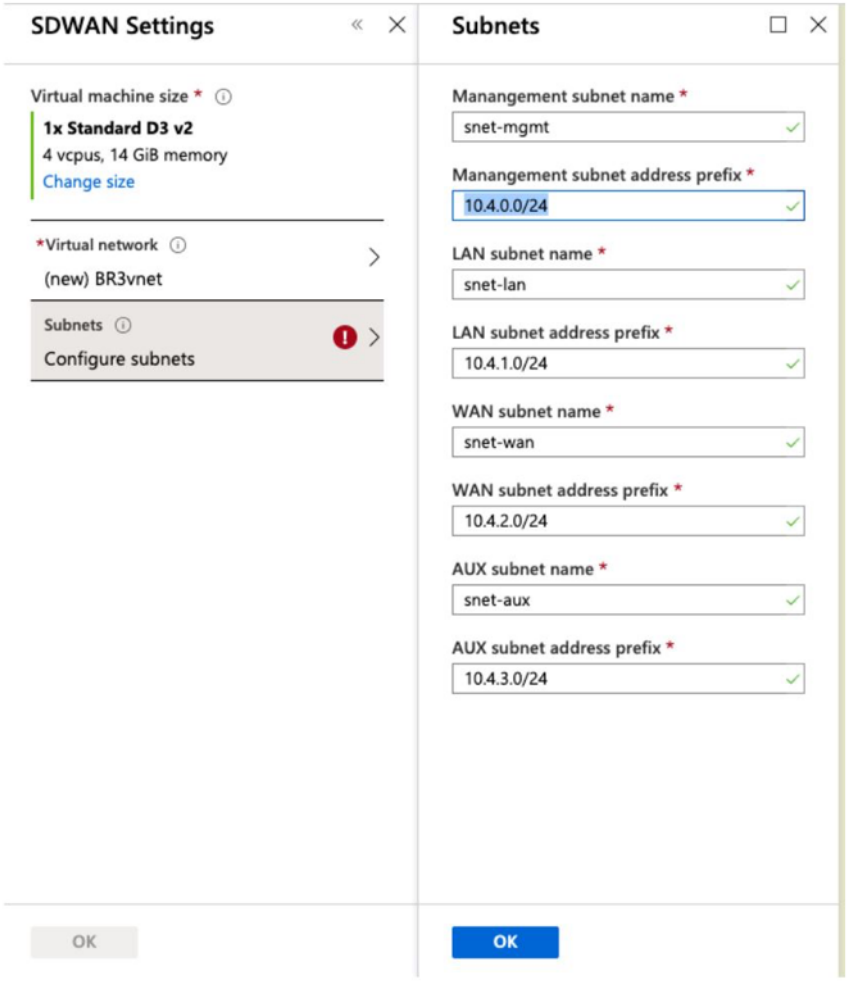
- 实例类型 D3_V2，最大单向吞吐量为 200 Mbps，最多可直接连接 16 个分支。
- 实例类型 D4_V2，最大单向吞吐量为 500 Mbps，最多可直接连接 16 个分支。
- 实例类型 F8 标准，最大单向吞吐量为 1 Gbps，最多可直接连接 64 个分支。
- 实例类型 F16 标准，最大单向吞吐量为 1 Gbps，最多可直接连接 128 个分支。



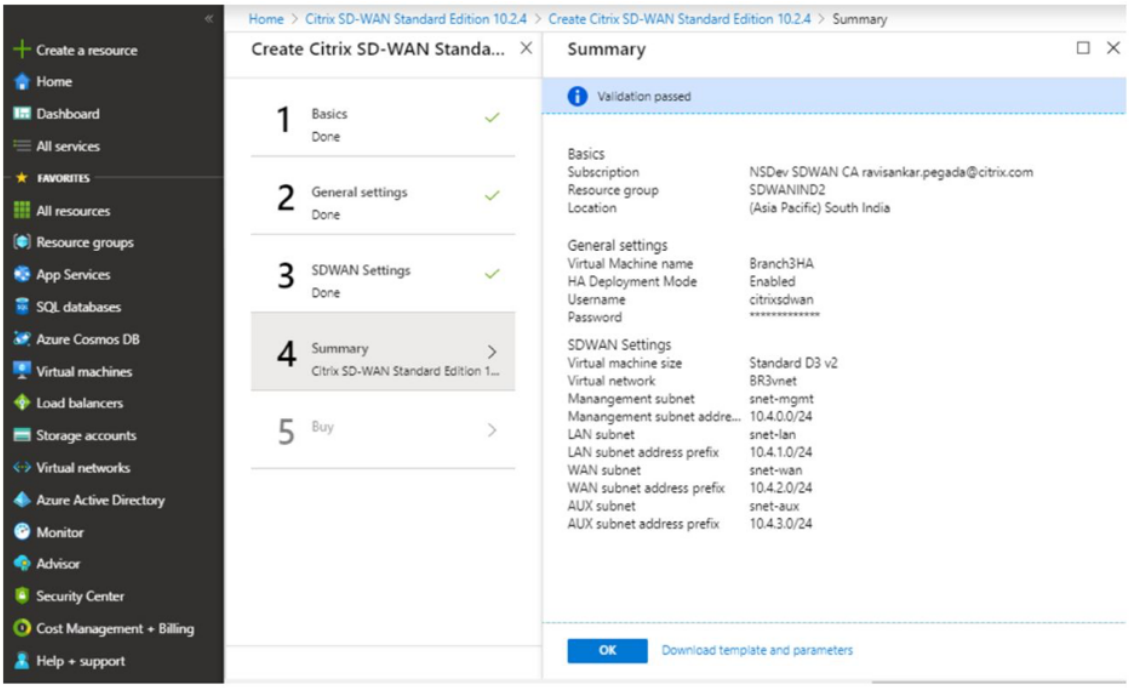
6. 创建新的虚拟网络 (VNet) 或使用现有虚拟网络。这是部署的最关键步骤，因为此步骤选择要分配给 SD-WAN VPX 虚拟机接口的子网。



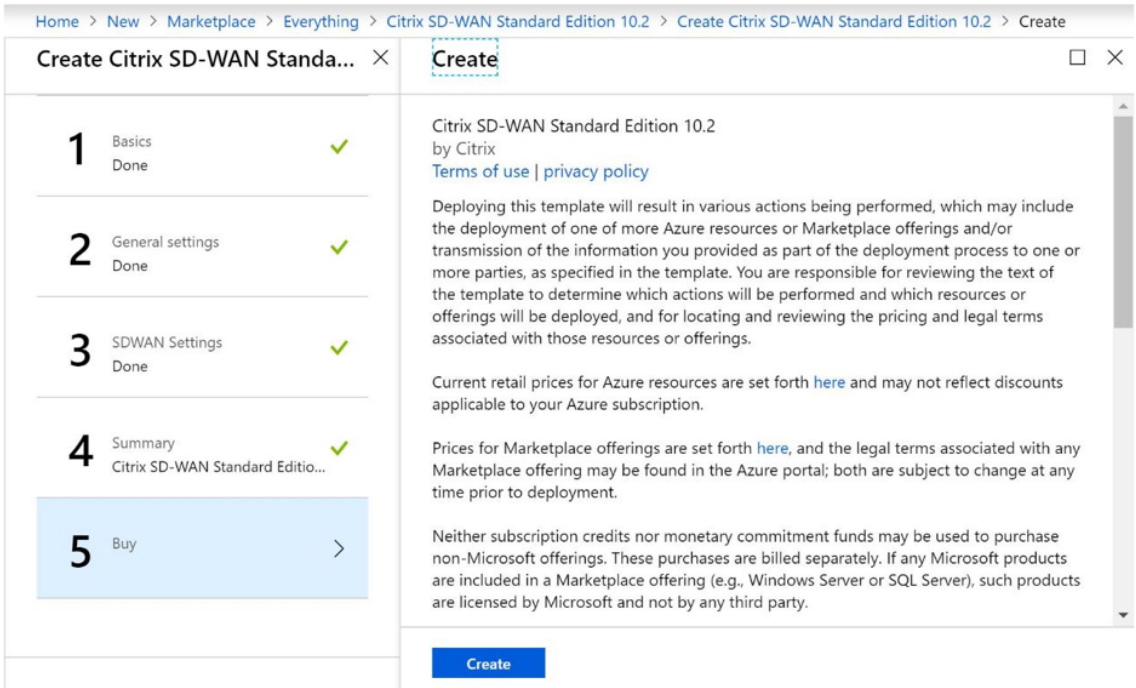
仅当您以 HA 模式部署实例时，才需要辅助子网。确保 SD-WAN 实例部署在与 Citrix Virtual Apps and Desktops 资源相同的 VNet 中，并且与 SD-WAN VPX 设备的 LAN 接口位于同一子网中。



7. 在“摘要”页面中验证配置，然后单击“确定”。



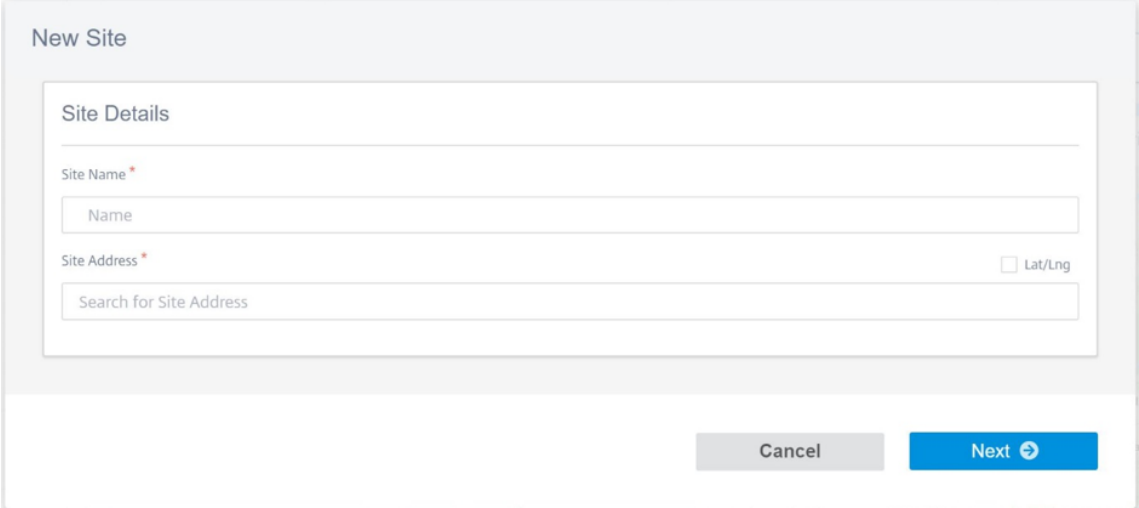
8. 在 购买 页面上，单击 创建 以启动实例的预配过程。预配置实例可能需要大约 10 分钟。您会在 Azure 管理门户中收到一条通知，建议实例创建成功/失败。



成功创建实例后，获取分配给 SD-WAN 实例管理接口的公有 IP。它可以在已预配实例的资源组的网络部分中找到。检索后，您可以使用它登录到实例。

> 注意
>
> 对于管理员访问，用户名是 **admin** ，密码是您在实例创建过程中设置的密码。

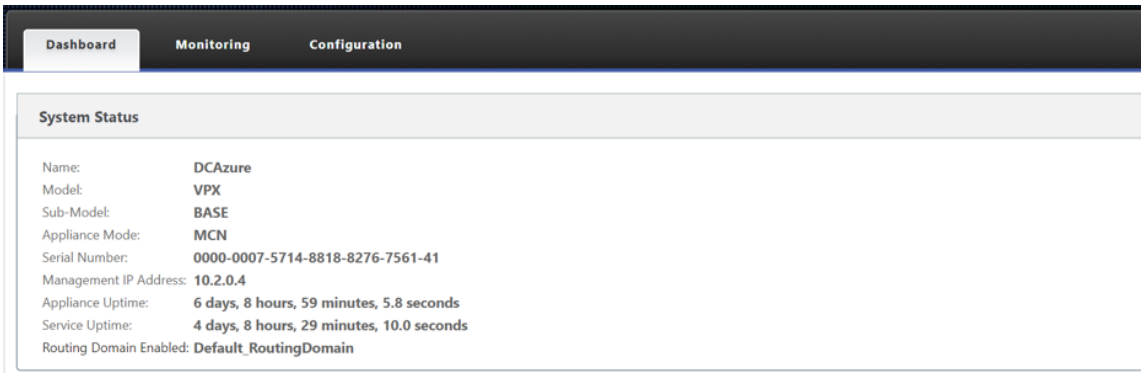
9. 置备站点后，登录 SD-WAN Orchestrator 以对其进行配置。如前提条件中所述，您必须拥有 SD-WAN Orchestrator 才能配置站点。如果您还没有，请参阅 Citrix SD-WAN Orchestrator 入职培训。
10. 如果您已经有 SD-WAN 网络，则继续为在 Azure 中置备的站点创建配置。否则，您必须创建一个 MCN。有关详细信息，请参阅 网络配置。
11. 一旦您有权访问 SD-WAN Orchestrator 并且已经设置了 MCN，请登录 SD-WAN Orchestrator，然后单击 **+** 新站 点开始配置 SD-WAN VPX 设备（您已在 Azure 中预配）。



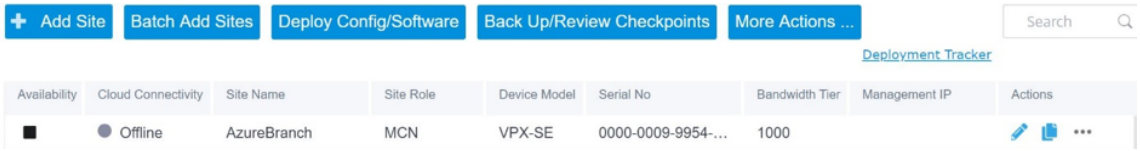
12. 提供唯一的站点名称，并根据要 Provisioning 映像的区域输入地址。要在 Azure 中设置实例，请参阅 基本设置。

> 注意
>
> 要在 Azure 中获取实例的序列号，请通过公共管理 IP 登录到实例。您可以在仪表板屏幕上看到序列号。如果要在 HA 中配置实例，则必须捕获两个序列号。此外，在配置实例时，请确保选择接口为 受信任。

13. 用于获取与 Azure 上的 LAN 和 WAN 接口相关联的 IP 地址。导航到 **Azure** 门户 **>** 资源组 **>** 置备 **SD-WAN** 的资源组 **>SD-WAN** 虚拟机 **>** 网络。



14. 完成实例配置后。导航到 配置 **>** 网络配置主页，单击部署配置/软件。

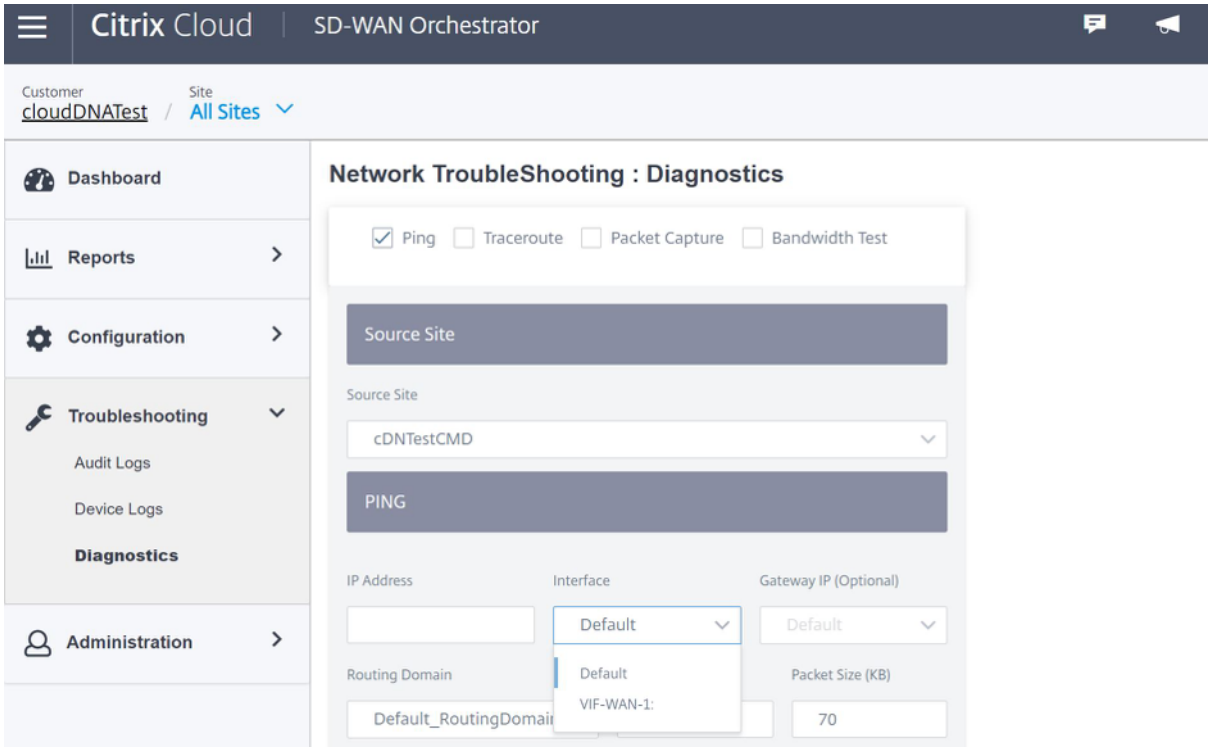


15. 如果没有问题且配置准确无误，则在运行配置部署后，必须在 Azure 中的实例和 MCN 之间建立虚拟路径。

Citrix Virtual Apps and Desktops 配置

正如部 署和配置 部分中突出显示的那样，AD/DNS 存在于充当 DC 的本地位置，而在具有 SD-WAN 的部署中则存在于 LAN 网络中的 SD-WAN 后面。这是您需要在此处配置的 AD/DNS 的 IP。如果您正在使用 Azure Active Directory 服务/DNS，请将 **168.63.129.16** 配置为 DNS IP。

如果您正在使用本地广告 /DNS。请检查您是否能够从 SD-WAN 设备 ping DNS 的 IP。您可以通过导航到“疑难解答” **>** “诊断”来完成此操作。选中 **Ping** 复选框，然后从 SD-WAN 设备的 LAN 接口/默认接口启动 ping 到 AD/DNS 的 IP。



如果 ping 成功，则表示可以成功访问您的 AD/DNS，如果没有，则意味着您的网络中存在路由问题，从而阻碍了您的 AD/DNS 的可访问性。如果可能，请尝试将您的 AD 和 SD-WAN 设备置置于同一个 LAN 网段上。

如果仍然存在问题，请与您的网络管理员联系。如果不成功完成此步骤，目录创建步骤将无法成功，并且您会收到一条错误消息，因为 未配置全局 **DNS IP**。

> 注意：
>
> 确保 DNS 能够同时解析内部和外部 IP。

网络定位服务

借助 Citrix Cloud 中的 网络定位 服务，您可以优化向订阅者工作区提供的应用程序和桌面的内部流量，从而加快 HDX 会话速度。内部和外部网络上的用户必须通过外部网关连接到 VDA。虽然外部用户需要这样做，但内部用户与虚拟资源的连接速度较慢。网络定位 服务允许内部用户绕过网关直接连接到 VDA，从而减少内部网络流量的延迟。

配置

要设置 网络定位 服务，请使用以下方法之一：

- **Citrix SD-WAN Orchestrator**：有关使用 Citrix SD-WAN Orchestrator 配置 NLS 的详细信息，请参阅网络定位服务。
- **Citrix** 提供的网络定位服务 **PowerShell** 模块：有关使用 PowerShell 模块配置 NLS 的详细信息，请参阅 PowerShell 模块和配置。

网络位置共享内部用户连接的网络的公共 IP 范围。当订阅者从其 Workspace 启动 Virtual Apps 和桌面会话时，Citrix Cloud 会根据用户所连接的网络的公有 IP 地址检测用户是否为公司网络的内部或外部。

如果用户从内部网络连接，Citrix Cloud 会将连接直接路由到 VDA，而绕过 Citrix Gateway。如果订阅者通过外部连接，Citrix Cloud 会按预期方式通过 Citrix Gateway 将订阅者路由，然后将该订阅者重定向到内部网络中的 VDA。

> 注意：
>
> 需要在网络定位服务中配置的公共 IP 必须是分配给 WAN 链路的公有 IP。

域名系统

September 2, 2022

域名系统 **(DNS)** 将人类可读的域名转换为机器可读的 IP 地址，反之亦然。Citrix SD-WAN 提供以下 DNS 功能：

- DNS 代理
- DNS 透明转发

您可以使用以下类型的 DNS 服务通过 Citrix SD-WAN Orchestrator 服务配置 DNS 代理或 DNS 透明转发：

- 静态 **DNS** 服务：允许您配置静态 IPv4 DNS 服务器 IP 地址。您可以创建内部、ISP、谷歌或任何其他开源 DNS 服务。静态 DNS 服务可以在全局和站点级别进行配置。

- 动态 **DNS** 服务：允许您配置动态 IPv4 DNS 服务器 IP 地址。动态 DNS 服务只能在站点级别配置。每个站点只允许一个动态 DNS 服务。
- **Staticv6 DNS** 服务：允许您配置静态 IPv6 DNS 服务器 IP 地址。您可以创建内部、ISP、谷歌或任何其他开源 DNS 服务。Staticv6 DNS 服务可以在全局和站点级别进行配置。
- **DynamicV6 DNS** 服务：允许您配置动态 IPv6 DNS 服务器 IP 地址。DynamicV6 DNS 服务只能在站点级别进行配置。每个站点只允许一个动态 DNS 服务。

DNS 代理

您可以配置包含多个转发器的代理，以帮助根据应用程序域名控制 DNS 请求。DNS 转发适用于通过 UDP 连接接收的请求。有关如何通过 SD-WAN Orchestrator 服务配置 DNS 代理的信息，请参阅 DNS 代理。

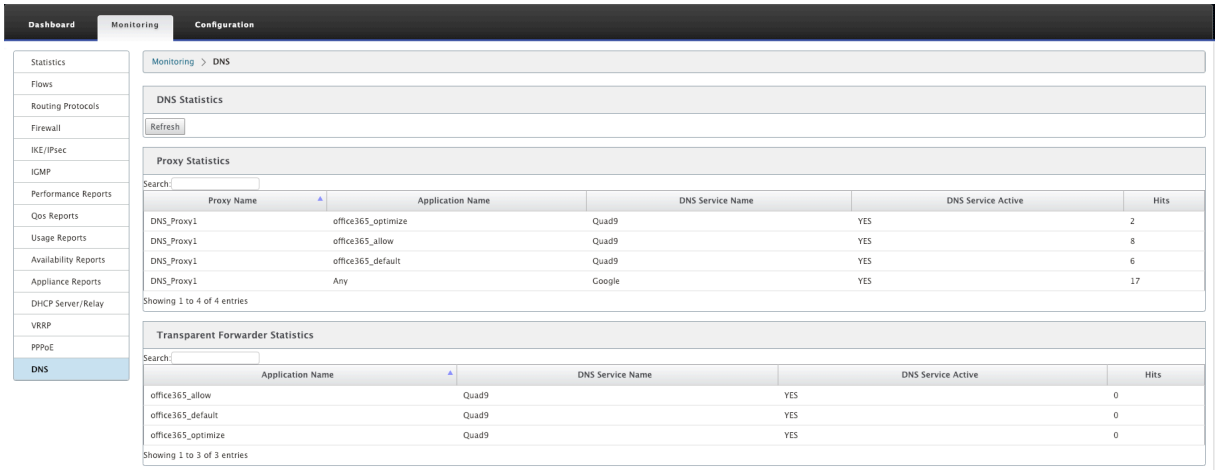
DNS 透明转发器

Citrix SD-WAN 可以配置为透明 DNS 转发器。在此模式下，SD-WAN 可以拦截未发往其 IP 地址的 DNS 请求，并将其转发到指定的 DNS 服务。只有来自受信任接口上的本地服务的 DNS 请求才会被拦截。如果 DNS 请求与 DNS 转发器列表中的任何应用程序相匹配，则会将其转发到已配置的 DNS 服务。只有通过 UDP 连接发出的请求才支持 DNS 转发。有关如何通过 SD-WAN Orchestrator 服务配置 DNS 透明转发器的信息，请参阅 DNS 透明转发器。

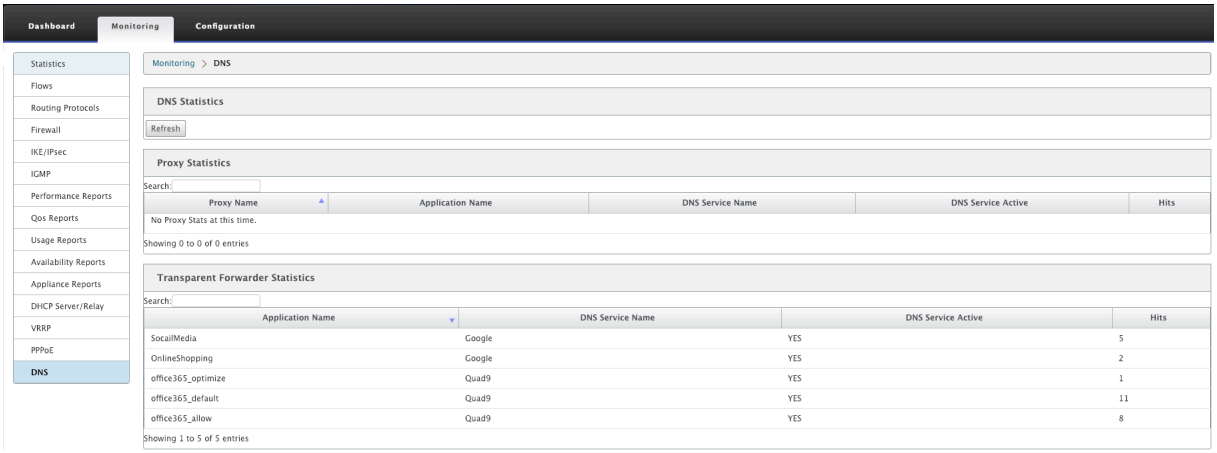
监视

要查看代理统计信息和透明转发器统计信息，请导航到 监控 **> DNS**。
您可以查看应用程序名称、DNS 服务名称、DNS 服务状态以及对 DNS 服务的单击次数。

代理统计



透明的转发器统计信息



DHCP

November 16, 2022

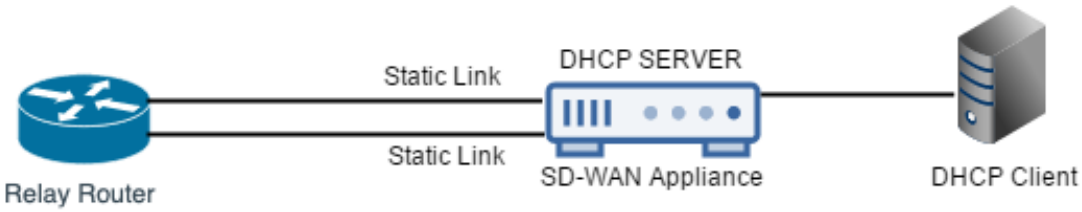
Citrix SD-WAN 引入了将标准版设备用作 DHCP 服务器或 DHCP 中继代理的功能。通过 DHCP 服务器功能，与 SD-WAN 设备的 LAN/WAN 接口位于同一网络中的设备可以从 SD-WAN 设备获取其 IP 配置。通过 DHCP 中继功能，您的 SD-WAN 设备可以在 DHCP 客户端与服务器之间转发 DHCP 数据包。

以下是使用 DHCP 服务器和 DHCP 中继功能的好处：

- 减少客户现场的设备量。
- 在客户端站点更换路由器（轻松部署边缘路由器服务）。
- 简化客户端站点网络。
- 没有 CLI 命令的路由器配置。
- 减少简单客户端站点上的手动配置。

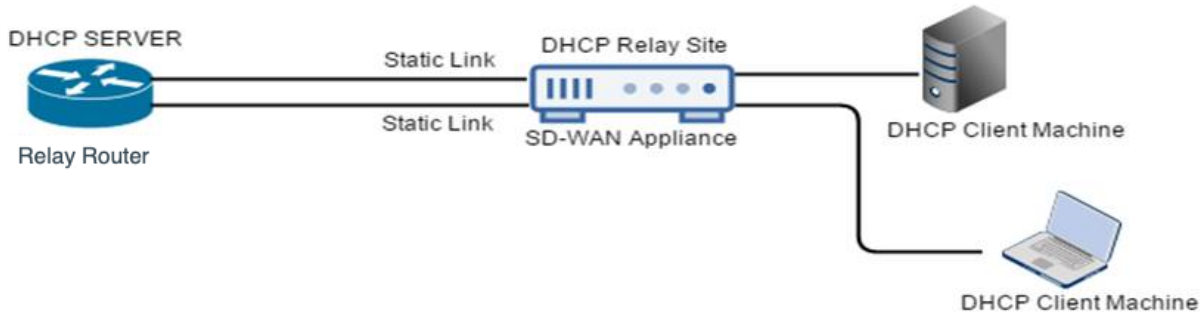
DHCP 服务器

可以将 Citrix SD-WAN 设备配置为 DHCP 服务器。它可以从网络中指定的地址池向 DHCP 客户端分配和管理 IP 地址。DHCP 服务器可以配置为分配更多参数，例如域名系统 (DNS) 服务器的 IP 地址和默认路由器。DHCP 服务器接受地址分配请求和续订。DHCP 服务器还接受来自本地连接的 LAN 段或网络中其他 DHCP 中继代理所转发的 DHCP 请求的广播。



DHCP 中继

DHCP 中继代理是在客户端和服务器之间转发 DHCP 数据包的主机或路由器。网络管理员可以使用 SD-WAN 设备的 DHCP 中继服务在本地 DHCP 客户端和远程 DHCP 服务器之间中继请求和答复。它允许本地主机从远程 DHCP 服务器获取动态 IP 地址。中继代理接收 DHCP 消息并生成要在另一个接口上发出的新 DHCP 消息。



通过 DHCP 客户端进行 WAN 链接 IP 地址学习

Citrix SD-WAN 设备支持通过 DHCP 客户端进行 WAN 链接 IP 地址学习。此功能减少了部署 SD-WAN 设备所需的手动配置量，并通过无需购买静态 IP 地址来降低 ISP 成本。SD-WAN 装置可以获取不受信任接口上 WAN 链路的动态 IP 地址。这样就不需要中间 WAN 路由器来执行此功能。

> 注意
>
> - DHCP 客户端只能配置为客户端节点的不受信任的非桥接接口。
> - 只有配置了公共 IP 地址，才能在 MCN/RCN 上启用 DHCP 客户端和数据端口。
> - 具有 DHCP 客户端配置的站点上不支持单臂或基于策略的路由 (PBR) 部署。
> - DHCP 事件仅从客户端的角度记录，不会生成 DHCP 服务器日志。

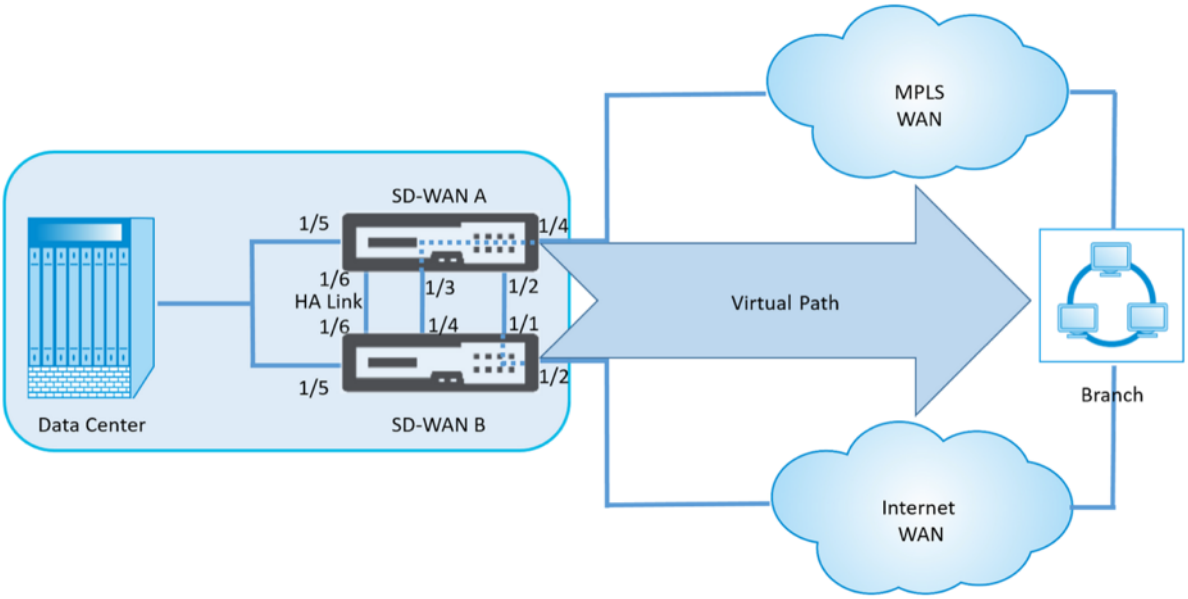
从 Citrix SD-WAN 11.5 版本开始，您可以通过 Citrix SD-WAN Orchestrator 服务在故障阻止模式下为不受信任的虚拟接口配置 DHCP。有关详细信息，请参阅 通过 DHCP 客户端获取 WAN 链路 IP 地址。

故障到线端口上的 **DHCP** 支持

此前，DHCP 客户端仅在故障到块端口上受支持。在 11.2.0 版本中，DHCP 客户端功能在具有串行高可用性 (HA) 部署的分支站点的故障到线端口上进行了扩展。此增强功能：

- 允许在具有故障到线网桥对和串行 HA 部署的不受信任接口组上进行 DHCP 客户端配置。
- 允许选择 DHCP 接口作为 私有内联网 **WAN** 链接的一部分。

专用内部网链接现在支持 DHCP 客户端。



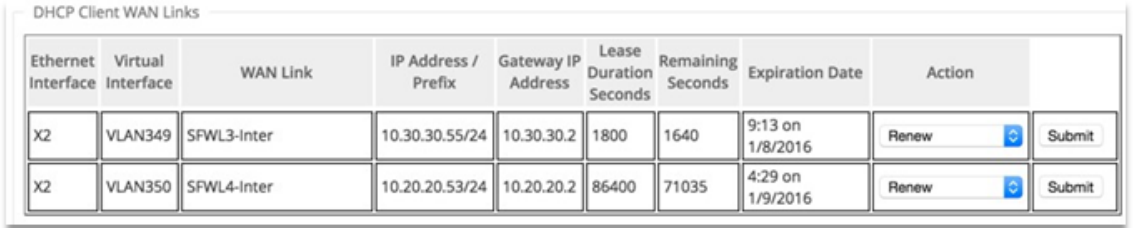
> 注意：
>
> 不得将 LAN 接口连接至失效线对，因为数据包可能会在接口之间桥接。

监视 **DHCP** 客户端 **WAN** 链接

运行时虚拟 IP 地址、子网掩码和网关设置记录并存档在名为 *SDWANVW_ip_learned.log* 的日志文件中。当学习、发布或过期动态虚拟 IP 以及学习到的网关或 DHCP 服务器出现通信问题时，都会生成事件。或者在存档的日志文件中检测到重复的 IP 地址时。如果在站点中检测到重复 IP，则动态虚拟 IP 地址将被释放和续订，直到站点上的所有虚拟接口获得唯一的虚拟 IP 地址为止。

要监视 DHCP 客户端 WAN 链接，请执行以下操作：

1. 在 SD-WAN 设备的 启用/禁用/清除流 程页面中，DHCP 客户端 WAN 链接表提供了已知 IP 的状态。
2. 您可以请求续订 IP，这会刷新租约时间。您还可以选择 发布续订，这会发出新的 IP 地址或与新租约相同的 IP 地址。

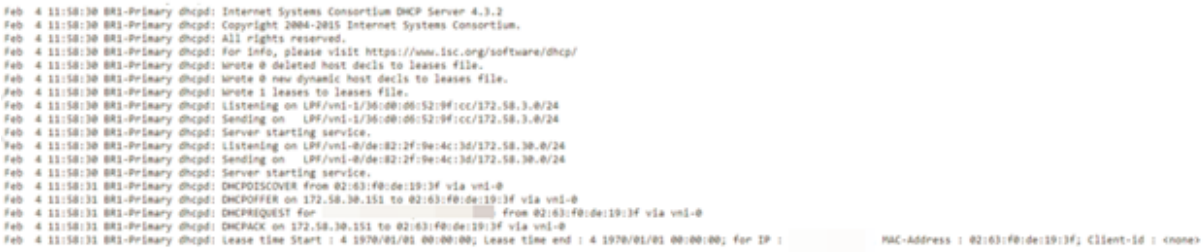

DHCP Client WAN Links

Ethernet Interface	Virtual Interface	WAN Link	IP Address / Prefix	Gateway IP Address	Lease Duration Seconds	Remaining Seconds	Expiration Date	Action	
X2	VLAN349	SFWL3-Inter	10.30.30.55/24	10.30.30.2	1800	1640	9:13 on 1/8/2016	Renew	Submit
X2	VLAN350	SFWL4-Inter	10.20.20.53/24	10.20.20.2	86400	71035	4:29 on 1/9/2016	Renew	Submit

DHCP 日志

Citrix SD-WAN 使您能够为 IP 地址生成 DHCP 服务器日志。每当将 IP 地址分配给端点时，都会生成日志。这些日志包含诸如 IP 地址分配和租用期限的时间戳、MAC 地址、客户端 ID 等详细信息。客户端 ID **none** 表示它不存在于 DHCP 请求中。

要生成和查看 DHCP 日志，请导航到 配置 > 日 志记录/监控。从下拉列表中选择 **SDWAN_dhcp.log** 选项，然后单击查看日志。



> 注意
>
> 只有当 Citrix SD-WAN 充当 DHCP 服务器时，才会生成这些日志。

动态 **PAC** 文件定制

September 2, 2022

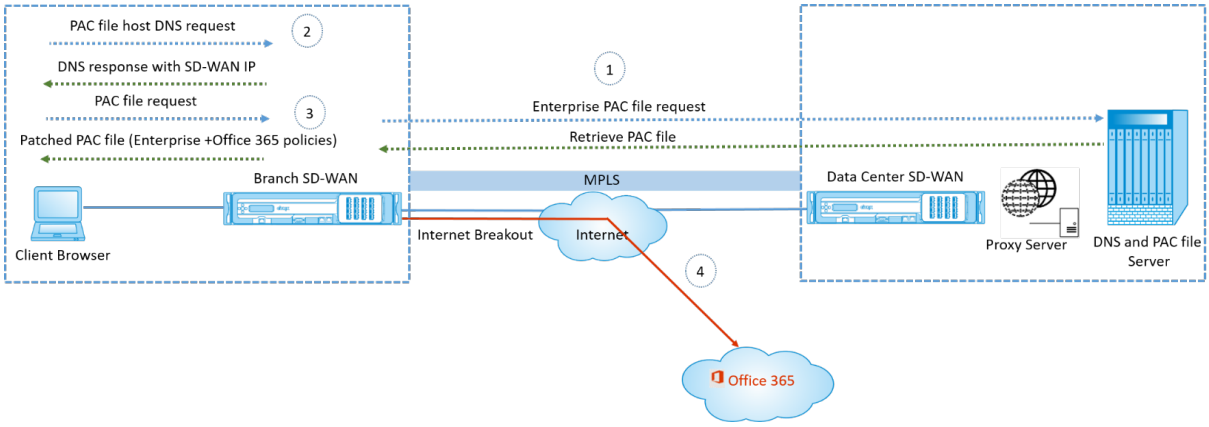
随着企业对任务关键型 SaaS 应用程序和分布式员工的采用率的增加，减少延迟和拥堵变得非常重要。延迟和拥堵是通过数据中心追加流量的传统方法所固有的。Citrix SD-WAN 允许直接 Internet 突破的 SaaS 应用程序，如 Office 365. 有关详细信息，请参阅 Office 365 优化。

如果在企业部署上配置了显式 Web 代理，则所有流量都会转向 Web 代理，从而难以进行分类和直接 Internet 突破。解决方案是通过自定义企业 PAC（代理自动配置）文件来排除 SaaS 应用程序流量获取代理。

Citrix SD-WAN 11.0 通过动态生成和提供自定义 PAC 文件，允许代理绕过和本地 Internet 突破 Office 365 应用程序流量。PAC 文件是一个 JavaScript 函数，用于定义 Web 浏览器请求是直接进入目标还是 Web 代理服务器。

PAC 文件自定义的工作原理

理想情况下，企业网络主机 PAC 文件在内部 Web 服务器上，这些代理设置通过组策略分发。客户端浏览器从企业 Web 服务器请求 PAC 文件。Citrix SD-WAN 设备为启用 Office 365 分组的站点提供自定义 PAC 文件。



1. Citrix SD-WAN 定期从企业 Web 服务器请求并检索企业 PAC 文件的最新副本。Citrix SD-WAN 设备将 Office 365 URL 修补到企业 PAC 文件。企业 PAC 文件预计将具有占位符（SD-WAN 特定标签），其中 Office 365 URL 无缝修补。
2. 客户端浏览器引发企业 PAC 文件主机的 DNS 请求。Citrix SD-WAN 拦截代理配置文件 FQDN 的请求，并使用 Citrix SD-WAN VIP 进行响应。
3. 客户端浏览器请求 PAC 文件。Citrix SD-WAN 设备在本地提供修补的 PAC 文件。PAC 文件包括企业代理配置和 Office 365 URL 排除策略。
4. 在收到 Office 365 应用程序的请求时，Citrix SD-WAN 设备将执行直接的 Internet 分组。

必备条件

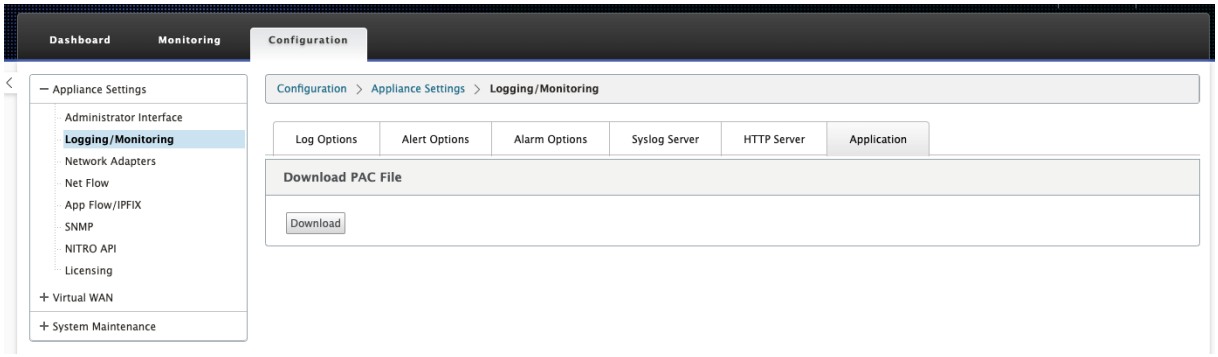
1. 企业应该有一个 PAC 文件托管。
2. PAC 文件应该有一个占位符 *SDWAN_TAG* 或一个用于修补 Office 365 网址的 *findproxyforurl* 函数。
3. PAC 文件 URL 应基于域，而不是基于 IP。
4. PAC 文件仅通过受信任的身份 VIP 提供。
5. Citrix SD-WAN 设备应能够通过其管理界面下载企业 PAC 文件。

配置 PAC 文件自定义

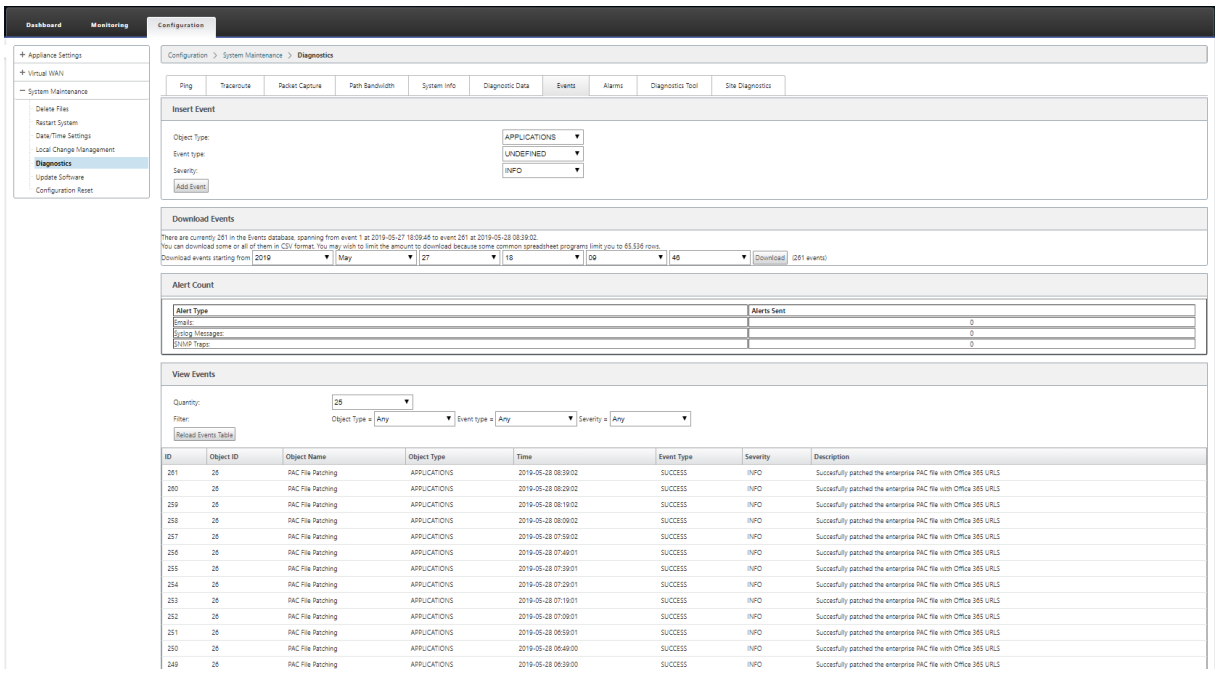
您可以使用 Citrix SD-WAN Orchestrator 服务启用 PAC 文件自定义。有关更多信息，请参阅 代理自动配置。

故障排除

您可以从 Citrix SD-WAN 设备下载自定义 PAC 文件以进行故障排除。导航到 配置 > 装置设置 > 日 志记录/监控 > 应用程序，然后单击下载。



您还可以在 事 件部分查看 PAC 文件的修补状态，导航到 配置 > 系统维护 > 诊断，单击 事 件选项卡。



限制

- 不支持 HTTPS PAC 文件服务器请求。
- 不支持网络中的多个 PAC 文件，包括路由域或安全区域的 PAC 文件。
- 不支持从头开始在 Citrix SD-WAN 上生成 PAC 文件。
- 不支持通过 DHCP 进行 WPAD。

GRE 通道

September 2, 2022

GRE 通道功能允许您配置 Citrix SD-WAN 设备以终止局域网或内联网上的 GRE 通道。要使用 SD-WAN Orchestrator 服务配置 GRE 通道，请参阅 GRE 服务。

带内和备份管理

September 2, 2022

带内管理

Citrix SD-WAN 允许您通过两种方式管理 SD-WAN 设备：带外管理和带内管理。带外管理允许您使用为管理保留的端口创建管理 IP，该端口仅承载管理流量。带内管理允许您使用 SD-WAN 数据端口进行管理。它同时承载数据和管理流量，而无需配置添加管理路径。

带内管理允许虚拟 IP 地址连接到管理服务，如 Web UI 和 SSH。您可以在启用可用于 IP 服务的多个受信任接口上启用带内管理。您可以使用管理 IP 和带内虚拟 IP 访问 Web UI 和 SSH。

从 Citrix SD-WAN 11.4.2 版本开始，必须配置带内管理才能通过带内管理端口与 Citrix SD-WAN Orchestrator 服务建立连接。否则，当管理端口未连接且未配置带内 IP 地址时，设备将失去与 Citrix SD-WAN Orchestrator 服务的连接。

> 注意
>
> - Citrix SD-WAN Orchestrator 服务不允许将 服务类型 配置为 任何 目标 NAT 策略。
> - 当唯一的管理连接是带内 HA 时，请避免禁用该服务。
>   如果禁用该服务，可以将自己锁定在设备之外。

从 Citrix SD-WAN 11.5 开始，只能通过 Citrix SD-WAN Orchestrator 服务在虚拟 IP 上启用带内管理。有关更多信息，请参阅 带内管理。

从 Citrix SD-WAN 11.3.1 以后的版本开始，带内管理支持高可用性设备对。主设备和辅助设备之间的通信通过使用 NAT 的虚拟接口进行。

以下端口允许与 HA 设备上的管理服务进行通信：

- HTTPS
  - 443-连接到活跃的 HA
  - 444-重定向到 HA 主

  - 445-重定向到医管局中学

- SSH
  - 22-连接到 HA 活动
  - 23-重定向到医管局主
  - 24-重定向到医管局二级

- SNMP
  - 161-连接到活动的 HA
  - 162-重定向到医管局主
  - 163-重定向到医管局辅助

使用目标 NAT 策略创建 IP 地址，允许连接到带内 HA，而无需输入端口。

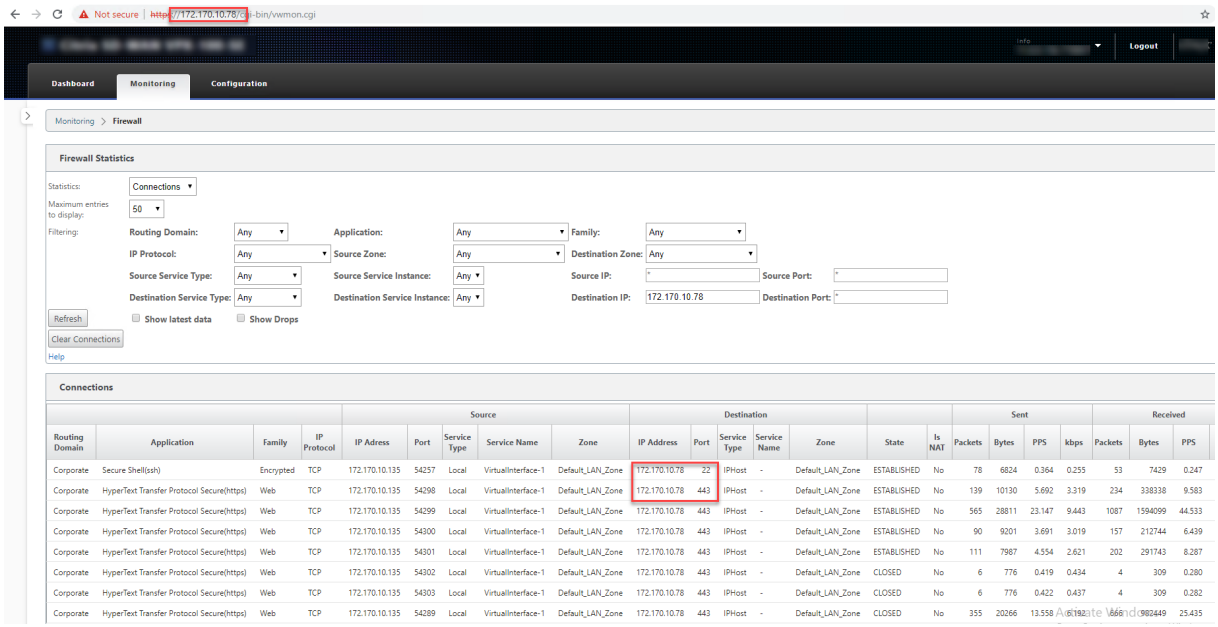
例如，以下带内 IP 地址用于访问设备：

- 主动设备-1.0.1.2
- 主要设备-1.0.1.10
- 辅助设备-1.0.1.11

监视带内管理

在前面的示例中，我们已经在 172.170.10.78 虚拟 IP 上启用了带内管理。您可以使用此 IP 访问 Web UI 和 SSH。

在 Web UI 中，导航到 监控 > 防火墙。您可以在 目标 IP 地 址 列中分别看到使用端口 **22** 和 **443** 上的虚拟 **IP** 访问 SSH 和 Web UI。



带内 **Provisioning**

在家庭或小型分支机构等较简单的环境中部署 SD-WAN 设备的需求显著增加。为更简单的部署配置单独的管理访问权限是额外的开销。零接触部署以及带内管理功能可通过指定的数据端口实现配置和配置管理。现在，指定的数据端口支持零接触部署，无需使用单独的管理端口进行零接触部署。Citrix SD-WAN 还允许在数据端口关闭时将管理流量无缝故障切换到管理端口，反之亦然。

处于出厂发货状态的设备（支持带内配置）可通过简单地将数据或管理端口连接到 Internet 进行 Provisioning。支持带内 Provisioning 的设备具有用于 LAN 和 WAN 的特定端口。处于出厂重置状态的设备具有默认配置，允许与零接触部署服务建立连接。LAN 端口充当 DHCP 服务器，并将动态 IP 分配给充当 DHCP 客户端的 WAN 端口。WAN 链路监视四 9 DNS 服务以确定 WAN 连接性。

> 注意
>
> 带内 Provisioning 仅适用于 SD-WAN 110 SE 和 SD-WAN VPX 平台。

获取 IP 地址并与零接触部署服务建立连接后，将下载配置包并安装在设备上。

注意：对于第 0 天通过数据端口置备 SD-WAN 设备，设备软件版本必须为 SD-WAN 11.1.0 或更高版本。

处于出厂重置状态的设备的默认配置包括以下配置：

- LAN 端口上的 DHCP 服务器
- WAN 端口上的 DHCP 客户端
- 适用于 DNS 的 QUAD9 配置
- 默认局域网 IP 为 192.168.0.1
- 35 天的宽限许可证。

置备设备后，默认配置将被禁用，并由零接触部署服务接收的配置覆盖。如果设备许可证或宽限许可证过期，则会激活默认配置，以确保设备保持连接到零接触部署服务并接收通过零接触部署管理的许可证。

默认/备用配置

回退配置可确保设备在链路故障、配置不匹配或软件不匹配时保持连接到零接触部署服务。默认情况下，在具有默认配置文件的设备上启用回退配置。您还可以根据现有 LAN 网络设置编辑备用配置。

注意：在初始设备置备之后，请确保为零接触部署服务连接启用了回退配置。

下表提供了在不同平台上用于备用配置的预先指定 WAN 和 LAN 端口的详细信息：

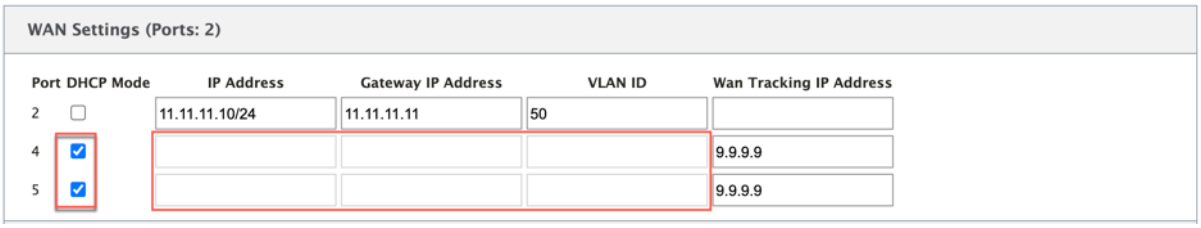
平台	WAN 端口	LAN 端口
110	1/2	1/1
110-LTE	1/2，LTE-1	1/1

平台	WAN 端口	LAN 端口
210	1/4、1/5	1/3
210-LTE	1/4、1/5、LTE-1	1/3
VPX	2	1
1100	1/4、1/5、1/6	1/3 (FTB)

从 Citrix SD-WAN 11.3.1 版本中，WAN 端口设置是可配置的。可以使用 DHCP 客户端将 WAN 端口配置为独立的 WAN 链路，并监视 Quad9 DNS 服务以确定 WAN 连接。在没有 DHCP 的情况下，您可以为 WAN 端口配置 WAN IPS/静态 IP，以便使用带内管理进行初始配置。

> 注意：
>
> 您只能使用静态 IP 配置以太网端口。静态 IP 无法使用 LTE-1 和 LTE-E1 端口进行配置。尽管您可以将 LTE-1 和 LTE-E1 端口添加为 WAN，但配置字段仍然是不可编辑的。

添加 WAN 端口时，它会被添加到 **WAN** 设置（端口：**2**）部分下，默认情况下选中 **DHCP** 模式 复选框。如果选中 **DHCP** 模式 复选框，则 **IP** 地址、网关 **IP** 地址 和 **VLAN ID** 文本字段将显示为灰色。如果要配置静态 IP，请清除 **DHCP** 模式 复选框。



默认情况下，**WAN** 跟踪 **IP** 地址字段将自动填充 9.9.9.9。您可以根据需要更改地址。

> 注意：
>
> 如果选中 动态 **DNS** 服务器 复选框，请确保添加/配置至少一个已选择 **DHCP** 模式 的 WAN 端口。

可配置的管理或数据端口

带内管理允许数据端口同时传输数据和管理流量，无需使用专用管理端口。这使得管理端口在已经具有较低端口密度的低端设备上未使用。Citrix SD-WAN 允许您将管理端口配置为作为数据端口或管理端口运行。

> 注意
>
> 只能在以下平台上将管理端口转换为数据端口：

- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

只有在设备上其他受信任接口上启用带内管理时，才能配置管理端口。

备份管理网络

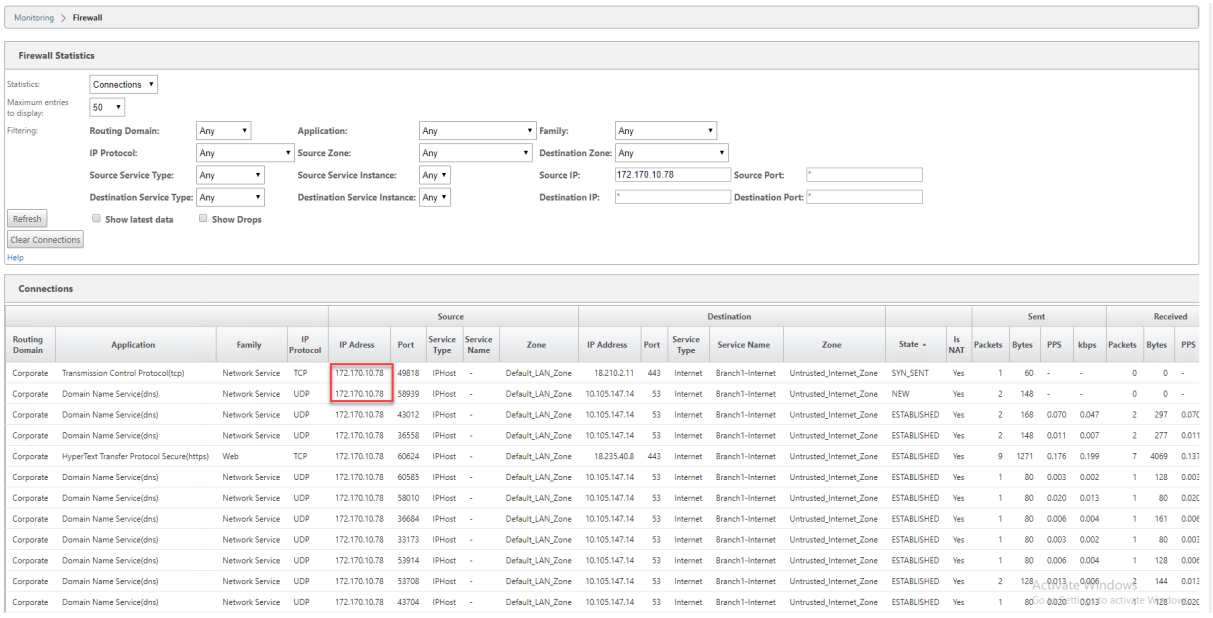
您可以将虚拟 IP 地址配置为备份管理网络。如果管理端口未使用默认 Gateway 配置，则将用作管理 IP 地址。

> 注意
>
> 如果站点的 Internet 服务配置了单个路由域，则默认情况下会选择启用身份的受信任接口作为备份管理网络。

监视备份管理

在前面的示例中，我们选择了 172.170.10.78 虚拟 IP 作为备份管理网络。如果管理 IP 地址未配置默认 Gateway，则可以使用此 IP 访问 Web UI 和 SSH。

在 Web UI 中，导航到 监控 > 防火墙。您可以看到此虚拟 IP 地址作为 SSH 和 Web UI 访问的源 IP 地址。



Internet 访问权限

November 16, 2022

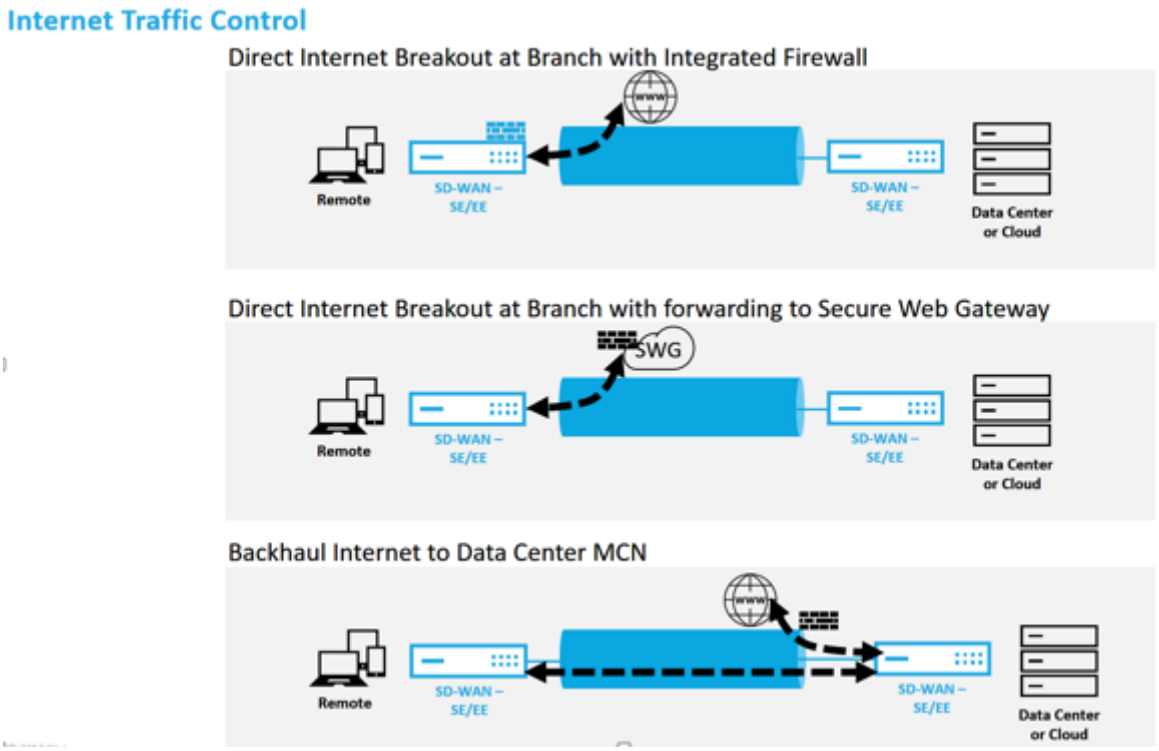
Internet 服务用于最终 用户站点与公共 Internet 上的网站之间的 流量。Internet 服务流量不被 SD-WAN 封装，且与通过虚拟路径服务传送的流量的能力不同。但是，对 SD-WAN 上的流量进行分类和考虑非常重要。标识为 Internet

服务的流量使 SD-WAN 能够通过根据管理员建立的配置限制 Internet 流量相对于跨虚拟路径和 Intranet 流量传输的流量的速率来主动管理 WAN 链路带宽。除了带宽配置功能之外，SD-WAN 还增加了 使用多个 Internet WAN 链接或可选的在主要或辅助配置中利用 Internet WAN 链路对通过 Internet Service 传输的流量进行负载平衡的功能。

可以在以下部署模式下配置使用 SD-WAN 设备上 Internet 服务的 Internet 流量控制：

- 带集成防火墙的分支机构直接 Internet 突破
- 在分支机构转发到 Secure Web Gateway 时直接进行 Internet 突围
- 回程 Internet 到数据中心 MCN

有关如何通过 Citrix SD-WAN Orchestrator 服务配置 Internet 服务的信息，请参阅 Internet 服务。



带集成防火墙的分支机构直接 **Internet** 突破

Internet 服务可以在 Citrix SD-WAN 支持的各种部署模式中使用。

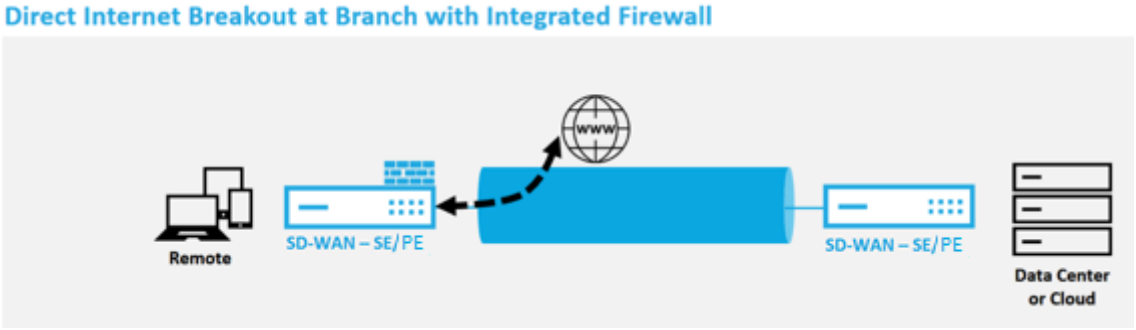
- 内联部署模式（SD-WAN 覆盖）

Citrix SD-WAN 可以作为覆盖解决方案部署在任何网络中。作为叠加解决方案，SD-WAN 通常部署在现有边缘路由器和/或防火墙后面。如果 SD-WAN 部署在网络防火墙后面，则可以将接口配置为受信任，并且 Internet 流量可以作为 Internet Gateway 传输到防火墙。

- 边缘或网关模式

Citrix SD-WAN 可以部署为边缘设备，替换现有的边缘路由器和/或防火墙设备。板载防火墙功能允许 SD-WAN 保护网络免受直接 Internet 连接。在此模式下，连接到公用 Internet 链接的接口配置为不受信任，强制启用加密，并启用防火墙和动态 NAT 功能以保护网络。

有关如何通过 Citrix SD-WAN Orchestrator 服务配置 Internet 服务的信息，请参阅 Internet 服务。



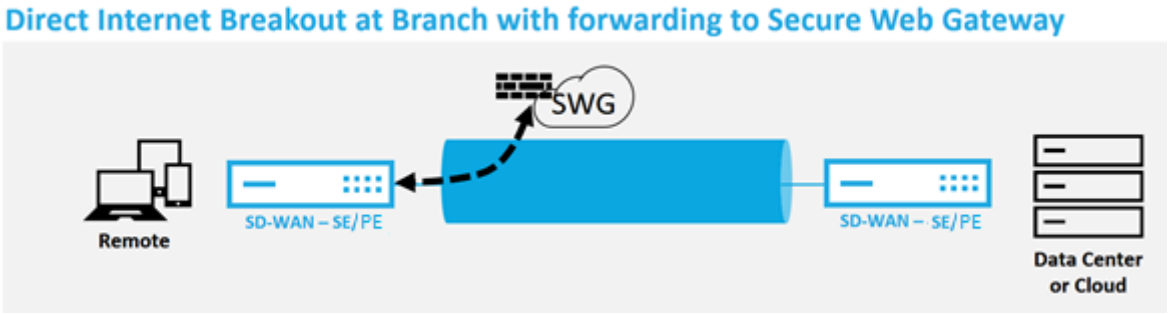
通过 **Secure Web Gateway** 直接访问 **Internet**

为了保护流量和执行策略，企业通常使用 MPLS 链接来回程分支流量到企业数据中心。数据中心应用安全策略，筛选通过安全设备检测恶意软件的流量，并通过 ISP 路由流量。这种通过私有 MPLS 链路进行后拖是昂贵的。它还会导致显著延迟，从而在分支站点造成较差的用户体验。还存在用户绕过您的安全控制的风险。

另一种替代方法是在分支机构添加安全设备。但是，成本和复杂性会随着您安装多个设备以在站点中保持一致的策略而增加。最重要的是，如果您有许多分支机构，成本管理变得不切实际。

一种替代方法是在不增加成本、复杂性或延迟的情况下强制实施安全性，那就是使用 Citrix SD-WAN 将所有分支机构 Internet 流量路由到 Secure Web Gateway 服务。第三方 Secure Web Gateway 服务使所有连接的网络都能使用精细的集中式安全策略创建。无论用户位于数据中心还是分支站点，都会一致地应用这些策略。由于 Secure Web Gateway 解决方案是基于云的，因此您不必向网络添加更昂贵的安全设备。

有关如何通过 Citrix SD-WAN Orchestrator 服务配置 Internet 服务的信息，请参阅 Internet 服务。



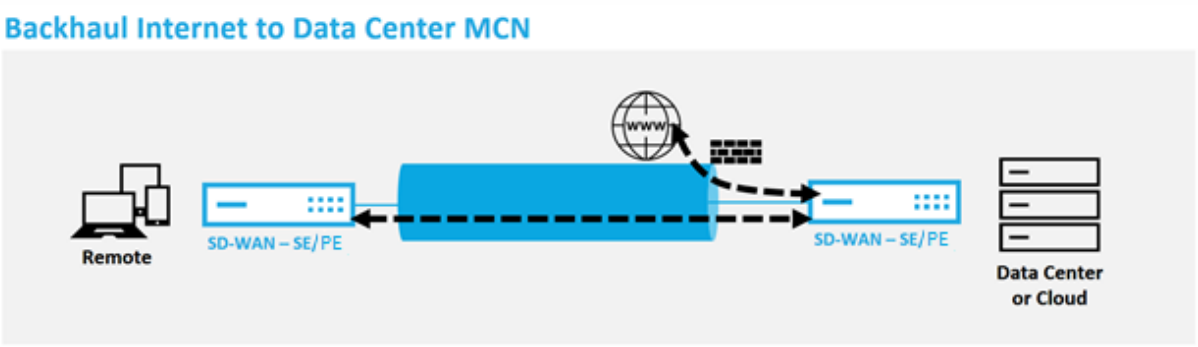
Citrix SD-WAN 支持以下第三方 Secure Web Gateway 解决方案：

- Zscaler
- Forcepoint
- Palo Alto
- Citrix Secure Internet Access

回程 **Internet**

Citrix SD-WAN 解决方案可以将 Internet 流量回传到 MCN 站点或其他分支站点。回传指示发往 Internet 的流量是通过另一个可以访问 Internet 的预定义站点发回的。它对于由于安全考虑或底层网络拓扑而不允许直接访问 Internet 的网络非常有用。一个例子是缺乏外部防火墙的远程站点，其中板载 SD-WAN 防火墙不符合该站点的安全要求。对于某些环境，通过数据中心强化的 DMZ 回传所有远程站点 Internet 流量可能是向远程办公室用户提供 Internet 访问的最佳方法。然而，这种方法确实有其局限性，因为需要注意以下和底层 WAN 链接大小适当。

- Internet 流量的回传增加了 Internet 连接的延迟，并且根据数据中心分支站点的距离而变化。
- Internet 流量的回传会消耗虚拟路径上的带宽，并在 WAN 链路的大小中被考虑。
- Internet 流量的回程可能会超额订阅数据中心的 Internet WAN 链接。

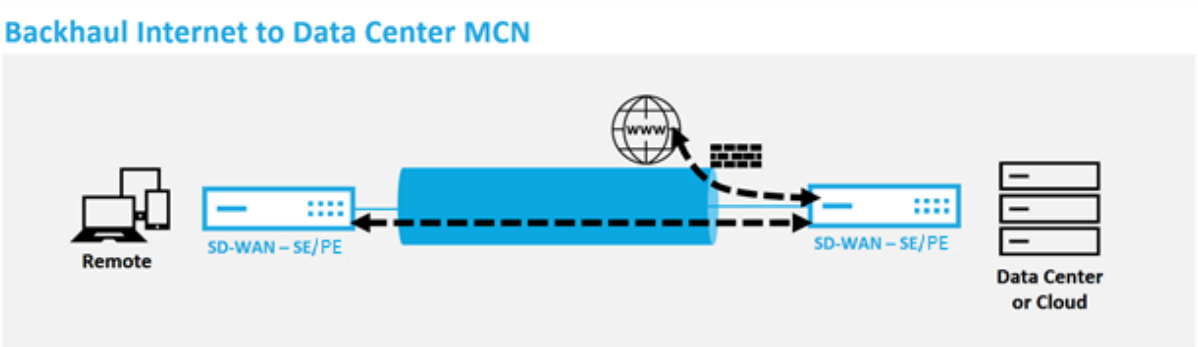


所有 Citrix SD-WAN 设备最多可以将八个不同的 Internet WAN 链接终止到单个设备中。聚合 WAN 链路的许可吞吐能力在 Citrix SD-WAN 数据手册中按相应设备列出。

发夹模式

借助发夹部署，当本地 Internet 服务不可用或流量较慢时，您可以通过回传或发夹实现使用远程中心站点进行 Internet 访问。您可以通过允许从特定站点进行备份，在客户端站点之间应用高带宽路由。

从非 WAN 转发站点部署到 WAN 转发站点的目的是提供更高效的部署流程和更简化的技术实施。您可以在需要时使用远程中心站点进行 Internet 访问，并可以通过虚拟路径将流路由到 SD-WAN 网络。



例如，考虑具有多个 SD-WAN 站点的管理员，A 和 B 站点 A 具有较差的 Internet 服务。站点 B 具有可用的 Internet 服务，您只想从站点 A 回传流量到站点 B。您可以尝试实现这一目标，而不需要战略性加权路由成本和传播到不应接收流量的站点的复杂性。

此外，路由表不会在头发夹部署中的所有站点之间共享。例如，如果通过站点 C 在站点 A 和站点 B 之间通过站点 C 划分流量，则只有站点 C 会知道站点 A 和 B 的路径。站点 A 和站点 B 不共享彼此的路由表，不像 WAN 到 WAN 转发。

当站点 A 和站点 B 之间通过站点 C 进行通信时，需要在站点 A 和站点 B 中添加静态路由，指示这两个站点的下一个跃点都是中间站点 C。

Wa 到 WAN 转发和发夹部署有一定的区别，即：

1. 未配置动态虚拟路径。中间站点始终会看到两个站点之间的所有流量。
2. 尚未加入 WAN 到 WAN 转发组。

   WAN 到 WAN 转发和发夹部署是相互排斥的。在任何给定的时间点，只能对其中一个进行配置。

   Citrix SD-WAN SE 和 VPX（虚拟）设备支持发夹部署。现在，您可以配置 0.0.0.0/0 路由以在两个位置之间固定流量，而不会影响任何其他位置。如果将头发固定用于 Intranet 流量，则会将特定 Intranet 路由添加到客户端站点，以便通过虚拟路径转发到头发夹站点的 Intranet 流量。不再需要启用 WAN 转发来完成发夹功能。

托管防火墙

November 16, 2022

Citrix SD-WAN Orchestrator 服务支持以下托管防火墙：

- 帕洛阿尔托网络
- Check Point

帕洛阿尔托网络防火墙集成 **SD-WAN 1100** 平台

Citrix SD-WAN 支持在 SD-WAN 1100 平台上托管帕洛阿尔托网络下一代虚拟机 (VM) 系列防火墙. 以下是受支持的虚拟机型号：

- 虚拟机 50
- 虚拟机 100

帕洛阿尔托网络虚拟机系列防火墙作为虚拟机运行在 SD-WAN 1100 平台上。防火墙虚拟机集成在 **Virtual Wire** 模式下，连接了两个数据虚拟接口。通过在 SD-WAN 上配置策略，可以将所需的流量重定向到防火墙虚拟机。

有关如何通过 SD-WAN Orchestrator 服务置备防火墙虚拟机的信息，请参阅 托管防火墙。

优势

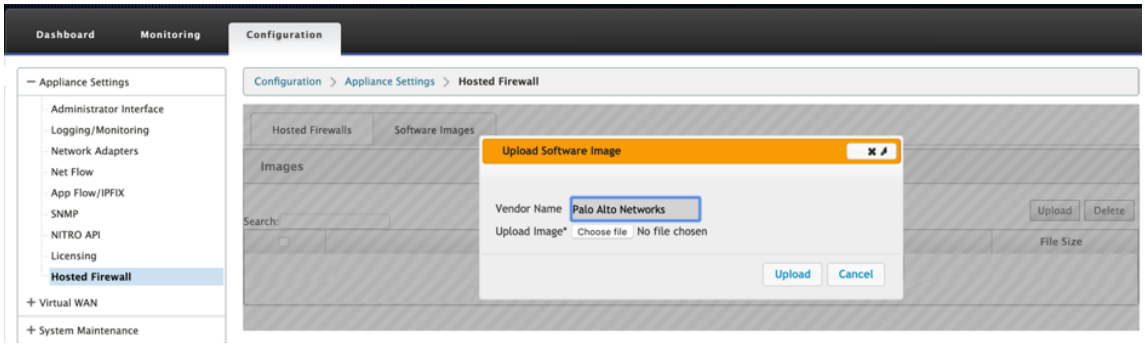
下面是在 SD-WAN 1100 平台上集成 Palo Alto 网络的主要目标或优势：

- 分支设备整合：同时执行 SD-WAN 和高级安全性的单个设备。
- 通过本地 NGFW（下一代防火墙）保护分支机构安全性，可保护局域网到局域网、局域网到 Internet 和 Internet 到局域网的流量。

通过 **SD-WAN** 设备 **GUI** 进行防火墙虚拟机 **Provisioning**

在 SD-WAN 平台上，预配和启动托管虚拟机。执行以下步骤进行 Provisioning：

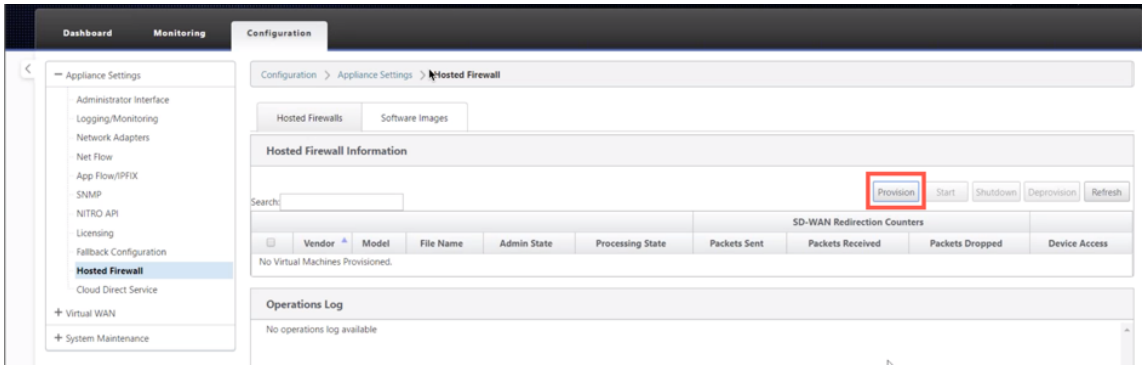
1. 从 Citrix SD-WAN GUI 中，导航到 配置 **>** 展开 设备设置 **>** 选择 托管防火墙。
2. 上传软件映像：
   - 选择 软件映像 选项卡。选择供应商名称作为 **Palo Alto** 网络。
   - 选择软件映像文件。
   - 单击上载。



> 注意
>
> 最多可以上传两个软件映像。上载 Palo Alto 网络虚拟机映像可能需要更长的时间，具体取决于带宽可用性。

   您可以看到一个状态栏来跟踪上载过程。图像成功上载后，文件详细信息会反映。无法删除用于预配的映像。不要执行任何操作或返回到任何其他页面，直到图像文件显示 100% 上载。

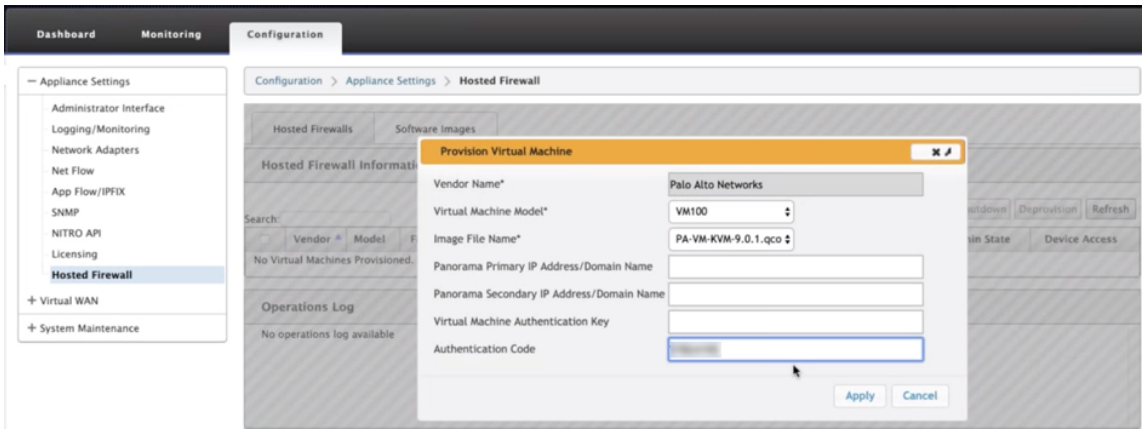
3. 对于预配，请选择 托管防火墙 选项卡，然后单击 置 备按钮



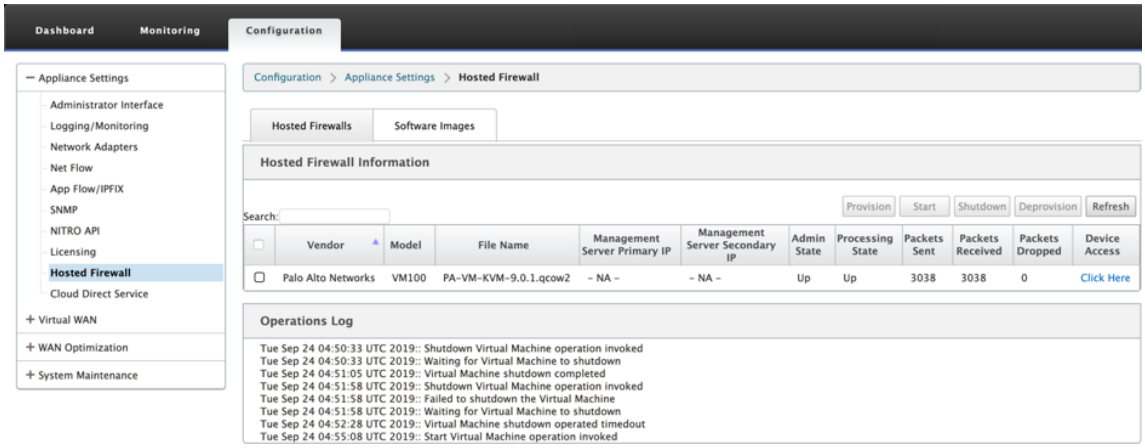
4. 请提供以下详细信息以供 Provisioning。

   - 供应商名称：选择供应商作为 **Palo Alto** 网络。
   - 虚拟机型号：从列表中选择虚拟机型号。
   - 映像文件名：选择图像文件。
   - **Panorama** 主 **IP** 地址/域名：提供 Panorama 主 IP 地址或完全限定域名（可选）。
   - **Panorama** 辅助 **IP** 地址/域名：提供 Panorama 辅助 IP 地址或完全限定域名（可选）。
   - 虚拟机身份验证密钥：提供虚拟机身份验证密钥（可选）。

     需要虚拟机身份验证密钥才能将帕洛阿尔托网络虚拟机自动注册到 Panorama。
   - 身份验证代码：输入身份验证代码（虚拟机许可证代码）（可选）。
   - 单击应用。



5. 单击 刷新 以获取最新状态。Palo Alto 网络虚拟机完全启动后，它将反映在 SD-WAN UI 上与操作日志详细信息。



- 管理状态：指示虚拟机是启动还是关闭。
- 处理状态：虚拟机的数据路径处理状态。
- 已发送的数据包：从 SD-WAN 发送到安全虚拟机的数据包。
- 收到的数据包：SD-WAN 从安全虚拟机接收的数据包。
- 丢弃的数据包：SD-WAN 丢弃的数据包（例如，当安全虚拟机关闭时）。
- 设备访问：单击链接以获取对安全虚拟机的 GUI 访问权限。

您可以根据需要 启动、关闭 和 取消 置备虚拟机。使用“单击此处”选项访问 Palo Alto Networks 虚拟机 GUI 或将管理 IP 与 4100 端口（管理 IP：4100）一起使用。

> 注意
>
> 始终使用隐身模式访问 Palo Alto 网络 GUI。

SD-WAN 1100 平台上的 Check Point 防火墙集成

Citrix SD-WAN 支持在 SD-WAN 1100 平台上托管 检查点量子边缘。

Check Point Quantum Edg e 在 SD-WAN 1100 SE 平台上作为虚拟机运行。防火墙虚拟机以 Bridge 模式集成，有两个数据虚拟接口连接到其上。通过在 SD-WAN 上配置策略，可以将所需的流量重定向到防火墙虚拟机。

有关如何通过 SD-WAN Orchestrator 服务置备防火墙虚拟机的信息，请参阅 托管防火墙。

> 注意
>
> 从 Citrix SD-WAN 11.3.1 开始，支持检查点虚拟机版本 80.20 及更高版本，以便在新站点上配置虚拟机。

优势

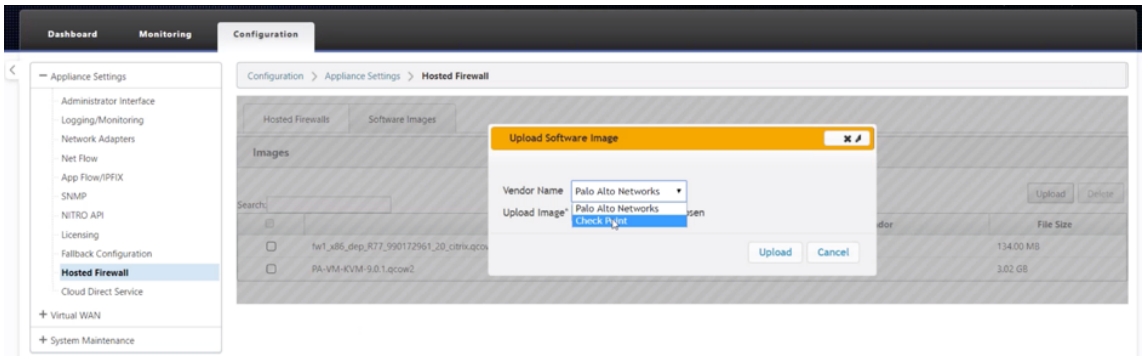
以下是在 SD-WAN 1100 平台上集成检查点的主要目标或优点：

- 分支设备整合：同时执行 SD-WAN 和高级安全性的单个设备
- 分支机构通过内部部署 NGFW（下一代防火墙）保护局域网到局域网、局域网到 Internet 和 Internet 到局域网的流量

通过 **SD-WAN** 设备 **GUI** 进行防火墙虚拟机 **Provisioning**

在 SD-WAN 平台上，预配和启动托管虚拟机。执行以下步骤进行 Provisioning：

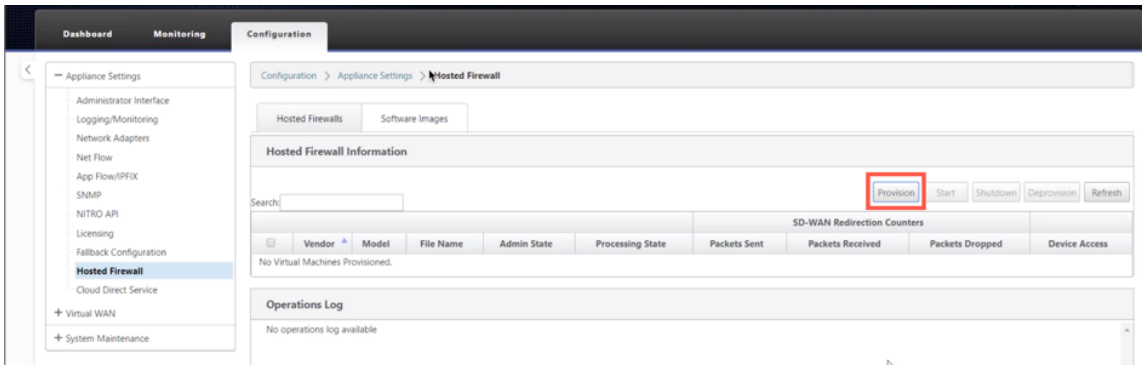
1. 从 Citrix SD-WAN GUI 中，导航到 配置 **>** 设 备设置 选择 托管防火墙。
2. 上传软件映像：
   - 选择 软件映像 选项卡。选择 供应商名称 作为检查点。
   - 选择软件映像文件。
   - 单击上载。



> 注意
>
> 最多可以上传两张图片。上传检查点虚拟机映像可能需要更长的时间，具体取决于带宽可用性。

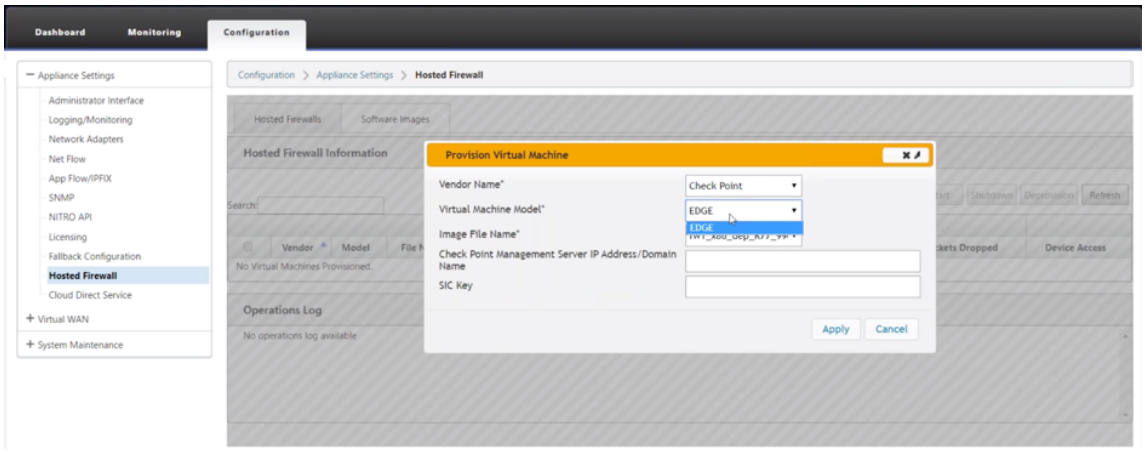
您可以看到一个状态栏来跟踪上载过程。图像成功上载后，文件详细信息会反映。无法删除用于预配的映像。不要执行任何操作或返回到任何其他页面，直到图像文件显示 100% 上载。

3. 对于预配，请选择 托管防火墙 选项卡 > 单击 置 备按钮

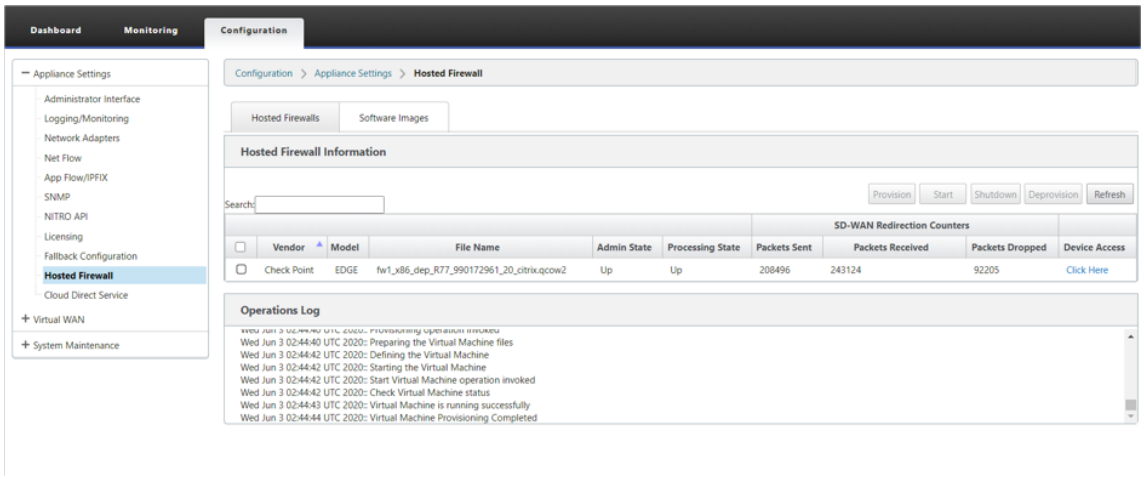


4. 请提供以下详细信息以供 Provisioning。
   - 供应商名称：选择 供应商名称 作为检查点。
   - 虚拟机模型：虚拟机模型自动填充为 **Edge**。
   - 映像文件名：图像文件名是自动填充的。
   - 检查点管理服务器 **IP** 地址/域：提供检查点管理服务器 IP 地址/域。

- **SIC** 密钥：提供 SIC 密钥（可选）。SIC 在 检查点 组件之间创建可信连接。单击应用。



5. 单击 刷新 以获取最新状态。检查点虚拟机完全启动后，它将在 SD-WAN UI 上反映操作日志详细信息。

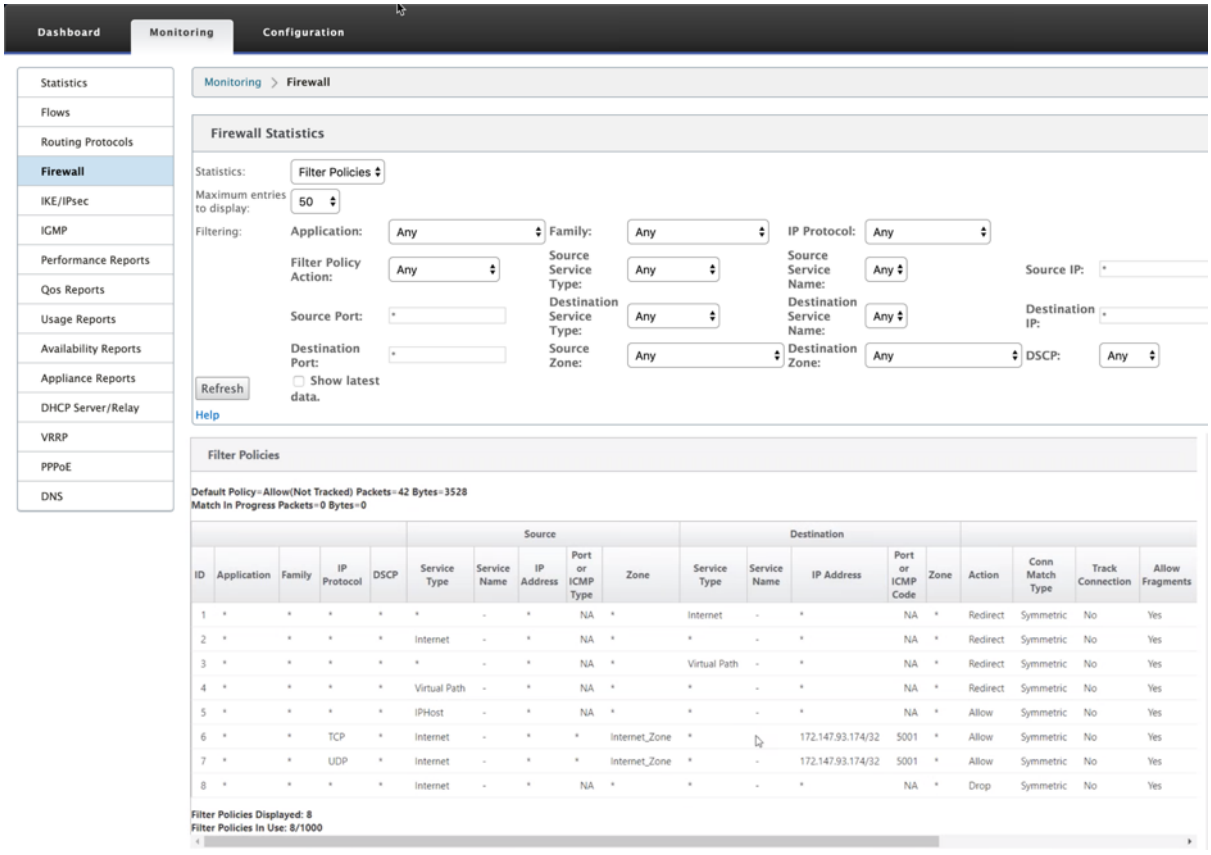


- 管理状态：指示虚拟机是启动还是关闭。
- 处理状态：虚拟机的数据路径处理状态。
- 已发送的数据包：从 SD-WAN 发送到安全虚拟机的数据包。
- 收到的数据包：SD-WAN 从安全虚拟机接收的数据包。
- 丢弃的数据包：SD-WAN 丢弃的数据包（例如，当安全虚拟机关闭时）。
- 设备访问：单击链接以获取对安全虚拟机的 GUI 访问权限。

您可以根据需要 启动、关闭 和 取消 置备虚拟机。使用 单击此处 选项访问检查点虚拟机 GUI 或将管理 IP 与 4100 端口（管理 IP：4100）一起使用。

> 注意
>
> 始终使用隐身模式访问检查点 GUI。

当所有网络配置都处于启动和运行模式时，您可以在“监控”>“防火墙”**>**“过滤策略”下监控连接。



链路聚合组

September 2, 2022

链路聚合组 (LAG) 功能允许您对 SD-WAN 设备上的两个或多个端口进行分组，以便作为单个端口一起工作。这可确保提高可用性、链路冗余性和增强性能。

之前，LAG 中只支持活动备份模式。从 Citrix SD-WAN 11.3 版本开始，支持基于 802.3AD 链路聚合控制协议 (LACP) 协议的协商。LACP 是标准协议，为 LAG 提供了更多功能。

在活动备份模式下，任何时候只有一个端口处于活动状态，其他端口处于备份模式。活动和备份支持依赖于数据平面开发工具包 (DPDK) 软件包来实现 LAG 功能。

使用 LACP，您可以同时通过所有端口发送流量。作为一项好处，您可以获得更多带宽以及链路冗余机制。LACP 实现支持 主动-主动 模式。现在，使用主动备份模式，您还可以选择从 SD-WAN UI 中选择完整的 LACP 主动-主动模式。

LAG 功能仅在以下 DPDK 支持的平台上可用：

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 1100 SE

- Citrix SD-WAN 2100 SE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE
- Citrix SD-WAN 6100 SE

> 注意
>
> VPX/VPXL 平台上不支持 LAG 功能。

限制

- 您最多可以创建四个 LAG，最多可以在 Citrix SD-WAN 设备上的每个 LAG 中分组四个端口。
- LACP 实施不支持端口优先级和系统优先级选项。

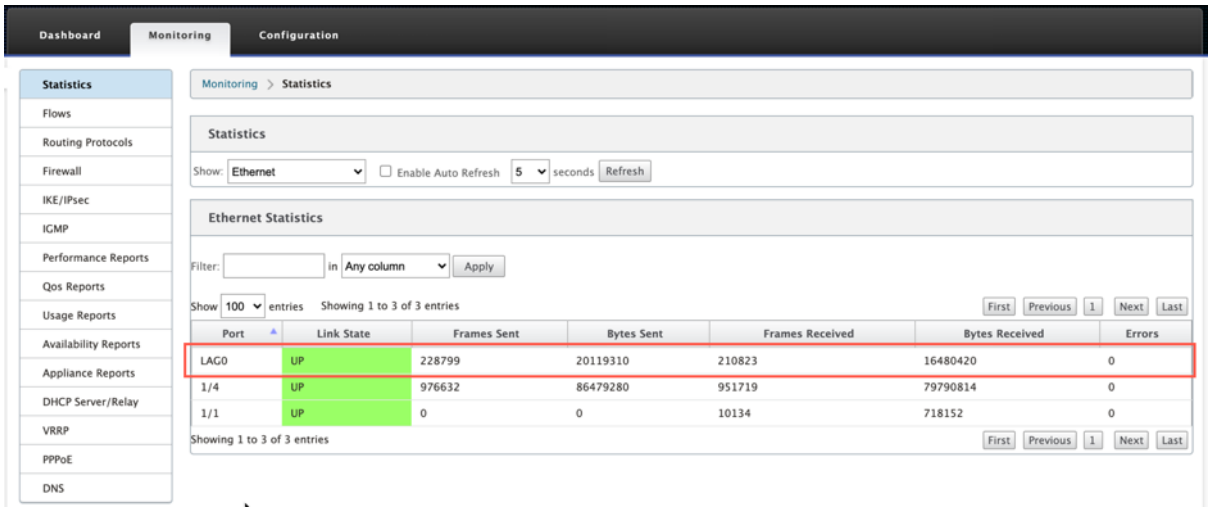
随着 11.3 版本的开始，在使用 LACP 实施的 SD-WAN 中，端口始终处于活动模式。这意味着 SD-WAN 始终可以开始谈判。

