Citrix SD-WAN 11.4

Machine translated content

Disclaimer

Contents

Citrix SD-WAN 11.4.0a 版本的发行说明

November 16, 2022

本发行说明文档介绍了 Citrix SD-WAN 11.4.0a 版本中存在的增强功能和更改、已修复和已知问题。

注意

- 有关安全相关建议的列表，请参阅 Citrix 安全公告。
- Citrix SD-WAN 11.4.0a 版本解决了 https://support.citrix.com/article/CTX319135 中描述的安全漏洞，并取代了 11.4.0 版。除了 11.4.0 版中提供的增强功能和错误修复之外，11.4.0a 版还包含以下错误修复程序-SDWANHELP-2106、SDWANHELP-2078、SDWANHELP-2066、NSSDW-35630、NSSDW-35596 和 NSSDW-34670。
- Citrix SD-WAN 11.4.0 版本是最后一个完全支持 Citrix SD-WAN 中心和 SD-WAN 配置编辑器的主线版本。Citrix SD-WAN Center 和 SD-WAN 配置编辑器均已过时。请注意，弃用是产品/功能被逐步淘汰的先行通知，但现已推出并得到全面支持。在下一个 Citrix SD-WAN 版本系列中，Citrix SD-WAN 中心和 SD-WAN 配置编辑器将被删除且不支持。Citrix 建议您将 Citrix SD-WAN Orchestrator 用于满足所有配置要求。Citrix SD-WAN Orchestrator 支持当前通过 Citrix SD-WAN 中心和 SD-WAN 配置编辑器完成的所有配置。有关更多详细信息，请参阅 Citrix SD-WAN Orchestrator 服务 和 适用于本地的 SD-WAN Orchestrator。

新增功能

11.4.0a 版中提供的增强功能和更改。

配置和管理

备用配置中 WAN 端口的静态 IP 地址的 NITRO Rest API

从 Citrix SD-WAN 11.4.0 版本开始，您可以使用 NITRO REST API 在备用配置中为 WAN 端口配置静态 IP 地址。在现有的回退配置 API 中添加了新参数。

[NSSDW-33255]

Citrix SD-WAN 新的 UI 增强功能

Citrix SD-WAN 新用户界面包括以下增强功能：

- 根据 Citrix 品牌重塑，Citrix SD-WAN 新用户界面的外观和外观已更改，以反映新的颜色和字体。
- 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 会将您重定向到旧版 UI。

- 您可以查看 LACP LAG 界面的详细信息。
- DNS 代理统计信息监控
- SLAAC WAN 链路监控

[NSSDW-30842、NSSDW-28818、NSSDW-32030]

SNMP

添加了以下 SNMP MIB：

- 家电统计
  - 设备使用 CPU 的百分比
  - 设备使用的 RAM 的百分比
- WAN 链接统计表
  - WAN 链路的最大局域网到 WAN 物理速率（以 Kbps 为单位）
  - WAN 链路的最大 WAN 到 LAN 物理速率（以 Kbps 为单位）
  - WAN 链接的局域网到 WAN 允许的费率（以 Kbps 为单位）
  - WAN 链接的 WAN 到局域网允许的费率（以 Kbps 为单位）

[NSSDW-30592]

带内管理

带内管理支持高可用性设备对。高可用性对中的设备使用带内访问相互通信。

[NSSDW-24534]

IPv6 互联网和内联网服务的静态 NAT 策略

将运行 Citrix SD-WAN 11.3.1 版的设备升级到版本 11.4.0 时，必须手动更新 IPv6 互联网/内部网服务的现有静态 NAT 策略。

[NSSDW-33726]

其他

边缘安全组件的补丁升级支持

Citrix SD-WAN 高级版 (AE) 支持修补程序升级机制，该机制允许升级边缘安全子系统。

如果从启用了边缘安全的现有版本升级到更高版本（包括更新版本的边缘安全组件），则只有子系统更新的奇偶校验才会下载和升级。

[NSSDW-26721]

SD-WAN Center 控制板

在 Citrix SD-WAN Center 仪表板上，配置多达 300 个站点时，多区域摘要仪表板可见。

[NSSDW-21753]

网络

班级

Citrix SD-WAN 仅显示那些在虚拟路径和动态虚拟路径上流动流量的类。如果显示一个类并显示 0 作为值，则表示之前流动的流量现在已停止。但是，如果根本不显示某个类，则表示该类从未有任何流量，因为虚拟路径服务状态已重置（例如，软件升级或重新启动）。

[NSSDW-33974]

IPv6 支持 IPFIX

Citrix SD-WAN 支持 IPFIX 的 IPv6 地址。Citrix SD-WAN 使用模板 615 和 616 导出 IPv6 IPFIX 流数据。您可以选择 应用程序流信息 **(IPFIX)** 以根据模板 615 导出数据集。如果导出流数据时出现问题，请选择 基本属性 **(IPFIX)** ，该属性根据模板 616 导出数据。

[NSSDW-29153]

IPv6 对 DNS 代理和 DNS 透明转发器的支持

Citrix SD-WAN 支持用于配置 **DNS** 代理和 **DNS** 透明转发的 IPv6 地址。您可以使用以下 IPv6 DNS 服务类型定义 DNS 代理或 DNS 透明转发：

- **Staticv6**：允许您配置静态 IPv6 DNS 服务器 IP 地址。可以创建内部、ISP、Google 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**：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。每个站点只允许使用一个 Dynamicv6 服务。

[NSSDW-29151]

ECMP 负载平衡

等价多路径 (ECMP) 组允许您对多条路由进行分组，使用相同的成本、目的地和服务类型。ECMP 负载均衡可确保：

- 通过多个等价连接分配流量。
- 最佳利用可用带宽。
- 如果路由无法到达，则动态将流量传输到其他 ECMP 成员路由。
- ECMP 支持 IPSEC/GRE 隧道上的静态路由。
- ECMP 组可以通过虚拟路径和内联网服务组成。

[NSSDW-1238]

平台和系统

Citrix Hypervisor 8.2

从 11.4.0 版本开始，Citrix Hypervisor 8.2 支持 Citrix SD-WAN。

[NSSDW-32037]

Office 365 类别

Citrix SD-WAN 11.4.0 为 允许 和 优化 Office 365 类别提供了更精细的分类，从而启用选择性启动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”类别分为以下子类别：

- 团队实时
- Exchange Online
- SharePoint 优化

允许 类别分为以下子类别：

- 团队 TCP 后备
- 交换邮件
- SharePoint 允许
- Office365 常见

[NSSDW-27324]

Google Cloud Platform 支持具有 HA 和高吞吐量的 SD-WAN SE

您现在可以在 Google Cloud Platform (GCP) 上配置具有高可用性的 SD-WAN SE 实例。GCP 上的 SD-WAN 实例还支持 1 Gbps 的更高吞吐量。

[NSSDW-17179]

有线 802.1X 身份验证

有线 802.1X 是一种身份验证机制，它要求客户端在能够访问 LAN 资源之前进行身份验证。Citrix SD-WAN Orchestrator 服务支持在局域网接口上配置有线 802.1X 身份验证。

在 Citrix SD-WAN 网络中，客户端向 Citrix SD-WAN 设备发送身份验证请求以访问 LAN 资源。Citrix SD-WAN 设备充当身份验证器并将身份验证请求发送到身份验证服务器。Citrix SD-WAN Orchestrator 服务仅支持将 RADIUS 服务器配置为身份验证服务器。

[NSSDW-1921]

已修复的问题

11.4.0a 版中解决的问题。

配置和管理

添加一些网络对象后，配置审核和导出失败。该问题已修复。

[SDWANHELP-2041]

由于允许的内存资源受到限制，将大型网络配置从 Citrix SD-WAN 设备导入 Citrix SD-WAN Center 失败。该问题已修复。

[SDWANHELP-2034]

Citrix SD-WAN 的电子邮件通知在 **AUTH** 命令中添加了额外的“CR”字符，从而导致 SMTP 会话终止。

[SDWANHELP-2028]

在大型网络的数据库存档期间，MCN 设备上的统计记录在几分钟内没有插入到统计数据库表中。

[SDWANHELP-1872]

在接口更改期间，VRRP 可能仍会使用旧的接口数据，这可能会导致核心转储。

[SDWANHELP-1867]

当防火墙虚拟机处于关闭状态时，本地 GUI 上的托管防火墙配置不会加载。

[SDWANHELP-1839]

配置虚拟 IP 地址时，不能将 备份管理网络 选择为“无”。

[SDWANHELP-1824]

配置编辑器的“基本”部分下的“公共 **IPv4** 地址”字段显示为灰色。

[SDWANHELP-1780]

虽然在分支广域网链路上启用了公共 IP 地址学习，但在以下情况下，RCN 可能无法学习新的公有 IP 地址并导致死路：

- 分支和 RCN 之间存在配置版本不匹配
- 分支 WAN 链接的公有 IP 地址已更改

[SDWANHELP-1580]

当设备管理端口配置了 DHCPv4 时，切换到静态 IPv4 地址将失败。

[NSSDW-35630]

如果设备同时配置了 DHCP IPv4 和 DHCP IPv6 地址，但网络只配置了 DHCP IPv6 服务器，则设备会继续等待 DHCP IPv4 地址，因此不会同时分配 IPv6 地址。

[NSSDW-33741]

为区域控制节点 (RCN) 网络创建的自动生成的摘要路由的成本为 30,000，而不是 65534。

[NSSDW-32629]

从 Citrix SD-WAN 中心推送设备设置时，不会应用于 Citrix SD-WAN。

[NSSDW-32257]

在旧版 UI 中启用和禁用外部调制解调器不起作用。

[NSSDW-32221]

配置过程中的审计错误会阻止用户在站点上配置 Internet 服务，除非所有 WAN 链接都配置了相同 IP 类型的访问接口。

[NSSDW-32185]

配置为 DHCP 客户端的 WAN 链路会导致虚拟路径故障。当 WAN 链接的名称发生更改且更改管理受到影响时，就会出现此问题。

[NSSDW-32110]

许可证

在 Citrix SD-WAN 110 和 210 平台上，如果管理端口配置为数据端口，则升级到较新版本后 主机 **ID** 可能会更改。如果出现此问题，SD-WAN 设备将使用宽限许可证。

[SDWANHELP-1866]

其他

克隆具有多个 HA 接口的站点时，不会克隆第二个 HA 接口 IP 地址。

[SDWANHELP-2005]

Citrix SD-WAN Center GUI 日志占用过多的磁盘空间，导致升级和 STS 失败。

[SDWANHELP-1960]

当您以全屏模式在浏览器上查看 Citrix SD-WAN Center 11.3.0 登录页面时，Citrix 徽标和产品名称将无法正确显示。

[SDWANHELP-1910]

网络管理员角色有权执行特定于安全管理员角色的活动，根据网络管理员角色的定义，这些活动不得允许。

[SDWANHELP-1906]

Citrix SD-WAN Center 上导入和导出 大型网络配置（当配置文件大小超过 16 MB 时）失败。

[SDWANHELP-1787]

Citrix SD-WAN Center 电子邮件通知在 **AUTH** 命令中添加了一个额外的 CR 字符，这会导致 SMTP 会话终止。

[SDWANHELP-1736]

Qualys 安全扫描程序工具导致 Citrix SD-WAN 设备的其中一项服务消耗较高的内存，导致设备无响应和重新启动。该问题已修复。

[SDWANHELP-1530]

当 Edge Security 防病毒和反恶意软件组件的内部许可证到期时，Citrix SD-WAN 将停止检测病毒和恶意软件。

[NSSDW-35596]

在执行重新身份验证时，Wi-Fi 客户端报告中的上传和下载数据将显示负值。

[NSSDW-31903]

要使 Citrix SD-WAN Orchestrator 本地管理随 11.2.1 或 11.2.2 软件提供的 SD-WAN 设备，必须将 SD-WAN 设备软件升级到 11.3.0 版本。

[NSSDW-31612]

网络

升级到 Citrix SD-WAN 11.3.1 后，当最大传输单元 (MTU) 大小设置为 1492 字节时，使用 PPPoE 进行 MSS（最大分段大小）夹紧失败。

[SDWANHELP-2048]

启用带内管理并且 RADIUS 服务器可通过数据平面访问时，Wi-Fi WPA2-企业身份验证将失败。

[SDWANHELP-2032]

应用程序路由、QoS 或 DNS 功能的应用程序标识相关条目会定期添加到第一个数据包分类器 (FPC) 哈希表中。当已过时的条目从表中移出时，在某些情况下，Citrix SD-WAN 设备可能会崩溃。

[SDWANHELP-1980]

当局域网端或通过本地服务收到的需要分段的数据包通过 LAN GRE 发送时，SD-WAN 服务崩溃。

[SDWANHELP-1846]

对于路径 MTU 发现，路径 MTU 探测事件会在计时器启动期间入队进行处理。如果尝试实际执行时探测事件无效，则会发生分段失败。

[SDWANHELP-1754]

对于非默认路由域中的 Internet 服务路由并配置了路径资格，当路径出现故障且未配置给定路由域的远程站点时，互联网路由不会被标记为无法访问。

[SDWANHELP-1400]

加载包含摘要路由的 Citrix SD-WAN 配置时，设备可能会持续重新加载。

[NSSDW-34670]

如果设备有配置为总结路由的静态路由，并且动态学习了另一个相同的前缀路由，则总结路由不会总结路由。

[NSSDW-34355]

添加导入过滤器以删除以前导入的 OSPF/BGP 路由可能会导致服务崩溃。

[NSSDW-34207]

一旦 SLAAC 从路由器获知 IP 和网关地址，除非当前地址过期，否则如果网关发生变化或我们更改网段，SLAAC 将不会重新获取 IP，即使在重新启动 SD-WAN 设备之后也是如此。移动端口时，这可能会延迟获取地址。

[NSSDW-33807]

一旦 SLAAC 从路由器获悉 IP 和网关地址，如果网关发生变化（除非当前地址过期），SLAAC 将不会重新获取网关。

示例：

- 分支设备从网关-1 学习其 IP 和网关。
- 网络管理员决定用新的网关-2 替换网关-1。管理员配置网关-2 与网关-1 相同，以便路由器通告发送的前缀信息与网关-1 发送的前缀信息相同。但是，网关-2 的源地址与网关-1 不同。
- 分支设备不会自动学习网关-2 的 IP。（除非和直到当前地址超时）

[NSSDW-33802]

配置更新可能会导致无法启动托管在前缀委派 LAN 虚拟网络接口上的 DHCP 服务器。Citrix SD-WAN 11.3.1 版本不支持前缀委派。

[NSSDW-33664]

在具有代理 NDP 的 Internet 或 Intranet 服务上启用静态 NAT 可能会导致 SD-WAN 响应网络中其他主机拥有和使用的地址的 NDP。

[NSSDW-33653]

Citrix SD-WAN 11.3.1 版本不支持底层站点诊断带宽测试。

[NSSDW-33597]

在具有 IPv6 访问接口的 WAN 链接上启用 Internet 服务时，配置更新后可能会发生服务中断。

[NSSDW-32212]

Citrix SD-WAN 11.3 版本中的 Wi-Fi 功能不支持高可用性 (HA)。

[NSSDW-32197]

如果在启用了互联网负载平衡的 Internet 服务上同时使用 IPv4 和 IPv6，动态 NAT 可能无法正常工作或在配置更新期间导致服务中断。

[NSSDW-32139]

LTE 接口上的 DHCPv4 和 DHCPv6 模式可能会导致 SD-WAN 设备在配置更新后丢失 IP 地址。

[NSSDW-31998]

平台和系统

当 Citrix SD-WAN 4000 设备升级到 11.3.0、11.3.1 或 11.4.0 时，SD-WAN 服务可能会由于竞争条件而失败。

[SDWANHELP-2106]

在配置更新期间执行筛选器策略规则验证，以区分新创建的规则与已修改的规则。由于缺少“match_type”的比较检查，大多数与互联网的连接都被防火墙屏蔽为“O_DENIED”
。解决方法是将默认规则从“拒绝”更改为“丢弃”。

[SDWANHELP-2078]

启用 HDX 报告并且存在通过 Citrix SD-WAN 设备运行的 HDX 流量时，Citrix SD-WAN 设备偶尔可能会观察核心转储。

[SDWANHELP-1957]

使用 CLI 转储防火墙 NAT 信息时，设备崩溃。

[SDWANHELP-1901]

启用透明 DSN 转发后，处理大型 DNS 响应数据包可能会因为没有适当的边界条件检查而导致堆栈溢出。一个使用案例是云服务可能需要从 DNS 学习 IP 才能启用 Office 365 默认类别的分类。

[SDWANHELP-1891]

防火墙规则允许在不受信任的接口上接收 ICMP ping 请求，但会丢弃 ping 响应，因此 SD-WAN 服务崩溃。

[SDWANHELP-1865]