> 注意
>
> - 对于 Citrix SD-WAN 210 SE 设备，只能创建一个 LAG，其中最多分组三个端口。
> - 如果在接口组中 将 LAG 用作以太网接口，则不支持链路状态传播 (LSP) 功能。

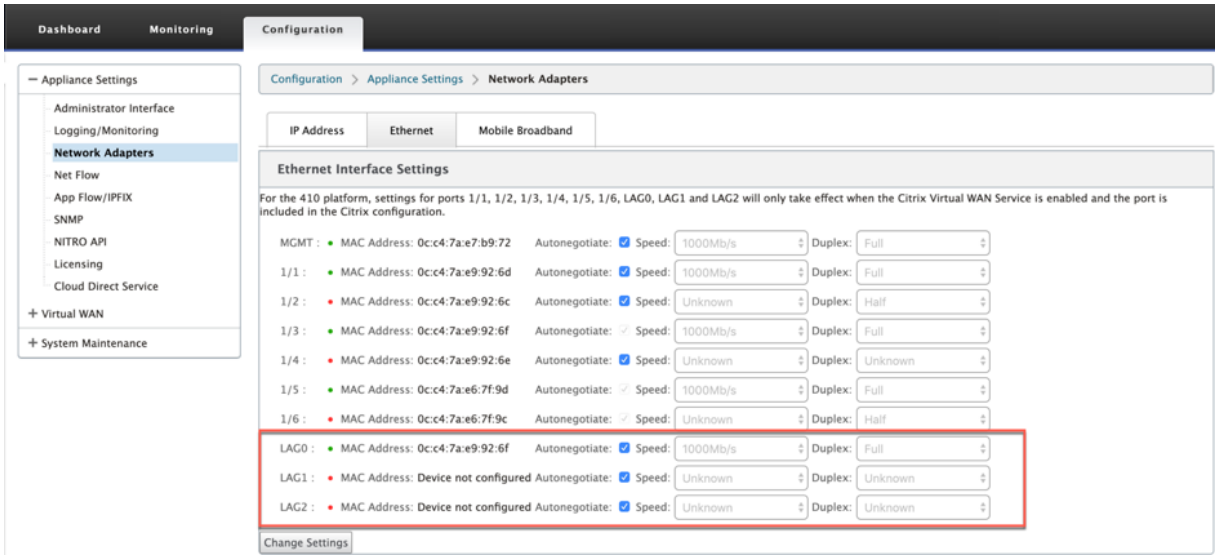
从 Citrix SD-WAN 11.5 开始，您可以通过 SD-WAN Orchestrator 服务配置链路聚合组。有关更多信息，请参阅 链路聚合组。

监视和故障排除

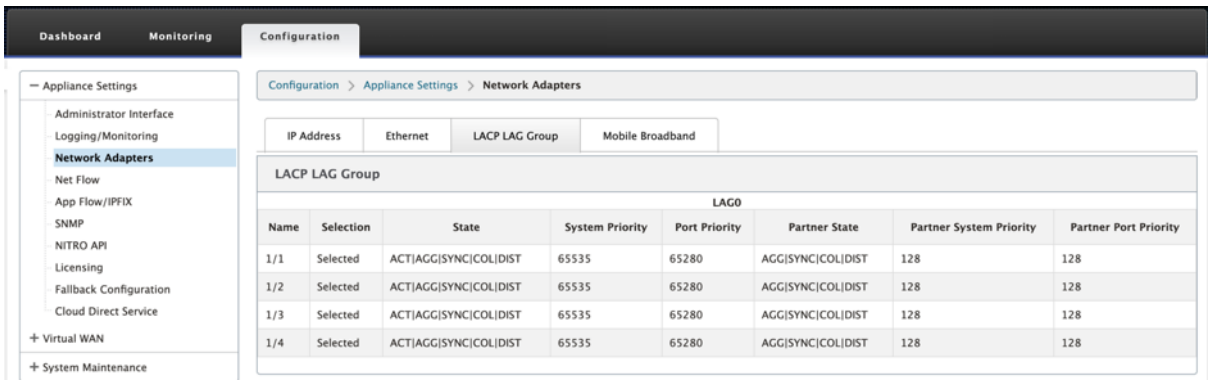
要查看统计信息或链接状态，请导航到 监视 **>** 统计信息。从 显 示下拉列表中选择 以太网。



要查看活动和备用 LAG 端口，请导航到 配置 **>** 装置设置 > 网络适配器 > 以太网。

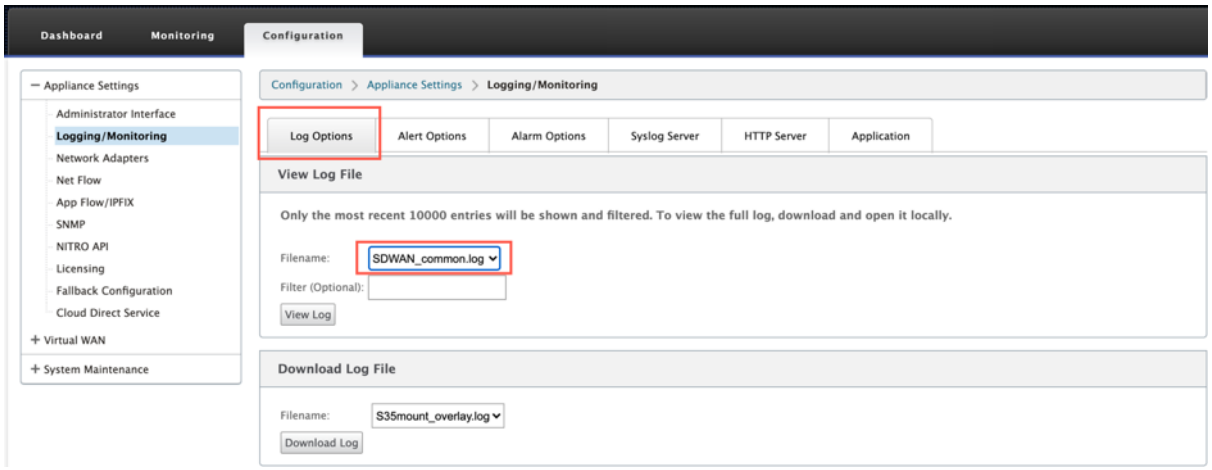


选择 L **ACP LAG Grou** p 选项卡以查看与 LACP LAG 组相关的各种详细信息。



> 注意
>
> 您无法更改单个成员端口的设置，对 LAG 所做的任何配置更改都会自动推送到成员端口。

您可以下载日志文件进行进一步故障排除。导航到“配置”**>**“日志/监视”，然后从“日志选项”选项卡中选 择 **SDWAN_common.log** 。



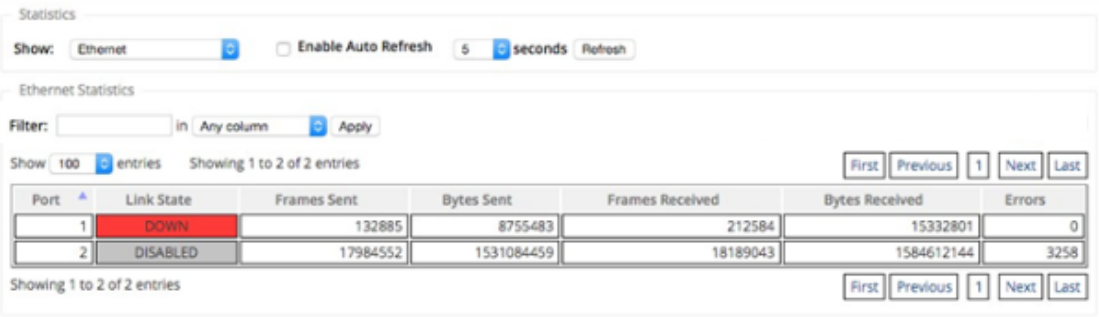
链路状态传播

September 2, 2022

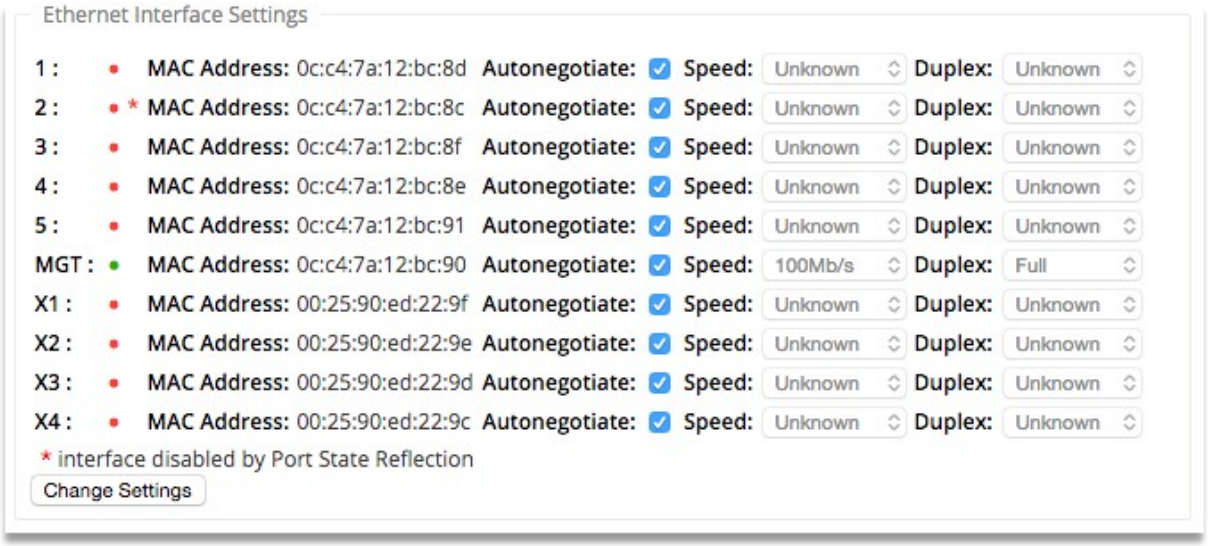
链路状态 传播 (LSP) 功能 允许 网络 管理员保持 旁路 对 的 链路 状态 同步，允许 连接 链接另一侧 的设备可在 链接处于非活动状态时 查看。当 旁路 对 的 一个 端口变为非活动状态时，将以管理方式取消激活 耦合链路。如果 您的网络 体系结构 包括 并行故障切换网络，则会 强制流量 过渡 到 该 网络。一旦中断的链接恢复，其对应的链接将自动变为活动状态。

监测链接统计

1. 在 监视器 **>** 统计信息 页面中，从显示下拉菜单中选择以太网，以查看启用了链路状态传播的旁路端口对的状态。观察局域网侧链接已关闭，然后旁路对的 WAN 侧链接在管理上被禁用。



2. 导航到 配置 **>** 装置设置 > 网络适配器 **>** 以太 网选项卡。在“以太网接口设置”列表中，管理性关闭的端口用红色星号 (*) 表示。



计量和备用 **WAN** 链接

November 16, 2022

Citrix SD-WAN 支持启用按计费链接，这些链接可以进行配置，只有在禁用所有其他可用 WAN 链接时，才会在特定 Internet WAN 链接上载输用户流量。

按计费的链接节省了根据使用情况计费的链接的带宽。使用按计费的链接，您可以将链接配置为最后手段链接，这样在所有其他未计费的链接关闭或降级之前不允许使用该链接。当有三个 WAN 链接到一个站点（即 MPLS、宽带 Internet 、4G/LTE）并且其中一个 WAN 链接是 4G/LTE 时，通常启用 设置最后措施，并且对于企业来说，除非有必要，否则可能成本太高，无法允许使用。默认情况下不启用计量，可以在任何访问类型的 WAN 链接（公共 Internet /专用 MPLS/专用 Intranet）上启用计量。如果启用了计量，您可以选择配置以下内容：

- 数据上限
- 计费周期（每周/每月）
- 开始日期
- 待机模式
- 优先级
- 活动检测信号间隔-当路径上至少有一个检测信号间隔时，设备向虚拟路径另一端的对等方发送检测信号消息的间隔

使用本地计量链接，设备的控制板会在底部显示带 计量信息的 **WAN** 链接 计量表。

根据配置的数据上限跟踪本地计费链接上的带宽使用情况。当使用量超过配置的数据上限的 50%、75% 或 90% 时，设备会生成一个事件以提醒用户，并在设备控制板顶部显示警告横幅。可以使用 1 个或 2 个计量链接形成计量路径。如果路径在两个按计量计量的链接之间形成，则在计量路径上使用的活动检测信号间隔是链接上两个已配置的活动检测信号间隔中较大的一个。

计费路径是非备用路径，始终符合用户流量的条件。当至少有一个处于“良好”状态的非按流量路径时，按流量计费的路径会减少控制通信量，并且在转发平面搜索路径中的重复数据包时避免使用。

待机模式

默认情况下，WAN 链接的待机模式处于禁用状态。要启用待机模式，必须指定待机链路在以下两种模式中的哪一种模式下运行

- 按需：满足其中一个条件时变为活动状态的备用链接。

  当虚拟路径中的可用带宽小于配置的按需带宽限制并且有足够的使用率时。足够的使用量被定义为当前可用带宽的 95% 以上 (ON_DEVIDE_USAGE_ 阈值 _PCT)，或者当前可用带宽和当前使用量之间的差值小于 250 kbps (ON_DEPD_GAP_KBPS) 两个参数都可以使用 t2_variables 更改路径已死亡或已禁用。

- 最后手段 -只有当所有非备用链接和按需备用链接处于死亡或禁用状态时才会处于活动状态的备用链接。

- 备用优先级指示备用链接处于活动状态的顺序，如果有多个备用链接：
  - 优先级 1 备用链路首先变为活动状态，优先级 3 备用链路最后变为活动状态
  - 多个备用链路可以分配相同的优先级

配预配用链路时，您可以指定备用优先级和两个检测信号间隔：

- 活动心跳间隔 -备用路径处于活动状态时使用的心跳间隔（默认为 50ms/1s/2s/3s/4s/5s/6s/7s/8S/9S/10s）
- 待机心跳间隔 -备用路径处于非活动状态时使用的心跳间隔（默认为 1s/2s/3s/4s/5s/6s/7s/8s/9s/10/ 禁用）

一个备用路径由 1 个或 2 个备用链路组成。

- 按需 -在以下之间形成按需备用路径：
  - 非备用链接和按需备用链接
  - 2 个按需备用链接
- 最后手段 -最后手段的备用途径在以下之间形成：
  - 非备用链接和最后手段备用链接
  - 按需备用链接和最后手段备用链接
  - 2 个最后手段备用链接

备用路径上使用的检测信号间隔按以下方式确定：

- 如果在两条链路中至少有一条上禁用了待机检测信号，则在待机路径上禁用检测信号。
- 如果任一链路上未禁用待机检测信号，则在待机路径处于待机状态时使用两个值中较大的值。
- 如果两条链路上都配置了活动检测信号间隔，则在待机路径处于活动状态时使用两个值中较大的值。

心跳（保持活动）消息：

- 在非备用路径上，只有在至少一个检测信号间隔内没有流量（控制器或用户）时才会发送检测信号消息。检测信号间隔因路径状态而异。对于 非备用、非计量 路径：
  - 当路径状态良好时，50 毫秒
  - 当路径状态为坏时 25 毫秒

在备用路径上，使用的检测信号间隔取决于活动状态和路径状态：

- 在非活动状态下，如果未禁用检测信号，检测信号消息将按配置的待机检测信号间隔定期发送，因为其中不允许其他流量。
- 当路径状态为好时，将使用配置的活动检测信号间隔。
- 1/2 当路径状态为坏时，使用配置的活动检测信号间隔。
- 与非备用路径一样，处于活动状态时，只有在至少配置的活动检测信号间隔内没有流量（控制器或用户）时才会发送检测信号消息。

- 当路径状态为好时，将使用配置的待机检测信号间隔。
- 1/2 路径状态为坏时使用配置的待机检测信号间隔。

在处于非活动状态时，备用路径不符合用户流量的条件。在非活动备用路径上发送的唯一控制协议消息是检测信号消息，用于检测连接故障和质量指标收集。当备用路径处于活动状态时，它们有资格获得用户流量并增加时间成本。这样做是为了在转发路径选择过程中首选非备用路径（如果可用）。

已禁用心跳的备用路径的路径状态虽然处于非活动状态，但被假定为良好，并在“监视”下的“路径统计信息”表中显示为良好。当它变为活动状态时，与以死状态启动的非备用路径不同，直到它从其虚拟路径对等方听到，它将以好状态启动。如果未检测到与虚拟路径对等方的连接，则路径变为坏，然后变为死亡。如果重新建立与虚拟路径对等方的连接，则路径变为坏，然后再次变为好。

如果此备用路径变为死亡，然后变为非活动状态，则路径状态不会立即更改为（假定）好。相反，它会保持一段时间的死亡状态，以便不能立即使用。这是为了防止活动在具有假设良好死亡路径的较低优先级路径组和具有实际好路径的较高优先级路径组之间发生振荡。此处于保留状态的时间段（NO_HB_PATH_ON_HOLD_PERIOD_MS）设置为 5 分钟，并且可以通过 t2_variables 进行更改。

如果在虚拟路径上启用了路径 MTU 发现，则在路径处于待机状态时不使用备用路径的 MTU 计算虚拟路径的 MTU。当备用路径变为活动状态时，将考虑备用路径的 MTU 重新计算虚拟路径的 MTU。（虚拟路径的 MTU 是虚拟路径中所有活动路径中的最小路径 MTU）。

当备用路径在备用路径和活动之间转换时，会生成事件和日志消息。

从 SD-WAN 11.5 开始，您可以使用 Citrix SD-WAN Orchestrator 服务配置计量和备用 WAN 链接。有关更多信息，请参阅 计量和备用 WAN 链路。

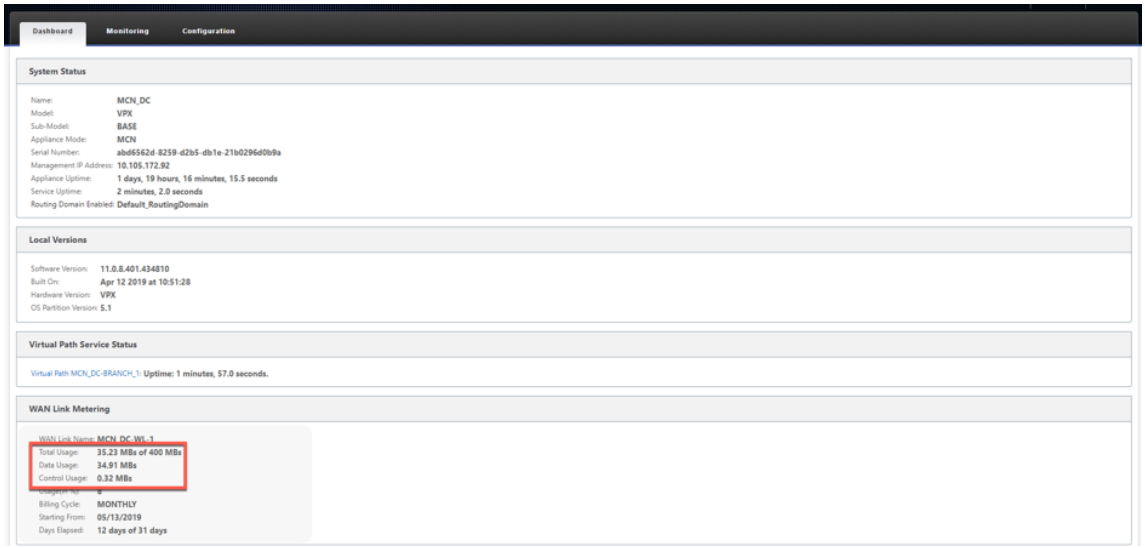
配置先决条件：

- 仪表链接可能是任何访问类型。
- 站点上的所有链接都可以在启用计量的情况下进行配置。
- 备用链接可能是公共 Internet 或专用 Intranet 访问类型。私有 MPLS 访问类型的 WAN 链接无法配置为备用链接。
- 每个站点必须至少配置一个非备用链接。每个站点最多支持 3 个备用链路。
- 可能不会在按需备用链接上配置 Internet/内联网服务。按需备用链接仅支持虚拟路径服务。
- Internet 服务可能在最后的备用链接上配置，但仅支持负载平衡模式。
- Intranet 服务可能在最后的备用链接上配置，但仅支持辅助模式，并且必须启用主回收。

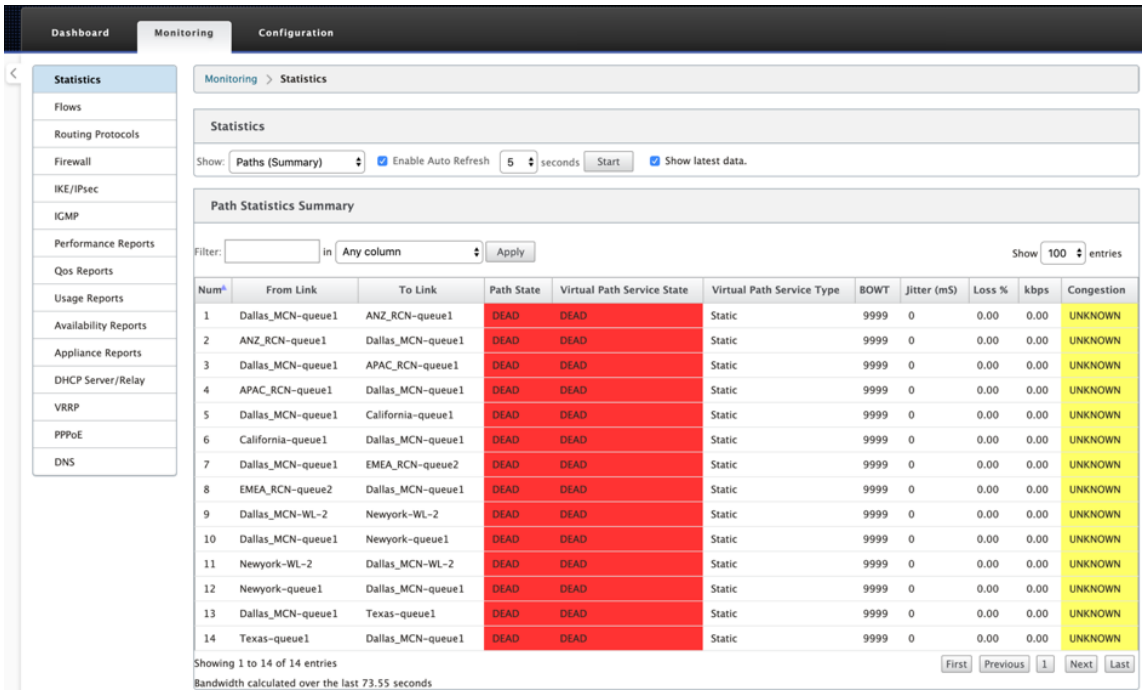
监视计量和备用 **WAN** 链接

- “控制面板”页面提供以下 **WAN Link** 计量 信息以及使用情况值：
  - **WAN** 链接名称：显示 WAN 链接名称。
  - 总使用量：显示总流量使用量（数据使用量 + 控制使用情况）。
  - 数据使用情况：按用户流量显示使用情况。

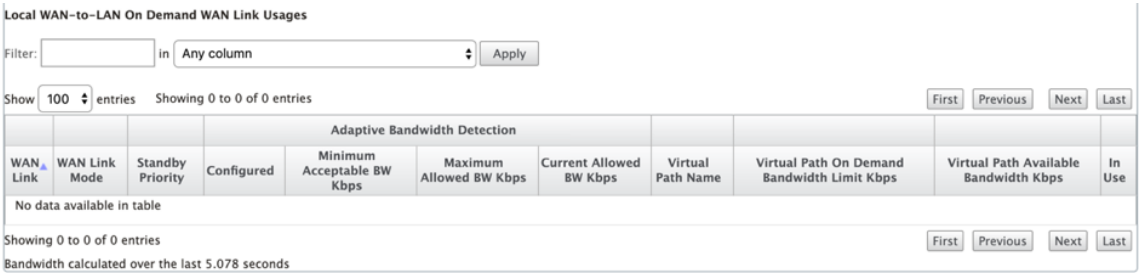
- 控制使用情况：显示控制流量的使用情况。
- 使用量（以**%** 为单位）：以百分比（总使用量/数据上限）x 100 的百分比显示已用数据上限值。
- 计费周期：计费频率（每周/每月）
- 起始日期：账单周期的起始日期
- 已用天数：已用时间（以天、小时、分钟和秒为单位）



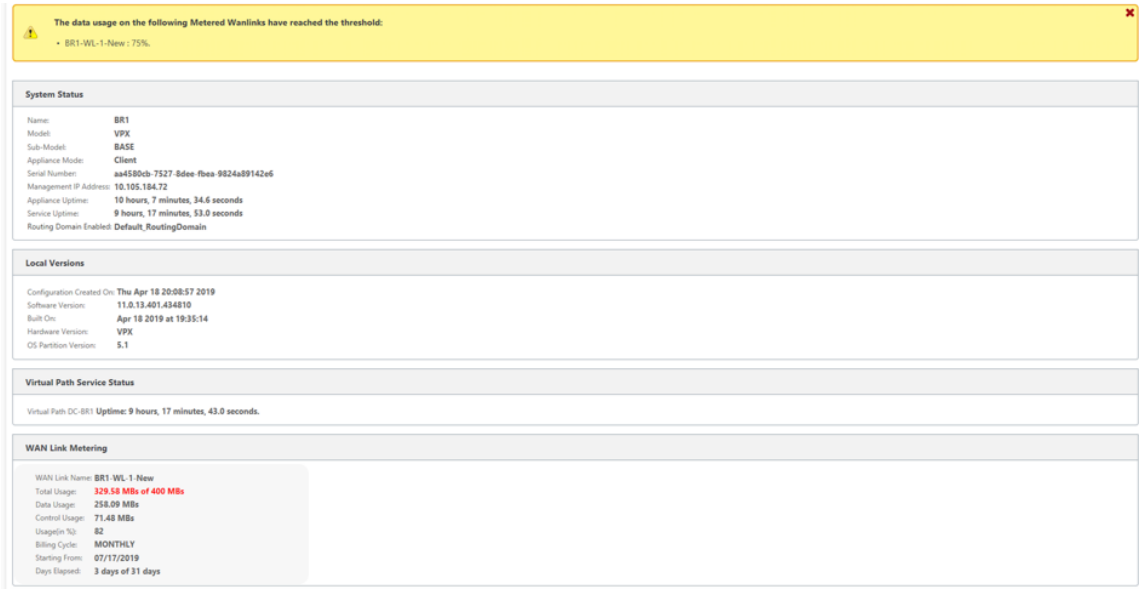
- 显示路径统计信息（监视 **>** 统计信息 **>** 路径）时，按照屏幕截图中所示标记按流量计量的链接和备用链接。



- 如果设备的虚拟路径具有本地或远程按需备用链接，则在查看 WAN 链接使用情况统计信息时，页面底部会显示一个额外的表格，显示按需带宽（监视 **>** 统计信息 **> WAN** 链接使用情况）。

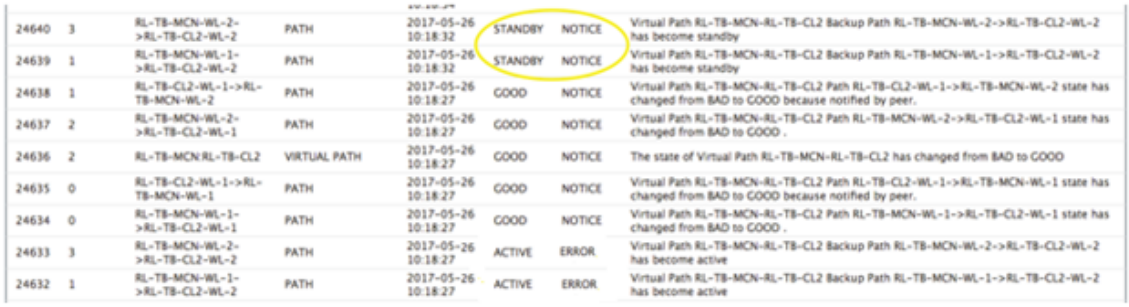


- 当按计费链接的使用率超过配置的数据上限的 50% 时，控制板顶部会显示一个警告横幅。此外，如果使用量超过配置数据上限的 75%，则会突出显示仪表板 底部的数字计量信息。

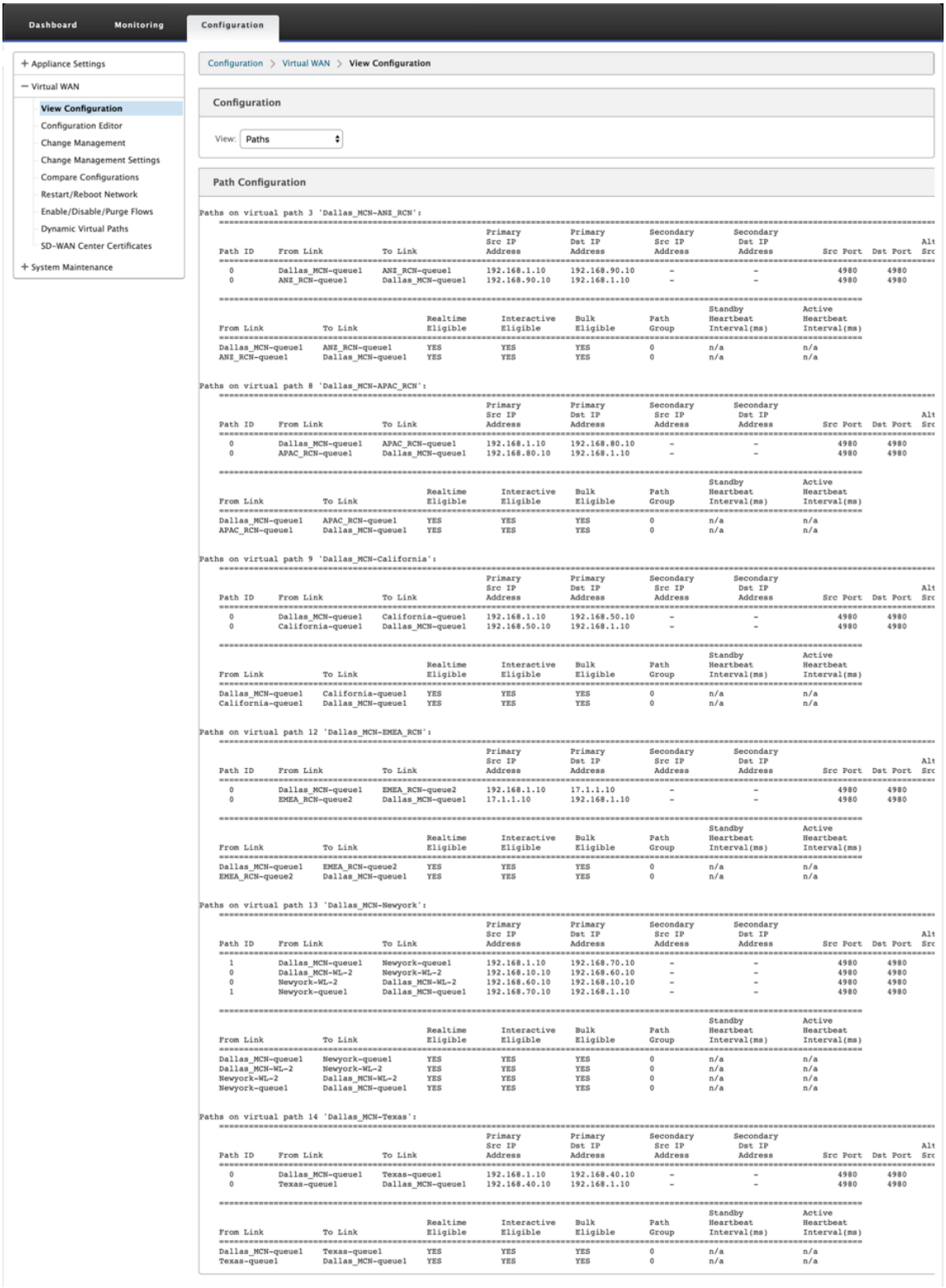


当使用量超过配置数据上限的 50%、75% 和 90% 时，也会在设备上生成 WAN 链路使用情况事件。

1. 当备用路径在待机状态和活动状态之间转换时，设备将生成一个事件。



2. 可以在 配置 **>** 虚拟 WAN**>** 查看配置 **>** 路径 中查看为每个路径配置 的活动和待机检测信号间隔。



Office 365 优化

November 16, 2022

Office 365 优化 功能遵循 微软 Office 365 网络连接原则，以优化 Office 365。Office 365 通过位于全球的多个服务终端节点（前门）作为服务提供。为了获得 Office 365 流量的最佳用户体验，Microsoft 建议将 Office365 流量从分支机构环境直接重定向到 Internet 。避免回传到中央代理等做法。Outlook、Word 等 Office 365 流量对延迟敏感，回传流量会导致延迟更长，从而导致用户体验差。Citrix SD-WAN 允许您配置策略以将 Office 365 流量分解到 Internet。

Office 365 流量被定向到最近的 Office 365 服务终端节点，该终端节点位于全球微软 Office 365 基础结构的边缘。一旦流量到达前门，它就会通过 Microsoft 的网络并到达实际目的地。随着从客户网络到 Office 365 终端节点的往返时间缩短，它可以最大限度地减少延迟。

Office 365 端点

Office 365 终结点是一组网络地址和子网。Office 365 终端节点分为 “优化”、“允许” 和 “默认” 类别。Citrix SD-WAN 11.4.0 提供了优化和允许 类别的更精细的分类，从而支持选择性引导以提高对网络敏感的 Office 365 流量的性能。将网络敏感流量定向到云中的 SD-WAN（Cloud Direct 或 Azure 上的 SD-WAN VPX），或者从家中 SD-WAN 设备到附近位置的具有更可靠 Internet 连接的 SD-WAN，与简单地将流量引导至最近的位置相比，可实现 QoS 和卓越的连接恢复能力 Office 365 前门，代价是延迟的增加。带 QoS 的书籍 SD-WAN 解决方案可减少 VoIP 丢失和断开连接、减少抖动并提高 Microsoft Teams 的媒体质量平均意见得分：

- 优化 -这些终端节点提供与每个 Office 365 服务和功能的连接，并对可用性、性能和延迟敏感。它代表了 Office 365 带宽、连接和数据量的 75% 以上。所有优化终结点都托管在 Microsoft 数据中心中。对这些端点的服务请求必须从分支机构分离到 Internet，并且不得通过数据中心。

“优化” 类别分为以下子类别：

```
- Teams Realtime
- Exchange Online
- SharePoint Optimize
```

有关升级注意事项的信息，请参阅 升级重要注意事项。

- 允许 -这些终端节点仅提供与特定 Office 365 服务和功能的连接，对网络性能和延迟不太敏感。Office 365 带宽和连接计数的表示也较低。这些端点托管在 Microsoft 数据中心中。对这些端点的服务请求可能会从分支机构分解到 Internet，或者可能会经过数据中心。

允许 类别分为以下子类别：

```
- Teams TCP Fallback
- Exchange Mail
- SharePoint Allow
```



```
4  - Office365 Common
```

有关升级注意事项的信息，请参阅 升级重要注意事项。

> 注意
>
> 团 队实时 子类别使用 UDP 实时传输协议来管理 Microsoft Teams 流量，而 **Teams TCP** 回退 子类别使用 TCP 传输层协议。由于媒体流量对延迟敏感性很高，因此您可能希望此流量尽可能采取最直接的路径，并使用 UDP 而不是 TCP 作为传输层协议（就质量而言，交互式实时媒体的最首选传输）。尽管 UDP 是 Teams 媒体流量的首选协议，但它要求在防火墙中允许某些端口。如果不允许使用端口，Teams 流量将使用 TCP 作为回退，并且为 Teams TCP 回退启用优化可确保在这种情况下更好地交付 Teams 应用程序。有关详细信息，请参阅 Microsoft Teams 呼叫流程。

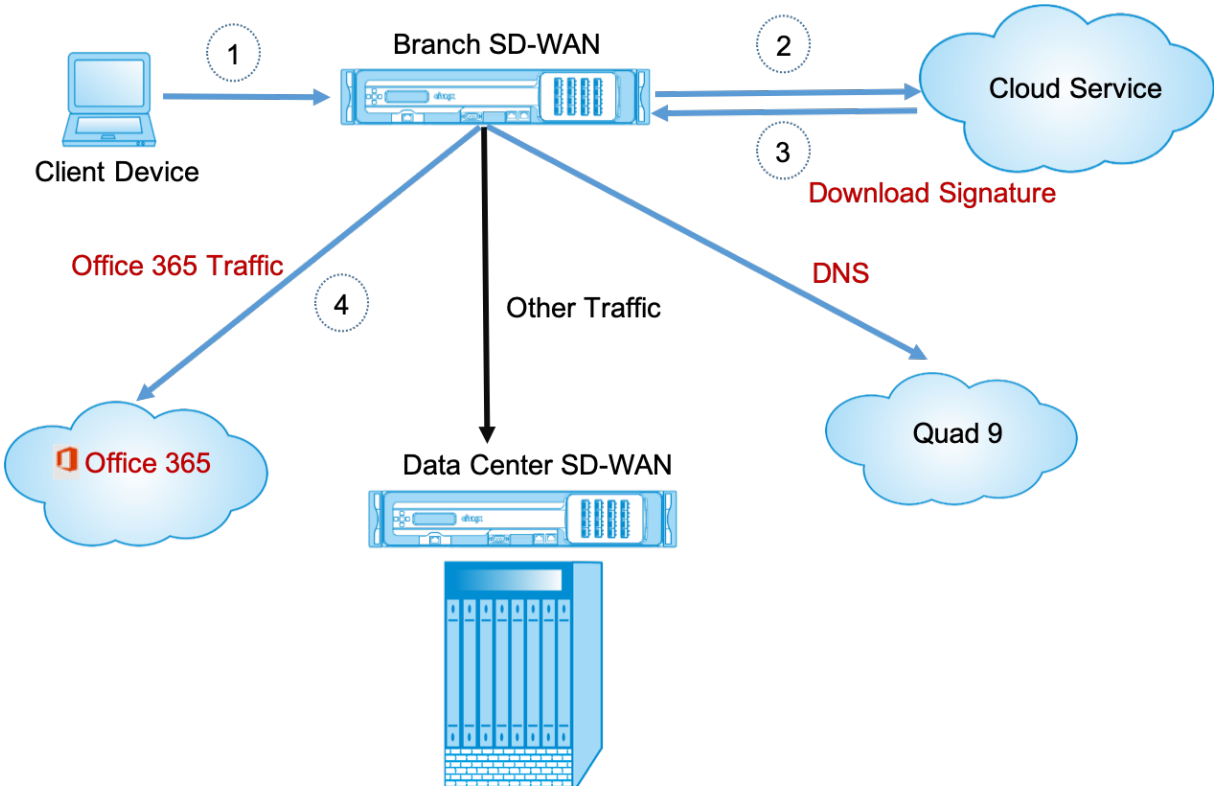
- 默认值 -这些终端节点提供不需要任何优化的 Office 365 服务，并且可以被视为正常的 Internet 流量。其中一些终端节点可能不会托管在 Microsoft 数据中心中。此类别中的流量不容易受到延迟变化的影响。因此，与 Internet 突破相比，直接脱离这种类型的流量不会导致任何性能改进。此外，此类别中的流量可能并不总是 Office 365 流量。因此，建议在网络中启用 Office 365 突破时禁用此选项。

Office 365 优化的工作原理

Microsoft 终端节点签名每天最多更新一次。设备上的代理每天轮询 Citrix 服务（SDWAN 应用程序路程.citrixnetworkapi.net），以获取最新的一组终点签名。SD-WAN 设备每天在设备打开时轮询 Citrix 服务（sdwan-app-路由.citrixnetworkapi.net）。如果有可用的新签名，设备会下载该签名并将其存储在数据库中。签名本质上是用于检测 Office 365 流量的 URL 和 IP 列表，可根据这些 URL 和 IP 配置流量指导策略。

> 注意：
>
> 除了 Office 365 默认类别之外，无论 Office 365 分组分组功能是否启用，默认情况下都会执行 Office 365 流量的第一个数据包检测和分类。

当 Office 365 应用程序的请求到达时，应用程序分类器将执行第一个数据包分类器数据库查找、识别和标记 Office 365 流量。对 Office 365 流量进行分类后，自动创建的应用程序路由和防火墙策略将生效，并将流量直接分解到 Internet。Office 365 DNS 请求将转发到特定的 DNS 服务，如 Quad9。有关详细信息，请参阅 域名系统。



签名是从云服务（SDWAN 应用程序程序.Citrixnetworkapi.net）下载的。

从 Citrix SD-WAN 11.5 开始，您可以使用 Citrix SD-WAN Orchestrator 服务配置 Office 365 分组讨论。有关详细信息，请参阅 Office 365 优化。

适用于 **Office 365** 的透明转发器

分支打破了 Office 365 开始的 DNS 请求。通过 Office 365 域的 DNS 请求必须在本地引导。如果启用 Office 365 Internet 中断，则确定内部 DNS 路由，并自动填充透明转发器列表。默认情况下，Office 365 DNS 请求转发到开源 DNS 服务四 9。四 9 DNS 服务是安全的，可扩展的，并具有多弹出的存在。如有必要，您可以更改 DNS 服务。每个启用了 Internet 服务和 Office 365 分组讨论的分支机构都会创建 Office 365 应用程序的透明转发器。

如果您正在使用其他 DNS 代理，或者如果 SD-WAN 配置为 DNS 代理，则将自动填充转发器列表的 Office 365 应用程序的转发器。

升级的重要注意事项

优化和允许类别

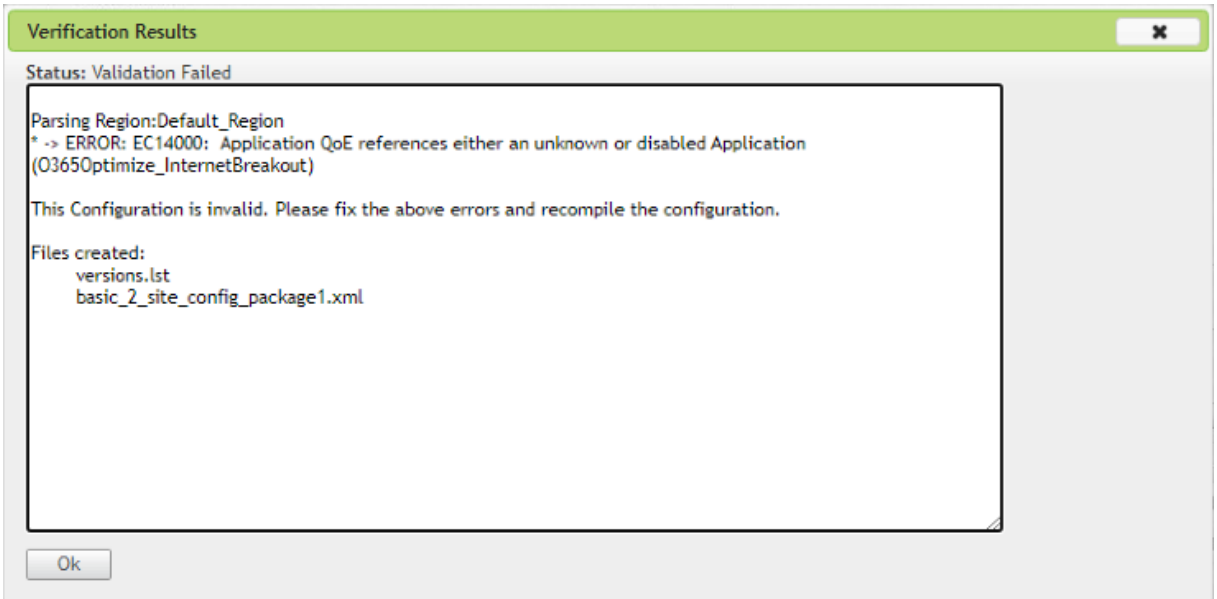
如果您已为 优化 和 允许 Office 365 类别启用了 Internet 分组策略，Citrix SD-WAN 会在 升级到 Citrix SD-WAN 11.4.0 时自动为相应子类别启用 Internet 突破策略。

降级到 Citrix SD-WAN 11.4.0 之前的软件版本时，无论是在 Citrix SD-WAN 11.4.0 版本中启用对应的子类别，都必须为优化或允许 Office 365 类别手动启用 Internet 突破。

Office 365 应用程序对象

如果您已使用 **O365Optimize_InternetBreakout** 和 **O365Allow_InternetBreakout** 自动生成的应用程序对象创建了规则/路由，请确保在升级到 Citrix SD-WAN 11.4.0 之前删除规则/路由。升级后，您可以使用相应的新应用程序对象创建规则/路由。

如果在不删除规则/路由的情况下继续 Citrix SD-WAN 11.4.0 升级，则会看到错误，因此升级失败。在以下示例中，用户配置了应用程序 QoE 配置文件，并在尝试在不删除规则/路由的情况下升级到 Citrix SD-WAN 11.4.0 时看到错误：



> 注意：
>
> 自动创建的规则/路由不需要此升级。它仅适用于您创建的规则/路由。

DNS

如果您已使用 **Office 365** 优化和 **Office 365** 允许 应用程序创建了 DNS 代理规则或 DNS 透明转发器规则，请确保在升级到 Citrix SD-WAN 11.4.0 之前删除规则。升级后，您可以使用相应的新应用程序再次创建规则。

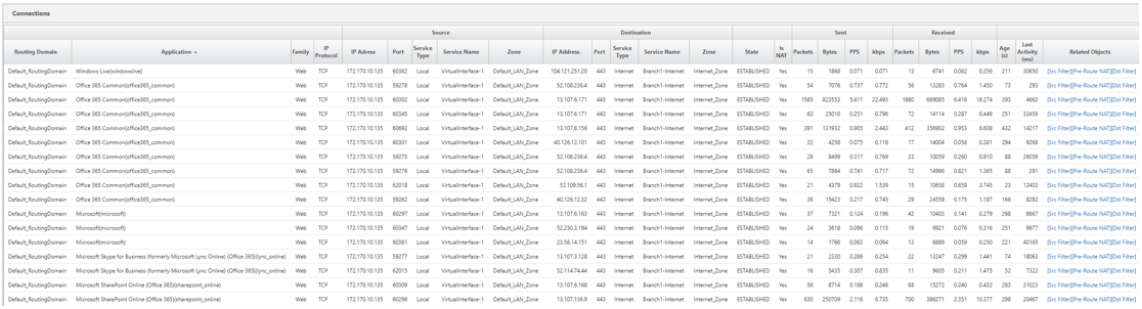
如果在不删除旧的 DNS 代理或透明转发器规则的情况下继续 Citrix SD-WAN 11.4.0 升级，则不会看到任何错误，升级也会成功。但是，DNS 代理规则和透明转发规则在 Citrix SD-WAN 11.4.0 中不生效。

> 注意：
>
> 本活动不适用于自动创建的 DNS 规则。它仅适用于您创建的 DNS 规则。

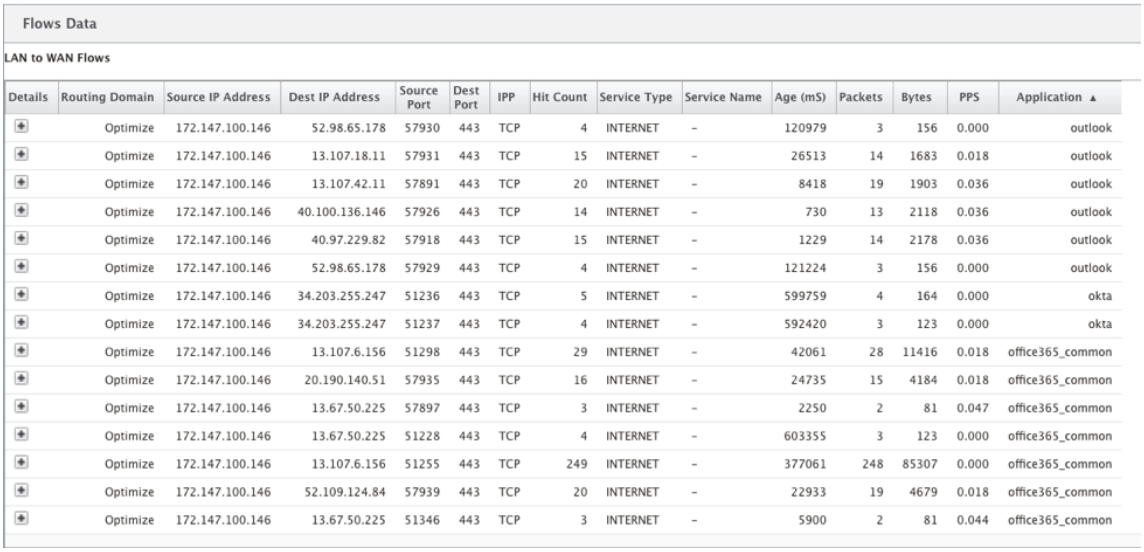
监视

您可以在以下 SD-WAN 统计报告中监视 Office 365 应用程序统计信息：

- 防火墙统计信息



- 流

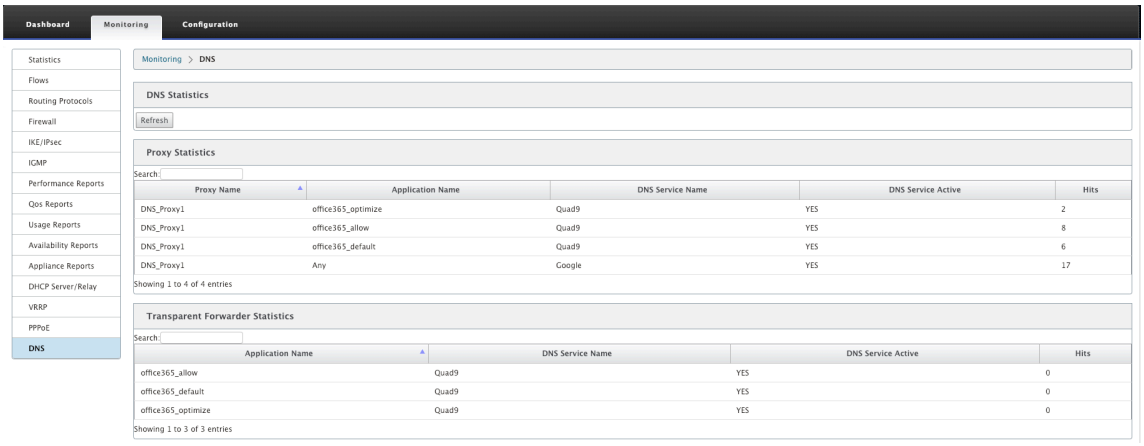


Flows Data

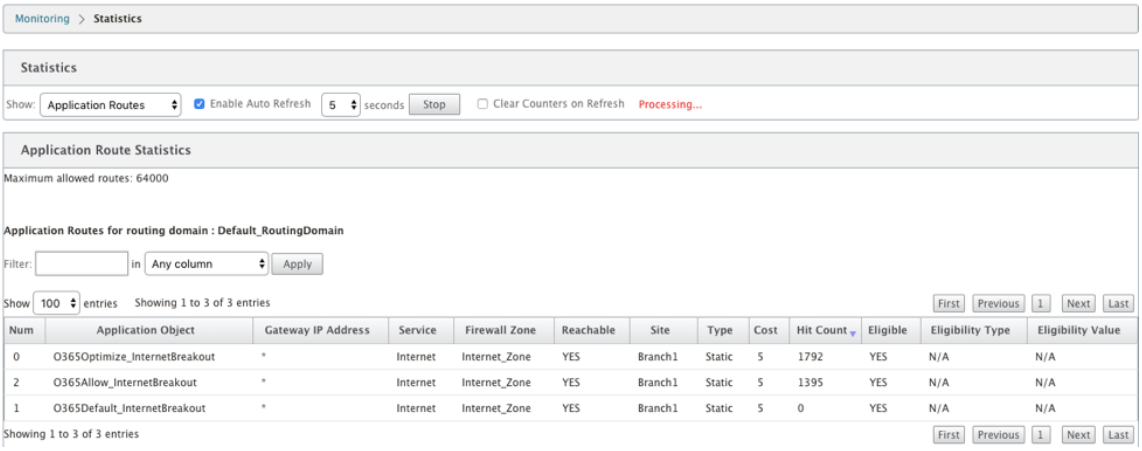
LAN to WAN Flows

Details	Routing Domain	Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Hit Count	Service Type	Service Name	Age (mS)	Packets	Bytes	PPS	Application ▲
	Optimize	172.147.100.146	52.98.65.178	57930	443	TCP	4	INTERNET	-	120979	3	156	0.000	outlook
	Optimize	172.147.100.146	13.107.18.11	57931	443	TCP	15	INTERNET	-	26513	14	1683	0.018	outlook
	Optimize	172.147.100.146	13.107.42.11	57891	443	TCP	20	INTERNET	-	8418	19	1903	0.036	outlook
	Optimize	172.147.100.146	40.100.136.146	57926	443	TCP	14	INTERNET	-	730	13	2118	0.036	outlook
	Optimize	172.147.100.146	40.97.229.82	57918	443	TCP	15	INTERNET	-	1229	14	2178	0.036	outlook
	Optimize	172.147.100.146	52.98.65.178	57929	443	TCP	4	INTERNET	-	121224	3	156	0.000	outlook
	Optimize	172.147.100.146	34.203.255.247	51236	443	TCP	5	INTERNET	-	599759	4	164	0.000	okta
	Optimize	172.147.100.146	34.203.255.247	51237	443	TCP	4	INTERNET	-	592420	3	123	0.000	okta
	Optimize	172.147.100.146	13.107.6.156	51298	443	TCP	29	INTERNET	-	42061	28	11416	0.018	office365_common
	Optimize	172.147.100.146	20.190.140.51	57935	443	TCP	16	INTERNET	-	24735	15	4184	0.018	office365_common
	Optimize	172.147.100.146	13.67.50.225	57897	443	TCP	3	INTERNET	-	2250	2	81	0.047	office365_common
	Optimize	172.147.100.146	13.67.50.225	51228	443	TCP	4	INTERNET	-	603355	3	123	0.000	office365_common
	Optimize	172.147.100.146	13.107.6.156	51255	443	TCP	249	INTERNET	-	377061	248	85307	0.000	office365_common
	Optimize	172.147.100.146	52.109.124.84	57939	443	TCP	20	INTERNET	-	22933	19	4679	0.018	office365_common
	Optimize	172.147.100.146	13.67.50.225	51346	443	TCP	3	INTERNET	-	5900	2	81	0.044	office365_common

- DNS 统计信息



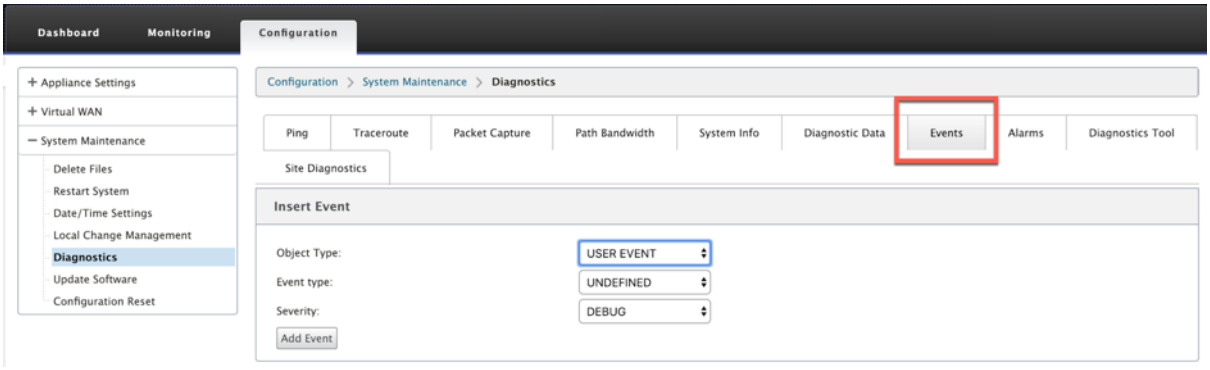
- 应用程序路由统计信息



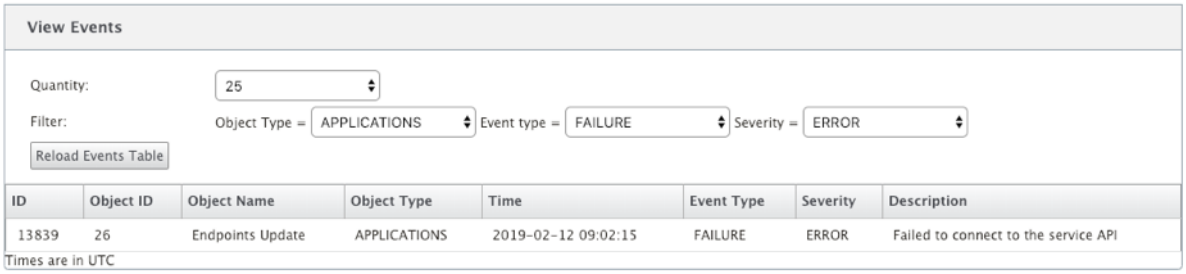
故障排除

您可以在 SD-WAN 设备的“事件”部分查看服务错误。

要检查错误，请导航到 配置 **>** 系统维护 **>** 诊断，单击 事件选项卡。

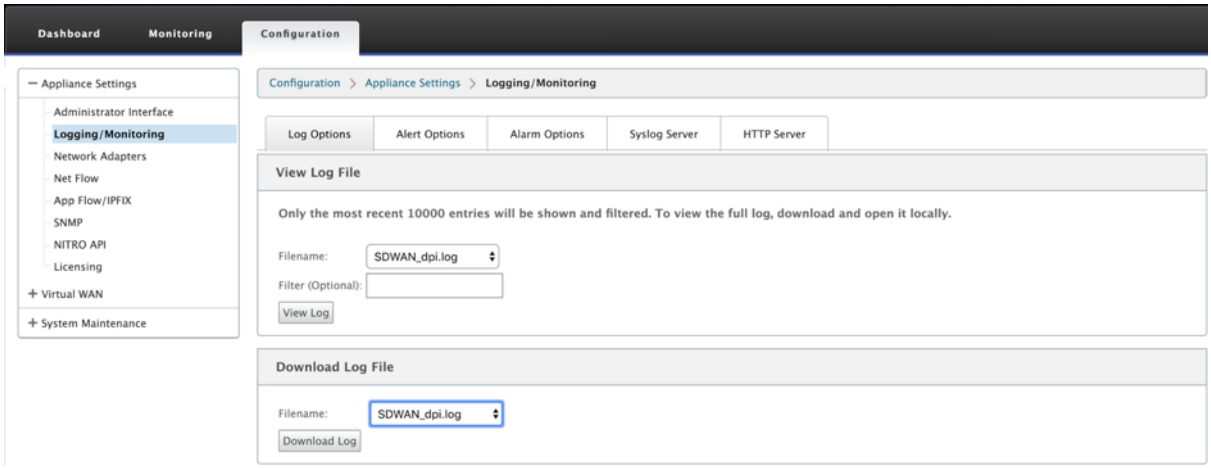


如果连接到 Citrix 服务（sdwan-app-路由.citrixnetworkapi.net）时出现问题，则错误消息将反映在“查看事件”表中。



连接错误也会记录到 **SDWAN_dpi.log** 中。要查看日志，请导航到 配置 **>** 装置设置 **>** 日志记录/监控 **>** 日志选项。从下拉列表中选择 **SDWAN_dpi.log** ，然后单击查看 日志。

您也可以下载日志文件。要下载日志文件，请从 下载日志文件 部分 下的下拉列表中选择所需的日志文件，然后单击 下载日志。



限制

- 如果配置了 Office 365 分组策略，则不会对指向已配置的 IP 地址类别的连接执行深度数据包检查。
- 自动创建的防火墙策略和应用程序路由不可编辑。
- 自动创建的防火墙策略的优先级最低且不可编辑。
- 自动创建的应用程序路由的路由成本为 5。您可以使用较低的成本路径覆盖它。

办公室 **365** 信标服务

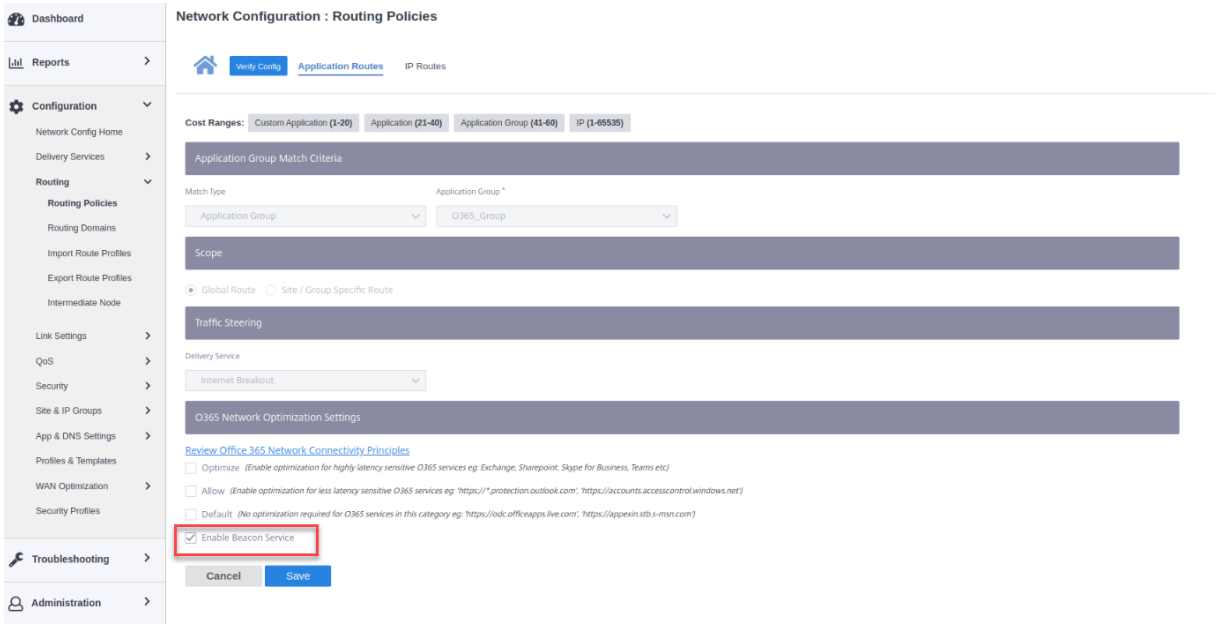
微软提供 Office 365 信标服务来衡量 Office 365 通过 WAN 链接的可达性。信标服务基本上是一个 URL-SDWAN. 测量. 办公室/apC/转接.png，它会定期进行探测。每台设备都会对每个启用 Internet 的 WAN 链路进行探测。对于每个探测器，HTTP 请求都会发送到信标服务，并且需要 HTTP 响应。HTTP 响应确认了 Office 365 服务的可用性和可访问性。

Citrix SD-WAN 不仅允许您执行信标探测，还可以确定通过每个 WAN 链接到达 Office 365 终端节点的延迟。延迟是通过 WAN 链路发送请求并从 Office 365 信标服务获取响应所花费的往返时间。这使网络管理员能够查看信标服务延迟报告，并手动选择最适合直接 Office 365 分组讨论的 Internet 链接。信标探测只能通过 Citrix SD-WAN Orchestrator 启用。默认情况下，当通过 Citrix SD-WAN Orchestrator 启用 Office 365 突破时，信标探测将在所有启用 Internet 的 WAN 链接上启用。

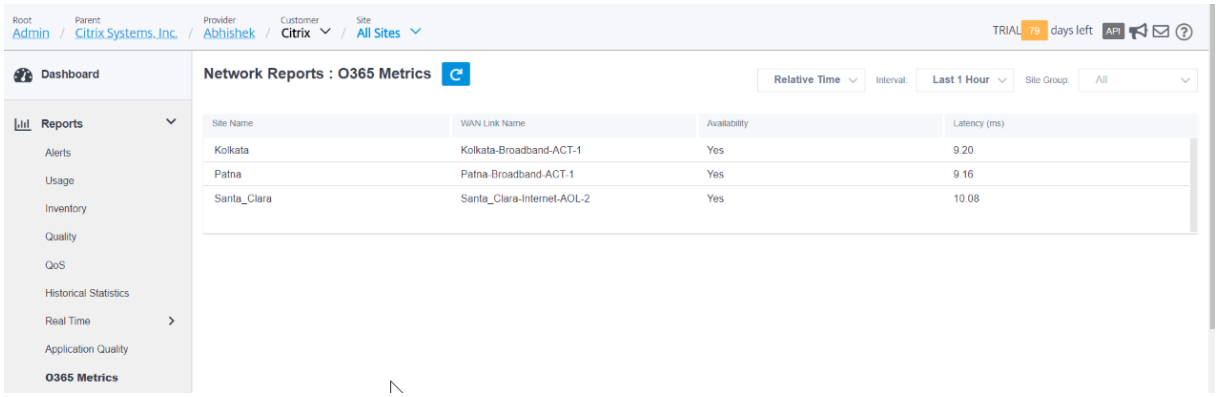
> 注意
>
> 在按流量计量的链接上未启用 Office 365 信标探测。

您可以选择禁用 Office 365 信标探测和查看 SD-WAN Orchestrator 上的延迟报告。有关详细信息，请参阅 Office 365 优化。

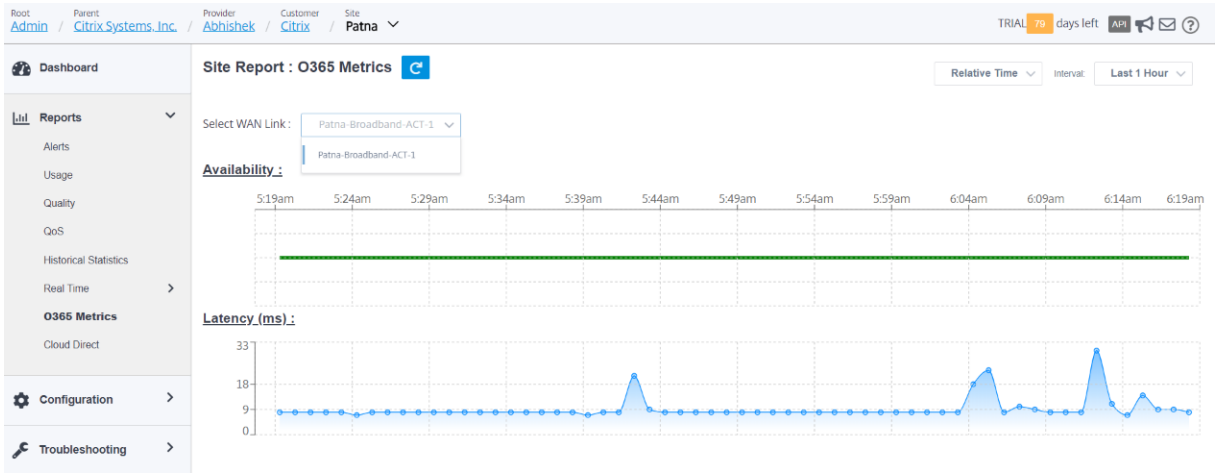
要禁用 Office 365 信标服务，请在 SD-WAN Orchestrator 中，在网络级别导航到 配置 > 路由 **>** 路由策略 >**O365** 网络优化设置，然后清除启用信标服务。



要查看信标探测可用性和延迟报告，请在 Citrix SD-WAN Orchestrator 中，在网络级别导航到 报告 > **O365** 指标。



要查看信标服务的详细站点级报告，请在 SD-WAN Orchestrator 中，在站点级导航到 报告 > **O365** 指标。



Citrix Cloud 和网关服务优化

September 2, 2022

借助 **Citrix Cloud** 和网关服务优化 功能增强功能，您可以检测和路由发往 Citrix Cloud 和网关服务的流量。您可以创建策略，直接将流量分解到 Internet，也可以通过虚拟路径的回程路由发送流量。在没有此功能的情况下，当默认路由为虚拟路径时，网关服务将发送回客户的数据中心，然后出入 Internet，增加不必要的延迟。除此之外，您现在可以了解 Citrix Gateway 服务和 Citrix Cloud 流量，并可以创建 QoS 策略以优先于虚拟路径。

Citrix SD-WAN 软件版本 11.2.1 及更高版本中默认启用 Citrix Cloud 和网关服务分组 功能。

对于 11.3.0 以下的 Citrix SD-WAN 软件版本，仅当未禁用 Citrix Cloud 和网关服务突破功能时，才会执行 Citrix Cloud 和网关服务流量的第一个数据包检测和分类。

对于 Citrix SD-WAN 软件版本 11.3.0 及更高版本，无论 Citrix Cloud 和网关服务突破功能是否启用，都会执行 Citrix Cloud 和网关服务流量的首次数据包检测和分类。

> 注意
>
> - 您只能通过 Citrix SD-WAN 协调器配置 Citrix Cloud 和网关服务优化。有关更多信息，请参阅 网关服务优化。
> - **Citrix SD-WAN Orchestrator** 流量优化 是从 Citrix SD-WAN 软件版本 11.2.3 或更高版本引入的。目标是提供更精细的分类，从而分别识别 Citrix SD-WAN Orchestrator 流量和来自 Citrix Cloud 的其他相关服务的流量，并提供 Internet 突破选项。因此，客户现在可以选择仅优化 Citrix SD-WAN Orchestrator 流量。

Citrix Cloud 和网关服务类别

以下是用于分类和优化目的的流量类别：

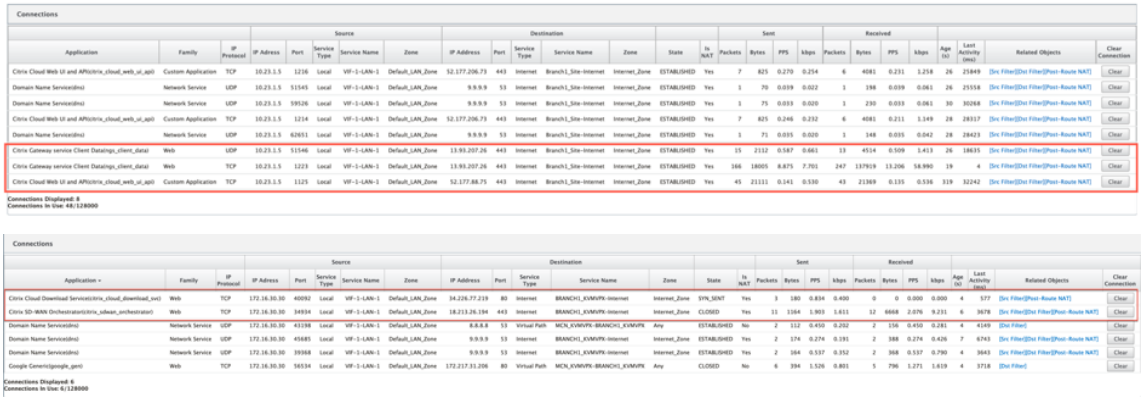
- **Citrix Cloud**：启用此功能可检测和路由发往 Citrix Cloud Web UI 和 API 的流量。
  - Citrix SD-WAN Orchestrator 和依赖的关键服务：
    - **Citrix SD-WAN Orchestrator**：支持在 Citrix SD-WAN 设备与 Citrix SD-WAN Orchestrator 之间建立和维护连接所需的心跳和其他流量的直接 Internet 突破。
    - **Citrix Cloud** 下载服务：启用直接 Internet 突围，以便将设备软件、配置、脚本等下载到 Citrix SD-WAN 设备上。
- **Citrix Gateway** 服务：启用以检测和路由发往 Citrix Gateway 服务的流量（控制和数据）。
  - 网关服务客户端数据：在客户端和 Citrix Gateway 服务之间启用 ICA 数据通道的直接 Internet 突破。它需要高带宽和低延迟。

- 网关服务服务器数据：在虚拟交付代理 (VDA) 和 Citrix Gateway 服务之间启用 ICA 数据通道的直接 Internet 突破。它需要高带宽和低延迟，并且仅适用于 VDA 资源位置（VDA 到 Citrix Gateway 关服务连接）。
- 网关服务控制流量：支持控制流量的直接 Internet 突破。没有特定的 QoS 注意事项。
- 网关服务 **Web** 代理流量：启用 Web 代理流量的直接 Internet 突破。它需要高带宽，但延迟要求可能会有所不同。

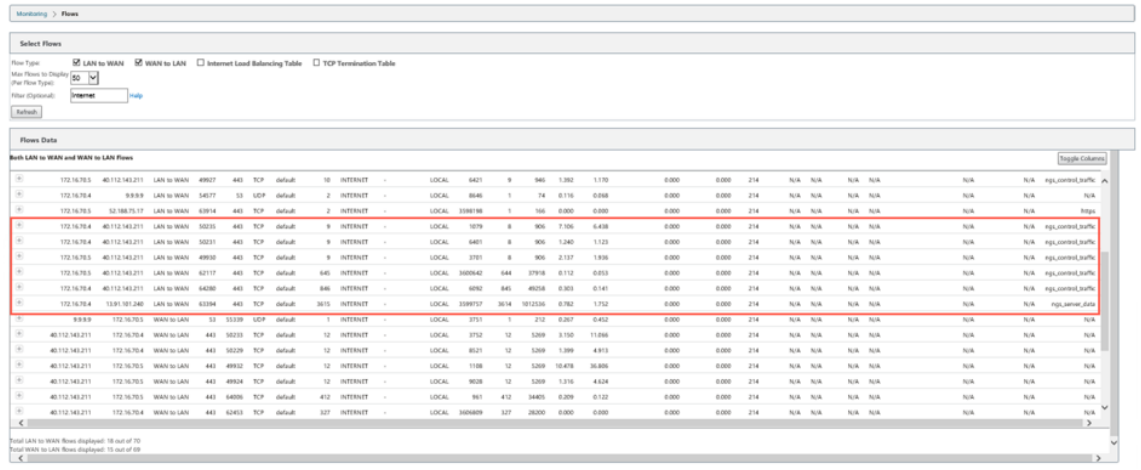
监视

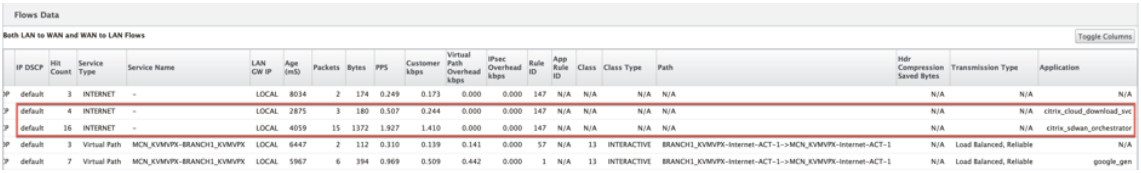
您可以在以下 SD-WAN 统计报告中监视网关服务统计信息：

- 防火墙统计信息

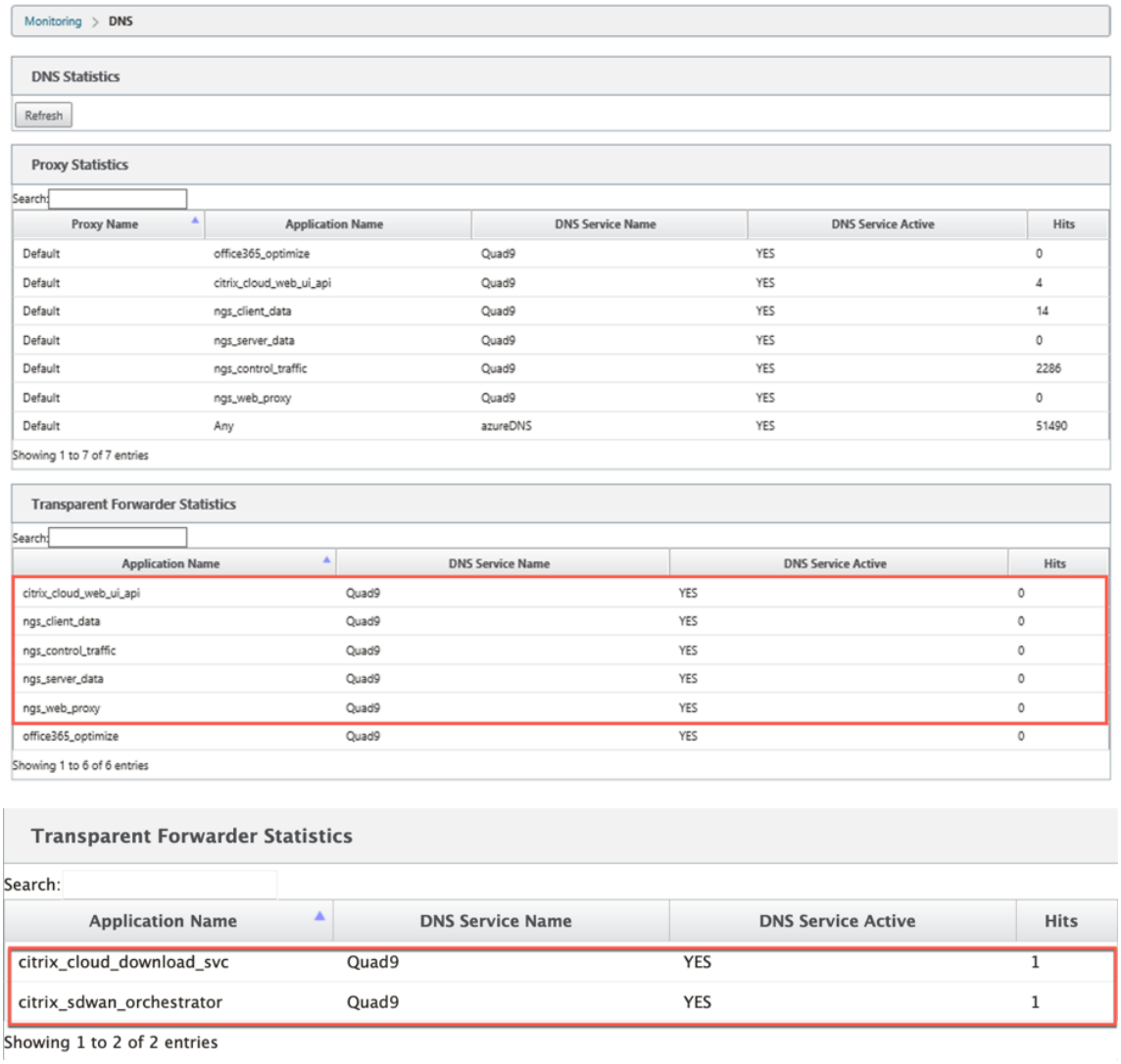


- 流

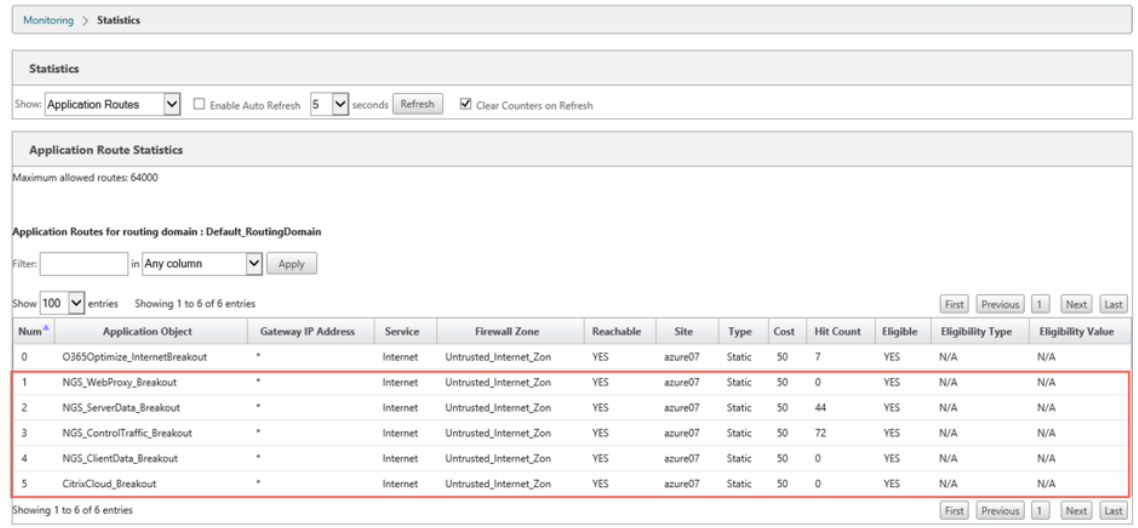


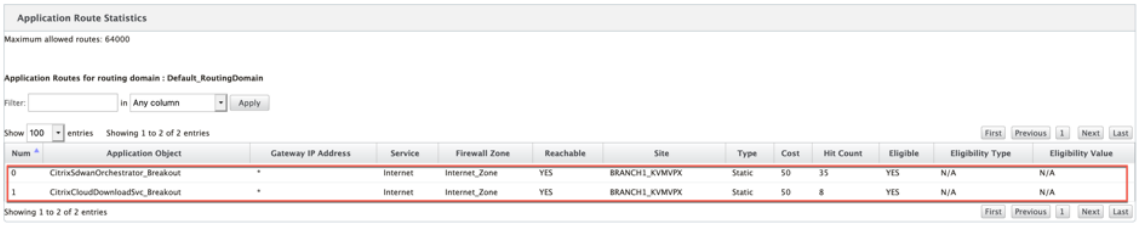


- DNS 统计信息



- 应用程序路由统计信息

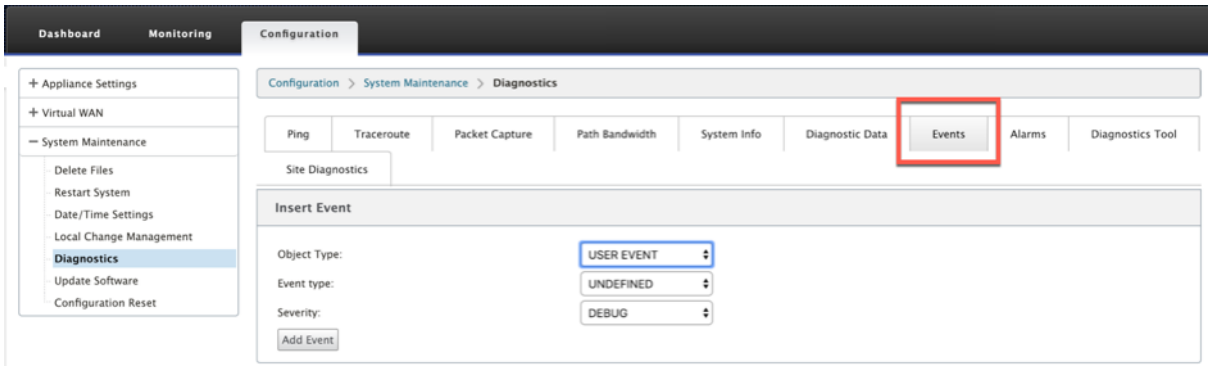




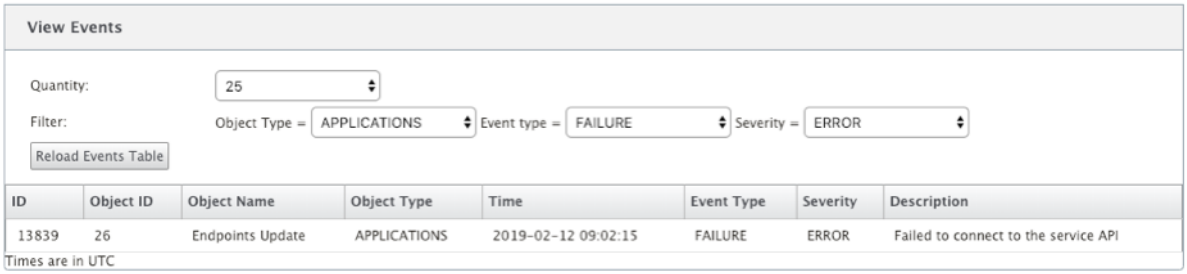
故障排除

您可以在 SD-WAN 设备的“事件”部分查看服务错误。

要检查错误，请导航到 配置 **>** 系统维护 **>** 诊断，单击 事件选项卡。

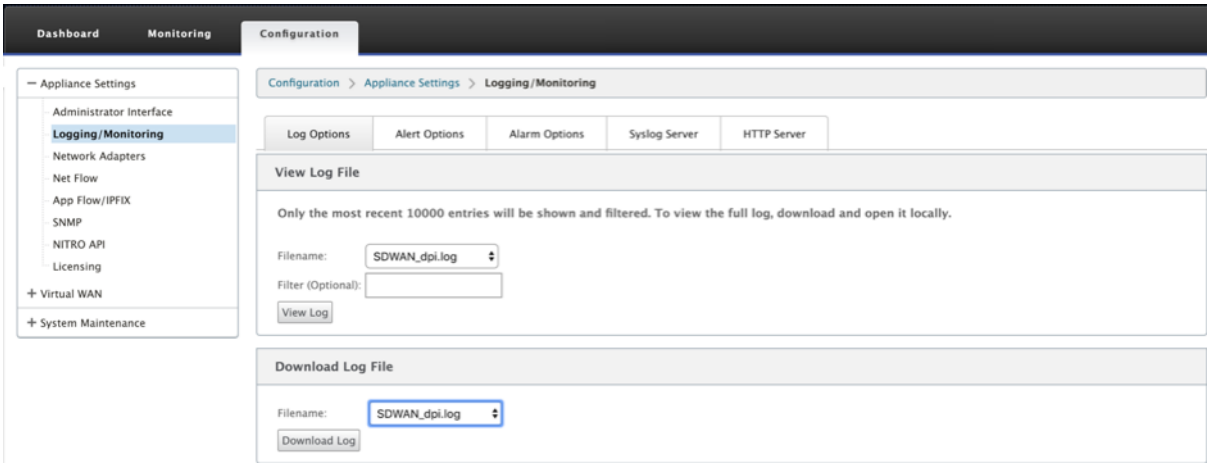


如果连接到 Citrix 服务（sdwan-app-路由.citrixnetworkapi.net）时出现问题，则错误消息将反映在“查看事件”表中。



连接错误也会记录到 **SDWAN_dpi.log** 中。要查看日志，请导航到 配置 **>** 装置设置 **>** 日志记录/监控 **>** 日志选项。从下拉列表中选择 SDWAN_dpi.log，然后单击查看日志。

您也可以下载日志文件。要下载日志文件，请从 下载日志文件 部分 下的下拉列表中选择所需的日志文件，然后单击 下载日志。



PPPoE 会话

September 2, 2022

以太网点对点协议 (PPPoE) 通过常用客户场所设备（例如 Citrix SD-WAN）将以太网 LAN 上的多个计算机用户连接到远程站点。PPPoE 允许用户共享通用的数字用户线 (DSL)、电缆调制解调器或无线连接到 Internet 。PPPoE 将通常用于拨号连接的点对点协议 (PPP) 与支持局域网中多个用户的以太网协议相结合。PPP 协议信息封装在以太网框架内。

Citrix SD-WAN 设备使用 PPPoE 向 Internet 服务提供商 (ISP) 提供支持以与拨号连接不同的方式建立持续不间断的 DSL 和电缆调制解调器连接。PPPoE 提供每个用户远程站点会话，通过称为 发现 的初始交换来学习彼此的网络地址。在单个用户和远程站点（例如 ISP 提供程序）之间建立会话后，可以监视该会话。公司使用以太网和 PPPoE 通过 DSL 线路使用共享 Internet 接入。

Citrix SD-WAN 充当 PPPoE 客户端。它通过 PPPoE 服务器进行身份验证并获取动态 IP 地址，或者使用静态 IP 地址建立 PPPoE 连接。

成功建立 PPPoE 会话需要以下内容：

- 配置虚拟网络接口 (VNI)。
- 用于创建 PPPoE 会话的唯一凭据。
- 配置 WAN 链接。每个 VNI 只能配置一个 WAN 链接。
- 配置虚拟 IP 地址。每个会话根据提供的配置获取唯一的 IP 地址（动态或静态）。
- 在桥接模式下部署设备以使用 PPPoE 静态 IP 地址，并将接口配置为“受信任”。
- 静态 IP 优先使用配置来强制服务器提出的 IP；如果与配置的静态 IP 不同，否则会发生错误。
- 将设备部署为边缘设备，以便将 PPPoE 与动态 IP 结合使用，并将接口配置为“不受信任”。
- 支持的身份验证协议有：PAP、CHAP、EA-MD5、EAP-SRP。
- 多个会话的最大数量取决于配置的 VNI 数量。
- 创建多个 VNI 以支持每个接口组的多个 PPPoE 会话。

  > 注意：允许使用相同的 802.1Q >VLAN 标记创建
  >
  > 多个 VNI。

PPPoE 配置的限制：

- 不支持 802.1q VLAN 标记。
- 不支持 EAP-TLS 身份验证。
- 地址/控制压缩。
- 放气压缩。
- 协议字段压缩协商。
- 压缩控制协议。
- BSD 压缩压缩。
- IPX 协议。
- 购买力平价多链接。
- 范雅各布森风格 TCP/IP 头压缩.
- Van Jacobson 风格的 Connection-ID 压缩选项 TCP/IP 标头压缩。
- LTE 接口不支持 PPPoE

从 Citrix SD-WAN 11.3.1 版本中，需要考虑额外的 8 字节 PPPoE 标头来调整 TCP 最大分段大小 (MSS)。额外的 8 个字节 PPPoE 报头根据 MTU 调整同步数据包中的 MSS。

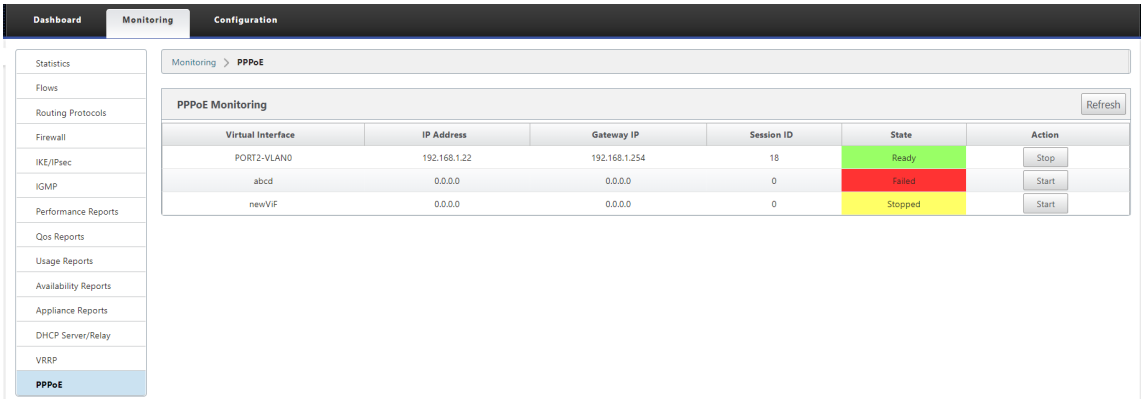
有关如何通过 Citrix SD-WAN Orchestrator 服务配置 PPPoE 的信息，请参阅 接口。

监测 **PPPoE** 会议

您可以通过导航到 SD-WAN GUI 中的 监控 **> PPPoE** 页面来监视 PPPoE 会话。

PPPoE 页面提供使用 PPPoE 静态或动态客户端模式配置的 VNI 的状态信息。它允许您从 Citrix SD-WAN Orchestrator 服务手动启动和停止会话以进行故障排除。

- 如果 VNI 已启动并准备就绪，**IP** 和网关 **IP** 列将显示会话中的当前值。它表示这些是最近接收的值。
- 如果 VNI 停止或处于失败状态，则这些值为上次接收的值。



状态 列使用三种颜色代码（绿色、红色、黄色和值）显示 **PPPoE** 会话的状态。下表描述了状态和描述。您可以将鼠标悬停在状态上以获取描述。

PPPoE 会话类型	颜色	说明
已配置	黄色	VNI 配置了 PPPoE。这是一个初始状态。
正在拨号	黄色	配置 VNI 后，PPPoE 会话状态通过启动 PPPoE 发现移动到拨号状态。数据包信息被捕获。
会话	黄色	VNI 从发现状态移动到会话状态。正在等待接收 IP，如果是动态的，或等待服务器对通告 IP 的确认（如果是静态的）。
已就绪	绿色	接收 IP 数据包，VNI 和关联的 WAN 链接已准备就绪可供使用。
失败	红色	PPP/PPPoE 会话终止。失败的原因可能是配置无效或致命错误。会话将在 30 秒后尝试重新连接。
已停止	黄色	PPP/PPPoE 会话手动停止。
终止	黄色	由于某种原因而终止的中间状态。此状态在一定持续时间后自动启动（正常错误为 5 秒，致命错误为 30 秒）。
已禁用	黄色	SD-WAN 服务处于禁用状态。

故障排除 **PPPoE** 会话故障

在 监视 页上，当建立 PPPoE 会话时出现问题时：

- 将鼠标悬停在 失败 状态上显示最近失败的原因。
- 若要建立新的会话或对活动 PPPoE 会话进行故障排除，请使用 监视-> PPPoE 页面并重新启动会话。
- 如果 PPPoE 会话手动停止，则在手动启动并激活配置更改或重新启动服务之前，无法启动该会话。

PPPoE 会话可能会因以下原因而失败：

- 当 SD-WAN 由于配置中的用户名/密码不正确而无法向对等方进行身份验证时。
- PPP 协商失败-协商没有达到至少一个网络协议正在运行的地步。
- 系统内存或系统资源问题。
- 配置无效/错误（错误的 AC 名称或服务名称）。
- 由于操作系统错误，无法打开串行端口。
- 没有收到回声数据包的响应（链接不好或服务器未响应）。
- 有几个连续不成功的拨号会话在一分钟内。

在连续 10 次失败后，观察到失败的原因。

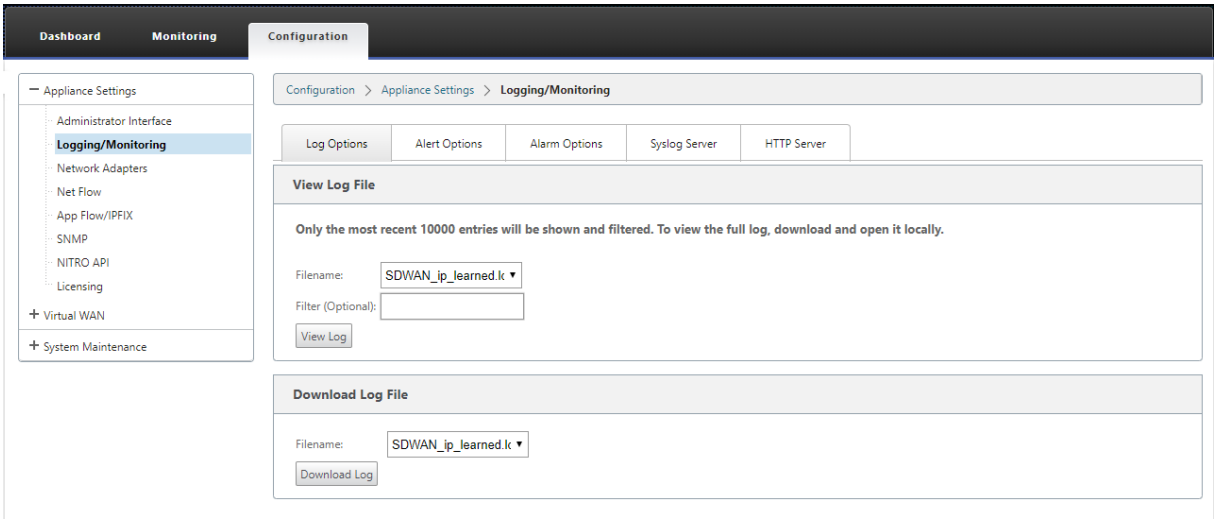
- 如果故障正常，它将立即重新启动。
- 如果失败是错误，则重新启动将恢复 10 秒。
- 如果失败是致命的，则重新启动将恢复 30 秒，然后重新启动。

LCP Echo 请求数据包每 60 秒从 SD-WAN 生成一次，未能接收 5 个回显响应被视为链路失败，并重新建立会话。

PPPoE 日志文件

SDWAN_ip_learned.log 文件包含与 PPPoE 相关的日志。

要从 SD-WAN GUI 查看或下载 *SDWAN_ip_learned.log* 文件，请导航到“装置设置” > “记 录/监 视” > “日志选项”。查看或下载 *SDWAN_IP* 学习的。日志 文件。



服务质量

November 16, 2022

办公地点与数据中心或云之间的网络必须传输大量的应用程序和数据，包括高质量的视频或实时语音。带宽敏感的应用程序可扩展网络的功能和资源。Citrix SD-WAN 提供有保证、安全、可测量且可预测的网络服务。这是通过管理网络上的延迟、抖动、带宽和数据包丢失来实现的。

Citrix SD-WAN 解决方案包括一个复杂的应用程序服务质量 (QoS) 引擎，用于访问应用程序流量并对关键应用程序进行优先级排序。它还了解 WAN 网络质量的要求，并根据质量特征实时选择网络路径。

以下各节中的主题将讨论 QoS 类、IP 规则、应用程序 QoS 规则以及定义应用程序 QoS 所需的其他组件。

从 SD-WAN 11.5 版本开始，QoS 功能可通过 Citrix SD-WAN Orchestrator 服务进行配置。有关更多信息，请参阅服务质量。

班级

Citrix SD-WAN 配置提供了一组默认的应用程序和基于 IP/端口的 QoS 策略，这些策略适用于通过虚拟路径传输的所有流量。这些设置可以根据部署需求进行自定义。

类对于确定流量的优先级非常有用。基于应用程序和 IP/端口的 QoS 策略对流量进行分类，并将其放入配置中指定的适当类中。

Citrix SD-WAN Orchestrator 服务支持 13 个类别。有关更多信息，请参阅 类。

以下是不同类型的类：

- 实时：用于低延迟、低带宽、时间敏感的流量。实时应用程序比较耗时，但实际上不需要高带宽 (例如 IP 语音)。实时应用程序对延迟和抖动敏感，但可以容忍一些损失。

- 交互式：用于具有低到中等延迟要求和低到中等带宽要求的交互式流量。通常情况下，在客户端与服务器之间进行交互。通信可能不需要高带宽，但对丢失和延迟非常敏感。
- 批量：用于高带宽流量和可容忍高延迟的应用程序。处理文件传输和需要高带宽的应用程序将分类为散装类。这些应用很少涉及人为干扰，主要由系统自己处理。

类之间的带宽共享

带宽在类之间共享，如下所示：

- 实时：进入实时课程的流量保证具有低延迟，并且在存在竞争流量时，带宽将限制在班级共享内。
- 互动：触及交互式课程的流量在提供实时流量后获得剩余带宽，可用带宽在互动课程之间公平分享。
- 批量：批量是最佳努力。提供实时和交互式流量后留下的带宽将以公平共享的方式分配给批量类。如果实时和交互式流量利用了所有可用带宽，则批量流量可能会饿死。

> 注意
>
> 在没有争用的情况下，任何课程都可以使用所有可用带宽。

以下示例说明了基于类配置的带宽分布：

假设虚拟路径上的聚合带宽为 10 Mbps。如果类配置为

- 实时：30%
- 互动高：40%
- 互动媒介：20%
- 交互式低：10%
- 批量：100%

带宽分配的结果是：

- 根据需要，实时流量可获得 10Mbps（3 Mbps）的 30%。如果需要的带宽少于 10%，则剩余的带宽将提供给其他类别。
- 互动课程在公平份额的基础上共享剩余的带宽（4 Mbps：2 Mbps：1 Mbps）。
- 当实时交互式流量没有完全使用其份额时，剩余的任何东西都会提供给 Bulk 类。

按 **IP** 地址和端口号进行规则

按 IP 地址和端口号的规则功能可帮助您为网络创建规则，并根据规则做出某些服务质量 (QoS) 决策。您可以为网络创建自定义规则。例如，您可以将规则创建为—如果源 IP 地址为 172.186.30.74 且目标 IP 地址为 172.186.10.89，则将传输模式 设置为持久路径，将局域网至 **WAN** 类设置为 10 (realtime_class)”。

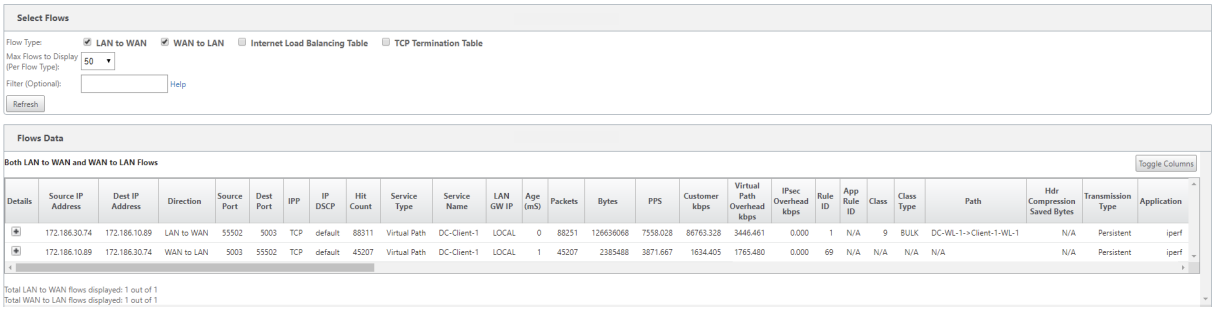
您可以在站点级别或全局级别本地创建规则。如果多个站点需要相同的规则，则可以在全局 **>** 虚拟路径默认集 **>** 规则下全局为规则创建模板。然后，模板可以附加到需要应用规则的站点。即使站点与全局创建的规则模板相关联，您也可以创建特定于站点的规则。在这种情况下，站点特定规则优先并覆盖全局创建的规则模板。

从 Citrix SD-WAN 11.5 版本开始，您可以使用 Citrix SD-WAN Orchestrator 服务创建 IP 规则。有关更多信息，请参阅 IP 规则。

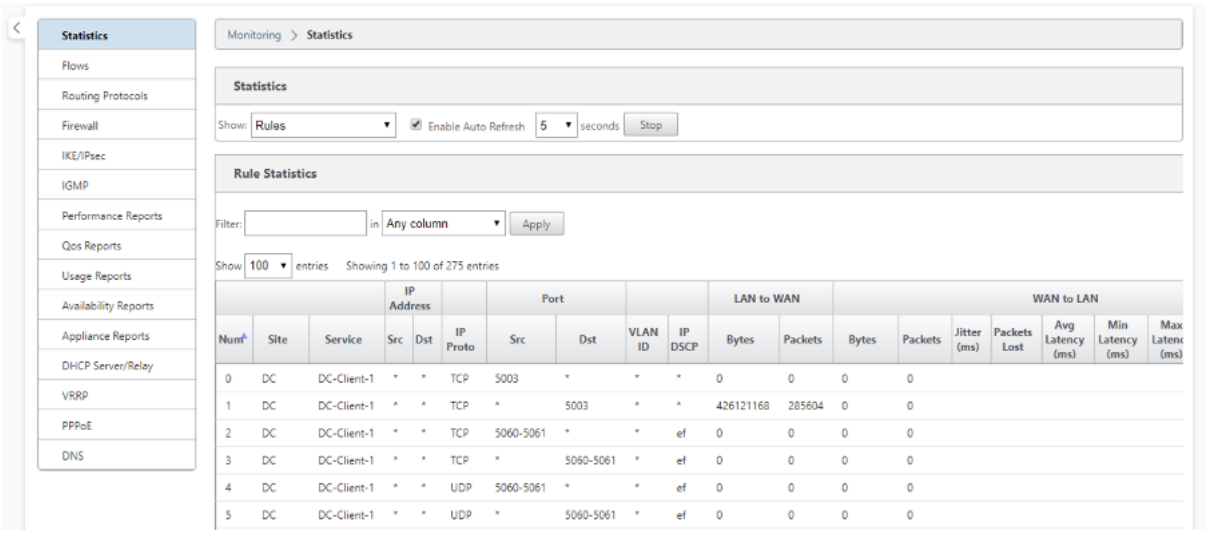
验证规则

导航到“监控”**>**“流量”。选择流程页面顶部的选择流程部分中的流程类型字段。在“流程类型”字段旁边有一行复选框，用于选择要查看的流程信息。验证流信息是否符合配置的规则。

示例：
如果源 IP 地址是 172.186.30.74 且目标 IP 地址是 172.186.10.89，则将传输模式设置为永久路径规则显示以下流量数据。



导航到 监控 **>** 统计信息 并验证配置的规则。



按应用程序名称进行的规则

应用程序分类功能允许 Citrix SD-WAN 设备分析传入流量并将其分类为属于特定应用程序或应用程序系列。通过这种分类，我们可以通过创建和应用应用程序规则来提高单个应用程序或应用程序系列的 QoS。

您可以根据应用程序、应用程序系列或应用程序对象匹配类型过滤流量，并对它们应用应用程序规则。应用程序规则类似于 Internet 协议 (IP) 规则。有关 IP 规则的信息，请参阅 按 IP 地址和端口号划分的规则。

对于每个应用程序规则，您可以指定传输模式。以下是可用的发射模式：

- 负载平衡路径：流的应用程序流量在多个路径之间进行平衡。通过最佳路径发送流量，直到使用该路径为止。剩余的数据包将通过下一个最佳路径发送。
- 持久路径：应用程序流量将保持在同一路径上，直到路径不再可用为止。
- 重复路径：应用程序流量跨多个路径复制，从而提高可靠性。

应用程序规则与类相关联。有关类的信息，请参阅 自定义类。

默认情况下，以下五个预定义的应用程序规则可用于 Citrix ICA 应用程序：

规则	类	传输模式	重新传输丢失的数据包	启用数据包聚合	启用数据包重新同步	重新平衡保持时间(毫秒)	丢弃延迟重新分配数据包	下降限制(毫秒)	下降深度（字节）	启用红色	禁用限制(毫秒)	禁用深度（字节）
HDX_Priority_0 (HDX_priority_tag_0)	0	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_1 (HDX_priority_tag_1)	1	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_2 (HDX_priority_tag_2)	2	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_3 (HDX_priority_tag_3)	3	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX	11（交互式高级）	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000

如何应用申请规则**?**

在 SD-WAN 网络中，当传入的数据包到达 SD-WAN 设备时，初始数据包不会进行 DPI 分类。此时，IP 规则属性（如类、TCP 终止）将应用于数据包。DPI 分类后，应用程序规则属性（如类、传输模式）将覆盖 IP 规则属性。

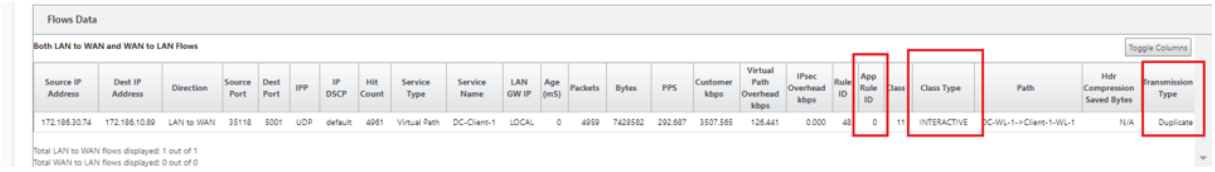
与应用程序规则相比，IP 规则具有更多的属性。应用程序规则仅覆盖少数 IP 规则属性，其余的 IP 规则属性仍在数据包上处理。

例如，假设您已为使用 SMTP 协议的 Web 邮件应用程序（例如 Google Mail）指定了应用程序规则。SMTP 协议的 IP 规则集最初应用于 DPI 分类之前。解析数据包并将其分类为属于 Google Mail 应用程序后，应用为 Google Mail 应用程序指定的应用程序规则。

要使用 Citrix SD-WAN Orchestrator 创建应用程序规则，请参阅 应用程序规则。

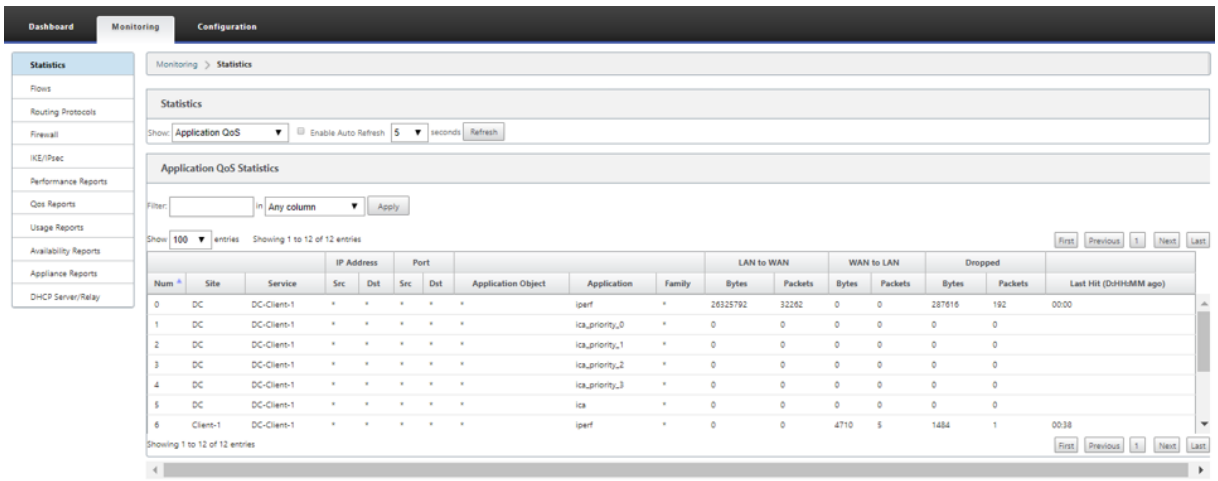
要确认应用程序规则是否应用于流量，请导航到 监控 > 流量。

记下应用程序规则 ID，并检查类类型和传输模式是否符合您的规则配置。



您可以通过导航到监视 > 统计信息 > 应用程序 **QoS** 来监视应用程序 QoS，例如在每个站点上没有上载、下载或丢弃的数据包/字节。

Num 参数指示应用程序规则 ID。检查从流中获取的应用程序规则 ID。



创建自定义应用程序

您可以使用应用程序对象基于以下匹配类型定义自定义应用程序：

- IP 协议
- 应用程序名称

- 应用程序系列

DPI 分类器分析传入的数据包，并根据指定的匹配条件将其分类为应用程序。您可以在 QoS、防火墙和应用程序路由中使用这些分类的自定义应用程序。

> 提示
>
> 您可以指定一个或多个匹配类型。

应用程序分类

Citrix SD-WAN 设备使用以下技术执行深度数据包检查 (DPI) 以识别应用程序并对其进行分类：

- 新闻部图书馆分类
- Citrix 专有的独立计算架构 (ICA) 分类
- 应用程序供应商 API（例如适用于 Office 365 的 Microsoft REST API）
- 基于域名的应用程序分类

新闻部图书馆分类

深度数据包检测 (DPI) 库可识别数以千计的商业应用程序。它可实现应用程序的实时发现和分类。SD-WAN 设备使用 DPI 技术分析传入的数据包，并将流量分类为属于特定应用程序或应用程序系列。每个连接的应用程序分类需要几个数据包。

要在 Citrix SD-WAN Orchestrator 服务上启用 DPI 库分类，请参阅 DPI 库分类。

ICA 分类

Citrix SD-WAN 设备还可以识别和分类虚拟应用程序和桌面的 Citrix HDX 流量。Citrix SD-WAN 识别 ICA 协议的以下变体：

- ICA
- CGP
- 单流 ICA (SSI)
- 多流 ICA (微星)
- ICA 对技术合作协议
- ICA over UDP/EDT
- ICA 通过非标准端口（包括多端口 ICA）
- HDX 自适应传输
- ICA over WebSocket（由 HTML5 Receiver 使用）

> 注意
>
> SD-WAN 标准版不支持对通过 SSL/TLS 或 DTLS 交付的 ICA 流量进行分类。
>
> 网络流量的分类是在初始连接或流量建立期间完成的。因此，预先存在的连接不被分类为 ICA。手动清除连接表时，连接分类也会丢失。
>
> Framehawk 流量和 UDP/RTP 上的音频不被归类为 HDX 应用程序。它们报告为 UDP 或 未知协议。
>
> 自 10 版本 1 以来，SD-WAN 设备即使在单端口配置中，也可以区分多流 ICA 中的每个 ICA 数据流。每个 ICA 流都被分类为一个单独的应用程序，具有其自己的默认 QoS 类来进行优先级排序。
>
> - 要使多流 ICA 功能正常运行，您必须拥有 SD-WAN 标准版 10.1 或更高版本。
> - 要在 SDWAN-Center 上显示基于 HDX 用户的报告，您必须拥有 SD-WAN 标准版 11.0 或更高版本。
>
> HDX 信息虚拟通道的最低软件要求：
>
> - Citrix Virtual Apps and Desktops（以前称为 XenApp 和 XenDesktop）的当前版本，因为必备功能是在 XenApp 和 XenDesktop 7.17 中引入的，不包括在 7.15 长期服务版本中。
> - 支持多流 ICA 和 HDX 见解信息虚拟通道 CTXNSAP 的 Citrix Workspace 应用程序（或其前身，Citrix Receiver）的版本。在 Citrix Workspace 应用程序功能矩阵 中查找 具有 **NSAP VC** 和多端口/多流 **ICA** 的 **HDX Insight**。在 HDX Insights上查看当前支持的发行版本。
> - 从 11.2 版本起，现在默认情况下，在使用多流 ICA 时，HDX 实时流量启用数据包复制功能。

分类后，ICA 应用程序可用于应用程序规则中，并查看与其他分类应用程序类似的应用程序统计信息。

ICA 应用程序有五个默认应用程序规则，每个规则针对以下优先级标记：

- 独立计算架构 (Citrix) (ICA)
- ICA 实时（ICA 优先级 _0）
- ICA 交互式 (ICA 优先级 _1)
- ICA 批量传输 (ica_prority_2)
- 国际合作社理事会背景 (优先级 _3)

有关详 细信息，请参阅按应用程序名称排

如果要通过单个端口运行不支持多流 ICA 的软件组合，则要执行 QoS，您必须为每个 ICA 流配置多个端口。
要按照 XA/XD 服务器策略中配置的非标准端口对 HDX 进行分类，必须在 ICA 端口配置中添加这些端口。此外，要将这些端口上的流量与有效的 IP 规则相匹配，您必须更新 ICA IP 规则。

在 ICA IP 和端口列表中，您可以指定 XA/XD 策略中使用的非标准端口以进行 HDX 分类。IP 地址用于进一步限制端口到特定目的地。使用“*”表示发往任何 IP 地址的端口。IP 地址与 SSL 端口组合也用于指示流量可能是 ICA，即使流量不是最终分类为 ICA。此指示用于发送 L4 AppFlow 记录以支持 Citrix Application Delivery Management 中的多跃点报告。

要在 Citrix SD-WAN Orchestrator 服务上启用基于 ICA 的分类，请参阅 ICA 分类。

应用程序供应商 **API** 基于分类

Citrix SD-WAN 支持以下基于应用程序供应商 API 的分类：

- 办公室 365 有关详细信息，请参阅 Office 365 优化。
- Citrix Cloud 和 Citrix Gateway 服务. 有关更多信息，请参阅 网关服务优化。

基于域名的应用程序分类

DPI 分类引擎得到了增强，可根据域名和模式对应用程序进行分类。DNS 转发器拦截并解析 DNS 请求后，DPI 引擎会使用 IP 分类器执行第一个数据包分类。进一步的 DPI 库和 ICA 分类完成，并附加基于域名的应用程序 ID。

基于域名的应用程序功能允许您对多个域名进行分组，并将其视为单个应用程序。更轻松地应用防火墙、应用程序指导、QoS 和其他规则。最多可配置 64 个基于域名的应用程序。

要在 Citrix SD-WAN Orchestrator 服务上定义基于 域名的应用程序，请参阅基于域名的应用程序分类。

> 注意
>
> - 从 11.4.2 版本起，基于域名的应用程序支持 Citrix SD-WAN Orchestrator 服务中的可配置端口和协议。有关详细信息，请参阅 域和应用程序。
> - 从 Citrix SD-WAN 11.5.0 版本开始，Citrix SD-WAN Orchestrator 服务支持 AAAA 记录。

限制

- 如果没有对应于基于域名的应用程序的 DNS 请求/响应，DPI 引擎不会对基于域名的应用程序进行分类，因此不会应用与基于域名的应用程序对应的应用程序规则。
- 如果创建的应用程序对象使端口范围包括端口 80 和/或端口 443，具有与基于域名的应用程序相对应的特定 IP 地址匹配类型，则 DPI 引擎不会对基于域名的应用程序进行分类。
- 如果配置了显式 Web 代理，则必须将所有域名模式添加到 PAC 文件中，以确保 DNS 响应并不总是返回相同的 IP 地址。
- 基于域名的应用程序分类会在配置升级时重置。重分类基于 11.0.2 之前版本的分类技术，例如 DPI 库分类、ICA 分类和基于供应商应用程序 API 的分类。
- 根据基于域名的应用程序分类获取的应用程序签名（目标 IP 地址）将在配置更新时重置。
- 仅处理标准 DNS 查询及其响应。
- 分割到多个数据包的 DNS 响应记录不会被处理。仅处理单个数据包中的 DNS 响应。
- 不支持通过 TCP 进行 DNS。
- 只支持顶级域作为域名模式。

对加密流量进行分类

Citrix SD-WAN 设备通过以下两种方法检测并报告加密流量，作为应用程序报告的一部分：

- 对于 HTTPS 流量，DPI 引擎会检查 SSL 证书以读取公用名称，该名称包含服务的名称（例如- Facebook，Twitter）。根据应用程序体系结构，只有一个证书可用于多种服务类型（例如电子邮件、新闻等）。如果不同的服务使用不同的证书，DPI 引擎将能够区分服务。
- 对于使用自己的加密协议的应用程序，DPI 引擎会在流程中查找二进制模式。例如，在 Skype 的情况下，DPI 引擎会在证书中查找二进制模式并确定应用程序。

应用程序对象

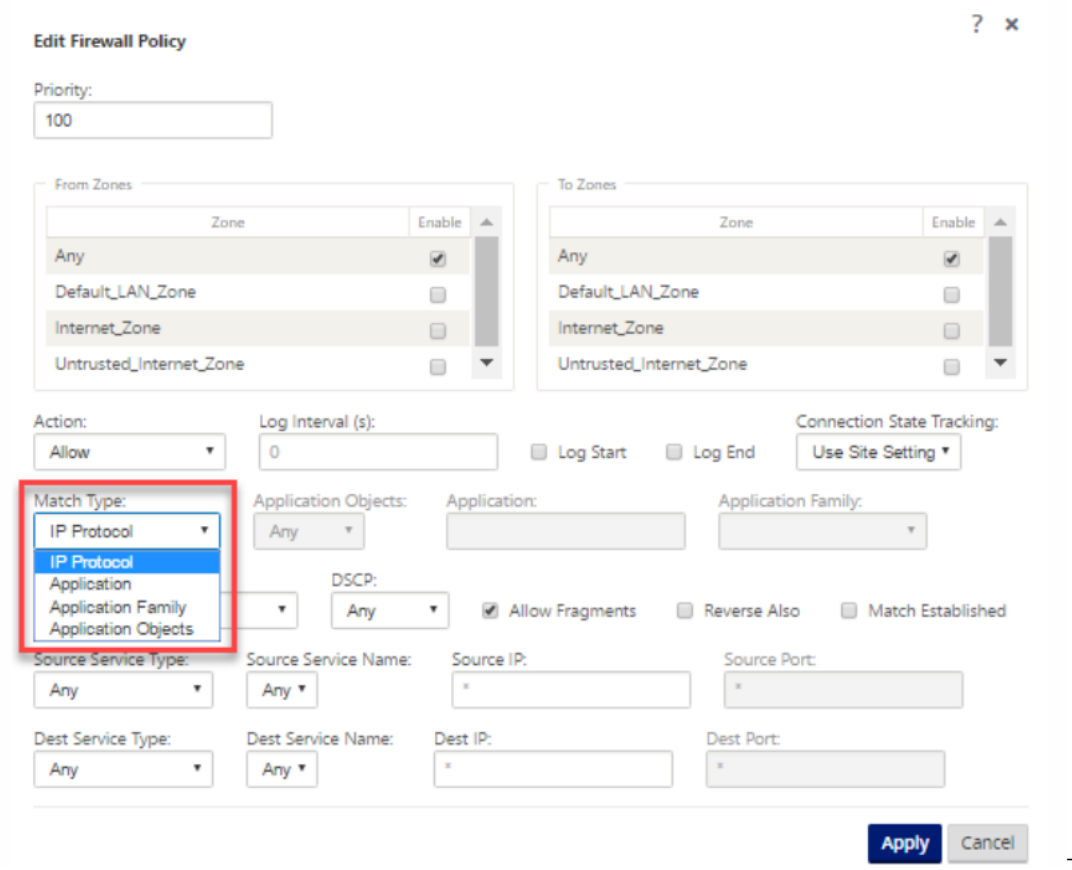
通过应用程序对象，您可以将不同类型的匹配条件分组到一个可用于防火墙策略和应用程序指导的单个对象中。IP 协议、应用程序和应用程序系列是可用的匹配类型。

以下功能使用应用程序对象作为匹配类型：

- 应用程序路由
- 防火墙策略
- 应用 QoS 规则
- 应用程序 QoE

将应用程序分类与防火墙结合使用

通过将流量分类为应用程序、应用程序系列或域名，您可以使用应用程序、应用程序系列和应用程序对象作为匹配类型来筛选流量并应用防火墙策略和规则。它适用于所有 前、后 和 本地 策略。有关防火墙的详细信息，请参阅 有状态防火墙和 NAT 支持。



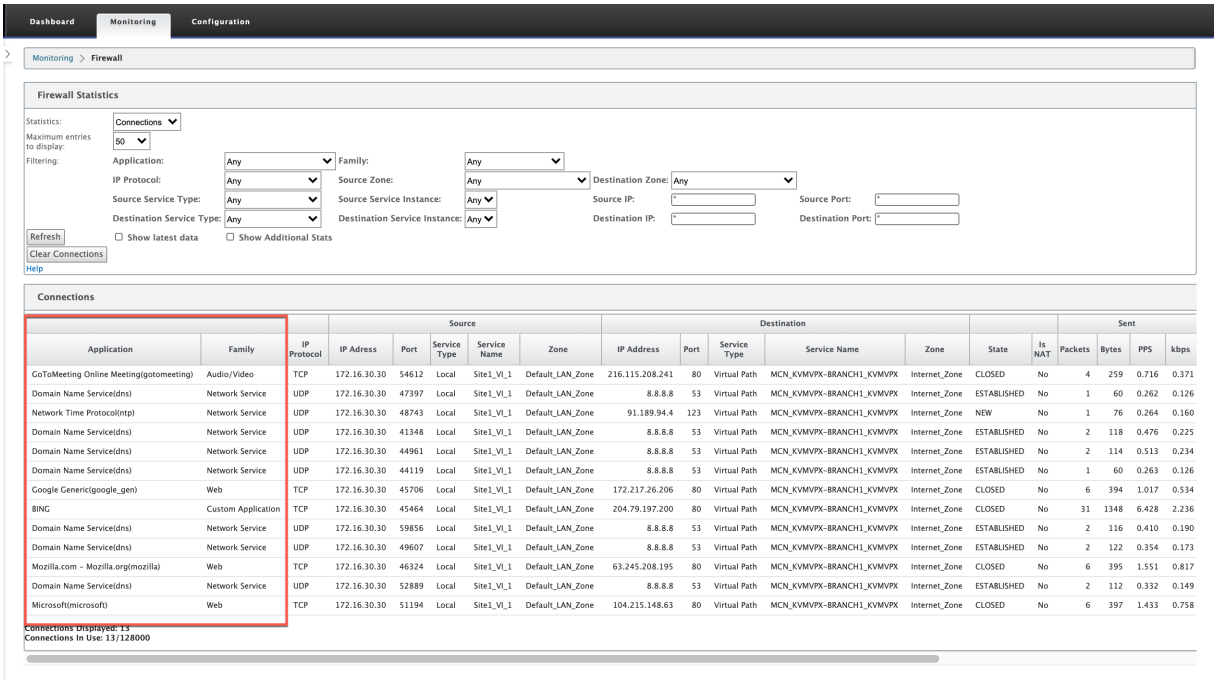
—>

查看应用程序分类

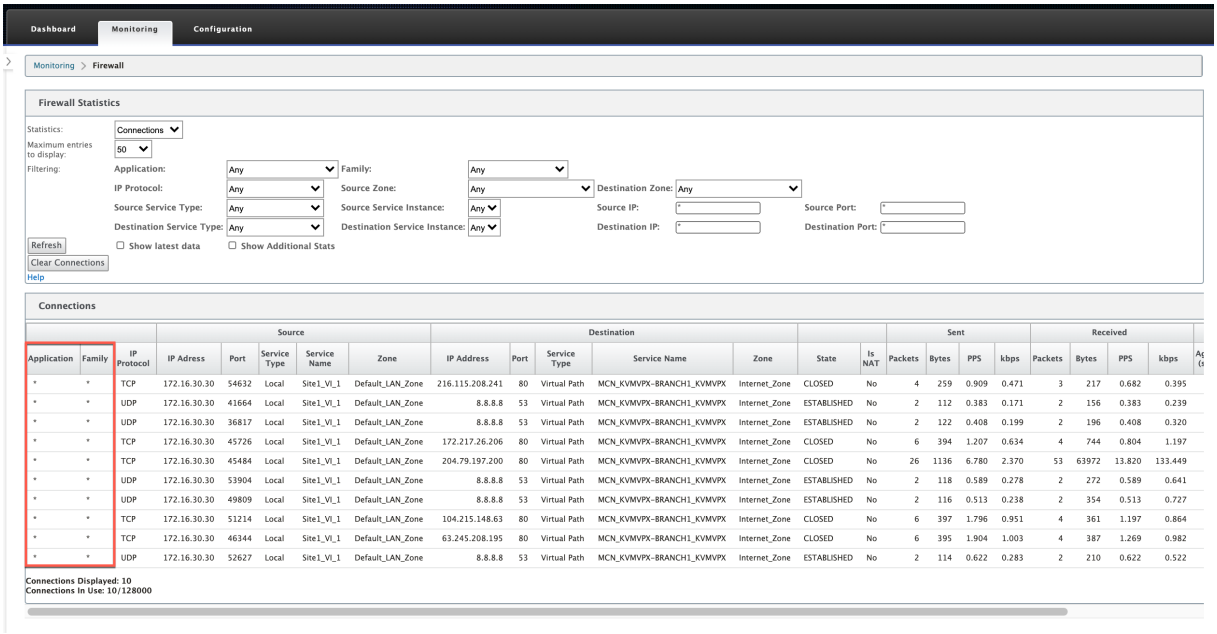
启用应用程序分类后，您可以在以下报告中查看应用程序名称和应用程序系列详细信息：

- 防火墙连接统计
- 流信息
- 应用程序统计

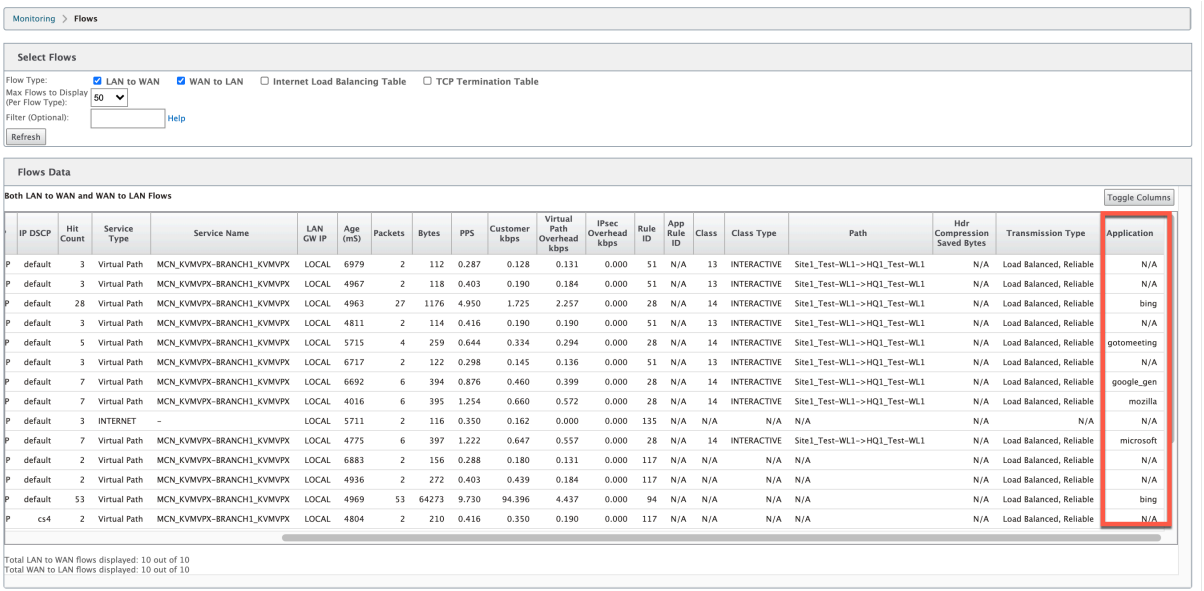
防火墙连接统计　导航到 监控 > 防火墙。在连接部分下，应用程序和系列列列出了应用程序及其关联系族。



如果未启用应用程序分类，则应用程序和系列列不显示任何数据。



流信息　导航到“监控”**>**“流量”。在流量数据部分下，应用程序列列出了应用程序



应用程序统计　导航到 监控 **>** 统计信息。在应用程序统计信息部分下，应用程序列列出了应用程序详细信息。

故障排除

启用应用程序分类后，您可以查看 监控 部分下的报告，并确保它们显示应用程序详细信息。有关详细信息，请参阅 查看应用分类。

如果存在任何意外行为，请在发现此问题时收集 STS 诊断程序包，并与 Citrix 技术支持团队共享。

可以使用 配置 **>** 系统维护 **>** 诊断 **>** 诊断信息创建和下载 STS 包。

QoS 公平性 **(**红色**)**

QoS 公平性功能通过使用 QoS 类 和随机早期检测 (RED) 提高了多个虚拟路径流的公平性。虚拟路径可以分配给 16 个不同的类中的一个。一个类可以是以下三种基本类型之一：

- 实时类服务的流量流量需要在特定带宽限制下提供及时服务。低延迟优先于总吞吐量。
- 交互式类的优先级低于实时，但优先于批量流量。
- 批量类获取实时和交互式类遗留的内容，因为延迟对于批量流量来说不太重要。

用户为不同的类指定不同的带宽要求，这使虚拟路径调度程序能够仲裁来自同一类型的多个类的竞争带宽请求。调度程序使用分层公平服务曲线 (HFSC) 算法来实现各类之间的公平性。

HFSC 按先进先出 (FIFO) 顺序提供服务。在计划数据包之前，Citrix SD-WAN 会检查数据包类的待处理流量。当过多的流量处于挂起状态时，数据包将被丢弃，而不是被放入队列（尾部丢弃）。

为什么 **TCP** 会导致排队**?**

TCP 无法控制网络传输数据的速度。为了控制带宽，TCP 实现了带宽窗口的概念，即它允许在网络中的未确认流量。它最初以一个小窗口开始，每当收到确认时，它将该窗口的大小加倍。这被称为缓慢启动或指数增长阶段。

TCP 通过检测丢弃的数据包来识别网络拥堵。如果 TCP 堆栈发送导致 250 ms 延迟的数据包突发，TCP 不会检测拥塞，如果没有丢弃任何数据包，因此它会继续增加窗口的大小。它可能会继续这样做，直到等待时间达到 600—800 毫秒。

当 TCP 不处于慢速启动模式时，它会在检测到数据包丢失时减少一半带宽，并为每次接收的确认增加一个数据包允许带宽。因此，TCP 在对带宽施加上升压力和退出之间交替。不幸的是，如果等待时间在检测到数据包丢失时达到 800 ms，带宽降低会导致传输延迟。

对 **QoS** 公平性的影响

当发生 TCP 传输延迟时，在虚拟路径类中提供任何类型的公平性保证都是困难的。虚拟路径调度程序必须应用尾放 行为，以避免持有大量流量。TCP 连接的性质是，少量流量流动到虚拟路径，这使得新的 TCP 连接难以获得公平的带宽份额。公平共享带宽需要确保带宽可用于传输新数据包。

随机早期检测

随机早期检测 (RED) 可防止流量队列填满并导致尾部掉落操作。它可以防止虚拟路径调度程序不必要地排队，而不会影响 TCP 连接可以实现的吞吐量。

有关如何使用和启用 RED 的信息，请参阅 如何使用 RED。

MPLS 队列

此功能在添加多协议层切换 (MPLS) WAN 链接时简化了创建 SD-WAN 配置的过程。以前，每个 MPLS 队列都需要创建一个 WAN 链接。每个 WAN 链接都需要一个唯一的虚拟 IP 地址 (VIP) 来创建 WAN 链接和一个与提供商的队列方案对应的唯一差异化服务代码点 (DSCP) 标签。为每个 MPLS 队列定义 WAN 链接后，定义映射到特定队列的 Intranet 服务。

目前，新的 MPLS 特定 WAN 链接定义（即访问类型）可用。选择新的专用 MPLS 访问类型后，您可以定义与 WAN 链路关联的 MPLS 队列。这允许一个具有多个 DSCP 标签的单个 VIP，这些标签对应于 MPLS WAN 链接的提供程序的队列实现。这将内联网服务映射到单个 MPLS WAN 链接上的多个 MPLS 队列。有关如何使用 Citrix SD-WAN Orchestrator 服务配置 MPLS 的信息，请参阅 MPLS 队列。

> 注意
>
> 如果您具有现有 MPLS 配置，并希望实施专用 MPLS 访问类型，请与 Citrix 支持部门联系以获得帮助。

将自动解决组分配给虚拟路径 **WAN** 链路

为 MCN 和客户端设备定义的自动传输组相同。这允许系统自动构建路径。在 MCN 站点，您还可以展开与虚拟路径关联的 WAN 链接。

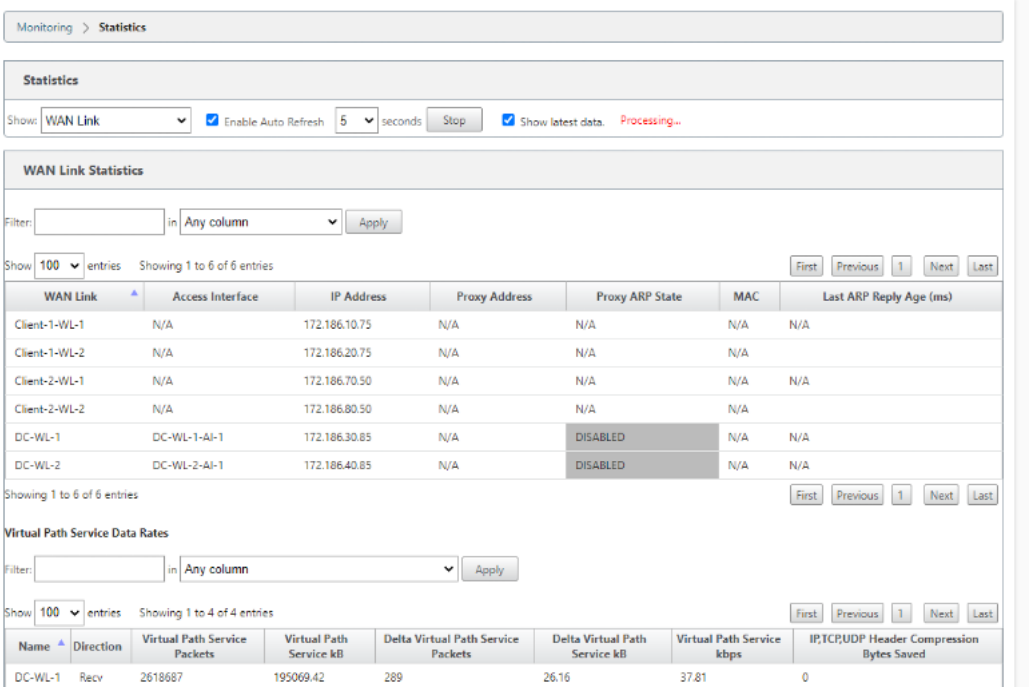
查看 **WAN** 链接允许的速率和拥堵

SD-WAN Web 界面现在允许您查看 WAN 链路和 WAN 链路使用的允许速率，以及 WAN 链路、路径或虚拟路径是否处于拥塞状态。在以前的版本中，此信息仅在 SD-WAN 日志文件中以及通过 CLI 提供。这些选项现在可在 Web 界面中使用，以帮助进行故障排除。

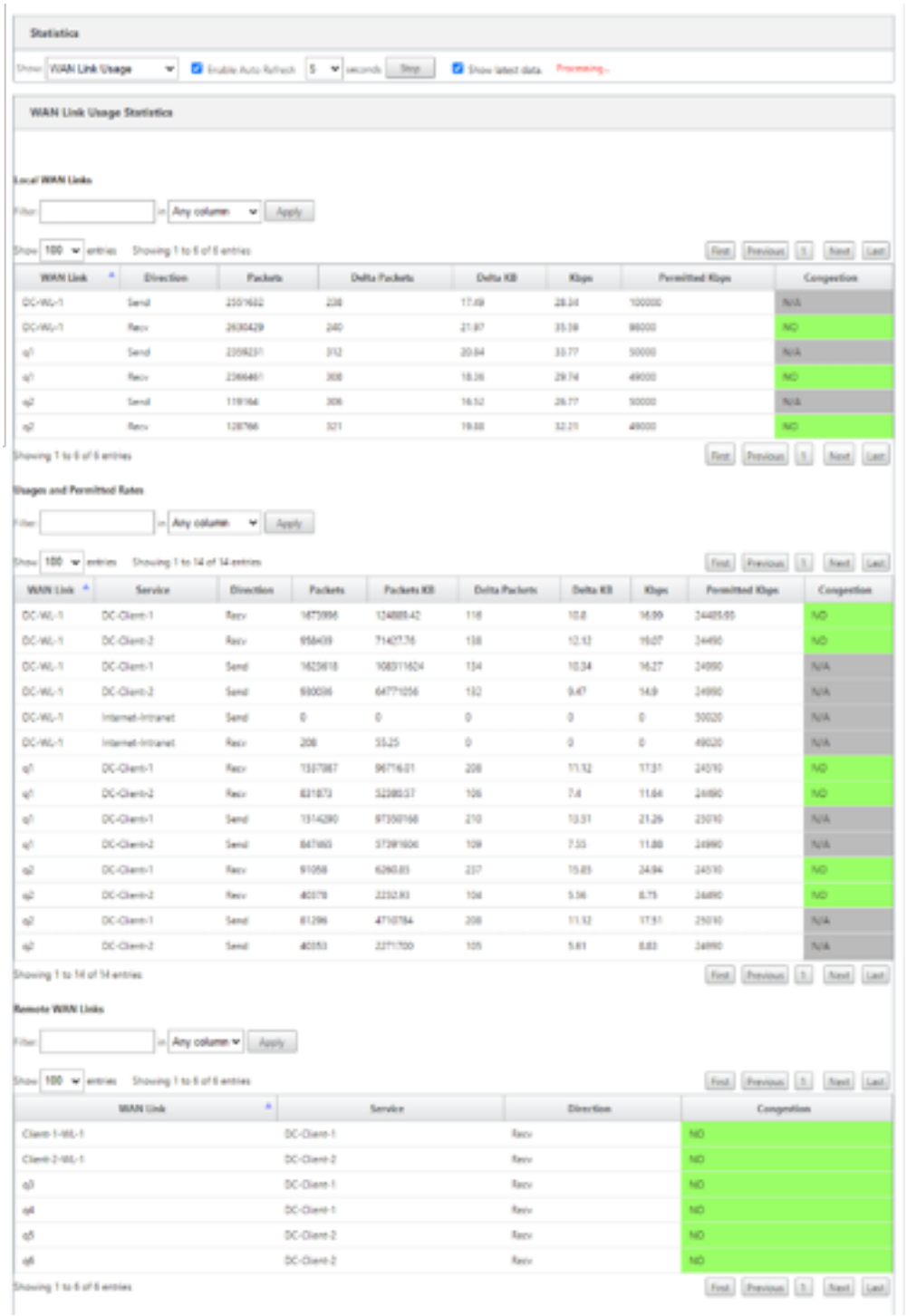
查看允许的费率　允许速率是指特定 WAN 链接、虚拟路径服务、Intranet 服务或 Internet 服务在给定时间点允许使用的带宽量。WAN 链接的允许速率是静态的，并且在 SD-WAN 配置中明确定义。虚拟路径服务、Intranet 服务或 Internet 服务的允许费率将随着时间的推移而波动，以响应拥堵、用户需求和公平分享，但始终大于或等于该服务的最低预留带宽。

监视广域网链接

转到 监控 > 统计信息，然后从 显示 下拉列表中选择 **WAN** 链接。

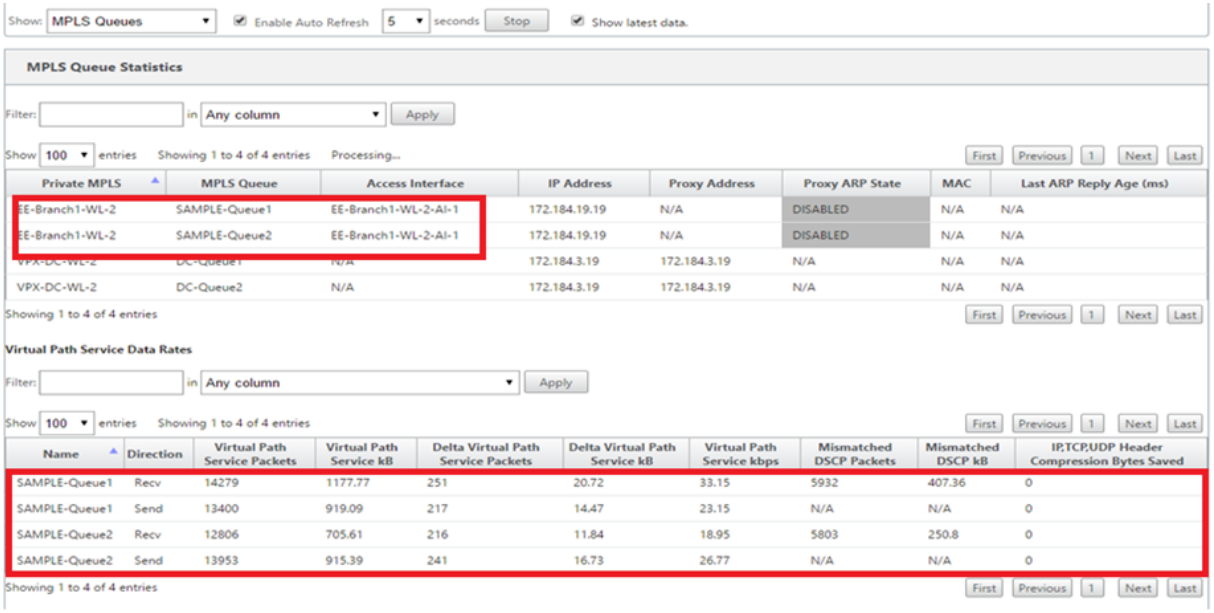


转到 监控 **>** 统计信息，然后从 显示 下拉列表中选择 **WAN** 链接使用情况。



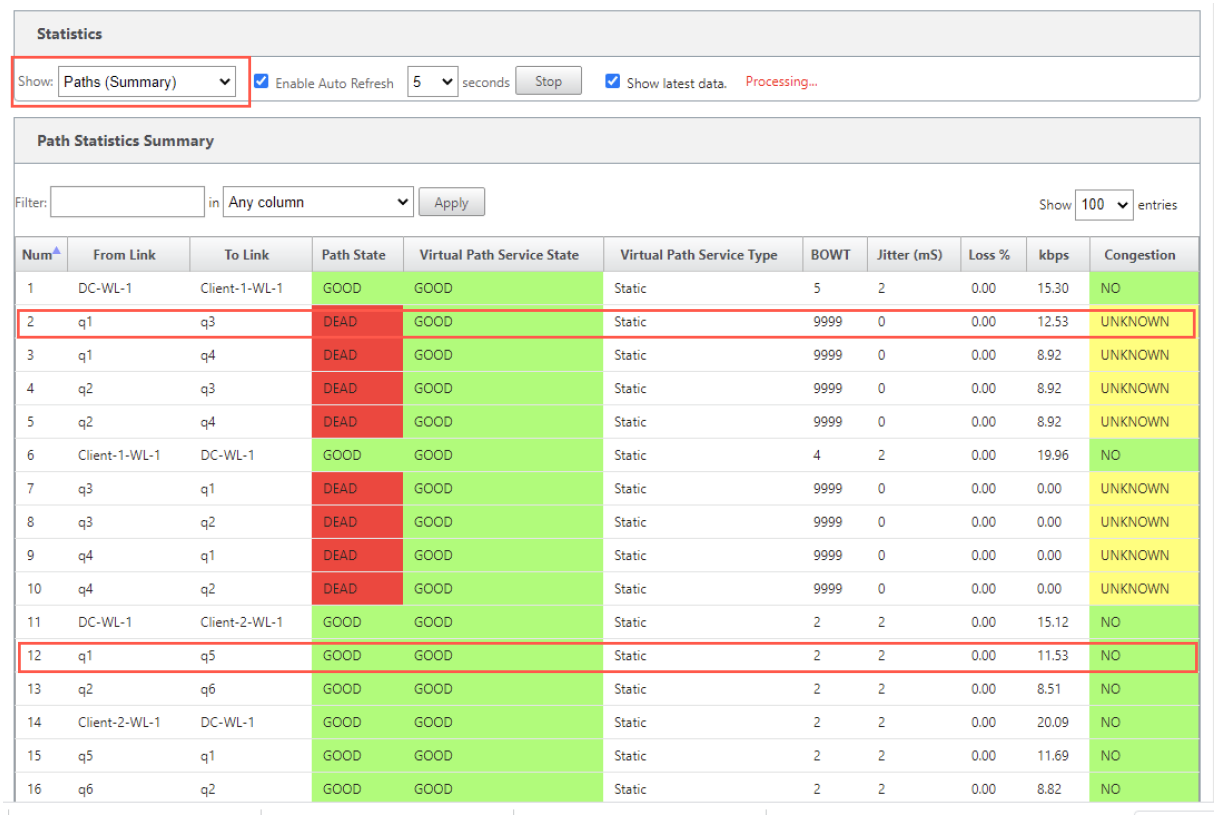
监视 **MPLS** 队列

转到 监控 > 统计信息，然后从 显示 下拉列表中选择 **MPLS** 队 列。



对 **MPLS** 队列进行故障排除

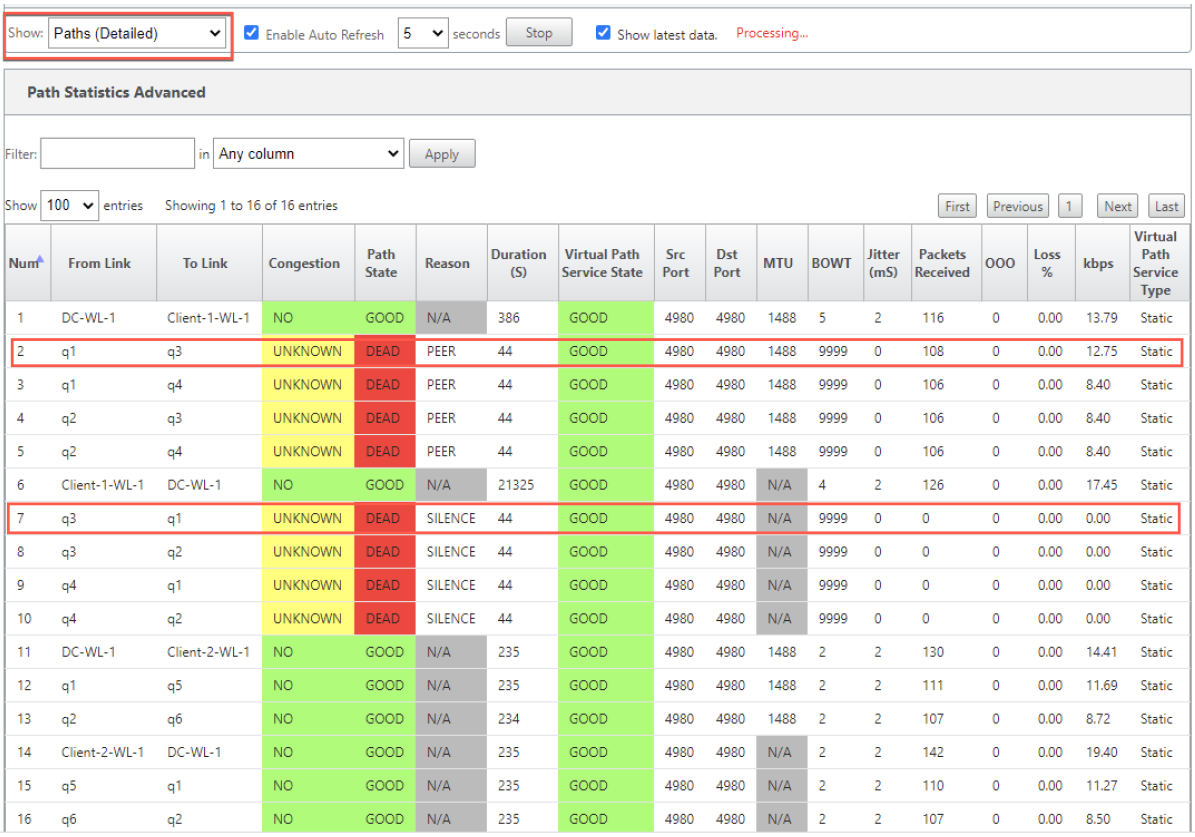
要检查 MPLS 队列的状态，请导航到 监控 **>** 统计信息，然后从 显示 下拉列表中选择 路径（摘要）。在以下示例中，从 MPLS 队列“q1”到“q3”的路径处于“死亡”状态，并以红色显示。从 MPLS 队列“q1”到“q5”的路径处于“良好”状态并显示为绿色。



有关路径的详细信息，请从 显示 下拉列表中选择 路径（详细信息）。有关路径的信息，例如状态的原因、持续时间、源端口、目的端口、MTU

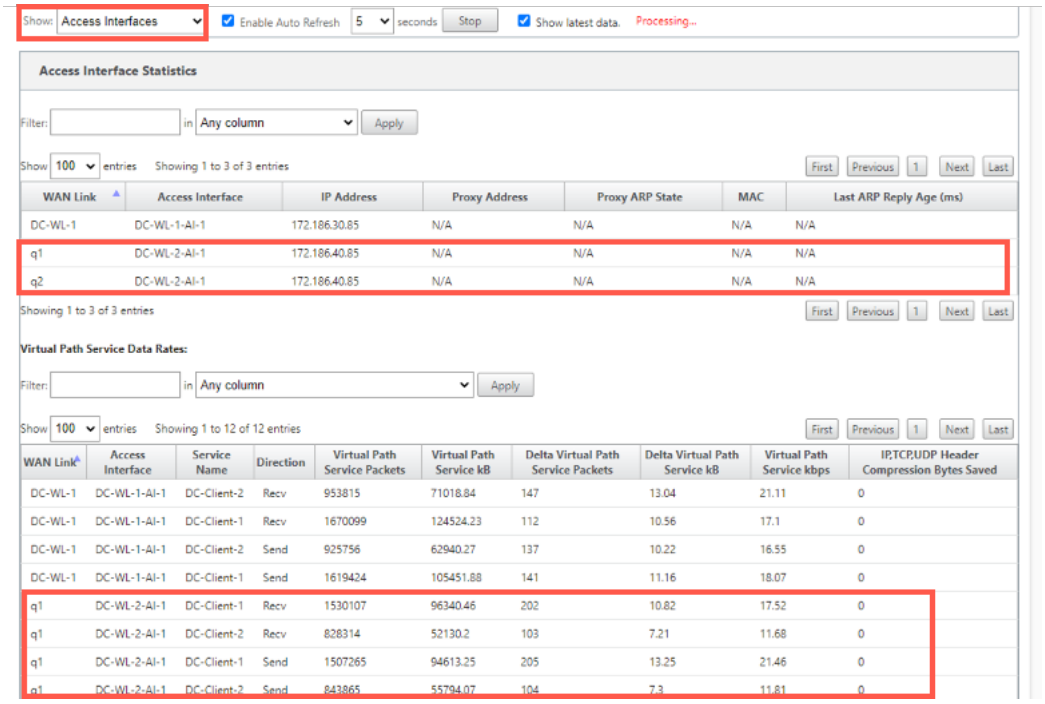
在下面的示例中，从 MPLS 队列“q1”到“q3”的路径处于死亡状态，原因是 PEER。从 MPLS 队列“q3”到“q1”的路径已死，原因是沉默。下表提供了列表（如果可用的原因）及其说明。

原因	说明
网关	由于设备无法访问或检测到网关，因此路径已死
无提示	路径为坏或死，因为设备尚未收到来自对等站点的数据包
损失	由于数据包丢失，路径不正确
同行	对等网站报告路径是坏的

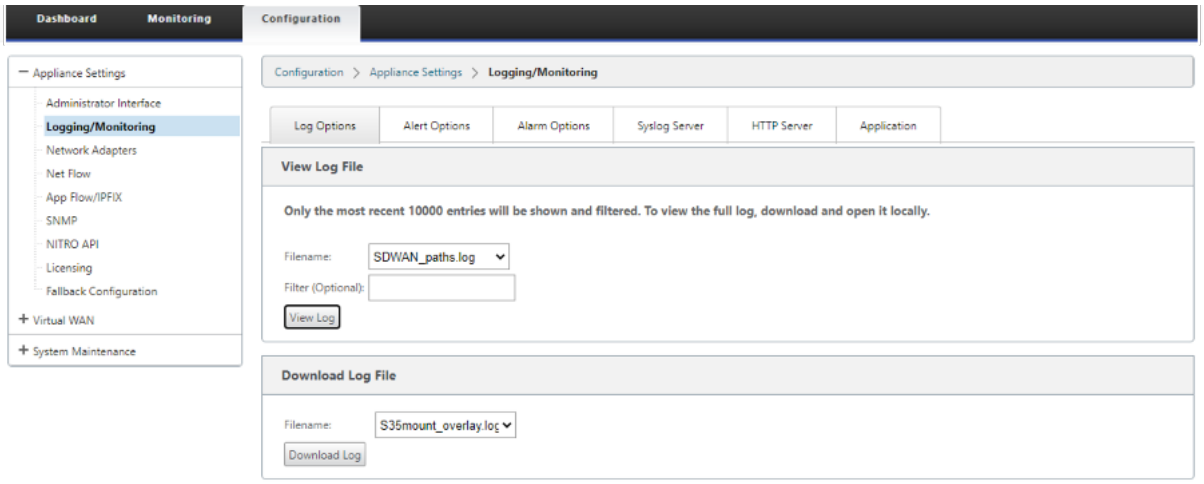


Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	108	0	0.00	12.75	Static
3	q1	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
4	q2	q3	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
5	q2	q4	UNKNOWN	DEAD	PEER	44	GOOD	4980	4980	1488	9999	0	106	0	0.00	8.40	Static
6	Client-1-WL-1	DC-WL-1	NO	GOOD	N/A	21325	GOOD	4980	4980	N/A	4	2	126	0	0.00	17.45	Static
7	q3	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
8	q3	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
9	q4	q1	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
10	q4	q2	UNKNOWN	DEAD	SILENCE	44	GOOD	4980	4980	N/A	9999	0	0	0	0.00	0.00	Static
11	DC-WL-1	Client-2-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	130	0	0.00	14.41	Static
12	q1	q5	NO	GOOD	N/A	235	GOOD	4980	4980	1488	2	2	111	0	0.00	11.69	Static
13	q2	q6	NO	GOOD	N/A	234	GOOD	4980	4980	1488	2	2	107	0	0.00	8.72	Static
14	Client-2-WL-1	DC-WL-1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	142	0	0.00	19.40	Static
15	q5	q1	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	110	0	0.00	11.27	Static
16	q6	q2	NO	GOOD	N/A	235	GOOD	4980	4980	N/A	2	2	107	0	0.00	8.50	Static

要检查与 MPLS 队列关联的访问接口和 IP 地址，请从 显示 下拉列表中选择 访问接口。



您可以下载日志文件进行进一步故障排除。导航到配置 **>** 日志/监视，然后从日志选项选项卡中选择 **SD-WAN_paths.log** 或 **SDWAN_common.log**。



报告

November 16, 2022

应用程序 **QoE**

应用程序 **QoE** 是 SD-WAN 网络中应用程序体验质量的度量标准。它测量通过两个 SD-WAN 设备之间的虚拟路径的应用程序的质量。应用程序 **QoE** 分数是介于 0 到 10 之间的值。它所属的分数范围决定了应用程序的质量。

质量	范围
良好	8–10
一般	4–8
不佳	0–4

应用程序 **QoE** 分数可用于衡量应用程序的质量并识别有问题的趋势。

您可以使用 QoE 配置文件定义实时和交互式设备的质量阈值，并将这些配置文件映射到应用程序或应用程序对象。

> 注意
>
> 要监视应用程序 QoE，启用深度数据包检测至关重要。有关更多信息，请参阅 应用程序分类。

实时应用 **QoE**

实时应用程序的应用程序 QoE 计算使用 Citrix 创新技术，该技术来自 MOS 分数。

默认阈值为：

- 延迟阈值：160 毫秒
- 抖动阈值：30 毫秒
- 数据包丢失阈值：2%

满足延迟、损耗和抖动阈值的实时应用程序流被认为具有良好的质量。

实时应用的 QoE 取决于达到阈值的流量百分比除以流量样本总数。

实时 QoE =（达到阈值的流量样本数量/流量样本总数）* 100

它被表示为 QoE 分数范围从 0 到 10。

您可以使用自定义阈值创建 QoE 配置文件，并应用于应用程序或应用程序对象。

> 注意
>
> 如果网络条件超出了实时流量的配置阈值，则 QoE 值可以为零。

互动应用程序 **QoE**

交互式应用程序的应用程序 QoE 使用基于丢包和突发速率阈值的 Citrix 创新技术。

交互式应用程序对数据包丢失和吞吐量很敏感。因此，我们测量流中的数据包丢失百分比以及入口和出口流量的突发率。

可配置阈值为：

- 数据包丢失百分比。
- 预期出口突发率与入口突发率的比较。

默认阈值为：

- 数据包丢失阈值：1%
- 爆发率：60%

如果满足以下条件，则流程质量良好：

- 流的百分比损失小于配置的阈值。
- 出口突发率至少是已配置的入口突发率百分比。

配置应用程序 **QoE**

将应用程序或应用程序对象映射到默认或自定义 QoE 配置文件。
您可以为实时和交互式流量创建自定义 QoE 配置文件，并使用 QoE 配置文件映射多达 10 个应用程序或应用程序对象。

要通过 Citrix SD-WAN Orchestrator 服务创建自定义 QoE 配置文件，请参阅 应用程序 QoE 配置文件。

HDX QoE

网络参数（如延迟、抖动和数据包丢弃）会影响 HDX 用户的用户体验。引入体验质量（QoE），以帮助用户了解和检查其 ICA 体验质量。QoE 是一个计算指数，指示 ICA 流量性能。用户可以调整规则和策略来改善 QoE。

QoE 是介于 0—100 之间的数值，值越高，用户体验越好。默认情况下，QoE 为所有 ICA/HDX 应用程序启用。

用于计算 QoE 的参数在位于客户端和服务器端的两个 SD-WAN 设备之间进行测量，而不是在客户端或服务器设备本身之间进行测量。延迟、抖动和数据包丢弃是在流级别测量的，它可能与链路级别的统计信息不同。最终主机（客户端或服务器）应用程序可能永远不会知道 WAN 上存在数据包丢失。如果重新传输成功，则流量级数据包丢失率低于链路级丢失。但是，因此，它可能会稍微增加延迟和抖动。

HDX 流量的默认配置使 SD-WAN 能够重新传输数据包，从而改善了由于网络中丢包而丢失的 QoE 索引值。

在 Citrix SD-WAN Orchestrator 的 HDX 控制面板中，您可以查看 HDX 应用程序整体质量的图形表示。HDX 应用分为以下三个质量类别：

质量	QoE 范围
良好	80–100
一般	50–80
不佳	0–50

HDX 控制面板中还会显示 QoE 最少的前五个站点的列表。

不同时间间隔的 QoE 图形表示允许您监视每个站点 HDX 应用程序的性能。

有关如何使用 Citrix SD-WAN Orchestrator 服务配置 HDX QoE 的更多信息，请参阅 HDX 仪表板和报告。

> 注意
>
> - 不要期望 *WAN* 链路延迟、抖动和数据包丢弃总是匹配应用程序延迟、抖动和数据包丢弃。*WAN* 链路丢失与实际 *WAN* 数据包丢失相关，而应用程序丢失是在重新传输后，这低于 *WAN* 链路丢失。
> - *GUI* 中显示的 *WAN* 链接延迟是 *BOWT*（最佳单程时间）。它是链接的最佳指标，作为衡量链接运行状况的一种手段。应用程序 *QoE* 跟踪和计算该应用程序所有数据包的总延迟和平均延迟。这通常与链接 *BOWT* 不匹配。
> - 当 *MSI* 会话启动时，*ICA* 握手期间，会话可能会暂时计为 *4* 个 *SSI*，而不是 *1* 个 *MSI*。握手完成后，它将收敛到 *1* 个 *MSI*。如果转换发生在 *SQL* 表更新之前，它可能会显示在该分钟的 *iCa_Summary* 中。
> - 在会话重新连接时，由于未交换初始协议信息，*SD-WAN* 无法识别 *MSI*，因此每个连接都计为 *SSI* 信息。
> - 对于 *UDP* 连接，连接关闭后，连接最多可能需要 *5* 分钟才能在 *iCa_Summary* 中显示为已关闭并更新。对于 *TCP* 连接，连接关闭后，最多可能需要 *2* 分钟才能在 *ICa_Summary* 中显示为已关闭。
> - 由于 *TCP* 和 *UDP* 之间固有的不同，*TCP* 会话和 *UDP* 会话的 *QoE* 在同一路径上可能不相同。
> - 如果一个用户启动两个虚拟桌面，则用户数将反数为两个。

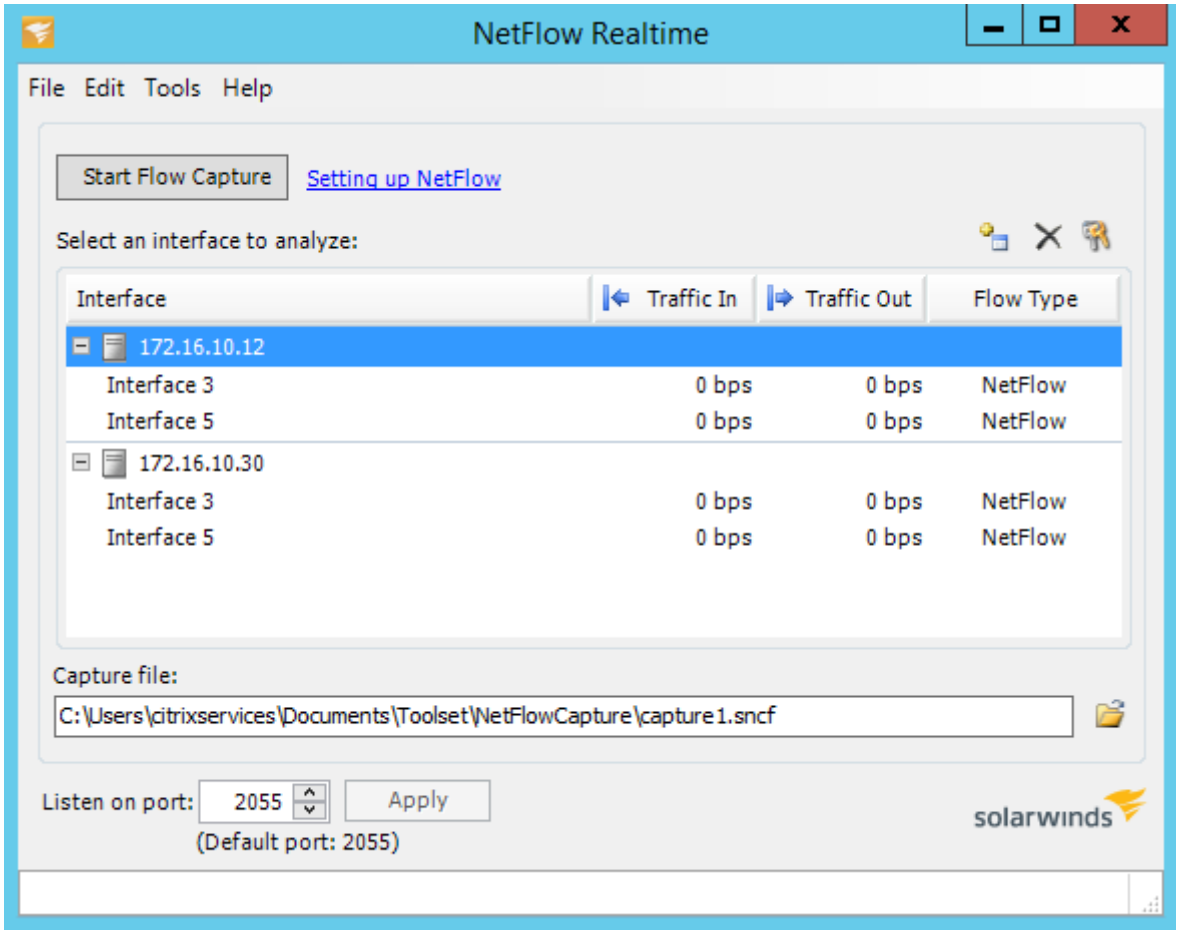
多个净流集热器

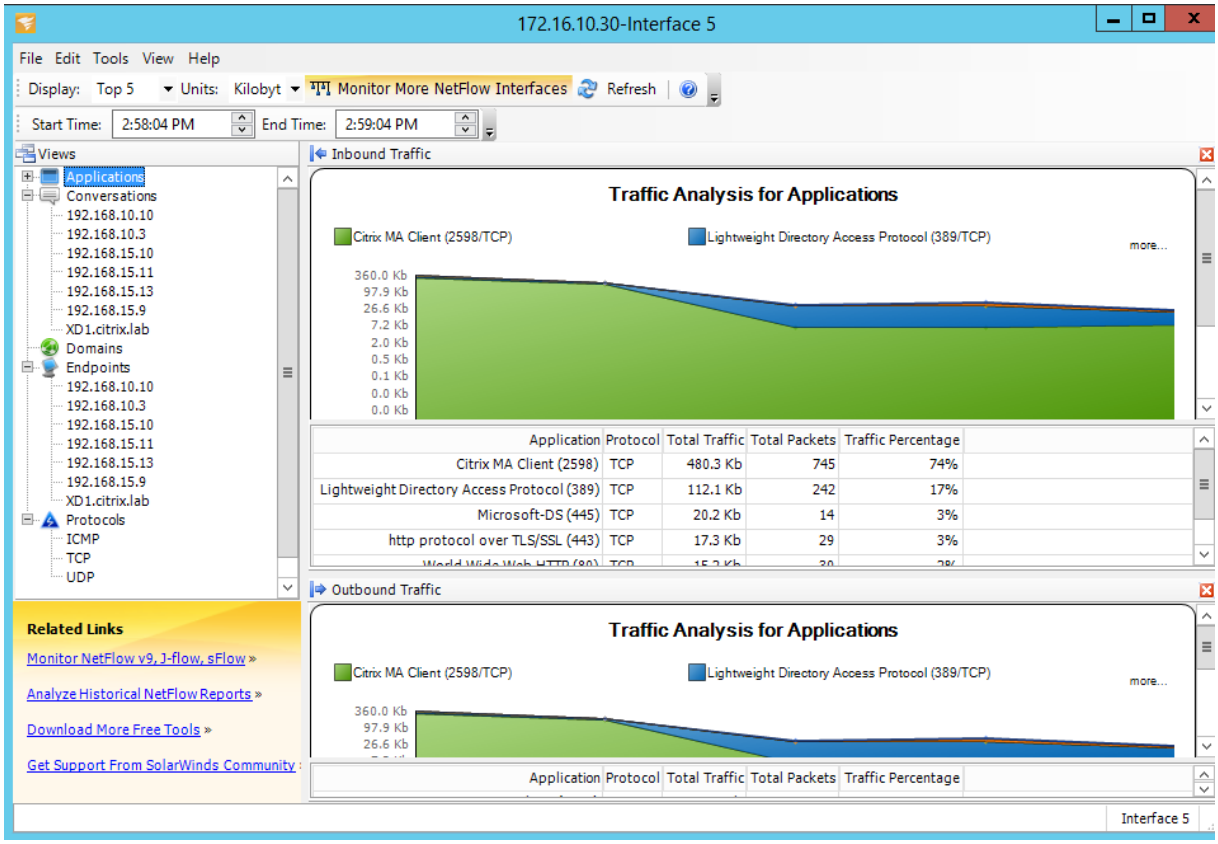
网络流量 收集器在进入或退出 SD-WAN 接口时收集 IP 网络流量。通过分析 Net Flow 提供的数据，您可以确定流量的来源和目的地、服务类别以及流量拥堵的原因。Citrix SD-WAN 设备可配置为将基本的净流量版本 5 统计数据发送到配置的净流量收集器。Citrix SD-WAN 为传输可靠协议所掩盖的流量提供净流支持。由于仅显示 SD-WAN 封装的 UDP 数据包，因此解决方案的 WAN 边缘上的设备无法收集 Net Flow 记录。Citrix SD-WAN 标准版设备支持网络流量。

有关如何使用 Citrix SD-WAN Orchestrator 服务配置网络 流主机的信息，请参阅 Netflow 主机设置。

NetFlow 导出

净流量数据是从 SD-WAN 设备管理端口导出的。在您的网络流量收集器工具上，SD-WAN 设备列为配置的管理 IP 地址（如果未配置 SNMP）。这些接口列为一个用于传入，另一个用于传出（虚拟路径流量）。有关更多信息，请参阅 SNMP。



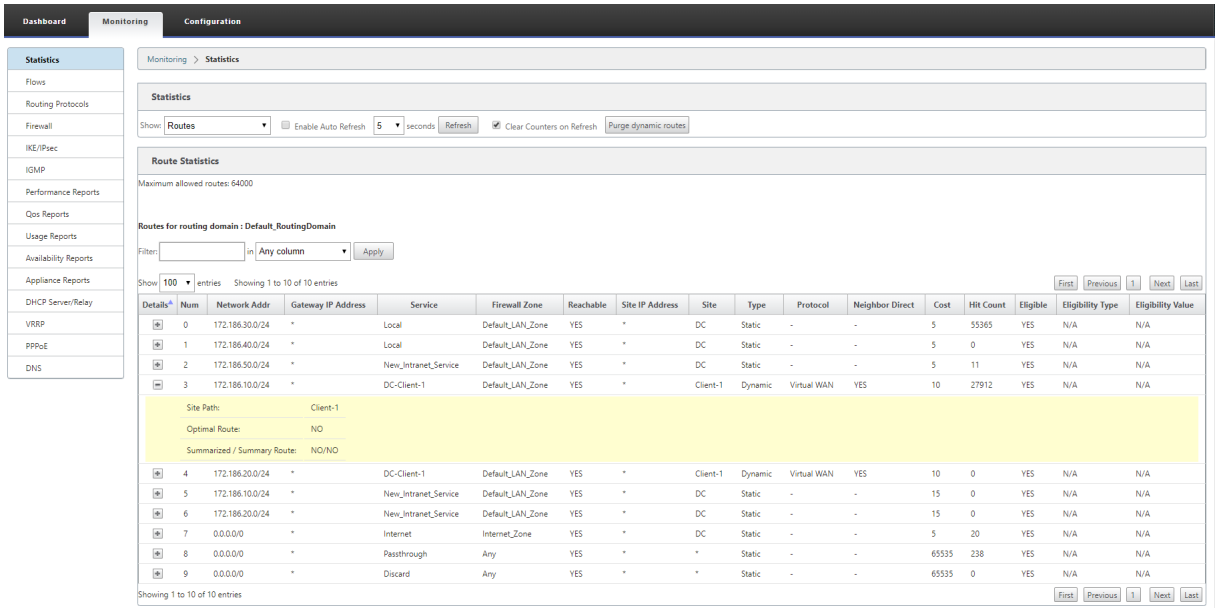


NetFlow 限制

- 在 SD-WAN 标准版设备上启用 Netflow 后，虚拟路径数据将流式传输到指定的 Netflow 收集器。其中一个限制是，无法区分 SD-WAN 正在使用哪个物理 WAN 链接，因为解决方案报告聚合的虚拟路径信息（虚拟路径可能由多个不同的 WAN 路径组成），因此无法筛选不同的 WAN 路径的 Netflow 记录。
- TCP 控制位报告为 N/A，表示 SD-WAN 不遵循基于 RFC 7011 的网络流导出的 Internet 标准，该 RFC 7011 具有 tcpControlBits (IANA) 的元素 ID 为 6。如果没有 TCP 标志，则无法计算流数据中的往返时间 (RTT)、延迟、抖动和其他性能指标。从安全方面来看，如果没有 TCP 标记，Net Flow 收集器无法确定是否存在 FIN、ACK/RST 或 SYN 扫描。

路由统计

要查看 SD-WAN 设备的路由统计信息，请在 SD-WAN GUI 中导航到 监控 > 统计信息 > 路由。



您可以查看以下参数：

- 网络地址：路由的网络地址和子网掩码。
- 详细信息：单击 + 可显示以下信息。
  - 站点路径：站点路径是收到的前缀的真实来源度量。它适用于在多个设备和网状部署中启用 WAN 到 WAN 转发的情况。接收多个此类前缀，管理员可以通过查看站点路径判断前缀属性。

    例如，考虑 Branch1、Branch2 和 MCN 的简单拓扑以及 Geo MCN。Branch1 有一个前缀 172.16.1.0/24，并且必须到达 Branch2。地理 MCN 和 MCN 已启用 WAN 到 WAN 转发。

    前缀 172.16.1.0/24 可以通过 Branch1-MCN-Branch2、Branch1-Geo-Branch2 和 Branch1-MCN-Geo-Branch2 到达 Branch2。对于这些不同的前缀，路由表将使用其站点路径衡量指标进行更新。站点路径衡量指标指示路由前缀的原点以及访问 Branch2 所涉及的成本。
  - 最佳路由：最佳路由表示与所有其他路由相比，该路由是否是到达该子网的最佳路由。此最佳路由将导出到其他站点。
  - 摘要/摘要路由：总结路由是管理员明确配置的路由，用于汇总超网中的多个前缀。汇总路径是汇总路径下的前缀。

    例如，假设我们有一个汇总路由 172.16.0.0/16。这仅是汇总工艺路径，而不是汇总工艺路径。摘要路由具有摘要‘是’和摘要‘否’。如果其他子网很少，例如 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24，则这三个子网在汇总路由线路或超级网络下路由，因此称为汇总路由线路。汇总路由有 是 和 汇总 否。
- 网关 **IP** 地址：用于到达此路由的网关/路由的 IP 地址。
- 服务：Citrix SD-WAN 服务的类型。
- 防火墙区域：路由使用的防火墙区域。

- 可达：路由是否可到达。
- 站点 **IP** 地址：站点的 IP 地址。
- 站点：站点的名称。
- 类型：路由的类型取决于路由学习的来源。局域网端的路由和在配置过程中手动输入的路由是静态路由。从 SD-WAN 或动态路由对等方获取的路由是动态路由。
- 协议：前缀的协议。
  - 本地：设备的本地虚拟 IP。
  - 虚拟 **WAN**：从对等 SD-WAN 设备中学到的前缀。
  - **OSPF**：从 OSPF 动态路由对等体获知的前缀。
  - **BGP**：从 BGP 动态路由对等体学习的前缀。
- 邻居直接：表示子网是否已连接到路由来自该设备的分支机构。
- 成本：用于确定通往目的网络的最佳路径的成本。
- 命中计数：路由为将数据包转发到该子网而被点击的次数。
- 合格：表示路由符合条件，用于在流量处理期间将数据包转发或路由到命中的前缀。
- 资格类型：以下两种资格类型可用。
  - 网关资格：确定网关是否可访问。
  - 路径资格：确定路径是 DEAD 还是非 DEAD。
- 资格值：在系统中创建路由时为配置中的网关或路径选择的值。例如，可以根据路径 MCN-WL-1->BR1-WL-2 调用符合条件的路径。因此，路径部分中此路径的资格值是 MCN-WL-1->BR1-WL-2 值。

路由

November 16, 2022

> 注意
>
> 从 SD-WAN 11.5 版本起，只有通过 Citrix SD-WAN Orchestrator 服务才能支持所有路由配置。有关 Citrix SD-WAN Orchestrator 服务路由配置的信息，请参阅 路由。

动态路由

Citrix SD-WAN 在 动态路由功能下引入了对众所周知的路由 协议的支持。此功能有助于发现 LAN 子网，通告虚拟路径路由，使用 BGP 和 OSPF 协议在网络中更无缝地工作，从而允许 SD-WAN 无缝部署在现有环境中，而无需静态路由配置和优雅的路由器故障切换。

路由过滤

对于启用了“路由学习”的网络，Citrix SD-WAN 可以更好地控制哪些 SD-WAN 路由通告给路由邻居，而不是通告和接受所有路由或不接受路由。

- 导出 筛选器 用于包含 或 排除 使用 OSPF 和 BGP 协议基于 特定 匹配的 播 发路由 标准。
- 导入过滤器用于接受或不接受基于特定匹配条件使用 OSPF 和 BGP 邻居接收的路由。

路由筛选在 SD-WAN 网络（数据中心/分支机构）中的 LAN 路由和虚拟路径路由上实现，并通过 BGP 和 OSPF 将路由通告到非 SD-WAN 网络。

路由汇总

路由汇总减少路由器必须维护的路由数。汇总路径是用于表示多个路径的单个路径。它通过发送单个路由公告来节省带宽，从而减少路由器之间的链接数量。它可以节省内存，因为只保留一个路由地址。通过避免递归查找，CPU 资源可以更有效地使用。

VRRP

虚拟路由器冗余协议 (VRRP) 是一种广泛使用的协议，用于提供设备冗余，以消除静态默认路由环境中固有的单点故障。通过 VRRP，您可以配置两个或更多个路由器以形成一个组。此组显示为具有一个虚拟 IP 地址和一个虚拟 MAC 地址的单个默认网关。

Citrix SD-WAN （版本 10.0 及更高版本）支持 VRP 版本 2 和版本 3 与任何第三方路由器互操作。SD-WAN 设备充当主路由器，并将流量引导到站点之间使用虚拟路径服务。可以将虚拟接口 IP 配置为 VRRP IP，并通过手动将优先级设置为高于对等路由器的值，来将 SD-WAN 设备配置为 VRRP 主服务器。您可以配置播发间隔和抢占选项。

使用 CLI 访问路由功能

您 可以查看与动态路由和协议状态相关的其他信息。键入以下命令和语法以访问路由守护程序并查看命令列表。

‘

dynamic_routing?

‘

SD-WAN 叠加路由

September 2, 2022

Citrix SD-WAN 可在远程站点、数据中心和云网络之间提供弹性强大的连接。SD-WAN 解决方案可以通过在网络中的 SD-WAN 设备之间建立通道来实现这一目标，通过应用覆盖现有底层网络的路由表来实现站点之间的连接。SD-WAN 路由表可以完全替换或与现有路由基础结构共存。

Citrix SD-WAN 设备根据可用性、丢失、延迟、抖动和拥塞特性统一测量可用路径，并根据每个数据包选择最佳路径。这意味着从站点 A 到站点 B 选择的路径不一定是从站点 B 到站点 A 选择的路径。给定时间的最佳路径是在每个方向上单独选择的。Citrix SD-WAN 提供基于数据包的路径选择，可快速适应任何网络更改。SD-WAN 设备可以检测仅在两个或三个数据包丢失后的路径中断，从而允许应用程序流量无缝亚秒级故障转移到下一个最佳 WAN 路径。SD-WAN 设备在约 50 毫秒内重新计算每个 WAN 链路状态。下面的文章提供了 Citrix SD-WAN 网络中的详细路由配置。

Citrix SD-WAN 路由表

SD-WAN 允许特定站点的静态路由条目，以及通过支持的路由协议（如 OSPF、eBGP 和 iBGP）从底层网络获知的路由条目。路由不仅由其下一个跃点定义，而且由其服务类型定义。这决定了路径的转发方式。以下是正在使用的主要服务类型：

- 本地服务：表示 SD-WAN 设备本地的任何路由或子网。这包括虚拟接口子网（自动创建本地路由）以及路由表中定义的任何本地路由（具有本地下一个跃点）。路由将播发到具有到此本地站点的虚拟路径的其他 SD-WAN 设备，当作为合作伙伴信任时，该路由将配置为此路由。

> 注意
>
> 添加默认路径和汇总路径作为本地路径时要谨慎，因为这些路径可能会导致其他站点的虚拟路径路径。始终检查路由表以确保正确的路由生效。

- 虚拟路径—表示从可通过虚拟路径访问的远程 SD-WAN 站点学习的任何本地路由。这些路由通常是自动的，但是可以在站点手动添加虚拟路径路由。此路由的任何流量都会转发到此目标路由（子网）的定义虚拟路径。
- **Intranet** —表示可通过专用 WAN 链路（MPLS、P2P、VPN 等）访问的路由。例如，位于 MPLS 网络上但没有 SD-WAN 设备的远程分支。假定这些路由必须转发到某个 WAN 路由器。默认情况下不启用 Intranet 服务。匹配此路由（子网）的任何流量都被分类为此设备的 Intranet，以便传送到没有 SD-WAN 解决方案的站点。

> 注意
>
> 请注意，添加 Intranet 路由时不存在下一个跃点，而是转发到 Intranet 服务。该服务与给定的 WAN 链接相关联。

- **Internet** —这类似于 Intranet，但用于定义流向公共 Internet WAN 链接而不是专用 WAN 链接的流量。一个独特的区别是，Internet 服务可以与多个 WAN 链接关联，并设置为负载平衡（每个流）或处于活动/备份。启用 Internet 服务时创建默认 Internet 路由（默认情况下处于关闭状态）。与此路由（子网）匹配的任何流量都被归类为 Internet，以便传输到公共 Internet 资源。

> 注意
>
> Internet 服务路由可以播发到其他 SD-WAN 设备或阻止导出，具体取决于您是否通过虚拟路径进行 Internet 访问。

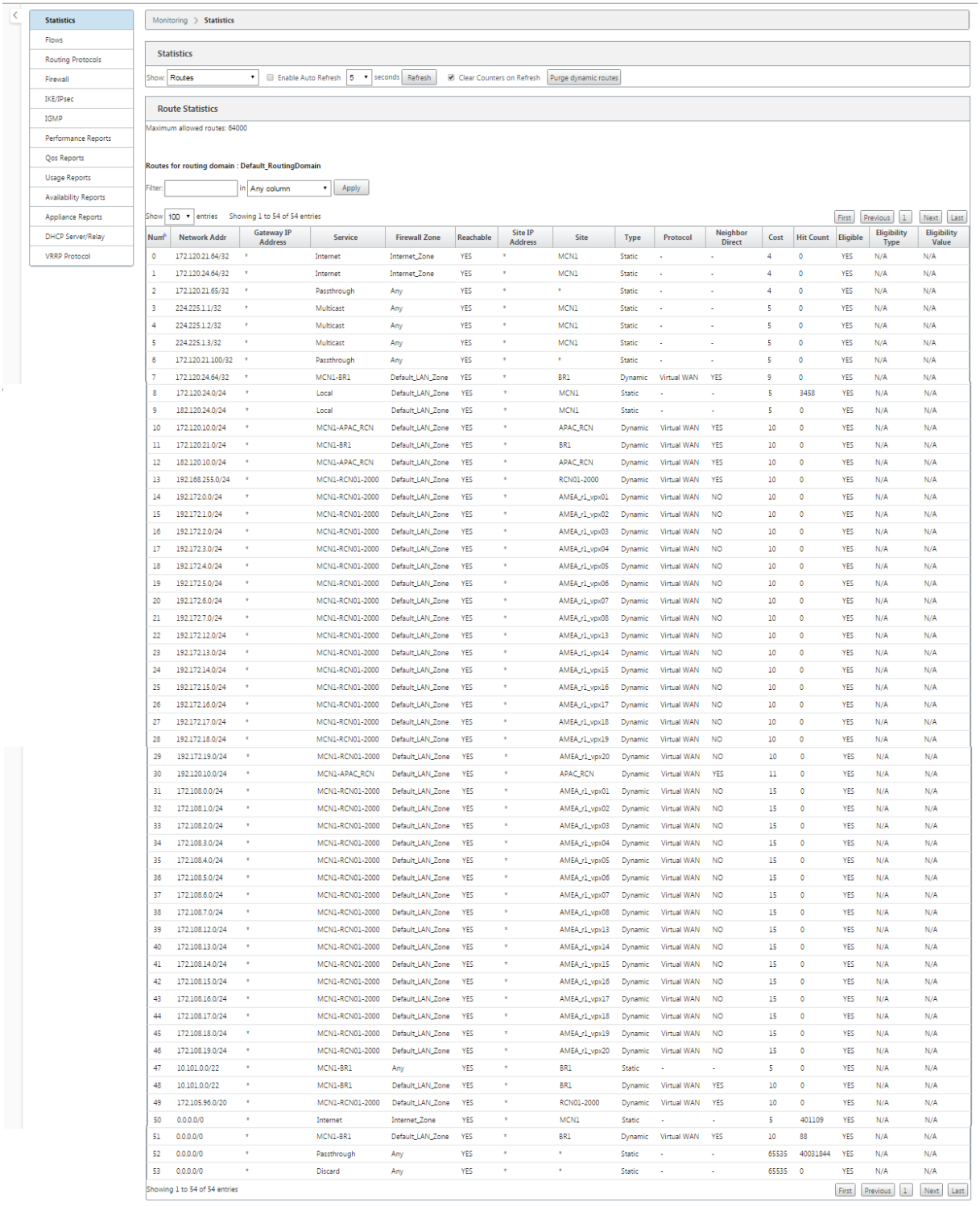
- 直通—当设备处于串联模式时，此服务作为最后手段或覆盖服务。如果目标 IP 地址与任何其他路由无法匹配，则 SD-WAN 设备只需将其转发到下一个跃点 WAN 链接。默认路由：16 条直通路由的 0.0.0.0/0 成本是自动创建

的。当 SD-WAN 设备部署在路径外或在边缘/网关模式下时，直通不起作用。匹配此路由（子网）的任何流量都被归类为此设备的直通。建议尽可能限制直通流量。

> 注意
>
> 在执行 POC 时，直通可能很有用，以避免必须配置大量路由，但在生产环境中要小心，因为 SD-WAN 不考虑发送到直通的流量的 WAN 链路利用率。当故障排除问题，并且您希望通过虚拟路径将某个 IP 流从交付中取出时，这也很有帮助。

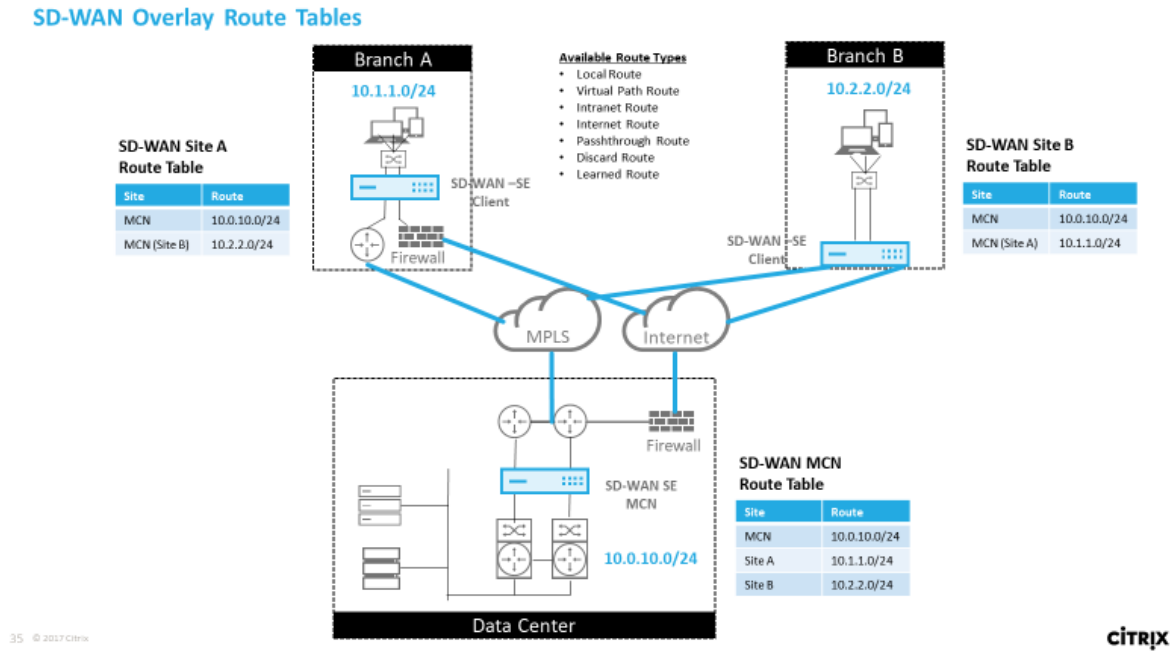
- 丢弃 -这不是服务，而是最后的手段路由，如果匹配，则会丢弃数据包。通常，当 SD-WAN 设备部署出路径时，不会发生这种情况。您必须有 Intranet 服务或本地路由作为捕获所有路由，否则流量将被丢弃，因为没有直通服务（即使存在直通默认路由）。

可以在“监视”>“统计信息”页面上 监 视本地客户端节点的路由表，同时为“显示”下拉列表选择了路由。



远程分支机构子网的每条路由都通过虚拟路径通告为服务，而 站 点列填充目标作为本地子网所在的客户端节点。

在以下示例中，在启用 **WAN** 到 **WAN** 转发（路由导出）的情况下，分支 A 具有通过 MCN 的分支 B 子网的路由表条目 (10.2.2.0/24) 作为下一跳。



Citrix SD-WAN 流量在已定义路由上如何匹配

Citrix SD-WAN 上定义的路由的匹配过程基于目标子网的最长前缀匹配（类似于路由器操作）。路由越具体，匹配的更改就越高。排序按以下顺序完成：

1. 最长前缀匹配
2. 成本
3. 服务

因此，/32 路由始终位于 /31 路由之前。对于两条 /32 路径，成本 4 路径始终位于成本 5 路径之前。对于两个 /32 成本 5 路由，路由是根据有序的 IP 主机选择. 服务顺序如下：本地、虚拟路径、内联网、Internet 、直通、丢弃。

例如，请考虑以下两条路由，如下所示：

- 192.168.1.0/24 成本 5
- 192.168.1.64/26 成本 10

发往 192.168.1.65 主机的数据包将使用后一条路由，即使开销较高。基于此，通常情况下，配置只适用于打算通过虚拟路径叠加传递的路由，而其他流量则捕获所有路由，例如直通服务的默认路由。

路由可以在具有相同前缀的站点节点路由表中进行配置。然后，断开连接转到路由开销、服务类型（虚拟路径、Intranet、Internet 等）和下一跳 IP。

Citrix SD-WAN 路由数据包流

- LAN 到 WAN（虚拟路径）流量路由匹配：

1. 传入流量由 LAN 接口接收并进行处理。
2. 将接收的帧与路由表进行比较，以获得最长前缀匹配。
3. 如果找到匹配项，则该帧将由规则引擎处理，并在流数据库中创建流。

- WAN 到 LAN（虚拟路径）流量路由匹配：
  1. 虚拟路径流量由 SD-WAN 从通道接收并进行处理。
  2. 设备比较源 IP 地址以查看源是否为本地。
     - 如果是—则符合 WAN 条件并将 IP 目标与路由表/虚拟路径匹配。
     - 如果没有—则启用 WAN 到 WAN 转发检查。
  3.（禁用 WAN 到 WAN 转发）基于本地路由转发到 LAN。
  4.（启用 WAN 到 WAN 转发）基于路由表转发到虚拟路径。
- 非虚拟路径流量：
  1. 传入流量在 LAN 接口上接收并进行处理。
  2. 将接收的帧与路由表进行比较，以获得最长前缀匹配。
  3. 如果找到匹配项，则该帧将由规则引擎处理，并在流数据库中创建流。

Citrix SD-WAN 路由协议支持

Citrix SD-WAN 版本 9.1 在配置中引入了 OSPF 和 BGP 路由协议。将路由协议引入 SD-WAN 使 SD-WAN 能够更轻松地集成到更复杂的底层网络中，其中路由协议正在积极使用。通过在 SD-WAN Orchestrator 服务上启用相同的路由协议，可以更轻松地配置表示使用 SD-WAN 覆盖的子网。此外，路由协议使 SD-WAN 和非 SD-WAN 站点之间的通信能够使用通用路由协议直接与现有客户边缘路由器进行通信。无论 SD-WAN 的部署模式（内联模式、虚拟内联模式或边缘/网关模式）如何，都可以完成参与底层网络中运行的路由协议的 Citrix SD-WAN。此外，SD-WAN 可以在“仅学”模式下部署，在这种模式下，SD-WAN 可以接收路由，但不能将路由通告回底层。当将 SD-WAN 解决方案引入路由基础结构复杂或不确定的网络时，这很有用。

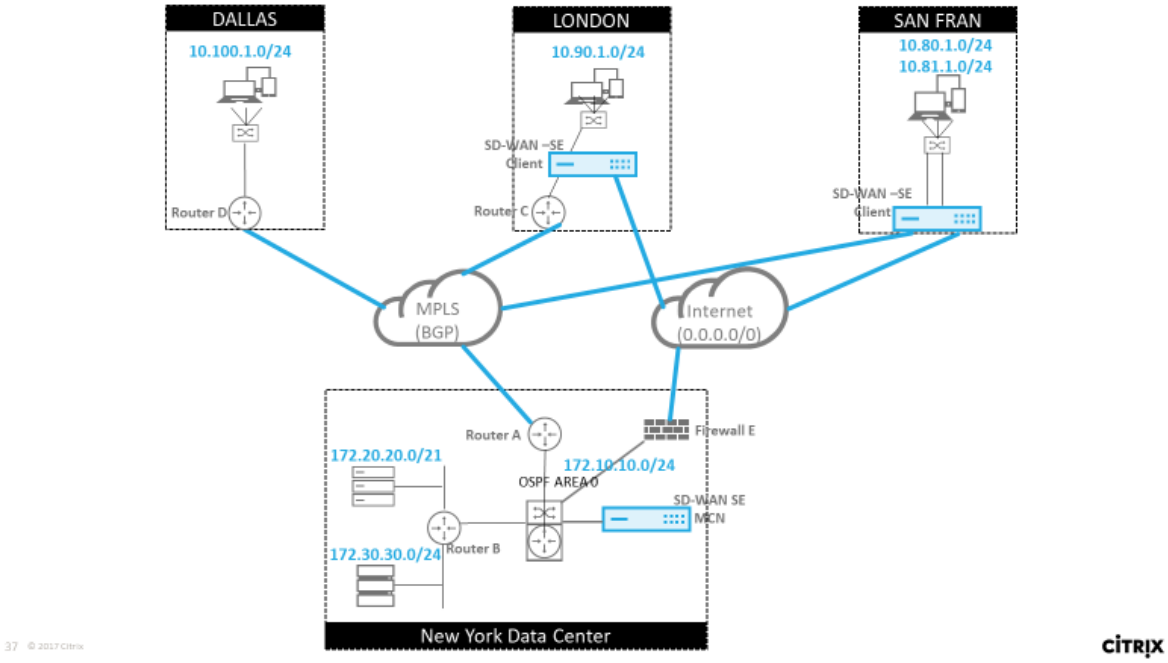
> 重要
>
> 如果您不小心，很容易泄漏不需要的路由。

SD-WAN 虚拟路径路由表用作外部网关协议 (EGP)，类似于 BGP（思考站点到站点）。例如，当 SD-WAN 通告从 SD-WAN 设备到 OSPF 的路由时，它们通常被视为站点和协议的外部。

> 注意
>
> 请注意在整个基础结构（跨 WAN）中具有 IGP 的环境，因为它确实使 SD-WAN 播发路由的使用方式复杂化。EIGRP 广泛应用于市场，SD-WAN 不与该协议互操作。

在 SD-WAN 部署中引入路由协议的一个挑战是，在启用 SD-WAN 服务并在网络中运行之前，路由表才可用，因此不建议最初启用 SD-WAN 设备的通告路由。使用导入和导出筛选器逐步引入 SD-WAN 上的路由协议。

让我们仔细看看下面的例子：



在此示例中，我们检查路由协议使用案例。前面的网络有四个地点：纽约、达拉斯、伦敦和旧金山。我们在其中三个地点部署 SD-WAN 设备，并利用 SD-WAN 创建混合 WAN 网络，其中 MPLS 和 Internet WAN 链接将用于提供虚拟化 WAN。由于达拉斯没有 SD-WAN 设备，我们必须考虑如何最好地集成到该站点的现有路由协议，以确保底层和 SD-WAN 叠加网络之间的完全连接。

在示例网络中，eBGP 在 MPLS 网络的所有四个位置之间使用。每个位置都有自己的自治系统号码 (ASN)。

在纽约数据中心中，OSPF 正在运行，以便将核心数据中心子网公告到远程站点，并宣布纽约防火墙 (E) 的默认路由。在此示例中，所有 Internet 流量都会回传到数据中心，即使伦敦分支机构和旧金山分支机构具有通往 Internet 的路径。

旧金山站点还必须注意没有路由器。SD-WAN 部署在边缘/网关模式下，该设备是旧金山子网的默认网 Gateway，并且还参与 MPLS 的 eBGP。

- 使用纽约数据中心，请注意 SD-WAN 部署在虚拟内联模式下。目的是参与现有的 OSPF 路由协议，以便将流量作为首选 Gateway 转发到设备。
- 伦敦站点以传统的内联模式部署。上游 WAN 路由器 (C) 仍然是伦敦子网的默认网 Gateway。
- 旧金山站点是该网络中新引入的站点，SD-WAN 计划以边缘/网关模式部署，并充当新旧金山子网的默认网 Gateway。

在实施 SD-WAN 之前，请查看一些现有的底层路由表。

纽约核心路由器 **B**:


```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

本地纽约子网 (172.x.x.x) 可在路由器 B 上直接连接，并从路由表中确定默认路由为 172.10.10.3（防火墙 E）。此外，我们可以看到达拉斯（10.90.1.0/24）和伦敦（10.100.1.0/24）的子网可以通过 172.10.10.1（MPLS 路由器 A）获得。路由成本表明它们是从 eBGP 学习的。

> 注意
>
> 在提供的示例中，旧金山未作为路由列出，因为我们尚未在边缘/网关模式下为该网络部署带 SD-WAN 的站点。

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:09:52
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h09m
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192.168.65.0/24 is directly connected, eth0
```

对于纽约广域网路由器 (A)，OSPF 通过 eBGP 了解到跨 MPLS 学习的路由和路由列出。请注意路由成本。与 OSPF 110/10 相比，BGP 默认情况下是低于 20/1 的管理域和成本。

达拉斯路由器 **D**:

对于达拉斯 WAN 路由器 (D)，所有路由都通过 MPLS 了解。

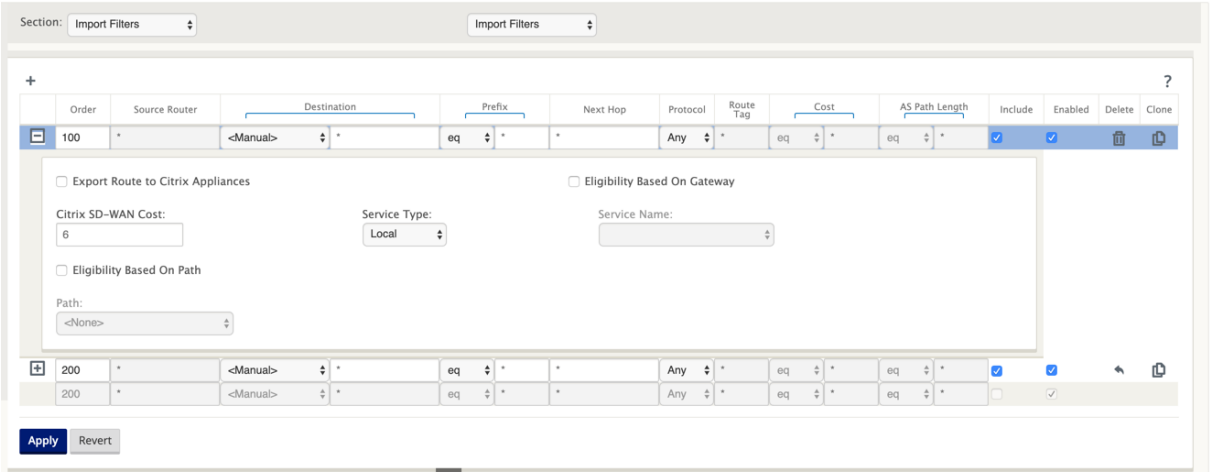

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

> 注意
>
> 在此示例中，您可以忽略 192.168.65.0/24 子网。这是一个管理网络，与示例无关。所有路由器都连接到管理子网，但没有在任何路由协议中通告。

eBGP 彼此之间的对等位置。每个 ASN 是不同的。

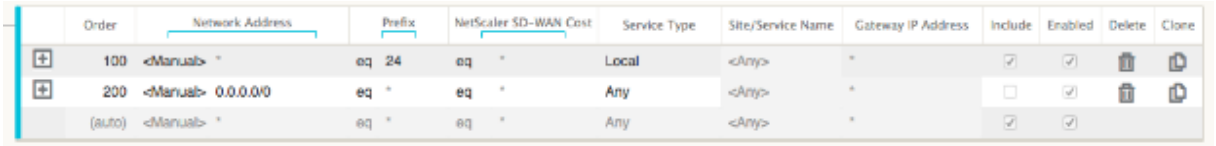
了解如何在虚拟路径路由表和正在使用的动态路由协议之间传递路由非常重要。以不利的方式创建路由循环或公告路由很容易。过滤器机制使我们能够控制进出路由表的内容。我们依次考虑每个位置。