将 Citrix SD-WAN 设备升级到 11.2.2 版本后，由于 SD-WAN 设备发送的 VRRP 通告数据包大小错误，多个 VRRP 设备充当 主 设备。

[SDWANHELP-1804]

在创建动态虚拟路径 (DVP) 期间，如果协议消息带有意外的 IP 类型服务 (TOS) 值到达，则可能会导致核心转储。

[SDWANHELP-1783]

当在同一子网中创建两个虚拟 IP 地址（一个私有，另一个非私有）时，会出现问题：为同一子网创建了两条路由，而子网未通告到远程站点。

[SDWANHELP-1739]

当 GRE 隧道可达性从向上变为向下时，符合 GRE 隧道条件的 GRE 隧道路由不会随可达性状态的变化进行更新。

[SDWANHELP-1623]

使用命令行界面 (CLI) 启动的 SSH 会话的硬编码空闲超时值为 120 分钟。超时期的较长时间似乎 SSH 会话没有超时。通过在 GUI 中添加新配置来配置 SSH 超时值（5—9999 分钟），该问题已得到修复。

[SDWANHELP-1622]

在 Azure HA 部署中，在 WAN 链接上配置辅助访问接口时，SD-WAN 路径不会出现。

[SDWANHELP-1578]

如果为 IPv4 和（或）IPv6 启用了数据包数据协议 (PDP)，某些运营商只允许 IPv6 数据会话。

[SDWANHELP-1777]

已知问题

11.4.0a 版中存在的问题。

配置和管理

如果用于配置规则的应用程序已弃用，则升级后，GUI 将在不同的应用程序下显示相同的规则。

[NSSDW-34618]

如果连接了带外管理接口，则只能从设备 UI 更新 DNS 设置。

如果配置了带内管理，则使用设备 UI 更新的 DNS 设置不会生效。您只能从 Citrix SD-WAN Orchestrator 服务 UI 更新 DNS 设置。

[NSSDW-33932]

VPX 分支将进入单站点模式，如果新置备的虚拟机首先降级，然后再升级回配置虚拟机的版本。

解决方法：

在受影响的分支上执行本地变更管理。

[NSSDW-29513]

其他

当您在 Citrix SD-WAN Center 中添加新本地用户时，将显示黄色横幅，其中包含一条消息，提示防火墙访问 已从“启用”更改为“已 禁用”。

[SDWANHELP-1737]

站点级警报下不会报告 WPA3 失败的身份验证。

[NSSDW-32053]

网络

在 SD-WAN 站点中频繁更改路由表以及配置更新或动态路由清除可能会导致远程站点中的路由同步问题。

[SDWANHELP-2043]

对防火墙动态 NAT 策略或端口转发规则进行的配置更改可能会导致核心转储。

[NSSDW-34603]

平台和系统

在以下平台上，如果启用 HDX 报告，如果将连接归类为 HDX 并开始报告统计信息后出现解析错误，则在有新的 HDX 连接时，设备崩溃：

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

[SDWANHELP-1882]

对 **Citrix SD-WAN 110 SE** 网络问题进行故障排除

November 1, 2021

本节介绍 Citrix SD-WAN 110 SE 设备的网络连接问题以及故障排除说明。

症状

在以下情况下，Citrix SD-WAN 110 SE 设备无法建立网络连接。

- 设备由 SD-WAN Orchestrator 管理和/或由零接触部署 (ZTD) 启动。
- 设备处于出厂状态，未安装 ZTD/SD-WAN Orchestrator 代理。
- 装置时间（CMOS 或硬件）早于实际时间。
- 在下载/安装 ZTD/SD-WAN Orchestrator 代理之前，设备时间由 NTP 守护程序向后设置。

解决方法

首次安装后（或将设备重置为原始出厂配置后），安装 SD-WAN 110 的最终用户必须验证设备是否已成功连接到组织网络。必须向最终用户提供组织特定的说明以及设备（例如，VoIP 电话上的拨号音），以验证网络连通性。如果设备未连接到网络，最终用户可以按照以下说明进行操作：

1. 保持设备通电并等待 30 分钟或更长时间。
2. 短暂但用力地按下电源按钮（1-2 秒钟）将其关闭。
3. 设备上的指示灯变暗后，再次按下电源按钮以重新打开设备。SD-WAN 110 设备现在重新启动并连接到网络。

Citrix SD-WAN 的发行说明 11.4.1 版本

November 1, 2021

本发行说明文档介绍了 Citrix SD-WAN 11.4.1 版本中存在的增强功能和更改以及已修复的问题和已知问题。

注意

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

11.4.1 版中提供的增强和更改。

配置和管理

DHCP 服务器

每个虚拟接口生成一个中继代理，每个中继代理总共可配置 16 台 DHCP 服务器。一个站点上最多可以配置 16 个中继代理。

[NSSDW-34083]

在 DHCP 客户端消息中用作选项 12 的主机名

从 Citrix SD-WAN 11.4.1 版起，主机名与站点名称相同。当管理接口充当 DHCP 客户机时，DHCP 客户端消息中将主机名作为选项 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**。

[NSSDW-32523]

平台和系统

AT 命令

支持 LTE 的 Citrix SD-WAN 平台型号支持运行 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。

[NSSDW-35671]

访问 shell 命令

您可以在 SD-WAN CLI 控制台上直接运行 `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。仅管理员帐户用户支持此功能。

[NSSDW-34942]

参考资料-应用程序签名库

DPI 应用程序签名库已更新。

[NSSDW-34527]

已修复的问题

11.4.1 版中解决的问题。

配置和管理

在 Citrix SD-WAN Center 中，当获取所有属性且选定的时间间隔大于一小时时时，路径和虚拟路径的报告 API 将失败。

[SDWANHELP-2231]

在极少数情况下，Citrix SD-WAN 设备可能会由于内部进程问题而失去管理访问权限。

[SDWANHELP-2179]

在使用 LTE 接口克隆站点时，UI 要求输入 LTE WAN Link 访问接口的静态 IP 地址。审核后，系统会认为配置不正确，并显示以下审计错误：

EC601、EC343 和 EC346

[SDWANHELP-2177]

每次从 Citrix SD-WAN Center 导出配置后，**tmpfolder** 中的临时文件都没有得到清理。

[SDWANHELP-2057]

Citrix SD-WAN UI 不会在配置 **>** 虚拟 **WAN >** 查看配置 **>** 路径下完全显示路径配置。只显示部分路径，其他路径被隐藏。

[SDWANHELP-2050]

如果在启用了 AppFlow 的 HDX 设置中添加 TCP 选项，则不会建立 TCP 连接。

[SDWANHELP-1741]

当设备管理端口配置了 DHCPv4 时，切换到静态 IPv4 地址将失败。

[NSSDW-35630]

当用户已禁用调制解调器并希望在操作模式切换到之前重新启用调制解调器时，会出现此问题 `Lower Power`。解决方法是在执行启用/禁用操作 `Operating Mode` 之前向用户发出警告并显示当前信息。

[NSSDW-25067]

安装和升级

当 MPLS WAN 链接配置为使用 WAN 链接模板并为 Intranet /Internet 服务启用时，编译配置时会出现意外的审计错误 EC14203。

当使用 WAN 链接模板配置 MPLS WAN 链接时，将 WAN 链接允许速率设置为低于使用 WAN 链接的所有服务所需的最小预留带宽的值时，Citrix SD-WAN 11.3.1 及更早版本可能不会引发错误。升级到 Citrix SD-WAN 11.3.2 或更高版本时，将显示错误。在执行升级之前，请设置正确的 WAN 链路允许速率并激活配置。

[SDWANHELP-2134]

其他

查询 WAN 链接统计信息时，Citrix SD-WAN 中心监控 REST API 不起作用。

[SDWANHELP-2274]

在 Citrix SD-WAN Center 中导入新配置时，不会导入 Zscaler 配置。

[SDWANHELP-2137]

当 Edge Security 防病毒和反恶意软件组件的内部许可证到期时，Citrix SD-WAN 将停止检测病毒和恶意软件。

[NSSDW-35596]

网络

当 GRE 流具有 IPv4 源 IP 地址和 IPv6 目标 IP 地址时，IPv4 GRE 隧道流量可能会被错误分类为 监控 **>** 流量下的 **IPv6** 隧道流 量并被阻止。

[SDWANHELP-2214]

升级到 Citrix SD-WAN 11.3.1 后，当最大传输单元 (MTU) 大小设置为 1492 字节时，使用 PPPoE 进行 MSS（最大分段大小）夹紧失败。

[SDWANHELP-2048]

在 SD-WAN 站点中频繁更改路由表以及配置更新或动态路由清除可能会导致远程站点中的路由同步问题。

[SDWANHELP-2043]

当 Citrix SD-WAN 设备无法检测到新端口 DEAD 时，WAN 链接路径状态将转换为。

[SDWANHELP-1998]

在极少数情况下，当路由表中发生路由更改时，Citrix SD-WAN 服务会重新加载。

[NSSDW-36289]

启用 CRL 处理后，第三方加密库中的内存问题可能会导致核心转储。

[NSSDW-35679]

加载包含摘要路由的 Citrix SD-WAN 配置后，设备可能会持续重新加载。

[NSSDW-34670]

在以下情况下，当删除两个站点之间的静态虚拟路径时，不会删除通过已删除的静态虚拟路径获知的路由：

- 作为配置更改的一部分，静态虚拟路径将被删除。
- 将新的 Geo-MCN 设为客户端后，旧的 Geo MCN 和分支之间的静态虚拟路径将被删除。

[NSSDW-34655]

平台和系统

当动态虚拟路径 (DVP) 启动时生成 STS 捆绑包时，Citrix 虚拟 WAN 服务可能会重新启动。

[SDWANHELP-2123]

当 Citrix SD-WAN 4000 设备升级到 11.3.0、11.3.1 或 11.4.0 时，SD-WAN 服务可能会由于竞争条件而失败。

[SDWANHELP-2106]

当站点名称包含“完 成”字符串时，旧版 UI 仪表板上的“系统状态”部分将显示以下错误消息。

```
Unable to obtain system data because the system is busy. Click
Refresh to retry.
```

[SDWANHELP-2098]

在配置更新期间执行筛选器策略规则验证，以区分新创建的规则与已修改的规则。由于缺少 **match_type** 的比较检查，大多数与互联网的连接都以 **O_DENIED** 的身份被防火墙阻止。

[SDWANHELP-2078]

从 SD-WAN Orchestrator 或 SD-WAN Branch 设备获取应用程序路由的实时统计信息时，设备将失去连接并观察到崩溃。只有当应用程序路由的数量超过 16 个时才会发生这种情况（包括自动生成的应用程序路由）。

[SDWANHELP-2066]

已知问题

11.4.1 版中存在的问题。

配置和管理

用于切换“监视” > “流量”页面下显示的列的选项未按预期运行。尽管选择或筛选了列，但仍会显示以下消息：

```
Please select at least one column.
```

[SDWANHELP-2272]

其他

Zscaler 配置更改管理流程的超时时间为两个小时。当出现配置错误时，整个进程将停止两个小时。

[SDWANHELP-2249]

站点级警报下不会报告 WPA3 失败的身份验证。

[NSSDW-32053]

网络

在极少数情况下，如果分支站点的其中一个 WAN 链接具有静态公共 IP 地址，则动态虚拟路径的形成将失败。

解决办法：使用静态公有 IP 地址在分支站点重新启动虚拟 WAN 服务。

[NSSDW-36429]

在 Citrix SD-WAN BGP 配置中，更改路由域的路由器 ID 时，SD-WAN 动态路由协议可能会重新启动。

[NSSDW-35657]

对防火墙动态 NAT 策略或端口转发规则进行的配置更改可能会导致核心转储。

[NSSDW-34603]

平台和系统

当 QMI 代理进程处于失效状态时，LTE 调制解调器会持续重新启动。

解决办法：重新启动设备。

[SDWANHELP-2270]

Citrix SD-WAN 11.4.2a 版本的发行说明

February 10, 2022

本发行说明文档介绍了 Citrix SD-WAN 版本 Build 11.4.2a 中存在的增强功能和更改、已修复问题和已知问题。

备注

- 有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。
- Citrix SD-WAN 11.4.2a 版本解决了 https://support.citrix.com/article/CTX330728 中描述的安全漏洞，并取代了 11.4.2 版。除了 11.4.2 版中提供的增强功能和错误修复外，11.4.2a 版还包含以下错误修复-SDWANHELP-2480 和 SDWANHELP-2456。

新增功能

Build 11.4.2a 中提供的增强功能和更改。

其他

带内管理

从 Citrix SD-WAN 11.4.2a 版本起，必须在 SD-WAN 设备上配置带内管理，才能通过带内管理端口建立与 Citrix SD-WAN Orchestrator 服务的连接。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。

[NSSDW-37174]

LTE 接口

现在，您可以使用 Citrix SD-WAN Orchestrator 服务将基于 LTE 接口的广域网链接配置为专用内联网 WAN 链接。通过此增强功能，您可以灵活地将 LTE 接口配置为公共互联网 WAN 链接或专用内联网 WAN 链接。

[NSSDW-37064]

Orchestrator 连接状态

SD-WAN 仪表板的新用户界面显示以下 Orchestrator 连接状态：

- 联机状态
- 服务状态
- DNS 状态
- 本地网关状态
- 失败原因
- 连接方式

[NSSDW-36434]

平台和系统

域和应用程序

基于域名的应用程序现在支持 Citrix SD-WAN Orchestrator 服务中的可配置端口和协议。选中 配置端口 复选框后，可以根据需要编辑、添加或删除任何端口或端口范围。此外，您还可以将协议更改/选择为 TCP、UDP 或任意。以前（在禁用配置端口复选框的情况下），分组在应用程序下的域仅支持端口 **80** 和 **443** 以及协议 **Any**。

[NSSDW-29930]

已修复的问题

内部版本 11.4.2a 中解决的问题。

其他

当基于域名的应用程序的 DNS 学习条目导致第一个数据包分类表达到最大限制时，设备崩溃。

[SDWANHELP-2480]

当流量一直很高且超过设备的最大流量容量限制时，流量映射的更改有时可能会导致数据路径重新启动。

[SDWANHELP-2456]

对于带有 VLAN 标记的未加密路径（例如 HA 控制路径），某些 SD-WAN 控制数据包使用错误的以太网标头发送，从而导致路径不稳定或失效。

[SDWANHELP-2384]

部署没有任何分支的独立 RCN 时会显示审计错误 ID。

[SDWANHELP-2381]

当从 Citrix SD-WAN Orchestrator 服务启用互联网服务的 ICMP 探测器时，如果互联网广域网链接断开，则在以下设备上重新启动 SD-WAN 服务

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

[SDWANHELP-2378]

CCitrix SD-WAN Center 仪表板不会加载任何信息。

[SDWANHELP-2373]

在通过更改管理流程将更改从 MCN 推送到网络设备的同时，设备上的 SD-WAN 服务重新启动断开设备连接约 2 分钟。

[SDWANHELP-2366]

无法为 Citrix SD-WAN 5100 型号配置 LAG 组。

[SDWANHELP-2339]

无法在支持 PE 的 Citrix SD-WAN 设备型号上下载 PAC 文件。

[SDWANHELP-2336]

关闭路径加密后，路径中会观察到高 MTU 和丢失。

[SDWANHELP-2327]

在 SD-WAN Orchestrator HA 设置中，当设备软件从低于 11.3.0 的版本升级到版本 11.4.1、11.3.2 或更低版本时，备用设备会崩溃。

[SDWANHELP-2315]

站点的丢包率逐渐增加，该站点的虚拟路径与其他远程站点之间已失效，WAN 链路配置为待机模式，并禁用了检测信号。

[SDWANHELP-2276]

用于切换“监视”**>**“流量”页面下显示的列的选项未按预期运行。尽管选择或筛选了列，但仍会显示以下消息：

请至少选择一列。

[SDWANHELP-2272]

当 QMI 代理进程处于失效状态时，LTE 调制解调器会持续重新启动。

[SDWANHELP-2270]

使用 TACACS+ 身份验证建立与 SD-WAN 的 SSH 连接时，会向同一用户发送多个身份验证请求，从而导致日志记录过多。

[SDWANHELP-2087]

当 SMTP 服务器名称设置为 FQDN 时，无法发送电子邮件通知。DNS 服务器包含以下内容时会出现此问题：

- FQDN 至少有 2 条 IPv4 A 记录。
- FQDN 至少有 1 条 IPv6 AAAA 记录。

[SDWANHELP-2027]

在极少数情况下，当路由表中发生路由更改时，Citrix SD-WAN 服务会重新加载。

[NSSDW-36289]

启用 CRL 处理后，第三方加密库中的内存问题可能会导致核心转储。

[NSSDW-35679]

当 Edge Security 防病毒和反恶意软件组件的内部许可证到期时，Citrix SD-WAN 将停止检测病毒和恶意软件。

[NSSDW-35596]

加载包含摘要路由的 Citrix SD-WAN 配置时，设备可能会持续重新加载。

[NSSDW-34670]

如果设备有配置为总结路由的静态路由，并且动态学习了另一个相同的前缀路由，则总结路由不会总结路由。

[NSSDW-34355]

如果网络中的 DNS 代理使用重复名称，Citrix SD-WAN UI 将显示错误。

[NSSDW-33842]

一旦 SLAAC 从路由器获知 IP 和网关地址，除非当前地址过期，否则如果网关发生变化或我们更改网段，SLAAC 将不会重新获取 IP，即使在重新启动 SD-WAN 设备之后也是如此。移动端口时，这可能会延迟获取地址。

[NSSDW-33807]

一旦 SLAAC 从路由器获悉 IP 和网关地址，如果网关发生变化（除非当前地址过期），SLAAC 将不会重新获取网关。

示例：

- 分支设备从网关-1 学习其 IP 和网关。
- 网络管理员决定用新的网关-2 替换网关-1。管理员配置网关-2 与网关-1 相同，以便路由器通告发送的前缀信息与网关-1 发送的前缀信息相同。但是，网关-2 的源地址与网关-1 不同。
- 分支设备不会自动学习网关-2 的 IP。（除非和直到当前地址超时）

[NSSDW-33802]

为区域控制节点 (RCN) 网络创建的自动生成的摘要路由的成本为 30,000，而不是 65534。

[NSSDW-32629]

从 Citrix SD-WAN 中心推送设备设置时，不会应用于 Citrix SD-WAN。

[NSSDW-32257]

已知问题

11.4.2a 版中存在的问题。

其他

SD-WAN WANOP UI 上的 **ICA** 连接 页面显示错误，该页面不显示任何连接。

[SDWANHELP-2431]

如果将带外端口用于 SNMP 服务的装置切换到带内端口，则该装置的所有管理服务都将通过带内端口连接到 Internet。发送到带外端口的 SNMP 请求失败。

解决办法：配置外部 SNMP 服务，以便在带外端口出现故障时向带内端口发送请求。

[SDWANHELP-2358]

无法在 VMware Hypervisor 上安装 Citrix SD-WAN VPX。AMD Opteron(tm) 或较早版本的 AMD 处理器不支持 Citrix SD-WAN VPX。Citrix SD-WAN 已通过认证，建议仅在 AMD EPYC 处理器上使用。

[SDWANHELP-2309]

同时启动实时、交互式高、交互式介质和交互式低类类型的流量时，UI 的“监视类”表中显示的流量速率大约降低 150 Kbps。

[NSSDW-37568]

当管理端口上配置的 DNS 无效或无法访问时，由于 DNS 解析错误，设备将无法连接到 SD-WAN Orchestrator 服务，即使带内配置了 DNS 代理和互联网服务

解决办法：在管理端口上配置有效的 DNS，或者清除 DNS，让其使用默认配置的 DNS (9.9.9.9)。

[NSSDW-37467]

对于通过 MCN 管理的 Citrix SD-WAN 设备，新用户界面仪表板中的 Orchestrator 连接状态显示为不良/未知。

[NSSDW-37462]

当无法访问 LTE 加密狗或管理端口提供的 DNS 时，即使网络已切换到带内管理进行连接，Citrix SD-WAN Orchestrator 服务连接也会失败。

[NSSDW-37428]

在极少数情况下，如果分支站点的其中一个 WAN 链接具有静态公共 IP 地址，则动态虚拟路径的形成将失败。

解决办法：

使用静态公共 IP 地址在分支站点重新启动虚拟 WAN 服务。

[NSSDW-36429]

在 Citrix SD-WAN BGP 配置中，更改路由域的路由器 ID 时，SD-WAN 动态路由协议可能会重新启动。

[NSSDW-35657]

对防火墙动态 NAT 策略或端口转发规则进行的配置更改可能会导致核心转储。

[NSSDW-34603]

站点级警报下不会报告 WPA3 失败的身份验证。

[NSSDW-32053]

Citrix SD-WAN 11.4.2b 版本的发行说明

June 8, 2022

本发行说明文档介绍了 Citrix SD-WAN 版本 Build 11.4.2b 的增强功能和更改、已修复的问题和已知问题。

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。
- 除了 11.4.2a 版中提供的增强功能和错误修复外，11.4.2b 版本还包含以下错误修复-SDWANHELP-2594。

新增功能

版本 11.4.2b 中提供的增强功能和更改。

LTE 接口

现在，您可以使用 Citrix SD-WAN Orchestrator 服务将基于 LTE 接口的广域网链接配置为专用内联网 WAN 链接。此增强功能提供了将 LTE 接口配置为公共互联网 WAN 链路或专用内联网 WAN 链路的灵活性。

[NSSDW-37064]

Orchestrator 连接状态

SD-WAN 的新用户界面仪表板显示以下 Orchestrator 连接状态：

- 联机状态
- 服务状态
- DNS 状态
- 本地网关状态
- 失败原因
- 连接方式

[NSSDW-36434]

设备设置

Citrix SD-WAN Orchestrator 服务引入了一个用于配置管理网络优先级的选项。您可以选择带内或带外作为网络的管理接口。仅当 SD-WAN 设备运行的软件版本为 11.4.2 或更高版本时，此选项才可用。

[NSSDW-35774]

Citrix SD-WAN 软件版本 11.4.2 及更高版本支持使用适用于本地 SD-WAN Orchestrator 的 IPv6 管理连接。

[NSSDW-35647]

平台和系统

基于域名的应用程序现在支持 Citrix SD-WAN Orchestrator 服务中的可配置端口和协议。选中 配置端口 复选框后，可以根据需要编辑、添加或删除任何端口或端口范围。此外，您还可以将协议更改/选择为 TCP、UDP 或任意。以前（在禁用配置端口复选框的情况下），应用程序下分组的域仅支持端口 80 和 443 以及协议 **Any**。

[NSSDW-29930]

已修复的问题

在 Build 11.4.2b 中解决的问题。

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

[SDWANHELP-2594]

当基于域名的应用程序的 DNS 学习条目导致第一个数据包分类表达到最大限制时，设备崩溃。

[SDWANHELP-2480]

当流量一直很高且超过设备的最大流量容量限制时，流量映射的更改有时可能会导致数据路径重新启动。

[SDWANHELP-2456]

对于带有 VLAN 标记的未加密路径（例如 HA 控制路径），某些 SD-WAN 控制数据包使用错误的以太网标头发送，从而导致路径不稳定或失效。

[SDWANHELP-2384]

部署没有任何分支的独立 RCN 时会显示审计错误 ID。

[SDWANHELP-2381]

从 Citrix SD-WAN Orchestrator 服务启用 ICMP 探测 Internet 服务时，如果 Internet WAN 链接断开，SD-WAN 服务将在以下设备上重新启动-

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

[SDWANHELP-2378]

CCitrix SD-WAN Center 仪表板不会加载任何信息。

[SDWANHELP-2373]

在通过更改管理流程将更改从 MCN 推送到网络设备的同时，设备上的 SD-WAN 服务重新启动断开设备连接约 2 分钟。

[SDWANHELP-2366]

无法为 Citrix SD-WAN 5100 型号配置 LAG 组。

[SDWANHELP-2339]

无法在支持 PE 的 Citrix SD-WAN 设备型号上下载 PAC 文件。

[SDWANHELP-2336]

关闭路径加密后，路径中会观察到高 MTU 和丢失。

[SDWANHELP-2327]

在 SD-WAN Orchestrator HA 设置中，当设备软件从低于 11.3.0 的版本升级到 11.4.1、11.3.2 或更低版本时，备用设备崩溃。

[SDWANHELP-2315]

站点的丢包率逐渐增加，该站点的虚拟路径与其他远程站点之间已失效，WAN 链路配置为待机模式，并禁用了检测信号。

[SDWANHELP-2276]

用于切换“监视” > “流量”页面下显示的列的选项未按预期运行。尽管选择或筛选了列，但仍会显示以下消息：

请至少选择一列。

[SDWANHELP-2272]

当 QMI 代理进程处于失效状态时，LTE 调制解调器会持续重新启动。

[SDWANHELP-2270]

使用 TACACS+ 身份验证建立与 SD-WAN 的 SSH 连接时，会向同一用户发送多个身份验证请求，从而导致日志记录过多。

[SDWANHELP-2087]

当 SMTP 服务器名称设置为 FQDN 时，无法发送电子邮件通知。DNS 服务器包含以下内容时会出现此问题：

- FQDN 至少有 2 条 IPv4 A 记录。
- FQDN 至少有 1 条 IPv6 AAAA 记录。

[SDWANHELP-2027]

在 Citrix SD-WAN 11.4.2 版本中，对于扩展名为.der 的文件，从适用于本地的 Citrix SD-WAN Orchestrator 上载签名的 CSR 证书失败。

[NSSDW-37813]

当无法访问 LTE 加密狗或管理端口提供的 DNS 时，即使网络已切换到带内管理进行连接，Citrix SD-WAN Orchestrator 服务连接也会失败。

[NSSDW-37428]

带内管理

从 Citrix SD-WAN 11.4.2 版本起，必须在 SD-WAN 设备上配置带内管理，才能通过带内管理端口建立与 Citrix SD-WAN Orchestrator 服务的连接。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。

[NSSDW-37174]

当 DHCP 服务器使用 DVP 和 HA 配置分配新地址时，Citrix SD-WAN 服务可能会崩溃。

[NSSDW-36513]

如果网络中的 DNS 代理使用重复名称，Citrix SD-WAN UI 将显示错误。

[NSSDW-33842]

平台和系统

首次添加自定义 SNMP 团体字符串不会删除现有的团体字符串配置。

[SDWANHELP-2561]

已知问题

版本 11.4.2b 中存在的问题。

其他

如果禁用了部分站点升级，然后将整个网络升级到新的软件版本，某些站点可能会自动更正回较旧的版本。

解决方法：如果触发了另一项更改管理，降级的站点将升级到预期的软件版本。

[SDWANHELP-2586]

旧版 GUI 将 CGI 会话文件保留在临时目录下。这些 CGI 会话将在启动期间清理，这可能会阻止 Citrix SD-WAN 服务运行。

解决方法：按住电源按钮 4 秒以上重新启动设备，然后重新打开盒子的电源，或者拔下电源线并在几秒钟后重新插入。

[SDWANHELP-2567]

由于 LTE 调制解调器事务超时错误，Citrix SD-WAN LTE 服务可能会挂起。

解决方法：重新启动设备。

[SDWANHELP-2565]

由于 Citrix SD-WAN UI 中出现罕见的争用情况，当使用错误的数据库索引请求统计信息时，t2_app 将崩溃。

[SDWANHELP-2548]

在 Citrix SD-WAN 1100 上分配给 Palo Alto VM（VM-50 型）的内存增加到 5.5 GB。

[SDWANHELP-2534]

修复 ICA 分类中可能存在的内存泄漏问题。

[SDWANHELP-2527]

在具有 Internet 负载平衡配置的 Advanced Edition (AE) 平台上，Citrix SD-WAN 服务有时可能会崩溃。

解决方法：将 Internet 服务配置为主模式和辅助模式。

[SDWANHELP-2521]

Citrix SD-WAN 设备仅允许传输管理端口上所需的流量，这会阻止用户在启用时访问 MiRIC 管理 GUI。

[SDWANHELP-2479]

尝试输入带前缀的 **IP** 地址未通过防火墙过滤器策略中的源/目标 IP 字段的验证。

[SDWANHELP-2471]

如果将带外端口用于 SNMP 服务的装置切换到带内端口，则该设备的所有管理服务都将通过带内端口连接到 Internet。发送到带外端口的 SNMP 请求失败。

解决办法：配置外部 SNMP 服务，以便在带外端口出现故障时向带内端口发送请求。

[SDWANHELP-2358]

在 Citrix SD-WAN 11.4.2 版本中，对于扩展名为.der 的文件，从适用于本地的 Citrix SD-WAN Orchestrator 上载签名的 CSR 证书失败。

解决方法：此问题不适用于.pem 文件。使用.pem 签名的 CSR。

[NSSDW-37813]

同时启动实时、交互式高、交互式介质和交互式低类类型的流量时，UI 的“监视类”表中显示的流量速率大约降低 150 Kbps。

[NSSDW-37568]

对于通过 MCN 管理的 Citrix SD-WAN 设备，新用户界面仪表板中的 Orchestrator 连接状态显示为不良/未知。

[NSSDW-37462]

当无法访问 LTE 加密狗或管理端口提供的 DNS 时，即使网络已切换到带内管理进行连接，Citrix SD-WAN Orchestrator 服务连接也会失败。

[NSSDW-37428]

在极少数情况下，如果分支站点的其中一个 WAN 链接具有静态公共 IP 地址，则动态虚拟路径的形成将失败。

解决方法：使用静态公有 IP 地址在分支站点重新启动虚拟 WAN 服务。

[NSSDW-36429]

在 Citrix SD-WAN BGP 配置中，更改路由域的路由器 ID 时，SD-WAN 动态路由协议可能会重新启动。

[NSSDW-35657]

对防火墙动态 NAT 策略或端口转发规则进行的配置更改可能会导致核心转储。

[NSSDW-34603]

站点级警报下不会报告 WPA3 失败的身份验证。

[NSSDW-32053]

平台和系统

首次添加自定义 SNMP 团体字符串不会删除现有的团体字符串配置。

解决方法：禁用然后启用 SNMP v1/v2 以清除现有团体字符串。

[SDWANHELP-2561]

Citrix SD-WAN 11.4.3a 版本的发行说明

June 8, 2022

本发行说明文档介绍了 Citrix SD-WAN 版本 Build 11.4.3a 中存在的增强功能和更改、已修复问题和已知问题。

> 注意
>
> Citrix SD-WAN 11.4.3a 版本解决了 https://support.citrix.com/article/CTX370550 中描述的安全漏洞，取代了 11.4.3 版。

新增功能

Build 11.4.3a 中提供的增强功能和更改。

DHCP 日志的增强

Citrix SD-WAN 设备可以为 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。

[NSSDW-36840]

硬件监视支持：您可以监视硬件组件，例如电源、磁盘、健康状态，还可以通过 **CLI** 命令 hw_mon 检查状态。严重的硬件事件记录在 Citrix SD-WAN 事件中。

[NSSDW-36660]

NAT 日志增强功能

从 Citrix SD-WAN 11.4.3 版本起，静态和动态 NAT 日志得到了增强，可以显示与转换后的 IP 地址和转换后的 IP 端口相关的信息。以下是新引入的字段：

转换后的 IP 地址

- **natsrc** -转换后的源 IP 地址
- **natdest** -转换后的目标 IP 地址

NAT 类型

- **snat** -当 snat 为 1 时，表示连接正在通过源 NAT 转换。
- **dnat** -当 dnat 为 1 时，表示连接正在通过目标 NAT 转换。

转换后的端口

- **natsport** -转换后的源端口地址
- **natdport** -转换后的目标端口地址

[NSSDW-34602]

已修复的问题

内部版本 11.4.3a 中解决的问题。

在任何站点或 WAN 链路上进行配置更改时扩展部署的情况下，路由引擎重新启动会导致 BGP 会话抖动。

[SDWANHELP-2594]

旧版 GUI 将 CGI 会话文件保留在临时目录下。这些 CGI 会话将在启动期间清理，这可能会阻止 Citrix SD-WAN 服务运行。

[SDWANHELP-2567]

由于 LTE 调制解调器事务超时错误，Citrix SD-WAN LTE 服务可能会挂起。

[SDWANHELP-2565]

添加动态规则时修复了可能的内存泄漏问题。

[SDWANHELP-2563]

由于 Citrix SD-WAN UI 中出现罕见的争用情况，当使用错误的数据库索引请求统计信息时，t2_app 将崩溃。

[SDWANHELP-2548]

在 Citrix SD-WAN 1100 上分配给 Palo Alto VM（VM-50 型）的内存增加到 5.5 GB。

[SDWANHELP-2534]

修复 ICA 分类中可能存在的内存泄漏问题。

[SDWANHELP-2527]

当基于域名的应用程序的 DNS 学习条目导致第一个数据包分类表达到最大限制时，设备崩溃。

[SDWANHELP-2480]

Citrix SD-WAN 设备仅允许传输管理端口上所需的流量，这会阻止用户在启用时访问 MiRIC 管理 GUI。

[SDWANHELP-2479]

尝试输入带前缀的 **IP** 地址未通过防火墙过滤器策略中的源/目标 IP 字段的验证。

[SDWANHELP-2471]

当流量一直很高且超过设备的最大流量容量限制时，流量映射的更改有时可能会导致数据路径重新启动。

[SDWANHELP-2456]

管理端口关闭/打开后，与 Syslog 服务器通信的源 IP 变为 169.254.200.2

[SDWANHELP-2450]

CCitrix SD-WAN Center 仪表板不会加载任何信息。

[SDWANHELP-2373]