- 旧金山位置有两个本地子网 **10.80.1.0/24** 和 **10.81.1.0/24**。我们希望通过 eBGP 对它们进行广告宣传，以便像达拉斯这样的站点仍然可以通过底层网络到达旧金山站点，而像伦敦和纽约这样的站点仍然可以通过虚拟路径叠加网络到达旧金山。我们还希望了解 EbGP 到所有站点的可达性，以防 SD-WAN 虚拟路径覆盖出现故障，环境必须回退到仅使用 MPLS。我们也不想重新读取 SD-WAN 从 eBGP 学习到 SD-WAN 路由器的任何内容。为此，必须按以下方式配置筛选器：
- 从 eBGP 导入所有路由。不要读取/导出到 SD-WAN 设备的路由。



- 出口本地航线至 eBGP

导出的默认规则是导出所有内容。规则 200 用于覆盖故障规则，而不是重新读取路由。所有与任何前缀 SD-WAN 匹配的路由已经通过虚拟路径了解到。



Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
100	<Manual> *	eq 24	eq *	Local	<Any>	*	✓	✓		
200	<Manual> 0.0.0.0/0	eq *	eq *	Any	<Any>	*		✓		
(auto)	<Manual> *	eq *	eq *	Any	<Any>	*	✓	✓		

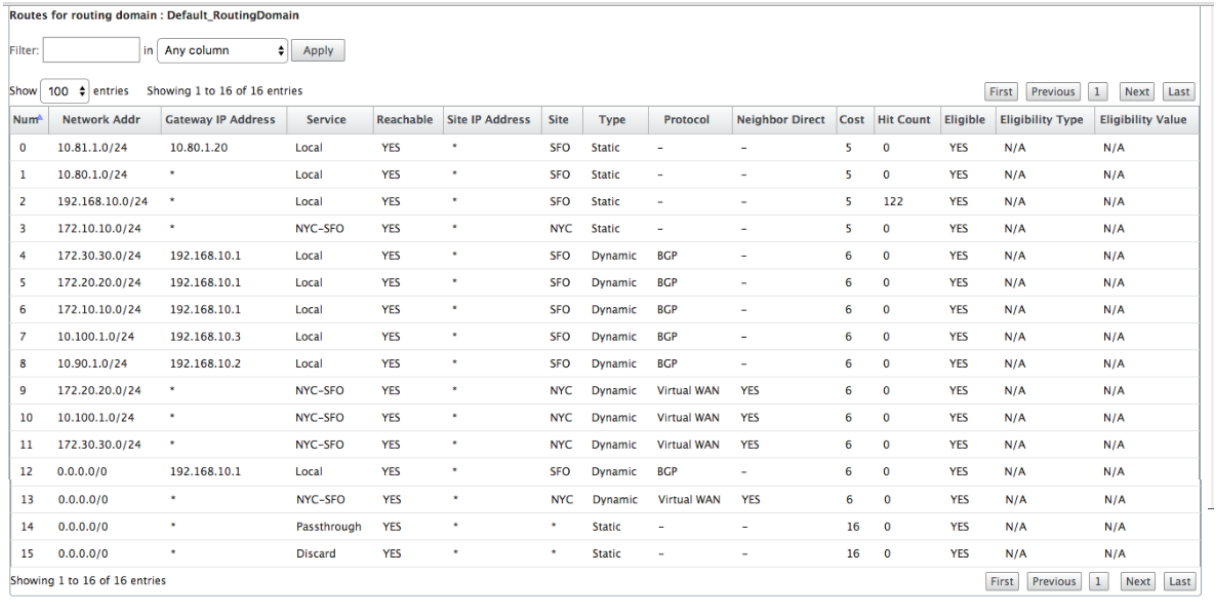
部署 Citrix SD-WAN 设备后，我们可以刷新查看达拉斯站点的 BGP 路由器的路由表。我们看到 10.80.1.0/24 和 10.81.1.0/24 的子网正在通过旧金山 SD-WAN 的 eBGP 正确看到。

达拉斯路由器 **D**：

```
vyos@VYATTA-ROUTER-D:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0
```

此外，可以在 监 视 > 统计信息 > 显示路由 页面上查看 Citrix SD-WAN 路由表。

旧金山 **Citrix SD-WAN**：



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 16 of 16 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	10.81.1.0/24	10.80.1.20	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
1	10.80.1.0/24	*	Local	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
2	192.168.10.0/24	*	Local	YES	*	SFO	Static	-	-	5	122	YES	N/A	N/A
3	172.10.10.0/24	*	NYC-SFO	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
4	172.30.30.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
5	172.20.20.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
6	172.10.10.0/24	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	192.168.10.3	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	10.90.1.0/24	192.168.10.2	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
9	172.20.20.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
10	10.100.1.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
11	172.30.30.0/24	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
12	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	6	0	YES	N/A	N/A
13	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 16 of 16 entries First Previous 1 Next Last

Citrix SD-WAN 显示了学习的所有路由，包括通过虚拟路径叠加可用的路由。

让我们考虑 172.10.10.0/24，它位于纽约数据中心。通过两种方式学习这条路由：

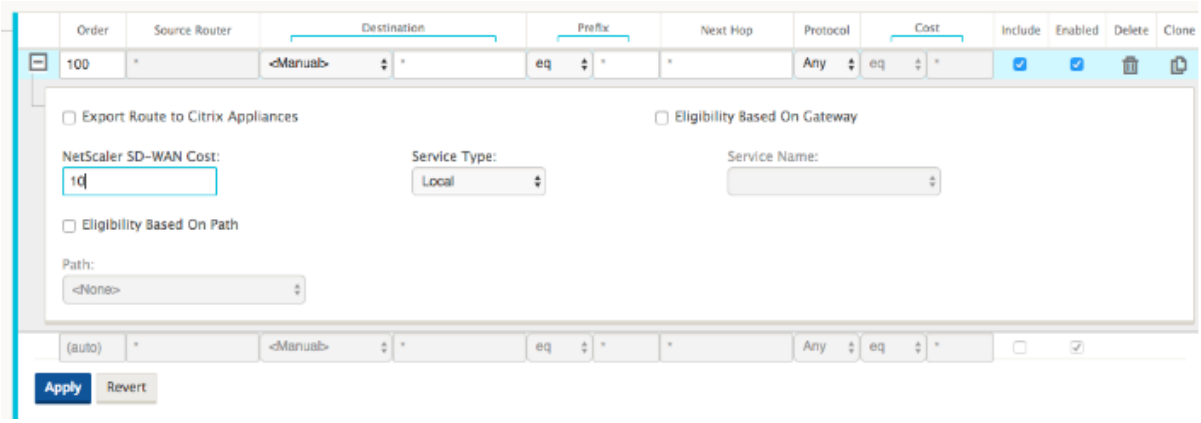
- 作为虚拟路径路由（数字 3），服务 = NYC-SFO，开销为 5 并键入静态。这是由 SD-WAN 设备在纽约宣传的本地子网。它是静态的，因为它直接连接到设备，或者它是在配置中输入的手动静态路由。它可以访问，因为站点之间的虚拟路径处于工作/启动状态。
- 作为通过 BGP（6 号）的广告路由，成本为 6。这现在被认为是一个后备路由。

由于前缀相等且开销不同，SD-WAN 将使用虚拟路径路由，除非在这种情况下，回退路由是通过 BGP 获取的。

现在，让我们假设路由线路 172.20.20.0/24。

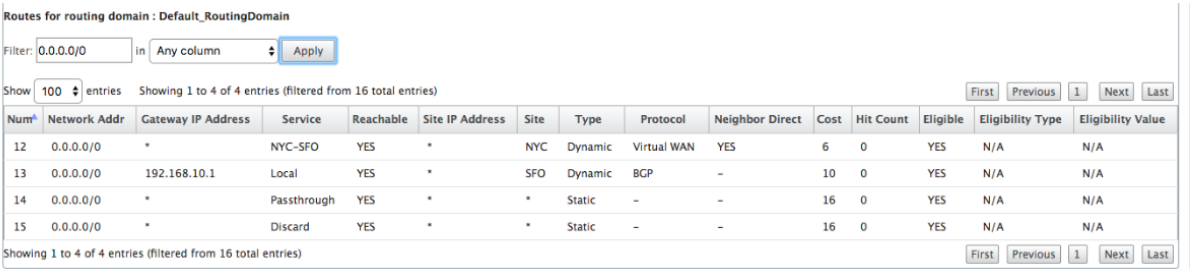
- 这是作为虚拟路径路由学习的（数字 9），但具有动态类型，开销为 6。这意味着远程 SD-WAN 设备通过路由协议（在本例中为 OSPF）了解此路由。默认情况下，路径成本较高。
- SD-WAN 还以相同的开销通过 BGP 获取此路由，因此在这种情况下，此路由可能优先于虚拟路径路由。

为了确保正确的路由，我们必须增加 BGP 路由成本，以确保我们是否有虚拟路径路由，它是首选路由。这可以通过将导入筛选器路径权重调整为高于默认值 6 来完成。



进行调整后，我们可以刷新旧金山设备上的 SD-WAN 路由表以查看调整的路由成本。使用筛选器选项聚焦显示的列表。

最后，让我们来看看旧金山 SD-WAN 上学习的默认路由。我们想要回传所有的 Internet 流量到纽约。我们可以看到，我们使用虚拟路径发送它，如果它已启动，或通过 MPLS 网络作为后备。


Routes for routing domain : Default_RoutingDomain

Filter: 0.0.0.0/0 in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
12	0.0.0.0/0	*	NYC-SFO	YES	*	NYC	Dynamic	Virtual WAN	YES	6	0	YES	N/A	N/A
13	0.0.0.0/0	192.168.10.1	Local	YES	*	SFO	Dynamic	BGP	-	10	0	YES	N/A	N/A
14	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
15	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 4 of 4 entries (filtered from 16 total entries) First Previous 1 Next Last

我们还看到一个直通和丢弃路由与成本 16. 这些是无法删除的自动路由。如果设备是内联的，则将使用直通路由作为最后的手段，因此如果数据包无法匹配到更具体的路由，SD-WAN 会将其传递到接口组的下一个跃点。如果 SD-WAN 超出路径或处于边缘/网关模式，则没有直通服务，在这种情况下，SD-WAN 使用默认丢弃路由丢弃数据包。命中计数指示每条路由中的数据包数，这在故障排除时非常有用。

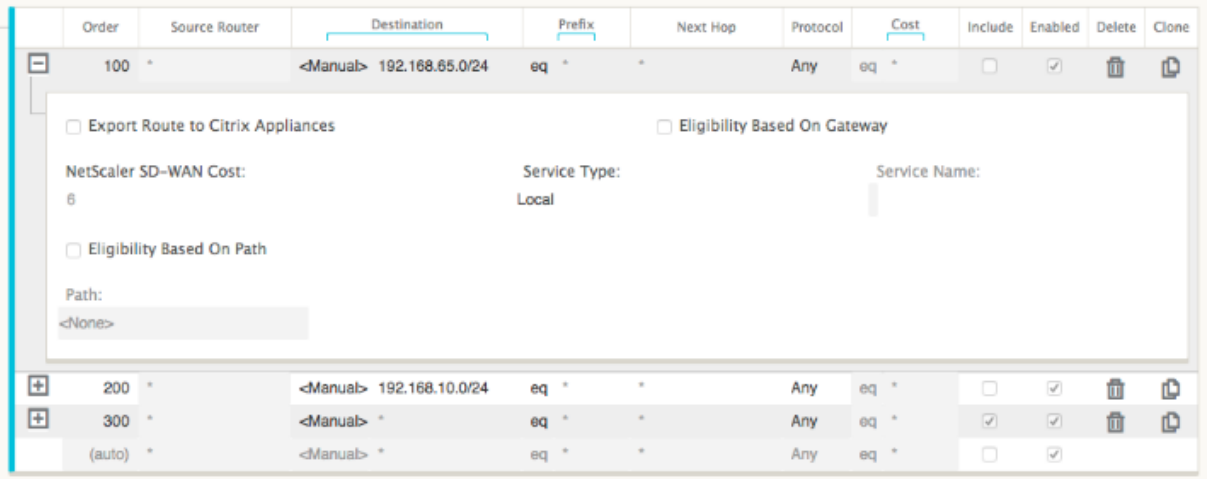
现在关注纽约站点，我们希望在虚拟路径处于活动状态时将发往远程站点（伦敦和旧金山）的流量定向到 SD-WAN 设备。

纽约站点中有多个子网可用：

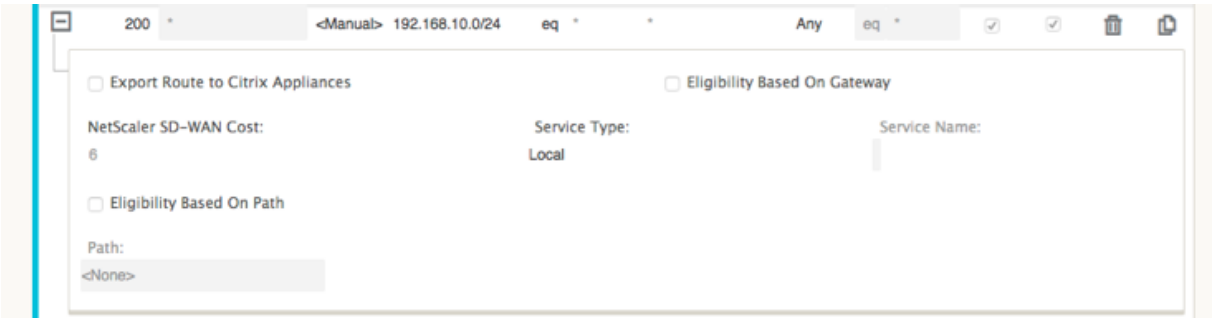
- 172.10.10.0/24（直接连接）
- 172.20.20.0/24（从核心路由器 B 通过 OSPF 公告）
- 172.30.30.0/24（从核心路由器 B 通过 OSPF 公告）

我们还需要通过 MPLS 提供前往达拉斯（10.100.1.0/24）的流量。

最后，我们希望通过 172.10.10.3 到防火墙 E 的所有 Internet 绑定流量路由作为下一个跃点。SD-WAN 通过 OSPF 学习此默认路由，并通过虚拟路径进行通告。纽约站点的筛选器是：

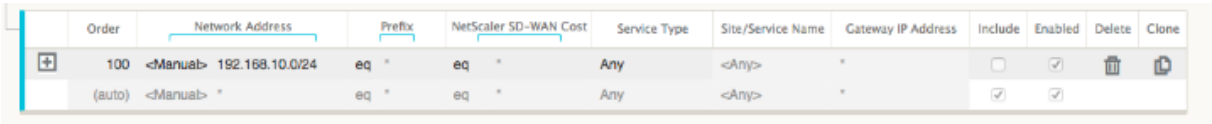


纽约 SD-WAN 站点导入管理网络的所有路由。这是可以忽略的。我们可以专注于滤波器 200。



过滤器 200 用于导入 192.168.10.0/24（我们的 MPLS 核心）以实现可达性，但不用于将其导出到虚拟路径。选中 包括 复选框，并确保清除 将路由导出到 **Citrix** 设备 复选框。然后包括所有其他路由。

对于导出过滤器，我们可以排除 192.168.10.0/24 的路由。这是因为，作为旧金山站点中的直接连接子网，我们无法在源位置过滤此路由，因此在此端将禁止该路由。



现在，让我们看看从纽约站点的核心路由开始刷新的路由表。

纽约路由器 **B**：

```
vyos@VYOS-ROUTER-B-CORE:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 4d22h22m
O>* 10.80.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.81.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h49m
O>* 10.90.1.0/24 [110/15] via 172.10.10.10, eth1, 3d19h50m
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 4d22h22m
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 4d22h22m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0
```

我们可以看到旧金山(10.80.1.0 和 10.81.1.0)和伦敦 (10.90.1.0) 的子网正在通过纽约 SD-WAN 设备 (172.10.10.10) 进行公告。10.100.1.0/24 路由仍在通过底层 MPLS 路由器 A. 公告中，让我们来看看纽约站点 SD-WAN 路由表。

纽约站点 **SD-WAN** 路由表：

Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 11 of 11 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.10.10.0/24	*	Local	YES	*	NYC	Static	-	-	5	0	YES	N/A	N/A
1	10.90.1.0/24	*	NYC-LON	YES	*	LON	Static	-	-	5	0	YES	N/A	N/A
2	10.81.1.0/24	10.80.1.20	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
3	10.80.1.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
4	192.168.10.0/24	*	NYC-SFO	YES	*	SFO	Static	-	-	5	0	YES	N/A	N/A
5	172.30.30.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	172.20.20.0/24	172.10.10.2	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	10.100.1.0/24	172.10.10.1	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	0.0.0.0/0	172.10.10.3	Local	YES	*	NYC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
10	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

我们可以看到通过 OSPF 获取的本地子网的正确路由，这是通过 MPLS 路由器 A 获得的达拉斯站点的路由，以及旧金山和伦敦站点的远程子网。让我们来看看 MPLS 路由器 A. 这个路由器正在参与 OSPF 和 BGP。

```
vyos@VYATTA-ROUTER-A:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:04:12
O   10.80.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.81.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 00:05:09
O   10.90.1.0/24 [110/15] via 172.10.10.10, 00:04:13
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 00:05:11
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 00:04:28
C>* 127.0.0.0/8 is directly connected, lo
O   172.10.10.0/24 [110/10] is directly connected, eth1, 00:05:24
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:04:12
B   192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 00:05:09
C>* 192.168.10.0/24 is directly connected, eth2
O   192.168.65.0/24 [110/20] via 172.10.10.2, 00:04:12
C>* 192.168.65.0/24 is directly connected, eth0
```

从路由表中，此路由器 A 通过 BGP 和 OSPF 学习远程子网，BGP 路由的管理距离和成本 (20/5) 低于 OSPF (110/10)，因此首选。在此示例中，只有一条核心路由的网络可能不会引起担忧。然而，到达此处的流量将通过 MPLS 网络传输，而非发送到 SD-WAN 设备 (172.10.10.10)。如果我们想要保持完整的路由对称性，我们需要一个路由图来调整 AD/衡量成本，以便从 172.10.10.10 的路由（而非通过 eBGP 学习的路由）中获得的路由偏好。

或者，可以配置 后门 路由，以强制路由器偏好 OSPF 路由，而不是 BGP 路由。请注意 SD-WAN 虚拟 IP 地址到伦敦站点 SD-WAN 设备的静态路由。

```
S>* 10.90.1.10/32 [5/0] via 192.168.10.2, eth2
```


如果 MPLS 路径出现故障，则必须确保虚拟路径重新路由回纽约站点 SD-WAN 设备。由于 10.90.1.0/24 的一个路由线路正在通过 172.10.10.10 （纽约 SD-WAN）公告。还建议创建覆盖服务规则来删除 SD-WAN 设备上的任何 UDP 4,980 数据包，以防止虚拟路径返回自己。

动态虚拟路径

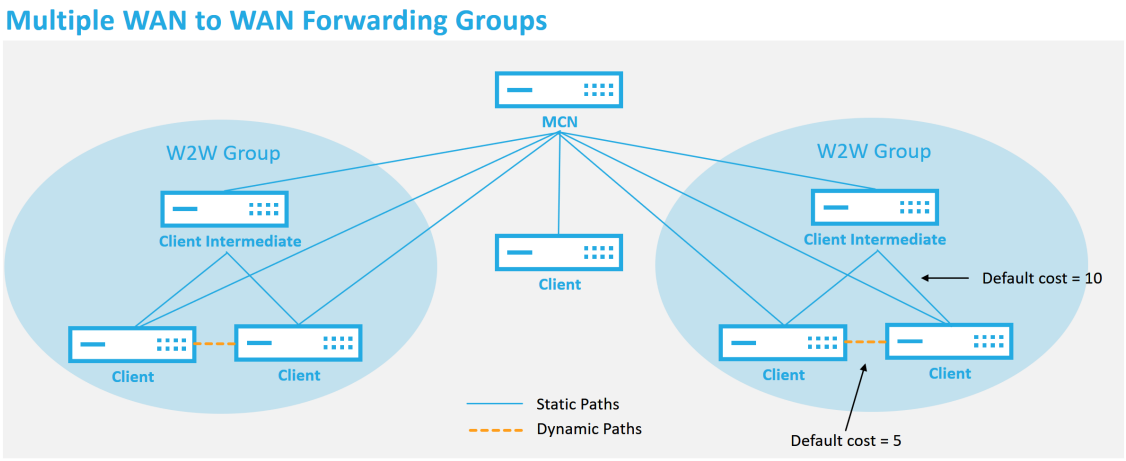
可以允许两个客户端节点之间的动态虚拟路径来构建按需虚拟路径，以便在两个站点之间进行直接通信。动态虚拟路径的优点是，流量可以直接从一个客户端节点流向第二个客户端节点，而无需遍历 MCN 或两个虚拟路径，这会增加流量的延迟。动态虚拟路径是根据用户定义的流量阈值动态构建和移除的。这些阈值被定义为每秒数据包 (pps) 或带宽 (kbps)。此功能可实现动态全网格 SD-WAN 叠加拓扑。

满足动态虚拟路径的阈值后，客户端节点会使用站点之间的所有可用 WAN 路径，动态地创建彼此的虚拟化路径，并按以下方式充分利用它：

- 发送批量数据（如果存在）并验证没有丢失，然后
- 发送交互式数据并验证没有丢失，然后
- 批量和交互式数据被认为稳定后发送实时数据（无丢失或可接受的水平）
- 如果没有批量或交互式数据在动态虚拟路径稳定一段时间后发送实时数据
- 如果用户数据在用户定义的时段内低于配置的阈值，则动态虚拟路径将被撕裂

动态虚拟路径具有中间站点的概念。中间站点可以是 MCN 站点或网络中配置了静态虚拟路径并连接到两个或多个其他客户端节点的任何其他站点。另一个设计考虑要求是启用 WAN 到 WAN 转发，允许将所有站点的所有路由播发到需要动态虚拟路径的客户端节点。

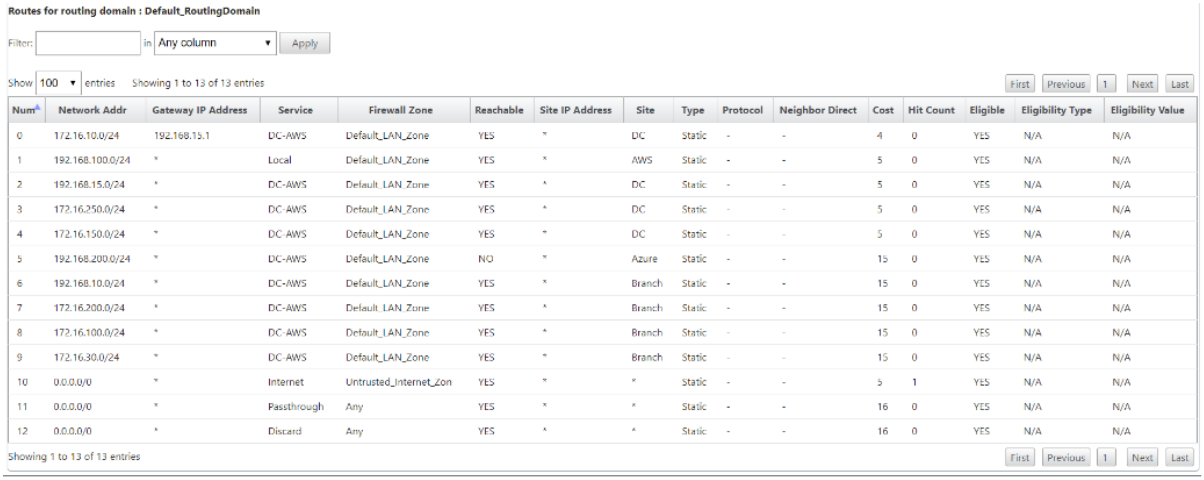
SD-WAN 中允许使用多个 WAN 到 WAN 转发组，从而可以完全控制某些客户端节点之间的路径建立，而不能控制其他客户端节点之间的路径建立。



每个 SD-WAN 设备都有自己的唯一路由表，并为每个路由定义了以下详细信息：

- Num —此设备基于匹配过程的路由顺序（最低处理的 Num）
- 网络地址—子网或主机地址
- 网关（如有必要）
- 服务—应用于此路由的服务
- 防火墙区域—路径的防火墙区域分类
- 可访问—标识此站点的虚拟路径状态是否处于活动状态
- 站点—预计路径存在的站点的名称
- 类型—路由类型的识别（静态或动态）
- 直接邻居
- 成本 -特定路由的成本
- 单击计数—每个数据包使用路由的次数。这将用于验证路由是否正确命中。
- 符合条件
- 资格类型
- 资格值

以下是一个示例 SD-WAN 站点路由表：



Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 13 of 13 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.16.10.0/24	192.168.15.1	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	4	0	YES	N/A	N/A
1	192.168.100.0/24	*	Local	Default_LAN_Zone	YES	*	AWS	Static	-	-	5	0	YES	N/A	N/A
2	192.168.15.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
3	172.16.250.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
4	172.16.150.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
5	192.168.200.0/24	*	DC-AWS	Default_LAN_Zone	NO	*	Azure	Static	-	-	15	0	YES	N/A	N/A
6	192.168.10.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
7	172.16.200.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
8	172.16.100.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
9	172.16.30.0/24	*	DC-AWS	Default_LAN_Zone	YES	*	Branch	Static	-	-	15	0	YES	N/A	N/A
10	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	1	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 13 of 13 entries First Previous 1 Next Last

从前面的 SD-WAN 路由表中注意，传统路由器中有更多的元素通常不可用。最值得注意的是 可访问 列，它根据 WAN 路径状态呈现路由活动或非活动（是/否）。此处列出的路由根据服务的不同状态（例如虚拟路径被关闭）被禁止。其他可以强制路由不符合条件的事件包括路径停止状态、下一跃点无法访问或 WAN 链接。

从上表中，我们可以看到 14 条定义的路由。路由或路由组的描述如下：

- 路由 0 —在 MCN 上，这是驻留在 DC 站点的主机子网路由。172.16.10.0/24 驻留在 DC LAN 中，192.168.15.1 是 LAN 上的网 Gateway，即将到达该子网的下一个跃点。
- 路由 1 —这是指向显示路由表的 SD-WAN 设备的本地路由。
- 路由 2—4 —这些是为 DC 站点 SD-WAN 配置的虚拟接口的一部分的子网。这些子网来自定义的受信任虚拟接口。
- 路由 5 —由于该站点和 MCN 之间的虚拟路径下降，这是由 MCN 共享的另一个客户端节点的共享路由，其可达状态为否。
- 路由 6—9 —这些路由存在于另一个客户端站点。对于此路由，将创建虚拟路径路由，用于匹配发往虚拟路径上远程站点的 WAN 入口流量。
- 路由 10 —与 Internet 服务定义，该系统添加了一个捕获所有路由直接 Internet 突破为本地站点.
- 路由 11 —直通是系统始终添加的默认路由，以便在任何现有路由上没有匹配的情况下允许数据包流通。直通不会修饰，通常会将本地广播和 ARP 流量映射到此服务。
- 路由 12 —丢弃是系统始终添加以删除未定义的任何东西的默认路由。

默认工艺路由成本值：

- 广域网到广域网转发—10
- 默认直接路由成本—5
- 自动生成的路由—5
- 虚拟路径—5

- 当地——5
- 内联网——5
- Internet —5
- 直通-5
- 可选—路由为定义为服务级别的 0.0.0.0/0

定义这些路径后，了解流量如何使用定义的路径流动非常重要。这些流量流分为以下流量：

- 局域网到 WAN（虚拟路径）—进入 SD-WAN 覆盖通道的流量
- WAN 到局域网（虚拟路径）—存在 SD-WAN 覆盖通道的流量
- 非虚拟路径流量—路由到底层网络的流量

内联网和 **Internet** 路由

对于 Intranet 和 Internet 服务类型，用户必须定义 SD-WAN WAN 链接以支持这些类型的服务。这是这些服务中任何一种定义路由的先决条件。如果 WAN 链接未定义为支持 Intranet 服务，则将其视为本地路由。Intranet、Internet 和直通路由仅与其配置的站点/设备相关。

在定义 Intranet、Internet 或直通路由时，以下是设计考虑因素：

- 必须在 WAN 链接上定义服务（内联网/Internet -必需）
- 内网/Internet 必须为 WAN 链接定义网 Gateway
- 与本地 SD-WAN 设备相关
- 内联网路由可以通过虚拟路径学习，但成本更高
- 使用 Internet 服务，会自动创建一个默认路由 (0.0.0.0/0) 以最大成本捕获所有路由
- 不要假设直通工作，它必须进行测试/验证，同时使用虚拟路径关闭/禁用进行测试以验证所需的行为
- 路由表是静态的，除非启用了路由学习功能

  多个路由参数支持的最大限制如下：

- 最大路由域名：255
- 每个 WAN 链路的最大访问接口：64
- 每个站点的最大 BGP 邻居值：255
- 每个站点最大 OSPF 面积：255
- 每个 OSPF 区域的最大虚拟接口：255
- 每个站点的最大路由学习导入过滤器：512

- 每个站点的最大路由学习导出过滤器：512
- 最大 BGP 路由策略：255
- 最大 BGP 社区字符串对象：255

路由域

September 2, 2022

Citrix SD-WAN 允许使用路由域对网络进行分段，以提高安全性和可管理性。例如，您可以将来宾网络流量与员工流量分开，创建不同的路由域以分割大型企业网络，并将流量分割为支持多个客户网络。每个路由域都有自己的路由表，并启用对重叠 IP 子网的支持。

Citrix SD-WAN 设备为路由域实施 OSPF 和 BGP 路由协议，以控制和分割网络流量。

无论访问点的定义如何，虚拟路径都可以使用所有路由域进行通信。这是可能的，因为 SD-WAN 封装包括数据包的路由域信息。因此，两个终端网络都 知道数据包所属的位置。无需为每个路由域创建 WAN 链接或访问接口。

以下是配置路由域功能时要考虑的要点列表：

- 默认情况下，在 MCN 上启用路由域。
- 路由域在分支站点上启用。
- 每个已启用的路由域必须具有与其关联的虚拟接口和虚拟 IP。
- 路由选择是以下所有配置的一部分：
  - 接口组
  - 虚拟 IP
  - GRE
  - WAN 链接-> 访问界面
  - IPsec 通道
  - 路由
  - 规则
- 仅当创建多个域时，路由域才会在 Web 界面配置中显示。
- 对于公共 Internet 链接，只能创建一个主要和辅助访问接口。
- 对于专用内联网 /MPLS 链接，可以为每个路由域创建一个主访问接口和辅助访问接口。

配置路由域

September 2, 2022

Citrix SD-WAN 设备支持配置路由协议，提供单点管理来管理企业网络、分支机构网络或数据中心网络。您最多可以配置 254 个路由域。

在 11.0.2 版本中，允许具有以下功能的 路由没有可路由虚拟 **IP (VIP)** 的域：

- 允许设备拥有不受信任或无接口的路由域。
- 允许分支机构通过在中间站点没有物理存在的路由域相互通信。

使用 **CLI** 访问路由

September 2, 2022

在 Citrix SD-WAN 版本 10.0 中，您可以查看与动态路由和协议状态相关的其他信息。键入以下命令和语法以访问路由守护进程并查看命令列表。

```
dynamic_routing?
<!--NeedCopy-->
```

动态路由

September 2, 2022

Citrix SD-WAN 支持以下两种动态路由协议：

- 开放最短路径优先 (OSPF)
- 边界网关协议 (BGP)

在 Citrix SD-WAN 11.3.1 版本之前，动态路由功能仅适用于单个路由器 ID。您可以为整个协议全局配置唯一的路由器 ID（OSPF 和 BGP 一个），也可以不提供路由器 ID。如果未提供路由器 ID，则会自动选择参与动态路由的虚拟网络实例 (VNI) 的最低 IP 作为默认路由器 ID。

从 Citrix SD-WAN 11.3.1 以后的版本中，您不仅可以为整个协议配置路由器 ID，还可以为每个路由域配置路由器 ID。借助此增强功能，您可以以稳定的方式在具有不同路由器 ID 的多个实例之间启用稳定的动态路由。

如果为特定路由域配置路由器 ID，则特定路由器 ID 将覆盖协议级路由域。

OSPF

OSPF 是 Internet 工程任务组（IETF）的内部网关协议（IGP）小组为 Internet 协议（IP）网络开发的路由协议。它包括 OSI 的中间系统到中间系统 (IS-IS) 路由协议的早期版本。

OSPF 协议是开放的，这意味着它的规范是在公共领域中（RFC 1247）。OSPF 基于称为 Dijkstra 的最短路径优先 (SPF) 算法。它是一个链路状态路由协议，它呼吁将链路状态公告 (LSA) 发送到同一层次结构区域内的所有其他路由器。有关附加接口、使用量度和其他变量的信息包含在 OSPF LSA 中。OSPF 路由器累积链接状态信息，SPF 算法使用该信息来计算每个节点的最短路径。

> 注意
>
> - Citrix SD-WAN 设备不作为指定路由器 (DR) 和 BDR (备份指定路由器) 参与每个多访问网络，因为默认 DR 优先级设置为“0”。
> - Citrix SD-WAN 设备不支持将总结作为区域边界路由器 (ABR)。

BGP

BGP 是一种自主的系统路由协议。自治网络或网络组在通用管理和通用路由策略下进行管理。BGP 用于交换 Internet 的路由信息，是 ISP 之间使用的协议。客户网络部署内部网 Gateway 协议，如 RIP 或 OSPF，用于在其网络中交换路由信息。客户连接到 ISP，ISP 使用 BGP 交换客户和 ISP 路由。在自治系统 (AS) 之间使用 BGP 时，协议称为外部 BGP (eBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则该协议称为内部 BGP (iBGP)。

BGP 是部署在 Internet 上的强大且可扩展的路由协议。为了实现可扩展性，BGP 使用许多名为属性的路由参数来定义路由策略并维护稳定的路由环境。当首次建立邻居之间的 TCP 连接时，BGP 邻居交换完整路由信息。检测到路由表的更改时，BGP 路由器仅向其邻居发送已更改的路由。BGP 路由器不会发送定期路由更新，并且只公布到目标网络的最佳路径。您可以将 Citrix SD-WAN 设备配置为使用 BGP 了解路由和通告路由。

外部 **BGP (eBGP)**

Citrix SD-WAN 设备连接到局域网侧的交换机和 WAN 侧的路由器. 随着 SD-WAN 技术开始成为企业网络部署的一个组成部分，SD-WAN 设备将取代路由器。SD-WAN 实现了 eBGP 动态路由协议，作为专用路由设备。

SD-WAN 设备建立了与对等路由器使用 eBGP 对 WAN 端的邻居关系，并且能够学习、宣传来自同行的路由和到同行的路由。您可以在对等设备上选择导入和导出 eBGP 学习路由。此外，可以将 SD-WAN 静态、虚拟路径学习路由配置为向 eBGP 对等机播发。

有关详细信息，请参阅以下用例：

- SD-WAN 站点通过 eBGP 与非 SD-WAN 站点通信
- 基于虚拟路径和 eBGP 的 SD-WAN 站点之间的通信
- 在单臂拓扑中实现 OSPF
- MPLS 网络中 OSPF Type5 到 Type1 部署
- SD-WAN 和非 SD-WAN（第三方）设备 OSPF 部署
- 使用 SD-WAN 网络实现 OSPF，具有高可用性设置

作为路径长度

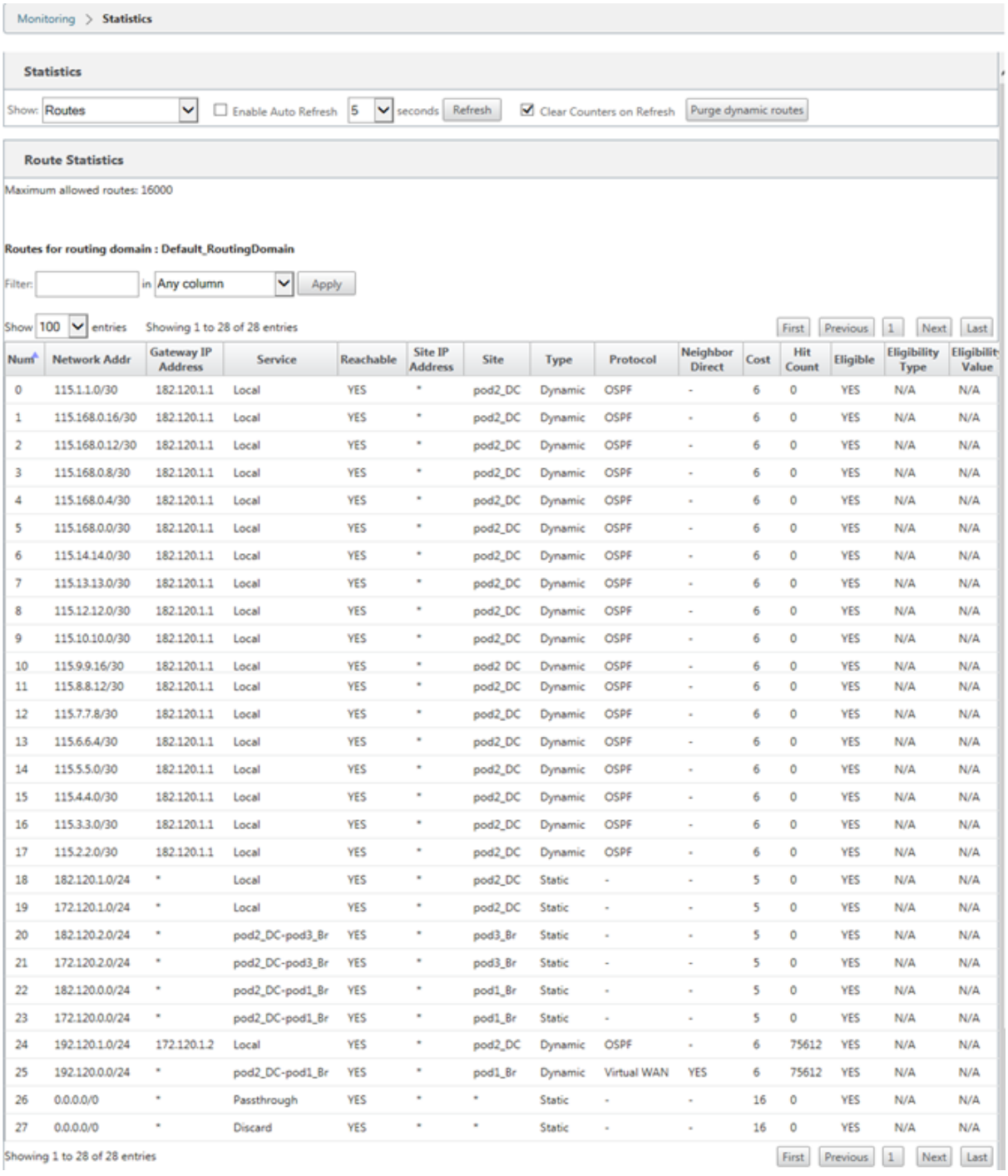
BGP 协议使用 **AS** 路径长度 属性来确定最佳路由。AS 路径长度表示在路径中遍历的自治系统的数量。Citrix SD-WAN 使用 **BGP AS** 路径长度 属性来筛选和导入路由。

非 SD-WAN 设备可以选择将流量路由路由路径长度导入到主 DC 或辅助 DC SD-WAN 设备。您还可以通过简单地增加路由器上主 DC 设备的作为路径长度，从而动态地将流量从路由器转向辅助 DC。无需更改路由成本和执行配置更新。

监视路由统计

导航到 监视器 > 统计信息。从 显示 下拉菜单中选择 路由。

无论路由是动态还是静态路由，Citrix SD-WAN 网络都支持适用路由的所有功能。



Monitoring > Statistics

Statistics

Show: Routes | Enable Auto Refresh | 5 seconds | Refresh | Clear Counters on Refresh | Purge dynamic routes

Route Statistics

Maximum allowed routes: 16000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column | Apply

Show 100 entries Showing 1 to 28 of 28 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	115.1.1.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
1	115.168.0.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
2	115.168.0.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
3	115.168.0.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
4	115.168.0.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
5	115.168.0.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
6	115.14.14.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
7	115.13.13.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
8	115.12.12.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
9	115.10.10.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
10	115.9.9.16/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
11	115.8.8.12/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
12	115.7.7.8/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
13	115.6.6.4/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
14	115.5.5.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
15	115.4.4.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
16	115.3.3.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
17	115.2.2.0/30	182.120.1.1	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	0	YES	N/A	N/A
18	182.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
19	172.120.1.0/24	*	Local	YES	*	pod2_DC	Static	-	-	5	0	YES	N/A	N/A
20	182.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
21	172.120.2.0/24	*	pod2_DC-pod3_Br	YES	*	pod3_Br	Static	-	-	5	0	YES	N/A	N/A
22	182.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
23	172.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Static	-	-	5	0	YES	N/A	N/A
24	192.120.1.0/24	172.120.1.2	Local	YES	*	pod2_DC	Dynamic	OSPF	-	6	75612	YES	N/A	N/A
25	192.120.0.0/24	*	pod2_DC-pod1_Br	YES	*	pod1_Br	Dynamic	Virtual WAN	YES	6	75612	YES	N/A	N/A
26	0.0.0.0/0	*	Passthrough	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
27	0.0.0.0/0	*	Discard	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 28 of 28 entries First Previous 1 Next Last

OSPF

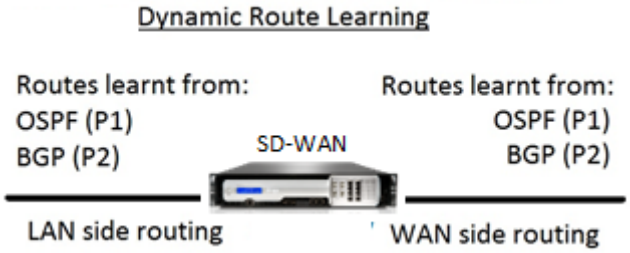
September 2, 2022

局域网侧：动态路径学习

在以网关模式部署的 Citrix SD-WAN 设备的 LAN 端口上运行的 OSPF：

Citrix SD-WAN 设备为每个所需的路由协议（OSPF 和 BGP）执行本地客户网络（分支机构和数据中心）中的第 3 层路由播发的路由发现。所学到的路由将动态捕获并显示。

这样，SD-WAN 管理员就无需静态定义作为 SD-WAN 网络一部分的每个设备的 LAN 端网络环境。



WAN 侧：动态路由共享

通过限制第 5 类作为外部 LSA 的学习，将区域定义为 STUB 区域的 Citrix SD-WAN 设备。

Citrix SD-WAN 设备可以通过 MCN 公布本地了解的动态路由。然后 MCN 可以将这些路由中继到网络中的其他 SD-WAN 设备。这种信息交换可以动态地在不断变化的网络中保持站点之间的连接。

OSPF 部署模式

在以前的版本中，OSPF 实例从 SD-WAN 获取的路由被视为仅具有类型 5 LSA 的外部路由。这些路由通告到类型 5 外部 LSA 中的邻居路由器。根据 OSPF 路径选择算法，SD-WAN 路由是不太优先的路由。

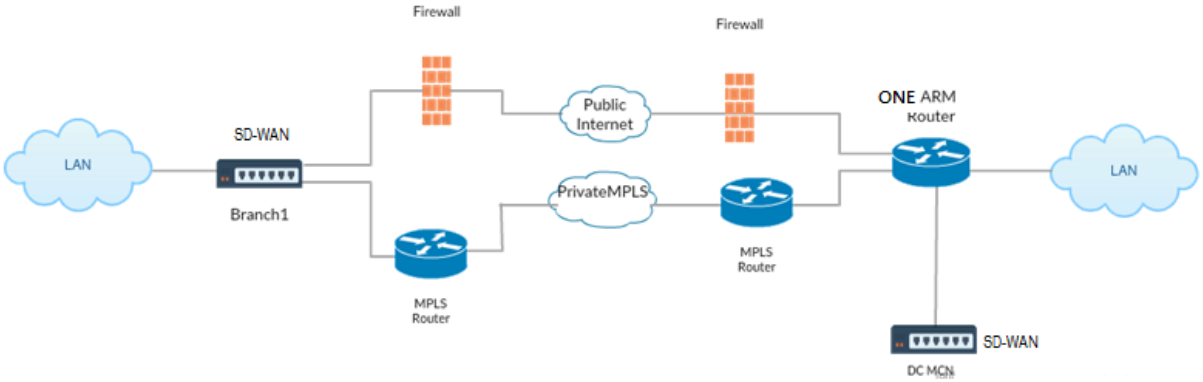
通过最新版本，SD-WAN 现在可以将路由作为区域内路由（LSA 类型 1）进行宣传，以便使用 OSPF 路径选择算法根据路径成本获得优先权。路由成本可以配置并公告到邻居路由器。这允许以下述单臂模式部署 SD-WAN 设备。

在单臂拓扑中实现 **OSPF**

在单臂配置中，路由器在 OSPF 部署中需要复杂的 PBR 或 WCCP 配置。通过将默认导出路由类型从类型 5 更改为类型 1，我们可以简化此部署。如果 SD-WAN 路由以较低的成本通告为区域内路由，并且 SD-WAN 设备变为活动状态，则邻居路由器会选择 SD-WAN 路由并自动开始通过 SD-WAN 网络转发流量。不再需要额外的 PBR 或 WCCP 配置。

必备条件：

- DC 和分支站点上的 SD-WAN 设备必须运行最新版本。
- 端到端 IP 连接必须配置并且工作正常。
- OSPF 已在所有站点上启用。

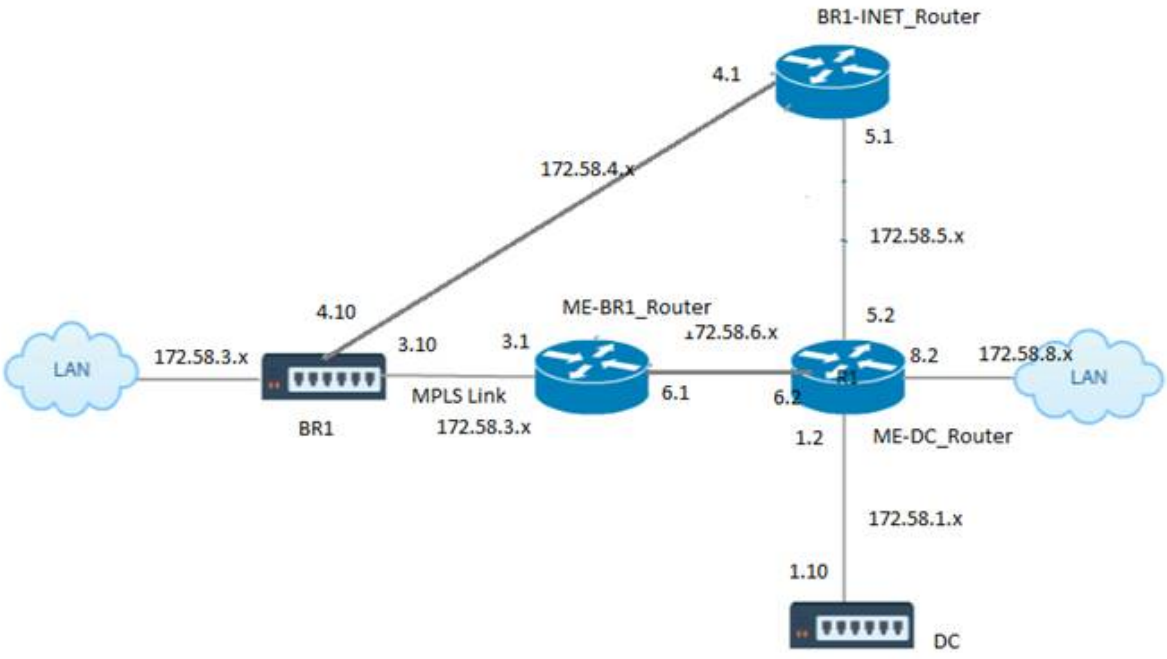


如上图所示，DC MCN 部署在单臂拓扑中。DC 站点启动时，单臂路由器会将所有流量从本地 LAN 转发到其他站点，例如目的 IP 地址位于同一子网内的分支本地 LAN，然后 SD-WAN 设备将所有数据包包装到路由器，并将其发送到所有数据包目标 IP 地址中的分支虚拟 IP 地址。然后，路由器将这些数据包转发到 WAN。

当 DC 站点关闭时，路由器将所有流量从本地 LAN 转发到其他站点（分支站点的本地 LAN，目标 IP 位于子网内）直接转发到 WAN，而不是 SD-WAN 设备。

MPLS 网络中 **OSPF Type5** 到 **Type1** 部署

提供以下部署模式，以避免在使用 SD-WAN 设备配置的 MPLS 网络中形成循环。下图描述了标准 MPLS 网络实现。



在上图中：

- OSPF 在区域 0 的 *ME-BR1_* 路由器 和 *ME-DC_* 路由器 之间配置。

- OSPF 在区域 0 的 *ME-DC_* 路由器 和 *DC* 之间配置。

推荐配置：

- area0 上的 DC VW 和 ME-DC_Router
- area0 上的 ME-BR1_Router 和 ME-DC_Router
- area0 上的 BR1 VW 和 ME-BR1_Router

在 ME-DC_ 路由器上：

1. 添加到 172.58.3.10/32 的静态路由（用于 MPLS 链路的 BR1 的虚拟 IP）至 172.58.6.1 的静态路由
2. 添加 172.58.4.10/32（INET 的 BR1 的虚拟 IP）到 172.58.5.1 的静态路由

添加静态路由可防止 ME-DC_ 路由器和 DC SD-WAN 设备之间形成循环。如果不添加静态路由，MCN 将流量转发到 ME-DC 路由器，然后从路由器返回到 MCN，这会连续创建一个环路。

静态路由不是 PBR 路由，而是基于目的主机 IP 的路由，会根据选择的路径和之后执行的封装，向正确的链路传输。因此，配置了这些静态路由后，带有 BR1 SD-WAN 设备任何目标虚拟 IP 的封装数据包将按照 DC MCN 选择的最佳路径使用这些链路。

添加 ACL 以避免在安装 IPhost 路由时形成循环（如果没有配置静态虚拟 IP）：

- 如果 BR1 SD-WAN 设备通告的 IPHOST 路由由 MCN 路由器 *ME-DC_Router* 安装，而没有像上面提到的那样添加为静态路由，那么 ME-BR1_Router 和 ME-DC_Router 之间的 OSPF 参与接口 (172.58.6.x) 关闭，则有可能形成环路。这是因为当这个接口关闭时，IPhost 路由会从 ME-DC_Router 的路由表中刷新。
- 如果发生这种情况，MCN 将发往 BR1 VIP 的封装数据包转发到 ME-DC 路由器，然后从路由器回到 MCN 并连续环路。

在我 BR1_ 路由器上：

将 172.58.3.x 网络通告给 ME-DC_Rou 器的成本高于 DC 为同一网络公布的成本，如果在 **ME-BR1_Router <-> ME-DC_Router** 与 **ME-DC_Router <-> DC (SD-WAN)** 之间使用相同的区域 ID。

- 基于 OSPF 10^8/BW 的成本度量计算，路由前缀的成本基于接口类型。SD-WAN 设备将虚拟路径和特定于虚拟 WAN 的静态路由通告到外部路由器或对等路由器，默认 SD-WAN 开销为 5。
- 如果 ME-BR1 路由器也将 *172.58.3.0/24* 作为内部 *OSPF* 类型 *1* 路由与 *DC (SD-WAN)* 同时通告与内部 *OSPF* 类型 *1* 路由相同的前缀，则根据成本计算，默认情况下将配置 *ME-BR1* 路由器的路由，因为开销低于开销默认成本为 5。为避免这种情况，并使 SD-WAN 设备最初选择为首选路由，必须操纵 (172.58.3.1) 的接口开销，使其在 ME-BR1_ 路由器上更高，以便在 ME-DC_ 路由器的路由表中配置 DC SD-WAN 路由。

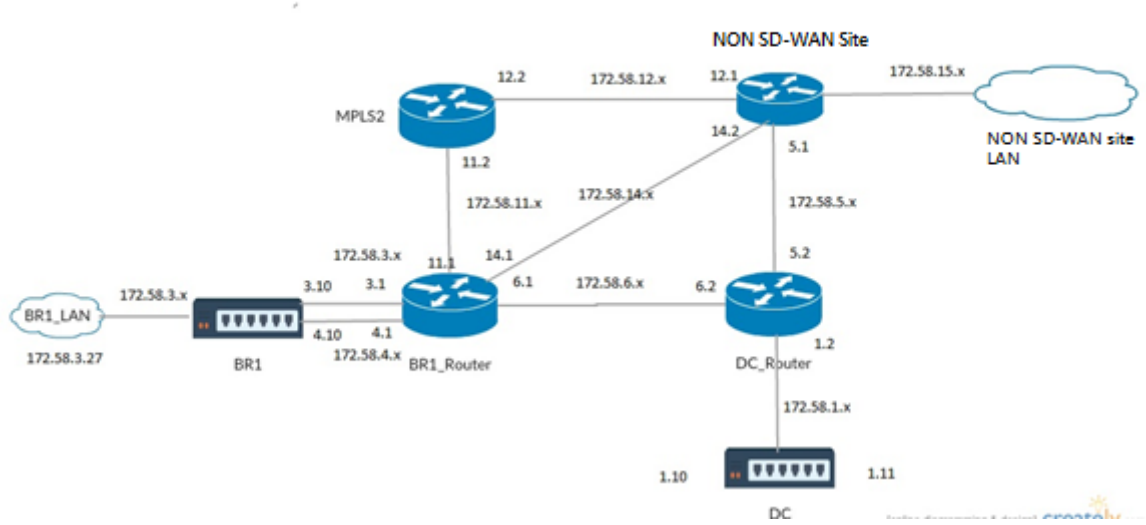
这还可确保 DC SD-WAN 设备发生故障时，使用 ME-BR1_ 路由器作为下一个首选 Gateway 的备用路由可确保流量不间断。

使用 ME-DC_Router 为 DC SD-WAN 和 ME-BR1_Router 公告 172.58.8.0/24 网络的来源：

通过此路由，DC SD-WAN 可以在解除胶囊后将数据包发送到上游路由器，以了解 LAN 子网。如果 DC SD-WAN 出现故障，旧版路由基础结构将帮助 ME-BR1_Router 使用 ME-DC_Router 作为下一个跃点以到达 172.58.8.x 网络。

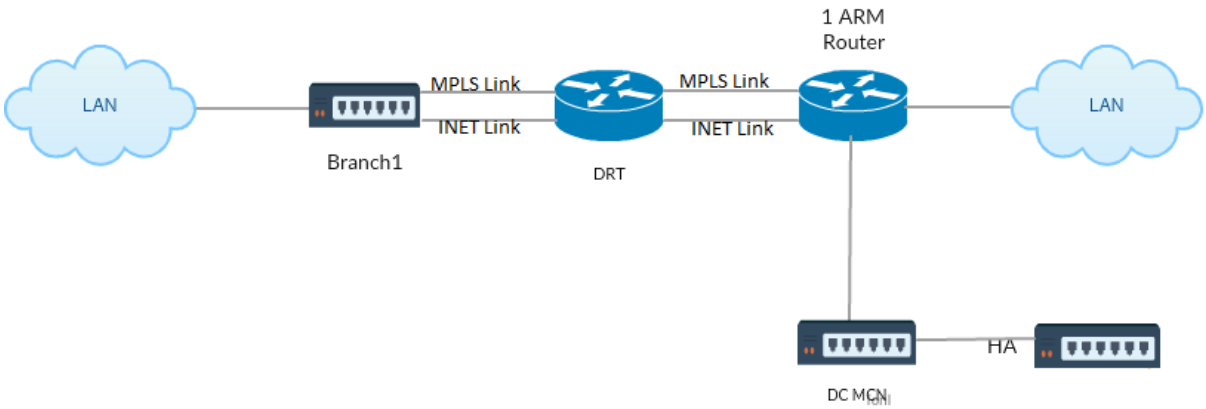
SD-WAN 和第三方（非 **SD-WAN**）设备部署

如下图所示，第三方设备站点可以通过直接将流量发送到站点 B 来访问站点 B 的 LAN。如果无法直接发送流量，则回退路由将转到站点 A，然后使用 DC 到分支站点之间的虚拟路径到达分支机构。如果失败，它使用 MPLS2 访问分支站点。



流量可以在 SD-WAN GUI 中观察到 监视 > 流 量。

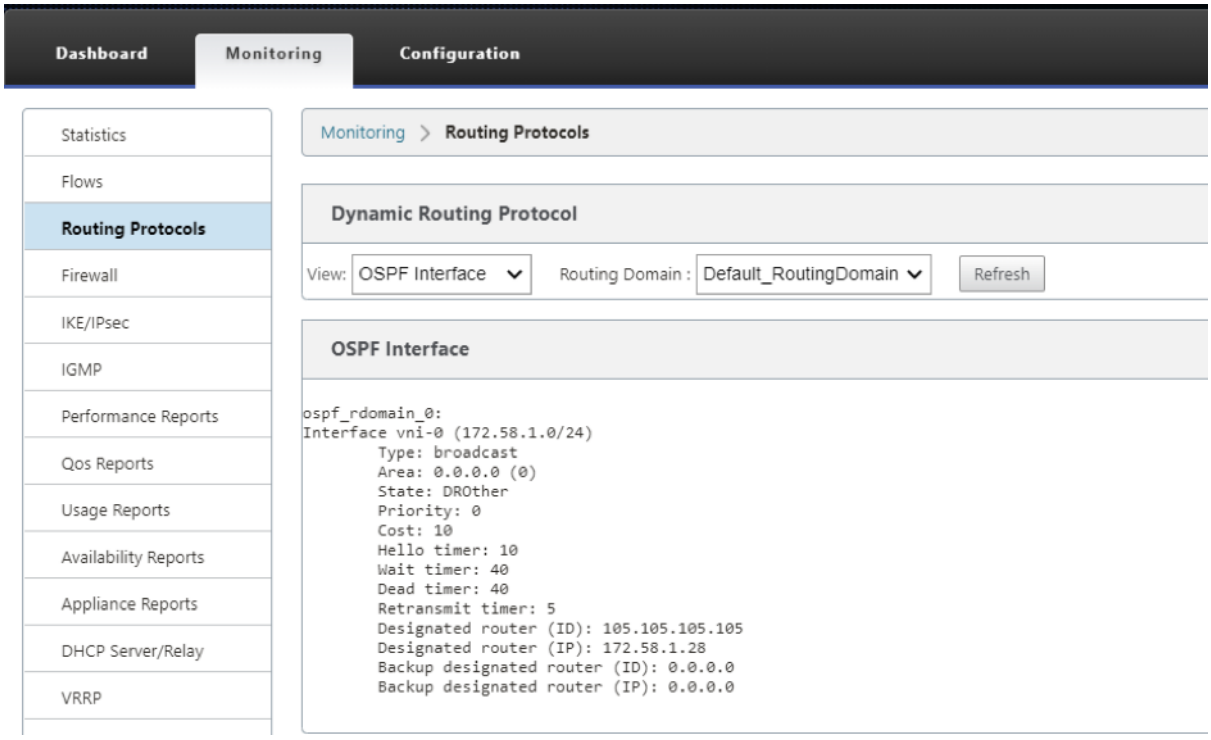
在高可用性设置中使用 **SD-WAN** 网络实现 **OSPF**

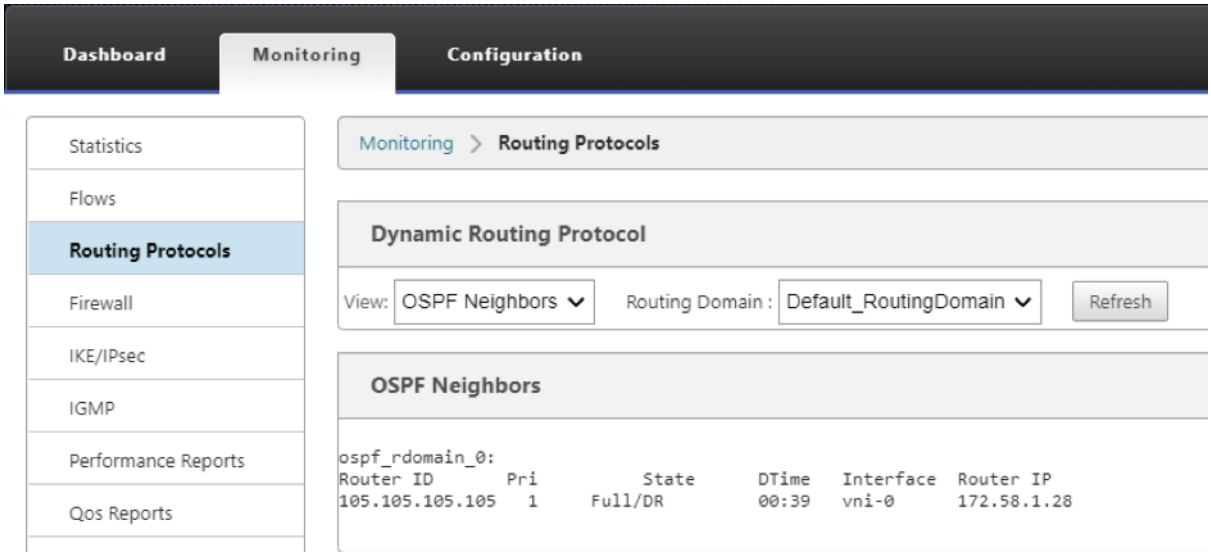


OSPF Type5 到 Type1 与高可用性站点在故障转移到备用设备并部署在高可用性设置中：

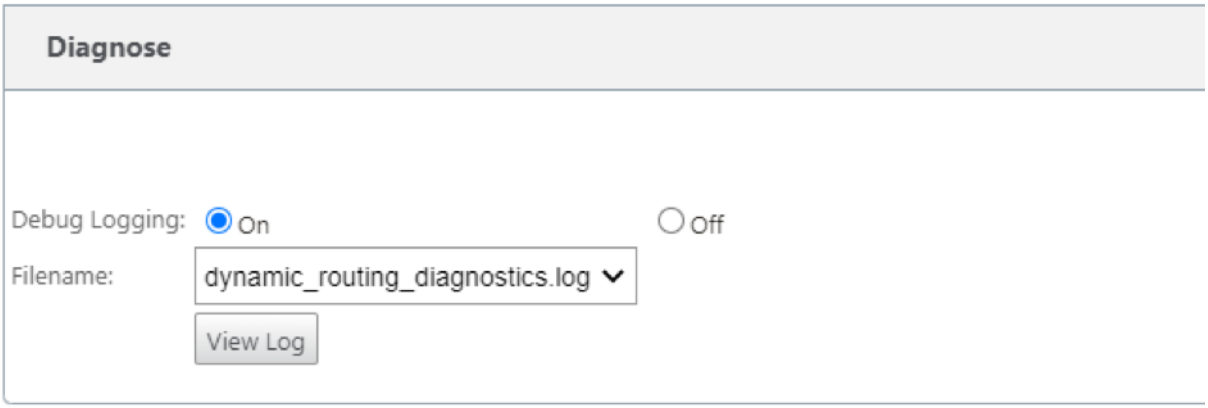
故障排除

您可以在 监视 **>** 路由协议下查看 OSPF 参数。





您还可以观察动态路由日志，查看 OSPF 融合是否存在任何问题。



BGP

September 2, 2022

SD-WAN BGP 路由功能使您能够：

- 配置邻居路由器或其他对等路由器（iBGP 或 EbGP）的自治系统 (AS) 号。
- 在任一方向（导入或导出）创建要选择性应用于每个邻居的一组网络的 BGP 策略。SD-WAN 设备支持每个站点八个策略，最多有八个与策略相关联的网络对象（或八个网络）。
- 对于每个策略，用户可以配置多个社区字符串、AS-PATH-PREPEND、MED 属性。用户最多可以为每个策略配置 10 个属性。

> 注意：
>
> 只允许使用本地首选项和 IGP 指标来选择和操作路径。

配置邻居

要配置 EBGP，需要在现有 BGP 邻居部分添加一个额外列，以配置邻居 AS 编号。当您使用 SD-WAN 9.2 配置编辑器导入以前的配置时，将使用本地伸缩编号预填充现有配置到此字段中。

邻居配置还具有可选的高级部分（可扩展行），您可以在其中为每个邻居添加策略。

配置高级邻居

使用此选项，您可以添加网络对象并为该网络对象添加配置的 BGP 策略。这类似于创建路径映射和 ACL 以匹配特定路径以及为该邻居配置 BGP 属性。您可以指定方向以指示此策略是否适用于传入或传出的路由。

默认策略是 <accept> 所有路由。接受和拒绝策略是默认策略，不能修改。

您可以根据网络地址（目标地址）、作为路径、社区字符串匹配路由，并分配策略并选择要应用的策略的方向。

1. 转到 监 控 > 路由协议 > 动态路由协议 以监视直流站点或分支站点设备的配置 BGP 策略和邻居。

您可以从 监视器 > 路由 协议页面启用调试日志记录并查看路由 的日志文件。路由守护进程的日志被拆分为单独的日志文件。标准路由信息存储在 *dynamic_routing.log* 中，而动态路由问题则在 *dynamic_routing_diagnostics.log* 中捕获，可通过监控路由协议查看。

BGP 软重新配置

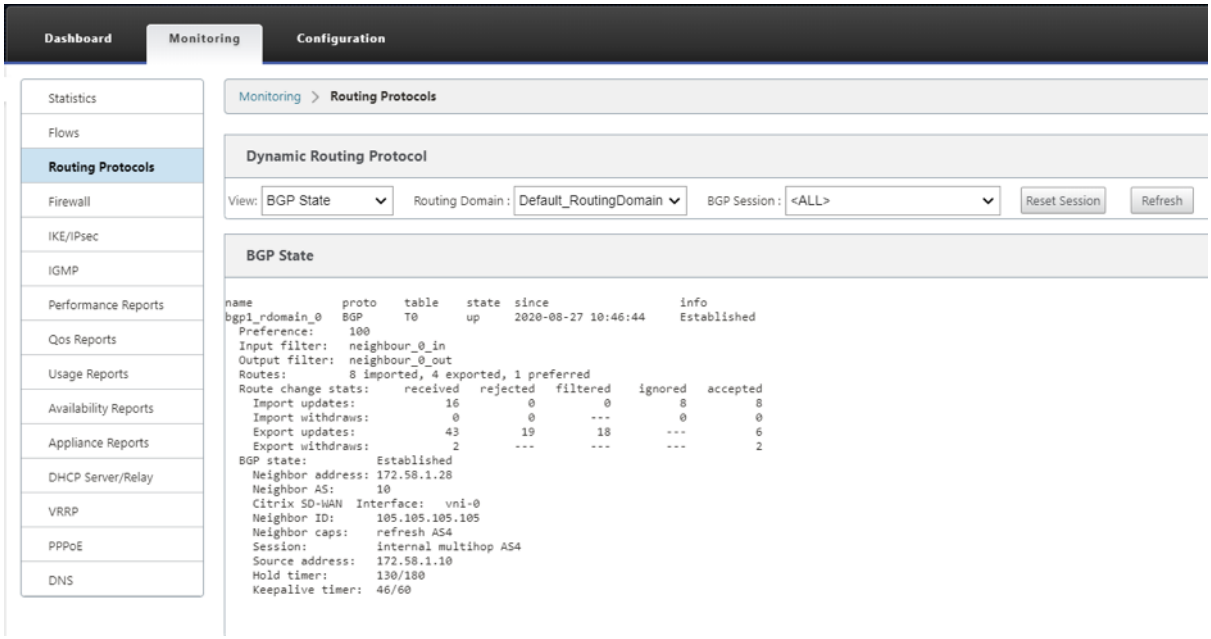
BGP 对等方的路由策略包括可能影响入站或出站路由表更新的路由映射、通讯组列表、前缀列表和筛选列表等配置。当路由策略发生更改时，必须清除或重置 BGP 会话，以使新策略生效。

使用硬重置清除 BGP 会话会使缓存失效，并导致缓存中的信息变得不可用时对网络运行造成负面影响。

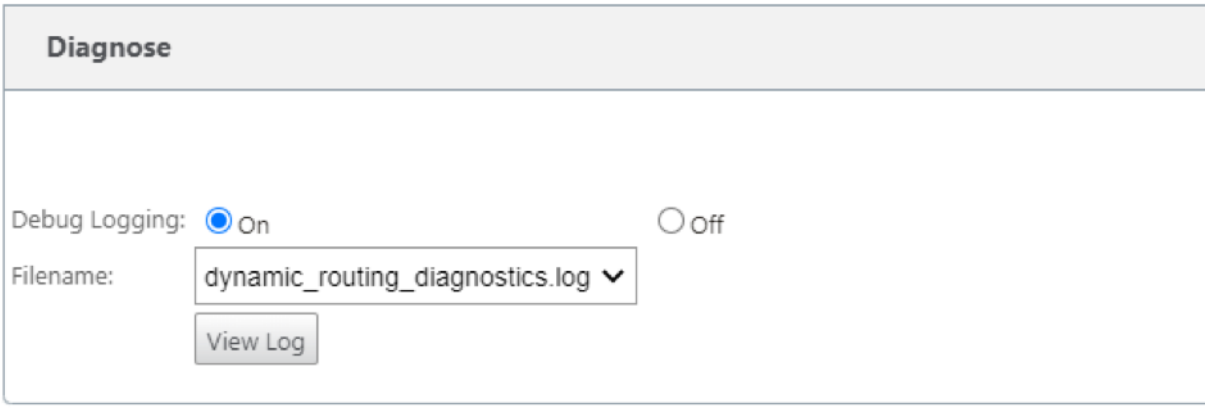
BGP 软重置增强功能为不依赖于存储的路由表更新信息的入站 BGP 路由表更新的动态软重置提供了自动支持。

故障排除

要查看 BGP 参数，请导航到 监视 **>** 路由协议 > 从 视图 字段中选择 **BGP** 状态。



您可以观察动态路由日志，查看 BGP 收敛是否存在任何问题。



iBGP

September 2, 2022

Citrix SD-WAN 设备具有局域网端的 iBGP 和 WAN 端的 eBGP：

Citrix SD-WAN 设备在局域网端使用 iBGP 部署时，通过 NEXT HOP 部署在局域网端和 eBGP 部署时，将所有的 eBGP 路由通知到 IGP 域中。

具有直接对等的线性网络拓扑中的多个 iBGP 局域网路由器，并与 Citrix SD-WAN 网格。

局限性：

- 不支持 AS-路径前缀、Med 和社区属性。
- 不支持在重新分配过程中 OSPF 和 BGP 之间的路由筛选。要么所有（或）从 OSPF 学到的路由都不会发布给 BGP 对等人，反之亦然。
- 不支持路由聚合。
- 只能配置最多 16 个 BGP 对等（包括 iBGP 和 eBGP）。

eBGP

September 2, 2022

SD-WAN 站点通过 eBGP 与非 SD-WAN 站点通信：

当没有 SD-WAN 设备的站点通过单个 WAN 路径（仅可用 Internet）与 SD-WAN 设备的另一站点（Site-A）通信时，如果具有 SD-WAN 设备的站点（Site-A）失去 Internet 连接，则没有 SD-WAN 的站点可以通过另一 SD-WAN 与 Site-A 通信站点 A 通信设备站点（站点 B）。站点 B 将来自没有 SD-WAN 设备的站点的流量传输到站点 A。

使用虚拟路径和 eBGP 在 SD-WAN 站点之间进行通信：

当 Virtual WAN 设备仍在运行时，两个站点之间的虚拟路径停止时，提供底层路径学习，以便与远程站点本地子网进行通信。

申请路由

September 2, 2022

在典型的企业网络中，分支机构可访问本地数据中心、云数据中心或 SaaS 应用程序上的应用程序。应用程序路由功能允许您轻松、经济高效地引导应用程序通过您的网络。例如，当分支站点上的用户尝试访问 SaaS 应用程序时，流量可以被路由，以便分支机构可以直接访问 Internet 上的 SaaS 应用程序，而无需先通过数据中心。

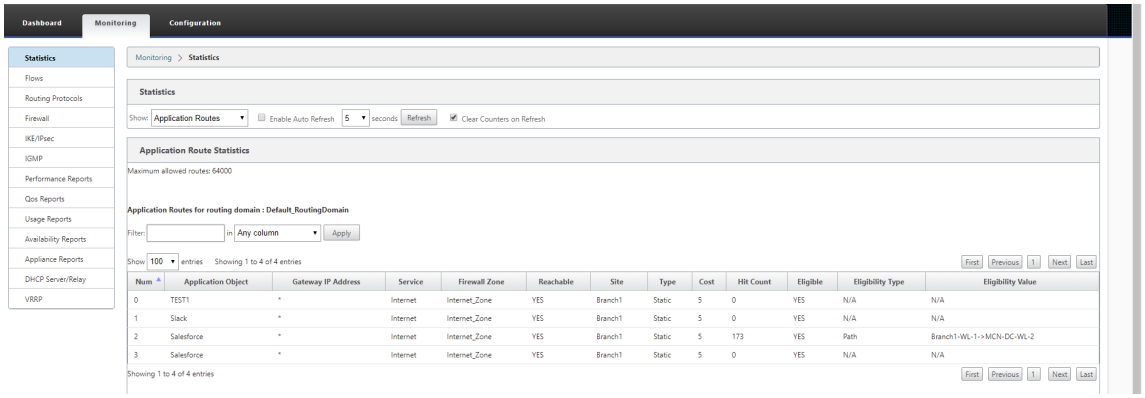
Citrix SD-WAN 允许您定义以下服务的应用程序路由：

- 虚拟路径：此服务管理虚拟路径中的流量。虚拟路径是两个 WAN 链接之间的逻辑链接。它由一组 WAN 路径组成，可在两个 SD-WAN 节点之间提供高服务级别的通信。SD-WAN 设备在每个路径的基础上测量网络，并适应不断变化的应用需求和 WAN 条件。虚拟路径可以是静态的（始终存在）或动态的（仅当两个 SD-WAN 设备之间的流量达到配置的阈值时才存在）。
- **Internet**：此服务管理企业站点与公共 Internet 上的站点之间的流量。Internet 流量没有封装。当发生拥塞时，SD-WAN 通过相对于虚拟路径和 Intranet 流量的速率限制 Internet 流量来主动管理带宽。
- **Intranet**：此服务管理尚未定义为通过虚拟路径进行传输的企业内部网流量。内部网流量未封装。SD-WAN 通过在拥塞期间相对于其他服务类型的速率限制此流量来管理带宽。在某些情况下，如果在虚拟路径上配置 Intranet 回退，则通常通过虚拟路径传输的流量可以被视为 Intranet 通信。
- 本地：此服务管理与其他服务不匹配的站点本地流量。SD-WAN 忽略来源和发往本地路由的流量。
- **GRE** 通道：此服务管理发往 GRE 通道的 IP 流量，并与站点配置的 LAN GRE 通道匹配。GRE 通道功能使您能够配置 SD-WAN 设备以终止局域网上的 GRE 通道。对于具有服务类型 GRE 通道的路由，Gateway 必须位于本地 GRE 通道的通道子网之一。
- **LAN IPSec** 通道：此服务管理发往 LAN IPsec 通道的 IP 流量，并与站点配置的 LAN IPsec 通道匹配。通过 LAN IPsec 通道功能，您可以将 SD-WAN 设备配置为终止局域网或 WAN 端的 IPsec 通道。

要执行应用程序的服务指导，必须在第一个数据包本身上识别应用程序。最初，一旦对流量进行分类并且已知应用程序，数据包将通过 IP 路由流动，则使用相应的应用程序路由。通过学习与应用程序对象关联的 IP 子网和端口来实现第一个数据包分类。使用 DPI 分类器的历史分类结果和用户配置的 IP 端口匹配类型获取这些结果。

要查看应用程序路由的统计数据：

1. 在 SD-WAN GUI 中，导航到 监控 > 统计信息。
2. 从 显示 下拉列表中，选择 应用程序路由。



您可以查看以下统计信息：

- 应用程序对象：应用程序对象的名称。
- 网关 **IP** 地址：GRE 通道服务类型的应用程序对象使用的网关 IP 地址。
- 服务：映射到应用程序对象的服务类型。
- 防火墙区域：此路由所在的防火墙区域。
- 可访问：应用程序路由的状态。
- 站点：站点的名称。
- 类型：指示路由是静态还是动态路由。
- 成本：路由的优先级。
- 命中计数：应用程序路由用于引导流量的次数。
- 符合条件：应用程序路由是否有资格发送流量。
- 资格类型：适用于此路径的路径资格条件的类型。资格类型可以是路径、网关或通道。
- 资格值：为路径资格条件指定的值。

> 注意
>
> 在当前版本中，属于应用程序系列、应用程序对象中定义的匹配类型的应用程序无法引导。

故障排除

创建应用程序路由后，您可以使用 监视 部分确认应用程序已正确路由到预期服务。

要查看应用程序是否正确路由到预期服务，请导航到以下页面：

- 监视 **>** 统计信息 **>** 应用程序路由
- 监控 **>** 流
- 监控 **>** 防火墙

如果存在任何意外路由行为，请在发现此问题时收集 STS 诊断程序包，并与 Citrix 技术支持团队共享。

可以使用 配置 **>** 系统维护 **>** 诊断 **>** 诊断信息创建和下载 STS 包。

路由过滤

September 2, 2022

对于启用了“路由学习”的网络，Citrix SD-WAN 可以更好地控制哪些 SD-WAN 路由通告给路由邻居，而不是通告和接受所有路由或不接受路由。

- 导出 筛选器 用于包含 或 排除 使用 OSPF 和 BGP 协议基于 特定 匹配的 播 发路由 标准。导出筛选器规则是在通过动态路由协议公告 SD-WAN 路由时必须满足的规则。默认情况下，所有路由都会公布给同级。
- 导入过滤器用于接受或不接受基于特定匹配条件使用 OSPF 和 BGP 邻居接收的路由。导入筛选器规则是在将动态路由导入 SD-WAN 路由数据库之前必须满足的规则。默认情况下不导入任何路由。

路由筛选在 SD-WAN 网络（数据中心/分支机构）中的 LAN 路由和虚拟路径路由上实现，并通过 BGP 和 OSPF 将路由通告到非 SD-WAN 网络。

您最多可以配置 512 个导出筛选器和 512 个导入筛选器。这是总体限制，而不是每个路由域限制。

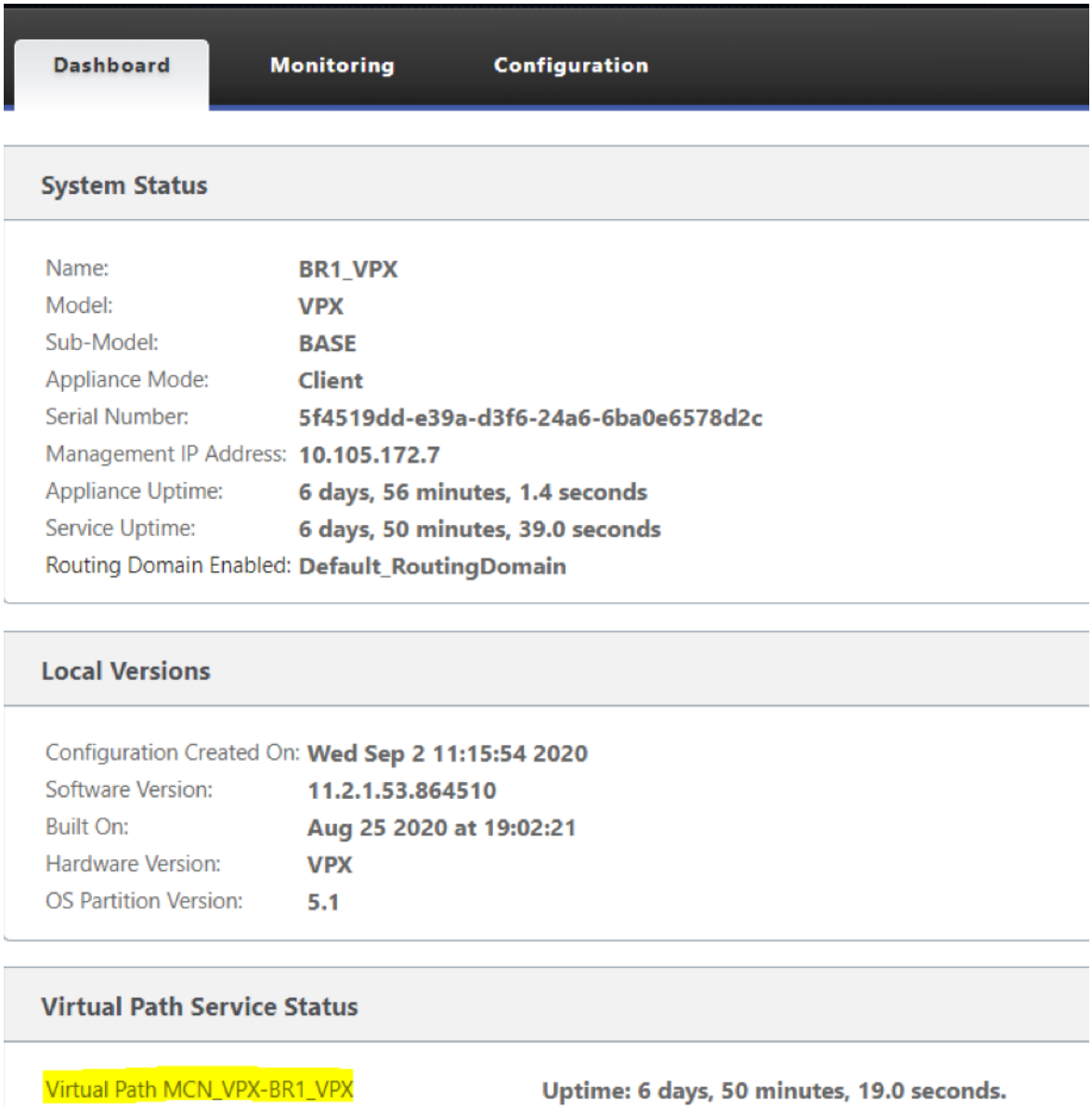
路由汇总

September 2, 2022

随着企业网络规模的增加，路由器需要在其路由表中保留大量路由。路由器需要更多的 CPU、内存和带宽资源来查找大型路由表并维护各个路由。您可以使用 本地 和 丢弃 服务类型配置摘要路由。此摘要路由会公布到下一个跃点设备。

故障排除

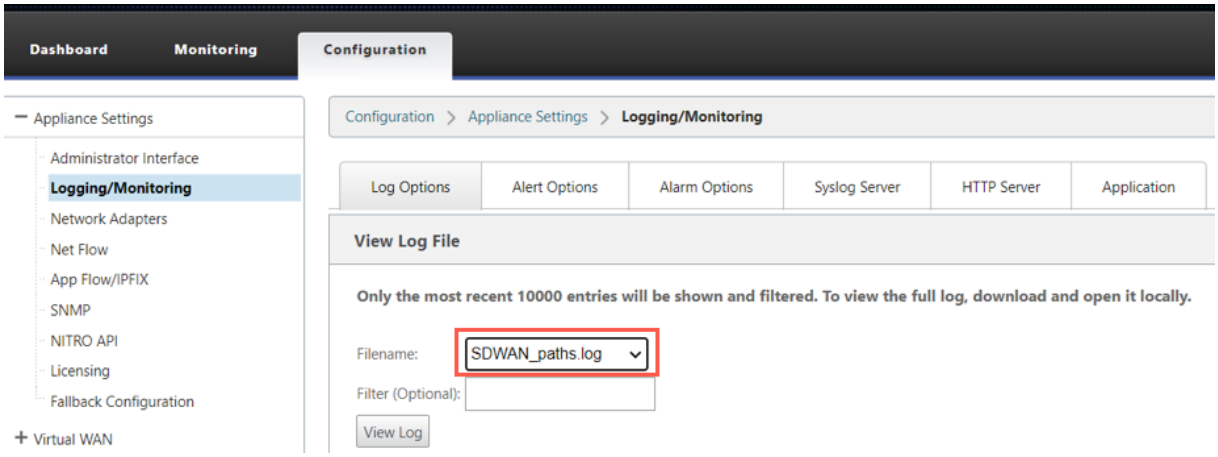
MCN 上配置的汇总路由通过虚拟路径发送到分支机构。如果您在分支的路由表中没有看到虚拟路径详细信息，请检查 Branch 控制面板。仪表板显示 MCN 和 Branch 之间的虚拟路径的状态。



如果虚拟路径关闭，请在 配置 **>** 日志/监视下检查其原因。

从文件名下拉列表中选择以下文件之一进行验证：

- SDWAN_paths.log
- SDWAN_common.log



协议偏好

September 2, 2022

协议首选项是 Citrix SD-WAN 特定功能，类似于路由器管理距离。首选顺序最高的协议是最优选的。使用协议首选项值最高的协议的路由。协议优先级信息是 Citrix SD-WAN 设备的本地信息，不会公布给对等网络元素。

多播路由

September 2, 2022

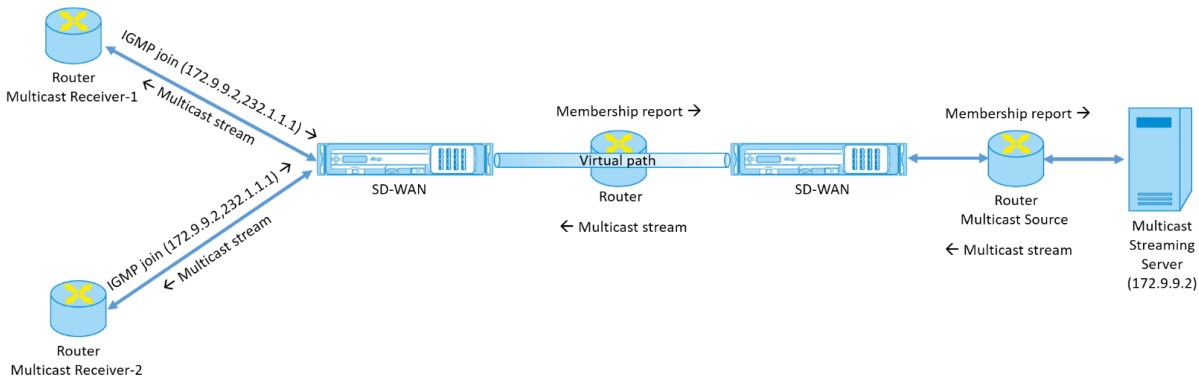
组播路由实现了一对多流量的高效分配。多播源，将单个流中的多播流量发送到多播组。多播组包含使用 IGMP 协议进行多播通信的主机和相邻路由器等接收器。IP 语音、视频点播、IP 电视和视频会议是使用多播路由的一些常见技术。在 Citrix SD-WAN 设备上启用多播路由时，该设备将充当多播路由器。

源特定组播

多播协议通常允许多播接收机接收来自任何源的多播通信。使用特定于源的多播 (SSM)，您可以指定接收机从中接收多播流量的源。它确保接收机不是每个发送多播流的源的侦听器，而是侦听特定多播源。SSM 降低了消耗来自每个可能来源的流量所使用的资源成本，并通过确保接收方接收来自已知发送方的流量来提供一个安全层。

以下拓扑显示了一个分支站点上的两个多播接收器和数据中心的一个组播服务器 (172.9.9.2)。多播服务器通过特定组 (232.1.1.1) 流式传输流量，接收机加入组。多播组上传送的任何流量都将中继到加入该组的所有接收机。

> 注意
>
> 要使 SSM 工作，组播组 IP 必须在 232.0.0.0/8 范围内。



1. 多播接收机发送 IP IGMP 加入请求，指示接收机希望加入多播组并希望从源接收多播流。IGMP 连接包括 2 个属性，即组播源和组（S, G）。IGMP 版本 3 用于组播源上的 SSM 和接收器中继一些包含特定源地址。SSM 允许接收方显式接收来自特定多播服务器的流，其源地址由接收方作为 JOIN 请求的一部分显式提供。在此示例中，通过显式包含源 172.9.9.2 来触发 IGMP v3 联接请求，该列表包含源 172.9.9.2，该列表是通过组 232.1.1.1 发送多播流的地址。
2. 分支机构的 Citrix SD-WAN 侦听来自这些接收机的所有 IGMP 请求，并将其转换为成员资格报告，然后通过虚拟路径将其发送到数据中心的 SD-WAN 设备。
3. 数据中心的 Citrix SD-WAN 设备通过虚拟路径接收成员资格报告并将其转发到多播源，从而建立控制通道。
4. 多播源通过虚拟路径将多播流传输到多播接收机。

控制通道流量和多播流经过分支机构和数据中心之间已建立的虚拟路径。Citrix SD-WAN 叠加路径可确保和隔离多播流量免受 WAN 降级或链路变化的影响。

配置多播

要配置多播，请在源和目标位置的 SD-WAN 设备上执行以下操作。

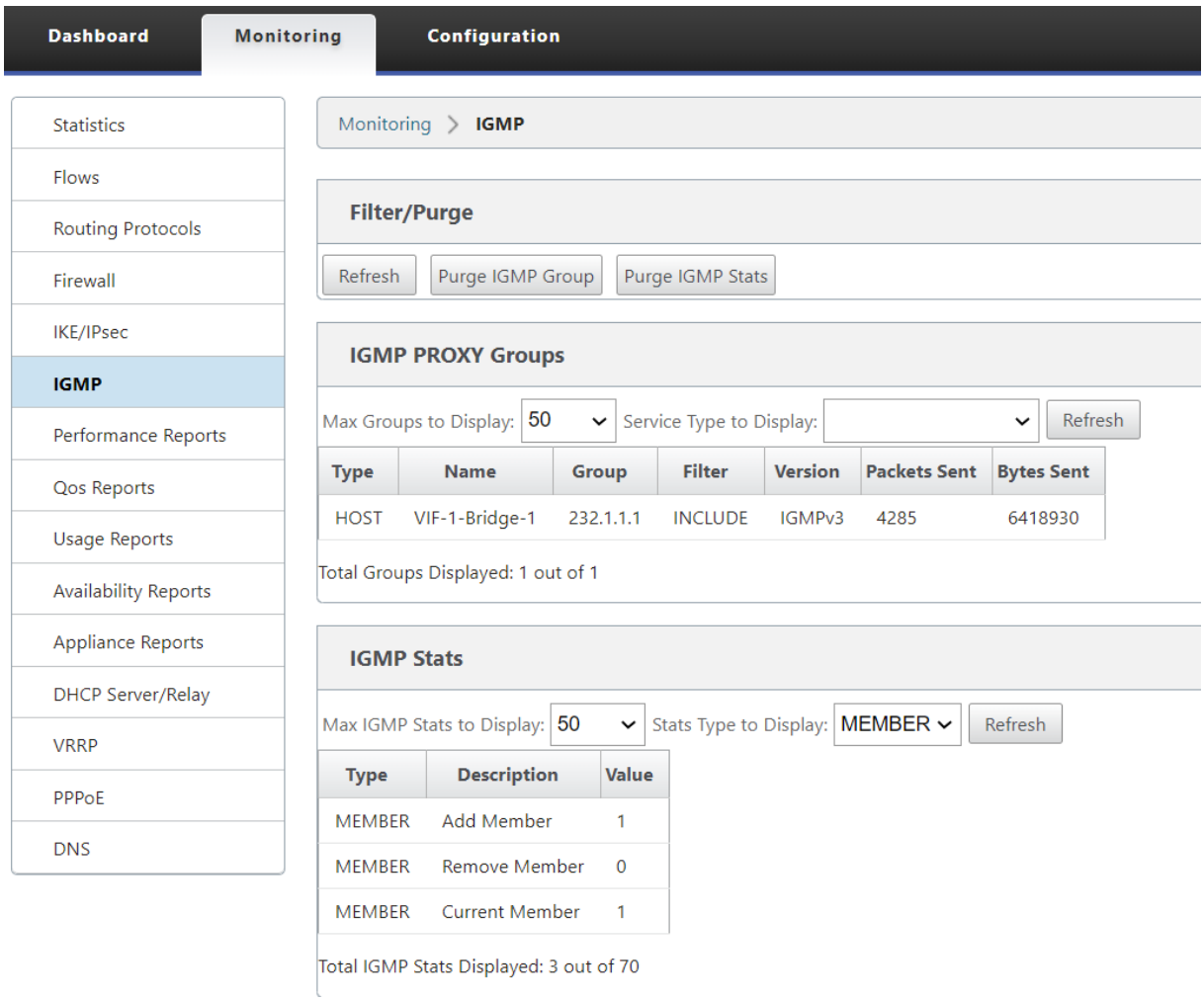
1. 创建多播组-为多播组提供名称和 IP 地址。对于源特定的多播，组播组 IP 必须在 232.0.0.0/8 范围内。
2. 启用 IGMP 代理—您可以将 Citrix SD-WAN 设备配置为 IGMP 代理，以便传输用于多播路由的 IGMP 控制通道信息。要进行单源多播，需要 IGMP V3。
3. 定义上游和下游服务-上游接口使 IGMP 代理能够连接到更接近实际多播源的 SD-WAN 设备，以流式传输流量。下游接口使 IGMP 代理能够连接到远离流通信量的实际多播源的主机。
   源设备和目标设备的上游和下游服务不同。

监视

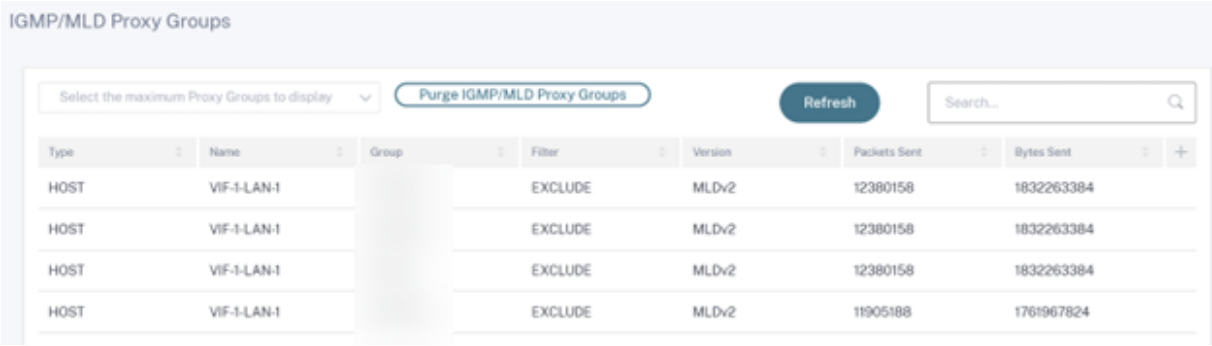
IGMP 统计

当多播接收方发起加入组请求时，您可以在设备上的 监控 > **IGMP** 下看到接收方详细信息。您可以在源设备和目标设备上查看此信息。

下图显示了已启动的 MLD 加入以及用于接收多播组地址的消息类型 RECV。您还可以在下面查看 IGMP/MLD 消息统计信息。



下图显示了有关 IGMP/MLD 代理组的信息。您还可以查看 IGMP/MLD 代理组统计数据和使用的版本。



配置虚拟路径路由成本

September 2, 2022

Citrix SD-WAN 支持以下与数据中心管理相关的路由增强功能。

例如，假设 SD-WAN 网络包含两个数据中心，一个位于北美，另一个位于欧洲。您希望北美地区的所有站点通过北美数据中心路由流量，而欧洲的所有站点都可以使用欧洲数据中心。以前，在 SD-WAN 9.3 和更早版本中，不支持此数据中心管理功能。这是通过引入虚拟路径路由成本来实现的。

- 虚拟路径路由开销：您可以为从远程站点获取路由时添加到路由开销中的各个虚拟路径配置虚拟路径路由开销。

此功能会使 WAN 到 WAN 转发成本失效或删除。

- OSPF 路由成本：您现在可以通过在导入筛选器中启用 复制 **OSPF** 路由成本来导入 **OSPF** 路由成本（类型 1 度量）。在路径选择中考虑 OSPF 路径成本，而不是 SD-WAN 成本。支持高达 65534（而不是 15）的成本，但建议在从远程站点获知路由时适当的虚拟路径路由开销。
- BGP-将 SD-WAN 路由导出（重新分配）到 BGP 对等点时，您现在可以将 SD-WAN 路由的虚拟路径路由开销复制为 BGP MED 值。这可以通过创建 BGP 策略并在每个邻居的“OUT”方向应用它来为单个邻居设置。
- 任何站点都可以有多个到其他站点的虚拟路径。有时，如果存在通过更多虚拟路径连接到服务的分支，则可能会有两条来自分支站点的虚拟路径。一个通过 DC1 的虚拟路径，另一个通过 DC2 的虚拟路径。DC1 可以是一个 MCN，DC2 可以是一个地理 MCN，并且可以配置为具有静态虚拟路径的另一个站点。
- 将每个 VP 的默认成本添加为 1。虚拟路径路由成本有助于将成本与站点的每个虚拟路径相关联。这有助于通过特定虚拟路径（而不是默认站点成本）操作路由交换/更新。有了这个，我们可以操作发送流量的首选数据中心。
- 允许在每个 VP 的小范围内配置成本（例如，1—10）。
- 必须将虚拟路径开销添加到与邻居站点共享的任何路由中，以指示路由首选项，包括通过动态路由获取的路由。
- 没有静态虚拟路径的成本必须低于动态虚拟路径。

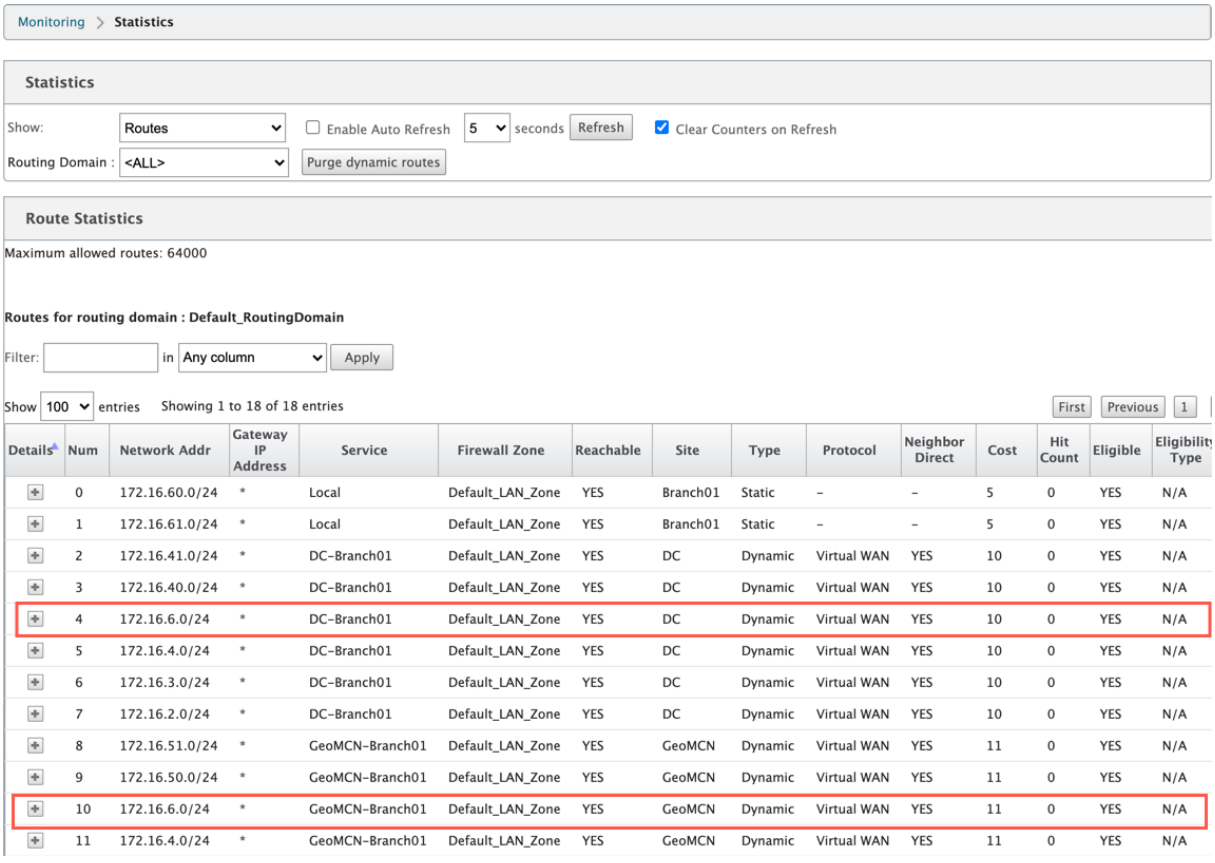
> 注意
>
> VP 路由成本将在版本 10.0 之前发布版本中存在的 WAN 转发成本排除在 WAN 转发成本。基于 WAN 到 WAN 转发成本的路由决策必须通过使用 VP 路由成本来重新影响，因为在迁移到版本 10.0 时，WAN 转发成本并不重要。

监视和故障排除

路由表显示了通过虚拟路径连接到分支站点的两个站点通告的相同子网如何安装，其开销优先级为虚拟路径路由开销。

要验证路由成本以及路由表中使用的路由，请导航到显示字段下的监控 **>** 统计 > 路由。路由成本和命中次数可以在同一页面中进行验证。

下图显示了同一路由的两种不同成本的路由表，即 172.16.6.0/24，服务的成本分别为 **DC-branch01** 和 **GeomCN-Branch01** 。



Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type
	0	172.16.60.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	–	–	5	0	YES	N/A
	1	172.16.61.0/24	*	Local	Default_LAN_Zone	YES	Branch01	Static	–	–	5	0	YES	N/A
	2	172.16.41.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	3	172.16.40.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	4	172.16.6.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	5	172.16.4.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	6	172.16.3.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	7	172.16.2.0/24	*	DC-Branch01	Default_LAN_Zone	YES	DC	Dynamic	Virtual WAN	YES	10	0	YES	N/A
	8	172.16.51.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	9	172.16.50.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	10	172.16.6.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A
	11	172.16.4.0/24	*	GeoMCN-Branch01	Default_LAN_Zone	YES	GeoMCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A

配置虚拟路由器冗余协议

September 2, 2022

虚拟路由器冗余协议 (VRRP) 是一种广泛使用的协议，用于提供设备冗余，以消除静态默认路由环境中固有的单点故障。通过 VRRP，您可以配置两个或更多个路由器以形成一个组。此组显示为具有一个虚拟 IP 地址和一个虚拟 MAC 地址的单个默认网关。

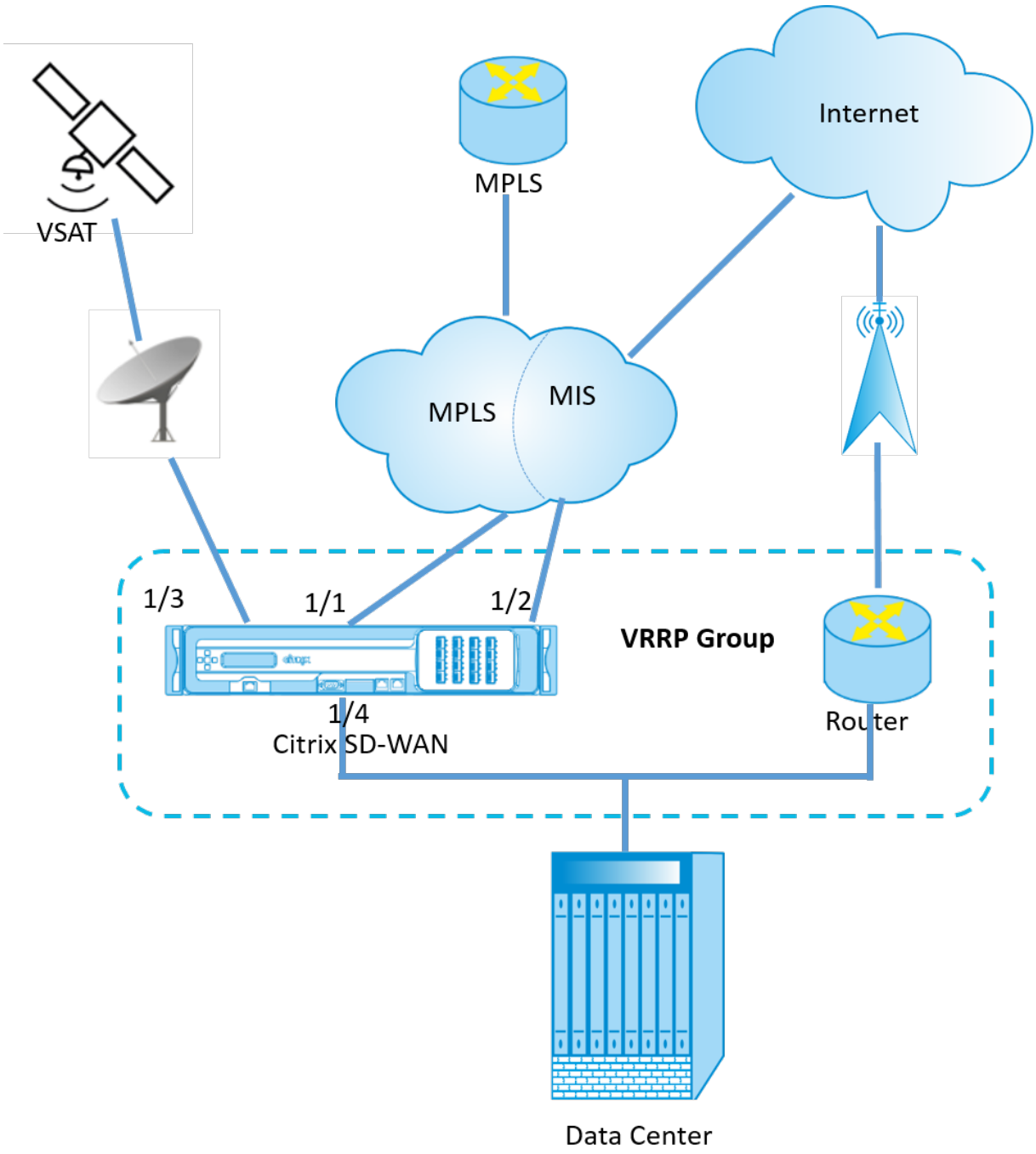
如果主路由器/主路由器出现故障，备份路由器会自动接管。在 VRRP 设置中，主路由器向备份路由器发送称为播发的 VRP 数据包。如果主路由器停止发送播发，备份路由器将设置间隔计时器。如果在此保留期内未收到播发，备份路由器将启动故障转移例程。

VRRP 指定了一个选举过程，其中优先级最高的路由器成为主路由器。如果路由器的优先级相同，则 IP 地址最高的路由器将成为主路由器。其他路由器处于备份状态。如果主服务器失败、新路由器加入组或现有路由器离开组，则会再次启动选择过程。

VRRP 可确保高可用性默认路径，而无需在每个终端主机上配置动态路由或路由器发现协议。

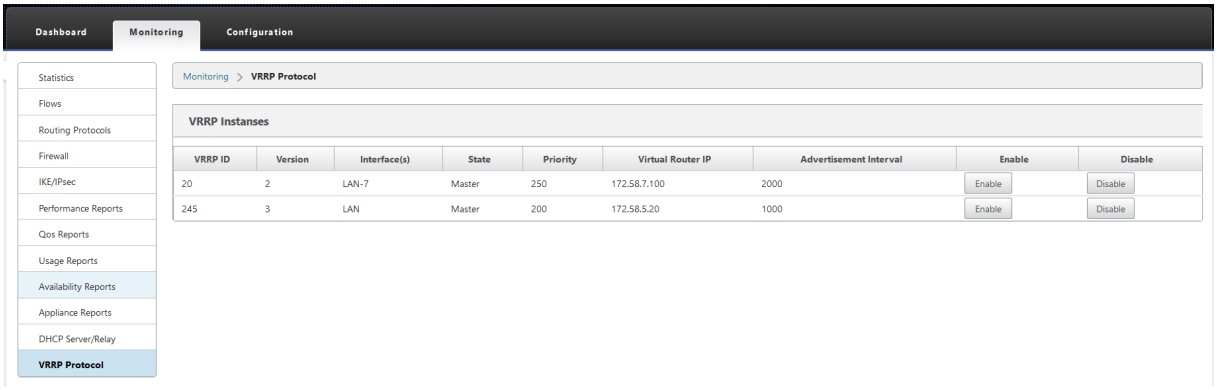
Citrix SD-WAN 版本 10.1 支持 VRP 版本 2 和版本 3 与任何第三方路由器互操作。SD-WAN 设备充当主路由器，并将流量引导到站点之间使用虚拟路径服务。可以将虚拟接口 IP 配置为 VRRP IP，并通过手动将优先级设置为高于对等路由器的值，来将 SD-WAN 设备配置为 VRRP 主服务器。您可以配置播发间隔和抢占选项。

下面的网络图显示了 Citrix SD-WAN 设备和配置为 VRRP 组的路由器。SD-WAN 设备配置为主设备。如果 SD-WAN 设备出现故障，备份路由器将在毫秒内接管，以确保没有停机时间。



VRRP 统计数据

您可以在 监控 > VRRP 下查看 **VRRP** 统计信息。



您可以查看以下统计数据：

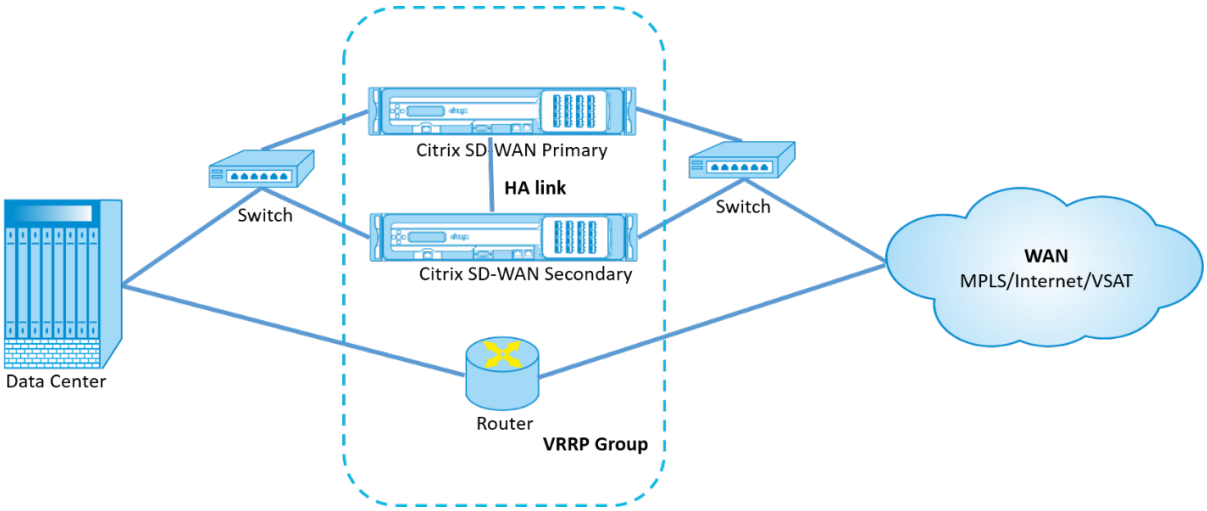
- **VRRP ID**：VRRP 组 ID
- 版本： VRRP 协议版本。
- 接口：用于 VRRP 的虚拟接口。
- 状态： SD-WAN 设备的 VRRP 状态。它指示设备是主设备还是备份。
- 优先级： VRRP 组的 SD-WAN 设备的优先级
- 虚拟路由器 **IP**： VRRP 组的虚拟路由器 IP 地址。
- 播发间隔： VRRP 播发的频率。
- 启用：选择此选项可在 SD-WAN 设备上启用 VRRP 实例。
- 禁用：选择此选项可在 SD-WAN 设备上禁用 VRRP 实例。

限制

- 仅在网关模式部署中支持 VRP。
- 您最多可以配置四个 VRRP ID (VRID)。
- 多达 16 个虚拟网络接口可以参与 VRID。

高可用性和 **VRRP**

通过利用 SD-WAN 网络上的高可用性和 VRRP 功能，您可以显著减少网络停机时间和流量中断。在主动/备用角色中部署一对 Citrix SD-WAN 设备以及备用路由器，以形成 VRRP 组。此组显示为具有一个虚拟 IP 地址和一个虚拟 MAC 地址的单个默认网关。



以下是上述部署的 2 个案例：

第一种情况：**SD-WAN** 上的高可用性故障转移计时器等于 **VRRP** 故障切换计时器。

预期的行为是在 VRRP 切换之前发生高可用性切换，即流量继续流经新的活动 SD-WAN 设备。在这种情况下，SD-WAN 将继续使用 VRRP 主角色。

第二种情况：**SD-WAN** 上的高可用性故障转移计时器大于 **VRRP** 故障切换计时器。

预期的行为是发生 VRRP 切换到路由器的情况，即路由器变成 VRRP Master，流量可能会暂时流经路由器，绕过 SD-WAN 设备。

但是，一旦高可用性切换发生，SD-WAN 将再次成为 VRRP 主机，也就是说，流量现在流经新的活动 SD-WAN 设备。

有关高可用性部署模式的详细信息，请参阅 高可用性。

LAN 分段路由支持

September 2, 2022

SD-WAN 标准版设备在部署了任一设备的不同站点之间实施局域网分段。设备识别并维护局域网端可用 VLAN 的记录，并围绕其他 SD-WAN 标准版设备可以在远程位置连接的其他 LAN 网段 (VLAN) 配置规则。

上述功能是通过使用在 SD-WAN 标准版设备中维护的虚拟路由和转发 (VRF) 表来实现的，该表跟踪本地 LAN 分段可访问的远程 IP 地址范围。此 VLAN 到 VLAN 的流量仍然会通过两个设备之间的相同预先建立的虚拟路径遍历 WAN（无需创建新路径）。

此功能的一个示例是，WAN 管理员可能能够通过 VLAN 对本地分支网络环境进行分割，并提供其中一些区段 (VLAN) 访问权限可以访问 Internet 的 DC 端 LAN 段，而其他人则可能无法获得此类访问权限。

路由间域服务

September 2, 2022

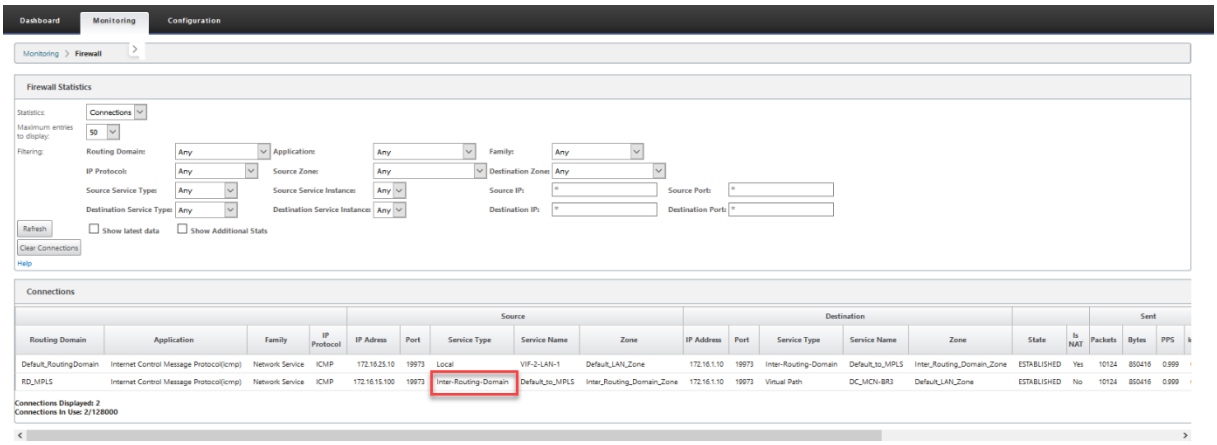
Citrix SD-WAN 允许您使用路由域对网络进行分段，从而确保高安全性和易于管理。使用路由域后，重叠网络中的流量彼此隔离。每个路由域都维护自己的路由表。但是，有时我们需要在路由域之间路由流量。例如，如果打印机、扫描仪和邮件服务器等共享服务被置备为单独的路由域。要使来自不同路由域的用户能够访问共享服务，需要路由间域。

Citrix SD-WAN 提供静态路由间域服务，允许在站点内部的路由域之间或不同站点之间发生路由泄漏。这样就不需要边缘路由器来处理路由泄漏。路由间域服务可以进一步用于设置路由、防火墙策略和 NAT 规则。

Inter_Rouing_Domain_Zone 是一个新的防火墙区 域，默认情况下创建，并作为路由间域服务的防火墙区域，用于路由和过滤。

监视

您可以在监视 > 防火墙统计 **>** 连接下查看使用路由域间服务的连接的监视统计信息。



ECMP 负载平衡

September 2, 2022

等价多路径 (ECMP) 组允许您将多条路径分组成相同的成本、目标和服务。连接或会话数据在 ECMP 组中的所有路径之间进行负载平衡，具体取决于 ECMP 组的类型。例如，假设分支机构和数据中心之间具有两条 WAN 链路的网络，路由成本相同。传统上，其中一个 WAN 链路将处于活动状态，另一条仍处于休眠状态，充当后备链路。使用 ECMP Groups，您可以将这些 WAN 链路组合在一起，并允许通过两个 WAN 链路进行负载平衡流量。ECMP 负载均衡可确保：

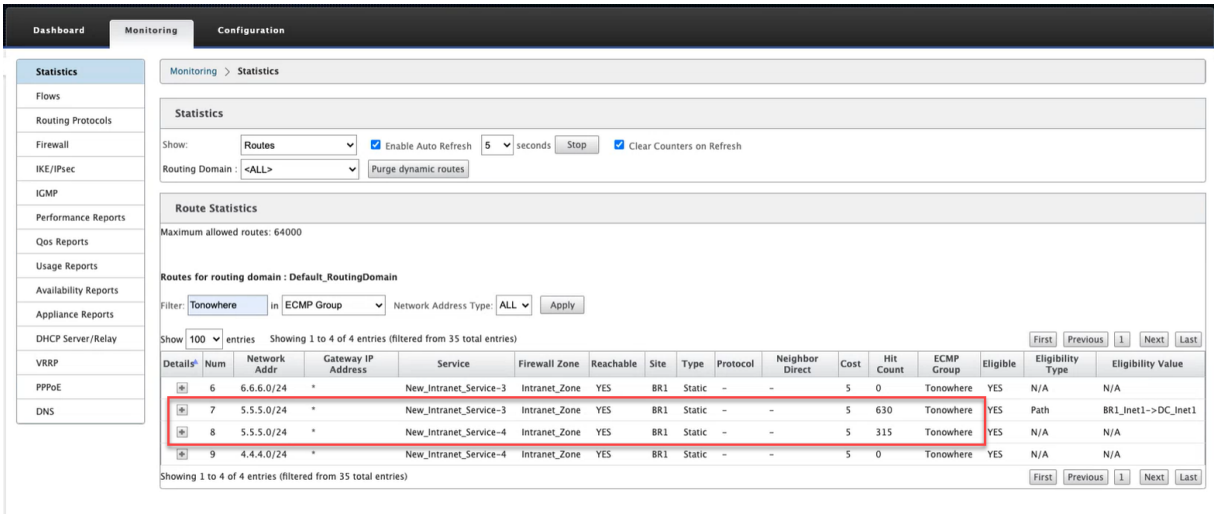
- 通过多条等价路径分布流量。

- 最佳利用可用带宽。
- 如果链路出现故障，将流量动态传输到其他 ECMP 成员路径。ECMP 支持 IPSEC/GRE 通道上的静态路由。

虚拟路径和内联网服务支持 ECMP 负载平衡。ECMP 组是在全球范围内定义的。您最多可以在网络中定义 254 个 ECMP 组。ECMP 组中符合 ECMP 条件的路由的最大数量取决于您的设备和许可证类型。Citrix SD-WAN 支持以下两种类型的 ECMP 组：

- 源/目标 IP 地址：多个客户端尝试连接到同一目标的 网络，连接在同等成本的 WAN 链路之间进行负载平衡。
- 会话：一个客户端连接到目标并生成多个会话的 网络。会话数据在同等成本的 WAN 链路之间进行负载平衡。

要监控 ECMP 负载平衡，请在 SD-WAN UI 中导航到 监 控 > 统计 > 路由，然后使用 ECMP 组名过滤搜索结果。



在示例数据中，我们看到服务中具有公共 ECMP 组的所有路由都是该 ECMP 组的一部分。例如，6.6.6.0/24 和 5.5.5.0/24 在 ECMP 组中无处不 在。但是，流量负载在共享目标 IP 5.5.5.0/24 并关联到同一 ECMP 组的 **New_Intranet_Ser**vice-3 和 **New_Intranet_Service-4** 之间进行平衡。

> 注意
>
> 对于 SIA 和 Zscaler 服务，您可以使用 ECMP（主动/主动）在两条 IPsec 通道路径之间进行负载均衡。

安全性

September 2, 2022

本节中的主题 提供了 Citrix SD-WAN 部署的一般安全指南。

Citrix SD-WAN 部署指南

为了在整个部署生命周期内维护安全性，Citrix 建议考虑以下安全因素：

- 物理安全
- 设备安全性
- 网络安全
- 行政和管理

以下链接中描述的主题提供了有关如何使用配置 SD-WAN 网络安全性的详细信息：

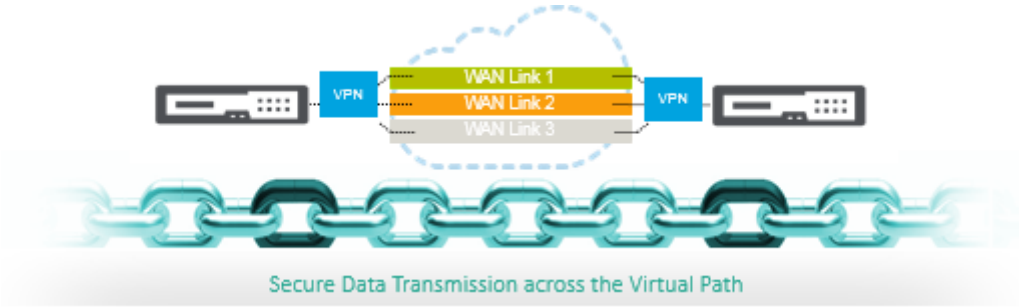
- IPsec 通道
- 防火墙

IPsec 通道终止

September 2, 2022

Citrix SD-WAN 支持 IPsec 虚拟路径，使第三方设备能够终止 Citrix SD-WAN 设备的局域网或广域网端的 IPsec VPN 通道。通过使用 140-2 级别 1 FIPS 认证的 IPsec 加密二进制文件，可以保护 SD-WAN 设备上站点到站点 IPsec 通道终止。

Citrix SD-WAN 还支持使用存在差别的虚拟路径通道机制的弹性 IPsec 通道。



> 重要注意事项：
>
> - 从 SD-WAN 11.5 版本起，所有 IPsec 通道配置和 IKE 设置都只能通过 Citrix SD-WAN Orchestrator 服务获得支持。有关 Citrix SD-WAN Orchestrator 服务 IPsec/IKE 配置的信息，请参阅 IPsec 服务。
> - Citrix SD-WAN 支持通过 IPsec 连接到 Oracle 云基础设施 (OCI)。

Citrix SD-WAN 与 AWS 传输网关的集成

November 16, 2022

Amazon Web Service (AWS) 中转网关 服务使客户能够将其亚马逊虚拟私有云 (VPC) 及其本地网络连接到单个网关。随着 AWS 上运行的工作负载数量的增加，您可以跨多个账户和 Amazon VPC 扩展网络，以跟上增长的步伐。

现在，您可以使用对等互连连接一对 Amazon VPC。但是，管理许多 Amazon VPC 之间的点对点连接，而无法集中管理连接策略，则可能会成本高昂且繁琐。对于本地连接，您需要将 AWS VPN 连接到每个单独的 Amazon VPC。当 VPC 数量增加到数百个时，此解决方案可能非常耗时，而且很难进行管理。

使用 **AWS Transit Gateway**，您只需创建和管理从中央网关到网络中的每个 Amazon VPC、本地数据中心或远程办公室的单个连接。Transit Gateway 充当一个集线器，控制如何在所有连接的网络之间路由流量，这些网络的作用类似于辐条。这种集线器和分支模式显著简化了管理并降低了运营成本，因为每个网络只需连接到 Transit Gateway 网关，而不是连接到所有其他网络。任何新 VPC 都连接到传输网关，并自动对连接到传输网关的所有其他网络使用。这种易于连接的方便性使您可以随着您的增长轻松扩展网络。

随着企业越来越多的应用、服务和基础设施迁移到云端，他们正在快速部署 SD-WAN，以实现宽带连接的优势，并将分支站点用户直接连接到云资源。使用 Internet 传输服务构建和管理全球专用网络，将分布在地理位置的位置和用户与基于邻近地区的云资源连接起来，面临许多挑战。**AWS Transit Gateway** 网络管理器 改变了这种模式。现在，使用 AWS 的 Citrix SD-WAN 客户可以通过集成 Citrix SD-WAN 分支设备 AWS Transway Gateway，将 Citrix SD-WAN 与 AWS 传输网关结合使用，从而为能够接触到连接到传输网关的所有 VPC 的用户提供最高质量的体验。

以下是将 Citrix SD-WAN 与 AWS 传输网关集成的步骤：

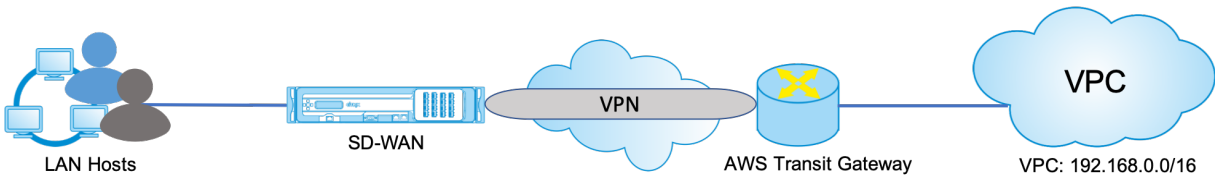
1. 创建 AWS 中转网关。
2. 将 VPN 连接到传输网关（现有 VPN 或新 VPN）。
3. 将 VPN 连接到配置的传输网关，其中 VPN 所在的 SD-WAN 站点位于 PREM 或任何云（AWS、Azure 或 GCP）中。
4. 通过 IPsec 通道与来自 Citrix SD-WAN 的 AWS 传输网关建立边界网关协议 (BGP) 对等，以了解连接到中转网关的网络 (VPC)。

用例

使用案例是从分支环境接触 AWS 内部（在任何 VPC 中）的资源。使用 AWS 中转网关可让流量到达连接到传输网关的所有 VPC，而无需处理 BGP 路由。要实现此目的，请执行以下方法：

- 从分支机构 Citrix SD-WAN 设备建立到 AWS 传输网关的 IPsec。在此部署方法中，您将无法获得完整的 SD-WAN 优势，因为流量将通过 IPsec 进行。
- 在 AWS 中部署 Citrix SD-WAN 设备，并通过虚拟路径将其连接到您的本地 Citrix SD-WAN 设备。

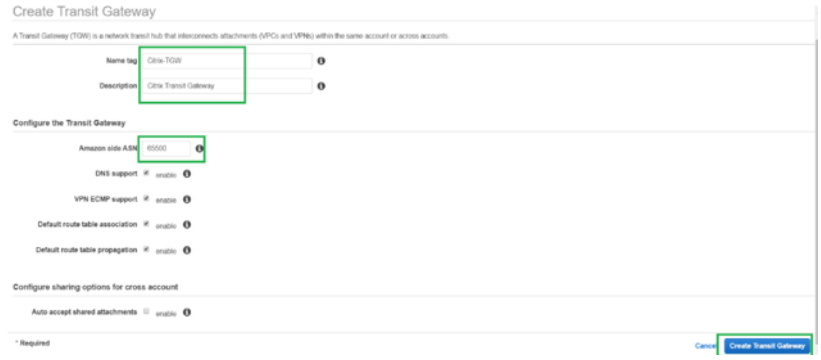
无论选择哪种方法，流量都会到达连接到传输网关的 VPC，而无需手动管理 AWS 下方的路由。



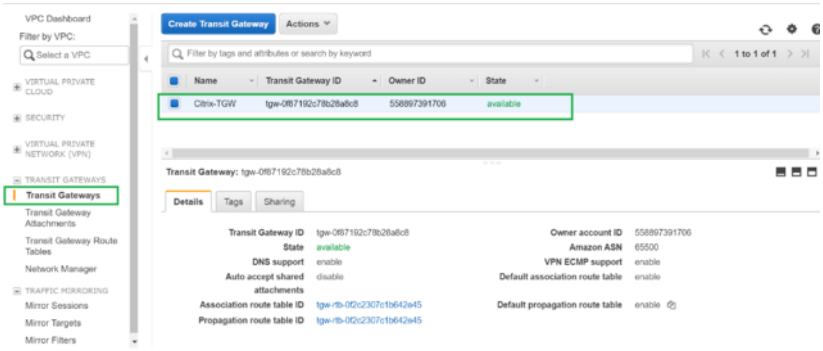
AWS 中转网关配置

要创建 **AWS Transit Gateway**，请导航到 VPC 控制面板，然后转到中 转网关 部分。

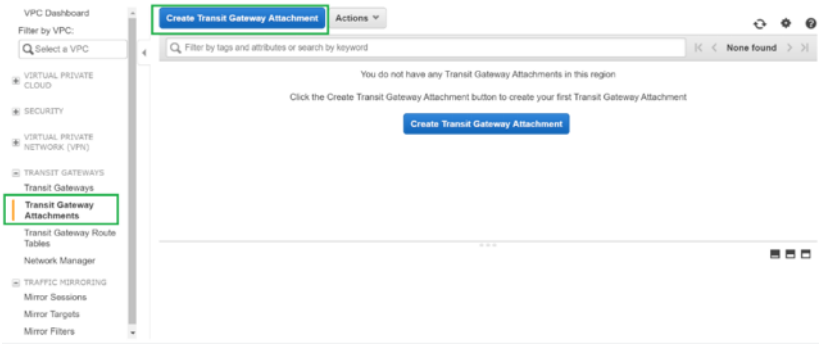
1. 提供以下屏幕截图中突出显示的中转网关名称、描述和 Amazon ASN 编号，然后单击 创建交通网关。



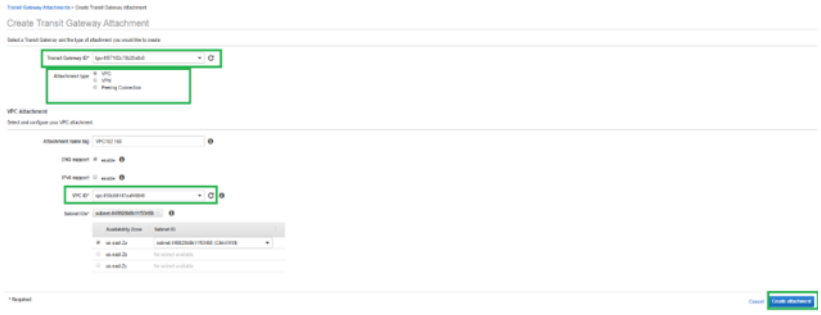
交通网关创建完成后，您可以看到状态为“可 用”。



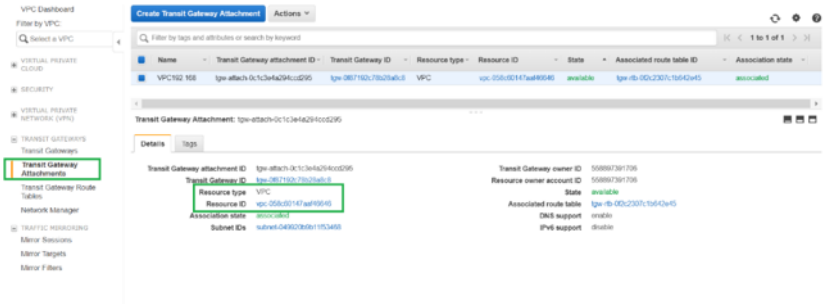
2. 要创建公 交网关附件，请导航到中 转网关 **>** 中转网关附件，然后单击 创建中转网关附件。



3. 从下拉列表中选择创建的中转网关，然后选择附件类型作为 **VPC**。提供附件名称标签，然后选择要连接到创建的传输网关的 VPC ID。将自动选择所选 VPC 中的其中一个子网。单击 创建附件 将 VPC 附加到中转网关。

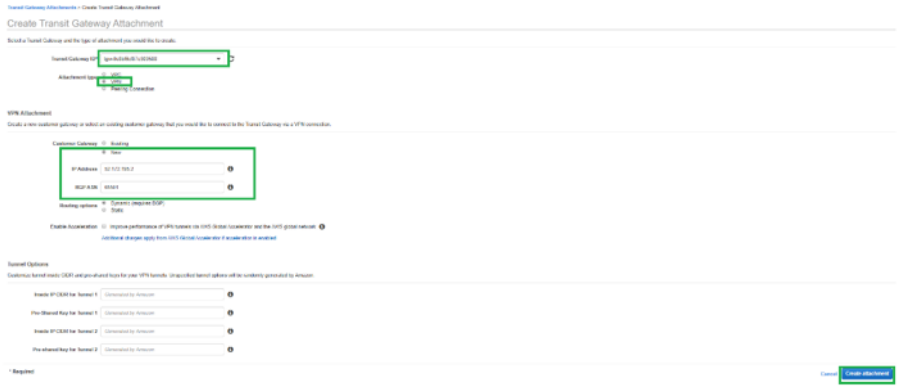


4. 将 VPC 连接到中转网关后，您可以看到 资源类型 **VPC** 已关联到中 转网关。

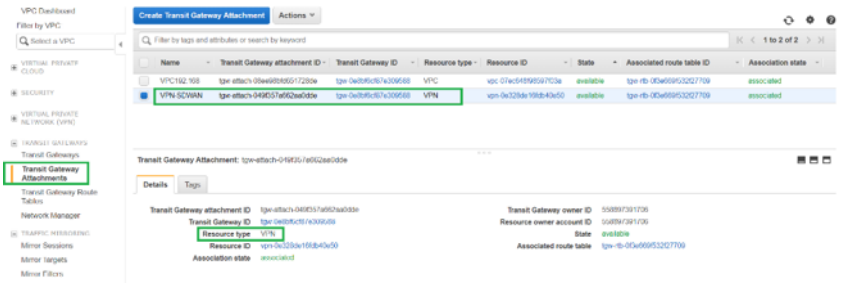


5. 要使用 VPN 将 SD-WAN 连接到中转网关，请从下拉列表中选择中 转网关 **ID** ，然后选择 附件类型 作为 **VPN**。确保您选择了正确的传输网关 ID。

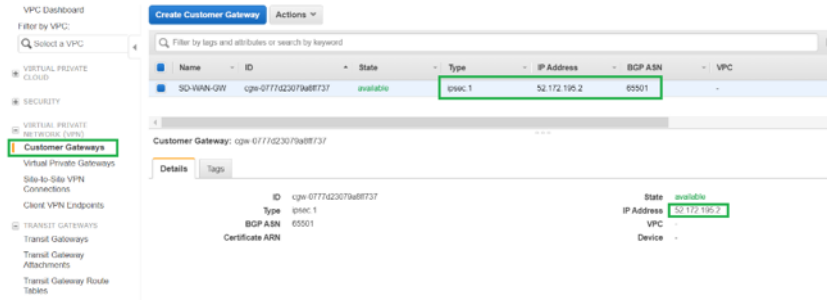
   通过提供 SD-WAN 链路公有 IP 地址及其 BGP ASN 编号，连接新的 VPN 客户网关。单击 创建附件 以使用中转网关连接 VPN。



6. 将 VPN 连接到传输网关后，您可以查看详细信息，如以下屏幕截图所示：

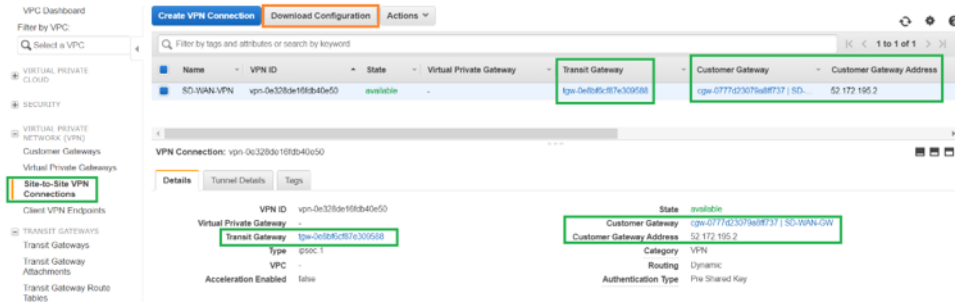


7. 在 客户网关下，SD-WAN 客户网关和站点到站点 VPN 连接是作为连接到中转网关的 VPN 的一部分创建的。您可以看到 SD-WAN 客户网关与此客户网关的 IP 地址一起创建，该地址代表 SD-WAN 的 WAN 链路公有 IP 地址。

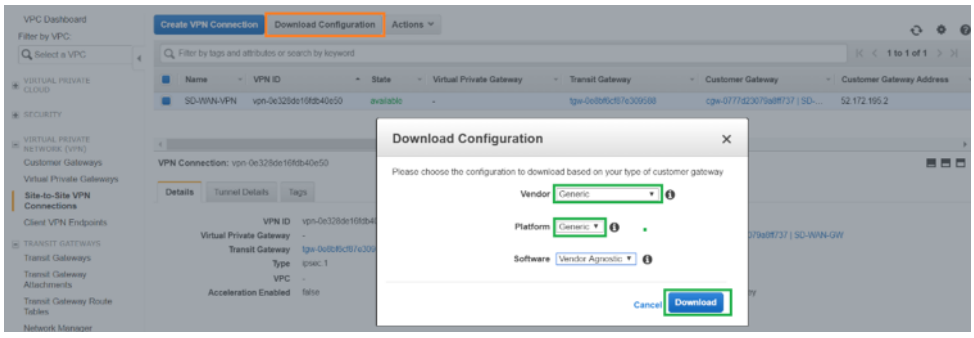


8. 导航 到站点到站点 **VPN** 连接 以下载 **SD-WAN** 客户网关 **VPN** 配置。此配置文件包含两个 IPSec 通道详细信息以及 BGP 对等信息。从 SD-WAN 到传输网关之间创建两条通道，以实现冗余。

   您可以看到 SD-WAN 链路公有 IP 地址被配置为客户网关地址。



9. 单击 下载配置，然后下载 VPN 配置文件。选择 供应商、平台 作为 通用模式和 软件 作为 供应商无关。



   下载的配置文件包含以下信息：

   - IKE 配置
   - AWS 中转网关的 IPSec 配置
   - 通道接口配置
   - BGP 配置

   此信息适用于两个 IPSec 通道以实现高可用性 (HA)。在 SD-WAN 中配置这两个通道端点时，请确保配置这两个通道端点。请参阅以下屏幕截图以供参考：

![两条 IPsec 通道] (/en-us/citrix-sd-wan/current-release/media/two-ipsec-tunnels.png)

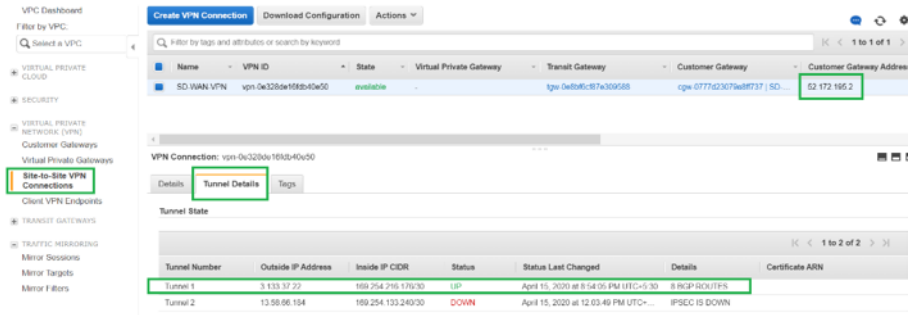
在 **SD-WAN** 上配置内部网服务

要通过 Citrix SD-WAN Orchestrator 服务配置内部网服务，请转到 交付服务。

AWS 上的监控和故障排除

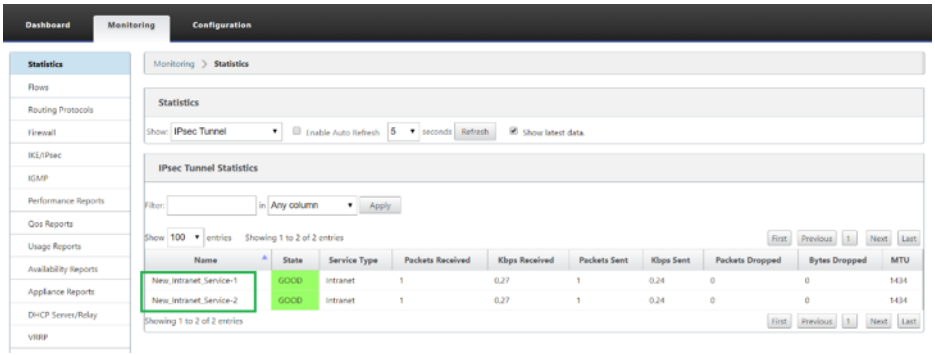
1. 要验证 AWS 上的 IPsec 通道建立状态，请导航到 虚拟专用网络 **(VPN) >** 站点到站点 **VPN** 连接。在以下屏幕截图中，您可以看到客户网关地址代表 SD-WAN 链路公有 IP 地址，您已使用该地址建立了通道。

   通道状态显示为 **UP**。此外，可以观察到，AWS 已从 SD-WAN 中学习了 **8** 个 **BGP ROUT** S。这意味着 SD-WAN 能够通过 AWS 中转网关建立通道，并能够通过 BGP 交换路由。

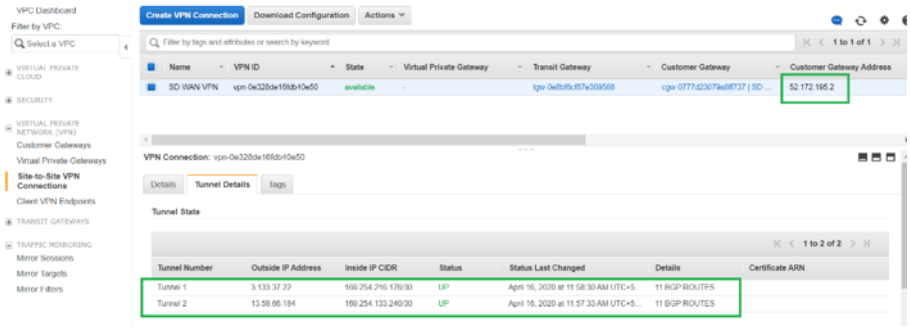


2. 根据 SD-WAN 上下载的配置文件，配置与第二条通道相关的 IPSec 和 BGP 详细信息。

   可以在 SD-WAN 上监控与两条通道相关的状态，如下所示：



3. 可以在 AWS 上监控与两个通道相关的状态，如下所示：

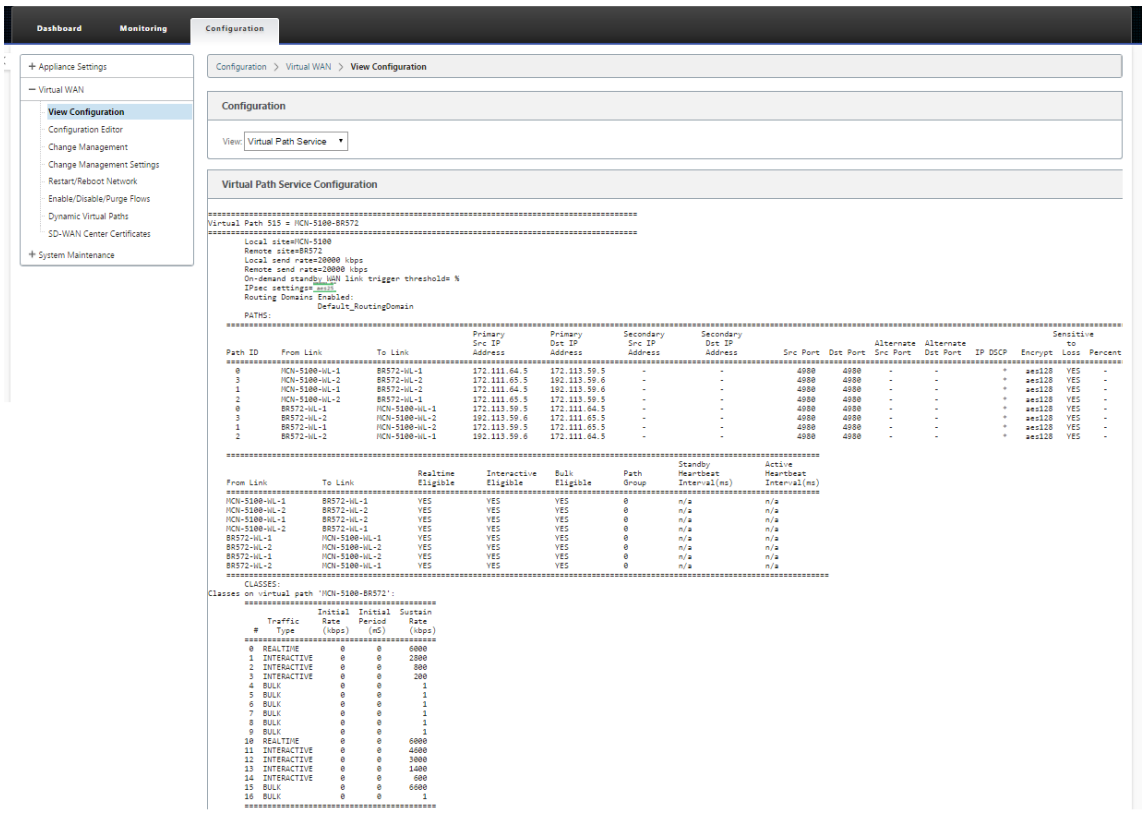


如何查看 **IPsec** 通道配置

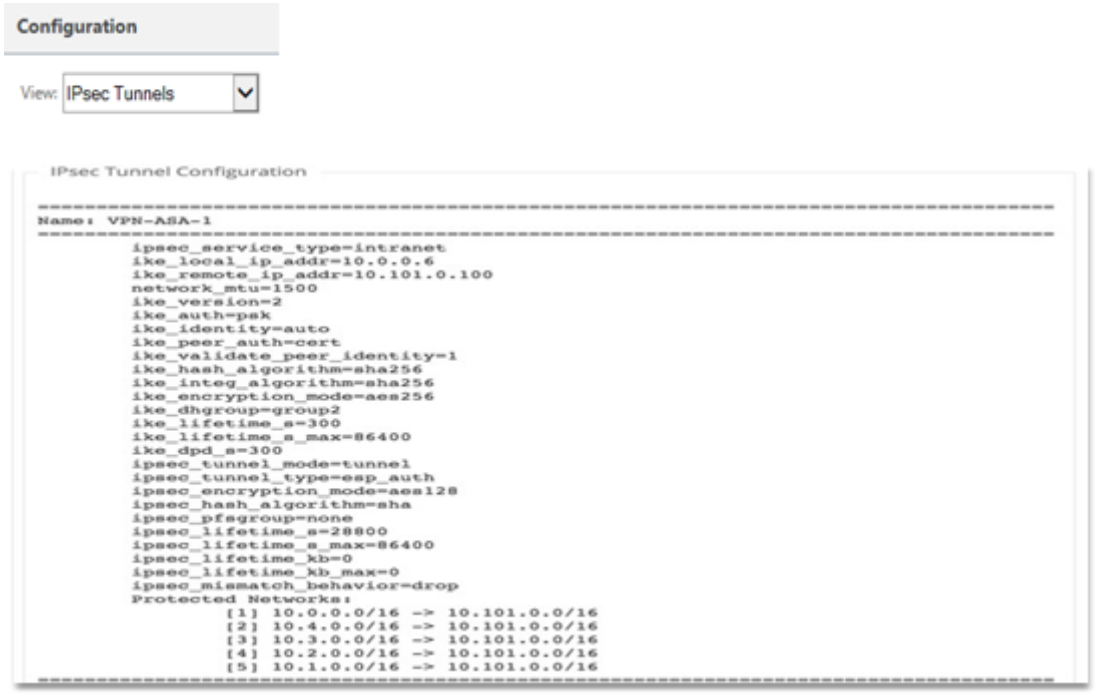
September 2, 2022

要查看 IPsec 通道配置，请执行以下操作：

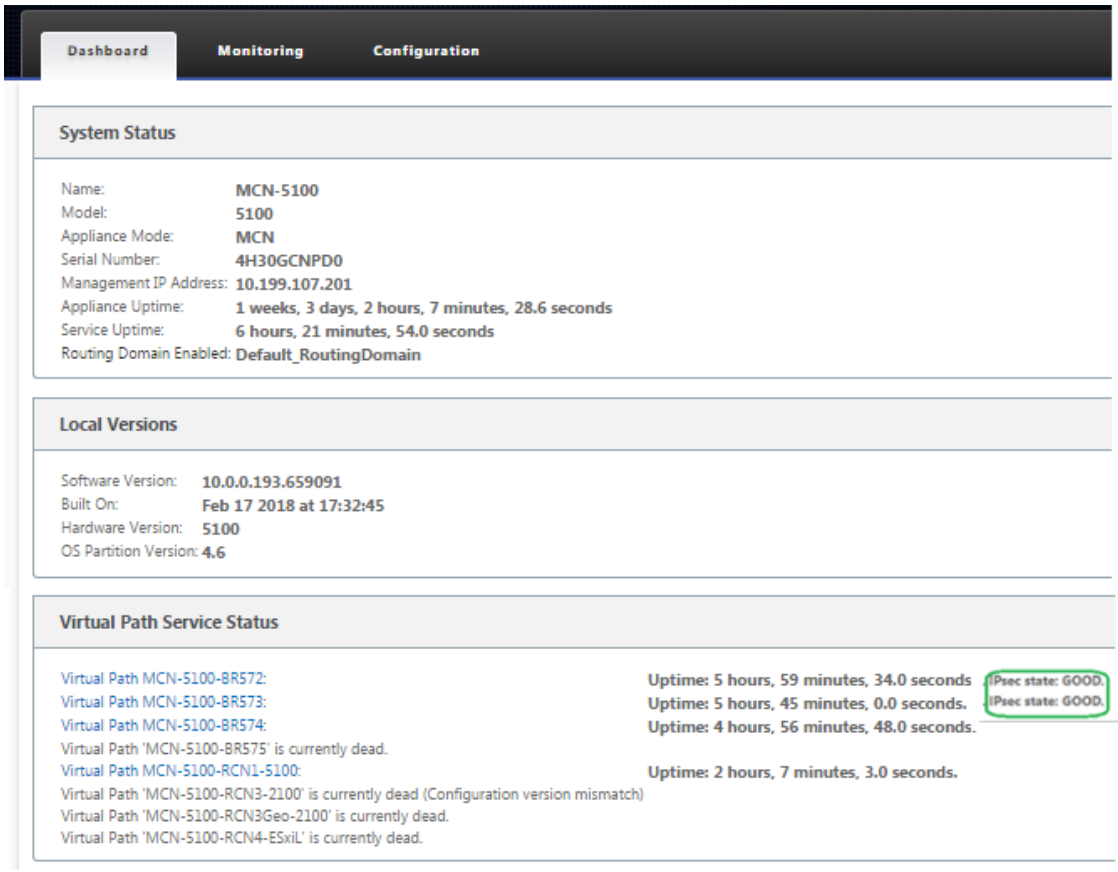
1. 导航到 配置 **>** 虚拟 **WAN** > 查看配置。
2. 从下拉菜单中选择 虚拟路径服务。仅当启用 IPsec 时，才会显示 IPSec 设置。



3. 从下拉菜单中选择 **IPsec** 隧 道以查看 IPsec 通道配置。



4. 每个虚拟路径将显示其自己的 IPsec 通道状态，如下所示。

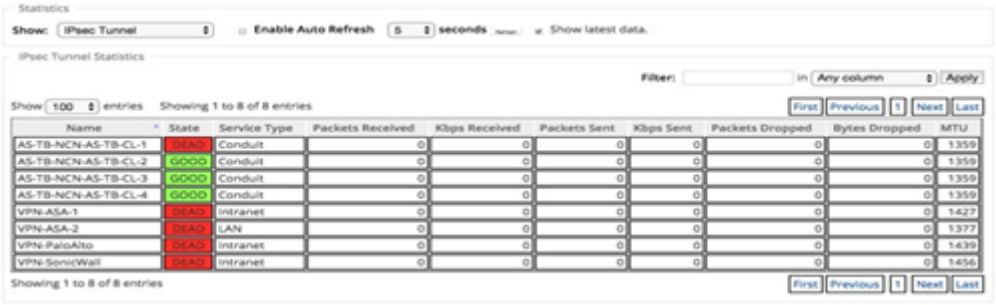


IPsec 监视和记录

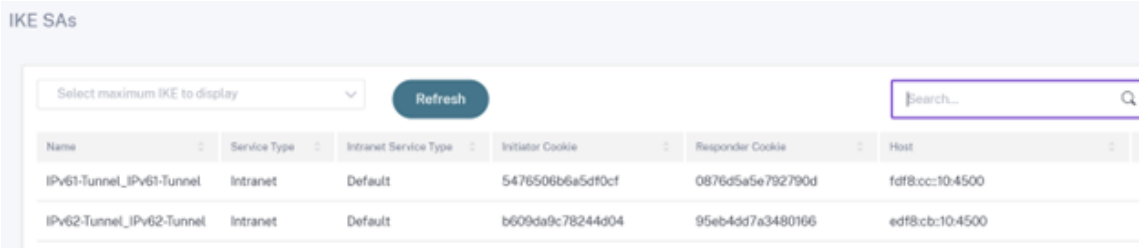
September 2, 2022

要监视 IPsec/IKE SA 统计信息，请执行以下操作

1. 导航到 监控 **> IPsec**。选择 **IPsec SA**:



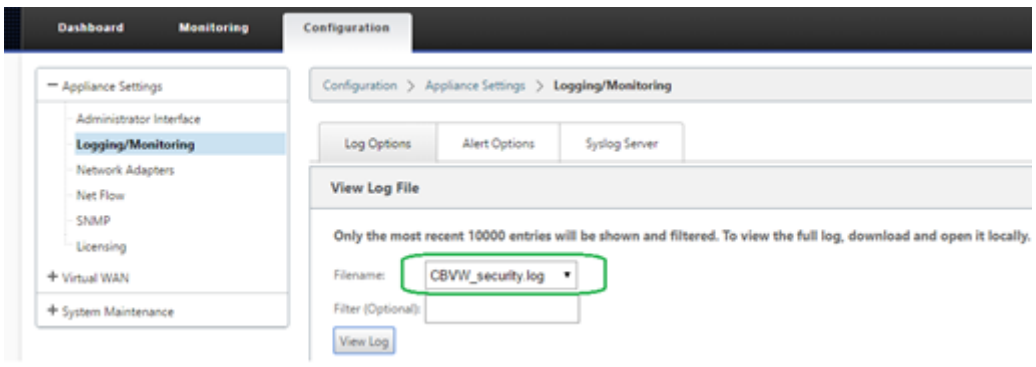
2. 导航到 监控 > **IKE SA**。观察在 SD-WAN 网络中配置的两个或模式 VPN 终端之间配置的 IPsec 通道、IKE 和 IPsec 服务关联。



如何监控 **IPsec** 日志

1. 导航到 配置 > 装置设 置 > 记录/监控。从下拉菜单中选择 文件名，然后单击 查看日志。您可以查看 IPsec 通道的以下日志详细信息：

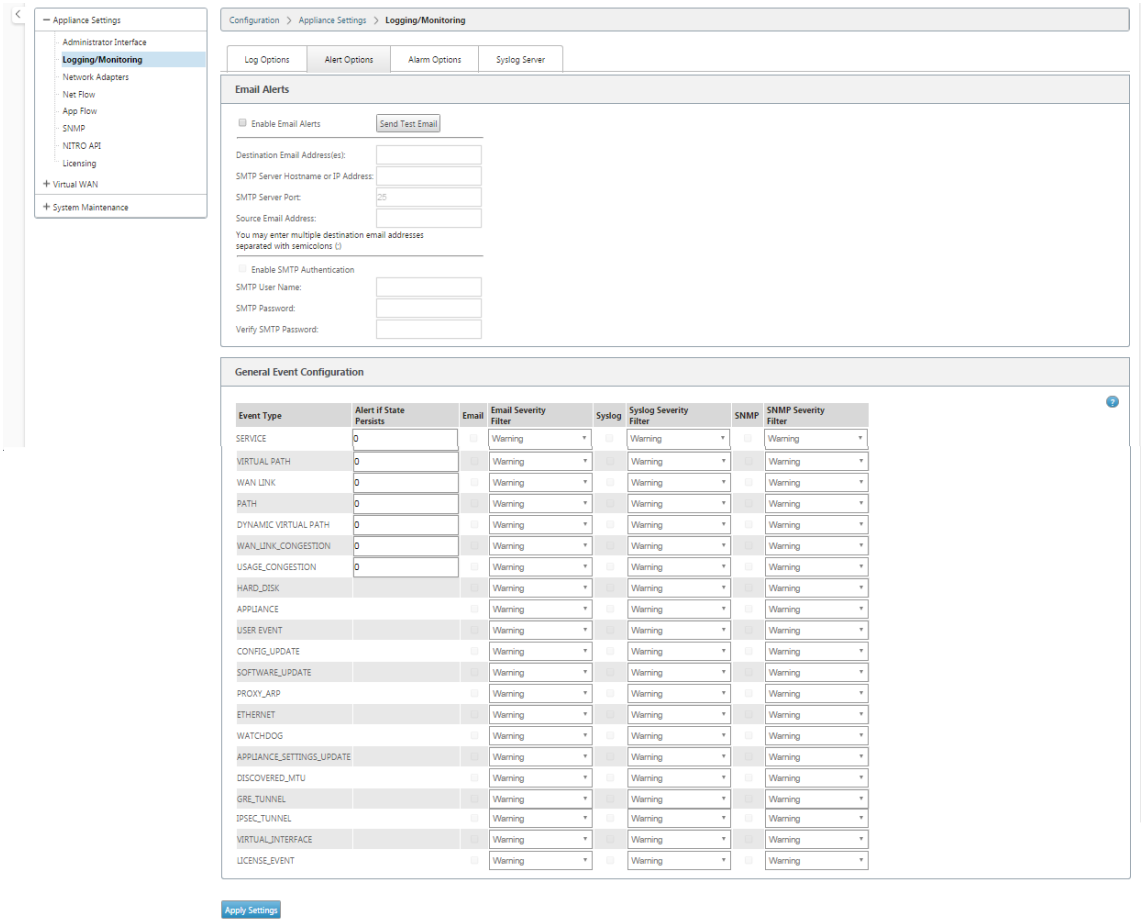
   - IPsec 通道的创建与删除
   - IPsec 通道状态更改




```
00028:940:324:607 INFO                Current time is:Tue Mar 22 19:02:46 2016
00029:000:334:900 INFO                Current time is:Tue Mar 22 19:03:46 2016
00029:060:345:638 INFO                Current time is:Tue Mar 22 19:04:46 2016
00029:064:056:825 INFO  Citrix_IkeStatHdlr@forward/hosted/ipsec_host.c:3327     IKE SA CREATED (Virtual Path MCN1-BR2CB2K): v=2,_R,id=0xaf3151ca,rc=OK,next state=GOOD
00029:064:492:766 INFO  Citrix_IkeStatHdlr@forward/hosted/ipsec_host.c:3327     IKE SA CREATED (Virtual Path MCN1-BR1): v=2,_R,id=0xaf3151c9,rc=OK,next state=GOOD
00029:119:436:901 INFO  Citrix_IkeStatHdlr@forward/hosted/ipsec_host.c:3361     IKE SA DELETED (Virtual Path MCN1-BR2CB2K: v=2,_R,id=0xaf3151ca,rc=STATUS_IKE_DELETE_PAYLOAD,next state=GOOD
00029:119:841:550 INFO  Citrix_IkeStatHdlr@forward/hosted/ipsec_host.c:3361     IKE SA DELETED (Virtual Path MCN1-BR1: v=2,_R,id=0xaf3151c9,rc=STATUS_IKE_DELETE_PAYLOAD,next state=GOOD
00029:120:356:054 INFO                Current time is:Tue Mar 22 19:05:46 2016
00029:180:366:422 INFO                Current time is:Tue Mar 22 19:06:46 2016
00029:240:376:931 INFO                Current time is:Tue Mar 22 19:07:46 2016
```

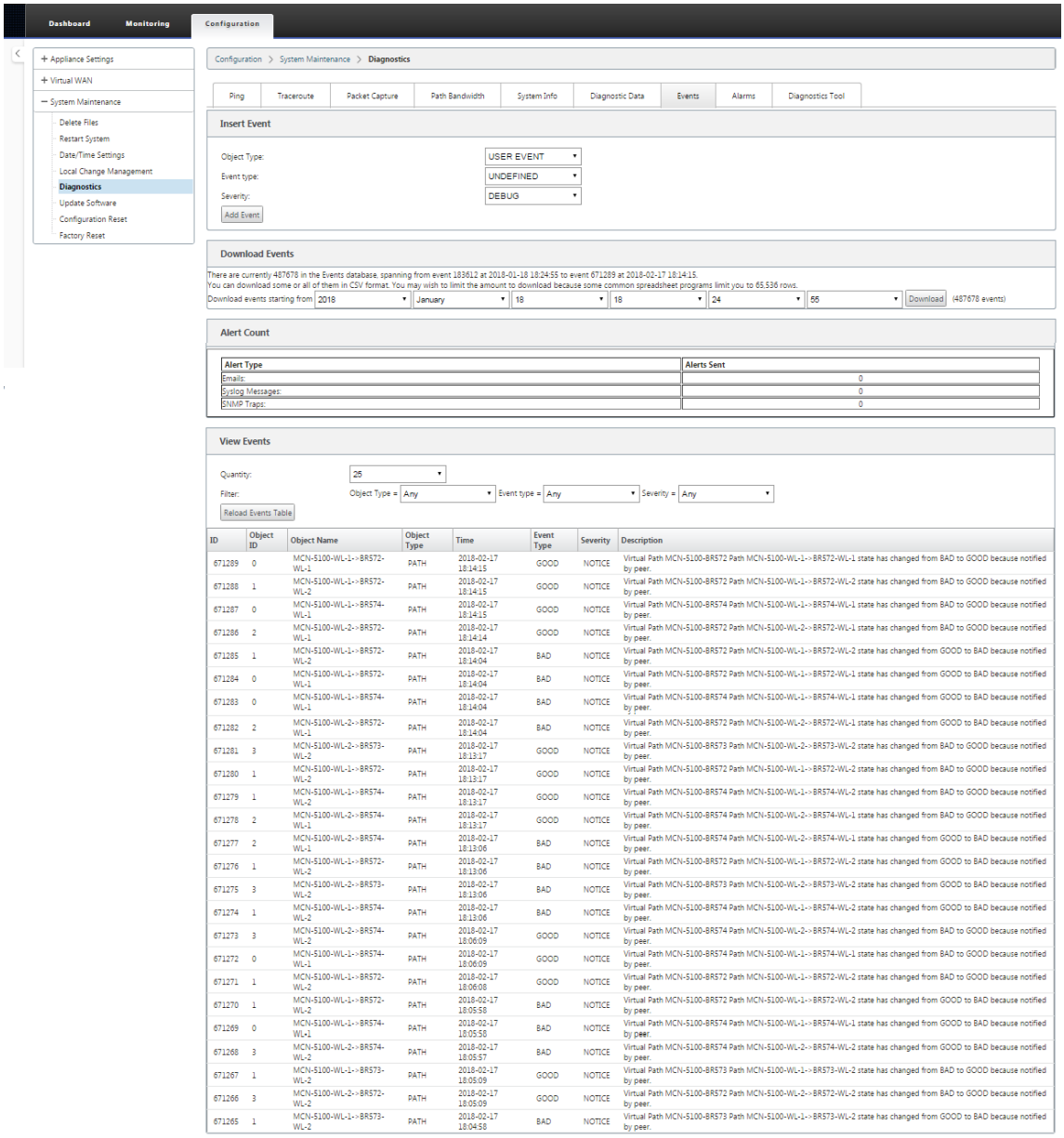
如何查看 **IPSec** 通道警报

1. 导航到 配置 > 装置设置 **>** 日志记录/监控 > 警报选项。
2. 为 IPsec 通道状态报告创建电子邮件和系统日志警报。
    - 支持 IPsec_TUNNEL 作为允许您配置电子邮件和系统日志严重性筛选器的事件类型之一。



如何监控 **IPSec** 通道事件

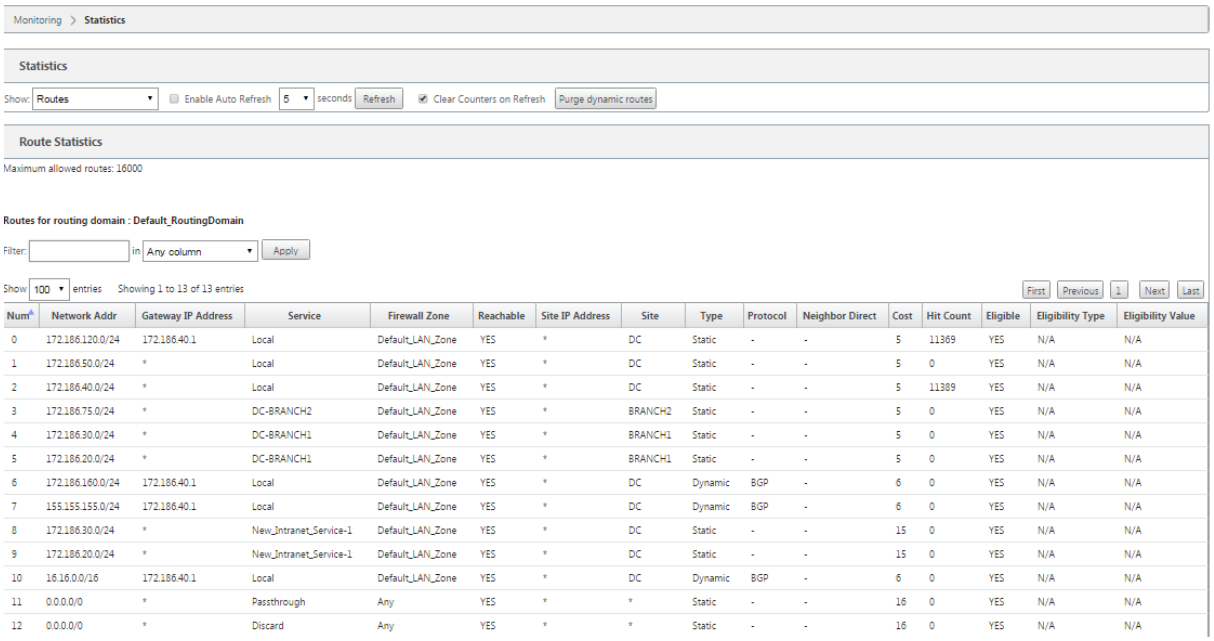
1. 导航到 配置 **>** 系统维护 > 诊断 > 事件。
2. 根据 **IPSEC_TUNDEN** D 对象类型添加事件。为所有 IPsec 相关事件创建过滤器。



IPsec 非虚拟路径路由的资格

September 2, 2022

在以前的版本中，IPsec 通道路由将保留在路由表中，即使通道变为不可用。



Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.186.120.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11369	YES	N/A	N/A
1	172.186.50.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11389	YES	N/A	N/A
3	172.186.75.0/24	*	DC-BRANCH2	Default_LAN_Zone	YES	*	BRANCH2	Static	-	-	5	0	YES	N/A	N/A
4	172.186.30.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
5	172.186.20.0/24	*	DC-BRANCH1	Default_LAN_Zone	YES	*	BRANCH1	Static	-	-	5	0	YES	N/A	N/A
6	172.186.160.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
7	155.155.155.0/24	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
8	172.186.30.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
9	172.186.20.0/24	*	New_Intranet_Service-1	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
10	16.16.0.0/16	172.186.40.1	Local	Default_LAN_Zone	YES	*	DC	Dynamic	BGP	-	6	0	YES	N/A	N/A
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

FIPS 合规性

September 2, 2022

在 Citrix SD-WAN 中，FIPS 模式强制用户为其 IPsec 通道配置 FIPS 兼容设置和虚拟路径的 IPsec 设置。

- 显示符合 FIPS 的 IKE 模式。
- 显示符合 FIPS 标准的 IKE DH 组，用户可以从中选择在 FIPS 兼容模式（2,5,14-21）下配置设备所需的参数。
- 在虚拟路径的 IPsec 设置中显示符合 FIPS 标准的 IPsec 通道类型
- IKE 哈希和（IKEv2）完整性模式，IPsec 身份验证模式。
- 对基于 FIPS 的生命周期设置执行审核错误

要使用 Citrix SD-WAN Orchestrator 服务启用 FIPS 合规性，请参阅 FIPS 模式。

Citrix SD-WAN Secure Web Gateway

September 2, 2022

为了保护流量和执行策略，企业通常使用 MPLS 链接来回程分支流量到企业数据中心。数据中心应用安全策略，筛选通过安全设备检测恶意软件的流量，并通过 ISP 路由流量。这种通过私有 MPLS 链路进行后拖是昂贵的。它还会导致显著延迟，从而在分支站点造成较差的用户体验。还存在用户绕过您的安全控制的风险。

另一种替代方法是在分支机构添加安全设备。但是，随着您安装多个设备以维护整个站点的一致策略，成本和复杂性会增加。如果您有许多分支机构，则成本管理变得不切实际。

Zscaler：

在不增加成本、复杂性或延迟的情况下实施安全性的理想解决方案是将所有分支 Internet 流量从 Citrix SD-WAN 设备路由到 Zscaler Cloud Security Platform。然后，您可以使用中央 Zscaler 控制台为用户创建精细安全策略。无论用户位于数据中心还是分支站点，都会一致地应用这些策略。由于 Zscaler 安全解决方案是基于云的，因此您无需向网络添加更多安全设备。

FIPS 遵守情况：

美国国家标准与技术研究院 (National Institute for Standards and Technology, NIST) 在没有自愿标准的领域制定了联邦信息处理标准 (Federal Information Processing Standards, FIPS)。FIPS 解决了以下问题：

- 不同系统之间的兼容性。
- 数据和软件可移植性。
- 经济高效的计算机安全和敏感信息隐私。

FIPS 指定安全系统中使用的加密模块的安全要求。要将这些安全标准应用于 Citrix SD-WAN 设备完成的处理，请配置 FIPS 模式。

Forcepoint：

通过使用 Citrix SD-WAN，您可以使用防火墙重定向（通过目标 NAT 透明代理）功能将 Internet（HTTP 和 HTTPS）流量从企业边缘的 SD-WAN 设备重定向到 Forcepoint 云托管安全模块。您可以将 HTTP 流量从端口 80 重定向到端口 8081，将 HTTPS 流量从端口 443 重定向到最近的 Forcepoint 云代理服务器的端口 8443。

使用 **GRE** 通道和 **IPsec** 通道的 **Zscaler** 集成

November 16, 2022

Zscaler 云安全平台在全球 100 多个数据中心作为一系列安全检查站。通过简单地将您的 Internet 流量重定向到 Zscaler，您可以立即保护您的商店、分支机构和远程位置。Zscaler 连接用户和 Internet ，检查每个字节的流量，即使它是加密或压缩。

Citrix SD-WAN 设备可以通过客户现场的 GRE 通道连接到 Zscaler 云网络。使用 SD-WAN 设备的 Zscaler 部署支持以下功能：

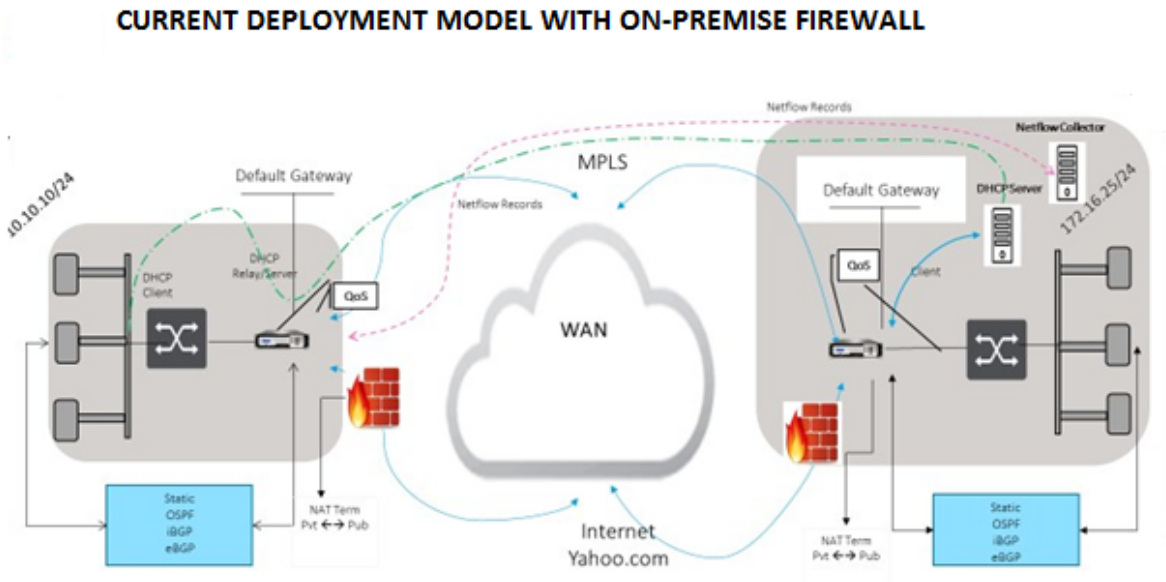
- 转发所有 GRE 流量 Zscaler, 从而使直接 Internet 突破.
- 基于每个客户站点使用 Zscaler 进行直接 Internet 访问（DIA)。
  - 在某些站点上，您可能希望向 DIA 提供本地安全设备，而不使用 Zscaler。
  - 在某些站点上，您可能会选择回程线路流量（另一个客户站点）以访问 Internet。

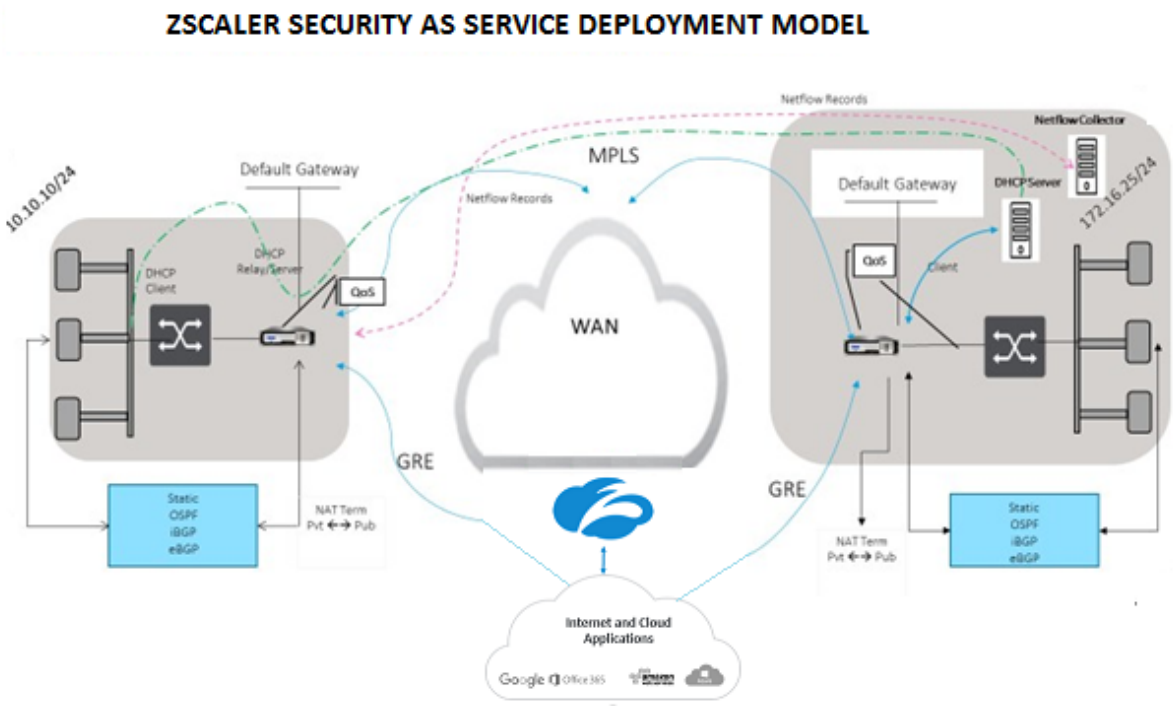
- 虚拟路由和转发部署。
- 一个 WAN 链接，作为 Internet 服务的一部分。

Zscaler 是一种云服务。必须将其设置为服务并定义底层 WAN 链接：

- 通过 GRE 在数据中心和分支机构配置 Internet 服务.
- 在数据中心和分支站点配置受信任的公共 Internet 链接。

拓扑





要使用 GRE 通道或 IPsec 通道流量转发：

1. 登录到 Zscaler 帮助门户网站：https://help.zscaler.com/submit-ticket。
2. 提出一个票证并提供静态公有 IP 地址，该地址用作 GRE 通道或 IPsec 通道源 IP 地址。

Zscaler 使用源 IP 地址来识别客户 IP 地址。源 IP 需要是静态公有 IP。Zscaler 通过两个 ZEN IP 地址（主要和辅助）进行响应，以便将流量传输到。GRE 保持活力的消息可以用来确定通道的健康.

Zscaler 使用源 IP 地址值来识别客户 IP 地址。此值必须是静态公有 IP 地址。Zscaler 使用两个 ZEN IP 地址 [DR1] 进行响应，以便将流量重定向到这些地址。GRE 保持活动的消息可以用来确定通道的健康。

示例 **IP** 地址

Primary

内部路由器 IP 地址：172.17.6.241/30
内部 ZEN IP 地址：172.17.6.242/30

Secondary

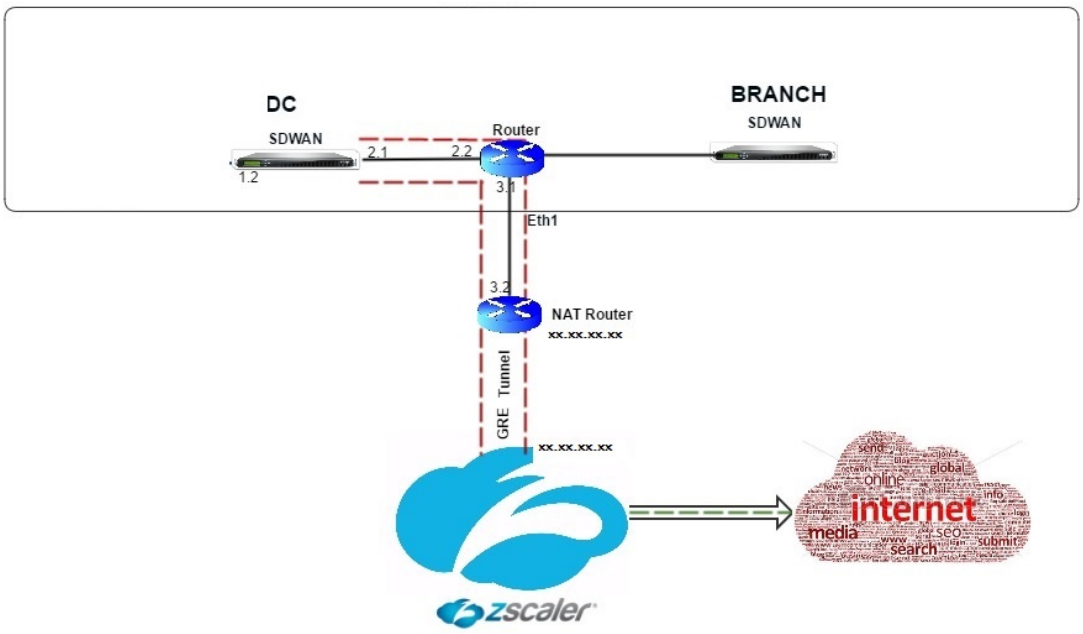
内部路由器 IP 地址：172.17.6.245/30
内部 ZEN IP 地址：172.17.6.246/30

配置 **Internet** 服务

要通过 Citrix SD-WAN Orchestrator 服务配置 Internet 服务，请参阅 交付服务。有关为站点启用 Internet 服务的详细信息，请参阅 直接 Internet 分组讨论。

配置 **GRE** 通道

1. 源 IP 地址是通道源 IP 地址。如果通道源 IP 地址已执行 NAT，则公共源 IP 地址是公共通道源 IP 地址，即使其在不同的中间设备上执行了 NAT 也是如此。
2. 目标 IP 地址是 Zscaler 提供的 ZEN IP 地址。
3. 源 IP 地址和目标 IP 地址是原始负载封装时路由器 GRE 头.
4. 通道 IP 地址和前缀是 GRE 通道本身的 IP 地址。这对于通过 GRE 通道路由流量非常有用。流量需要此 IP 地址作为网关地址。



要通过 Cirix SD-WAN Orchestrator 服务配置 GRE 通道，请参阅 GRE 通道。

为 **GRE** 通道配置路由

配置路由以将 Internet 前缀服务转发到 Zscaler GRE 通道.

- ZEN IP 地址（通道目标 IP，如上图 104.129.194.38 所示）必须设置为服务类型的 Internet 。这是必需的，以便从 Internet 服务中计入发往 Zscaler 的流量。

- 所有发往 Zscaler 的流量必须与默认路由 0/0 匹配，并通过 GRE 通道传输。确保 GRE 通道 [DR1] 使用的 0/0 路由的成本低于直通或任何其他服务类型。
- 同样，备份 GRE 通道 Zscaler 必须具有比主 GRE 通道更高的成本.
- 确保 ZEN IP 地址存在非递归路由。

> 注意
>
> 如果您没有 Zscaler IP 地址的特定路由，请配置路由前缀 0.0.0.0/0 以匹配 ZEN IP 地址，并通过 GRE 通道封装循环路由。此配置使用主动备份模式下的通道。如上图所示的值，流量会自动切换到 Gateway 关 IP 地址 172.17.6.242 的通道。如果需要，请配置回程虚拟路径路由。否则，将备份通道的保持活动时间间隔设置为零。这使得安全的 Internet 访问网站，即使两个通道 Zscaler 失败。
>
> 支持 GRE 保持活动状态的消息。Citrix SD-WAN GUI 界面中添加了一个名为 公共源 **IP** 的新字段，该字段提供 GRE 源地址的 NAT 地址（在 SD-WAN 设备通道源由中间设备 NAT 的情况下）。Citrix SD-WAN GUI 包括一个名为公共源 IP 的字段，当 Citrix SD-WAN 设备的通道源由中间设备 NATE 时，该字段提供 GRE 源地址的 NAT 地址。

限制

- 不支持多个 VRF 部署。
- 主备份 GRE 通道仅支持高可用性设计模式。

要监视 GRE 和 IPsec 通道统计信息：

在 SD-WAN Web 界面中，导航到 监控 > 统计信息 > **IPsec** 通道]。 [**GRE** 通道]

有关详细信息，请参阅；监视 IPsec 通道 和 GRE 通道 主题。

使用 **Citrix SD-WAN** 中的 **Forcepoint** 支持防火墙流量重定向

September 2, 2022

Forcepoint 支持以下功能，虽然 SD-WAN 仅支持防火墙重定向功能：

- 采用 PSK 的 IPsec
- 采用 PSK 的 IPsec
- 使用 PAC 文件配置的代理链接
- 使用标准头进行代理链接
- 使用专有标头进行代理链接，无需配置客户端 IP 范围-合作/开发

- 防火墙重定向（目标 NAT 的透明代理）

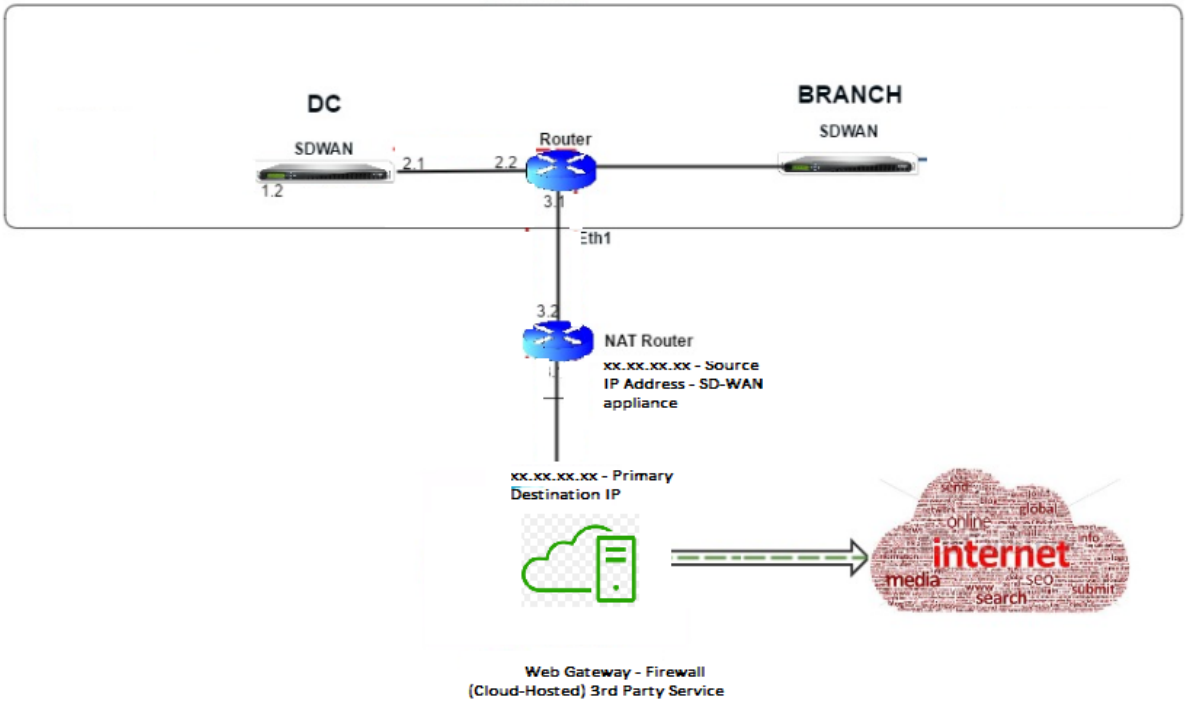
目标 NAT 策略使企业能够使用 ForcePoint 通过云托管安全服务路由 Internet 流量。

查看以下使用案例，了解如何在 SD-WAN 设备中配置目标 NAT，并通过基于云的安全防火墙服务重定向 Internet 流量。

必备条件：

1. 登录 Forcepoint 门户网站。通过提供企业公有 IP 地址来创建策略，Internet 流量需要重定向到 Forcepoint。获取 Internet 流量应重定向到的主 IP 和辅助 IP 地址。
2. 在 SD-WAN GUI 中，在 DC 站点的 SD-WAN 设备上，配置与 WAN 链接关联的 Internet 服务。
3. 目标 NAT 使用 Internet 流量的目标 IP 地址执行。此目标地址更改为 Forcepoint 公有 IP 地址。
4. 通过提供源 IP 地址和主 IP 地址来配置目标 NAT 策略。源 IP 是 SD-WAN 设备在端口 80 (http) 和 443 (https) 内的 Internet IP 地址，该 IP 地址分别被重定向/转换为基于云的防火墙 Gateway 的主目标 IP 地址，其外部端口 8081 (http) 和 8443 (https)。
5. 配置 DNAT 策略后，请确保 DC 上配置的路由选择了 SD-WAN 网络 IP 地址的 Internet 服务类型。

您可以使用 Citrix SD-WAN Orchestrator 服务配置 NAT。有关更多信息，请参阅 网络地址转换。

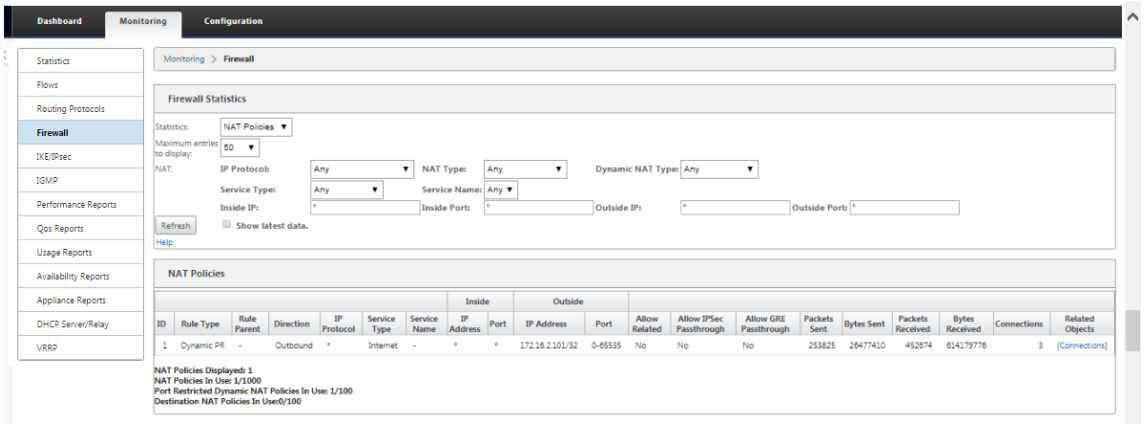


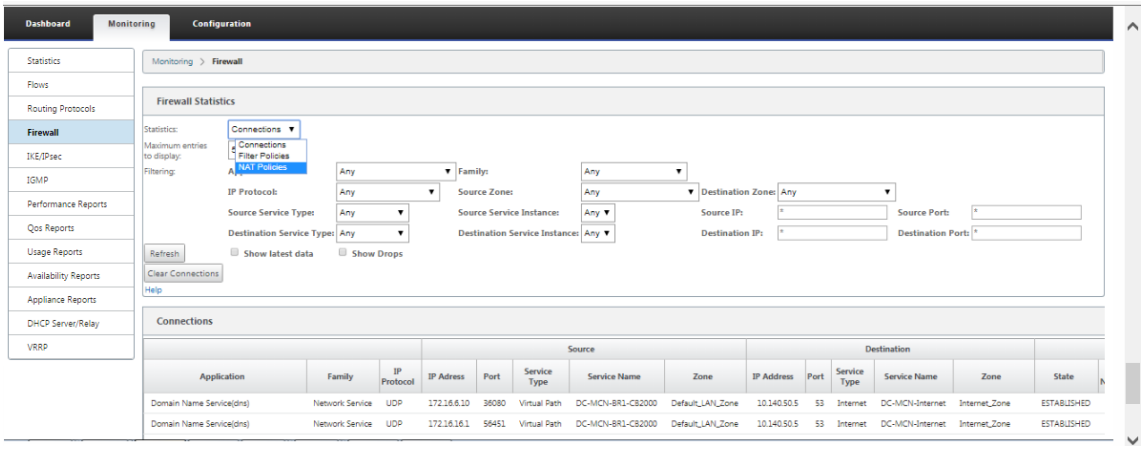
监视目标 **NAT** 策略（防火墙）

您还可以使用 Citrix SD-WAN GUI 来监视当前 DNAT 策略配置。

要监视当前目标 NAT 策略配置：

1. 在 Citrix SD-WAN GUI 中，导航到 监控 > 防火墙 > **NAT** 策略。
2. 选择包含要监视的统计信息的选项卡。





使用 **IPsec** 通道的 **Palo Alto** 集成

September 2, 2022

Palo Alto 网络提供基于云的安全基础设施，用于保护远程网络。它通过允许组织设置区域、基于云的防火墙来保护 SD-WAN 架构来提供安全性。

适用于远程网络的 Prisma Access 服务允许您登载远程网络位置，并为用户提供安全性。它消除了在每个远程位置配置和管理设备的复杂性。该服务提供了一种有效的方式，可以轻松添加新的远程网络位置，并通过确保这些位置的用户始终保持连接和安全，最大限度地减少运营挑战，并允许您从 Panorama 集中管理策略，为远程提供一致和简化的安全性网络位置。

要将远程网络位置连接到 Prisma Access 服务，您可以使用 Palo Alto Networks 下一代防火墙或符合 IPSEC 标准的第三方设备（包括

SD-WAN），后者可以建立通往该服务的 IPsec 通道。

- 规划远程网络的 Prisma Access 服务
- 配置远程网络的 Prisma Access 服务
- 带配置导入的板载远程网络

Citrix SD-WAN 解决方案已经提供了从分支中分离 Internet 流量的功能。这对于提供更可靠、低延迟的用户体验至关重要，同时避免在每个分支机构引入昂贵的安全堆栈。Citrix SD-WAN 和 Palo Alto 网络现在为分布式企业提供了一种更可靠和安全的方式，将分支机构中的用户连接到云中的应用程序。

Citrix SD-WAN 设备可以通过 IPsec 通道从具有最低配置的 SD-WAN 设备位置连接到 Palo Alto 云服务（Prisma Access 服务）网络。

有状态防火墙和 **NAT** 支持

September 2, 2022

此功能提供内置于 SD-WAN 应用程序中的防火墙。防火墙允许服务和区域之间的策略，并支持静态 NAT、动态 NAT (PAT) 和带端口转发的动态 NAT。更多防火墙功能包括：

- 为 SD-WAN 网络内的用户流量提供安全性（企业和服务提供商）
- (潜在) 减少外部设备 (企业和服务供应商)
- 为多个客户使用相同的 IP 地址空间：NAT 功能（服务提供商）
- 从全局角度应用多个防火墙（服务提供商）
- 过滤区域之间的流量
- 筛选区域内服务之间的流量
- 过滤位于不同区域的服务之间的流量
- 筛选站点上的服务之间的流量
- 定义过滤器策略以允许、拒绝或拒绝流
- 跟踪选定流量的流量状态
- 应用全局策略模板
- 支持端口地址转换到不受信任端口上的 Internet 流量，以及端口转发入站和出站
- 提供静态网络地址转换（静态 NAT）
- 提供动态网络地址转换 (动态 NAT)
- 端口地址翻译 (PAT)
- 端口转发

> 注意
>
> 出于安全原因，不建议在故障到线联模式下使用防火墙。

全局防火墙设置

September 2, 2022

创建防火墙策略模板后，您可以使用此策略为 Citrix SD-WAN 网络配置防火墙设置。使用全局防火墙设置时，可以配置全局防火墙参数，这些设置将应用到虚拟 WAN 网络上的所有站点。

高级防火墙设置

November 16, 2022

您可以单独配置每个站点的高级防火墙设置。这将覆盖全局设置。

要在站点级别配置高级防火墙设置，请参阅 防火墙设置。

区域

September 2, 2022

您可以在网络中配置区域并定义策略以控制流量进出区域的方式。默认情况下，将创建以下区域：

- Internet_Zone
  - 适用于使用受信任界面进出 Internet 服务的流量。
- Untrusted_Internet_Zone
  - 适用于使用不受信任界面进出 Internet 服务的流量。
- Default_LAN_Zone
  - 适用于流入或流出具有可配置区域的对象（其中尚未设置区域）的流量。

您可以创建自己的区域并将它们分配给以下类型的对象：

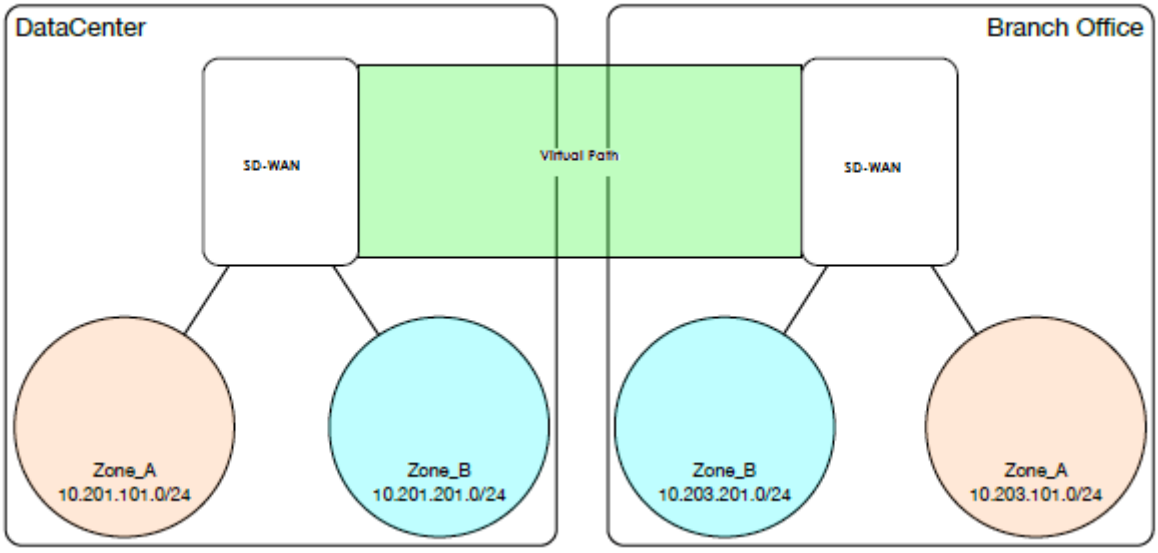
- 虚拟网络接口 (VNI)
- 内联网服务
- GRE 通道
- 局域网 IPsec 通道

数据包的目标区域根据目标路由匹配确定。SD-WAN 设备在路由表中查找目标子网时，数据包将匹配一个路由，路由分配了一个区域。

- 源区
  - 非虚拟路径：通过在接收虚拟网络接口数据包确定。
  - 虚拟路径：通过数据包流头中的源区域字段确定。
  - 虚拟网络接口-在源站点上接收数据包。
- 目的地区
  - 通过数据包的目标路由查找确定。

与 SD-WAN 中的远程站点共享的路由会维护有关目标区域的信息，包括通过动态路由协议（BGP、OSPF）学习的路由。利用这种机制，区域在 SD-WAN 网络中具有全局意义，并允许在网络中进行端到端过滤。使用区域为网络管理员提供了根据客户、业务单位或部门分割网络流量的有效方法。

SD-WAN 防火墙的功能允许用户筛选单个区域内的服务之间的流量，或创建可在不同区域内的服务之间应用的策略，如下图所示。在下面的例子中，我们有区域 _A 和区域 B，每个区域都有一个 LAN 虚拟网络接口。



策略

September 2, 2022

策略提供了允许、拒绝、拒绝或计数和继续特定流量流量的功能。您可以通过 Citrix SD-WAN Orchestrator 服务配置防火墙策略。有关更多信息，请参阅 防火墙策略。

网络地址转换 (NAT)

September 2, 2022

网络地址转换 (NAT) 执行 IP 地址保护，以保留有限数量的已注册 IPv4 地址。它使使用未注册 IP 地址的私有 IP 网络能够连接到 Internet 。Citrix SD-WAN 上的 NAT 功能将您的私有 SD-WAN 网络与公共 Internet 连接起来。它将内部网络中的私有地址转换为合法的公有地址。NAT 还通过将整个网络的一个地址广告到 Internet ，隐藏整个内部网络，从而确保额外的安全性。Citrix SD-WAN 支持以下 NAT 类型：

- 静态一对一 NAT
- 动态 NAT（PAT-端口地址转换）
- 具有端口转发规则的动态 NAT

> 注意
>
> 只能通过 Citrix SD-WAN Orchestrator 服务在站点级别配置 NAT 功能。NAT 没有全局配置（模板）。所有 NAT 策略都是通过源 NAT（“SNAT)”转换定义的。相应的目标 NAT（“DNT”）规则将自动为用户创建。有关更多信息，请参阅 网络地址转换。

静态 NAT

September 2, 2022

静态 NAT 是 SD-WAN 网络内部的私有 IP 地址或子网到 SD-WAN 网络外部的公有 IP 地址或子网的一对一映射。通过手动输入内部 IP 地址和必须转换到的外部 IP 地址来配置静态 NAT。您可以为本地、虚拟路径、Internet、内部网和路由间域服务配置静态 NAT。