静态路由支持 GRE 隧道作为传送服务。如果删除 GRE 隧道但未首先正确删除静态路由，则使用 GRE 隧道传送服务的路由会出现问题。

此修复会在删除 GRE 隧道时自动删除使用 GRE 隧道作为传递服务配置的路由。

[NSSDW-37846]

在 Citrix SD-WAN 11.4.2 版本中，对于扩展名为.der 的文件，从适用于本地的 Citrix SD-WAN Orchestrator 上载签名的 CSR 证书失败。

[NSSDW-37813]

AT & T 3G 网络计划于 2022 年 2 月失效。Citrix SD-WAN 110 LTE 调制解调器已设置为以语音为中心，在 AT & T 的 3G 失效后它不支持 VoLTE。

[NSSDW-37736]

当 LTE 加密狗或管理端口提供的 DNS 无法访问时，Citrix SD-WAN Orchestrator 服务连接将失败。尽管网络已切换到带内管理以实现连接。

[NSSDW-37428]

带内管理

从 Citrix SD-WAN 11.4.2 版本起，必须在 SD-WAN 设备上配置带内管理，才能通过带内管理端口建立与 Citrix SD-WAN Orchestrator 服务的连接。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。

[NSSDW-37174]

当 DHCP 服务器使用 DVP 和 HA 配置分配新地址时，Citrix SD-WAN 服务可能会崩溃。

[NSSDW-36513]

在极少数情况下，当路由表中发生路由更改时，Citrix SD-WAN 服务会重新加载。

[NSSDW-36289]

启用 CRL 处理后，第三方加密库中的内存问题可能会导致核心转储。

[NSSDW-35679]

当 Edge Security 防病毒和反恶意软件组件的内部许可证到期时，Citrix SD-WAN 将停止检测病毒和恶意软件。

[NSSDW-35596]

加载包含摘要路由的 Citrix SD-WAN 配置时，设备可能会持续重新加载。

[NSSDW-34670]

如果设备具有配置为总结路由的静态路由，并且动态获知了另一个相同前缀的路由，则该总结路由不会汇总路由。

[NSSDW-34355]

Citrix SD-WAN 仅允许在移动宽带设备上使用 DHCP，这不适用于在其数据计划中分配了静态 IP 的客户。

[NSSDW-33971]

一旦 SLAAC 从路由器获知 IP 和网关地址，除非当前地址过期，否则如果网关发生变化或我们更改网段，SLAAC 将不会重新获取 IP，即使在重新启动 SD-WAN 设备之后也是如此。移动端口时，这可能会延迟获取地址。

[NSSDW-33807]

一旦 SLAAC 从路由器获悉 IP 和网关地址，如果网关发生变化（除非当前地址过期），SLAAC 将不会重新获取网关。

示例：

- 分支设备从网关-1 学习其 IP 和网关。
- 网络管理员决定用新的网关-2 替换网关-1。管理员配置网关-2 与网关-1 相同，以便路由器通告发送的前缀信息与网关-1 发送的前缀信息相同。但是，网关-2 的源地址与网关-1 不同。
- 分支设备不会自动学习网关-2 的 IP。（除非和直到当前地址超时）

[NSSDW-33802]

为区域控制节点 (RCN) 网络创建的自动生成的汇总路由分配的成本为 30,000，而不是 65534。

[NSSDW-32629]

从 Citrix SD-WAN 中心推送设备设置时，不会应用于 Citrix SD-WAN。

[NSSDW-32257]

站点级警报下不会报告 WPA3 失败的身份验证。

[NSSDW-32053]

在执行重新身份验证时，Wi-Fi 客户端报告中的上传和下载数据将显示负值。

[NSSDW-31903]

平台和系统

首次添加自定义 SNMP 团体字符串不会删除现有的团体字符串配置。

[SDWANHELP-2561]

已知问题

11.4.3a 版中存在的问题。

如果禁用了部分站点升级，然后将整个网络升级到新的软件版本，某些站点可能会自动更正回较旧的版本。

解决方法：如果触发了另一项更改管理，降级的站点将升级到预期的软件版本。

[SDWANHELP-2586]

在具有 Internet 负载平衡配置的 Advanced Edition (AE) 平台上，Citrix SD-WAN 服务有时可能会崩溃。

解决方法：将 Internet 服务配置为主模式和辅助模式。

[SDWANHELP-2521]

如果将带外端口用于 SNMP 服务的装置切换到带内端口，则该设备的所有管理服务都将通过带内端口连接到 Internet。发送到带外端口的 SNMP 请求失败。

解决办法：配置外部 SNMP 服务，以便在带外端口出现故障时向带内端口发送请求。

[SDWANHELP-2358]

在 VPX 中，如果没有有效的许可证，守护进程将自动重启。在这种情况下，守护进程有时可能会崩溃。没有用户影响，因为守护进程会自动正常运行。

[NSSDW-37981]

同时启动实时、交互式高、交互式介质和交互式低类类型的流量时，UI 的“监视类”表中显示的流量速率大约降低 150 Kbps。

[NSSDW-37568]

对于通过 MCN 管理的 Citrix SD-WAN 设备，新用户界面仪表板中的 Orchestrator 连接状态显示为不良/未知。

[NSSDW-37462]

在极少数情况下，如果分支站点的其中一个 WAN 链接具有静态公共 IP 地址，则动态虚拟路径的形成将失败。

解决方法：

使用静态公共 IP 地址在分支站点重新启动虚拟 WAN 服务。

[NSSDW-36429]

在 Citrix SD-WAN BGP 配置中，更改路由域的路由器 ID 时，SD-WAN 动态路由协议可能会重新启动。

[NSSDW-35657]

对防火墙动态 NAT 策略或端口转发规则进行的配置更改可能会导致核心转储。

[NSSDW-34603]

当用户选择查看内部调制解调器的状态时，旧版 UI 还会显示外部调制解调器的状态。

[NSSDW-32219]

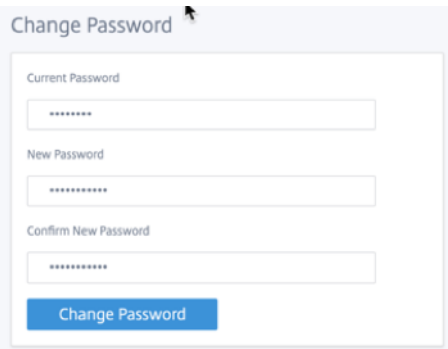
用于 **SD-WAN** 设备的新用户界面

February 10, 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：

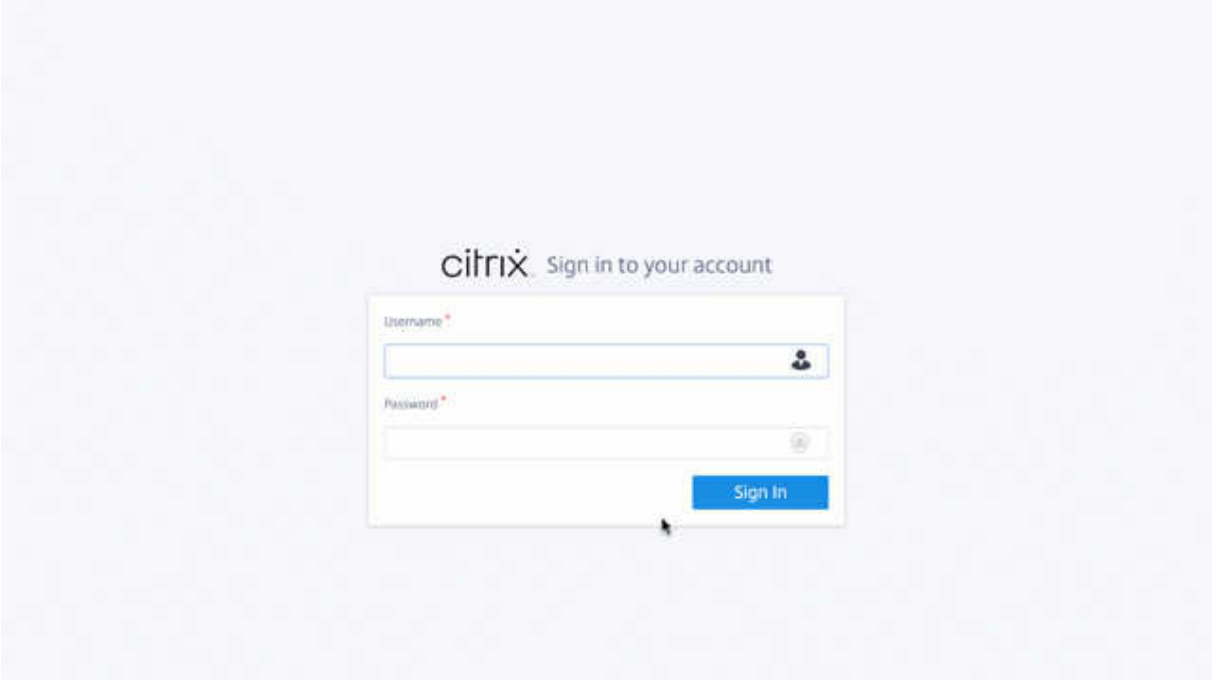
1. 打开新的浏览器选项卡并导航到 **https: // < management-ip >** 以访问 SD-WAN 设备上的新 UI。如果您正在访问 IPv6 地址，请输入 `https://<[IPv6 address]>`。

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

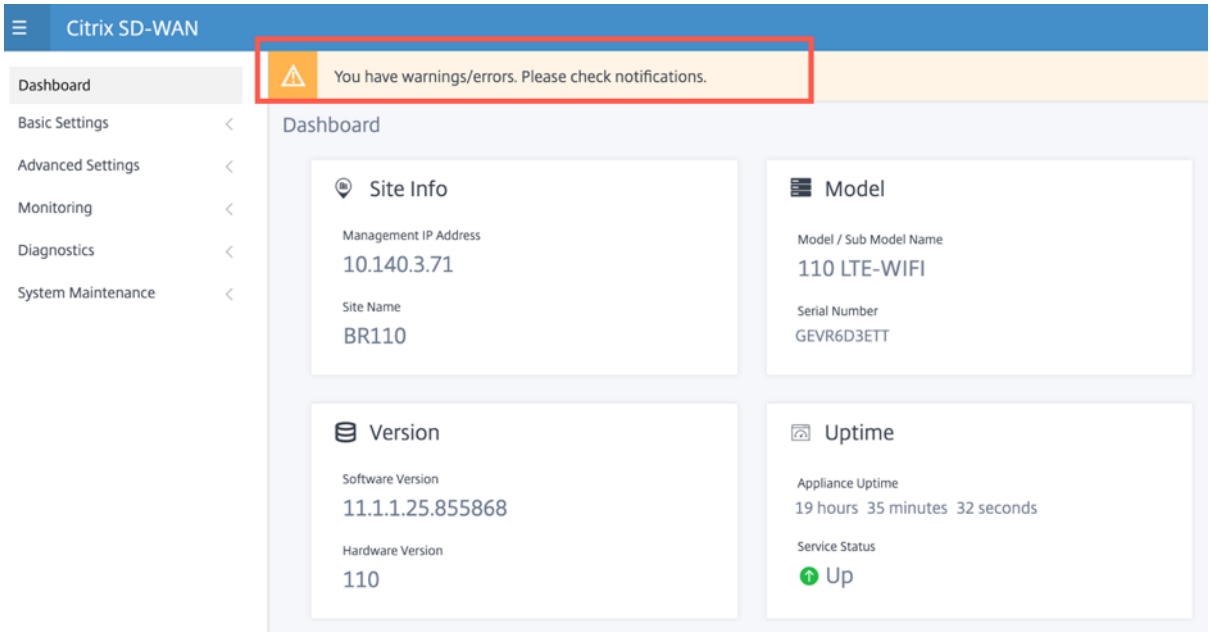
> 注意：
>
> 在启用带内管理的情况下，可以在中提供接口 IP 地址 ** < management-ip > 以访问新 UI。可以在启用用于 IP 服务的多个受信任接口上启用带内管理。您可以使用管理 IP 和带内虚拟 IP 访问 UI。

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。

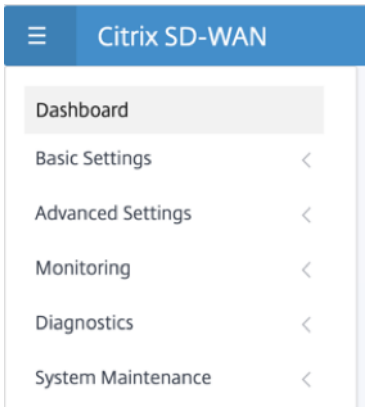


成功登录后，您可以看到导航面板位于左侧。此外，如果有任何警告或错误，您可以在仪表板上看到通知横幅。



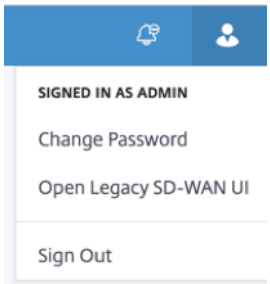
导航

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。

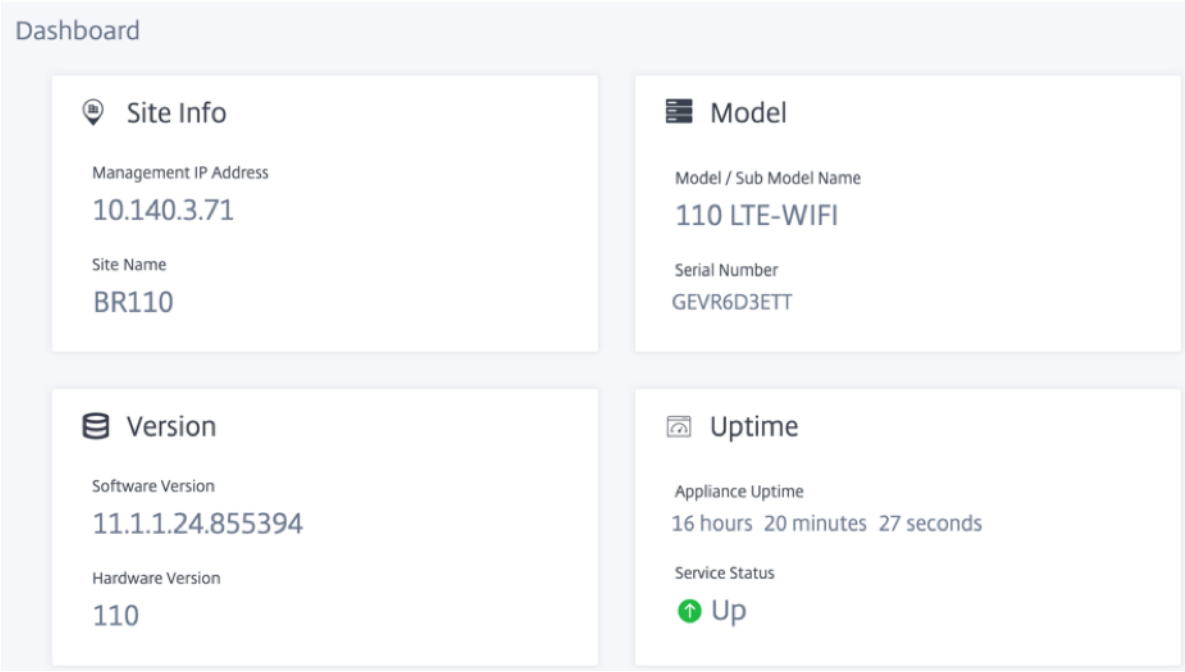


控制板

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。

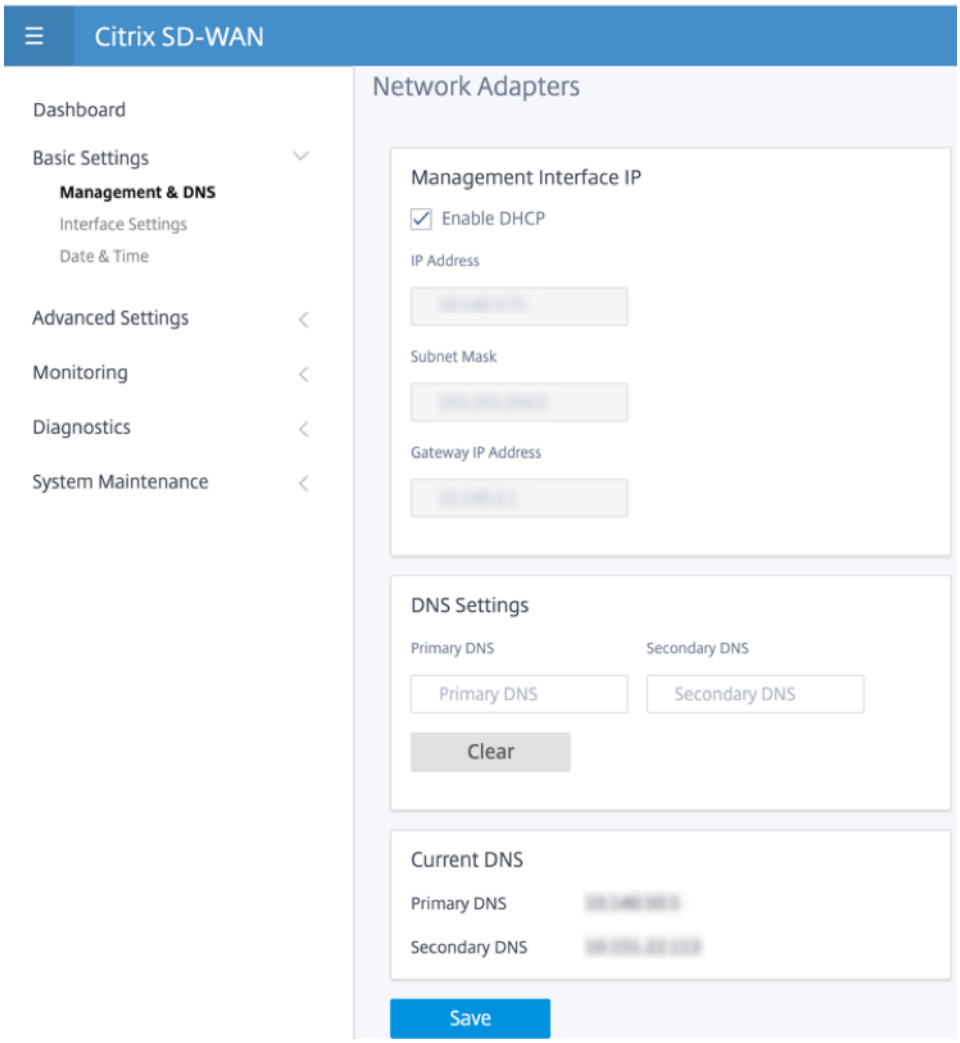
- 管理和 DNS
- 接口设置
- LACP LAG 组
- 日期和时间
- 半径服务器
- TACACS+ 服务器

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。

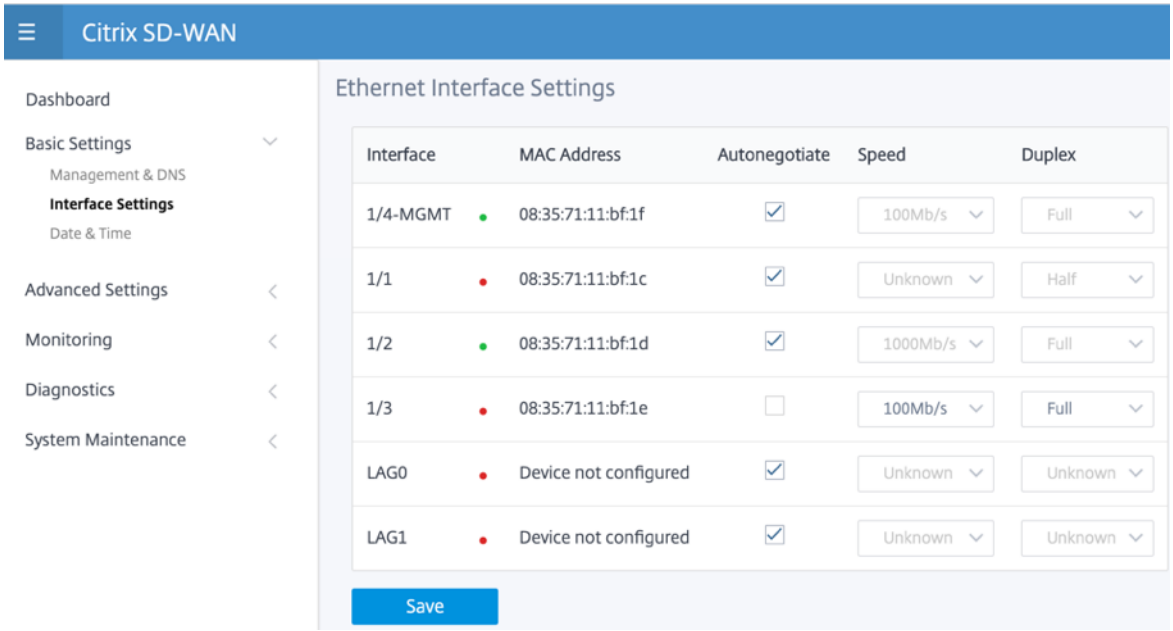
要在允许列表中添加或删除 IPv4 地址，必须仅使用 IPv4 地址访问 SD-WAN 设备管理界面。同样，要在允许列表中添加或删除 IPv6 地址，必须仅使用 IPv6 地址访问 SD-WAN 设备管理界面



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。

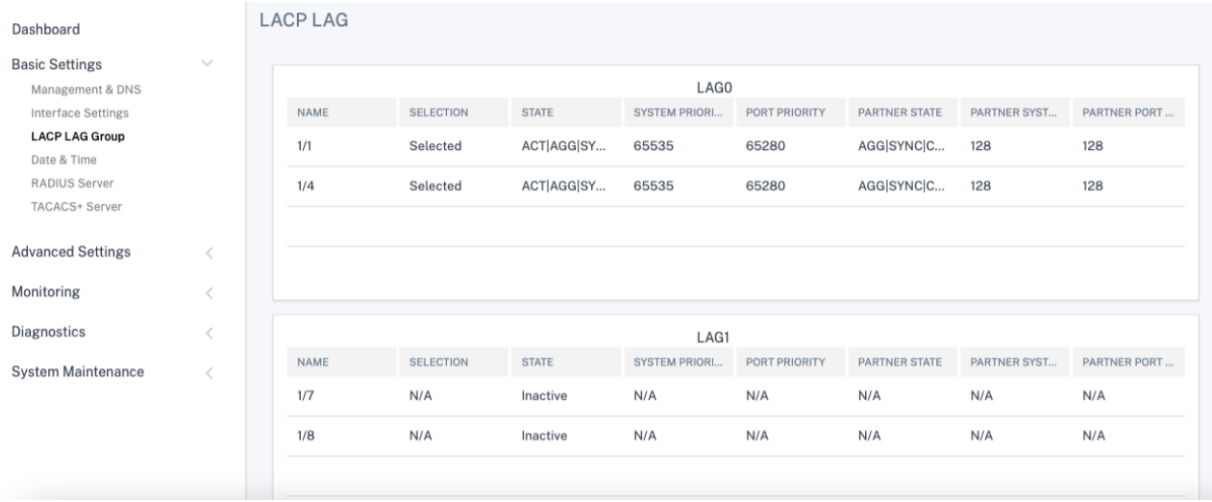
在 Citrix SD-WAN 设备上，最多可以创建 4 个 LAG，其中每个 LAG 中最多分组 4 个端口。

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。

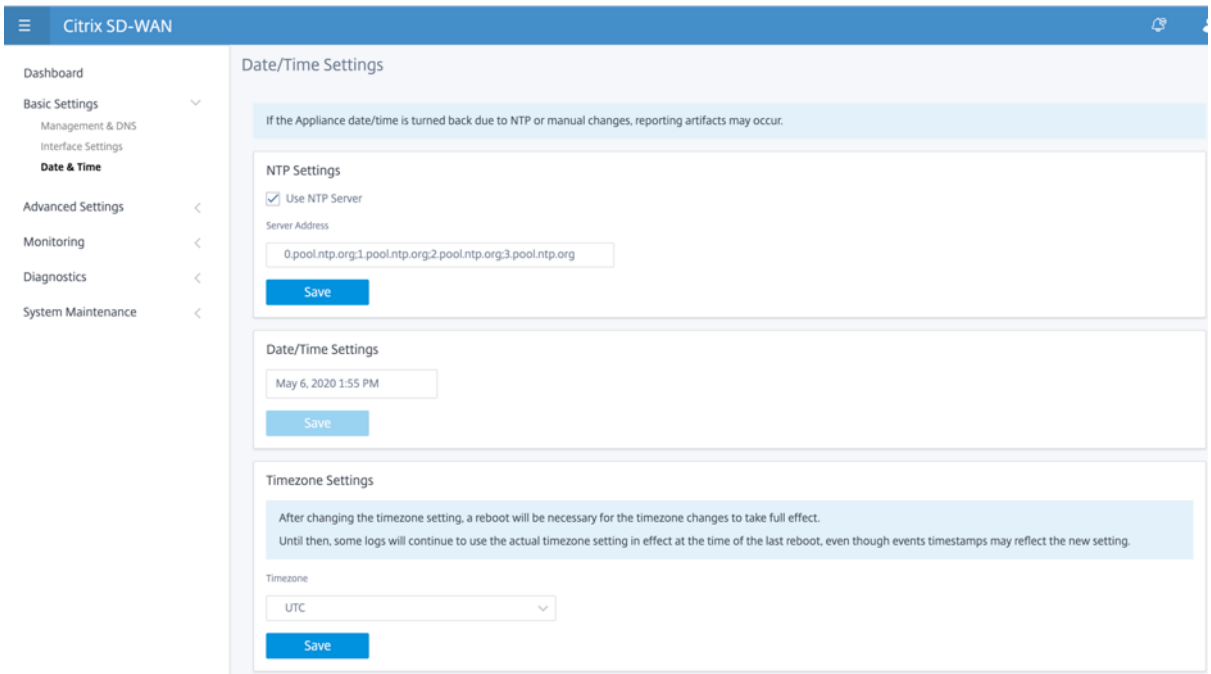
要查看 LAG 详细信息，请导航到 基本设置 > **LACP LAG** 组。