入站和出站 NAT

连接的方向可以是内部到外部，也可以是外部到内部。创建 NAT 规则时，根据方向匹配类型将其应用于两个方向。

- 入站：对于在服务上接收的数据包，将转换源地址。转换服务上传输的数据包的目的地址。例如，Internet 服务到局域网服务—对于接收的数据包（Internet 到局域网），将转换源 IP 地址。对于传输的数据包（LAN 到 Internet ），将转换目的 IP 地址。
- 出站：对于在服务上接收的数据包，将转换目标地址。对于在服务上传输的数据包，将转换源地址。例如，局域网服务到 Internet 服务—对于传输的数据包（局域网到 Internet ），将转换源 IP 地址。对于接收的数据包（Internet 到局域网），将转换目的 IP 地址。

区域派生

入站或出站流量的源和目标防火墙区域不应相同。如果源防火墙区域和目标防火墙区域相同，则不会对流量执行 NAT。

对于出站 NAT，外部区域将自动从服务派生。默认情况下，SD-WAN 上的每个服务都与一个区域相关联。例如，受信任的 Internet 链接上的 Internet 服务与受信任的 Internet 区域相关联。同样，对于入站 NAT，内部区域是从服务派生的。

对于虚拟路径服务 NAT 区域派生不会自动发生，您必须手动输入内部和外部区域。NAT 仅对属于这些区域的流量执行。无法为虚拟路径派生区域，因为虚拟路径子网中可能有多个区域。

IPv6 Internet 服务的静态 **NAT** 策略

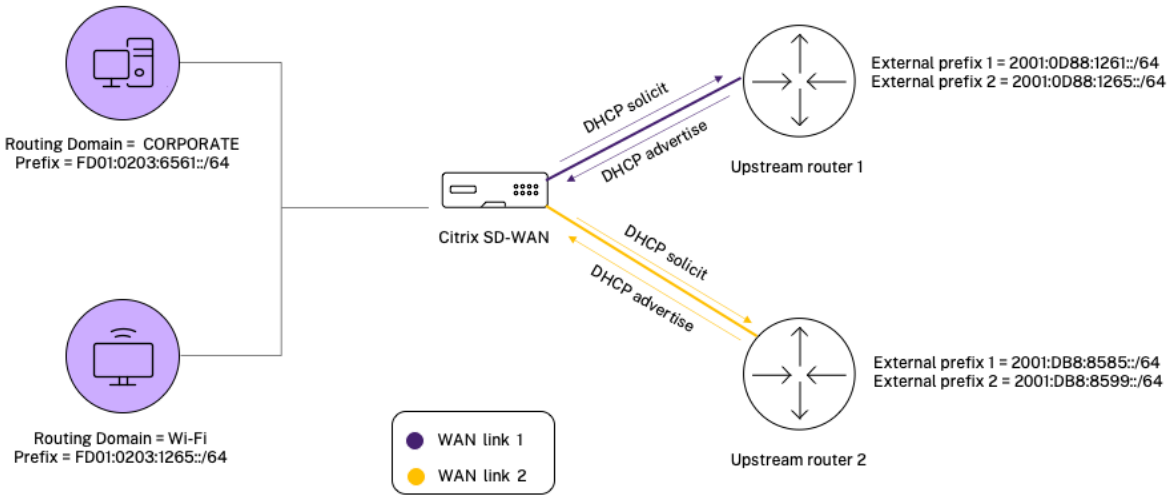
Citrix SD-WAN 从 11.4.0 版开始支持 IPv6 Internet 服务的静态 NAT 策略。IPv6 Internet 服务的静态 NAT 策略指定将内部网络前缀映射到外部网络前缀。所需的静态 NAT 策略的数量取决于内部网络的数量和外部网络（WAN 链路）的数量。如果有 **M** 个内部网络和 **N** 个 WAN 链路，则所需的静态 NAT 策略数为 **M x N**。

从 Citrix SD-WAN 11.4.0 版开始，在创建静态 NAT 策略时，您可以手动输入外部 IP 地址或 通过 **PD** 启用自动学习。启用 通过 **PD** 进行自动学习 后，Citrix SD-WAN 设备将通过 DHCPv6 前缀委派从上游委派路由器接收委派前缀。在 Citrix SD-WAN 11.4.0 版之前，外部 IP 地址是自动从服务派生的，因此无法选择手动输入外部 IP 地址。如果要将设备升级到 11.4.0 或更高版本，并且为 IPv6 Internet 服务配置了静态 NAT 策略，则必须手动更新这些策略。

配置示例

在以下拓扑中，Citrix SD-WAN 设备配置有 2 个内部网络和 2 个 WAN 链接：

- 内部网络 1 驻留在具有网络前缀 FD01:0203:6561::/64 的企业路由域中
- 内部网络 2 驻留在 Wi-Fi 路由域中，网络前缀为 FD01:0203:1265::/64
- 通过 WAN Link 1，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001:0D88:1261::/64 和 2001:0D88:1265::/64 从上游委派路由器接收。当来自内部网络的流量通过 WAN link 1 时，这两个委派的前缀将用作外部网络前缀。
- 通过 WAN Link 2，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001:DB8:8585::/64 和 2001:DB8:8599::/64 从上游委派路由器接收。当来自内部网络的流量通过 WAN link 2 时，这两个委派的前缀用作外部网络前缀。

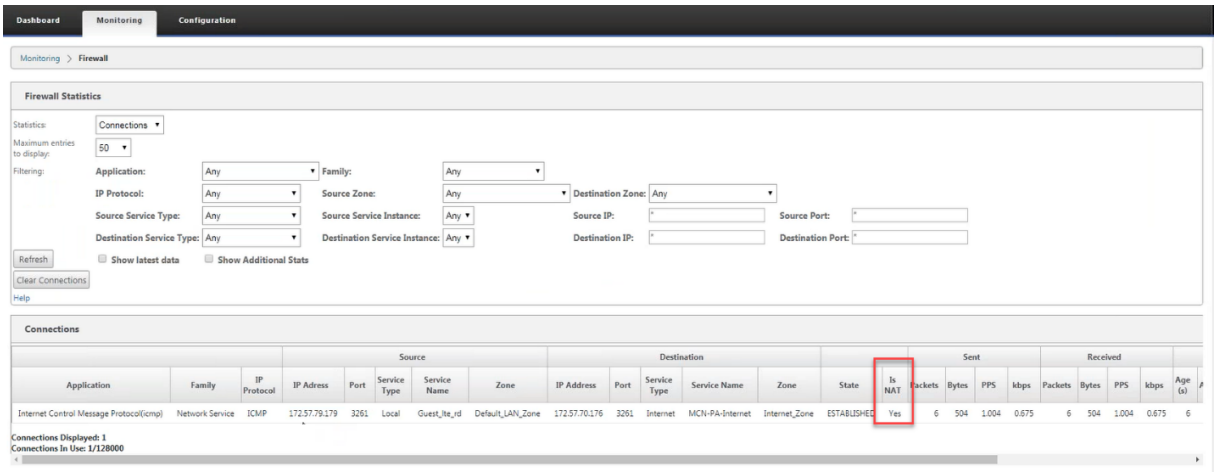


在这种情况下，网络内有 M=2 和 N = 2 WAN 链路。因此，正确部署 IPv6 Internet 服务所需的静态 NAT 策略数为 2 x 2 = 4。这 4 个静态 NAT 策略为以下各项指定了地址转换：

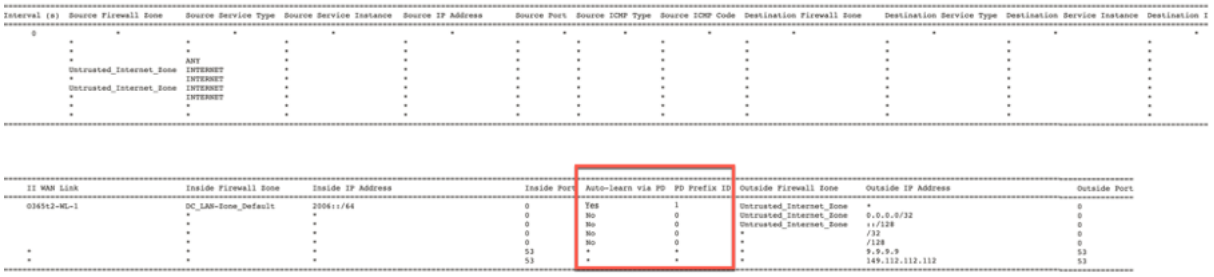
- 通过 WAN 链路 1 在网络 1 内部
- 在网络 1 内部通过 WAN 链路 2
- 通过 WAN 链路 1 在网络 2 内部
- 通过 WAN 链路 2 在网络 2 内部

监视

要监控 NAT，请导航到 监 控 > 防火墙统计 > 连接。对于连接，您可以看到 NAT 是否完成。

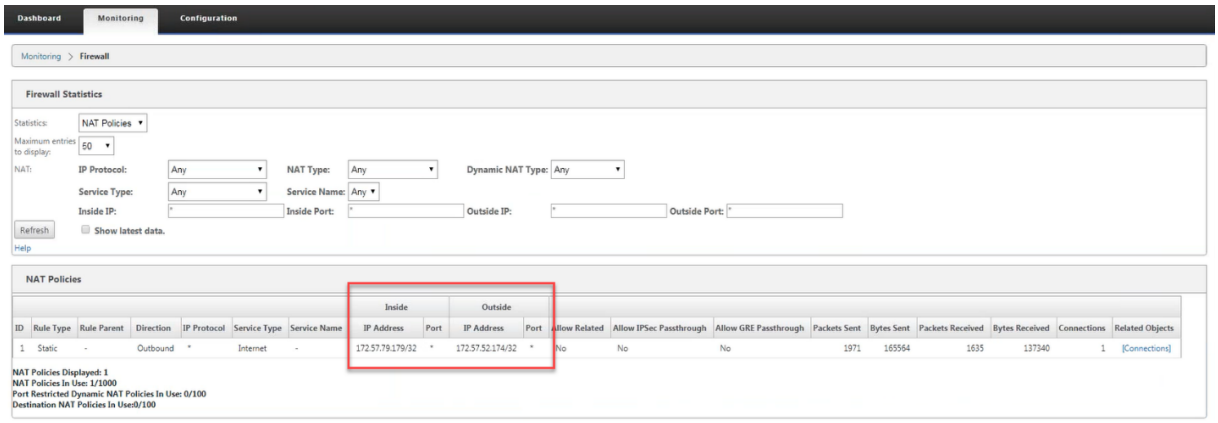


要检查是否为任何 NAT 规则配置了通过 PD 自动学习，请导航到 配置 **>** 虚拟 **WAN >** 查看配置，然后从视 图 下拉列表中选择 防火墙。通过 **PD** 自动学习 和 **PD** 前缀 **ID** 列显示详细信息。

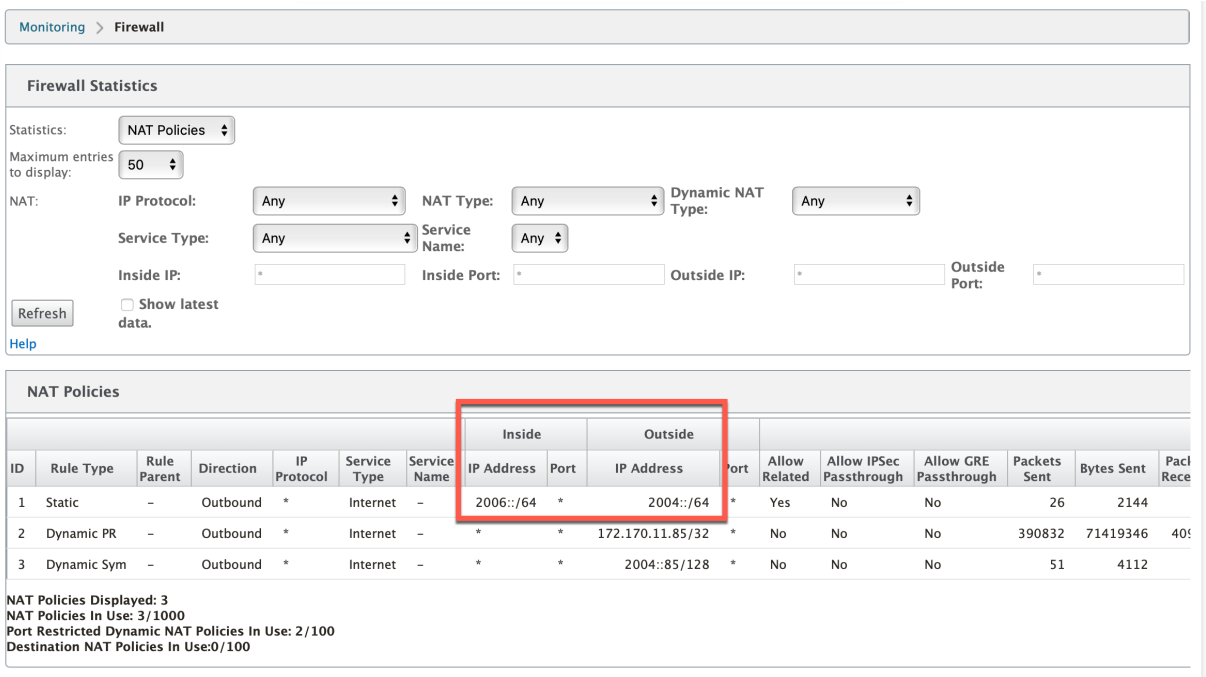


要进一步查看内部 IP 地址到外部 IP 地址的映射，请单击 相关对象 下的 路由后 **NAT** ，或导航到 监控 > 防火墙统计 > **NAT** 策略。

以下屏幕截图显示了 IPv4 静态 NAT 策略中内部地址与外部地址的映射。



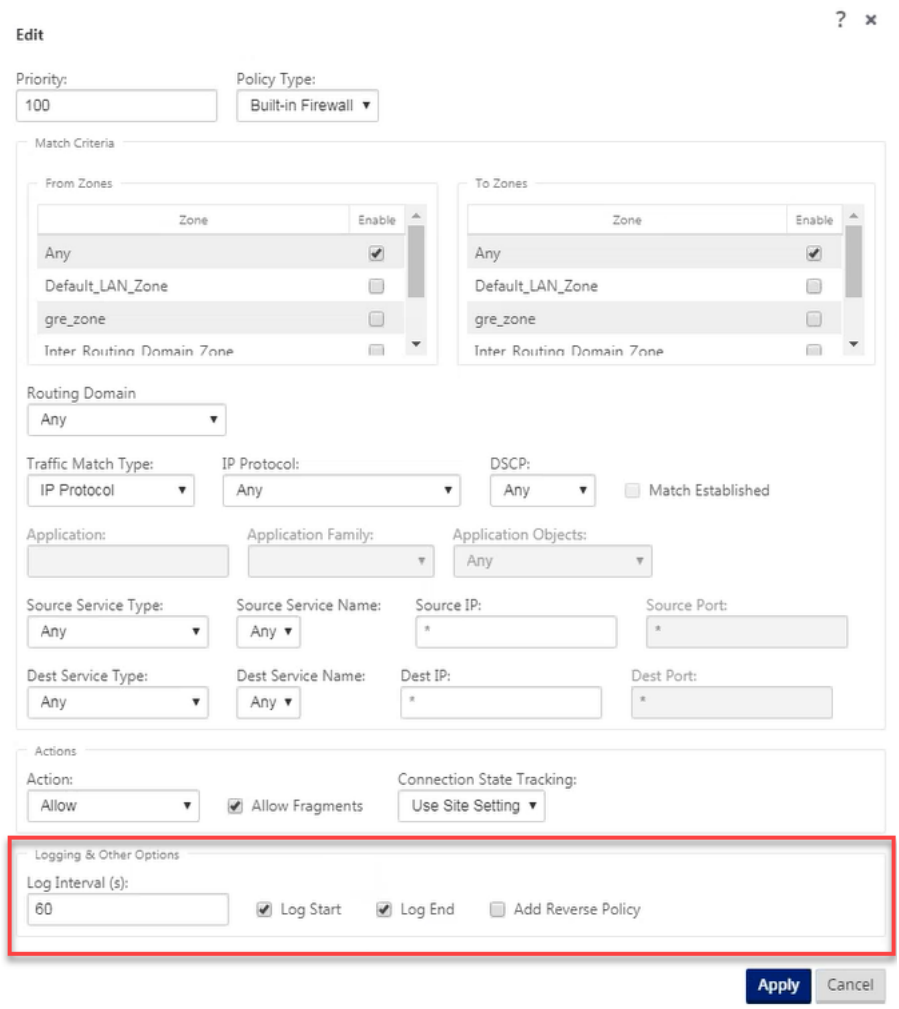
以下屏幕截图显示了 IPv6 静态 NAT 策略中内部地址与外部地址的映射。



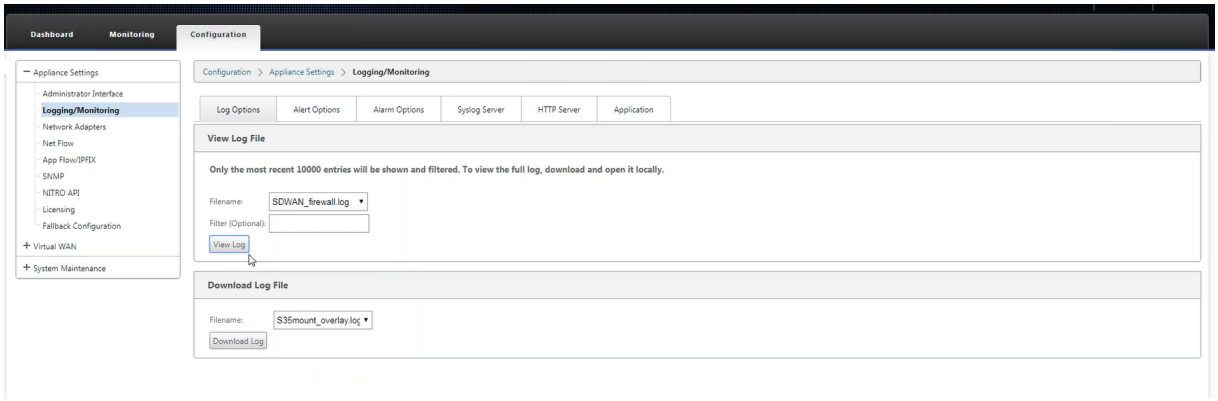
日志

您可以在防火墙日志中查看与 NAT 相关的日志。要查看 NAT 的日志，请创建与 NAT 策略匹配的防火墙策略，并确保在防火墙筛选器上启用了日志记录。NAT 日志显示以下信息：

- 日期和时间
- 路由域
- IP 协议
- 源端口
- 源 IP 地址
- 转换后的 IP 地址
- 转换后的端口
- 目标 IP 地址
- 目的端口



要生成 NAT 日志，请导航到日志记录/监视 > 日志选项，选择 **SDWAN_firewall.log**，然后单击查看日志。



NAT 连接详细信息将显示在日志文件中。

```
2020-05-11T10:14:19.861597+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:19.166668+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:15:19.986378+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:15:44.749959+0000 INFO    conn_clear_all@forward/firewall/connection.c:8796    Removed 1 Connections
2020-05-11T10:15:44.750109+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:16.981504+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.70.176-->172.57.79.179 (ID:10743)
2020-05-11T10:16:20.108292+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 21 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.79.179-->172.57.70.176 (ID:10743)
2020-05-11T10:16:21.299055+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112286+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:16:22.112650+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:17:21.768837+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:17:22.255262+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.235843+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 56 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:18:22.371729+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:19:21.353441+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:19:22.483705+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:20:22.374898+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:20:22.598370+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:21:20.464917+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:21:22.716765+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 60 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:20.474915+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 50 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REQUEST 172.57.79.179-->172.57.70.176 (ID:3261)
2020-05-11T10:22:22.846123+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 54 packets for (Routing Domain Default_RoutingDomain) ICMP ECHO REPLY 172.57.70.176-->172.57.79.179 (ID:3261)
2020-05-11T10:23:09.456757+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) ICMP 172.57.79.179-->172.57.70.176 (ID:3261)
```

```
2022-02-14T11:43:53.184990+0000 WARN    find_and_update_connection@forward/firewall/connection.c:4828   CONN 0x7fffdbf5f168 Aborted, NAT
2022-02-14T11:43:53.185044+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:43:53.565134+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:43:59.572977+0000 INFO    t2_firewall_monitor.pl   Connection DELETED for (Routing Domain Default_RoutingDomain) IPv6_ICMP
2022-02-14T11:45:12.399564+0000 INFO    t2_firewall_monitor.pl   NAT Connection DELETED for (Routing Domain Default_RoutingDomain) UDP 1
2022-02-14T11:45:48.516174+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) IPv6_
2022-02-14T11:45:48.717951+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 488 packets for (Routing Domain Default_RoutingDomai
2022-02-14T11:46:18.786955+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:21.760939+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:21.761368+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 3 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:27.766610+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
2022-02-14T11:46:32.774464+0000 INFO    t2_firewall_monitor.pl   NAT Connection CREATED for (Routing Domain Default_RoutingDomain) TCP 2
2022-02-14T11:46:32.775063+0000 INFO    t2_firewall_monitor.pl   Filter (1) ALLOWED 1 packets for (Routing Domain Default_RoutingDomain)
```

动态 **NAT**

November 16, 2022

动态 NAT 是将 SD-WAN 网络内部的一个或多个私有 IP 地址映射到 SD-WAN 网络外部的公有 IP 地址或子网的多对一映射。来自不同区域和子网通过 LAN 段中受信任（内部）IP 地址的流量通过单个公有（外部）IP 地址发送。

动态 **NAT** 类型

动态 NAT 执行端口地址转换 (PAT) 以及 IP 地址转换。端口号用于区分哪些流量属于哪个 IP 地址。所有内部私有 IP 地址均使用单个公有 IP 地址，但是为每个私有 IP 地址分配了不同的端口号。PAT 是一种经济高效的方式，允许多台主机使用单个公有 IP 地址连接到 Internet 。

- 端口限制：端口受限 NAT 对与内部 IP 地址和端口对相关的所有转换使用同一个外部端口。此模式通常用于允许 Internet P2P 应用程序。
- 对称：对称 NAT 将同一个外部端口用于与内部 IP 地址、内部端口、外部 IP 地址和外部端口元组相关的所有转换。此模式通常用于增强安全性或扩展 NAT 会话的最大数量。

入站和出站 **NAT**

连接的方向可以是内部到外部，也可以是外部到内部。创建 NAT 规则时，根据方向匹配类型将其应用于两个方向。

- 出站：对于在服务上接收的数据包，将转换目标地址。对于在服务上传输的数据包，将转换源地址。本地、Internet、内部网和路由间域服务支持出站动态 NAT。对于 WAN 服务（如 Internet 和内部网服务），配置的 WAN 链路 IP 地址将动态选择为外部 IP 地址。对于本地和路由间域服务，请提供外部 IP 地址。外部区域是从所选服务派生的。出站动态 NAT 的一个典型用例是同时允许 LAN 中的多个用户使用单个公共 IP 地址安全地访问 Internet 。
- 入站：对于在服务上接收的数据包，将转换源地址。转换服务上传输的数据包的目的地址。WAN 服务（如 Internet 和内部网）不支持入站动态 NAT。有一个显式的审计错误来指示相同的情况。仅本地和路由间域服务支持入站动态 NAT。提供要转换到的外部区域和外部 IP 地址。入站动态 NAT 的典型用例是允许外部用户访问您专用网络中托管的电子邮件或 Web 服务器。

端口转发

具有端口转发功能的动态 NAT 允许您将特定流量转发到已定义的 IP 地址。这通常用于诸如 Web 服务器之类的主机内部。配置动态 NAT 后，您可以定义端口转发策略。配置用于 IP 地址转换的动态 NAT，并定义端口转发策略以将外部端口映射到内部端口。动态 NAT 端口转发通常用于允许远程主机连接到专用网络上的主机或服务器。有关更详细的用例，请参阅 Citrix SD-WAN 动态 NAT 说明。

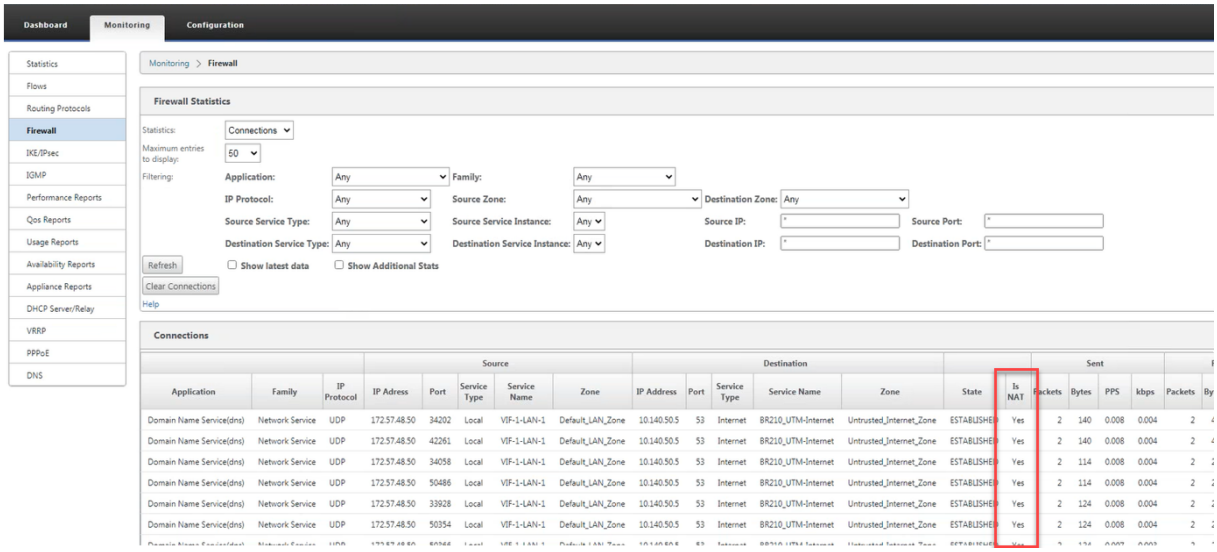
自动创建的动态 **NAT** 策略

在以下情况下，将自动创建 Internet 服务的动态 NAT 策略：

- 在不受信任的接口（WAN 链接）上配置 Internet 服务。
- 使用 Citrix SD-WAN Orchestrator 服务为单个 WAN 链接上的所有路由域启用 Internet 访问。有关更多详细信息，请参阅 配置防火墙分段。
- 在 SD-WAN Orchestrator 服务上配置 DNS 转发器或 DNS 代理。有关更多详细信息，请参阅 域名系统。

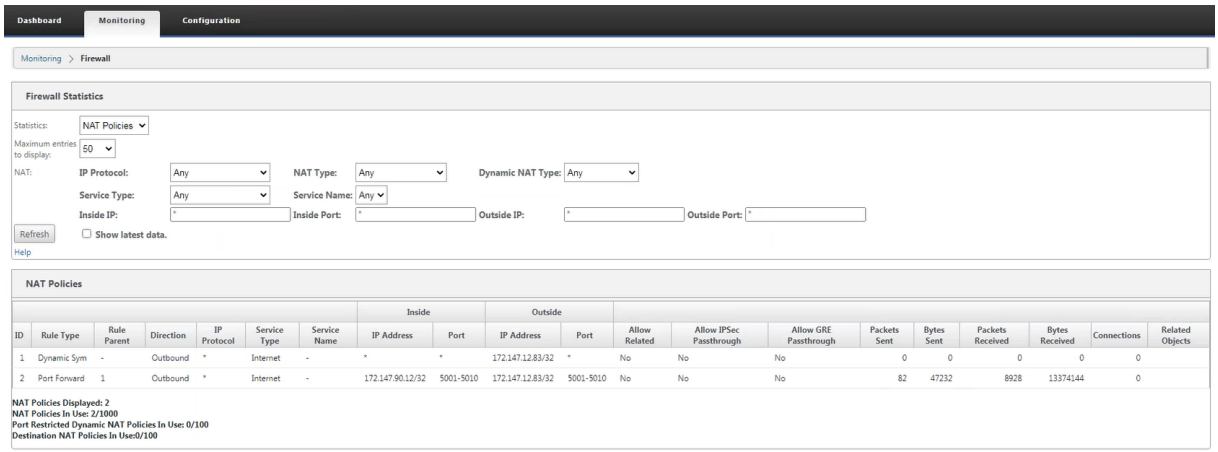
监视

要监视动态 NAT，请导航到 监 控 > 防火墙统计 > 连接。对于连接，您可以看到 NAT 是否完成。

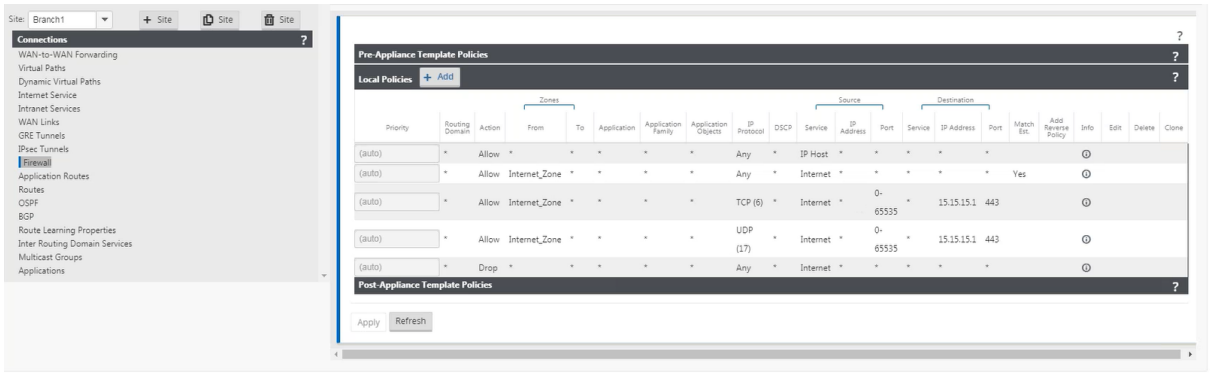


要进一步查看内部 IP 地址到外部 IP 地址的映射，请单击 相关对象 下的 预路由 **NAT** 或路由后 NAT，或导航到监控 > 防火墙统计 >**NAT** 策略。

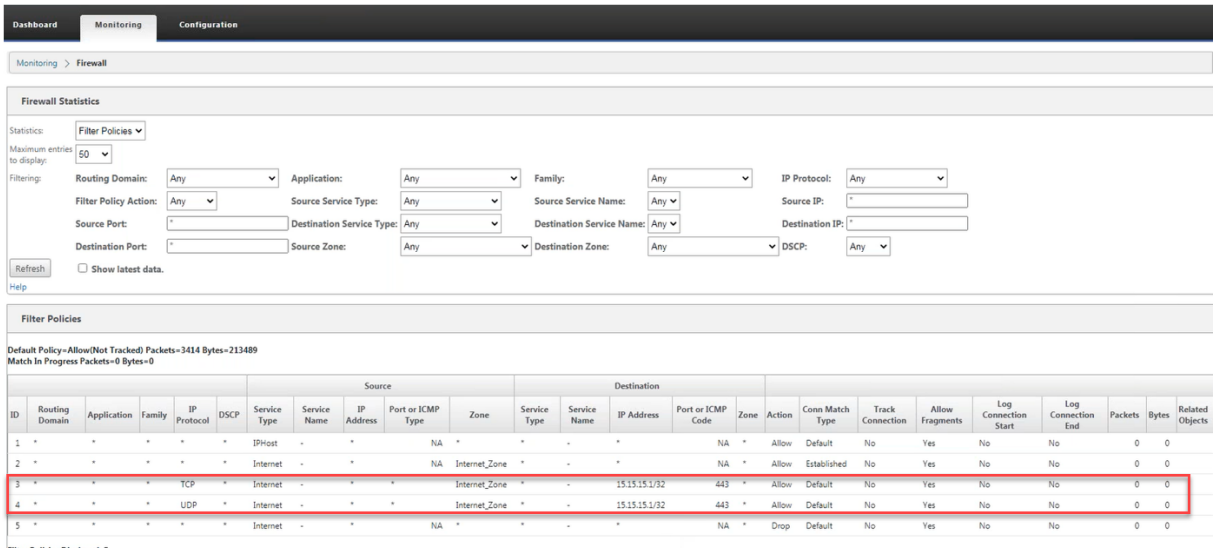
以下屏幕截图显示了对称类型的动态 NAT 规则及其相应的端口转发规则的统计信息。



创建端口转发规则时，也会创建相应的防火墙规则。



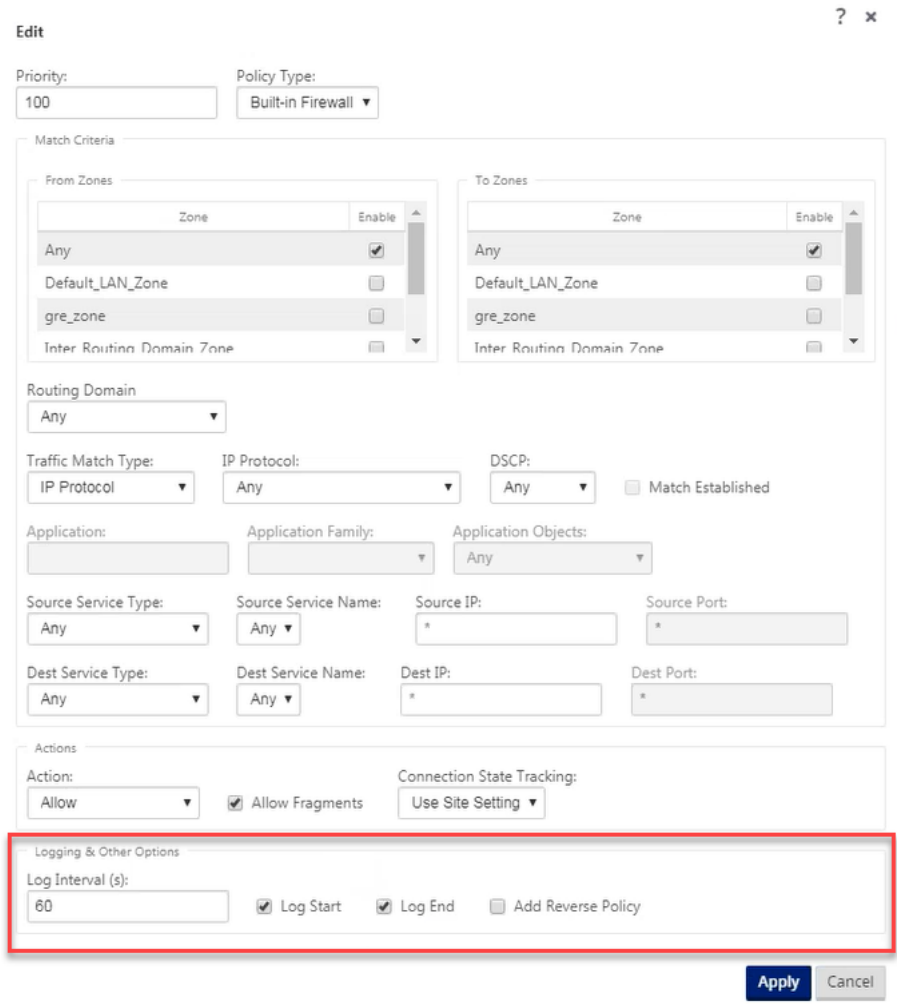
您可以通过导航到 监视 > 防火墙统计信息 **>** 筛选器策略来查看筛选器策略统计信息



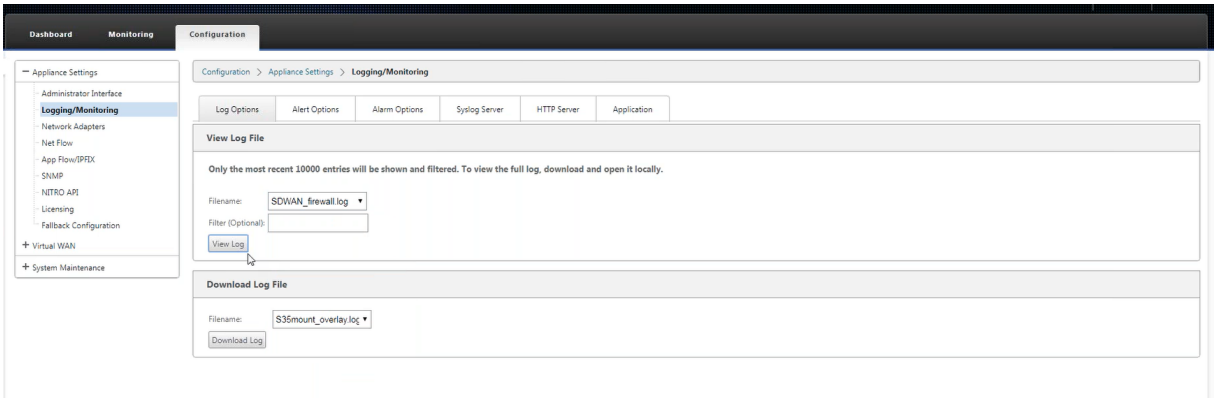
日志

您可以在防火墙日志中查看与 NAT 相关的日志。要查看 NAT 的日志，请创建与 NAT 策略匹配的防火墙策略，并确保在防火墙筛选器上启用了日志记录。NAT 日志包含以下信息：

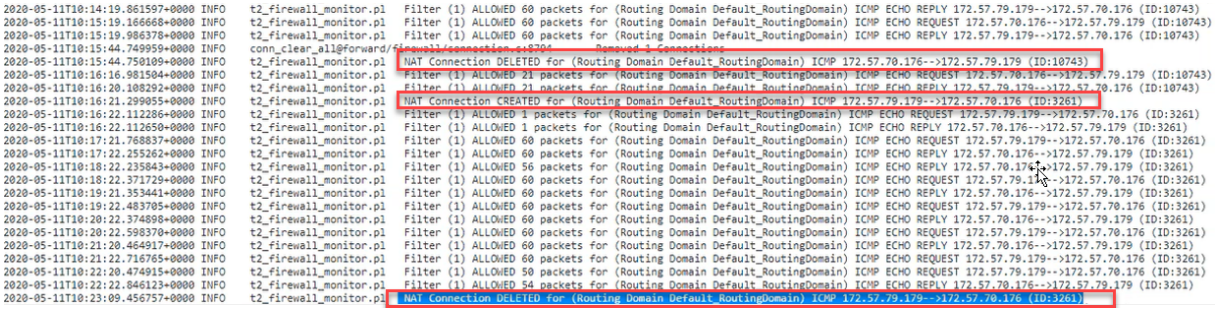
- 日期和时间
- 路由域
- IP 协议
- 源端口
- 源 IP 地址
- 转换后的 IP 地址
- 转换后的端口
- 目标 IP 地址
- 目的端口



要生成 NAT 日志，请导航到日志记录/监视 > 日志选项，选择 **SDWAN_firewall.log**，然后单击查看日志。



NAT 连接详细信息将显示在日志文件中。



配置虚拟广域网服务

September 2, 2022

Citrix SD-WAN 配置描述并定义了 Citrix SD-WAN 网络的拓扑。有关如何使用 Citrix SD-WAN Orchestrator 服务配置虚拟广域网服务的信息，请参阅 流程。

安全和加密

启用 SD-WAN（对于虚拟路径）的加密是可选的。启用加密后，SD-WAN 使用高级加密标准 (AES) 来保护整个虚拟路径的流量。SD-WAN 设备支持 AES 128 位和 256 位密码（密钥大小），并且是可配置的选项。

使用虚拟 WAN 配置的站点之间的身份验证功能。网络配置具有每个站点的私有密钥。对于每个虚拟路径，网络配置通过组合来自虚拟路径每一端的站点的私有密钥来生成密钥。首次设置虚拟路径后发生的初始密钥交换取决于使用该组合密钥加密和解密数据包的能力。

配置防火墙分割

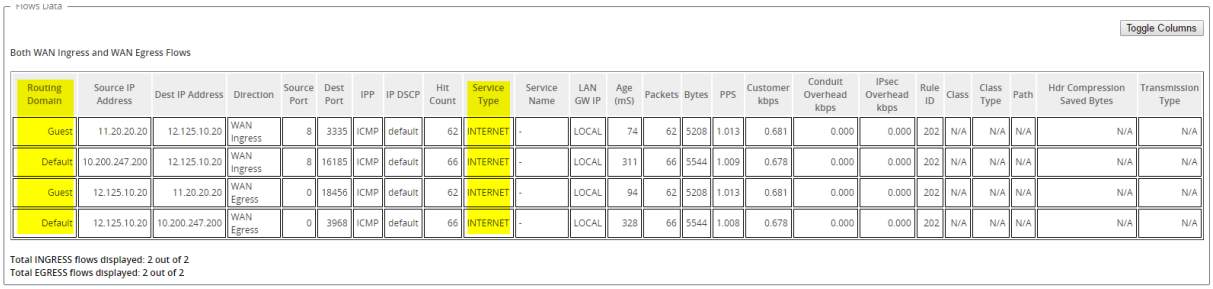
November 16, 2022

虚拟路由转发 (VRF) 防火墙分段 提供了多个路由域通过一个通用接口访问 Internet 的路由域，每个域的流量与其他域的流量隔离。例如，员工和访客可以通过相同的界面访问 Internet ，而无需访问彼此的流量。从 SD-WAN 11.5 版本开始，您可以使用 Citrix SD-WAN Orchestrator 服务配置防火墙分段。有关更多信息，请参阅 防火墙分段。

- 本地访客用户 Internet 接入
- 定义应用程序的员工-用户 Internet 访问
- 员工-用户可以继续将所有其他流量固定到 MCN
- 允许用户为特定路由域添加特定路由。
- 启用后，此功能将应用于所有路由域。

您还可以创建多个访问接口，以容纳单独的面向公共的 IP 地址。任一选项都为每个用户组提供所需的安全性。

通过选中 **Web** 管理界面的“监视器”**>**“流量”下的“流量”表中的“路由域”列，可以确认每个路由域都在使用 **Internet** 服务。



Flows Data

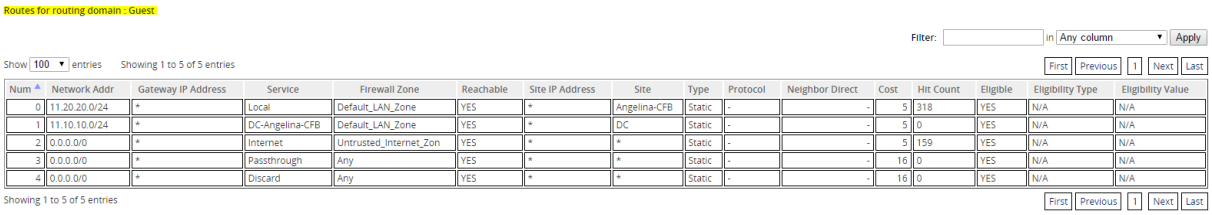
Toggle Columns

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
Guest	11.20.20.20	12.125.10.20	WAN Ingress	8	3335	ICMP	default	62	INTERNET	-	LOCAL	74	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	10.200.247.200	12.125.10.20	WAN Ingress	8	16185	ICMP	default	66	INTERNET	-	LOCAL	311	66	5544	1.009	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Guest	12.125.10.20	11.20.20.20	WAN Egress	0	18456	ICMP	default	62	INTERNET	-	LOCAL	94	62	5208	1.013	0.681	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A
Default	12.125.10.20	10.200.247.200	WAN Egress	0	3968	ICMP	default	66	INTERNET	-	LOCAL	328	66	5544	1.008	0.678	0.000	0.000	202	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 2 out of 2
Total EGRESS flows displayed: 2 out of 2

您还可以在 监控 > 统计信息 > 路由下查看每个路由域的 路由表。



Routes for routing domain : Guest

Filter: in Any column Apply

Show 100 entries Showing 1 to 5 of 5 entries First Previous 1 Next Last

Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	11.20.20.0/24	*	Local	Default_LAN_Zone	YES	*	Angelina-CFB	Static	-	-	5	318	YES	N/A	N/A
1	11.10.10.0/24	*	DC-Angelina-CFB	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
2	0.0.0.0/0	*	Internet	Untrusted_Internet_Zon	YES	*	*	Static	-	-	5	159	YES	N/A	N/A
3	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A
4	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	16	0	YES	N/A	N/A

Showing 1 to 5 of 5 entries First Previous 1 Next Last

用例

在以前的 Citrix SD-WAN 版本中，虚拟路由和转发存在以下问题，这些问题已得到解决。

- 客户在一个分支站点有多个路由域，而无需包含数据中心 (MCN) 的所有域。他们需要能够以安全的方式隔离不同客户的流量
- 客户必须能够为多个路由域提供单个可访问的防火墙公有 IP 地址，才能在一个站点访问 Internet （超出 VRF lite 版）。
- 客户需要为支持不同服务的每个路由域提供 Internet 路由。
- 分支站点上的多个路由域。
- 不同路由域的 Internet 接入。

分支站点上的多个路由域

通过虚拟转发和路由防火墙分段增强功能，您可以：

- 在分支站点提供支持至少两个用户组（如员工和来宾）的安全连接的基础结构。该基础架构最多可支持 16 个路由域。
- 隔离每个路由域的流量与任何其他路由域的流量。
- 为每个路由域提供 Internet 接入，
  - 一个通用的访问接口是必需的，并且可以接受

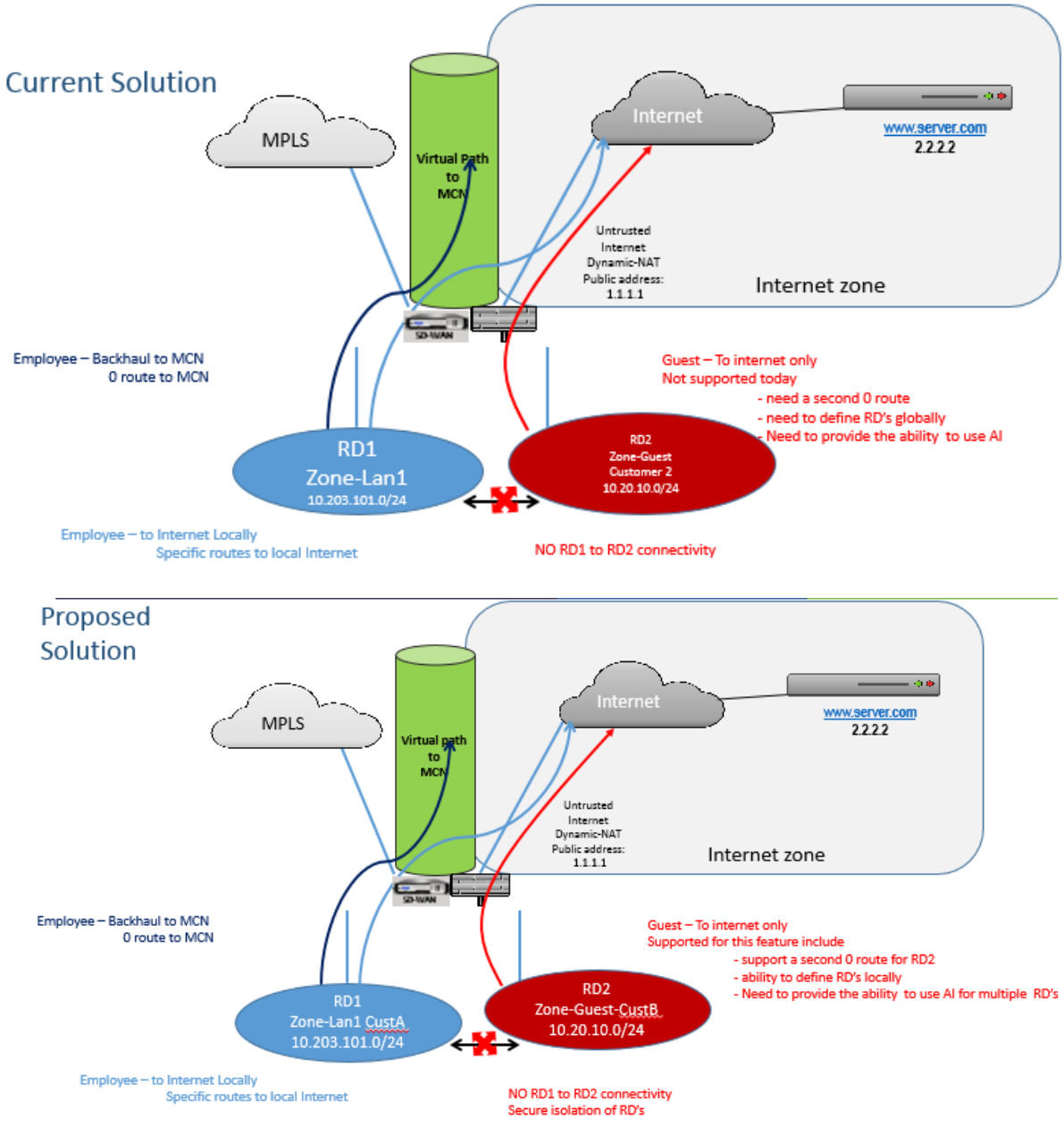
  - 具有单独面向公众的 IP 地址的每个组的访问接口

- 员工的流量可以直接路由到本地 Internet （特定应用程序）
- 员工的流量可以路由或回溯到 MCN 进行广泛筛选（0 路由）
- 路由域的流量可以直接路由到本地 Internet （0 路由）
- 如有必要，支持每个路由域的特定路由
- 路由域基于 VLAN 的路由域
- 删除 RD 必须驻留在 MCN 的要求
- 现在只能在分支站点配置路由域
- 允许您将多个 RD 分配给访问接口（一旦启用）
- 为每个 RD 分配一条 0.0.0.0 路径
- 允许为 RD 添加特定路由
- 允许来自不同 RD 的流量使用相同的接入界面退出到 Internet
- 允许您为每个 RD 配置不同的访问接口
- 必须是唯一的子网（RD 分配给 VLAN）
- 每个 RD 可以使用相同的 FW 默认区域
- 通过路由域隔离流量
- 出站流将 RD 作为流头的组成部分。允许 SD-WAN 将返回流映射到正确的路由域。

配置多个路由域的先决条件：

- Internet 访问配置并分配给 WAN 链接。
- 为 NAT 配置的防火墙，并应用了正确的策略。
- 全局添加第二个路由域。
- 添加到站点的每个路由域。
- 确保已正确定义 Internet 服务。

部署方案



限制

- 必须先将 Internet 服务添加到 WAN 链接，然后才能为所有路由域启用 Internet 访问。（在此之前，启用此选项的复选框显示为灰色）。

  为所有路由域启用 Internet 访问后，自动添加动态 NAT 规则。
- 每个站点最多可达 16 个路由域。
- 访问接口 (AI)：每个子网的单个 AI。

- 多个 AI 需要为每个 AI 单独的 VLAN。
- 如果一个站点中有两个路由域并有一个 WAN 链接，则两个域使用相同的公有 IP 地址。
- 如果为所有路由域启用 Internet 访问，则所有站点都可以路由到 Internet。（如果一个路由域不需要 Internet 访问，则可以使用防火墙阻止其流量。）
- 不支持多个路由域中的同一子网。
- 没有审核功能
- WAN 链接是共享的，以便访问 Internet 。
- 每个路由域没有 QoS；先到先得。

证书身份验证

September 2, 2022

Citrix SD-WAN 通过使用网络加密和虚拟路径 IPsec 通道等安全技术，确保在 SD-WAN 网络中的设备之间建立安全路径。除了现有的安全措施之外，Citrix SD-WAN 11.0.2 中还引入了基于证书的身份验证。

证书身份验证允许组织使用其私有证书颁发机构 (CA) 颁发的证书对设备进行身份验证。设备在建立虚拟路径之前进行身份验证。例如，如果分支设备尝试连接到数据中心，并且分支中心的证书与数据中心期望的证书不匹配，则不会建立虚拟路径。

CA 颁发的证书将公钥绑定到设备名称。公钥与证书标识的设备所拥有的相应私钥一起工作。

您可以使用 Citrix SD-WAN Orchestrator 服务启用 SD-WAN 设备的证书身份验证。有关证书身份验证的更多信息，请参阅 证书身份验证。

AppFlow 和 IPFIX

September 26, 2023

AppFlow 和 IPFIX 是流导出标准，用于识别和收集网络基础架构中的应用程序和事务数据。此数据可更好地了解应用程序流量利用率和性能。

收集的数据（称为流记录）将传输到一个或多个 IPv4 或 IPv6 收集器。收集器可聚合流记录，并生成实时或历史报告。

AppFlow

AppFlow 仅导出 HDX/ICA 连接的流量级数据。您可以为 HDX 数据集模板启用 TCP，也可以启用 HDX 数据集模板。仅适用于 HDX 的 TCP 数据集提供 多跳数据。HDX 数据集提供 HDX 洞察数据。

像 Splunk 和 Citrix ADM 这样的 AppFlow 收集器具有控制板来解释和呈现这些模板。

IPFIX

IPFIX 是一种收集器导出协议，用于导出所有连接的流量级数据。对于任何连接，您都可以查看数据包计数、字节计数、服务类型、流向、路由域、应用程序名称等信息。IPFIX 流通过管理界面传输。大多数收集器可以接收 IPFIX 流记录，但可能需要构建自定义控制板来解释 IPFIX 模板。

IPFIX 模板定义了解释数据流的顺序。收集器接收模板记录，后接数据记录。Citrix SD-WAN 使用模板 611 和 613 来导出 IPv4 IPFIX 流数据，615 和 616 导出 IPv6 IPFIX 流数据以及选项模板 612。

应用程序流信息 (IPFIX) 根据 IPv4 流程的模板 611 导出数据集，IPv6 流程为 615 个模板和带应用程序信息的 612 个选项模板导出数据集。

基本属性 (IPFIX) 按照 IPv4 流的模板 613 和 IPv6 流程的模板 616 导出数据集。

下表提供了与每个 IPFIX 模板相关联的流数据的详细列表。

应用程序流信息 **(IPFIX)-V10** 模板

模板 **ID - 611**

信息元素 **(IE)**	**IE** 名称和 **ID**	类型和莱恩	说明
观测点 ID	观测点 d，138	Unsigned32, 4	
导出进程 ID	出口加工 d，144	Unsigned32, 4	
流 ID	弗洛伊德，148	Unsigned64, 8	
IPv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
IPv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
伊普版	网络版本，60	Unsigned8, 1	设置为 4。
IP 协议编号	协议成员，4	Unsigned8, 1	
填充	不适用	Unsigned16, 2	
SRC 端口	来源运输港口, 7	Unsigned16, 2	
DST 端口	目的地交通工具,11	Unsigned16, 2	
Pkt 计数	数据包增数据包，2	Unsigned64, 8	
字节计数	八位变量，1	Unsigned64, 8	
第一个 pkt 的时间（以微秒为单位）	流动起动微秒, 154	日期时间微秒, 8	

信息元素 **(IE)**	**IE** 名称和 **ID**	类型和莱恩	说明
最后的时间（以微秒为单位）	流动微秒，155	日期时间微秒, 8	
IP ToS	分类管理服务, 5	Unsigned8, 1	
流标志	tcpControlBits, 6	Unsigned8, 2	当前设置为 0。
流动方向	流动方向，61	Unsigned8, 1	0x00：入口流量 0x01：出口流量-广域网和局域网-局域网流在 SDWAN 中是可能的
输入接口	入口接口，10	Unsigned32, 4	Citrix SD-WAN 负载平衡通过多个成员路径的数据流，因此单个数据流可以具有多个输入/输出接口组合。
输出接口	出格雷斯接口，14	Unsigned32, 4	Citrix SD-WAN 负载平衡通过多个成员路径的数据流，因此单个数据流可以具有多个输入/输出接口组合。
输入 VLAN ID	虚拟网路 ID, 58	Unsigned16, 2	
输出 VLAN ID	VLANID, 59	Unsigned16, 2	
VRF ID	英格雷斯维尔定位器, 234	Unsigned32, 4	
流程键指示器	流程键指示器，173	Unsigned64, 8	设置为 0x1E037F。
应用程序 ID	applicationId, 95	八角形，变量	应用程序 ID 与 DPI 引擎分类的应用程序的 ID 相同。应用程序 ID 保持不变。基于自定义域名的应用程序的应用程序 ID 随每次配置更新而发生变化。

模板 **ID —615**（**IPv6** 流程） | 信息元素 (IE)|IE 名称和 ID| 类型和莱恩 | 备注 |
|-|-|-|-|
| 观测点 ID| 观测点 d，138|Unsigned32, 4|
| 导出进程 ID| 出口加工 d，144|Unsigned32, 4|
| 流 ID| 弗洛伊德，148|Unsigned64, 8|
|Ipv6 SRC IP|sourceIPv6Address, 27|Ipv6address, 16|
|IPv6 DST IP|destinationIpv6Addres, 28|Ipv6address, 16|
|Ipversion|ipVersion, 60|Unsigned8, 1|Set to 6| |

IP protocol number	protocoldentifier, 4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds	flowStartMicroseconds, 154	dateTimeMicroseconds, 8	
Time for lastpkt in microseconds	flowEndMicroseconds, 155	dateTimeMicroseconds, 8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. 应用程序 ID 保持不变。基于自定义域名的应用程序的应用程序 ID 随每次配置更新而变化。

模板 **612**（选项模板）

信息元素 **(IE)**	**IE** 名称和 **ID**	类型	备注
应用程序 ID	applicationId, 95	八角星	应用程序 ID 与 DPI 引擎分类的应用程序的 ID 相同。应用程序 ID 保持不变。基于自定义域名的应用程序的应用程序 ID 随每次配置更新而发生变化。
应用程序名称	应用程序名称，96	string	指定特定于 Citrix SDWAN 的专有应用程序的名称。

信息元素 **(IE)**	**IE** 名称和 **ID**	类型	备注
应用程序说明	应用说明, 94	string	指定应用程序的描述。

基本属性 **(IPFIX)** —**V9** 兼容模板**-**模板 **613**（**IPv4** 流程）

信息元素 **(IE)**	**IE** 名称和 **ID**	类型和莱恩	备注
IPv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
IPv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
伊普版	网络版本，60	Unsigned8, 1	
IP 协议编号	协议程序，4	Unsigned8, 1	
IP ToS	分类管理服务, 5	Unsigned8, 1	
流动方向	流动方向，61	Unsigned8, 1	0x00：入口流量 0x01：出口流量-广域网和局域网-局域网流在 SDWAN 中是可能的
SRC 端口	来源运输港口, 7	Unsigned16, 2	
DST 端口	目的地运输港口，11	Unsigned16, 2	
Pkt 计数	数据包增数据包，2	Unsigned64, 8	
字节计数	八位变量，1	Unsigned64, 8	
输入接口	入口接口，10	Unsigned32, 4	Citrix SD-WAN 负载平衡通过多个成员路径的数据流，因此单个数据流可以具有多个输入/输出接口组合。
输出接口	出格雷斯接口，14	Unsigned32, 4	Citrix SD-WAN 负载平衡通过多个成员路径的数据流，因此单个数据流可以具有多个输入/输出接口组合。
输入 VLAN ID	虚拟网路 ID, 58	Unsigned16, 2	
输出 VLAN ID	VLANID, 59	Unsigned16, 2	

模板 **ID** —**616**（**IPv6** 流程） | 信息元素 (IE)|IE 名称和 ID| 类型和莱恩 | 备注 |
|-|-|-|-|

Ipv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16
IPv6 DST IP	destinationIpv6Addres, 28	Ipv6address, 16
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6	
IP protocol number	protocoldentifier,4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort, 11	Unsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

限制

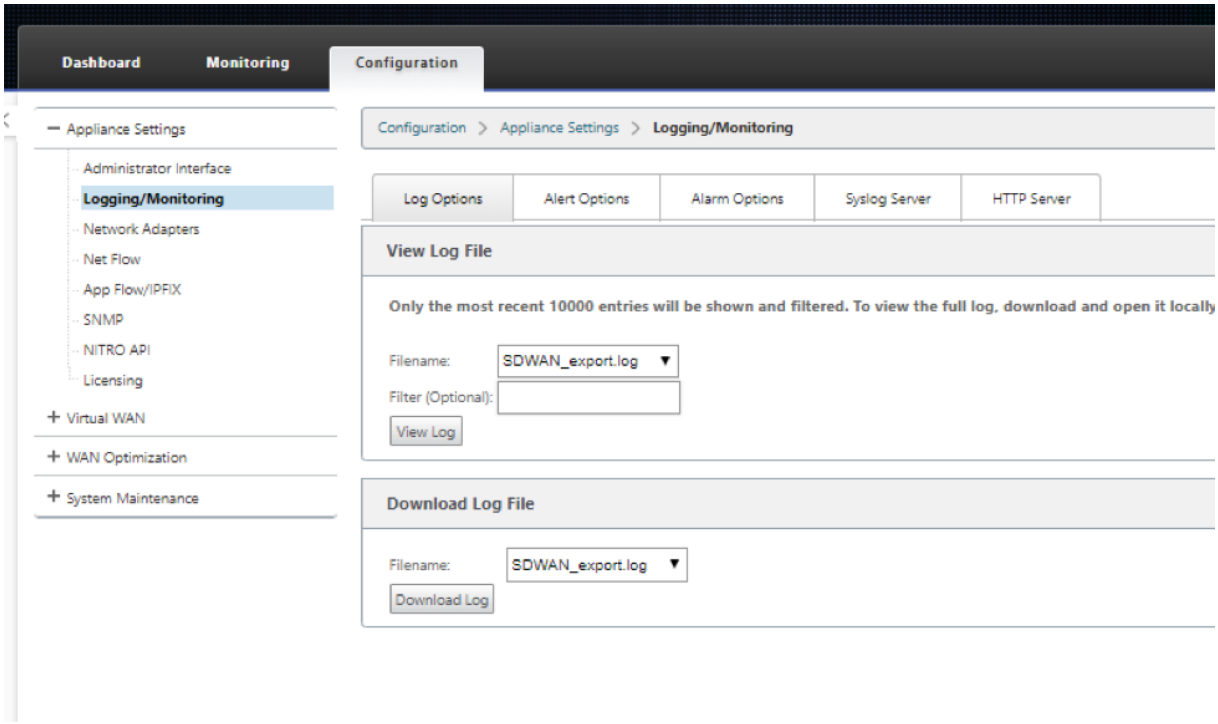
- AppFlow 不支持 IPv6 收集器和流记录。
- 净流的导出间隔从 15 秒增加到 60 秒。
- AppFlow /IPFIX 流通过 UDP 传输，连接丢失不是所有的数据都被重新传输。如果导出间隔设置为 X 分钟，则设备仅存储 X 分钟的数据。连接损失 X 分钟后重新传输。
- 在 Citrix SD-WAN 版本 10 版本 2 中，**AppFlow** 设置为每个设备的本地设置，而在以前的版本中，它是全局设置。如果 SD-WAN 软件版本降级为以前的任何版本，并且如果 AppFlow 在任何一台设备上配置，则该版本将在全球范围内应用于所有联盟。

配置 **AppFlow/IPFIX**

只能通过 Citrix SD-WAN Orchestrator 服务配置 AppFlow/IPFIX。有关详细信息，请参阅 AppFlow 和 IPFIX。

日志文件

有关 AppFlow/IPFIX 导出协议的疑难解答，您可以查看并下载 SDWAN_Export.log 文件。导航到 配置 **>** 日志记录/监视，然后选择 **SDWAN_Export.log** 文件。



SNMP

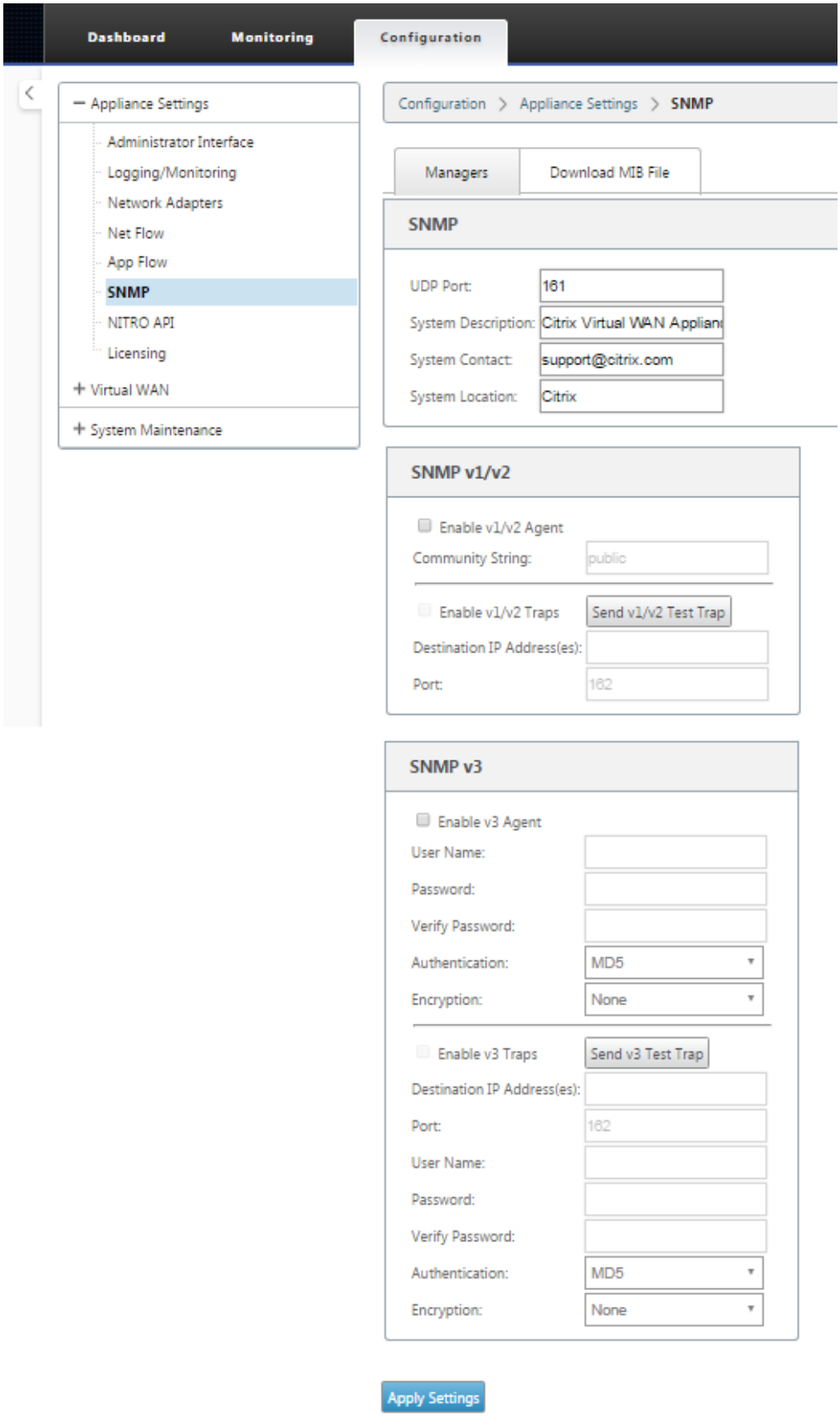
November 16, 2022

Citrix SD-WAN 支持 SNMPV1/V2 功能，每个 SNMPv3 功能只有一个用户帐户。此限制具有以下优点：

- 确保网络设备的 SNMPv3 合规性
- 验证 SNMPv3 能力
- 轻松配置 SNMPv3

要配置 SNMPv3 轮询和陷阱，请导航到配置 -> 设备设置 -> **SNMP** 页面的 SNMPv3 部分，并根据需要填写字段。

> 注意：
>
> 要配置 IPv6 地址，请确保 SNMP 服务器也配置了 IPv6 地址。



标准 **MIB** 支持

SD-WAN 设备支持以下标准 MIB。

MIB	RFC（定义链接）
DISMAN-EVENT-MIB	https://www.ietf.org/rfc/rfc2981.txt
IF-MIB	https://www.ietf.org/rfc/rfc2863.txt
IP-FORWARD-MIB	https://www.ietf.org/rfc/rfc4292.txt
IP-MIB (部分)	https://www.ietf.org/rfc/rfc4293.txt
Q-BRIDGE-MIB（部分）	http://www.ieee802.org/1/files/public/MIBs/IEEE8021-Q-BRIDGE-MIB-201112120000Z.mib
RFC1213-MIB	https://www.ietf.org/rfc/rfc1213.txt
SNMPv2-MIB	https://www.ietf.org/rfc/rfc3418.txt
TCP-MIB	https://www.ietf.org/rfc/rfc4022.txt
P-BRIDGE-MIB.txt	http://www.icir.org/fenner/mibs/extracted/P-BRIDGE-MIB-rfc2674.txt
RMON2-MIB.txt	https://www.ietf.org/rfc/rfc3273.txt
TOKEN-RING-RMON-MIB.txt	http://www.icir.org/fenner/mibs/extracted/TOKEN-RING-RMON-MIB-rmonmib-01.txt

必须先下载以下 SNMP 文件，然后才能开始监视 Citrix SD-WAN 设备：

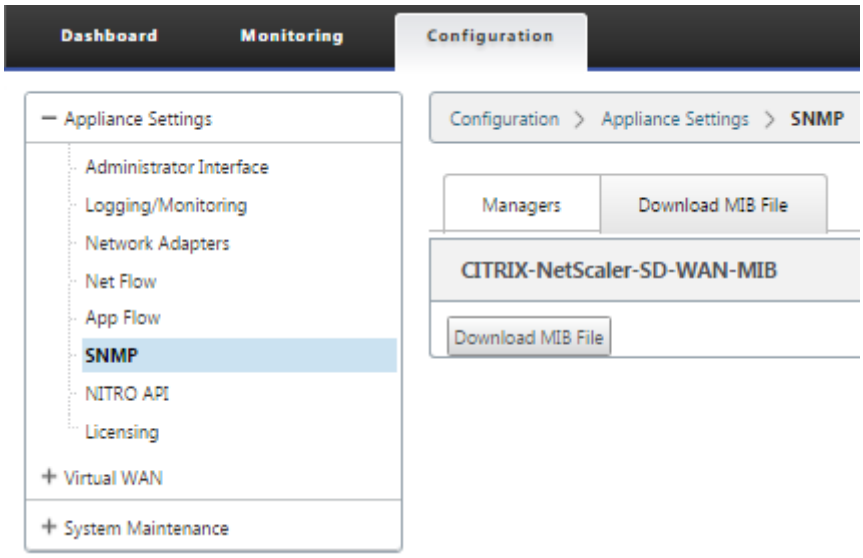
- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

MIB 文件由 SNMPv3 管理器和 SNMPv3 陷阱侦听器使用。这些文件包括 SD-WAN 设备企业 MIB，它们提供 SD-WAN 特定事件。要下载 MIB 文件，请在 SD-WAN Web 管理界面中执行以下操作：

1. 导航到 配置 > 装置设 置 > **SNMP** > 下载 **MIB** 文件页面。
2. 选择所需的 **MIB** 文件。

3. 单击“查看”。

   MIB 文件在 MIB 浏览器中打开。



> 注意
>
> - 默认情况下，Linux 系统上的 **net-snmp snmpd** 守护进程提供对这些 MIB 的支持。MIB 为支持网络管理应用程序提供了基础。
> - 以太网端口数据包和字节计数器位于 **ifTable** 内的 **IF-MIB** 中。系统信息位于系统对象中。
> - **ifTable** 中包含以太网端口，因此步行必须足以确保 SNMP 子系统正在运行。
> - **Q-BRIDGE-MIB** 和 IP-MIB** 支持为网络映射应用程序提供支持。

管理界面

September 2, 2022

可以使用 Citrix SD-WAN Orchestrator 服务使用以下管理选项管理和维护 Citrix SD-WAN 设备。有关详细信息，请参阅设备设置。

- 用户帐户
- RADIUS 服务器
- TACACS+ 服务器
- HTTPS 证书
- HTTPS 设置
- 其他

用户帐户

您可以在配置 > 装置 设置 **>** 管理员界面页面 **>** 用户帐户选项卡下添加新用户帐户并管理现有用户帐户。

您可以选择通过 SD-WAN 设备在本地或远程对新添加的用户帐户进行身份验证。远程验证的用户帐户通过 RADIUS 或 TACACS+ 身份验证服务器进行身份验证。

用户角色

支持以下用户角色：

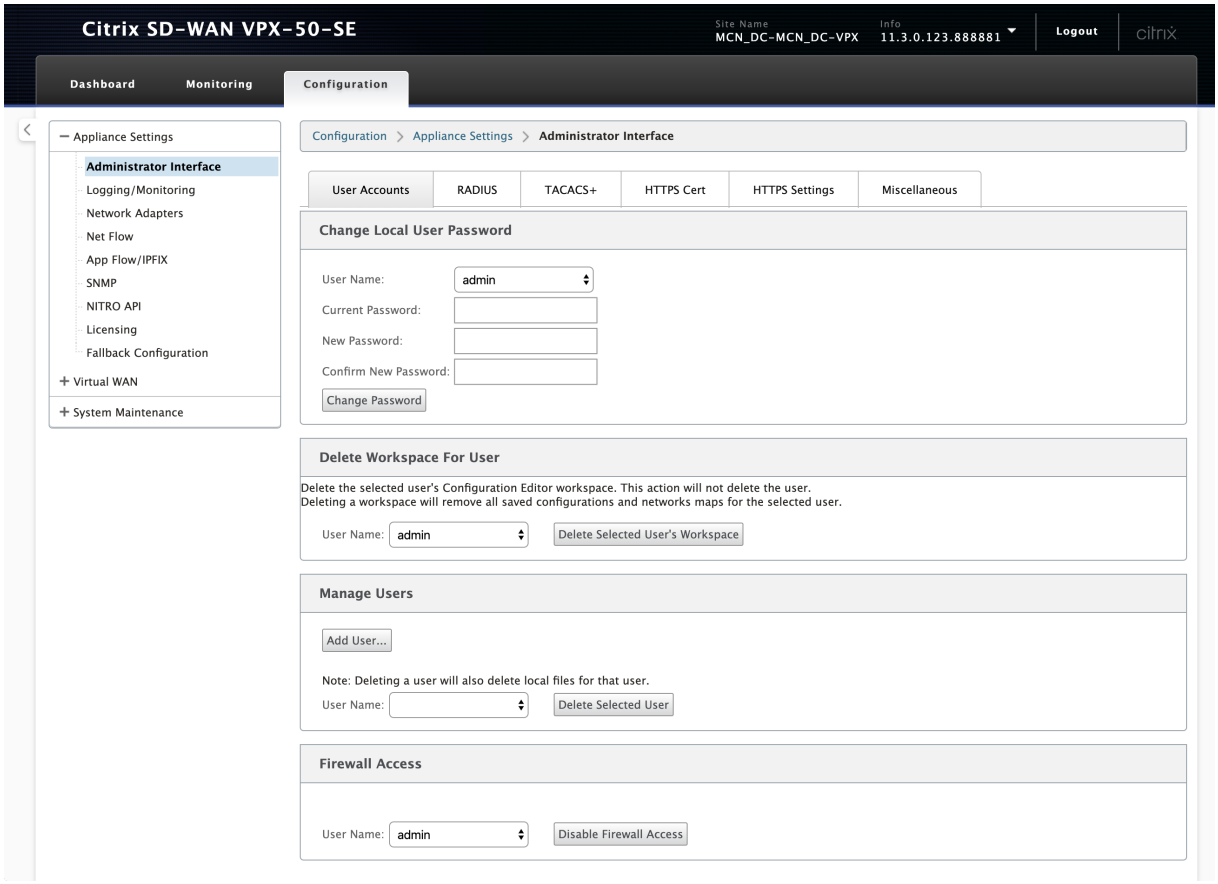
- 查看者：查看者帐户是一个只读帐户，可以访问控制面 板、报告和 监 控页面。
- 管理员：管理员帐户对所有部分具有管理权限和读写权限。

  超级管理员具有以下权限：

  - 可以将配置导出到更改管理收件箱，以便对网络执行配置和软件更新。
  - 还可以切换网络管理员和安全管理员的读写访问权限。
  - 维护与网络和安全相关的设置。
- 安全管理员：安全管理员仅具有防火墙和安全相关设置的读写访问权限，而对其他部分具有只读访问权限。安全管理员还可以为超级管理员 (admin) 以外的其他用户启用或禁用对防火墙的写访问权限。
- 网络管理员：网络管理员对所有部分都具有读写权限，并且可以完全配置除防火墙和安全相关设置之外的分支。网络管理员不能使用托管防火墙节点。在这种情况下，网络管理员必须导入新配置。

网络管理员和安全管理员都可以对配置进行更改，也可以将其部署到网络上。

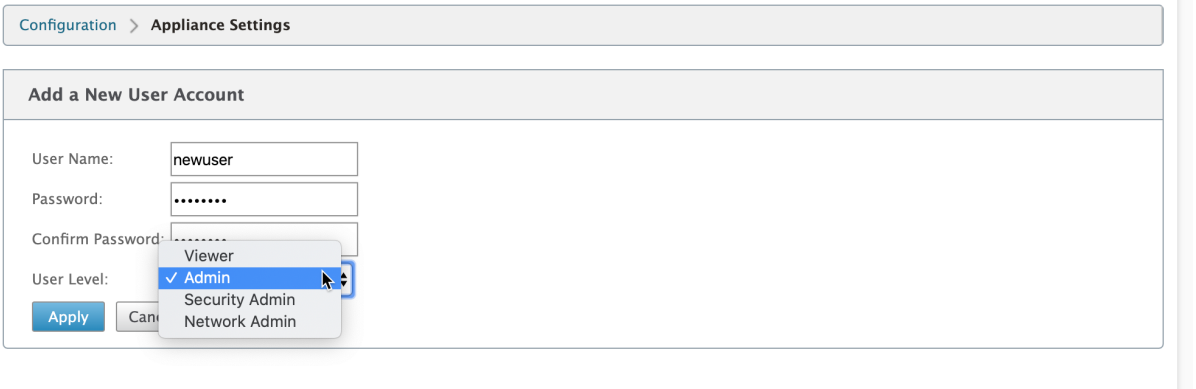
> 注意：
>
> 网络管理员和安全管理员无法添加或删除用户帐户。他们只能编辑自己的帐户密码。



添加用户

要添加用户，请单击 管理用户部分中的添加用 户。提供用 户名 和 密码。从用户 级别下拉列表中选择用户 角色，然后单击 应用。

如果需要，您还可以删除用户帐户。删除用户还会删除属于该用户的本地文件。要删除，请在“管理用户”部分下的“用户 名”下拉列表中选择用户，然后单击 删除选定用户。



更改用户的密码

管理员角色可以更改由 SD-WAN 设备在本地进行身份验证的用户帐户的密码。

要更改密码，请在“更改本地用户密码”部分下，从“用 户名”下拉列表中选择用户。输入当前密码和新密码。单击“更改密码”。

RADIUS 服务器

您可以将 SD-WAN 设备配置为使用一个或最多三个 RADIUS 服务器验证用户访问权限。默认端口是 1812。

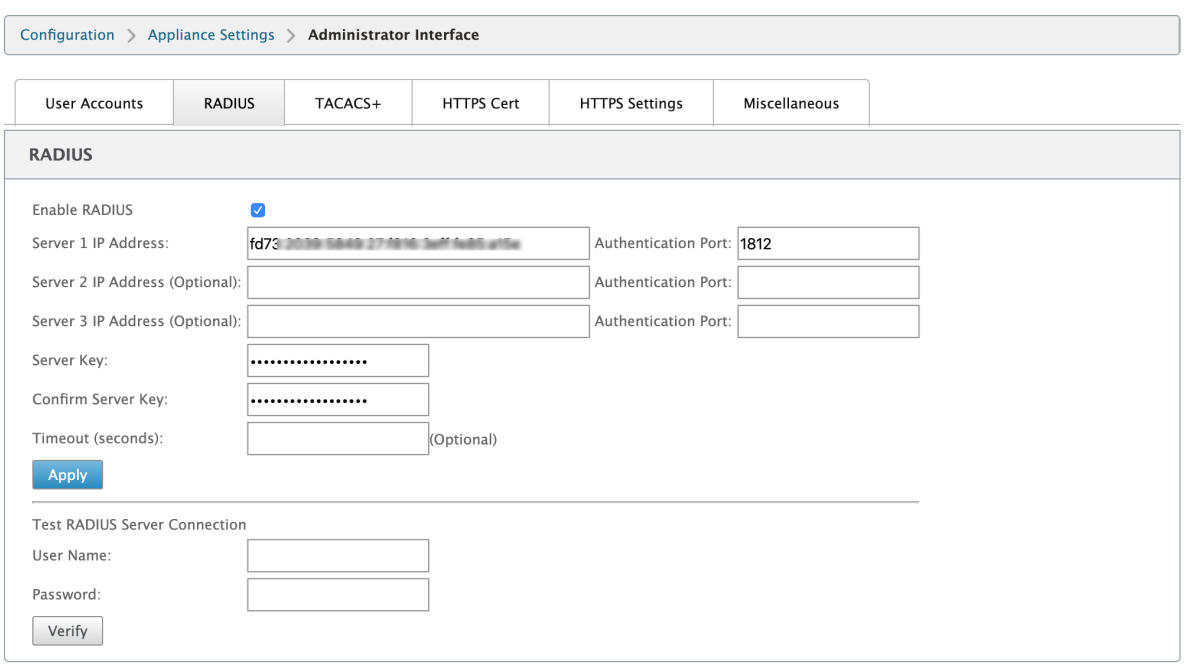
要配置 RADIUS 服务器：

1. 导航到 配置 **>** 装置设置 **>** 管理员界面 **> RADIUS**。
2. 选中 启用 **RADIUS** 复选框。
3. 输入 服务器 **IP** 地址 和 身份验证端口。最多可以配置三个服务器 IP 地址。

   > 注意：
   >
   > 要配置 IPv6 地址，请确保 RADIUS 服务器还配置了 IPv6 地址。

4. 输入 服务器密钥 并确认。
5. 输入 超 时值（以秒为单位）。
6. 单击保存。

您还可以测试 RADIUS 服务器连接。输入 用户名 和 密码。单击 **Verify**（验证）。



TACACS+ 服务器

您可以配置 TACACS+ 服务器进行身份验证。与 RADIUS 身份验证类似，TACACS+ 使用私钥、IP 地址和端口号。默认端口号为 49。

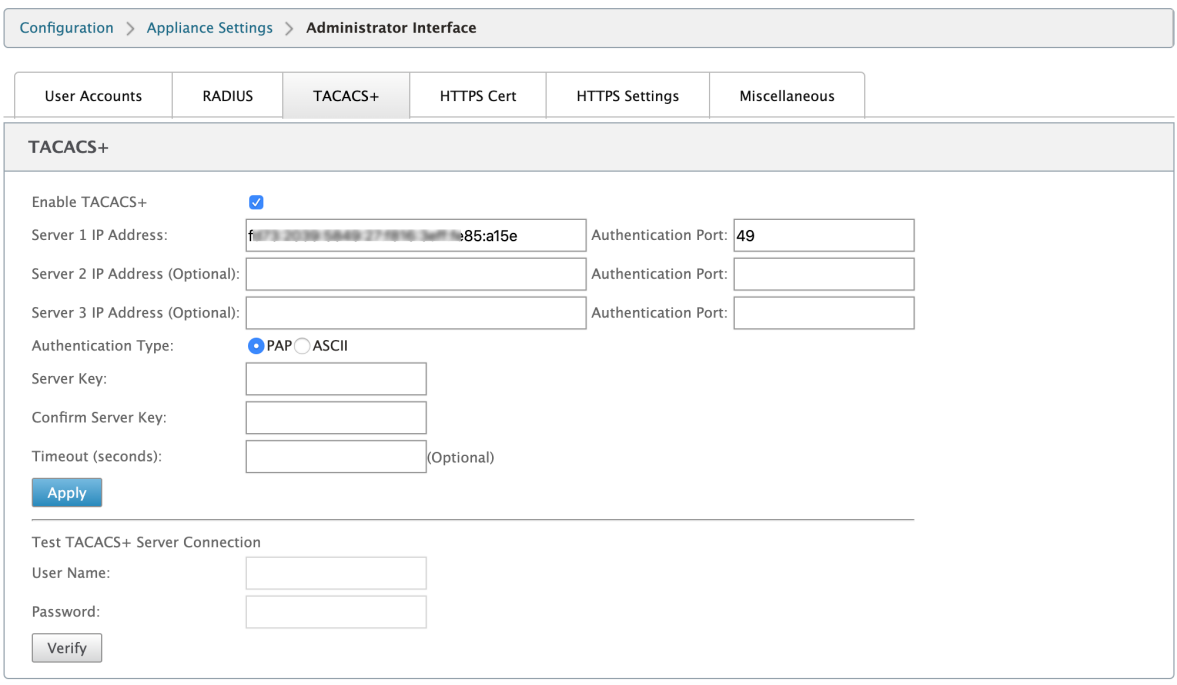
要配置 TACACS+ 服务器，请执行以下操作：

1. 导航到 配置 **>** 装置设置 **>** 管理员界面 **> TACACS+**。
2. 选中 启用 **TACACS+** 复选框。
3. 输入 服务器 **IP** 地址 和 身份验证端口。最多可以配置三个服务器 IP 地址。

   > 注意：
   >
   > 要配置 IPv6 地址，请确保 TACACS+ 服务器还配置了 IPv6 地址。

4. 选择 **PAP** 或 **ASCII** 作为身份验证类型。
   - PAP：使用密码身份验证协议 (PAP) 通过向 TACACS+ 服务器分配强共享密钥来加强用户身份验证。
   - ASCII：使用 ASCII 字符集通过向 TACACS+ 服务器分配强共享密钥来加强用户身份验证。
5. 输入 服务器密钥 并确认。
6. 输入 超 时值（以秒为单位）。
7. 单击保存。

您还可以测试 TACACS+ 服务器连接。输入 用户名 和 密码。单击 **Verify**（验证）。



NDP 路由器通告和前缀委派组

November 16, 2022

NDP 路由器通告

在 IPv6 网络中，SD-WAN 设备定期多播路由器通告 (RA) 消息，以宣布其可用性并将信息传达给 SD-WAN 网络中的邻近设备。路由器通告包括 IPv6 前缀信息。在 SD-WAN 设备上运行的邻居发现协议 (NDP) 使用这些路由器通告来确定同一链路上的相邻设备。它还可以确定彼此的链路层地址、查找邻居以及维护有关通往活动邻居的路径的可达性信息。

您可以使用 Citrix SD-WAN Orchestrator 服务配置 NDP 路由器播发。有关详细信息，请参阅 NDP 路由器通告。

前缀委派组

> 注意
>
> Citrix SD-WAN 11.3 版本不支持前缀委派。

Citrix SD-WAN 设备可配置为 DHCPv6 客户端，以使用配置的 WAN 端口向 ISP 请求前缀。Citrix SD-WAN 设备收到前缀后，它将使用前缀创建 IP 地址池以满足 LAN 客户端需求。然后，Citrix SD-WAN 设备将作为 DHCP 服务器行为，并将 LAN 端口上的前缀通告给 LAN 端口客户端。

您可以通过 Citrix SD-WAN Orchestrator 服务配置前缀委派。有关更多信息，请参阅为 委托组添加前缀。

如何查看文章

September 2, 2022

如何处理文章 描述了 Citrix SD-WAN 配置支持的功能的过程。这些文章包含有关以下一些重要功能的信息：

单击下面的功能名称以查看该功能的操作方法文章列表。

- 虚拟路由和转发
- 启用 RED 实现 QoS 公平性
- 配置
- 动态路由
- DHCP 服务器和 DHCP 中继
- 路由过滤器

- IPsec 终止和监视
- Secure Web Gateway
- QoS
- 符合 FIPS 标准的操作-IPsec 通道
- 动态 NAT 配置
- 自适应带宽检测
- 主动带宽测试
- BGP 增强功能
- 与 SSL 配置文件的服务类关联
- 零接触部署

配置访问接口

September 2, 2022

要通过 Citrix SD-WAN Orchestrator 服务配置访问接口，请参阅 广域网链接。

配置虚拟 **IP** 地址

September 2, 2022

要通过 Citrix SD-WAN Orchestrator 服务配置虚拟 IP 地址，请参阅 广域网链接。

配置 **GRE** 通道

September 2, 2022

要使用 Citrix SD-WAN Orchestrator 服务配置 GRE 通道，请参阅 GRE 服务。

设置分支到分支通信的动态路径

November 16, 2022

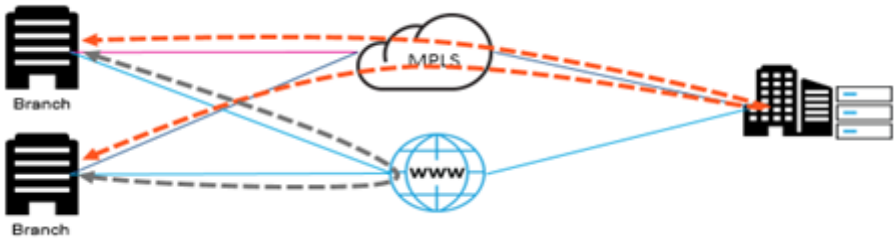
随着对 VoIP 和视频会议的需求，办公室之间的流量越来越多。通过数据中心设置完整的网状连接效率低下，这可能会很耗时。

使用 Citrix SD-WAN，您无需在每个办公室之间配置路径。您可以启用动态路径功能，SD-WAN 解决方案可根据需要自动创建办公室之间的路径。会话最初使用现有的固定路径。当满足带宽和时间阈值时，如果新路径具有比固定路径更好的性能特征，则会动态创建路径。会话流量通过新路径传输。这将导致资源的有效利用。路径仅在需要时才存在，从而减少传输到数据中心和传出数据中心的流量。

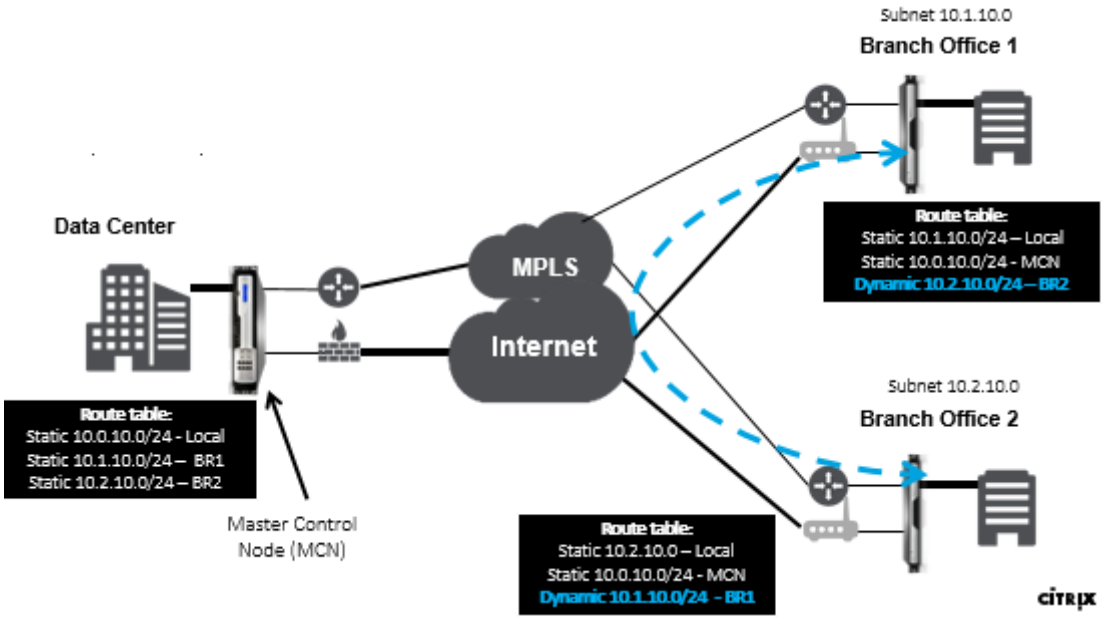
SD-WAN 网络的其他优势包括：

- 允许分支到分支连接的带宽和 PPS 阈值
- 降低进出数据中心的带宽需求，同时最大限度地减少延迟
- 根据需求创建的路径取决于设置的阈值
- 不需要时动态释放网络资源
- 减少主控节点上的负载和延迟

使用动态虚拟路径的分支到分支通信：



带动态路径的 SD-WAN 网络：



- 动态虚拟路径用于大规模部署，例如企业
- 较小的部署使用静态虚拟路径和任何到任何虚拟路径
- 始终使用两个数据中心（DC 到 DC）之间的静态虚拟路径
- 并非所有 WAN 路径都需要配置为使用动态虚拟路径
- 每个 SD-WAN 设备都具有可配置的动态虚拟路径数量有限（8 个动态最低限值，8 个静态最低限值 = 共 16 个）。

如何在 **SD-WAN GUI** 中启用动态虚拟路径

要使用 Citrix SD-WAN Orchestrator 服务启用动态虚拟路径，请参阅 虚拟路径。

广域网转发

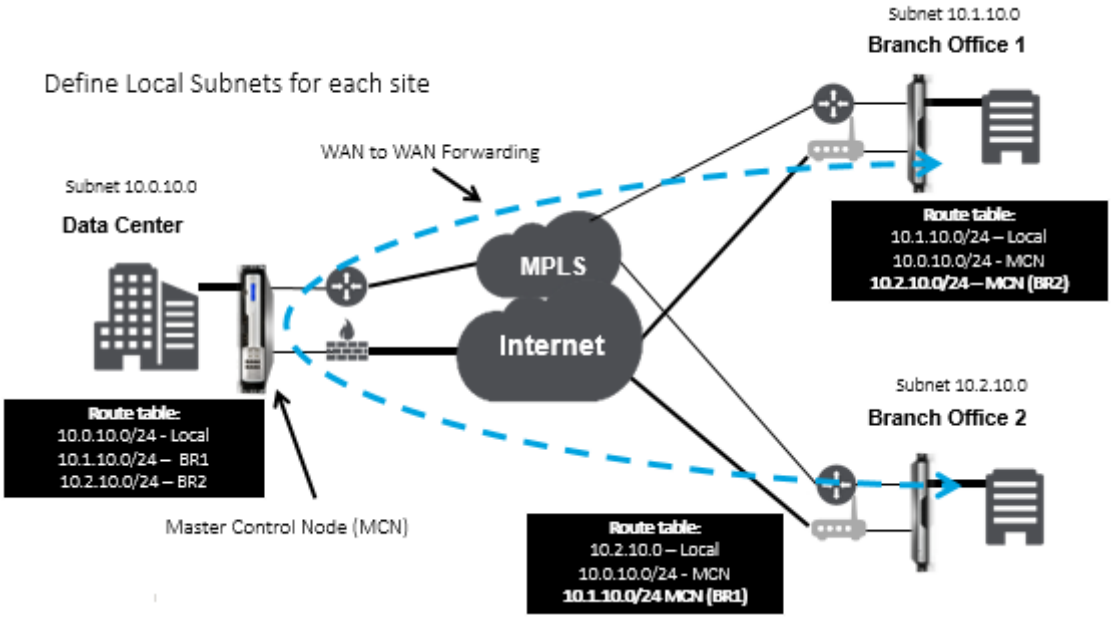
September 2, 2022

在 MCN 上启用 WAN 到 WAN 转发，允许 MCN 通告远程站点路由。

- 客户了解 MCN 本地路由和其他客户端站点路由
- 从客户端角度来看，所有路由都被视为 MCN 路由

当在 MCN 上未启用 WAN 转发时，客户网络中会遇到分支到分支的通信问题。

在 MCN 上启用 WAN 到 WAN 转发之前，在客户端模式下运行的设备不知道其他分支子网。启用此选项可使分支 SD-WAN 节点了解其他分支子网。发往其他分支的流量将转发到 MCN。MCN 将其路由到正确的目的地。



监视和故障排除

September 2, 2022

您可以使用 Citrix SD-WAN 设备 Web 管理界面来监视支持的功能并进行故障排除。以下是适用于 Citrix SD-WAN 设备的监视和故障排除主题的链接。

监视虚拟广域网

查看统计信息

查看流信息

查看报告

查看防火墙统计信息

诊断工具

改进了路径映射和带宽

管理 IP 故障排除

主动带宽测试

自适应带宽检测

监视虚拟广域网

September 2, 2022

查看设备的基本信息

使用浏览器连接到要监视的装置的管理 Web 界面，然后单击控 制板 选项卡以显示该装置的基本信息。

控制板 页面显示本地设备的以下基本信息：

系统状态：

- 名称—这是您将设备添加到系统时分配给设备的名称。
- 型 号—这是虚拟 WAN 设备型号。
- 装置模式—这表明此设备是否已配置为主 MCN 或辅助 MCN，还是作为客户端设备。
- 管理 **IP** 地址—这是设备的管理 IP 地址。
- 设备正常运行时间—这指定自上次重新启动以来设备一直在运行的持续时间。
- 服务正常运 行时间—这指定自上次重新启动以来虚拟 WAN 服务一直在运行的持续时间。

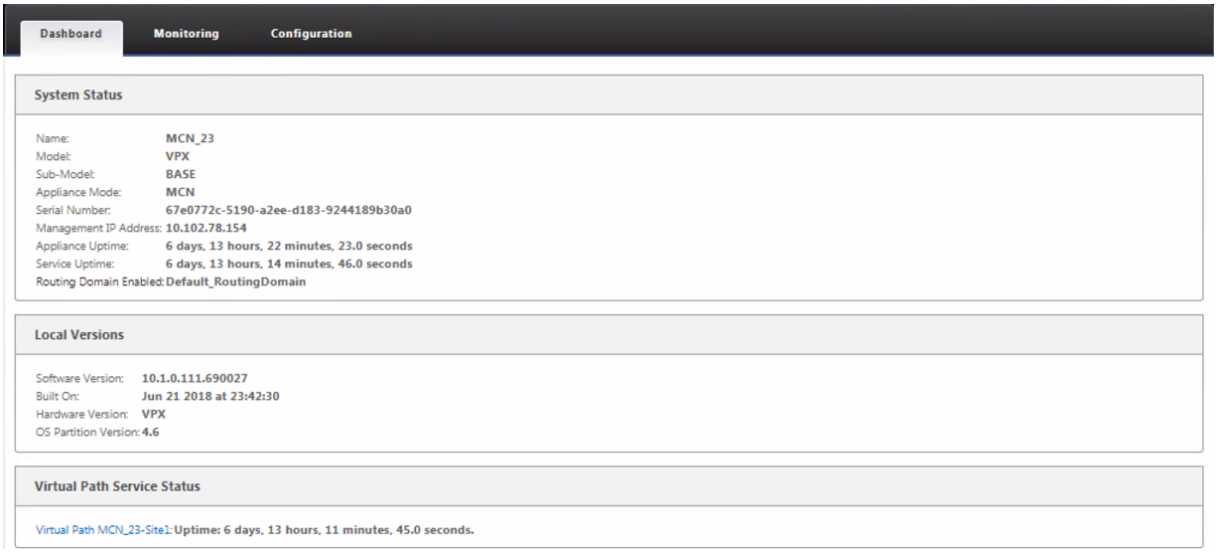
虚拟路径服务状态：

虚拟路径 **[**站点名称**]** —显示与此设备关联的所有虚拟路径的状态。如果启用了虚拟广域网服务，则页面上将包含此部分。如果禁用了虚拟广域网服务，则会显示一个警报图标（金色增量）和该效果的警报消息来代替此部分。

本地版本信息：

- 软件版本—这是设备上当前激活的 CloudBridge 虚拟路径软件包的版本。
- **Build on** —这是当前在本地设备上运行的产品版本的构建日期。
- 硬件版本—这是设备的硬件型号和版本。
- 操作系统分区版本—这是设备上当前活动的操作系统分区的版本。

下图 显示了一个示例控制板页面。



查看统计信息

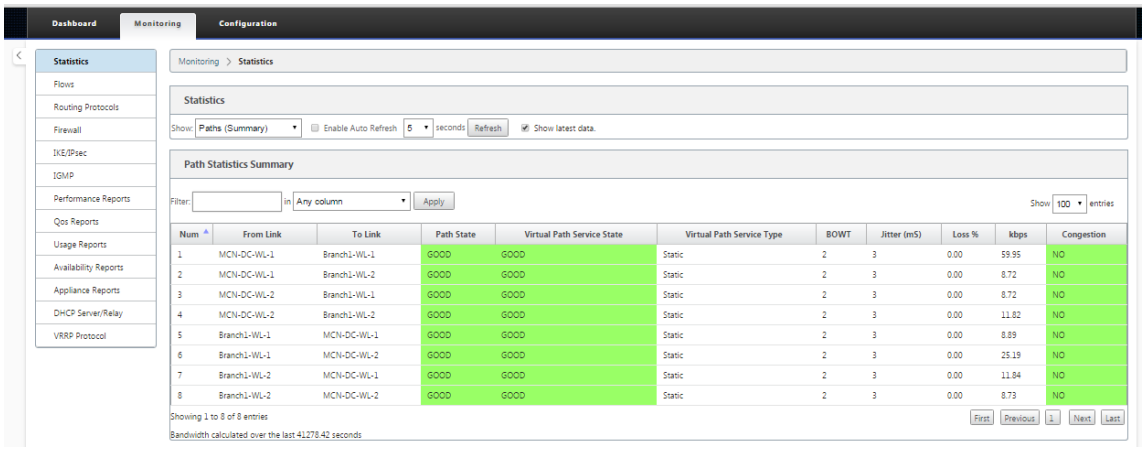
September 2, 2022

本节提供有关查看虚拟 WAN 统计信息的基本说明。

1. 登录 到 MCN 的管理 Web 界面。
2. 选择“监视”选项卡。

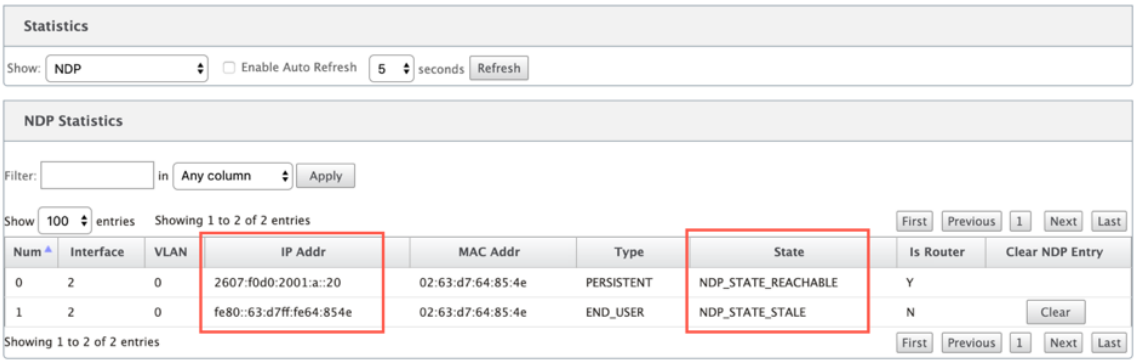
   这将在左窗格中打开“监视”导航树。默认情况下，这还会显示 统计信息 页面，其中在“显 示”字段中预先选择了 路径这包含路径统计信息的详细表。

   > 注意
   >
   > 如果导航到另一个 监视 页面（例如，流量），则可以通过在 监视 导航树（左窗格）中选择 统计 来返回到此页面。

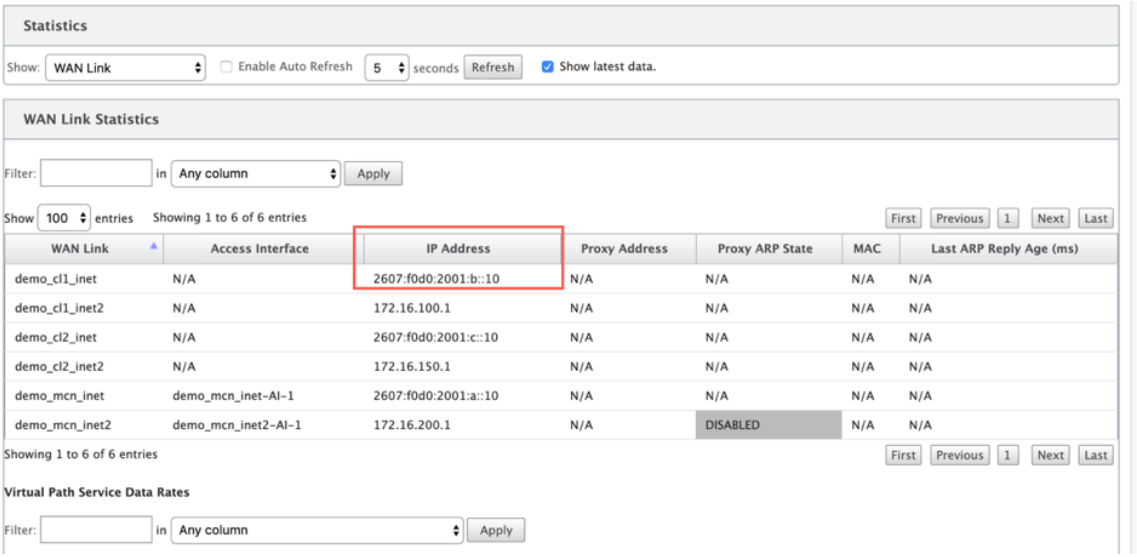


在 11.1.0 版本中，添加了邻居发现协议 (NDP) 选项以调试邻居发现问题。

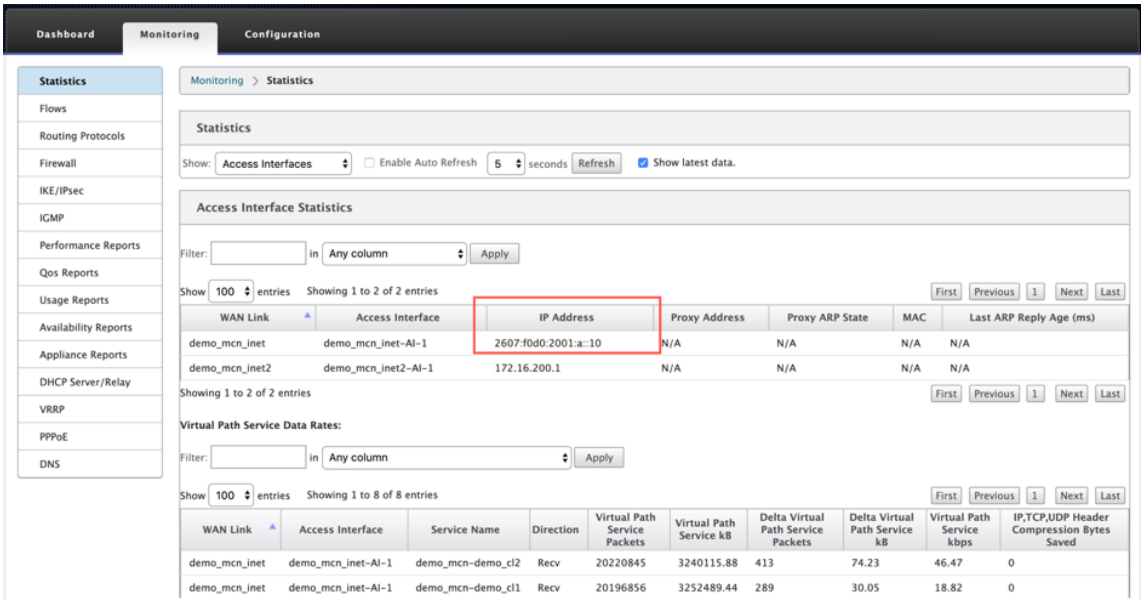
1. 从“显示”下拉菜单中选择“NDP”选项，您可以查看 NDP 的状态以及 IPv6 地址。



2. 从下拉菜单中选择 WAN 链接。如果在“IP 地址”选项卡下配置，也可以查看 IPv6 地址。

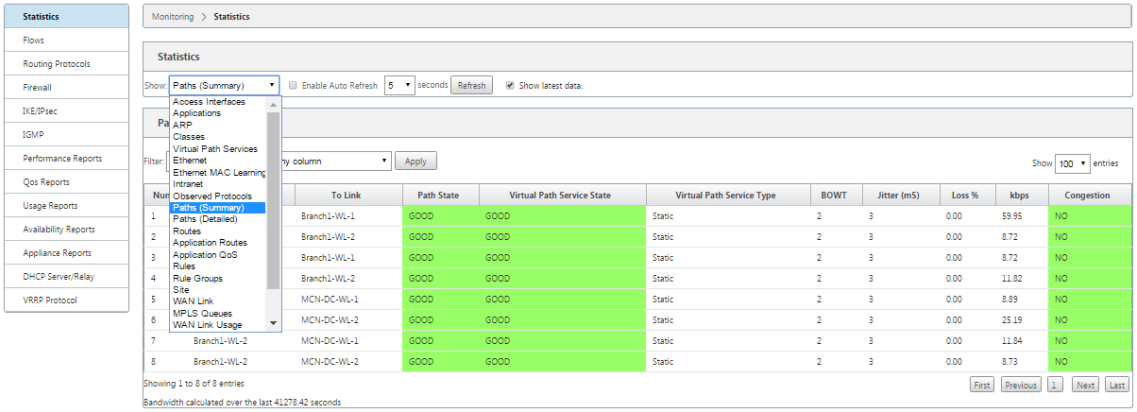


3. 您还可以查看接入接口统计信息。



4. 打开显 示 下拉菜单。

   除了 路径、**NDP**、访问接口和 WAN 链接统计信息之外，显示 菜单还提供了多个用于筛选和查看统计信息的选项。



从 显示 菜单中选择一个筛选器，以查看该主题的统计信息表。

查看流信息

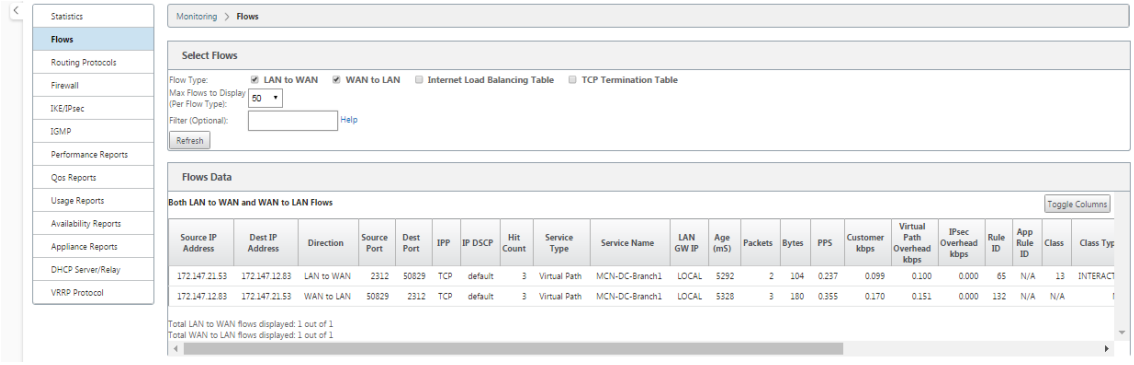
September 2, 2022

本节提供有关查看虚拟 WAN 流信息的基本说明。

要查看流信息，请执行以下操作：

1. 登录到 MCN 的管理 Web 界面，然后选择 监视 选项卡。它会在左侧窗格中打开“监控”导航树。

2. 在导航树中选择 流量 分支。它显示流量页面，其中包含在流程类型字段中预先选择了 **LAN** 到 **WAN**。



3. 选择 流量类型。流量类型字段位于流量页面顶部的选择流量部分。“流程类型”字段旁边有一行复选框选项，用于选择要查看的流程信息。您可以选中一个或多个框来筛选要显示的信息。

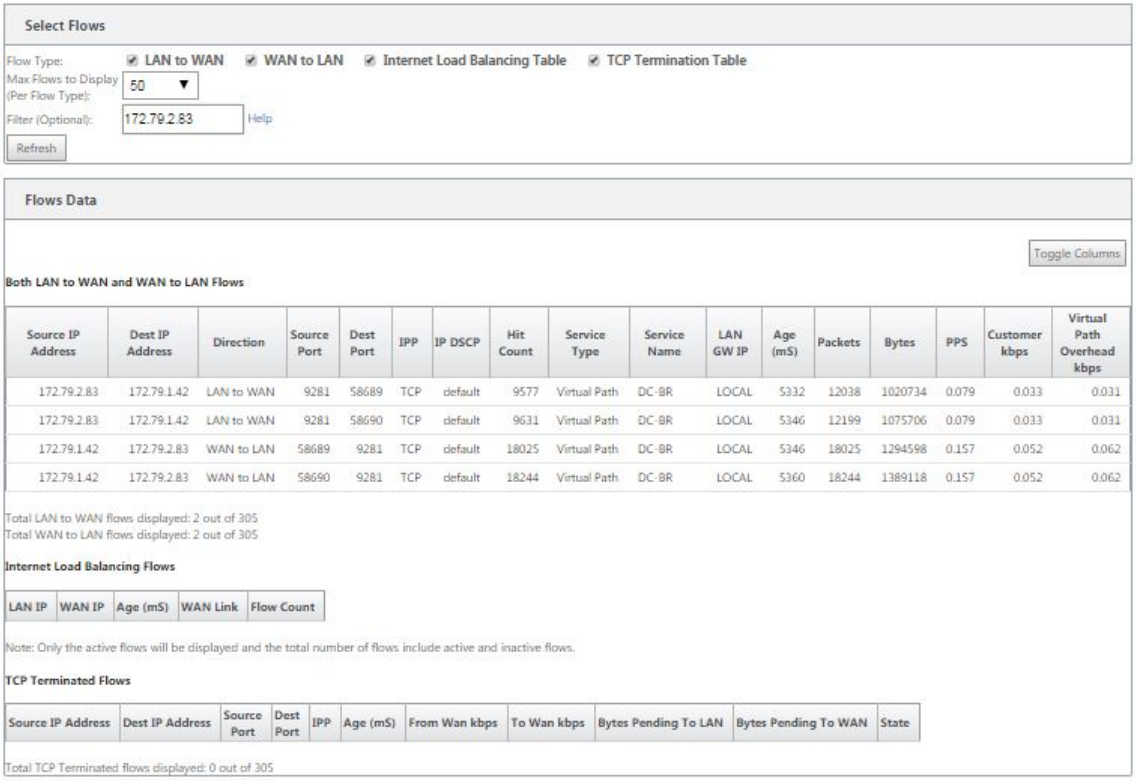
4. 从该字段旁边的下拉菜单中选择要显示的最大流量。

5. 它决定了要在流量表格中显示的条目数。选项包括：**50**、**100**、**1000**。

6. （可选）在 筛选器 字段中输入搜索文本。它筛选表格结果，以便表格中仅显示包含搜索文本的条目。

> 提示
>
> 要查看有关使用筛选器优化 流程 表结果的详细说明，请单击筛选 器 字段右侧的 帮助。要关闭帮助显示，请单击“选择流程”部分左下角的“刷新”。

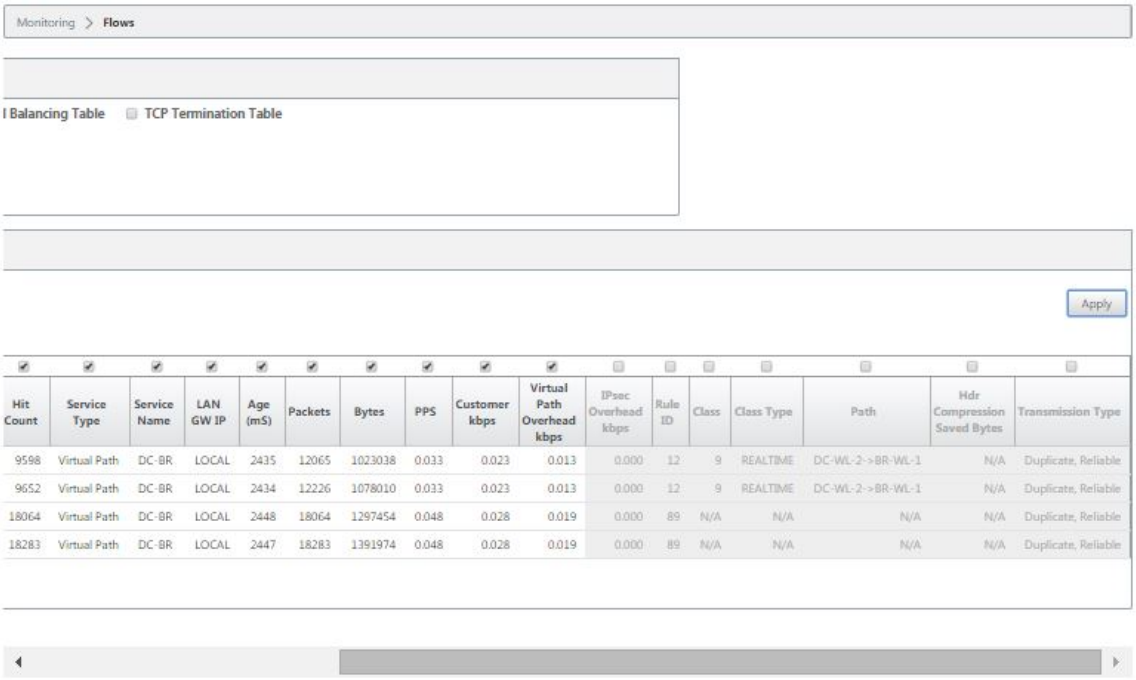
7. 单击刷新以显示筛选结果。图中显示了一个已过滤的流量页面示例，其中选择了所有流程类型。



8. （可选）选择要包括在表中的列。请执行以下操作：

9. 单击“流量数据”表右上角的“切换列”。它会显示所有取消选定的列，并在每列上方打开一个复选框，用于选择或取消选择该列。取消选定的列显示为灰色，如图所示。

> 注意
>
> 默认情况下，所有列都处于选中状态，这可能会导致表格在显示屏中被截断，从而遮盖切换列按钮。如果是这样，则表下方会显示水平滚动条。向右滑动滚动条可查看表格的截断部分并显示 切换列 按钮。如果滚动条不可用，请尝试调整浏览器窗口的宽度，直到显示滚动条为止。

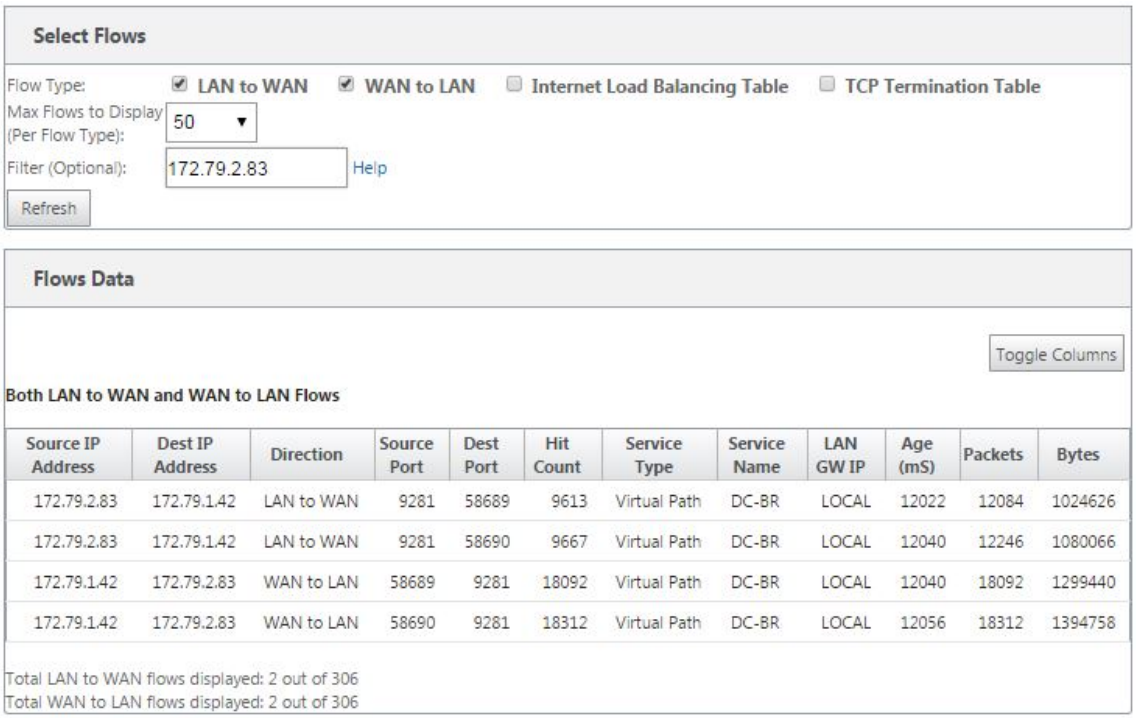


10. 单击复选框以选择或取消选择列。

- 源 **IP** 地址 -此流中数据包的源 IP 地址。
- 目标 **IP** 地址 -此流中数据包的目标 IP 地址。
- 方向 -此流中数据包的方向-局域网到广域网或广域网到局域网。
- 源端口 -此流中数据包的源端口。
- 目标端口 -此流上数据包的目标端口。
- **IPP** -此流中数据包的 IP 协议编号。
- **IP DSCP** -此流中数据包的 IP DSCP 标记设置。
- 命中次数 -搜索和找到此流的次数。
- 服务类型 -指示此流量类型是虚拟路径、Internet 还是 Intranet 流量。
- 服务名称 -虚拟路径流量使用的虚拟路径的名称。
- **LAN GW IP** -局域网网关的 IP 地址（如果已指定）。
- 存在时间 **(**毫秒**)** -自数据包在此流中分类以来的时间（以毫秒为单位）。
- 数据包 - 在流的生命周期内发送的数据包数。

- 字节 - 在流的生命周期内发送的字节数。
- **PPS** -自上次刷新以来的时间段内的每秒数据包数。
- 客户 **kbps**/虚拟路径开销 **kbps**/**IPsec** 开销 **kbps** - 自上次刷新以来的时间段内的每秒千比特数。
- 规则 **ID** -此流上的流量匹配的规则的 ID。
- 应用程序规则 **ID** -此流上的流量匹配的规则的应用程序的 ID。
- **Class** -流量正在使用的虚拟路径类的 ID。
- 类类型 -流量使用的虚拟路径类的类型（实时、交互式、批量）。
- 路径 -流量使用的路径。
- **Hdr** 压缩保存的字节 数-由于标头压缩而保存的字节数。
- 传输类型 -流量使用的传输类型。
- 应用程序 -正在使用的应用程序的名称。

11. 单击 应用（在表格右上角）。它会取消选择选项，并刷新表格以仅包含所选列。



SD-WAN Center 中的 **DPI** 应用程序

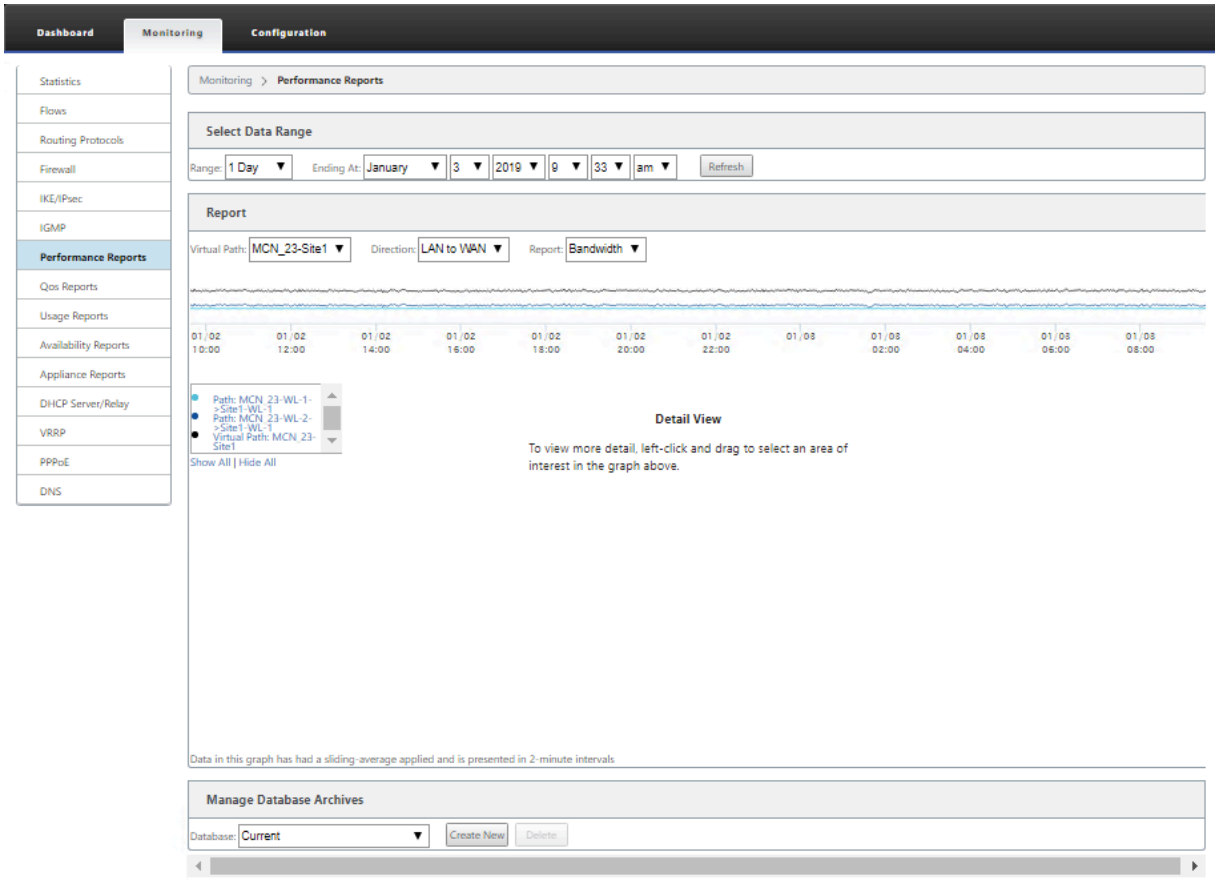
在 早期版本中，可以识别约 4,000 个应用程序，并配置为 800 个服务（550 个虚拟路径、256 个内联网服务）。存储此数据会影响整体系统性能（存储数据所需的 CPU 周期和磁盘空间）。如果支持按使用量或路径报告数据，它也会产生影响。

虽然数据路径在一分钟内提供有关收集的每个应用程序的信息，但每分钟统计数据报告确定了前 100 个应用程序，并将所有其他应用程序的汇总报告为 其他。如果网络中可跟踪应用程序的多样性高，则可能会影响数据的清晰度，特别是如果我们希望跟踪/绘制应用程序的使用情况，并且应用程序超出前 100 个限制。

查看报告

September 2, 2022

本节提供了有关使用管理 Web 界面生成和查看有关本地设备的 虚拟 WAN 报告的基本说明。设备最多可以维护 30 个归档文件，并清除包含 30 个以上条目的最旧存档文件。



> 注意
>
> 在管理 Web 界面上生成的报告仅适用于本地设备。要生成和查看虚拟广域网的报告，请使用虚拟广域网中心 Web 界面。

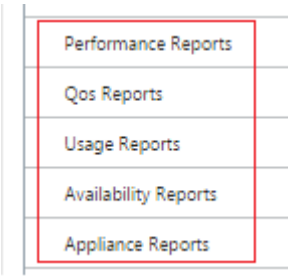
要生成和查看虚拟 WAN 报表，请执行以下操作：

1. 登录 MCN 的管理 Web 界面，然后选择 监控 选项卡。

   这将在左窗格中打开“监视”导航树。

2. 从导航树中选择报表类型。

   报表类型在导航树中列为分支，位于 流量 分支下方。



可用报表类型如下：

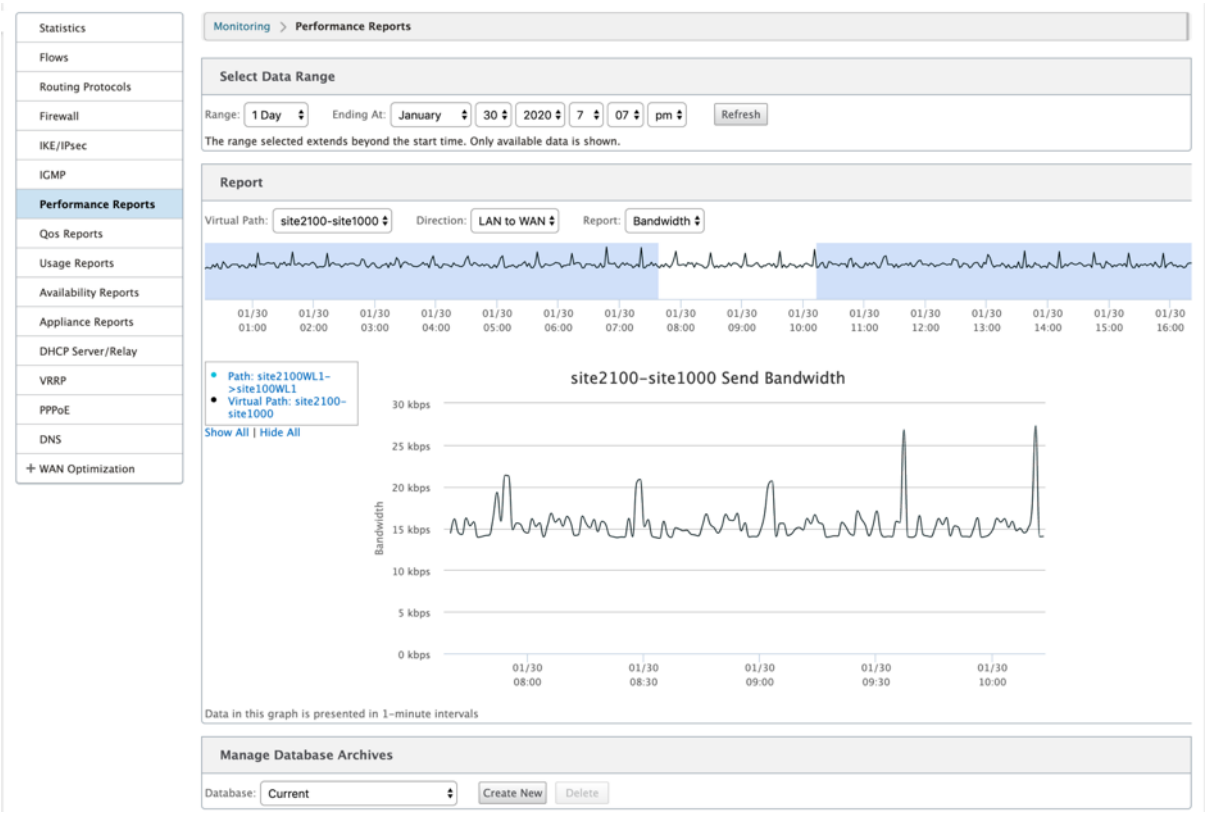
- 性能报告
- **QoS** 报告
- 使用情况报告
- 可用性报告
- 设备报告

3. 选择报告选项。

除了各种类型的报表外，对于每种报表类型，还有许多选项和筛选器用于精炼报表结果。

执行情况报告

Citrix SD-WAN 可以在站点、虚拟路径或方向（LAN 到 WAN 和 WAN 到 LAN）级别显示性能统计信息。借助 Citrix SD-WAN，您可以收集以毫秒为单位显示每条链路效率的指标。要查看更多详细信息，请左键单击并在图形线中选择路径或时间范围的特定区域。

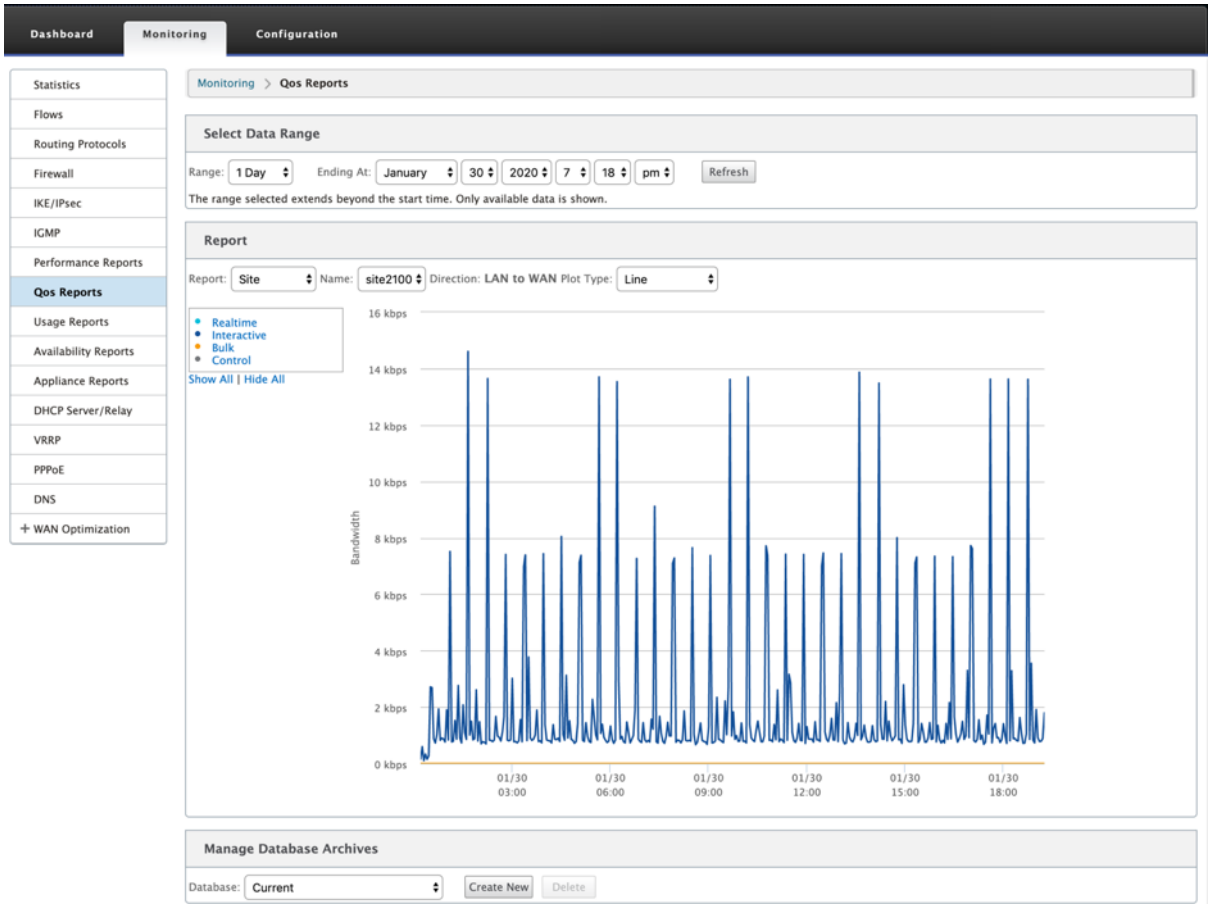


您可以根据需要使用以下字段选择数据范围以查看性能报告：

- 虚拟路径：从下拉列表中选择虚拟路径。
- 方向：根据需要选择方向（局域网到 WAN 或 WAN 到 LAN）。
- 报告：选择以下网络参数以查看报告：
  - Bandwidth（带宽）
  - 延迟
  - 抖动
  - 损失
  - 质量

QoS 报告

您可以监视应用程序 QoS 报告，例如在每个站点、WAN 链路、虚拟路径和路径级别上载、下载或丢弃的数据包或字节数。

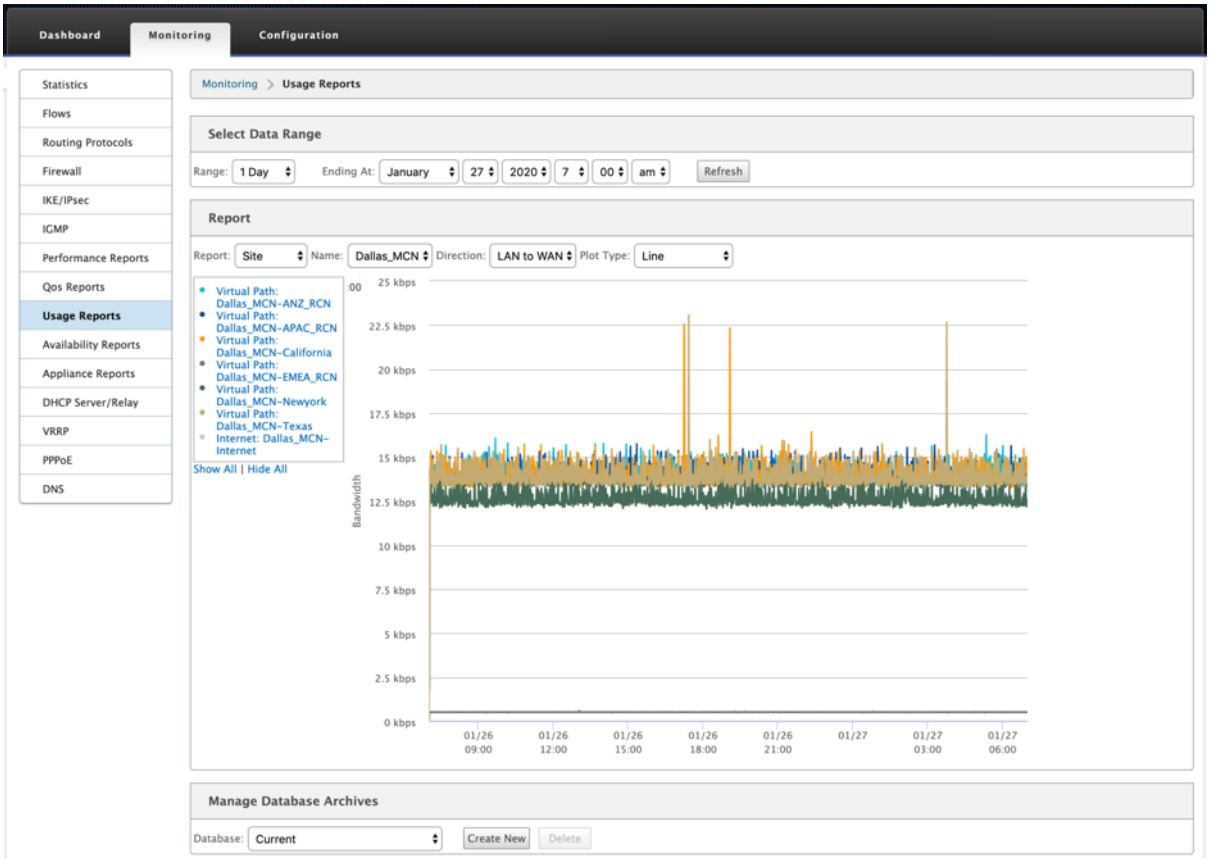


您可以查看以下指标：

- 实时：属于 Citrix SD-WAN 配置中实时类型的应用程序占用的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互式： Citrix SD-WAN 配置中属于交互类类型的应用程序消耗的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量： Citrix SD-WAN 配置中属于批量类型的应用程序消耗的带宽。这些应用程序几乎不需要人工干预，主要由系统本身处理（例如 FTP、备份操作）。
- 控制：用于传输包含路由、调度和链路统计信息的控制数据包的带宽。

使用情况报告

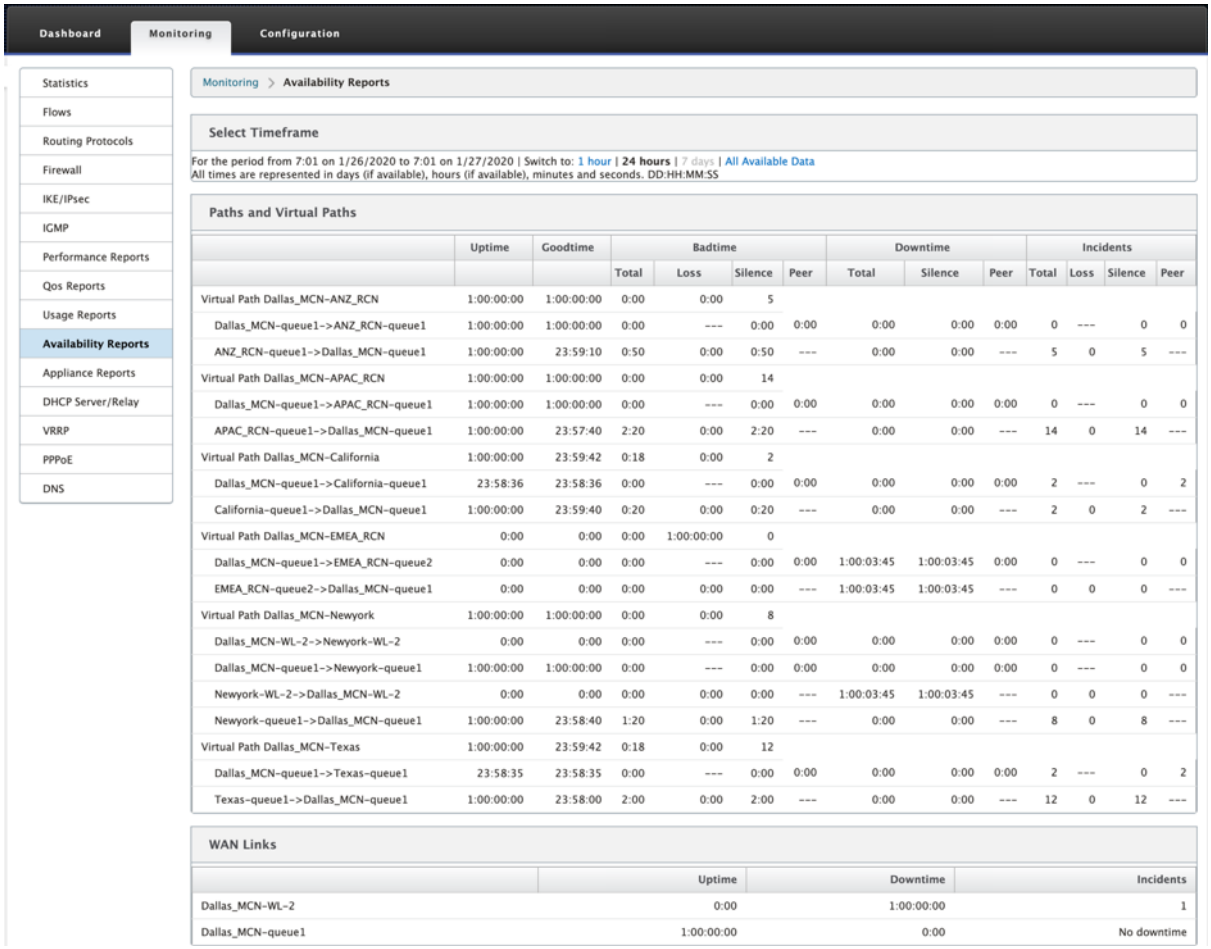
使用情况报告提供虚拟路径使用情况信息。



- 报告：从下拉列表中选择 站点 或 **WAN** 链接 以查看报告。
- 名称：从下拉列表中选择站点或 WAN 链接的名称。
- 方向：根据需要选择方向（局域网到 WAN 或 WAN 到 LAN）。
- 绘图类型：从下拉列表中选择绘图类型（线或面积）。

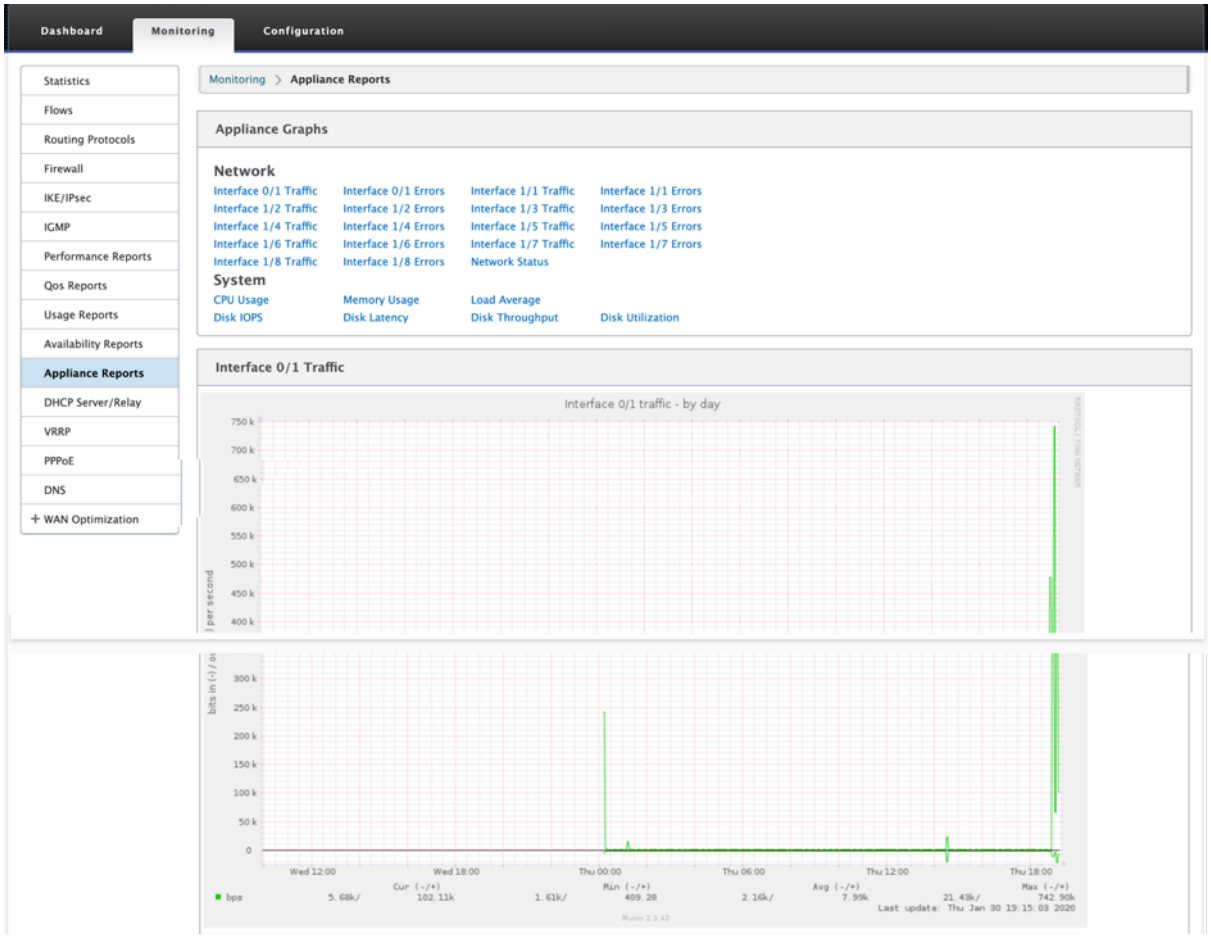
可用性报告

在此报告中，您可以查看 WAN 链路、路径和虚拟路径的可用性数据。您还可以切换到或选择特定的时间范围，例如 1 小时、24 小时和 7 天以查看可用数据。路径和虚拟路径数据以 **DD:HH:MM:SS** 格式表示。



设备报告

设备报告提供网络流量和系统使用情况报告。单击每个链接可按天、每周、每月和每年查看或监视设备图表。



查看防火墙统计信息

September 2, 2022

配置防火墙和 NAT 策略后，可以将连接、防火墙策略和 NAT 策略的统计信息作为报告查看。您可以使用各种过滤参数筛选报表。

有关配置防火墙和 NAT 策略的信息，请参阅 有状态防火墙和 NAT 支持。

要查看防火墙统计信息，请执行以下操作：

1. 导航到 监控 > 防火墙。
2. 根据需要选择、连接、筛选策略或 **NAT** 策略。
3. 根据需要设置筛选条件。
4. 单击 刷新。

连接

您可以检查防火墙策略的应用程序的统计信息。这使您能够查看与所选应用程序匹配的所有连接、它们来自何处、要去何处以及它们产生的流量。您可以查看防火墙策略如何对每个应用程序的流量进行操作。

您可以使用以下参数筛选连接统计信息：

- 应用程序-用作连接筛选条件的应用程序。
- Family-用作连接筛选条件的应用程序系列。
- IP 协议-连接使用的 IP 协议。
- 源区域-连接起源的区域。
- 目标区域-响应流量源自的区域。
- 源服务类型-连接源自的服务。
- 源服务实例-连接源自的服务实例。
- 源 IP-连接源自的 IP 地址，输入带有可选子网掩码的小数点符号。
- 源端口-连接源自的端口或端口范围。接受使用 - 字符的单个端口或一系列端口。
- 目标服务类型-响应流量源自的服务。
- 目标服务实例-响应流量源自的服务实例。
- 目标 IP-响应设备的 IP 地址，输入带有可选子网掩码的小数点符号。
- 目标端口-响应设备使用的端口或端口范围。接受使用 - 字符的单个端口或一系列端口。

筛选策略

策略允许您为流量指定操作。防火墙筛选器组使用防火墙策略模板创建，可应用于网络中的所有站点或仅应用于特定站点。

您可以查看所有筛选器策略的统计信息报告，并使用以下参数进行筛选。

- 应用程序对象-用作防火墙策略中筛选条件的应用程序对象。
- 应用程序- 用作防火墙策略中筛选条件的应用程序
- Family-用作防火墙策略中筛选条件的应用程序系列。
- IP 协议-筛选器策略匹配的 IP 协议。
- DSCP：筛选器策略匹配的 DSCP 标记。
- 筛选策略操作-当数据包匹配筛选器时策略采取的操作。
- 源服务类型-连接源自的服务。

- 源服务名称-连接源自的服务实例。
- 源 IP-连接源自的 IP 地址，输入带有可选子网掩码的小数点符号。
- 源端口-连接源自的端口或端口范围。接受使用 - 字符的单个端口或一系列端口。
- 目标服务类型-响应流量发往的服务。
- 目标服务名称-如果适用，响应流量发往的服务。
- 目标 IP-响应设备的 IP 地址，输入带有可选子网掩码的小数点符号。
- 目标端口-响应设备使用的端口或端口范围。接受使用 - 字符的单个端口或一系列端口。
- 源区域-与筛选器策略匹配的起始区域。
- 目标区域-与筛选器策略匹配的响应区域。

NAT 策略

您可以查看所有网络地址转换 (NAT) 策略的统计信息，并使用以下参数筛选报表。

- IP 协议-NAT 策略匹配的 IP 协议。
- NAT 类型-NAT 策略正在使用的 NAT 类型。
- 动态 NAT 类型-NAT 策略正在使用的动态 NAT 类型。
- 服务类型-NAT 策略使用的服务类型。
- 服务名称-NAT 策略使用的服务实例。
- 内部 IP-内部 IP 地址，输入带有可选子网掩码的小数点符号。
- 内端口-NAT 策略使用的内端口范围。接受使用 - 字符的单个端口或一系列端口。
- 外部 IP-外部 IP 地址，输入带有可选子网掩码的小数点符号。
- 外端口-NAT 策略使用的外端口范围。接受使用 - 字符的单个端口或一系列端口。

诊断

September 2, 2022

Citrix SD-WAN 诊断 实用程序提供以下选项来测试和调查连接问题：

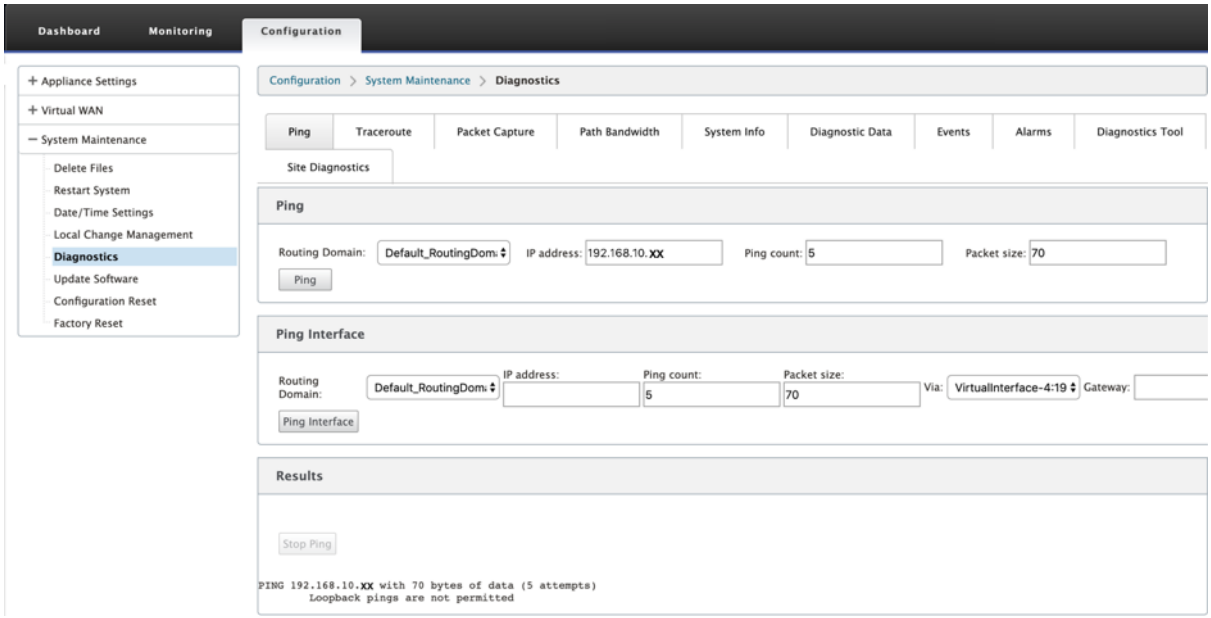
- Ping
- Traceroute
- 数据包捕获

- 路径带宽
- 系统信息
- 诊断数据
- 事件
- 警报
- 诊断工具
- 站点诊断

Citrix SD-WAN 仪表板 中的诊断选项控制数据收集。

Ping

要使用 **Ping** 选项，请导航到 配置 **>** 诊断，然后选择 **Ping**。您可以使用 Ping 检查主机可访问性和网络连接性。

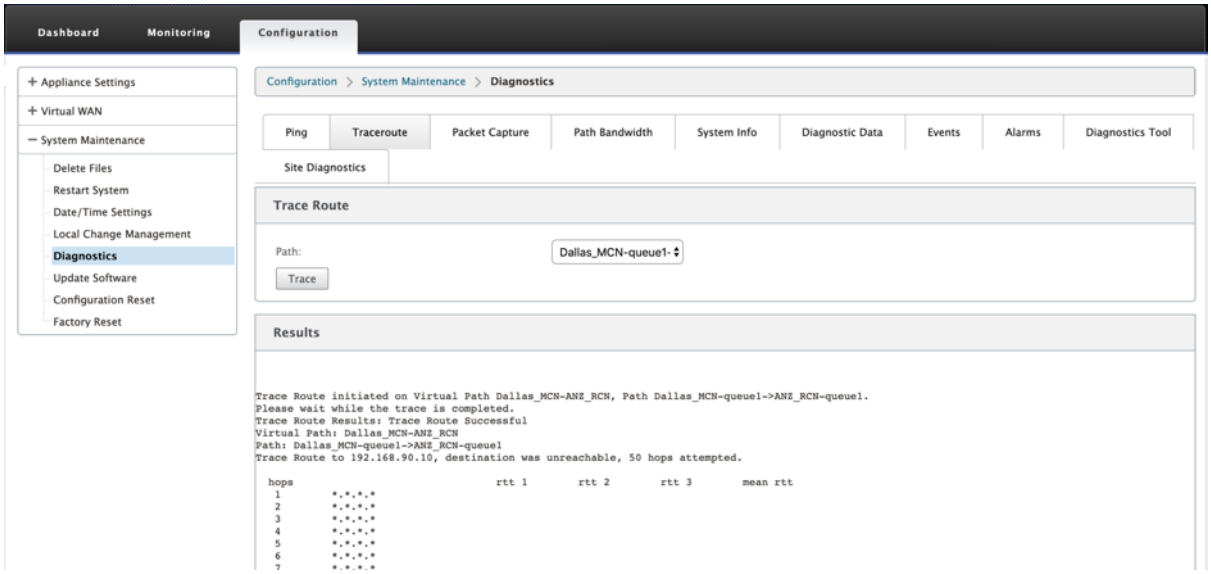


选择路由域。提供有效的 IP 地址、ping 计数次数（发送 ping 请求的次数）和数据包大小（数据字节数）。单击 停止 **Ping** 可停止正在进行的 ping 搜索。

您可以通过特定界面 ping。选择路由域并指定 IP 地址以及 ping 计数和数据包大小，然后从下拉列表中选择虚拟接口。

Traceroute

要使用 **Traceroute** 选项，请导航到 配置 **>** 展开系统维护 **>** 诊断，然后选择 **Traceroute**。

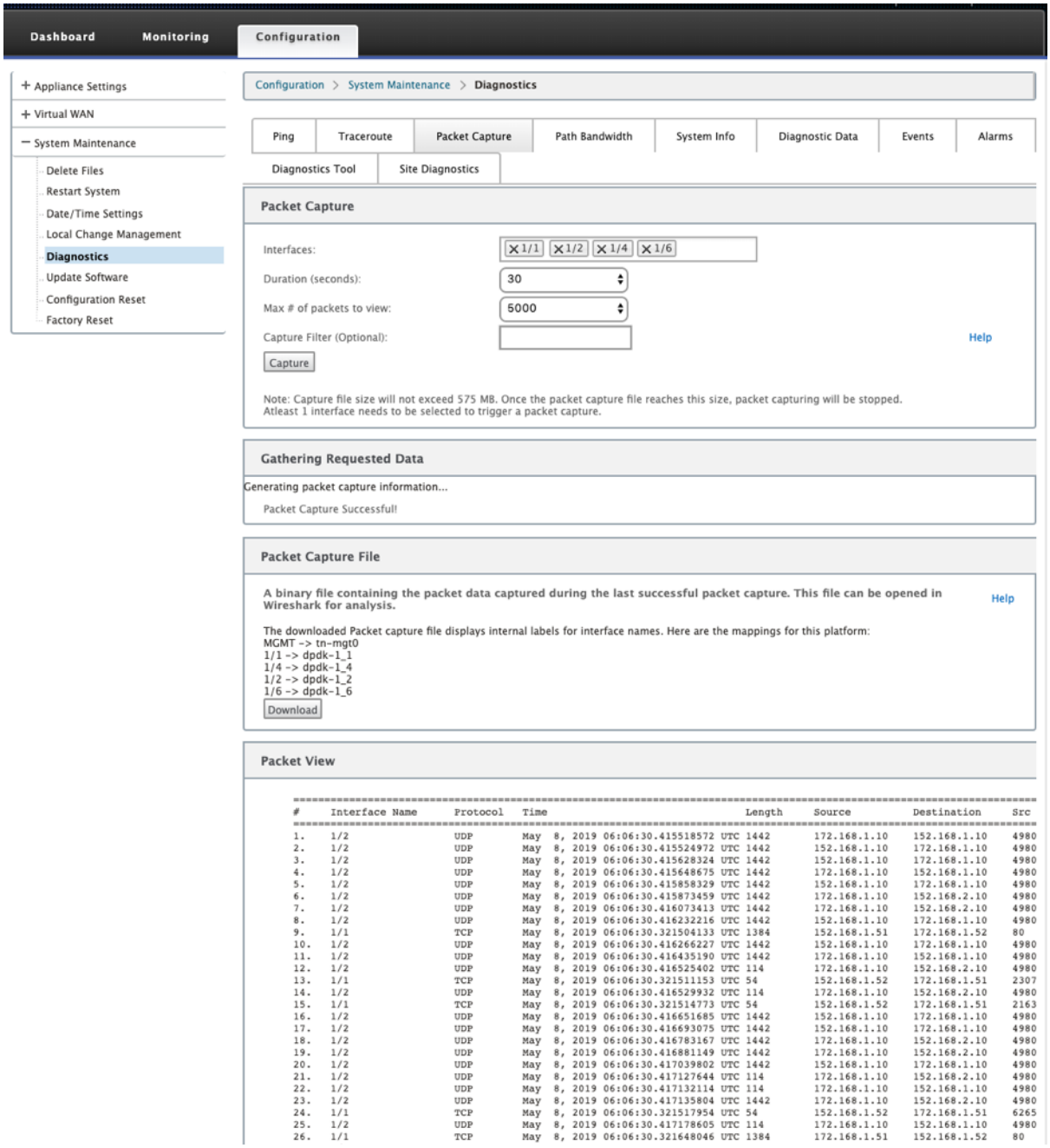


Traceroute 有助于发现并显示通往远程服务器的路径或路由。使用 **Traceroute** 选项作为调试工具来检测网络中的故障点。

从下拉列表中选择一个路径，然后单击 **Trace**。您可以在“结果”部分下查看详细信息。

数据包捕获

您可以使用“数据 包捕获”选项拦截通过选定站点中存在的选定活动接口的实时数据包。数据包捕获可帮助您分析和解决网络问题。



为数据包捕获操作提供以下输入：

- 接口 -活动接口可用于 SD-WAN 设备的数据包捕获。从下拉列表中选择接口或添加接口。至少需要选择一个接口来触发数据包捕获。

  > 注意：
  >
  > 能够一次在所有接口上运行数据包捕获，有助于加快故障排除任务。

- 持续时间（秒）-必须捕获数据的持续时间（以秒为单位）。
- 要查看的最大数据包数-要 在数据包捕获结果中查看的数据包的最大限制。

- 捕获过滤器（可选） -可选的捕获过滤器字段接受用于确定捕获哪些数据包的过滤器字符串。数据包与过滤字符串相比较，如果比较结果为 true，则捕获数据包。如果过滤器为空，则将捕获所有数据包。有关详细信息，请参阅 捕获过滤器。

下面是此捕获过滤器的一些示例：

- 以太原子\ **ARP** -仅捕获 ARP 数据包
- 以太原型\ **IP** -仅捕获 IPv4 数据包
- **VLAN 100** -仅捕获 VLAN 为 100 的数据包
- 主机 **10.40.10.20** -仅捕获进出地址为 10.40.10.20 的主机的 IPv4 数据包
- **Net 10.40.10.0** 掩码 **255.255.255.0** -仅捕获 10.40.10.0/24 子网中的 IPv4 数据包
- **IP** 原型\ **TCP** -仅捕获 IPv4/TCP 数据包
- 端口 **80** -仅捕获进出端口 80 的 IP 数据包
- 端口范围 **20**—**30** -仅捕获进出端口 20 至 30 的 IP 数据包

> 注意
>
> 捕获文件的最大大小限制为 575 MB。数据包捕获文件达到此大小时，将停止数据包捕获。

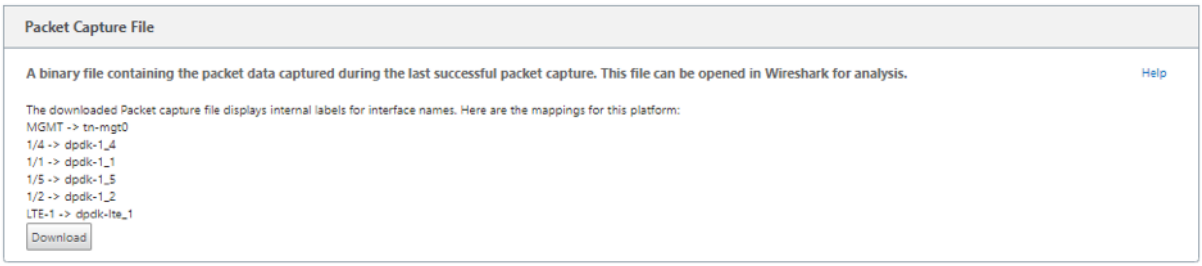
单击 捕获 查看数据包捕获结果。您还可以下载包含上次成功捕获数据包期间捕获的数据包数据的二进制文件。

收集所要求的数据

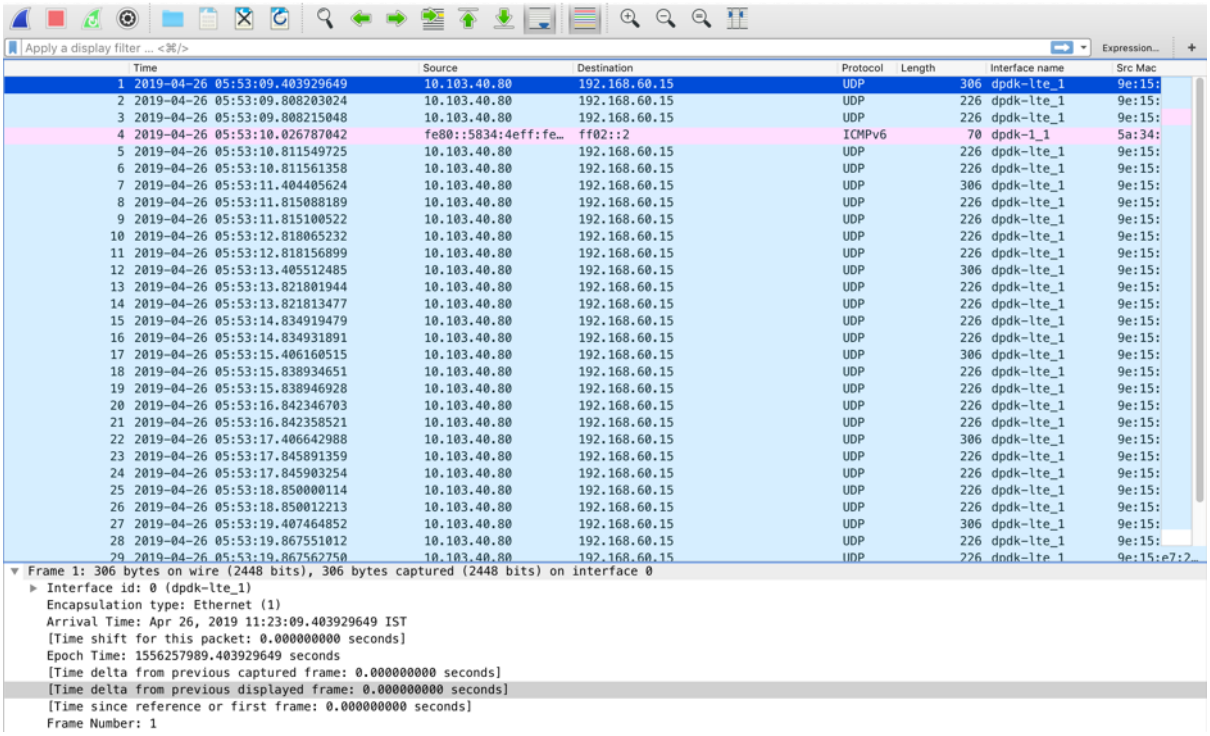
您可以在此表中查看生成数据包捕获信息的状态（数据包捕获是成功还是没有数据包捕获）。

数据包捕获文件

在上次成功捕获数据包期间将数据包作为二进制数据捕获。您可以下载二进制文件以脱机分析数据包信息。与 GUI 界面相比，下载文件中的接口名称不同。要查看内部界面映射，请单击 帮助 选项。



您需要 **Wireshark** 软件 2.4.13 版或更高版本才能打开和读取二进制文件。

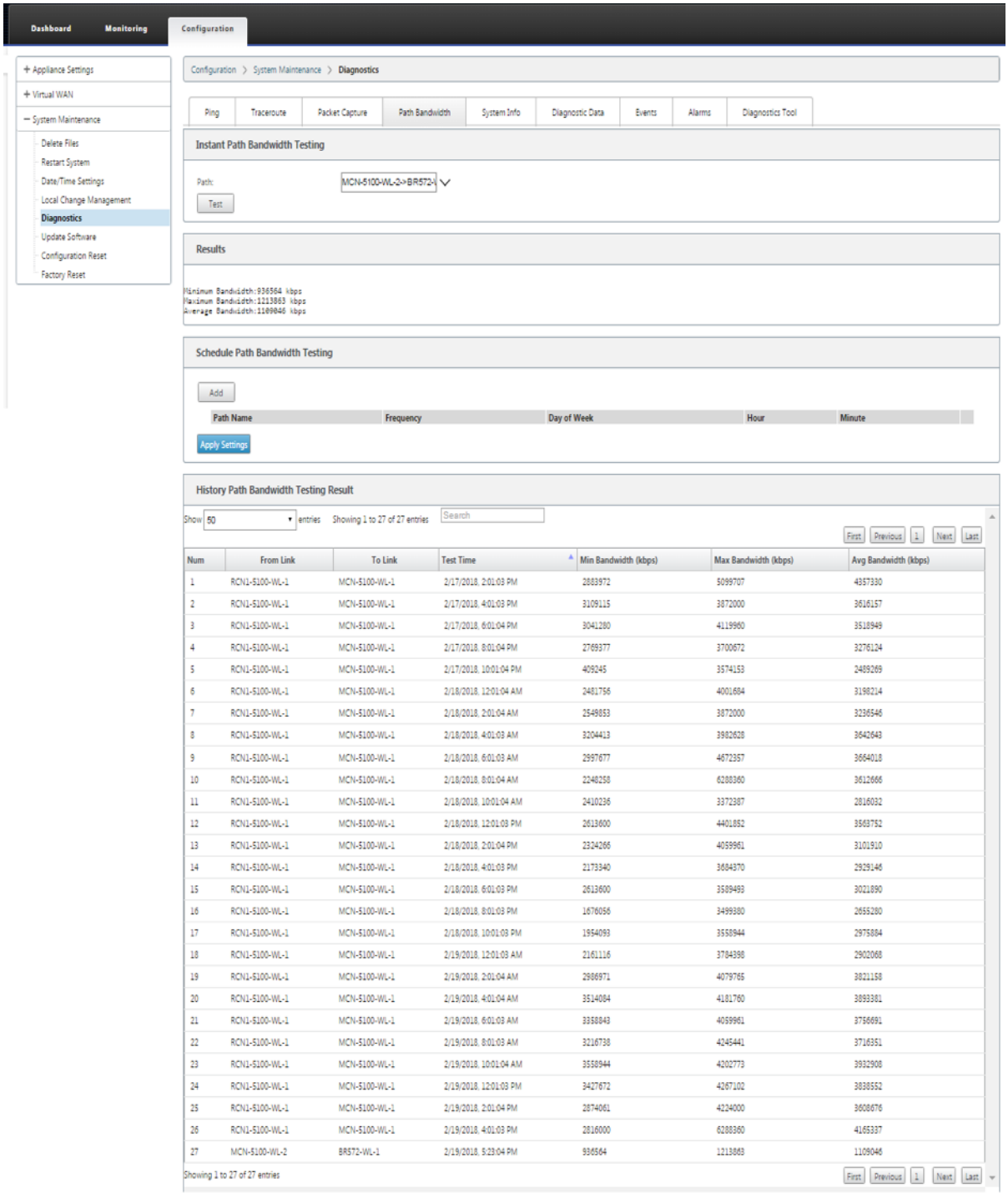


数据包视图

如果数据包捕获文件大小更大，则完成数据包视图的渲染过程需要更多的时间。在这种情况下，建议下载文件并使用 **Wireshark** 进行分析，而不是依赖 **Packet View** 结果。

路径带宽

要使用 路径带宽 功能，请导航到 配置 **>** 展开系统维护 **>** 诊断，然后选择 路径带宽。



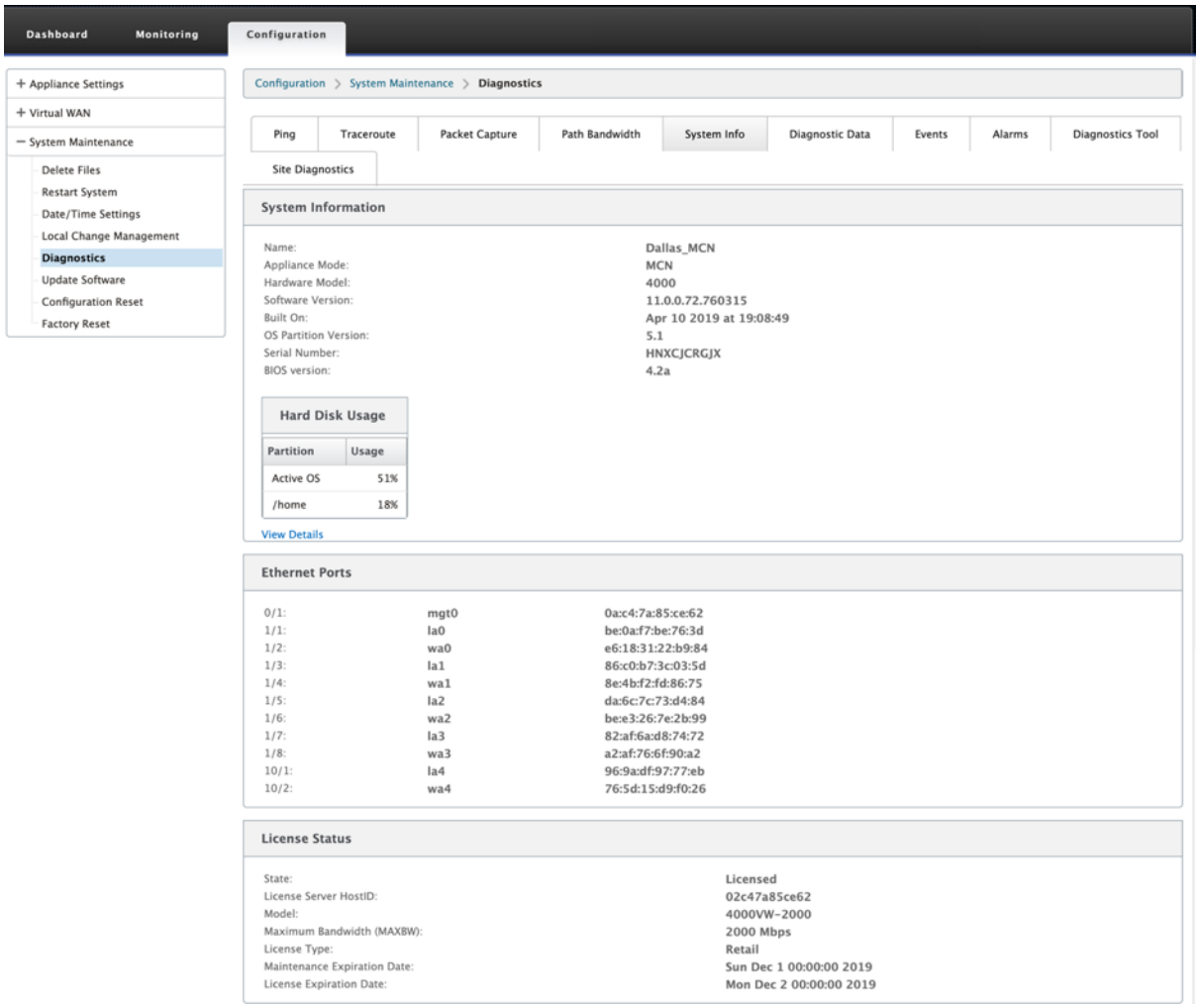
主动带宽测试使您能够通过公共 Internet WAN 链接发出即时路径带宽测试，或安排公共 Internet WAN 链接带宽测试在特定时间定期完成。

路径带宽 功能可用于演示在新安装和现有安装过程中两个位置之间的可用带宽量。路径带宽中的值表示可能的最大带宽。要获得准确的允许带宽，请导航到 配置 > 系统维护 > 诊断 > 站点诊断 > 带宽测试。有关更多信息，请参阅 主动带宽测试。

系统信息

系统信息 页面提供系统信息、以太网端口详细信息和许可证状态。

要查看系统信息，请导航到 配置 **>** 展开系统维护 **>** 诊断，然后选择 系统信息。

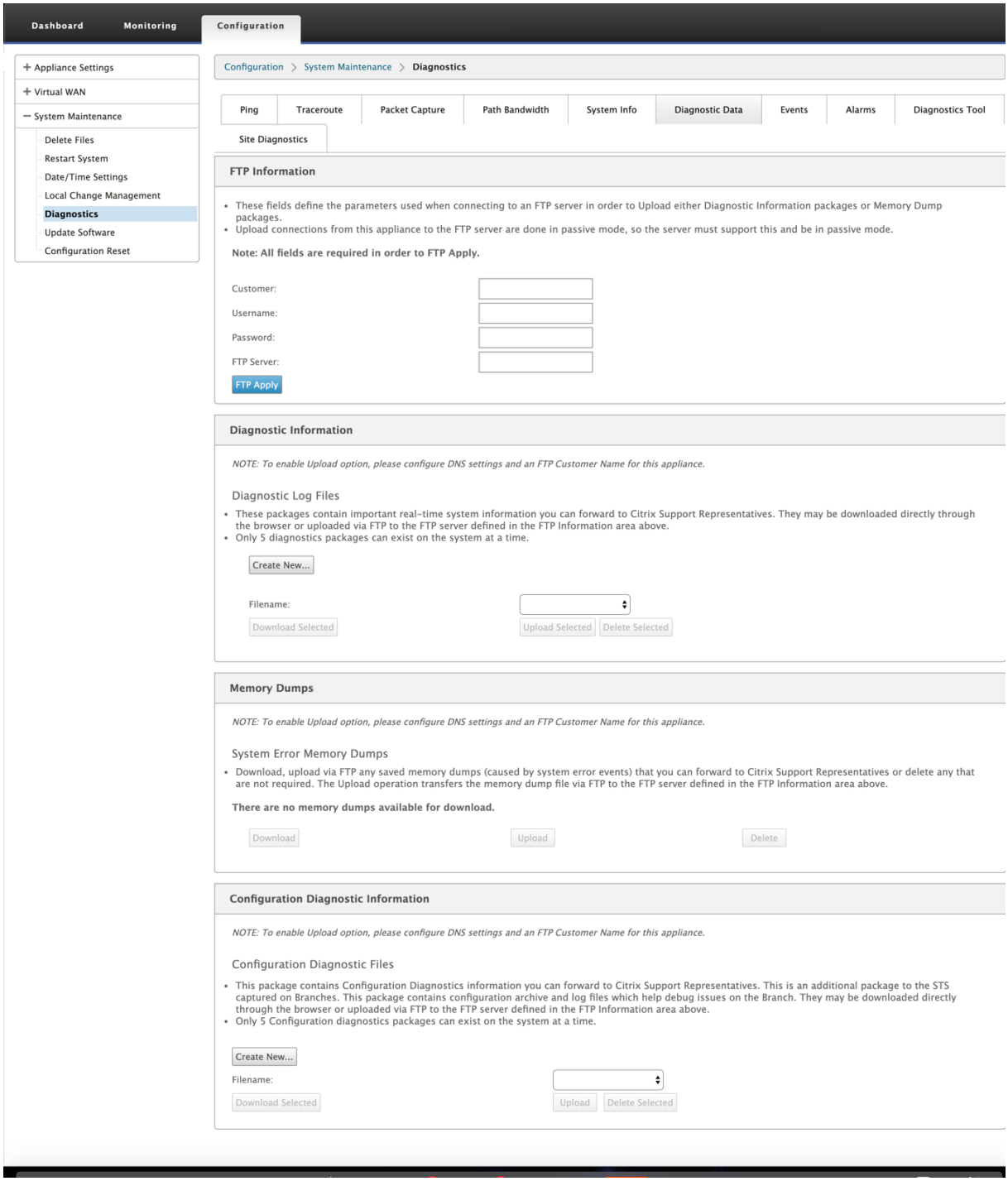


系 统信息 列出了所有未设置为默认值的参数。此信息为只读信息。如果怀疑存在某种错误配置，则由支持部门使用。当您报告问题时，系统可能会要求您检查此页面上的一个或多个值。

诊断数据

诊断数据 允许您生成诊断数据包以供 Citrix 支持团队进行分析。您可以下载 诊断日志文件 包并将其共享给 Citrix 支持团队。

要查看 诊断数据，请导航到 配置 **>** 展开系统维护 **>** 诊 断，然后选择 诊断数据。



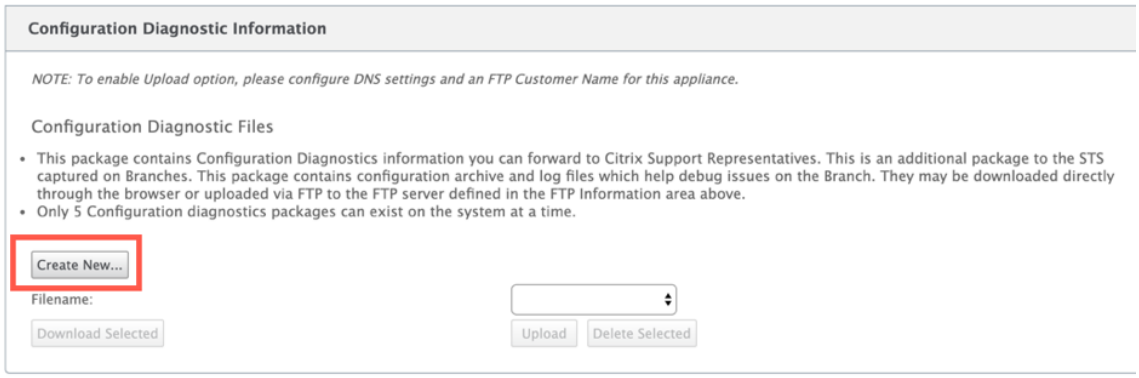
诊断数据 包括：

- **FTP** 信息—提供 FTP 参数详细信息，然后单击 **FTP** 应用。连接 FTP 服务器以上载诊断信息包所需的 FTP 信息。
- 诊断信息—诊断日志文件包包含可通过浏览器下载或通过 FTP 上传到 FTP 服务器的实时系统信息。

> 注意：
>
> 系统一次只能存在五个诊断软件包。

- 配置诊断信息 -在 Citrix SD-WAN 11.0 版本中，为分支收集的诊断信息中将无法使用网络配置文件。对于任何支持案例，请从分支连接到的控制节点提供分支的诊断信息和配置诊断信息。

  要从控制节点 GUI 收集配置诊断信息，请导航到 配置 **>** 系统维护 **>** 诊断 **>** 诊断数据 > 在 配置诊断信息下，单击 新建。

  完成 配置诊断信息 创建后，单击 下载所选 文件并将此文件提供给 Citrix 支持人员，或使用同一页面中提供的 FTP 应用操作来 FTP 此文件。

- 内存转储—您可以下载或上载系统错误内存转储文件，并与 Citrix 支持团队共享。如果不需要，您也可以删除这些文件。

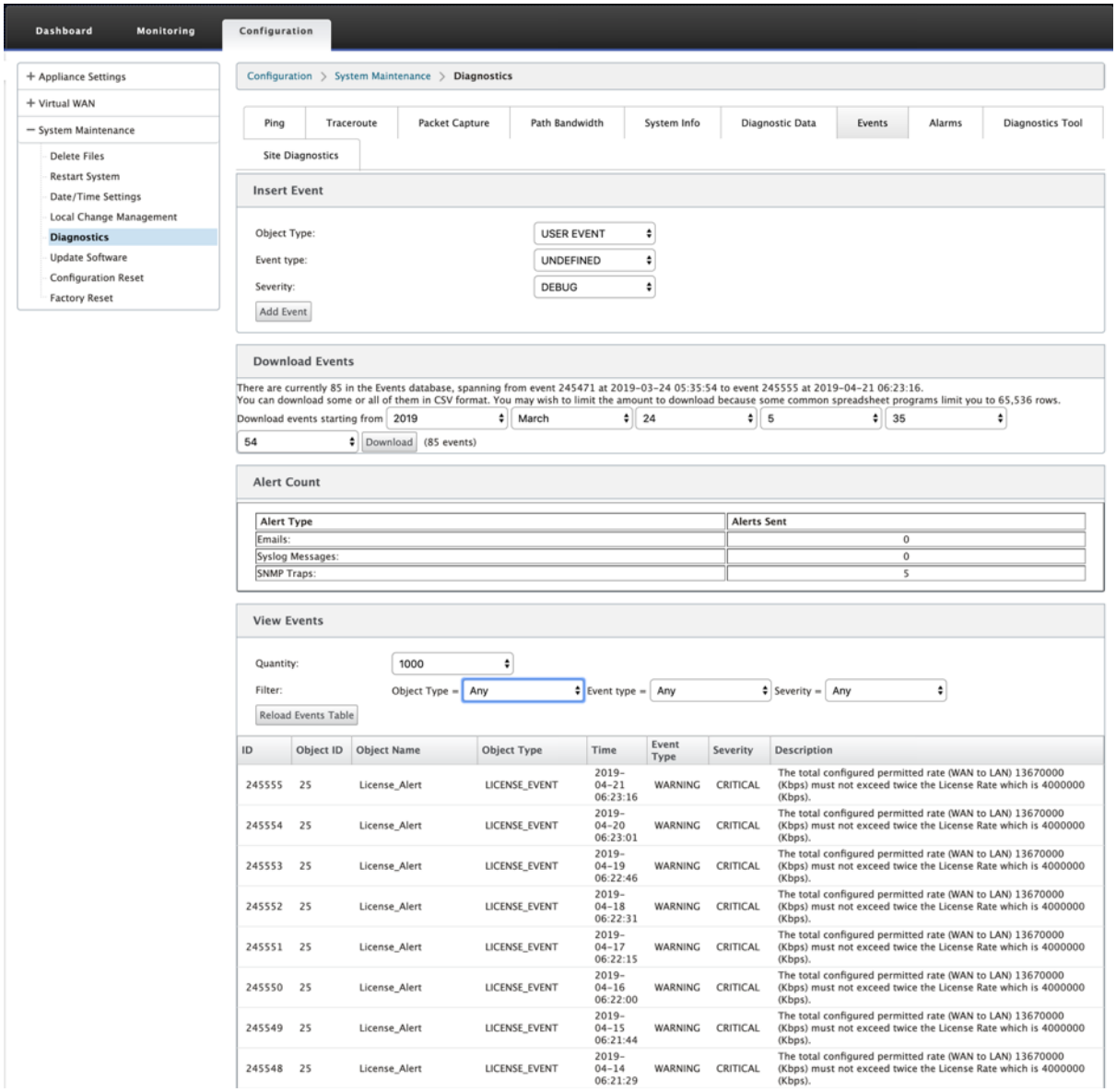
  > 注意：
  >
  > 默认情况下，上传 选项处于禁用模式。要启用它，请为此设备配置 **DNS** 设置和 **FTP** 客户名称。

事件

使用 事件 功能添加、监控和管理生成的事件。它有助于实时识别事件，帮助您立即解决问题并保持 Citrix SD-WAN 设备有效运行。您可以下载 CSV 格式的事件。

要添加事件，请从下拉列表中选择对象类型、事件类型和严重性，然后单击 添加事件。

要查看 事件，请导航到 配置 展开 系统维护 **>** 诊断，然后选择 事件。



您可以将 Citrix SD-WAN 配置为针对电子邮件、**SNMP** 陷阱或系统日志消息等不同事件类型发送事件通知。

配置了电子邮件、SNMP 和 syslog 通知设置后，您可以选择不同事件类型的严重性，并选择模式（电子邮件、SNMP、syslog）来发送事件通知。

对于等于或高于事件类型的指定严重级别的事件，将生成通知。

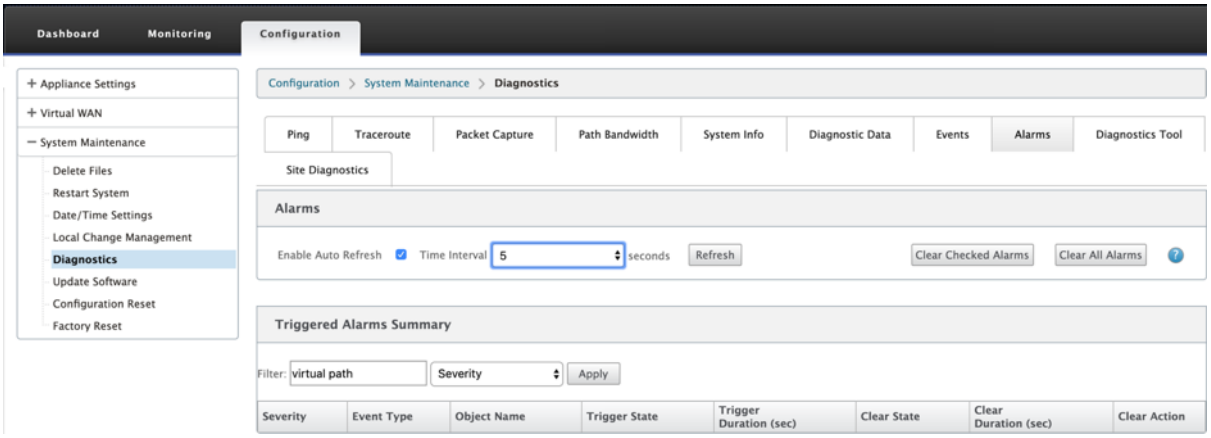
您可以在“查看事件”表格下 查看事件 详细信息。活动详情包括以下信息。

- **ID** —事件 ID。
- 对象 **ID** -生成事件的对象的 ID。
- 对象名称 -生成事件的对象的名称。
- 对象类型—生成事件的对象的类型。
- 时间—生成事件的时间。

- 事件类型—事件发生时对象的状态。
- 严重性—事件的严重性级别。
- 说明—事件的文本说明。

警报

您可以查看并清除触发的警报。要查看 警报，请导航到 配置 **>** 展开系统维护 **>** 诊断，然后选择 警报。



选择要清除的警报，然后单击 清除已选中的警报 或单击 清除所有警报 以清除所有警报。

您可以查看所有触发警报的以下摘要：

- 严重性—严重性显示在触发或清除警报时发送的警报中以及触发的警报摘要中。
- 事件类型—SD-WAN 设备可以触发网络中特定子系统或对象的警报。这些警报称为事件类型。
- 对象名称—生成事件的对象的名称。
- 触发器状态—触发事件类型警报的事件状态。
- 触发持续时间 (秒) —以秒为单位的持续时间决定设备触发警报的速度。
- 清除状态—触发警报后清除事件类型警报的事件状态。
- 清除持续时间 (秒) —以秒为单位的持续时间决定在清除警报之前需要等待多长时间。
- 清除操作—清除警报时采取的操作。

诊断工具

诊断工具 用于生成测试流量，使您能够对可能导致以下情况的网络问题进行故障排除：

- 频繁地改变路径状态从好到坏。
- 应用程序性能差。
- 更高的数据包丢失

大多数情况下，这些问题是由于在防火墙和路由器上配置的速率限制、不正确的带宽设置、低链路速度、网络提供商设置的优先级队列等。诊断工具允许您识别此类问题的根本原因并对其进行故障排除。

诊断工具消除了对第三方工具（如 iPerf）的依赖性，该工具必须手动安装在数据中心和分支主机上。它可以更好地控制发送的诊断流量的类型、诊断流量的流向以及诊断流量的路径。

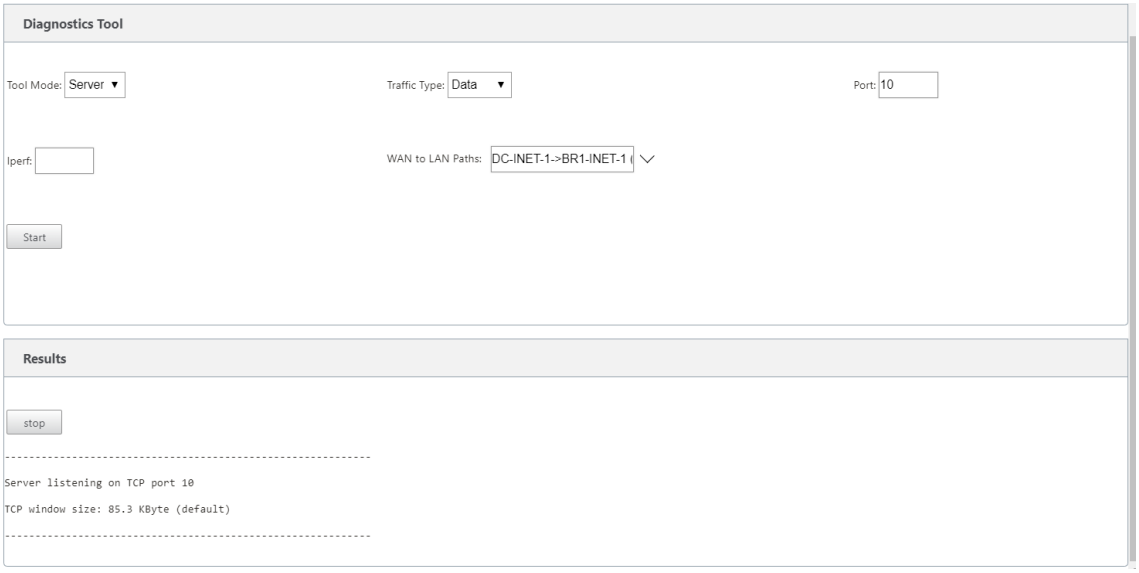
诊断工具允许生成以下两种类型的流量：

- 控制：在没有对数据包应用 QoS/ 调度的情况下生成流量。因此，数据包将通过 UI 中选定的路径发送，即使路径当时不是最佳路径。此流量用于测试特定路径，并帮助识别 ISP 相关问题。您还可以使用此选项来确定所选路径的带宽。
- 数据：使用 SD-WAN 流量处理模拟从主机生成的流量。由于 QoS/调度应用于数据包，因此数据包将通过可用的最佳路径发送。如果启用了负载平衡，则通过多个路径发送流量。此流量用于解决 QoS/排定程序相关问题。

> 注意
>
> 要在路径上运行诊断测试，必须在路径两端的设备上启动测试。作为一台设备上的服务器和另一台设备上的客户端启动诊断测试。

要使用诊断工具：

1. 在两台设备上，单击 配置 > 系统维护 > 诊断 > 诊断工具。



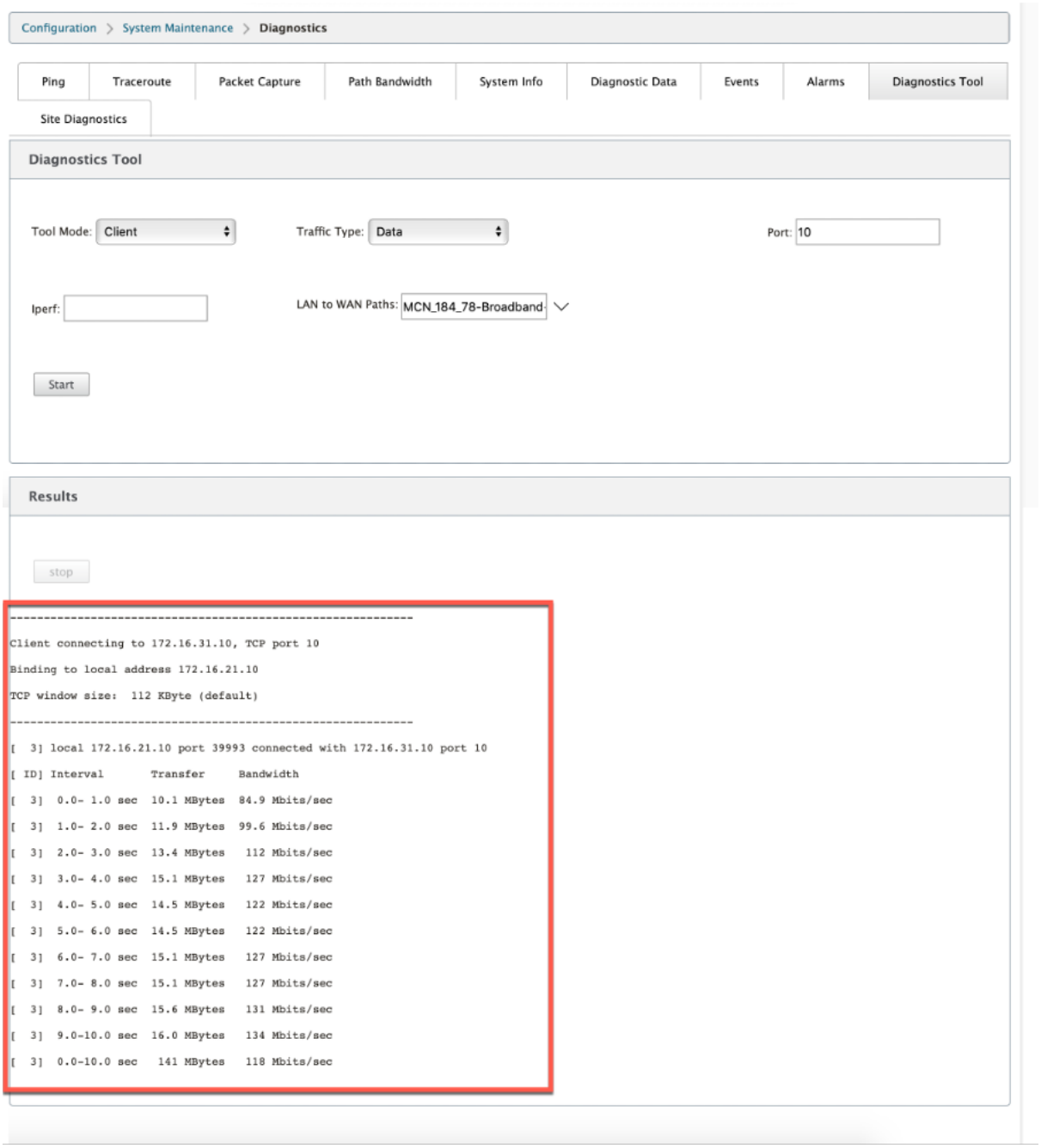
2. 在“工具模式”字段中，选择一台设备上的 服务器，然后选择位于所选路径远程端的设备上的 客户 端。
3. 在“流量类型”字段中，选择诊断流量的类型，即“控制”或“数据”。在两个设备上选择相同的流量类型。
4. 在“端口”字段中，指定发送诊断流量的 **TCP /UDP** 端口号。在两个设备上指定相同的端口号。
5. 在 **Iperf** 字段中，指定 IPPERF 命令行选项（如果有）。

> 注意
>
> 您无需指定以下 iPerf 命令行选项：
>
> - -c：诊断工具添加客户端模式选项。

- -s：服务器模式选项由诊断工具添加。
- -B: 将 iPerf 绑定到特定的 IP/接口是由诊断工具完成的，具体取决于所选路径。
  - -p：端口号在诊断工具中提供。
- -i：输出间隔（以秒为单位）。
- -t：测试的总持续时间（以秒为单位）。

6. 选择要发送诊断流量的 WAN 到 LAN 路径。在两个设备上选择相同的路径。
7. 在两台设备上单击“开始”。

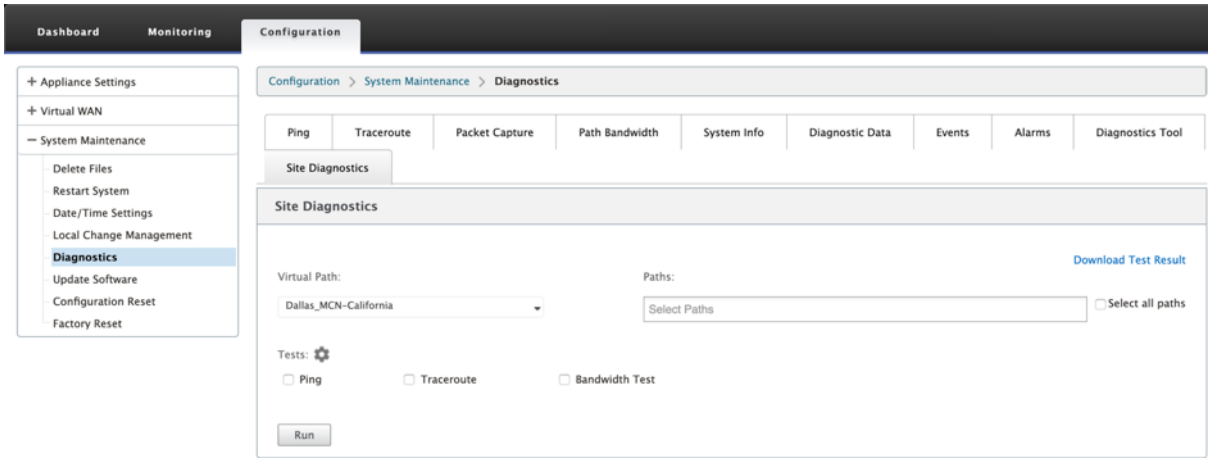
结果将显示所选设备的模式（客户端或服务器）以及运行测试的 TCP 或 UDP 端口。它会定期显示在指定时间间隔内传输的数据和占用的带宽，直到达到测试的总持续时间。



站点诊断

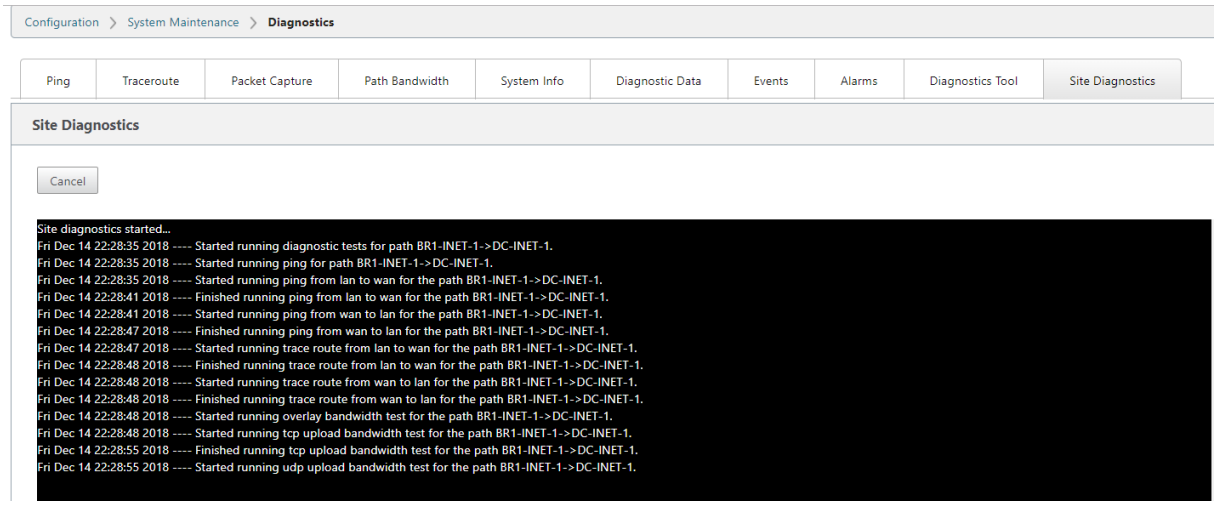
您可以对在 Citrix SD-WAN 网络中的不同站点配置的 WAN 链接测试带宽使用情况、ping 和执行 traceroute。它提供的信息有助于对现有配置中的问题进行故障排除。