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。



半径服务器

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。

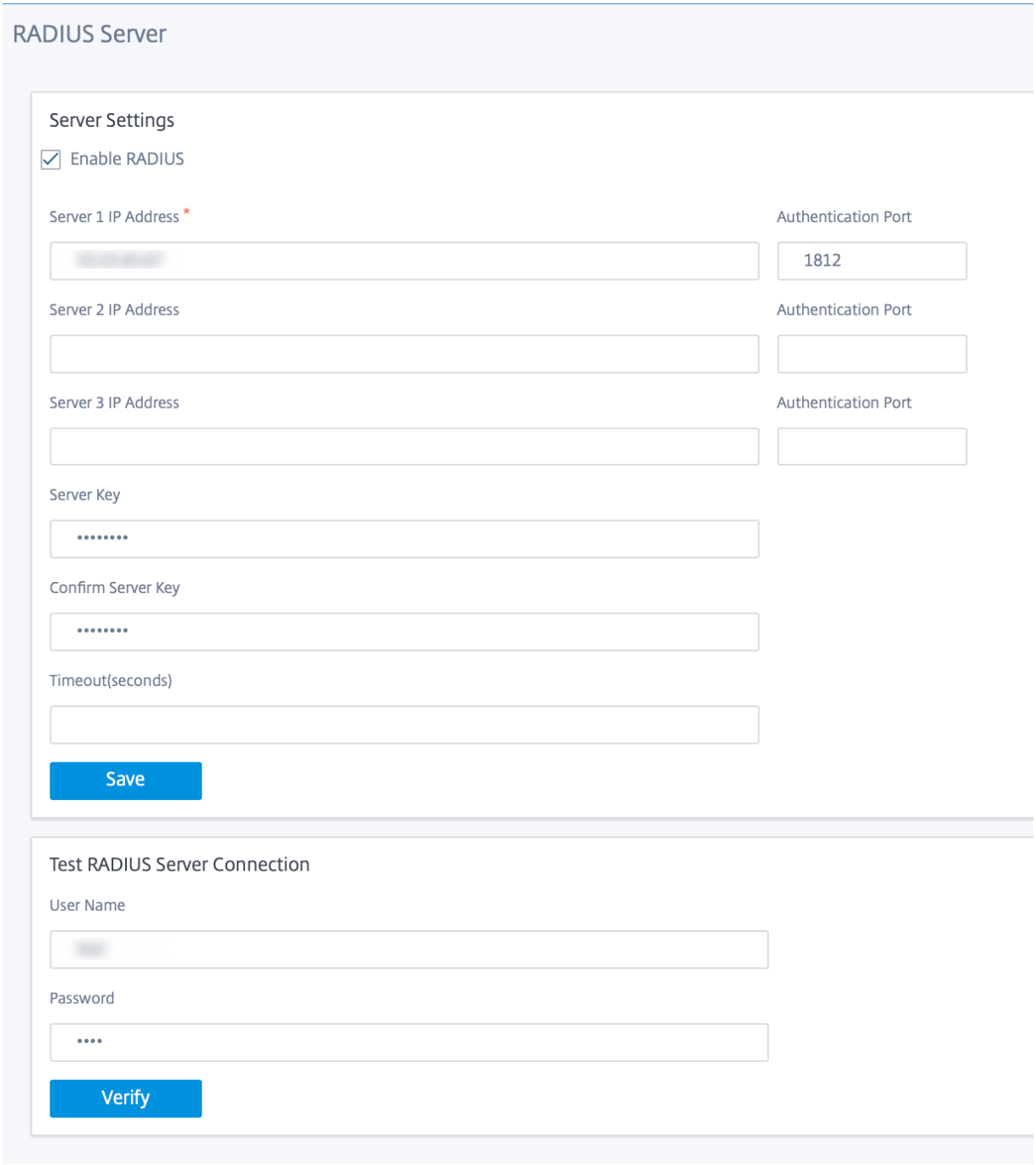
要配置 RADIUS 服务器：

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：

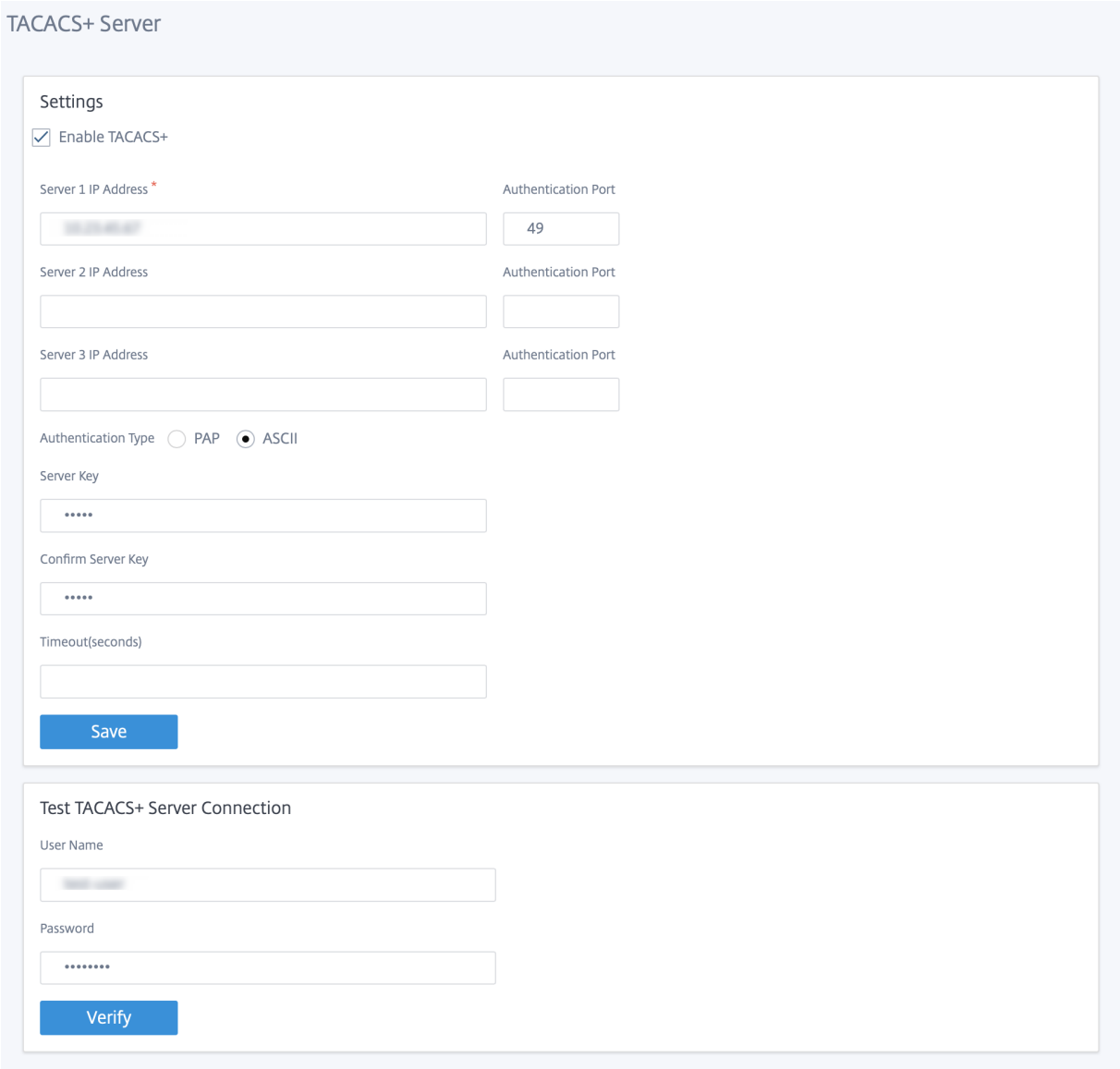
1. 选中 启用 **TACACS+** 复选框。

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）。



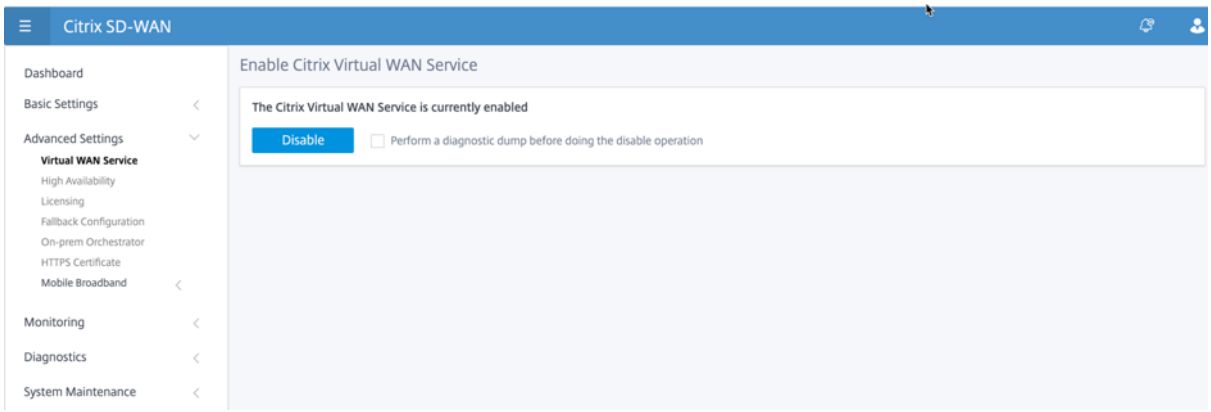
高级设置

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

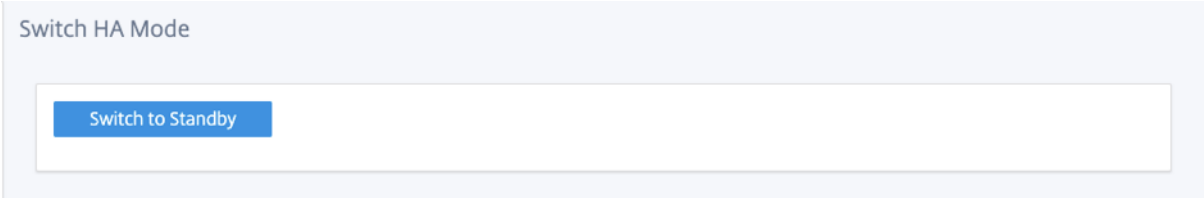
Citrix 虚拟广域网服务

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。

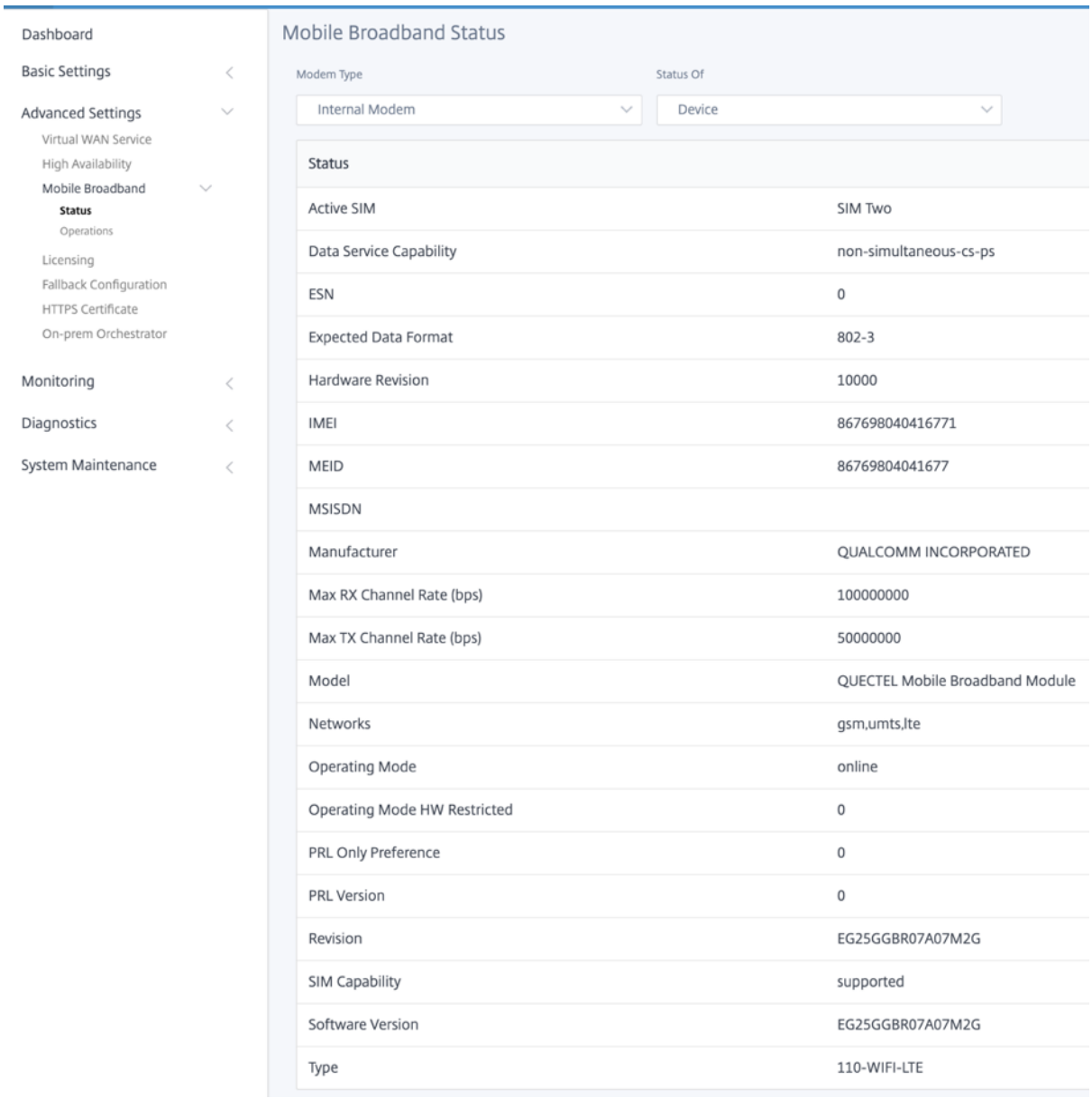
> 注意：
>
> Citrix SD-WAN 110-LTE-WiFi 设备具有两个标准 (2FF) SIM 插槽。要使用微型（3FF）和纳米（4FF）大小的 SIM 卡，请使用 SIM 适配器。将较小的 SIM 卡扣入适配器。您可以从 Citrix 获取适配器作为现场可更换单元 (FRU) 或从 SIM 提供程序获取适配器。仅在 Citrix SD-WAN 110-LTE-WiFi 设备上支持对内部 LTE 调制解调器进行热交换。

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，并确保互联网正常工作，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。

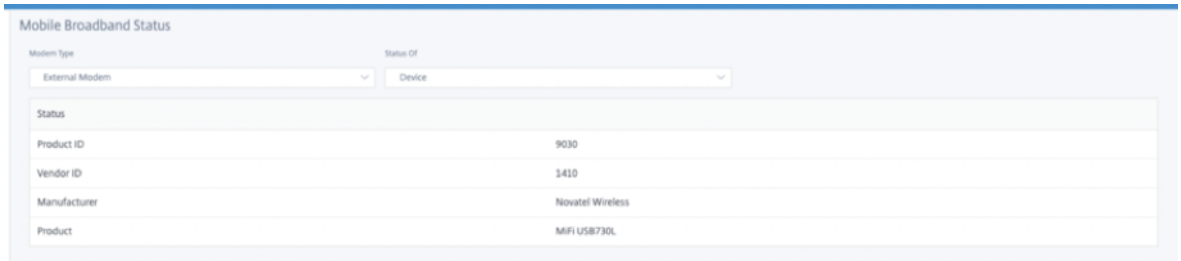


以下是一些有用的状态信息：

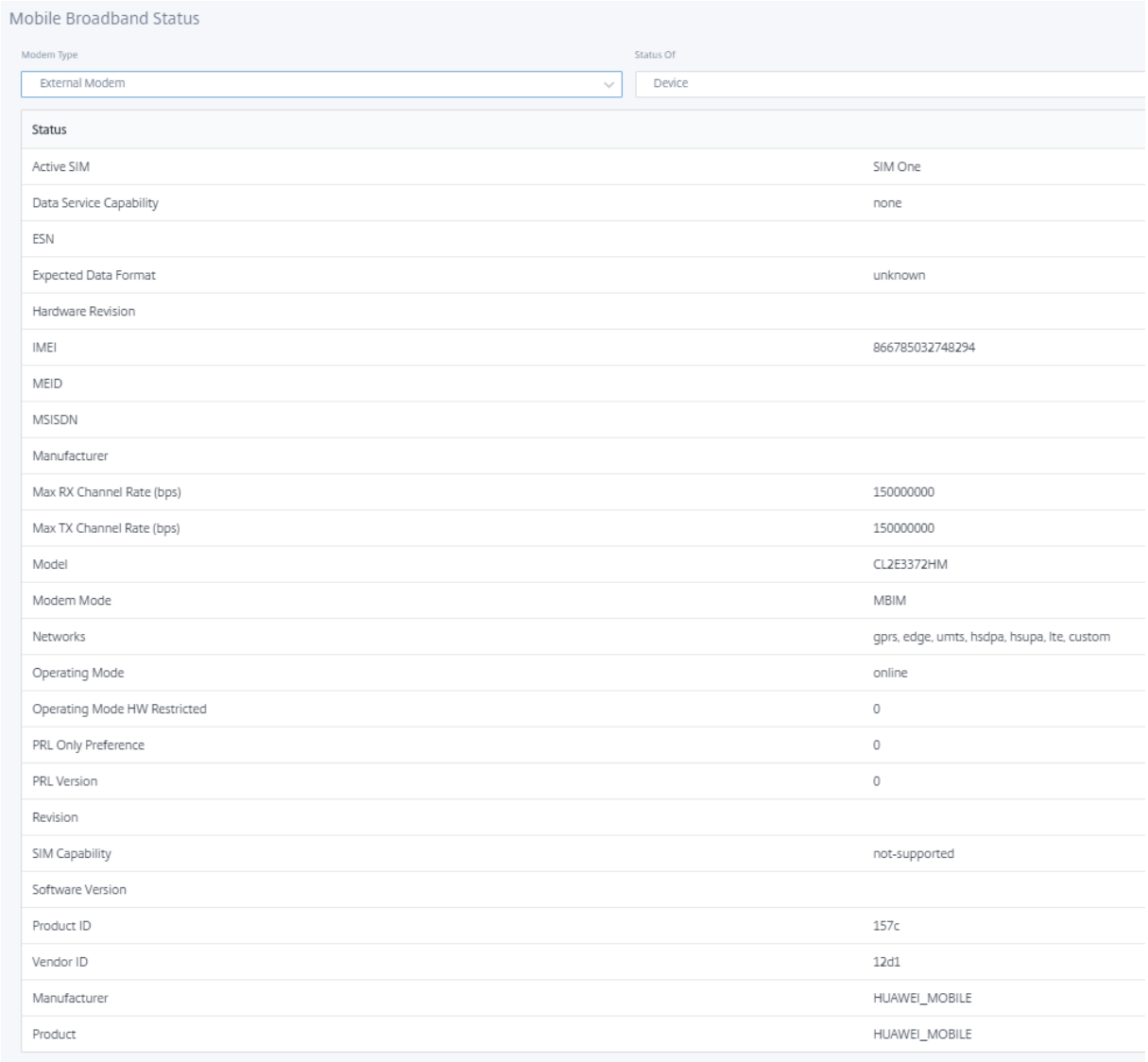
- 调制解调器类型：选择调制解调器类型为外部或内部内部调制解调器在 移动宽带 **>** 状态页面下显示状态。所有其他部分，例如 SIM 首选项、APN 设置、启用/禁用调制解调器、重启调制解调器和刷新 SIM 卡在 移动宽带 **>** 操作页面下提供。
- 活动 **SIM** 卡：在任何给定时间，只能有一个 SIM 卡处于活动状态。显示当前处于活动状态的 SIM 卡。
- 操作模式：显示调制解调器状态。
- **SIM** 功能：显示 SIM 卡是否受支持。
- 型号：显示移动宽带模块名称。

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。

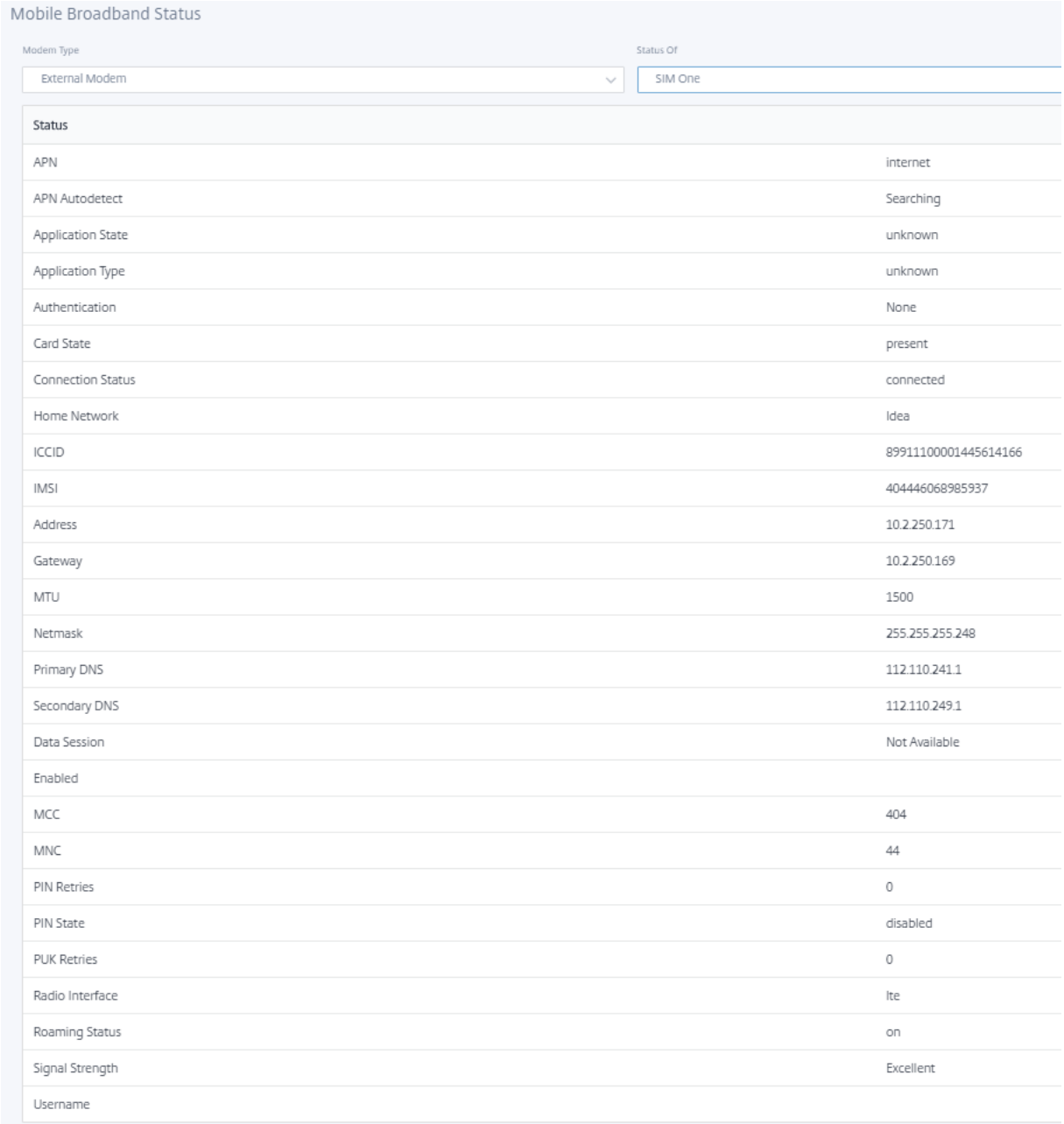
CDC 以太网外部调制解调器的设备详细信息。



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：

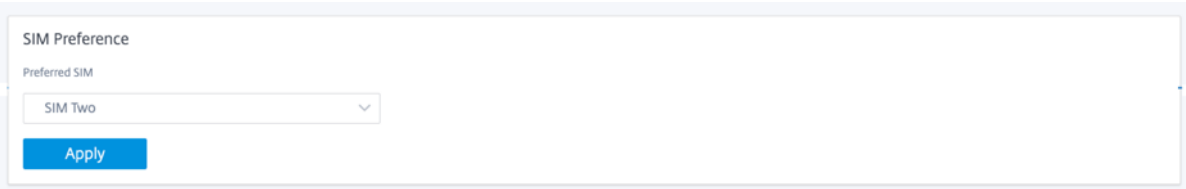
操作	调制解调器	外部调制解调器-CDC 以太网	外部调制解调器-MBIM 和 NCM
SIM 卡首选项	是-适用于支持双 SIM 卡的装置	否	否
SIM PIN	是	否	否
APN 设置	是	否	是