要使用 站点诊断，请导航到 配置 展开 系统维护 **>** 诊断，然后选择 诊断工具。



结果区显示以下内容：

- 接口状态：提供接口名称、与接口关联的防火墙区域数、VLAN ID 及其关联端口。
- 路径状态：提供目标专用 IP、网关 IP、目标公用 IP、合作伙伴 IP、合作伙伴公用 IP 地址的详细信息。它还显示网关 ARP 和路径 MTU 的状态。
- **Ping** 结果：提供 ping 的方向、状态、计数（包括尝试次数和失败次数）和 RTT。
- **Traceroute Result**：提供跳数的方向、状态、跳数、IP 地址或 RTT。
- 带宽结果：提供 TCP 和 UDP 的状态以及覆盖和底层网络使用的带宽（以 kbps 为单位）。与 UDP 相比，TCP 使用的带宽更多，因为 UDP 是基于带宽的，因此只使用配置的带宽。TCP 是一种提升协议；根据底层网络配置，与配置的带宽相比，使用情况可能会报告更高的带宽。



改进路径映射和带宽使用情况

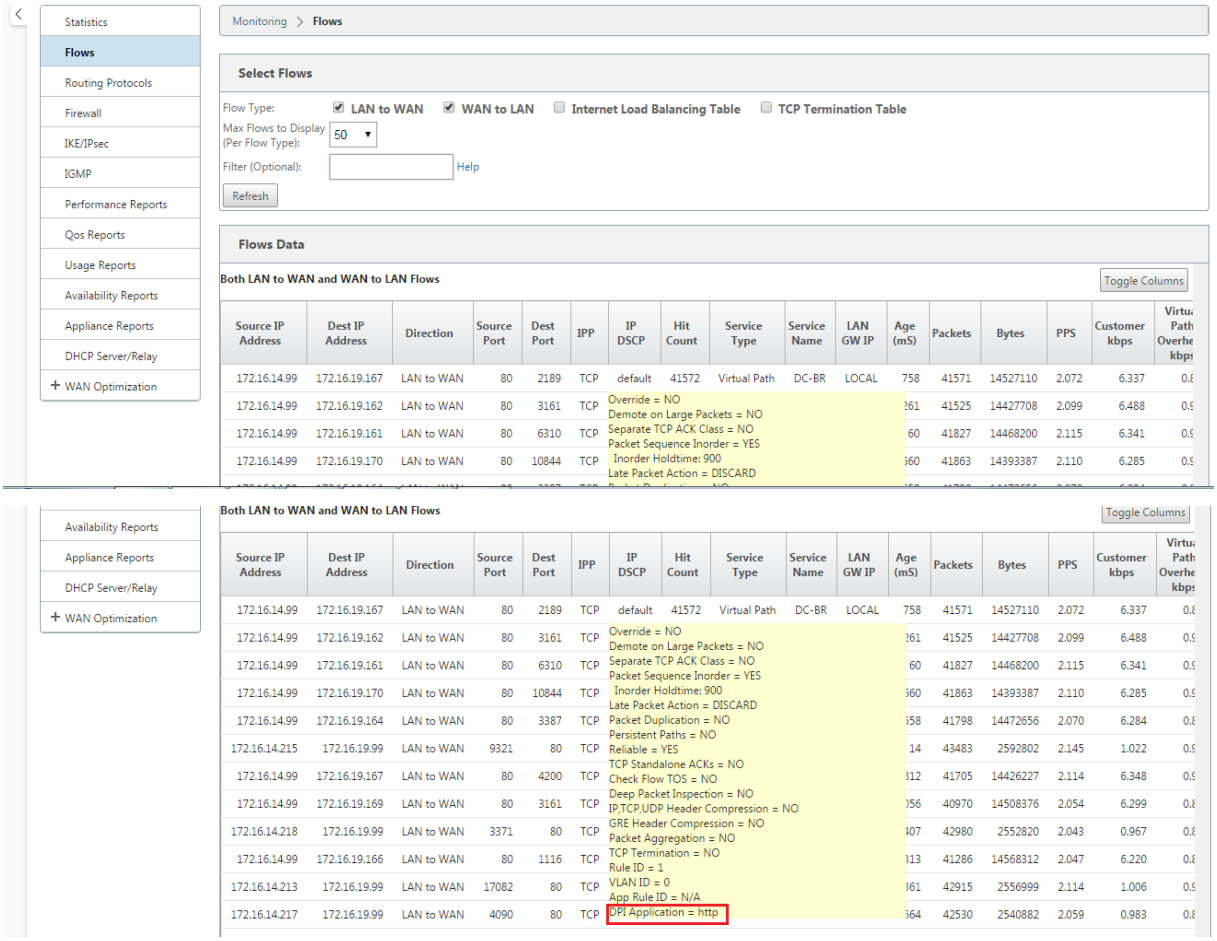
September 2, 2022

路径映射和带宽使用增强功能在 监视 选项卡中实现，以显示流量。例如，当只有一个虚拟路径为网络连接提供服务时，如果该虚拟路径变为非活动状态，则会选择一个新的最佳路径，初始路径将成为最后一个最佳路径。当对带宽的需求较少且只选择一个路径时，会实现此方案

当多个虚拟路径提供连接时，您会注意到一个当前最佳路径和下一个最佳路径（如果可用）。如果只存在一个路径来处理流量，假设有两个以上路径处理流量，并且路径表使用两个路径更新，则 SD-WAN 流量 GUI 中的监视选项卡将显示当前最佳路径作为第一个路径，下一个逗号分隔的路径作为最后一个最佳路径。当需要具有带宽需求的更多路径时，会实现此方案。

在 **SD-WAN GUI** 中监视 **DPI** 应用程序信息

监视流程上的 DPI 应用程序对象名称存储并显示在 SD-WAN GUI 监视 -> 流 程页面中。将显示一个工具提示来标识 DPI 应用程序。



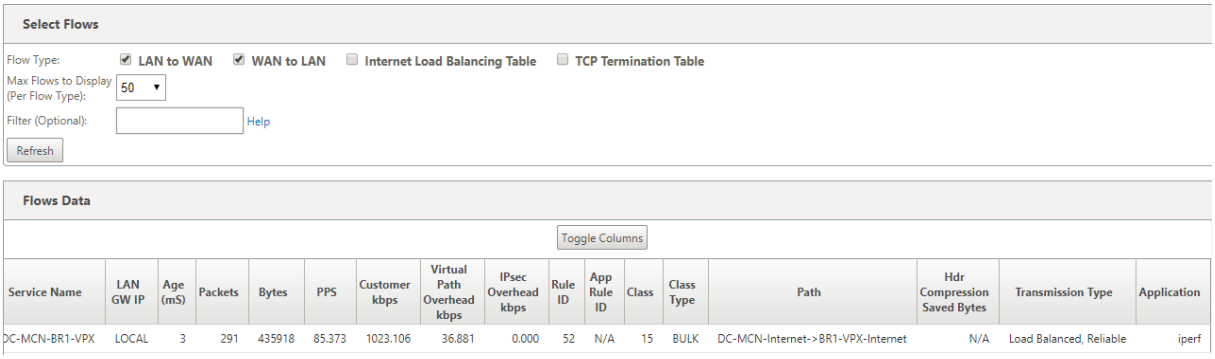
SD-WAN GUI 中交通流量的路径信息监视

根据要求带宽的传入流量速率，可能需要一个或多个路径来处理流量。

要确定路径映射的执行方式，请查看以下方案：

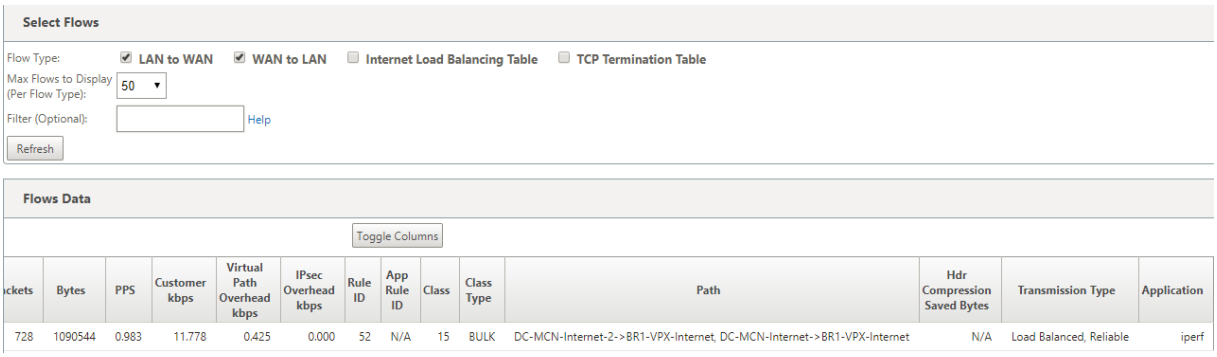
负载平衡传输模式：

下图说明了启动流量且所有路径均良好的情况，选择一条最佳路径，因为带宽需求足以满足一条路径。您注意到只选择了一个路径 **DC-MCN-Internet** -> **BR1-VPX-Internet**，并且传输类型显示为负载平衡。



下图说明了流量何时流动以及路径的 WAN 属性降级，您注意到选择了一个新路径来处理流量而不中断。在这种情况下，路径映射功能允许您指示当前处理流量的最佳路径是 **DC-MCN-Internet2 -> BR1-VPX-Internet**，处理流量的最后一个最佳路径是 **DC-MCN-Internet -> BR1-VPX-Internet**。

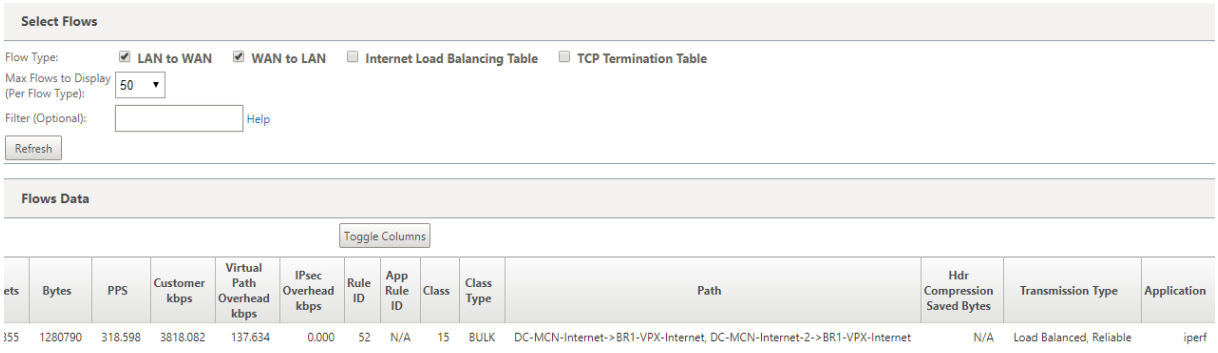
此示例中最后一个最佳路径是一个指示器，指示哪个路径之前为连接提供服务。



下图显示，当流量处于持续状态时，由于带宽需求而选择了多个路径进行流量处理时，如下所示，发送流量时会选择多个路径。与上述情况不同，这里可能有两个以上的路径也提供流量服务，但在 GUI 中只显示当前服务流量的两个最佳路径。

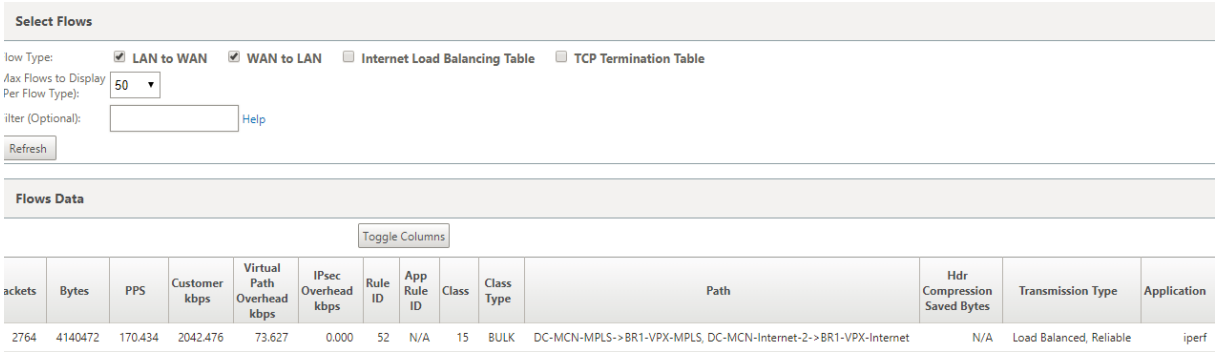
观察 **DC-MCN-Internet->BR1-VPX-Internet**、**DC-MCN-Internet2->BR1-VPX-Internet** 是流量数据表中显示的两条路径。

> 注意
>
> 如上所示，只显示流表中最多两个路径。



下图说明了当流量仍在流动时，如果 WAN 属性中的当前最佳路径 **DC-MCN-Internet->BR1-VPX-Internet** 在 WAN 属性中不可用/不活动/降级，则当前选择的最佳路径将首先出现在流量数据表的路径部分中，然后是在为流量提供服务的最后一条最佳路径前进。

由于 **DC-MCN-Internet->BR1-VPX-Internet** 不再是最好的，因此系统选择了一条新的当前最佳路径作为 **DC-MCN-MPLS->BR1-VPX-MPLS**，与当前最佳路径一起主动提供连接的最后一个最佳路径是 **DC-MCN-Internet2->BR1-VPX-Internet** 因为两者都是满足当前带宽的流量需求所必需的。



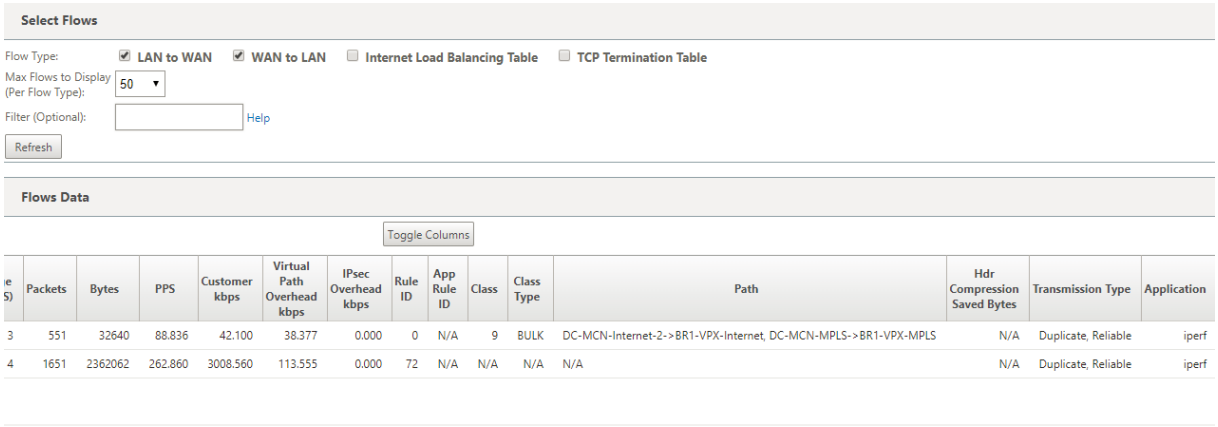
重复发送模式

通用数据包复制模式可确保最初采用两个路径来处理同一连接的数据包，从而通过在两个单独的路径上复制数据包来确保可靠的传递。

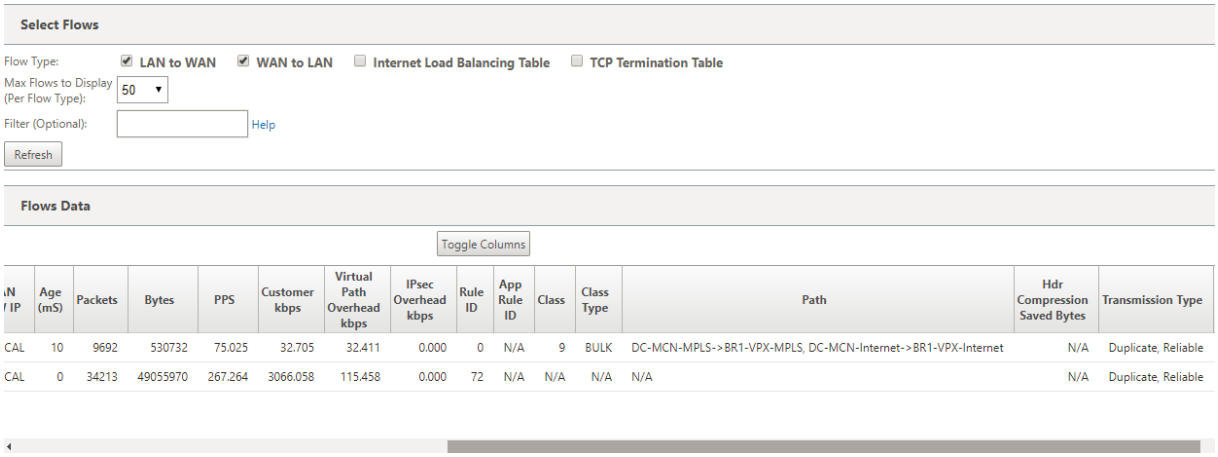
对于路径映射，您会注意到，只要存在两个路径来通过复制来处理流，在流表的路径部分中采用两个路径。

下图说明了 wen 流量正在流动，可以注意到有两条路径正在处理流量。与任何其他模式不同，即使流量需要较少的带宽（只能由一个路径提供），此模式将始终在两个路径上复制流量，以实现可靠的应用程序交付。

您会注意到在下图中，流量数据表的路径部分中有两条路径：**DC-MCN-Internet2->BR-VPX-Internet**、**DC-MCN-MPLS->BR1-VPX-MPLS**。



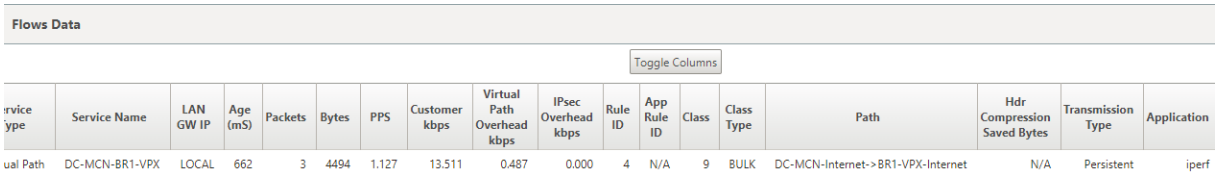
下图说明了当流量流动时，如果当前最佳路径之一变为非活动路径，则会选择另一条路径，并且 F **lows Data** 表中的路径部分仍有两条路径。



持久路径传输模式

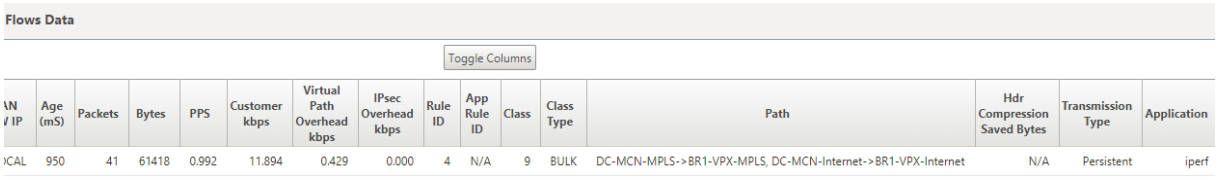
持久路径传输模式有助于保留基于路径延迟阻抗的流量数据包。

下图仅说明了一个路径，该路径是当前处理流及其数据包的最佳路径。没有带宽的需求，一条路径可以满足所有需求。目前只有一条最好的路径是 **DC-MCN-Internet->BR1-VPX-Internet**。



下图说明了如果路径 **DC-MCN-Internet->BR1-VPX-Internet** 变得容易延迟或被禁用，您会注意到新路径生效，并且当前路径 **DC-MCN-Internet->BR1-VPX-Internet** 成为最后一个最佳路径。

因此，新的路径部分显示了 **DC-MCN-MPLS->BR1-VPX-MPLS**、**DC-MCN-Internet->BR1-VPX-Internet**。

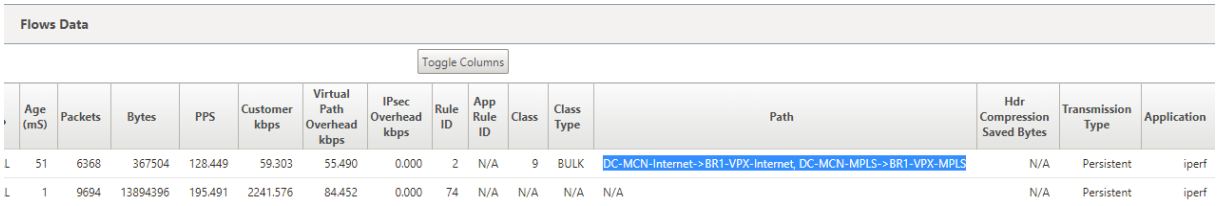

Flows Data

Toggle Columns

...N / IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
...CAL	950	41	61418	0.992	11.894	0.429	0.000	4	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

在持久模式下，可以选择多个路径来处理流量。在这种情况下，GUI 会从流量流的开始在流量表的路径部分显示具有最佳路径和下一个最佳路径。

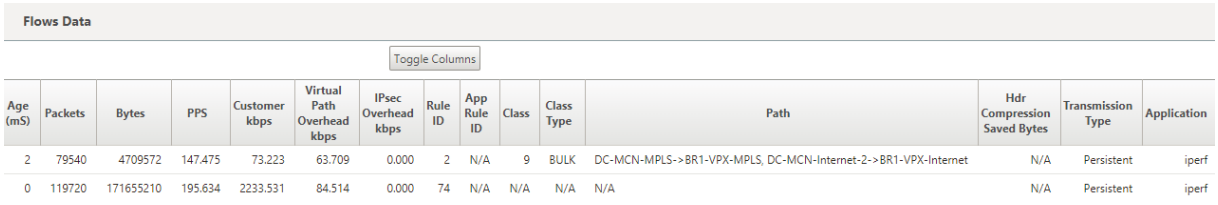
下图说明流最初只需要两个以上的路径，只要没有路径延迟阻抗交叉 (50 ms)，它们就会保持持久性。所采用的两条路径如下所示：**DC-MCN-Internet->BR1-VPX-Internet**、**DC-MCN-MPLS->BR1-VPX-MPLS**。


Flows Data

Toggle Columns

	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
L	51	6368	367504	128.449	59.303	55.490	0.000	2	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Persistent	iperf
L	1	9694	13894396	195.491	2241.576	84.452	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

假设 **DC-MCN-Internet** 的最佳路径之一进入高延迟或被禁用。这使得新路径出现，新路径可能是最佳路径，也可能是基于该时间路径选择的决策的第二个最佳路径。


Flows Data

Toggle Columns

Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
2	79540	4709572	147.475	73.223	63.709	0.000	2	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet-2->BR1-VPX-Internet	N/A	Persistent	iperf
0	119720	171655210	195.634	2233.531	84.514	0.000	74	N/A	N/A	N/A	N/A	N/A	Persistent	iperf

管理 IP 故障排除

September 2, 2022

以下是您在配置 DHCP IP 地址时可能遇到的情况。它还包括在部署 SD-WAN 设备时配置 DHCP 管理 IP 地址的最佳实践和建议。

这些建议适用于 SD-WAN 标准版的所有平台型号-物理设备和虚拟设备。

> 注意
>
> SD-WAN 设备的所有硬件型号都配有出厂默认管理 IP 地址。确保在安装过程中为设备配置所需的 DHCP IP 地址。
>
> 所有 SD-WAN 设备的虚拟模型（VPX 型号）和可以在 AWS 环境中部署的设备都没有分配出厂默认 IP 地址。

无需连接 **DHCP** 服务器即可打开电源：

- 原因：

  - 以太网管理电缆断开
  - 已连接网络的 DHCP 服务已关闭

- 预期行为

  - 启用 DHCP 服务的设备将每 300 秒重试一次 DHCP 请求（默认值）。实际间隔约 7 分钟
  - 因此，启用 DHCP 服务的设备将在 DHCP 服务器可用后 7 分钟内获取 DHCP 地址。延迟范围从 0 到 7 分钟

分配的 **DHCP** 地址过期：

- 预期行为：

  - 启用 DHCP 服务的设备将尝试在地址过期前续订租约
  - 如果续订失败，设备以新 DHCP 发现启动

启用 **DHCP** 服务的设备从一个启用 **DHCP** 的子网移动到另一个子网：

- 原因：设备从分配的 DHCP 子网移动到不同的 DHCP 子网
- 预期行为：

  - 永久租约 DHCP IP 地址分配可能需要重新启动设备才能从新 DHCP 服务器获取 IP 地址。
  - DHCP 租约到期后，如果当前 DHCP 服务器无法访问，设备可能会重新启动 DHCP 发现协议。
  - 设备获取新的 IP 地址，延迟 8 分钟。在 GUI 和 CLI 中不修改 Gateway IP 地址。它在重新启动过程完成后进行更新。

建议**:**

- 始终为分配给 Citrix SD-WAN 设备（物理/虚拟）的 DHCP 地址分配永久租约。这允许设备具有可预测的管理 IP 地址。

基于会话的 **HTTP** 通知

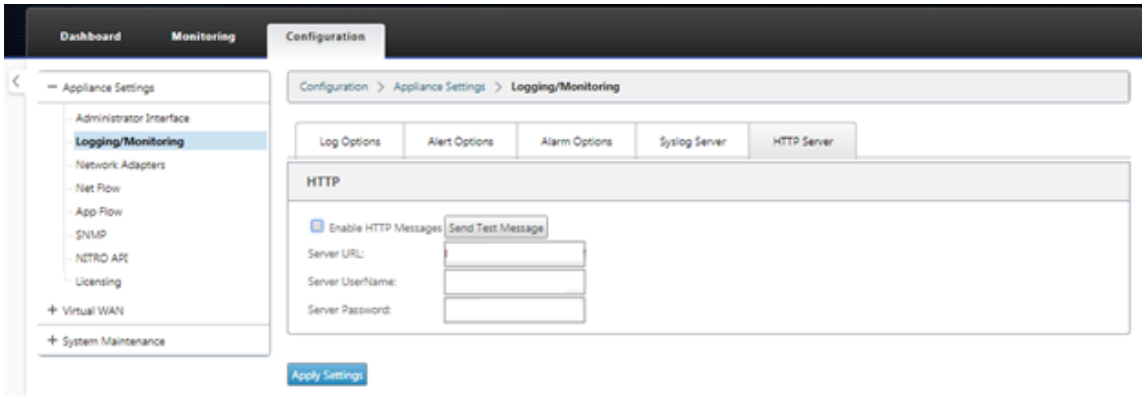
September 2, 2022

现在，您可以在 Citrix SD-WAN 设备 GUI 中为通用 HTTP POST API 服务请求配置事件和警报报告。HTTP 警报和事件通知 配置类似于 SD-WAN 中支持的事件和警报的电子邮件和 SNMP 事件。

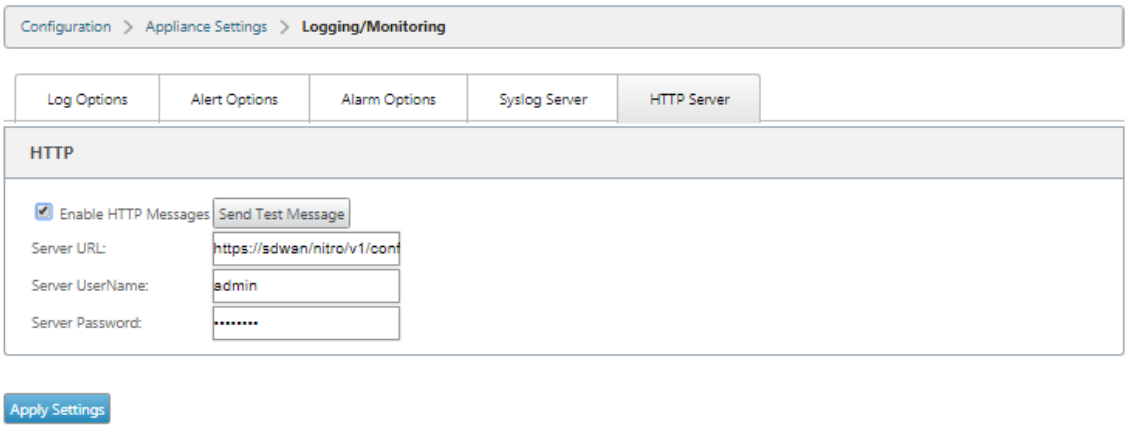
基于会话的 HTTP Post 通知会发送到外部服务，如立即服务。可以在 Citrix SD-WAN 设备 GUI 和 Citrix SD-WAN Center 中配置 HTTP 服务器的事件通知。

要在 Citrix SD-WAN 设备 GUI 中配置 HTTP POST 通知，请执行以下操作：

1. 导航到 配置 > 日 志记录/监控 > **HTTP** 服务器。



2. 单击 启用 **HTTP** 消息。
3. 输入要从中接收通知的 HTTP 服务器的服务器 **URL** 。输入 服务器用户名 和 服务器密码。

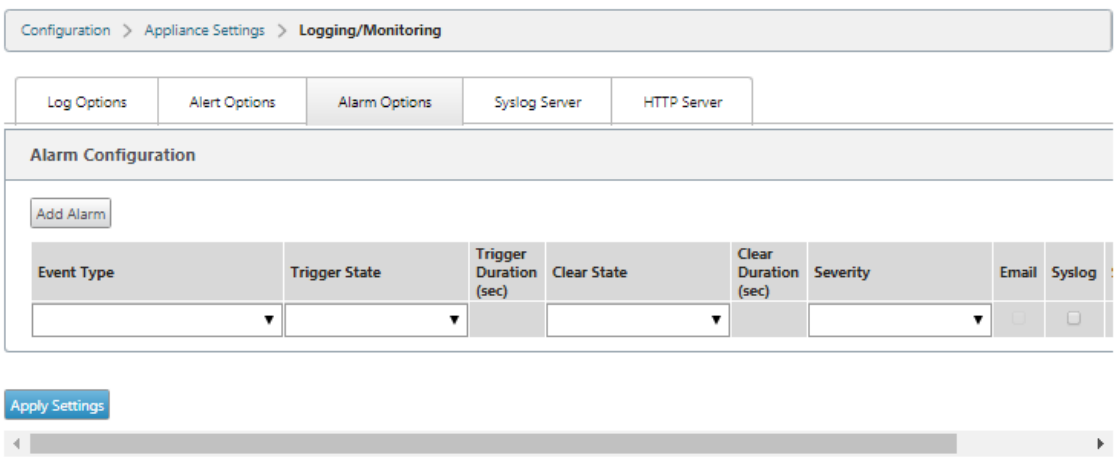


4. 单击 应用设置。应用 HTTP 服务器通知设置后，页面将刷新。

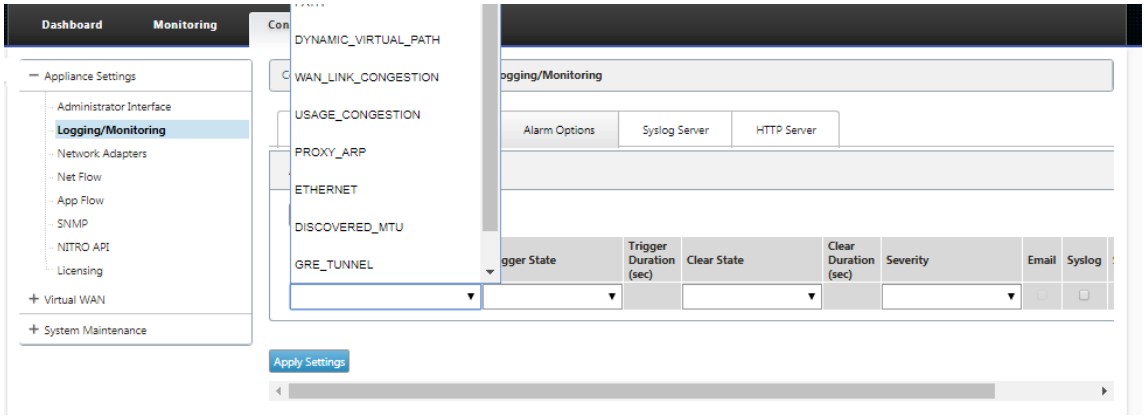
> 注意
>
> 使用“发 送测试消息”选项来验证 HTTP 服务器连接是否成功。

要为 HTTP 服务器会话添加警报通知：

1. 在“记录/监控”页面中，转到“警报选项”选项 卡页面。
2. 点击 添加警报。

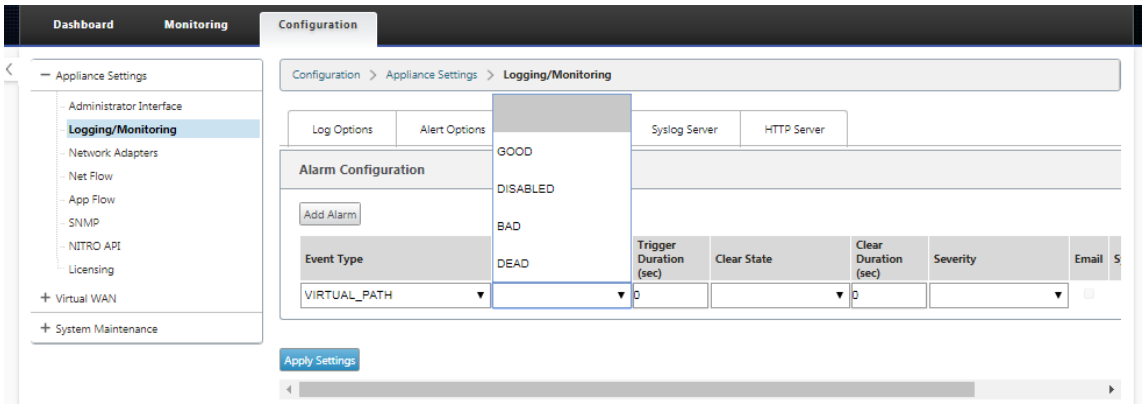


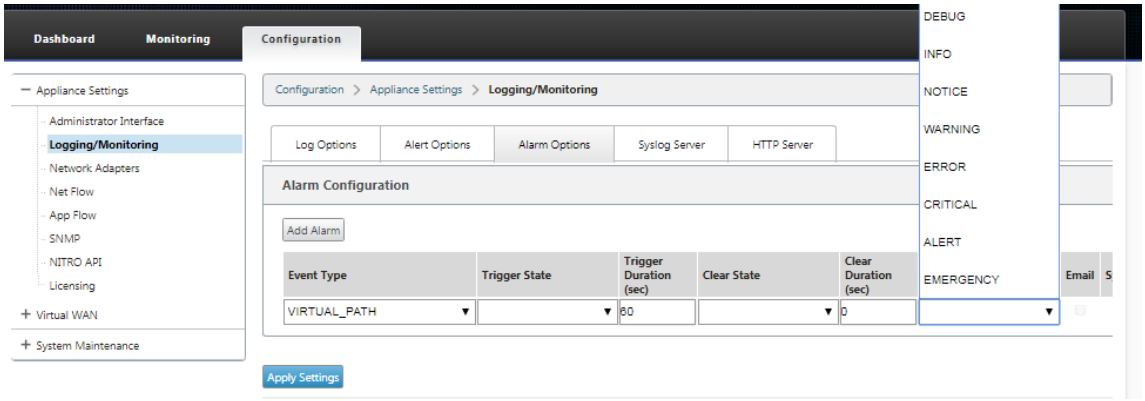
3. 从下拉列表中选择 事件类型。



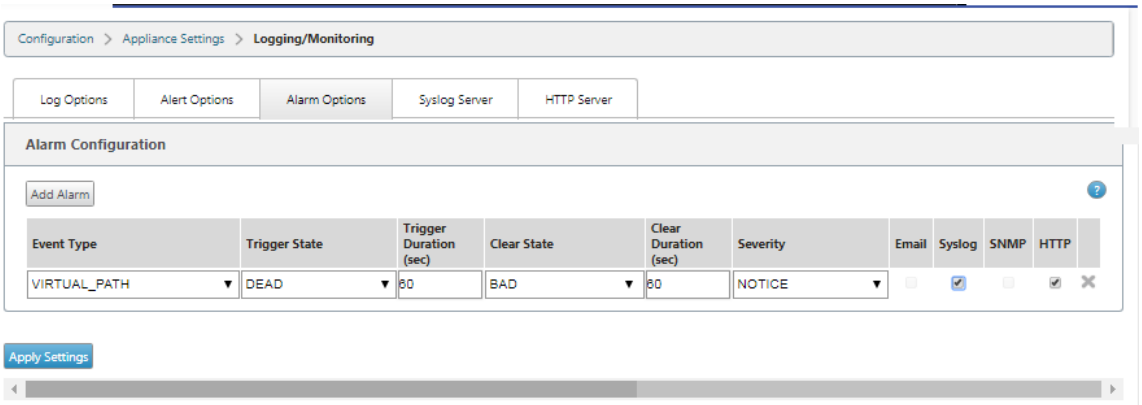
4. 为所选 事件类型选择以下警报通知状态。触发器状态和清除状态根据选定的事件类型发生变化。

   - 触发状态-好，禁用，坏，死
   - 触发持续时间—以秒为单位的时间
   - 清除状态-好，禁用，坏，死
   - 清除持续时间-以秒为单位的时间
   - 严重性—调试、信息、通知、警告、错误、严重、事件、紧急情况





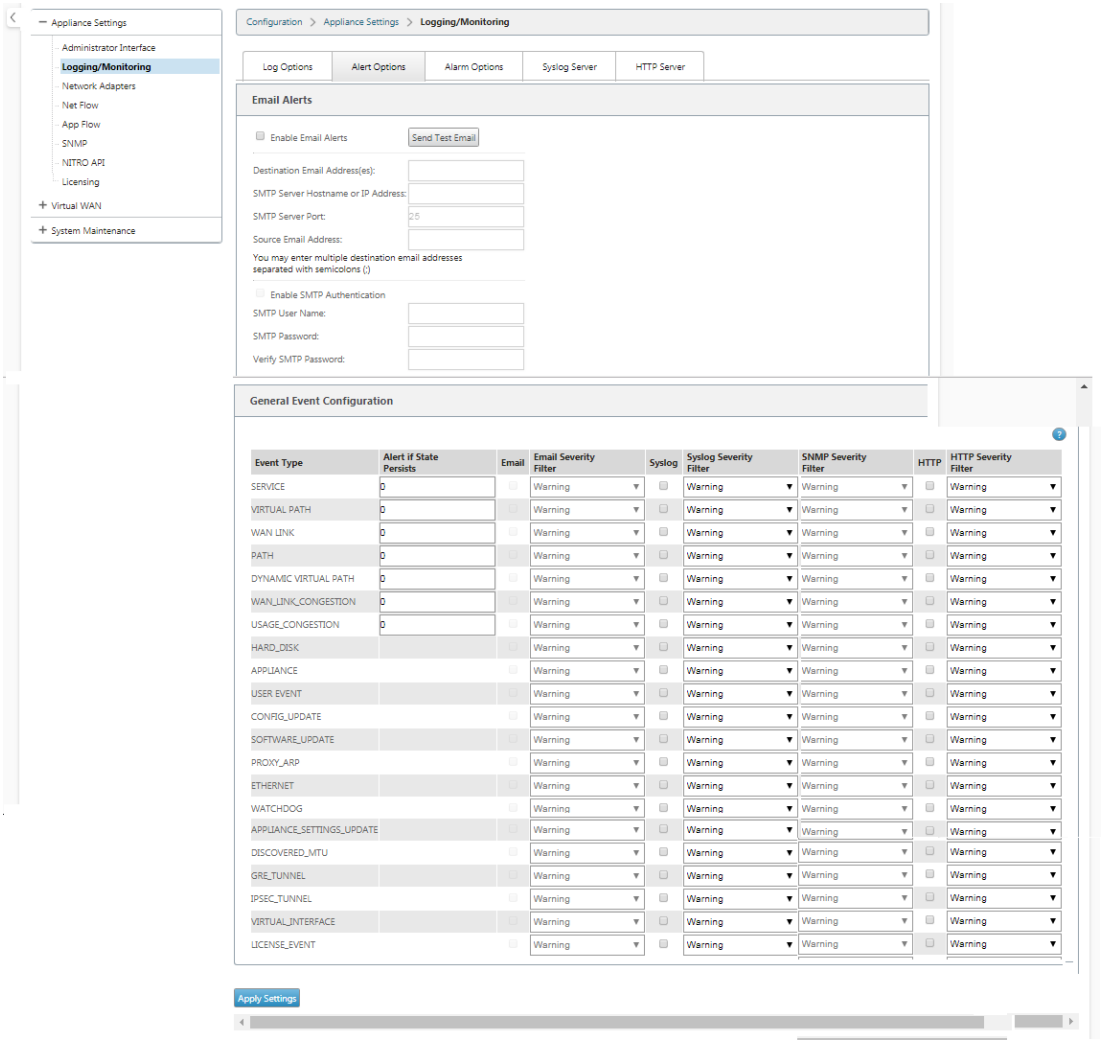
5. 选中 系统日志 和 **HTTP** 复选框以接收特定于 Syslog 和 HTTP 服务器事件的通知。单击 应用设置。



要配置事件选项，请执行以下操作：

转到“警报选项”选项 卡页面。在“常规事件配置”页下；为事 件类型 选择 HTTP 服务器通知过滤器，然后单击“应用设置”。

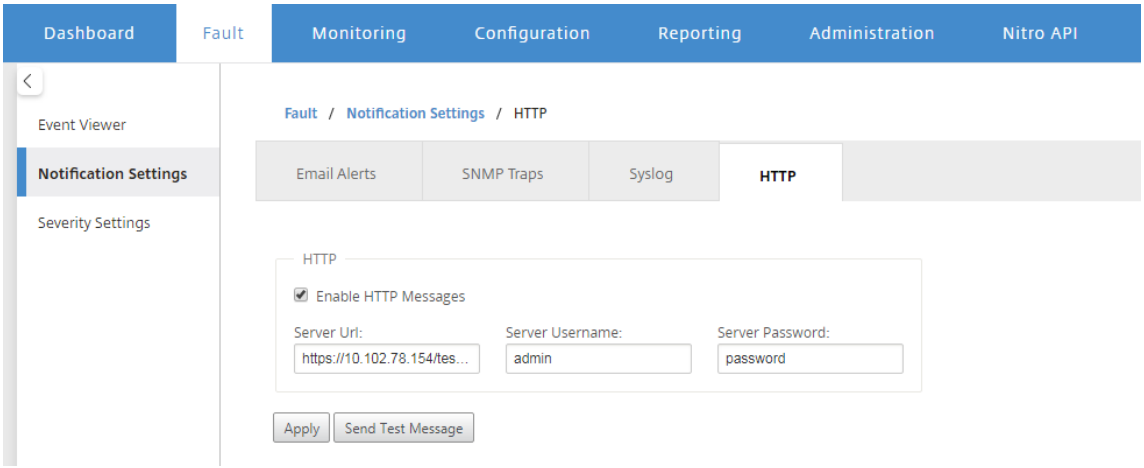
- HTTP
- HTTP 严重性筛选器



在 **Citrix SD-WAN Center** 中配置 **HTTP** 通知

要配置 HTTP 通知，请执行以下操作：

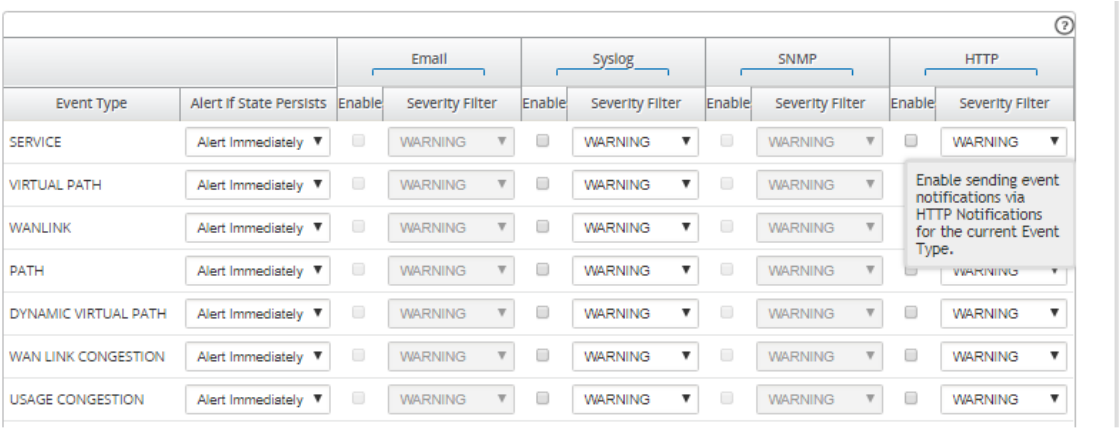
1. 导航到 故障 > 通知设置 > **HTTP**。



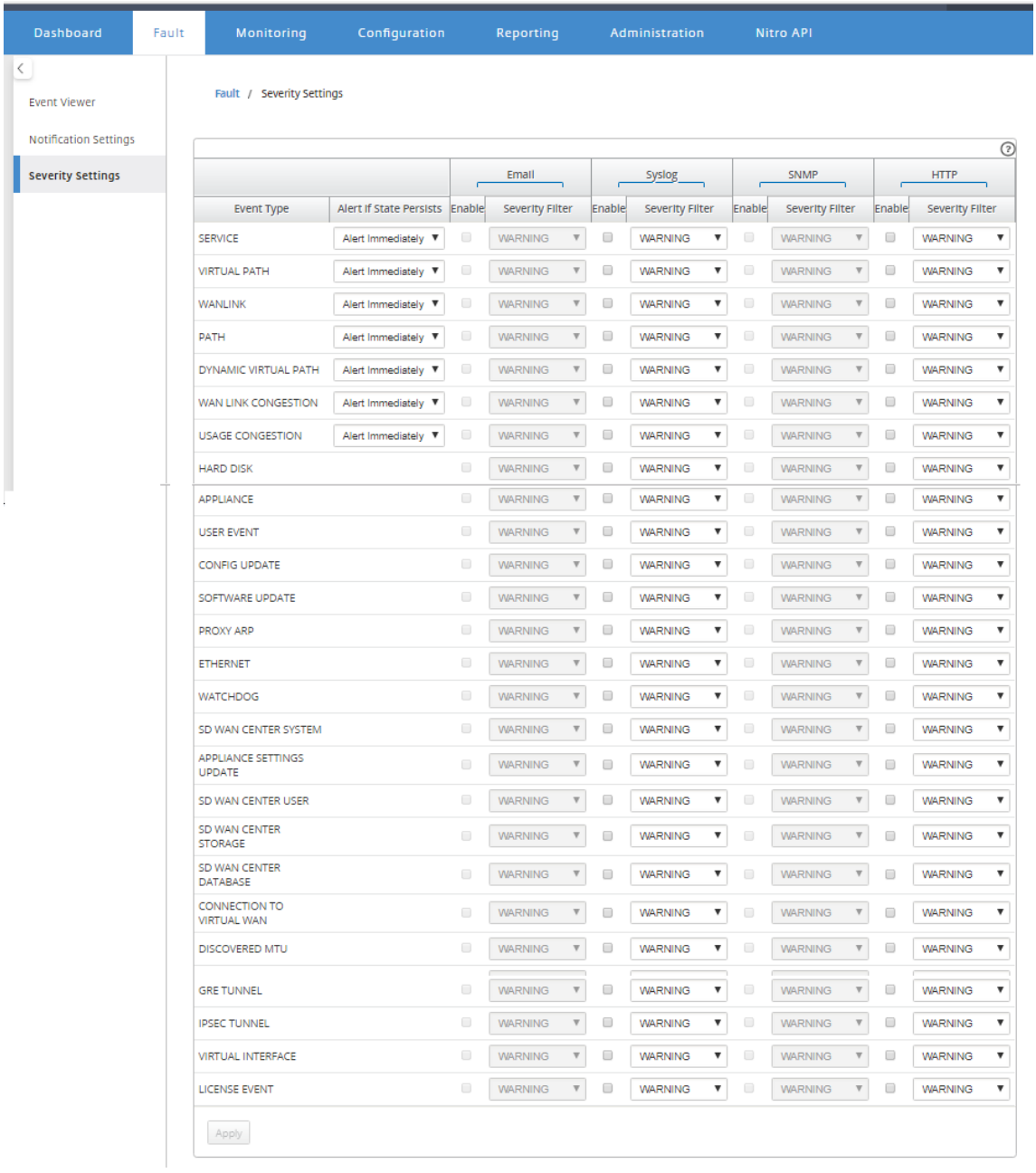
2. 输入 HTTP 服务器的服务器 **URL**、服务器用户名和服务器密码。
3. 单击 应用

要配置严重性设置，请执行以下操作：

1. 转到 严重性设置 页面。单击 启用 开始监视所选事件类型的 HTTP 通知。



2. 您可以选择监视以下事件类型的电子邮件、系统日志、SNMP 和 HTTP 事件通知。单击应用。



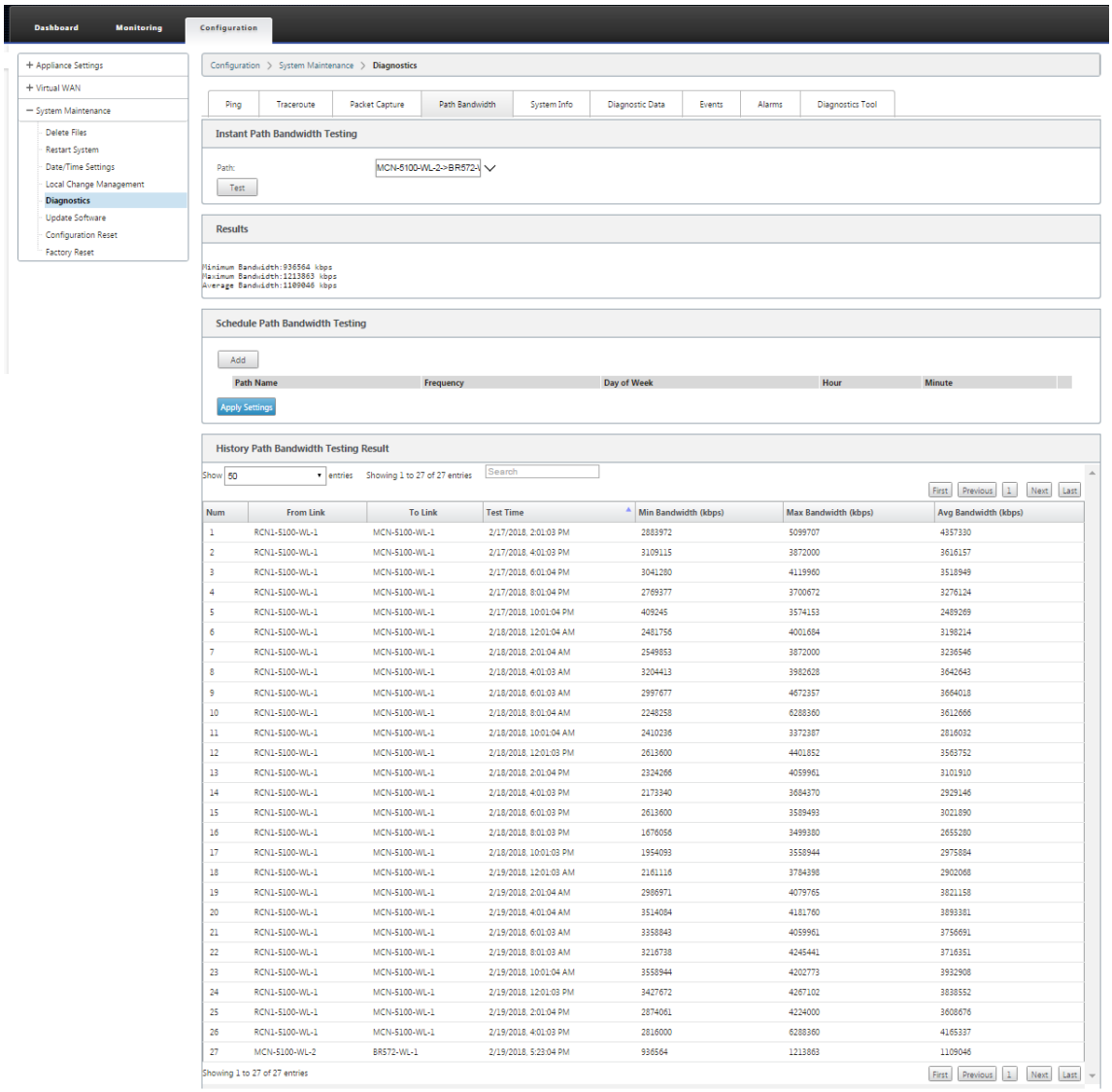
主动带宽测试

September 2, 2022

主动带宽测试使您能够通过公共 Internet WAN 链接发出即时路径带宽测试，或安排公共 Internet WAN 链接带宽测试在特定时间定期完成。此功能可用于演示新安装和现有安装期间两个位置之间的可用带宽量，也可用于测试路径以确定设置和确认更改的结果，例如调整 DSCP 标签设置或带宽允许速率。

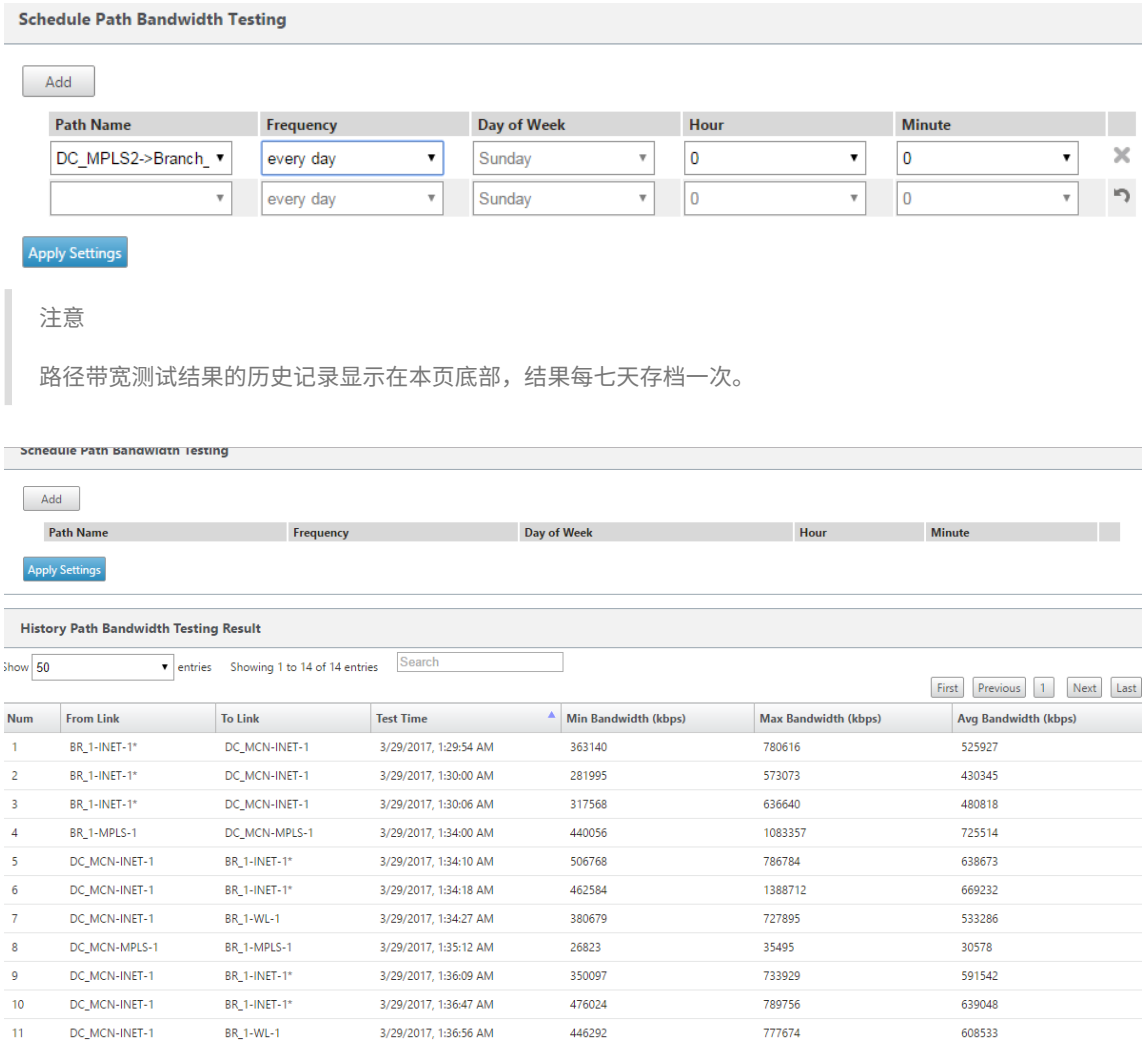
要使用主动带宽测试功能，请执行以下操作：

1. 导航到 系统维护 > 诊断 > 路径带宽。
2. 选择所需的 路径，然后单击 测试。



输出显示用作值的平均带宽，以设置为测试的 WAN Link 最小和最大带宽结果的允许速率。除了测试带宽的功能外，您现在可以更改配置文件以使用学习的带宽。这是通过站点 > [站点 名称] > WAN 链接 > [**WAN** 链接名称] > 设置 下的“自动学习”选项来完成的，如果启用，系统将使用学习的带宽。

您还可以安排每周、每日或每小时间隔的路径带宽的重复测试。



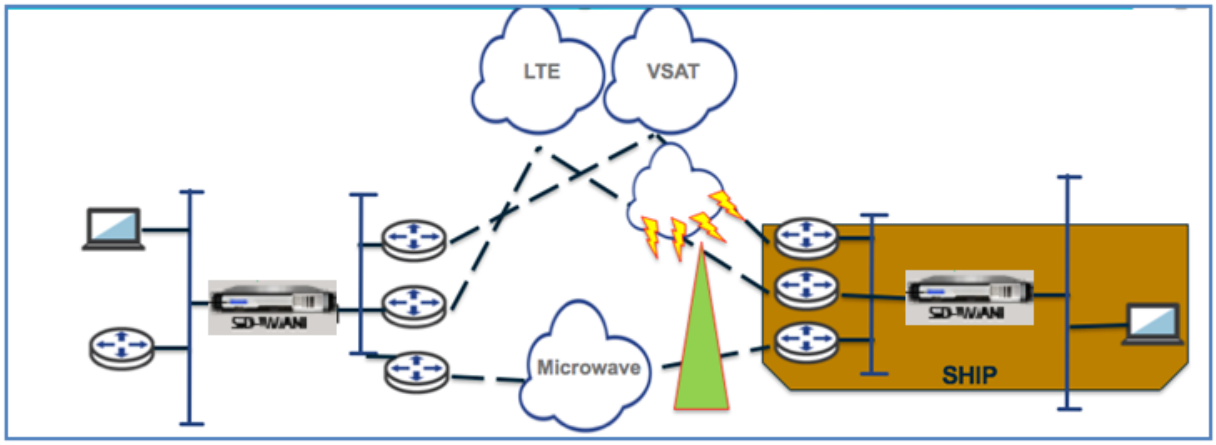
> **注意**
>
> 路径带宽测试结果的历史记录显示在本页底部，结果每七天存档一次。

自适应带宽检测

November 16, 2022

此功能适用于具有 VSAT、LOS、Microwave、3G/4G/LTE WAN 链路的网络，其可用带宽因天气和大气条件、位置和站点障碍物线而异。它允许 SD-WAN 设备根据定义的带宽范围（最小和最大 WAN 链路速率）动态调整 WAN 链路上的带宽速率，以使用可用带宽的最大量，而无需将路径标记为坏。

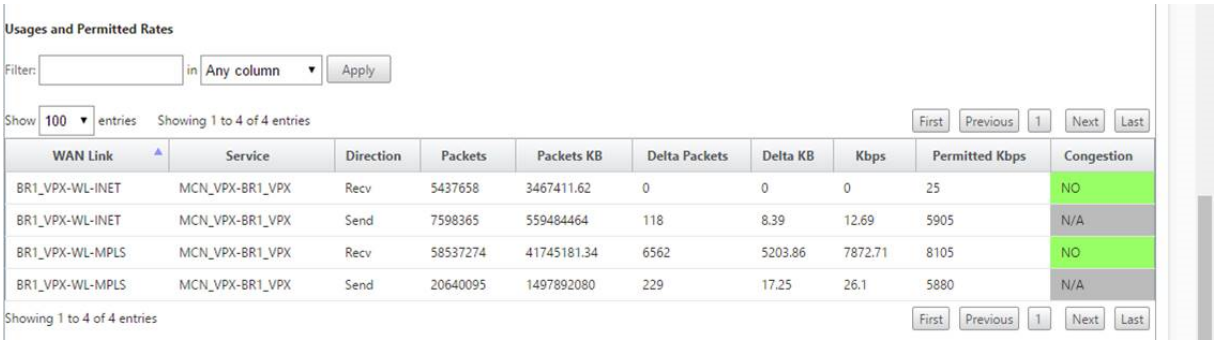
- 更高的带宽可靠性（通过 VSAT、Microwave、3G/4G 和 LTE）
- 与用户配置设置相比，自适应带宽可预测性更高



要启用自适应带宽检测，请执行以下操作：

此功能需要启用坏损失敏感度选项（默认/自定义）作为先决条件。从 SD-WAN 11.5 版本起，您可以在 Citrix SD-WAN Orchestrator 服务上启用它。有关更多信息，请参阅 自适应带宽检测。

导航到监控 > 统计信息 > WAN 链路使用情况 **> 使用率和允许费率，以查看“使用 率和 允许费率”表。**



Usages and Permitted Rates

Filter: in Any column Apply

Show 100 entries Showing 1 to 4 of 4 entries First Previous 1 Next Last

WAN Link	Service	Direction	Packets	Packets KB	Delta Packets	Delta KB	Kbps	Permitted Kbps	Congestion
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Recv	5437658	3467411.62	0	0	0	25	NO
BR1_VPX-WL-INET	MCN_VPX-BR1_VPX	Send	7598365	559484464	118	8.39	12.69	5905	N/A
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Recv	58537274	41745181.34	6562	5203.86	7872.71	8105	NO
BR1_VPX-WL-MPLS	MCN_VPX-BR1_VPX	Send	20640095	1497892080	229	17.25	26.1	5880	N/A

Showing 1 to 4 of 4 entries First Previous 1 Next Last

最佳做法

September 2, 2022

以下主题提供了在网络中设计、规划和执行 Citrix SD-WAN 解决方案时应遵循的最佳做法。

安全性

路由

QoS

WAN 链接

安全性

September 2, 2022

本文概述了 Citrix SD-WAN 解决方案的安全最佳实践。它为 Citrix SD-WAN 部署提供了一般安全指南。

Citrix SD-WAN 部署指南

为了在整个部署生命周期内维护安全性，Citrix 建议考虑以下安全因素：

- 物理安全
- 设备安全性
- 网络安全
- 行政和管理

物理安全

在安全服务器房中部署 Citrix SD-WAN 设备-安装 Citrix SD-WAN 的设备或服务器应放置在安全服务器房或受限数据中心设施中，以防止设备遭受未经授权的访问。至少，访问应由电子读卡器控制。对设备的访问由 CCTV 监视，并持续记录所有活动以供审核。如果发生闯入事件，电子监控系统应向保安人员发出警报，以便立即作出反应。

保护前面板和控制台端口免受未经授权的访问-通过物理密钥访问控制将设备安全在一个大笼子或机架中。

保护电源-确保设备受到不间断电源的保护。

设备安全性

为了确保设备安全，请确保托管 Citrix SD-WAN 虚拟设备 (VPX) 的任何服务器的操作系统的安全，执行远程软件更新，并遵循安全的生命周期管理实践：

- 保护托管 Citrix SD-WAN VPX 设备的服务器的操作系统-Citrix SD-WAN VPX 设备作为虚拟设备在标准服务器上运行。应通过基于角色的访问控制和强大的密码管理来保护对标准服务器的访问。此外，Citrix 建议使用操作系统的最新安全修补程序以及服务器上的最新防病毒软件对服务器进行定期更新。
- 执行远程软件更新-安装所有安全更新以解决任何已知问题。请参阅安全公告网页注册并接收最新的安全警报。
- 遵循安全生命周期管理实践-要在重新部署或启动 RMA 时管理设备并停用敏感数据，请通过从设备中删除持久数据来完成数据回忆对策。
- 在 DMZ 后面部署设备的管理界面，以确保无法直接通过 Internet 访问管理界面。要增加保护，请确保管理网络与 Internet 隔离，并且只有拥有批准的管理应用程序的授权用户才能在网络中运行。

网络安全

为了网络安全，请勿使用默认 SSL 证书。访问管理员界面时，请使用传输层安全性 (TLS)，保护设备的不可路由的管理 IP 地址，配置高可用性设置，并根据部署情况实施管理和管理安全措施。

- 请勿使用默认 SSL 证书-来自信誉良好的证书颁发机构的 SSL 证书可简化面向 Internet 的 Web 应用程序的用户体验。与自签名证书或来自信誉良好的证书颁发机构的证书不同，Web 浏览器不要求用户安装来自信誉良好的证书颁发机构的证书来启动与 Web 服务器的安全通信。
- 在访问管理员界面时使用传输层安全性-确保管理 IP 地址无法从 Internet 访问或至少受到安全防火墙的保护。请确保 LOM IP 地址无法从 Internet 访问或至少受到安全防火墙的保护。
- 安全管理和管理帐户-创建替代管理帐户，为管理员和查看者帐户设置强密码。配置远程帐户访问时，请考虑使用 RADIUS 和 TACS 配置对帐户进行外部身份验证的管理管理。更改管理员用户帐户的默认密码，配置 NTP，使用默认会话超时值，使用带 SHA 身份验证和 AES 加密的 SNMPv3。

Citrix SD-WAN 覆盖网络保护遍历 SD-WAN 覆盖网络的数据。

安全管理员界面

为了安全的 Web 管理访问，请通过上载和安装来自信誉良好的证书颁发机构的证书来替换默认系统证书。转到 SD-WAN 设备 GUI 中的**配置 > 设备设置 > 管理员界面**。

用户帐户：

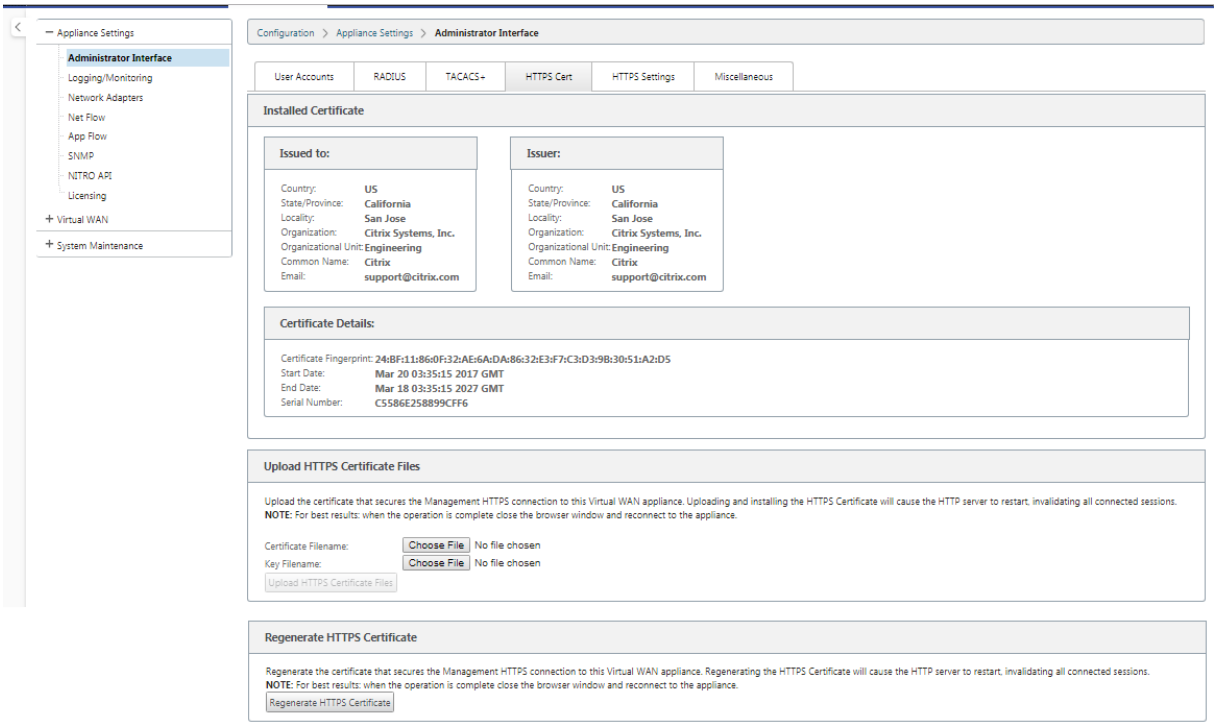
- 更改本地用户密码
- 管理用户

HTTPS 证书：

- 证书
- 键

杂项：

- Web 控制台超时



考虑使用 **Citrix Web App Firewall**

Citrix ADC 许可设备提供了内置的 Citrix Web App Firewall，该防火墙使用积极的安全模型，并自动学习正确的应用程序行为以防范命令注入、SQL 注入和跨站点脚本等威胁。

当您使用 Citrix Web App Firewall 时，用户可以在不更改代码的情况下为 Web 应用程序添加额外的安全性，也不需要更改配置。有关详细信息，请参阅 Citrix Web Application Firewall 简介。

全局虚拟路径加密设置

- 默认情况下启用 AES-128 数据加密。建议使用 AES-128 或更多 AES-256 加密级别的保护进行路径加密。确保设置“启用加密密钥轮换”，以确保每个启用加密的虚拟路径的密钥再生密钥，每隔 10-15 分钟使用椭圆曲线差异-赫尔曼密钥交换启用。

如果网络除了保密性（即篡改保护）之外还需要消息身份验证，Citrix 建议使用 IPsec 数据加密。如果仅需要保密性，Citrix 建议使用增强型标头。

- 扩展的数据包加密头可以在每个加密邮件的开头预先添加随机种子计数器。加密后，此计数器将用作随机初始化向量，仅使用加密密钥确定性。这会随机化加密的输出，从而无法区分地提供强有力的信息。请记住，启用此选项时会增加 16 个字节的数据包开销
- 扩展数据包身份验证拖车将身份验证代码附加到每个加密邮件的末尾。此拖车允许验证数据包在传输过程中未被修改。请记住，此选项会增加数据包开销。

防火墙安全

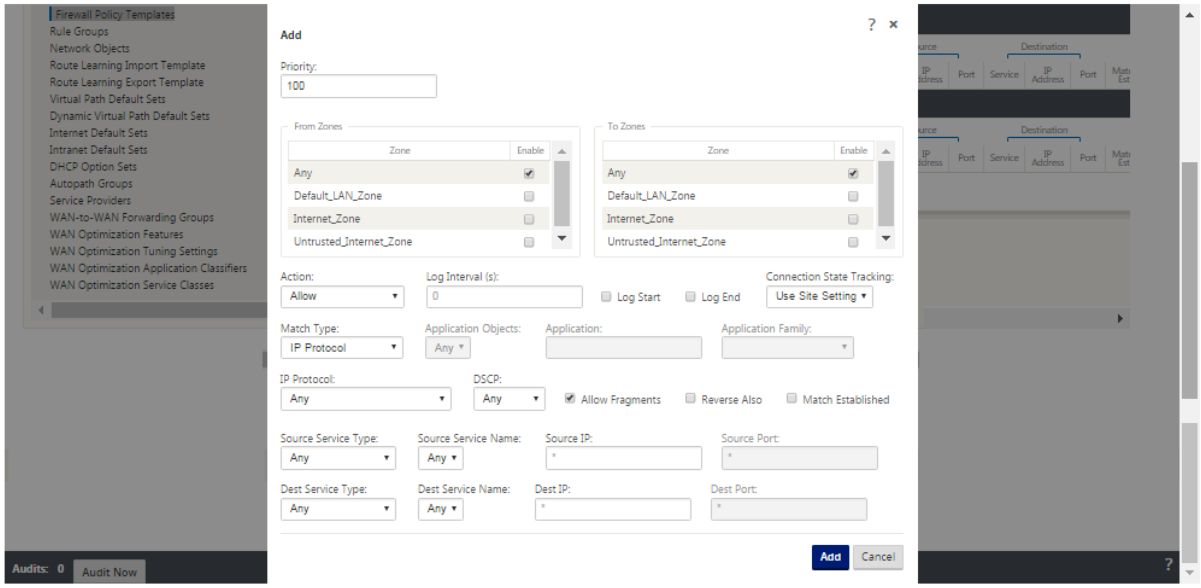
建议的防火墙配置首先使用默认防火墙操作作为全部拒绝，然后添加例外。在添加任何规则之前，记录并查看防火墙规则的用途。尽可能使用状态检查和应用级别检查。简化规则并消除冗余规则。定义并遵守更改管理流程，以跟踪并允许审查对 防火墙 设置的更改。将所有设备的防火墙设置为使用全局设置跟踪通过设备的连接。跟踪连接验证数据包是否正确形成，并且是否适合连接状态。创建适合组织网络或功能区域逻辑层次结构的区域。请记住，区域在全球范围内具有重要意义，可以将不同地理位置的网络视为同一个安全区域。创建最具体的策略，以降低安全漏洞的风险，避免在允许规则中使用任意。配置和维护全局策略模板，为网络中的所有设备创建基本安全级别。根据设备在网络中的功能角色定义策略模板，并在适当时应用它们。仅在必要时在单个站点上定义策略。

全局防火墙模板 -防火墙模板允许配置全局参数，这些参数会影响在 SD-WAN 覆盖环境中运行的各个设备上的防火墙运行。

默认防火墙操作—允许启用与任何过滤器策略不匹配的数据包。拒绝启用与任何筛选器策略不匹配的数据包被删除。

默认连接状态跟踪—为与筛选器策略或 NAT 规则不匹配的 TCP、UDP 和 ICMP 流启用双向连接状态跟踪。即使未定义防火墙策略，启用此功能时，非对称流也会被阻止。可以在站点级别定义设置，这些设置将覆盖全局设置。如果某个地点存在不对称流量的可能性，建议在一个地点或政策层面而不是在全球范围内实现这一目标。

区域 -防火墙区域定义连接到 Citrix SD-WAN 的网络的逻辑安全分组。区域可应用于虚拟接口、内联网服务、GRE 通道和 LAN IPsec 通道。



WAN 链接安全区

应在直接连接到公共（不安全）网络的 WAN 链接上配置不受信任的安全区域。不受信任会将 WAN 链接设置为最安全的状态，从而只允许接口组接受加密、经过身份验证和授权的流量。ARP 和 ICMP 到虚拟 IP 地址是唯一允许的其他流量类型。此设置还将确保仅从与接口组关联的接口中发送加密的流量。

路由域

路由域是包含用于分割网络流量的一组路由器的网络系统。新创建的站点会自动与默认路由域关联。

IPsec 通道

IPsec 通道保护用户数据和标头信息。Citrix SD-WAN 设备可以与非 SD-WAN 对等方协商局域网或 WAN 端的固定 IPsec 通道。对于 LAN 上的 IPsec 通道，必须选择路由域。如果 IPsec 通道使用 Intranet 服务，则路由域由所选的 Intranet 服务预先确定。

在数据可以通过 SD-WAN 覆盖网络流动之前，跨虚拟路径建立 IPsec 通道。

- 封装类型选项包括 ESP-数据封装和加密，ESP+Auth-数据封装、加密并使用 HMAC 验证，AH 进行数据验证。
- 加密模式是启用 ESP 时使用的加密算法。
- 哈希算法用于生成 HMAC。
- 生命周期是 IPsec 安全关联存在的首选持续时间（以秒为单位）。0 可用于无限制。

IKE 设置

Internet 密钥交换 (IKE) 是一种 IPsec 协议，用于创建安全关联 (SA)。Citrix SD-WAN 设备同时支持 IKEv1 和 IKEv2 协议。

- 模式可以是主模式或主模式。
- 身份可以自动识别对等体，也可以使用 IP 地址手动指定对等方的 IP 地址。
- 身份验证启用预共享密钥身份验证或证书作为身份验证方法。
- 如果支持对等体的 ID 类型，“验证对等体身份”将启用 IKE 的对等体身份验证，否则不要启用此功能。
- 差异-赫尔曼组可用于 IKE 密钥生成，组 1 为 768 位，组 2 为 1024 位，组 5 为 1536 位。
- 哈希算法包括 MD5、SHA1 和 SHA-256 的算法可用于 IKE 消息。
- 加密模式包括 AES-128、AES-192 和 AES-256 加密模式可用于 IKE 消息。
- IKEv2 设置包括对等身份验证和完整性算法。

配置防火墙

通过验证上游路由器和防火墙配置，可以发现以下常见问题：

- MPLS 队列/QoS 设置：验证 SD-WAN 虚拟 IP 地址之间的 UDP 封装流量是否不会因网络中间设备上的 **Qo** S 设置而受到影响。
- 在 SD-WAN 网络上配置的 WAN 链接上的所有流量应由 Citrix SD-WAN 设备使用正确的服务类型（虚拟路径、Internet、Intranet 和本地）进行处理。
- 如果流量必须绕过 Citrix SD-WAN 设备并使用相同的基础链接，则应在路由器上为 SD-WAN 流量进行适当的带宽预留。此外，应在 SD-WAN 配置中相应地配置链路容量。

- 验证中间路由器/防火墙没有强制执行任何 UDP 洪水和/或 PPS 限制。当通过虚拟路径（UDP 封装）发送流量时，这会限制流量。

路由

September 2, 2022

本文概述了 Citrix SD-WAN 解决方案的路由最佳实践。

Internet /内联网路由服务

如果 Internet 服务未配置为 Internet 绑定的流量，而是将 本地 路由或 直通 路由配置为到达网关路由器。路由器使用 SD-WAN 设备上配置的 WAN 链接，导致链接超额订阅问题。

如果在 MCN 上将 Internet 路由配置为本地路由，则所有分支 SD-WAN 站点都会学习该路由，默认情况下将其配置为虚拟路径路由。这意味着分支设备上的 Internet 绑定流量通过虚拟路径路由到 MCN。

路由优先级

路由优先顺序：

- 前缀匹配：最长前缀匹配。
- 服务：本地、虚拟路径服务、Internet 、内联网、直通
- 路由成本

路由不对称

确保网络中没有路由不对称（NetScaler SD-WAN 设备仅在一个方向传输流量）。这会导致防火墙连接跟踪和深度数据包检查的问题。

QoS

September 2, 2022

配置 QoS 时请考虑以下事项：

- 了解您的网络流量模式和需求。您可能必须观察 **QoS** 类别统计信息，更改队列深度和/或更改默认 QoS 类别份额百分比，以避免 QoS 统计信息中显示的尾巴丢失。

- 有时，为了便于配置，会将整个子网添加到规则中，而不是为特定的应用程序 IP 地址创建规则。将整个子网添加到规则时会错误地将子网中的所有流量映射到一个规则。因此，与该规则关联的 QoS 类可能会导致尾部落和应用程序性能或用户体验差。

WAN 链接

September 2, 2022

Citrix SD-WAN 平台支持多达 8 个公共 Internet 连接和 32 个专用 MPLS 连接。本文概述了 Citrix SD-WAN 解决方案的 WAN 链接配置最佳实践。

配置 WAN 链接时要记住的要点：

- 将“允许”和“物理 速率”配置为实际的 WAN 链路带宽。如果 SD-WAN 设备不应使用整个 WAN 链路容量，请相应地更改 允许 的速率。
- 当您不确定带宽并且链接不可靠时，可以启用 自动学习 功能。自动学习 功能仅学习底层链路容量，并在将来使用相同的值。
- 如果底层链路不稳定且不能保证固定带宽（例如，4G 链路），请使用 自适应带宽检测 功能。
- 不建议在同一 WAN 链接上启用 自动学习 和 自适应带宽检测。
- 使用所有 WAN 链路的入口/出口物理速率手动配置 MCN/RCN，因为它是多个分支机构间带宽分配的中心点。
- 为了提高重要数据中心工作负载/服务的可靠性，如果不使用自动学习，请使用与 SLA 的可靠链接，且不存在容量随机变化。
- 如果基础链接不稳定，请更改以下路径设置：
  - 丢失设置
  - 禁用不稳定敏感
  - 沉默时间
- 使用 诊断工具 检查链路的运行状况/容量。
- 如果 SD-WAN 以 单臂 模式部署，请确保不会超出底层链路的物理容量。

验证 ISP 链接运行状况

对于新部署，早于 SD-WAN 部署以及将新 ISP 链接添加到现有 SD-WAN 部署时：

- 验证链接类型。例如，MPLS、ADSL、4G。
- 网络特点. 例如-带宽、损耗、延迟和抖动。

此信息有助于根据您的要求配置 SD-WAN 网络。

网络拓扑

通常会发现，特定网络流量绕过 Citrix SD-WAN 设备，并使用 SD-WAN 网络中配置的相同基础链接。由于 SD-WAN 对链接利用率没有完全可见性，因此 SD-WAN 有可能超额订阅链接，导致性能和 PATH 问题。

预配

Provisioning SD-WAN 时需要考虑的事项：

- 默认情况下，所有分支机构和 WAN 服务（虚拟路径/Internet/Intranet）接收相同的带宽份额。
- 当连接站点之间在带宽要求或可用性方面存在很大差异时，需要更改预配站点。
- 当在最大可用站点之间启用动态虚拟路径时，WAN 链接容量将在 DC 的静态虚拟路径和动态虚拟路径之间共享。

常见问题解答

September 2, 2022

高可用性

高可用性和辅助（Geo）设备有什么区别?

- 高可用性确保容错能力。辅助（Geo）设备启用灾难恢复。
- 可为 MCN、RCN 和分支设备配置高可用性。只能为 MCN 和 RCN 配置辅助（Geo）设备。
- 高可用性设备在同一站点或地理位置内进行配置。位于不同地理位置的分支设备配置为辅助 (Geo) MCN/RCN 设备。
- 高可用性主设备和次级设备应该是相同的平台型号。辅助（Geo）设备可能是也可能不是与主 MCN/RCN 相同的平台型号。
- 高可用性优先于辅助 (Geo)。如果设备 (MCN/RCN) 配置了高可用性和辅助 (Geo) 设备，则当设备发生故障时，辅助高可用性设备将变为活动状态。如果两个高可用性设备都出现故障或数据中心站点崩溃，则辅助 (Geo) 设备将变为活动状态。
- 在高可用性中，主/辅助切换即时或在 10-12 秒内进行，具体取决于高可用性部署。主 MCN/RCN 到辅助 (Geo) MCN/RCN 切换, 发生在 15 秒主处于非活动状态后.
- 高可用性配置允许您配置主回收。无法为辅助 (Geo) 设备配置主回收，主回收会在主要设备恢复并保持计时器过期后自动执行。

单步升级

> 注意
>
> WANOP、SVM 和 XenServer 补充包/HF 被视为操作系统组件。

我应该使用 *.tar.gz* 还是单步升级 *.zip* 包从当前版本（8.1.x、9.1.x、9.2.x）升级到 9.3.x?

使用相关平台的 *.tar.gz* 文件将 SD-WAN 软件升级到 9.3.x。在 SD-WAN 软件升级到 9.3.x 版本后，使用 *.zip* 软件包执行更改管理以传输/暂存操作系统组件软件包。激活后，MCN 为所有相关分支传输/阶段操作系统组件。

使用单步升级包（.zip 文件）升级到 9.3.0 后，我需要执行。*upg* 在每台设备上升级?

不可以，操作系统软件更新/升级将通过单步升级 *.zip* 软件包进行，并根据您在相应站点的“变更管理设置”中提供的计划详细信息进行安装。

为什么我应该使用 *.tar.gz* 后跟 *.zip* 包从 9.3 版本之前的版本升级到 9.3.x 版本，为什么不直接使用 9.3.x 的 *.zip* 包?

从 9.3.0.161 开始支持单步升级软件包，在早期版本（9.3 版之前）版本中，此软件包无法识别。将单步升级 *.zip* 包上载到“变更管理”收件箱时，系统会抛出错误消息，指出无法识别该软件包。因此，首先要将 SD-WAN 软件升级到 9.3 或更高版本，然后使用执行变更管理。*zip* 包。

如何通过单步升级安装操作系统组件, 如果. 没有执行 *upg* 升级?

使用单步升级 *.zip* 软件包完成变更管理后，MCN 将根据设备型号传输/暂存操作系统组件软件包。激活后，MCN 开始传输/暂存操作系统组件软件包，用于计划的更新/升级需要它们的分支。

如何安装操作系统组件，而不安排以后的安装?

将“维护时段”值设置为“**0**”以立即安装操作系统组件。

> 注意
>
> 只有在设备收到站点所需的所有软件包后，即使“维护时段”值设置为“**0**”，安装也会开始。

调度安装有什么用处? 我可以使用日程安排说明单独升级大众吗?

计划安装在 SD-WAN 9.3 版中引入，仅适用于操作系统组件，不适用于大众软件升级。通过单步升级，您无需登录每个设备来执行操作系统组件升级，并且通过调度选项，您可以在除大众软件版本升级之外的其他时间安排操作系统组件安装。

为什么 更改管理设置 页面中的计划信息默认显示过去的计划日期，这意味着什么?

“更改管理设置”页面显示默认计划信息，即“开始”：“*2016-05-21 21:20:00*”，“窗口”：*1*，“重复”：*1*，“单位”：“天数”。如果日期是过去的日期，则表示计划的安装基于时间和其他参数，如维护窗口、重复窗口和单位，而不是日期。

默认计划安装日期/时间设置为什么，它是否依赖于通用设备还是本地设备?

默认情况下，计划详细信息设置为“*2016-05-21 21:20:00*（维护窗口为 *1* 小时，每 *1* 天重复一次）”。此详细信息取决于本地设备站点。

如何在不等待维护/计划窗口的情况下立即安装操作系统组件?

在“更改管理设置”页面中将“维护时段”值设置为“**0**”，这将覆盖计划的安装时间。

当当前软件版本为 9.3.x 或更高版本时，我应该使用哪个软件包进行升级？

当前软件版本为 9.3.x 或更高时，使用单步升级 *.zip* 包升级到任何更高版本。

操作系统组件文件何时被传输/暂存到分支？

当使用单步升级 *.zip* 包升级系统完成更改管理时，激活完成后，操作系统组件文件会传输/暂存到相关分支。

哪些设备接收操作系统组件文件，它 是否依赖于平台还是所有分支机构都接收它？

基于虚拟机管理程序的设备，例如 **SD-WAN** —**400**、**800**、**1000**、**2000 SE** 和裸机 **SD-WAN-2100** 在 EE 许可证上运行，将收到要升级的操作系统组件。

日程安排是如何工作的？

默认情况下，计划详细信息设置为 *2016-05-21 21:20:00*（维护窗口为 *1* 小时，每 *1* 天重复一次），这意味着系统将检查新软件是否可以每天安装，因为重复值设置为 **1** 天 并将进行维护时间为 **1** 小 时，安装将在 **2016-05-21** 日的 **21:20:00**（本地设备时间）触发/尝试安装（如果有新软件）

如何知道操作系统组件是否已升级？

在“状态”列中，您可以看到绿色刻度标记。将鼠标悬停在它上面时，您可以看 到升级成功 消息。

如何安排 RCN 及其分支机构的操作系统组件的安装？

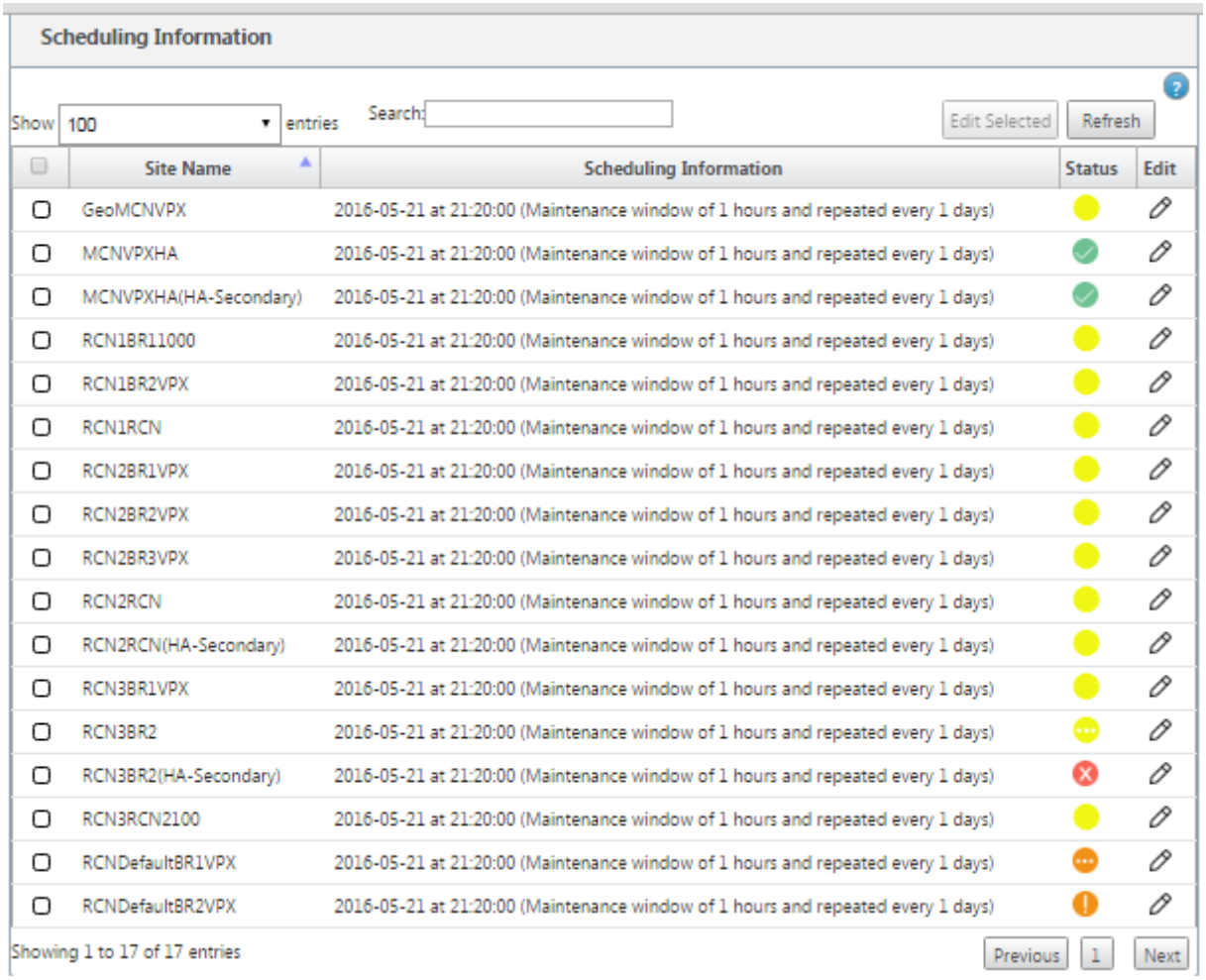
RCN 的计划是从 MCN 更改管理设置 页面执行的。对于 RCN 分支机构，您需要登录相应的 RCN 并设置计划详细信息。

从哪里可以获取计划安装的状态？

可以从 MCN 更改管理设置 页面获取 RCN 的计划安装状态。对于 RCN 分支机构，您需要登录相应的 RCN 才能获取状态。

如何获取计划安装的状态？

使用“更改管理设置”页面上提供的刷新按钮可分别从 MCN 和“默认区域”中的分支机构的 RCN 获取状态。



当之前的软件升级使用单步升级时，我可以使用 *tar.gz* 文件升级到下一个版本吗？

您可以使用 *tar.gz* 文件进行升级，但不建议这样做，因为您可以使用执行软件升级。*upg* 文件。通过登录每个适用的设备，上载以升级操作系统 (OS) 组件软件。从 9.3 版本 1 开始，“更新操作系统软件”页面已折旧。因此，您可以通过使用 *.zip* 软件包升级操作系统组件来执行更改管理。

我们如何验证操作系统组件的当前运行版本？

现在，您无法从 UI 验证操作系统组件的当前运行版本。您 可以从每个控制台登录或让 STS 查看此信息。

如果我的网络中有裸机设备，会有什么区别？调度是否会影响裸机/虚拟设备？

SD-WAN 之类的裸机设备—**410,2100,4100,5100 SD-WAN** 仅运行 SD-WAN 软件。裸机设备 不需要操作系统组件包。在软件需求方面，这些平台的处理与 SD-WAN VPX-SE 设备相同。MCN 不会将操作系统组件包传输到这些设备。设置计划信息不会对这些设备生效，因为它们没有任何需要升级的操作系统组件。

SSU 在高可用性环境/部署中如何工作？

在 MCN 的高可用性部署中，我们有一个局限性，即活动 MCN 交换机‘/切换主 MCN 在更改管理和备用/辅助 MCN 接管期间的角色。在这种情况下，您可以使用活动 MCN 上的 *.zip* 软件包再次执行更改管理，也可以通过切换活动 MCN 角色切换回主 MCN，以便原始主 MCN 可以担任将操作系统组件包转发到其他方面的角色分支机构。

单步升级如何在高可用性环境/部署中工作?

在高可用性部署中执行单步升级时，将切换主 MCN 和备用 MCN 的角色。这是一个限制。如果发生这种情况，请使用活动 MCN 上的 *.zip* 包再次执行变更管理。或者，您可以通过切换活动 MCN 的角色切换回主 MCN，以便原始主 MCN 可以将操作系统组件包分配到分支。

单步升级是否支持零接触部署以重新启动带设备?

是的，它可以使用。

我可以使用单步升级来升级我的独立 WANOP 设备吗?

不能。

是否可以使用单步升级升级来升级以两个盒式模式部署的独立 WANOP 设备?

否。只有 属于两个盒子模式的 SD-WAN 设备才会升级，而不是 WANOP 独立设备。

我应该使用哪个软件包来升级到 多层网络?

<release-version> 当前软件版本为 9.3.x 或更高版本时，请使用单步升级包 *ns-sdw-sw-.zip* 文件。MCN 负责分期包 到 RCN 和 RCN 阶段 软件包 到其各自的分支机构。

上传 *ns-sdw-sw-.zip* <release-version> 文件后，我在当前软件下只能看到一个平台型号?

从版本 10.0 开始，引入了对规模架构的 支持，以加快单步升级的处理速度。您只能在当前软件下看到 MCN 平台模型。当您选择“验证”或“暂存设备”按钮时，将列出/显示/处理其他装置 软件包。

对于 VPX/VPXL/裸机设备，哪些软件包是为 RCN 上演?

软件包 已分阶段到 RCN，因为 RCN 分支机构可以是任何平台模型。因此，他们需要所有的软件包。

如果 RCN 是 VPX 设备，而分支机构是需要这些软件包的设备，RCN 后面的分支站点如何 获取操作系统组件包?

RCN 在激活 SD-WAN VW 软件包后，将相关软件包分级到需要操作系统组件包的分支。

我是否可以在暂存期间选择 忽略未完成 并继续进入下一阶段的更改管理? 选择此按钮后，它会对尚未完成暂存的站点产生什 么影响?

是的，您可以点击 忽略不完整。这将启用“下一 步”按钮，并显示进度条。此选项适用于站点无法访问且更改管理仍在等待这些站点的分段完成的情况，因此用户可以通过忽略阶段状态继续进入下一阶段并继续激活。网站出现后，MCN 会在激活完成后分阶段封装。

部分软件升级

什么是部分网站升级? 如何使用它?

部分站点软件升级是版本 10.0 中引入的一项新功能。您可以从 MCN 暂存 10.x 版本的较新版本，并从选定站点/分支上的“本 地更改管理”页面激活暂存的软件版本。在站点/分支机构激活暂存软件之前，请 确保已从 MCN 启用复选框。

- 默认情况下，此功能处于禁用状态。现有的校正机制使网络保持同步。用户必须通过启用 配置 **>** 更改管理设置 页面上的复选框来选择允许部分站点升级。

- 部分软件升级只能在分支或 RCN 上完成，而不能在 MCN 上完成。

以下是可以使用部分站点软件升级的用法/场景：

验证具有相关更改的软件修补程序是否兼容并适用于特定站点（部分站点升级）。验证升级后的软件是否按预期工作。这有助于验证新软件并在使用新软件升级整个网络之前修复特定站点。

我可以使用此功能从以下方式升级：

- 10.0 到 10.x
- 10.0.x 到 10.0.y
- 11.0 到 11.y
- 11.0.x 到 11.0.y
- 以上所有升级方式

部分站点软件升级仅适用于设备运行 10.x 及更新版本的 软件版本，并且可以在同一主要版本的软件中使用。它可以在 10.0 到 10.0.x/10.x 之间使用。仅作为部分站点软件升级的一部分，无法更改配置。

我可以通过从配置启用它们来测试新功能，作为部分软件升级的一部分进行测试吗？

不，部分软件升级要求现在的 活动 和 暂存 配置相同。只有软件版本才能更改。

我可以 禁用 RCN 的部分软件升级吗？

不，只能从 MCN 启用或禁用部分软件升级。在 RCN 中，该功能处于只读模式。

当我的活动状态为 9.3.x 和 10.0.x 时，我是否可以使用部分软件升级？

否，设备应在版本 10.0 上作为活动软件运行。

如果从 MCN 禁用了 部分软件升级 选项，而某些分支已通过此功能升级，会发生什么情况？

MCN 向网络中的所有设备发送通知，说明 部分软件升级 功能已禁用，然后 MCN 自动更 正网络中的所有设备，以匹配其活动版本和暂存版本。但是，请注意，MCN 期待从“变更管理”的“激活”页面单击“激活暂存”选项。您可以通过单击“激活 已暂存”按钮来激活 网络，或者单击“更改准备”以通过接受确认来取消状态。

更改管理回滚

更改管理过程中的回滚功能是什么？

从版本 9.3 中，更改管理回滚功能启 用在配置更新 后 意外事件（如 t2-app 崩溃或虚拟路径状态）变为非活动 时回滚到工作配置。在配置更新后，如果满足以下条件（前提是用户已启用此功能），网络和设备将被监视 10 分钟，则将激活暂存配置。活动软件将回滚到暂存。

配置回滚以重新启动的条件 是什么？

如果遇到以下情况，则会发生回滚：

1. MCN-配置/软件更改后，如果 t2_app 服务因 30 分钟间隔内崩溃而被禁用。

2. MCN-配置/软件更改后，如果虚拟路径服务在激活后关闭 30 分钟或更长时间。在站点上 启动回滚 功能。
3. 站点-配置/软件更改后，如果站点与 MCN 失去通信，则 启动回滚功能。
4. 站点-在配置/软件更改后，t2_app 服务因 30 分钟内崩溃而被禁用。

回滚后会发生什么？

配置回滚后，错误的配置/软件将 显示为分阶段软件。

如何 通 知用户发生了回滚？

显示 GUI 顶部的黄色横幅，说配置由于相应的错误而回滚。此外，您 可以看到它是更改管理状态表。它显示与发生回滚的站点相对应的 配置错误或软件错误。

配置和软件是否都回滚？

是的，如果软件升级也与配置一起执行，并 遇到回滚方案，则软件也会回滚。

如果 MCN 中出现问题，并且崩溃或失去与所有站点的连接，会发生什么？

除了 MCN 之外，整个网络将回滚。将 显示通知，并且所有站点在更改管理部分显示回滚状态。您 可以手动解决 MCN 上的问题。

我们可以禁用此功能吗？

是的，我们可以在激活前禁用此功能。但是，默认情况下，此功能处于启用状态。

当我有多层网络时，回滚如何与部分软件升级进行交互？

- 如果禁用了部分软件升级，并且区域（或 RCN）中的站点回滚，则出现问题的区域将 被回滚，一旦 完成，回滚会向上传播到 MCN。因此，MCN 和网络的其余部分回滚。回滚区域中的 RCN 和 MCN 都 显示回滚横幅，而 MCN 无法在 RCN 上自动关闭回滚横幅。
- 如果启用了部分软件升级，并且区域（或 RCN）中的站点回滚，则仅回滚该区域。回滚事件 不会 传播回 MCN。因此，MCN 离开该区域。MCN 不显示回滚横幅，也不回滚自身或网络。

在这两种情况下，RCN 会 显 示回滚横幅，直到 它被 解除。因为，它 不能被 MCN 自动解除。

参考资料

September 2, 2022

应用程序签名库

Citrix SD-WAN 设备可以使用深度数据包检查识别的应用程序的列表。