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 One**：如果插入了两张 SIM 卡，启动时 LTE 调制解调器将使用 SIM One（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 1 或 SIM 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 1 或 SIM 2），并将继续使用它，直到 SIM 处于活动状态。
- **SIM One**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM One。SIM 卡一始终处于活动状态。
- **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。

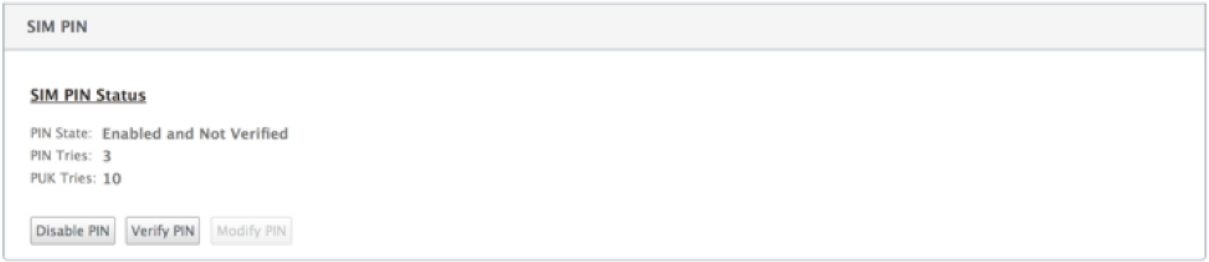
> 注意：
>
> Citrix SD-WAN 210-SE LTE Wi-Fi 设备不可用“SIM 首选项”选项，因为它只有一个 SIM 卡插槽。



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 卡。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 卡 PIN 码，然后单击 验证。状态更改为 已启用 和 已验证。
- 启用 **SIM** 卡 **PIN**：您可以为禁用 SIM 卡 PIN 的 SIM 卡启用 SIM 卡密码。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 卡 PIN 码，然后单击 验证。
- 禁用 **SIM** 卡 **PIN**：您可以选择禁用已启用并验证 SIM 卡 PIN 的 SIM 卡的 SIM 卡功能。单击禁用。输入 SIM 卡 PIN，然后单击 禁用。
- 修改 **SIM** 卡 **PIN**：密码处于“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 卡 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

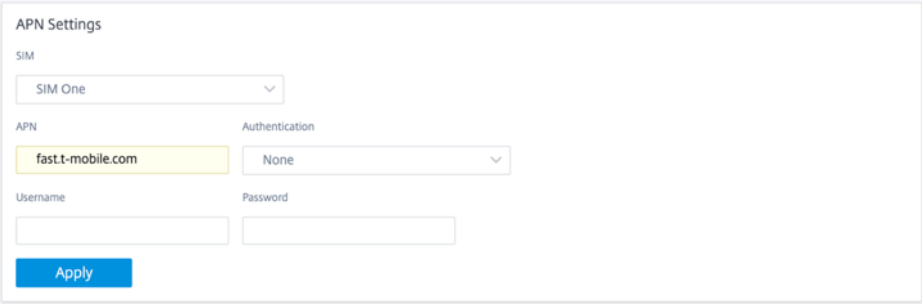
1. 要配置 APN 设置，请导航到 高级设置 **>** 移动宽带 **>** 操作 **>** 然后转到 **APN** 设置 部分。

   > 注意
   >
   > 从运营商处获取 APN 信息。

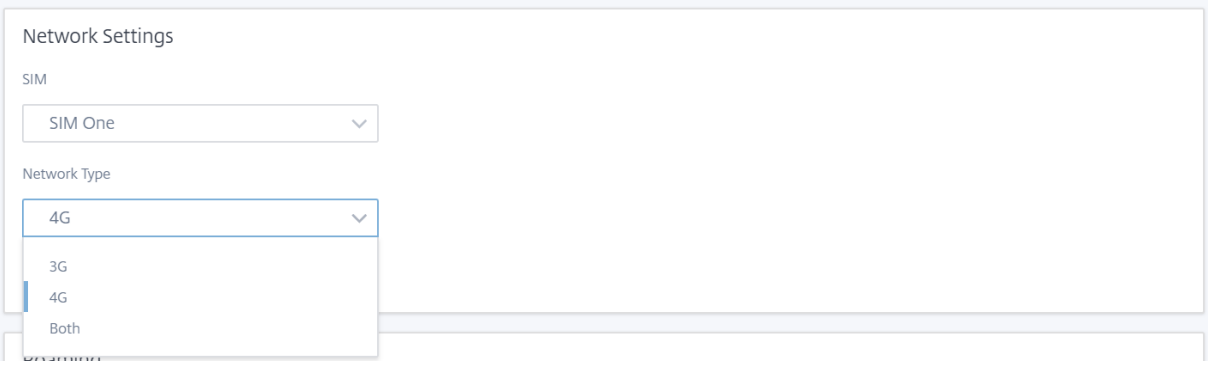
2. 选择 SIM 卡，输入运营商提供的 **APN**、用户名、密码 和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。

   > 注意
   >
   > 所有这些字段都是可选的。

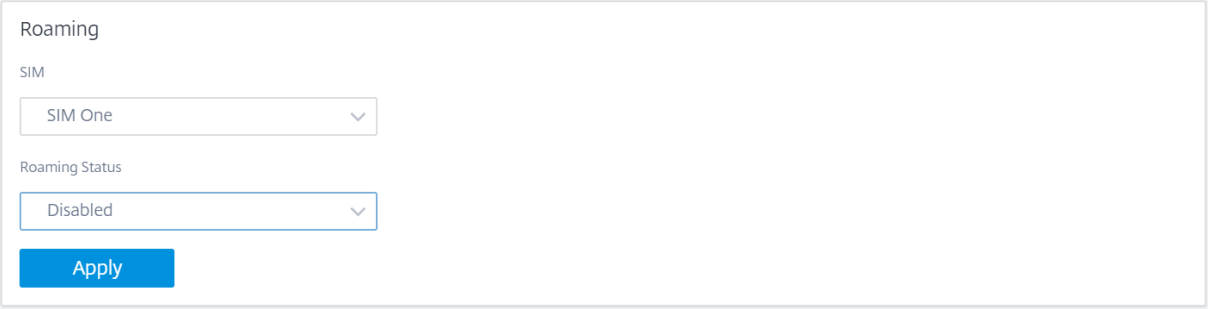
3. 单击应用。



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。



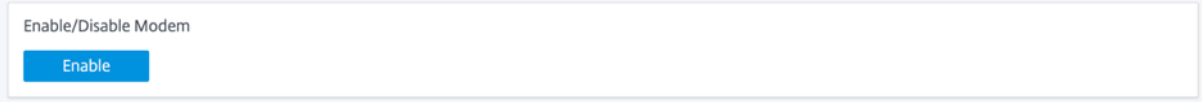
漫游　默认情况下，LTE 设备上启用漫游选项，您可以选择禁用它。



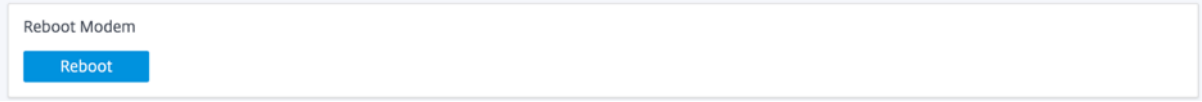
管理固件

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。

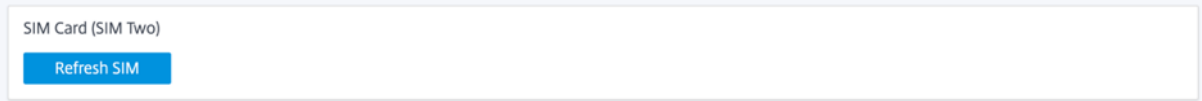


重启调制解调器　重新启动调制解调器。重新启动操作最多可能需要 7 分钟才能完成。



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。



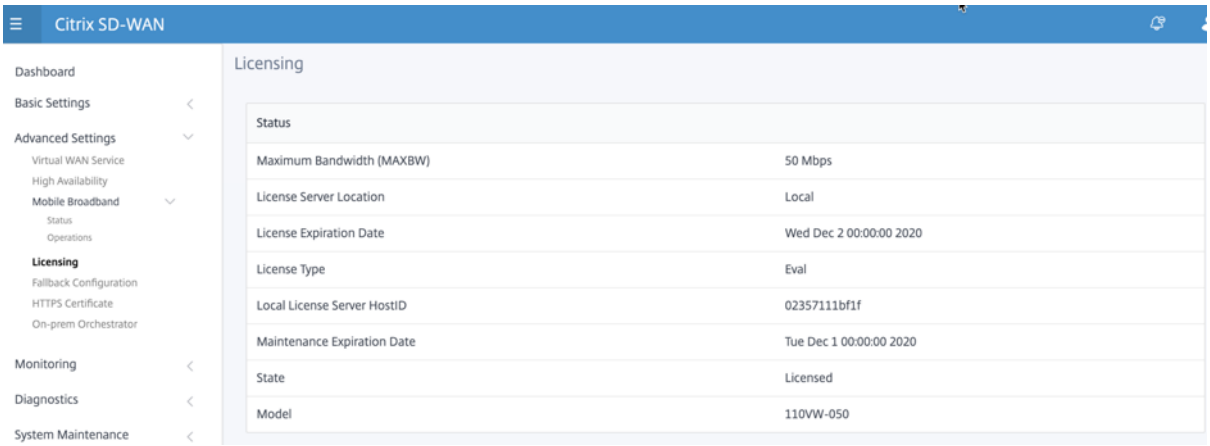
您可以使用 Citrix SD-WAN 中心远程查看和管理网络中的所有 LTE 站点。有关更多信息，请参阅 远程 LTE 站点管理。

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。

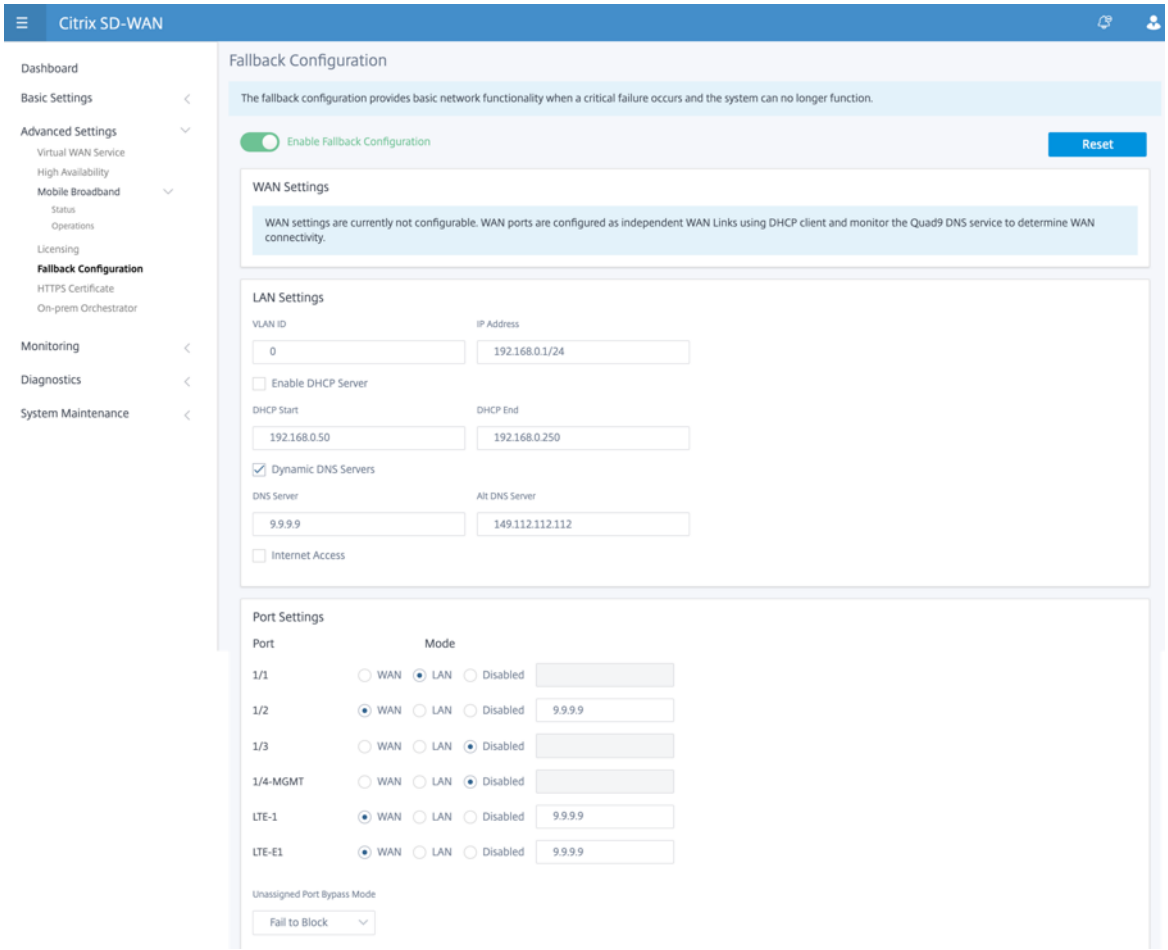


> 注意：
>
> 在安装和应用 SD-WAN Center 中的许可证时，请确保您的特定设备支持要启用的 SD-WAN 设备版本，并且可

> 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。

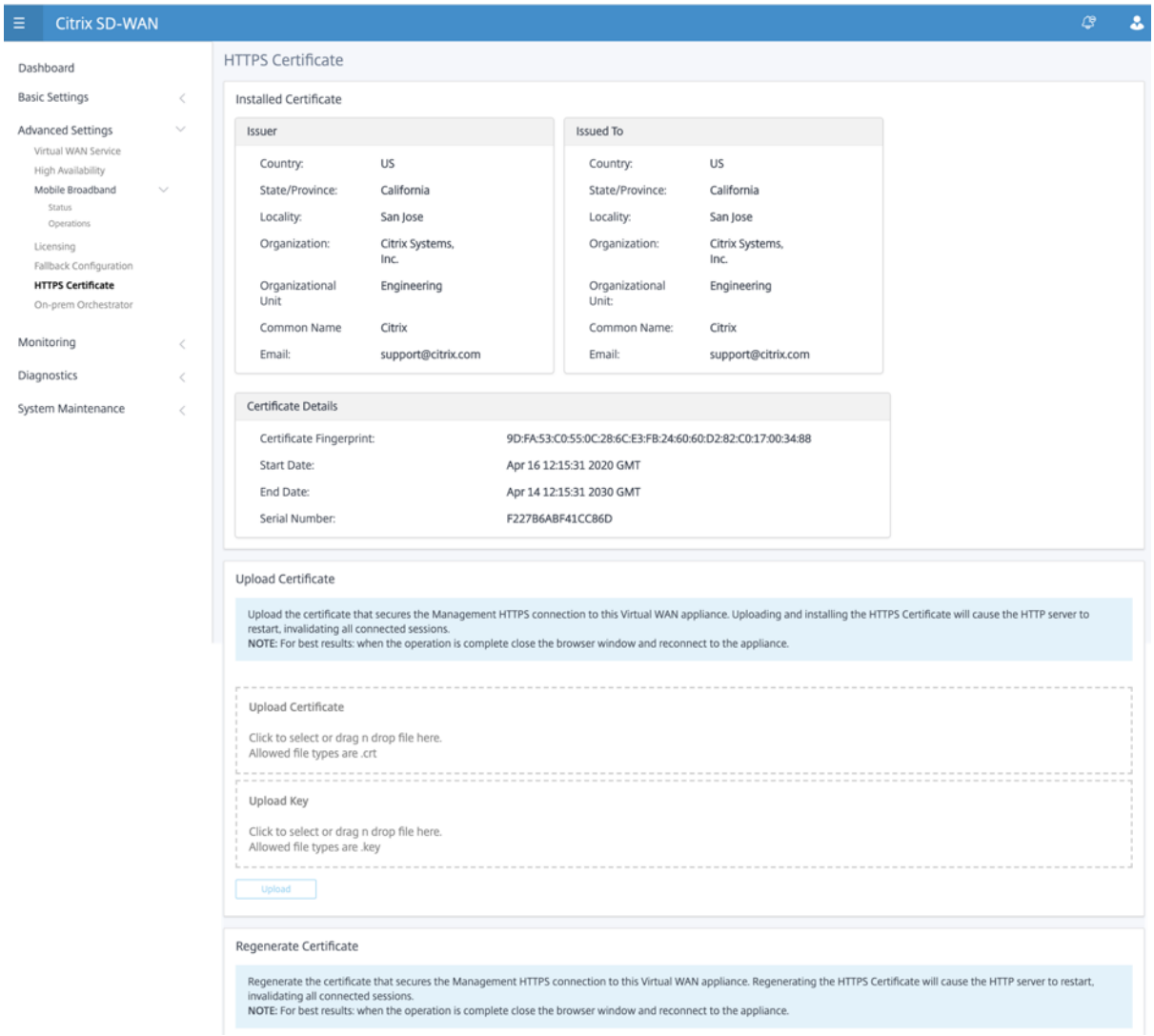


> 注意
>
> LTE 接口不能配置静态 IP 地址。

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。

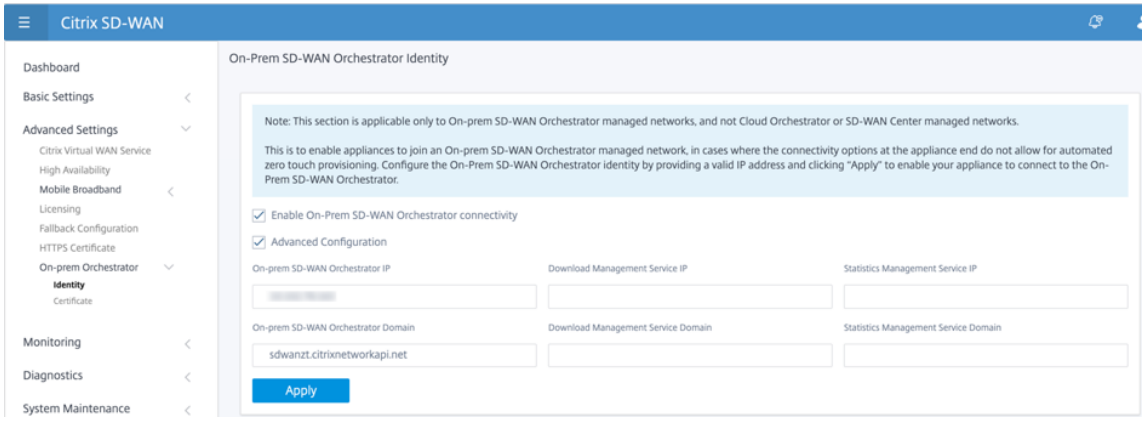
您可以通过启用 Orchestrator 连接并指定内部 PREM SD-WAN 协调器标识，在 Citrix SD-WAN 设备和 Citrix On-PREM SD-WAN 协调器之间建立连接。

> 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。

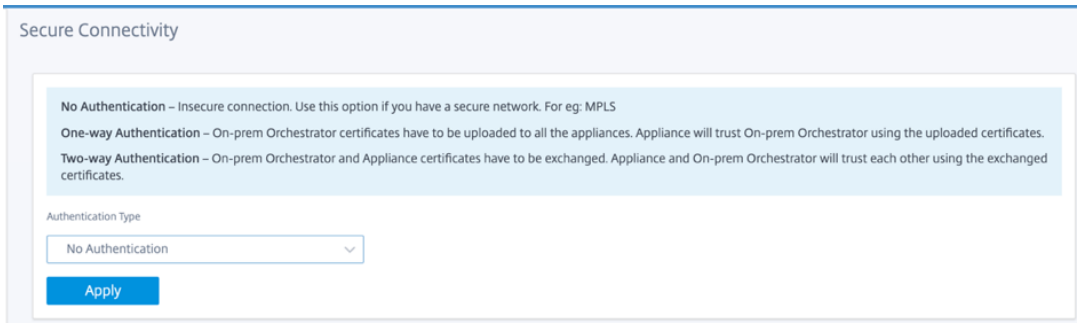
   如果启用了 Onprem Orchestrator 身份验证类型，则设备只能通过 双向身份验证连接到 Onprem Orchestrator。

   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。

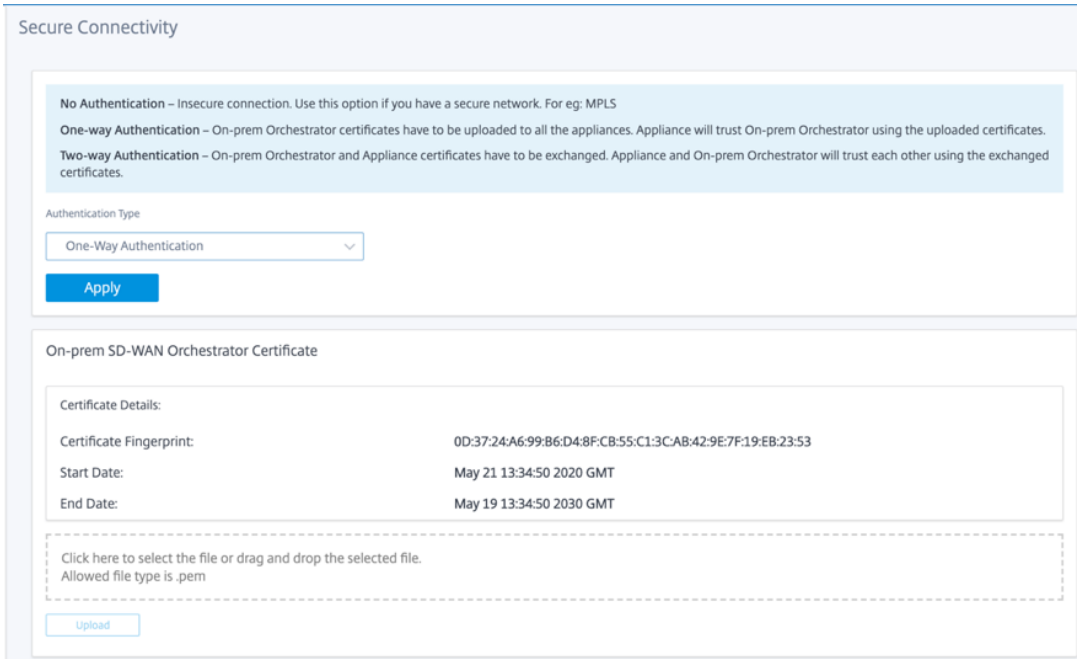
   > 注意
   >
   > - 生成的证书是 X509 自签名证书。
   > - 如果证书过期或破坏，客户必须重新生成证书。
   > - 证书的有效期为 10 年。
   > - 您可以查看证书详细信息，如指纹、开始日期和结束日期
   > - 客户必须确保在 On-PREM Orchestrator 和 SD-WAN 设备之间重新生成并交换证书，以避免设备与 ON-PREM 编排器的连接丢失。

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：

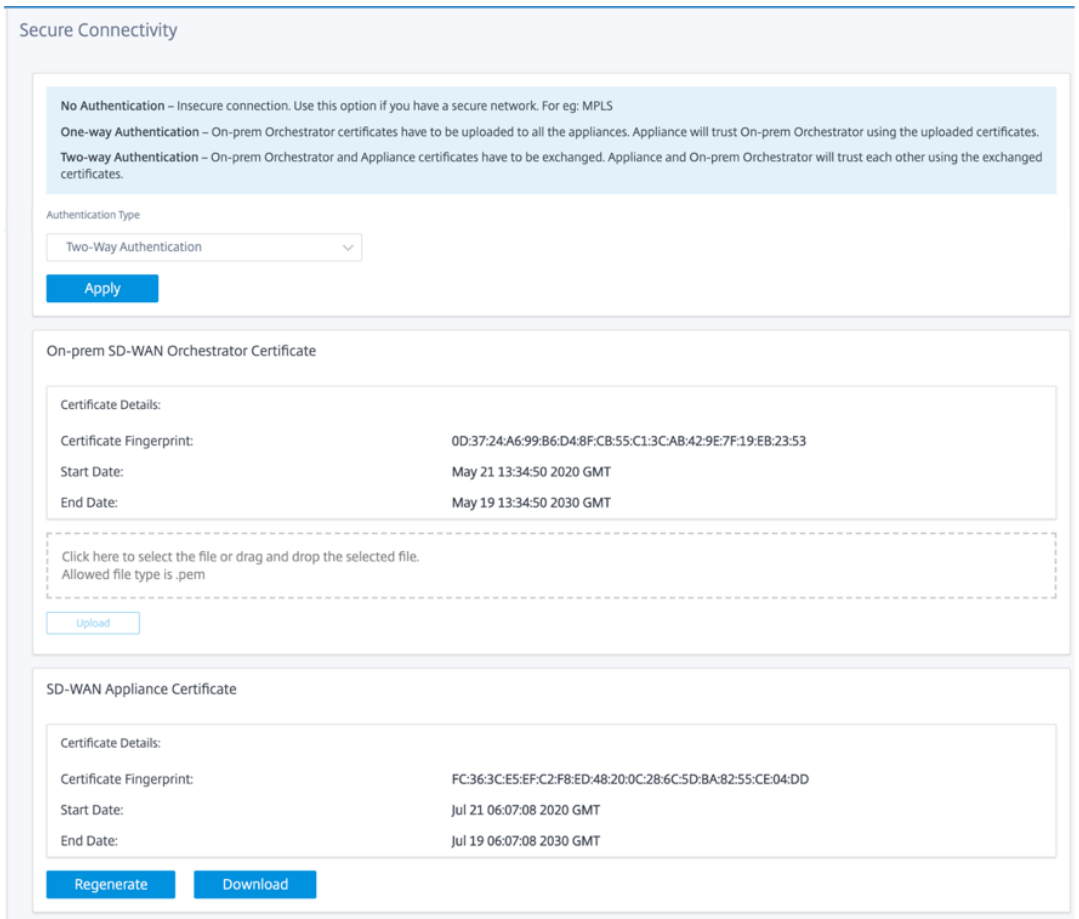
   - 无身份验证—在本地 SD-WAN Orchestrator 和 SD-WAN 设备之间不进行身份验证，也无需使用 SD-WAN 设备或本地 SD-WAN Orchestrator 证书。但是，如果您有一个安全的网络，如 MPLS，则可以使用此选项。

   - 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

在监控部分下，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

系统要求

June 22, 2021

硬件要求

中提供了安装 SD-WAN 设备的说明设置 SD-WAN 设备。

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

有关许可证要求的详细信息，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+
- Microsoft Internet Explorer 11+
- 微软边缘 13 +
- 野生动物园 9+

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 云端平台

SD-WAN 平台模型和软件包

September 26, 2023

本节提供有关下载 Citrix SD-WAN 软件包的信息。

> 注意
>
> 下载软件之前，必须获取并注册 Citrix SD-WAN 软件许可证。有关信息，请参阅许可。

SD-WAN 设备包包含与特定 SD-WAN 配置包捆绑在一起的特定设备型号的 SD-WAN 软件包。通过使用主控制节点 (MCN) 上运行的管理 Web 界面中的“更改管理”向导，将这两个软件包捆绑在一起并分发给客户端。

如果这是初始安装，则必须在 SD-WAN 网络中的每个客户端设备上手动上载、暂存和激活相应的设备包。如果要更新现有 SD-WAN 部署的配置，则当客户端的虚拟路径开始运行时，MCN 会在每个现有客户端上自动分发和激活相应的设备包。

下载软件包

对于每个设备型号，都有不同的 Citrix SD-WAN 软件包。您需要为要包含在网络中的每个设备型号下载相应的软件包。

要下载 Citrix SD-WAN 软件包，请转到 URL；产品下载。
本网站提供了下载软件的说明。

Citrix SD-WAN 软件包

对于每个受支持的 SD-WAN 设备型号，都有不同的 Citrix SD-WAN 软件包。您需要为计划整合到网络中的每个设备型号获取适当的软件包。

支持 **SD-WAN** 设备型号

Citrix SD-WAN 设备主要有三种类别：

- SD-WAN 设备五金型号
  - WANOP、Standard Edition 和 Premium Edition
- SD-WAN VPX 虚拟设备（SD-WAN 虚拟设备）
  - 标准版和 WANOP 版

> 注意
>
> SD-WAN 环境中的所有 SD-WAN 设备型号都需要运行相同的 SD-WAN 固件版本。有关其他信息，请联系 Citrix SD-WAN 客户支持。

有关 SD-WAN 设备的完整说明，请参阅产品下载站点上的 SD-WAN 产品平台版 数据表 。

SD-WAN 标准版五金设备

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
410-SE	小分支机器
1000-SE	小分支机器
1100-SE	大型分支设备
2000-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 广域网优化硬件设备 **(SD-WANOP)**

以下是受支持的 SD-WAN WAN 优化 (WANOP) 设备型号：

SD-WAN WANOP 平台模型	角色
WANOP 4100	数据中心设备
WANOP 5100	数据中心设备

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

SD-WAN VPX-SE 平台模型	角色
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 。

SD-WAN WANOP 虚拟设备 (SD-WAN VPX-WANOP)

以下是受支持的 SD-WAN WANOP 虚拟设备 (VPX-WANOP) 型号：

SD-WAN VPX WANOP 平台模型	角色
WANOP VPX-2	小分支机器
WANOP VPX-6	小分支机器
WANOP VPX-10	小分支机器
WANOP VPX-20	小分支机器
WANOP VPX-50	大型分支设备
WANOP VPX-100	大型分支设备
瓦诺普 VPX-200	大型分支设备

> 重要
>
> 在版本 10.1 中，Enterprise 平台版将更名为“Premium Edition”。

SD-WAN Premium Edition 硬件设备 (SD-WAN PE)

以下是受支持的 SD-WAN 高级（企业）版设备 (SD-WAN PE) 型号：

SD-WAN EE 平台模型	角色
1000-PE	大型分支机构，数据中心设备
1100-PE	大型分支机构，数据中心设备
2000-PE	大型分支机构，数据中心设备

SD-WAN EE 平台模型	角色
2100-PE	大型分支机构，数据中心设备
5100-PE	大型分支机构，数据中心设备
6100-PE	大型分支机构，数据中心设备

不受支持的功能

Citrix SD-WAN 1000 SE /PE、Citrix SD-WAN 2000 SE /PE 和 Citrix SD-WAN 4000 SE 设备不支持以下功能：

- IPv6
- SD-WAN 设备的新用户界面
- 外部 LTE USB 调制解调器
- 带内管理
- 用作数据接口的管理端口
- DNS 代理服务
- 802.1x 支持
- 回退配置
- 第 0/Day-N 设置
- 动态路由器 ID
- 高级版
- Wi-Fi
- LTE
- 云直接服务
- ECMP 负载平衡
- LACP 滞后

升级路径

November 1, 2021

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。

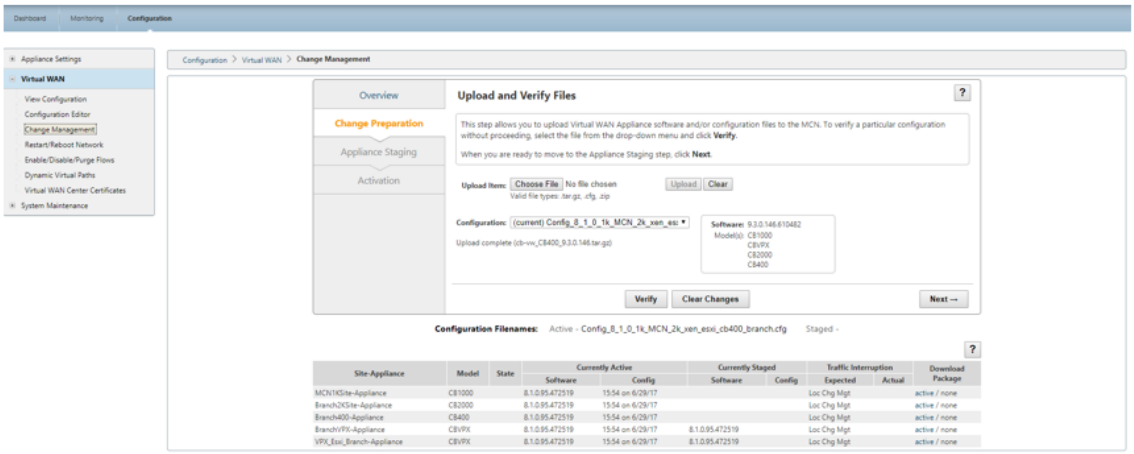
虚拟广域网软件升级到 **9.3.5**，使用工作虚拟广域网部署

June 22, 2021

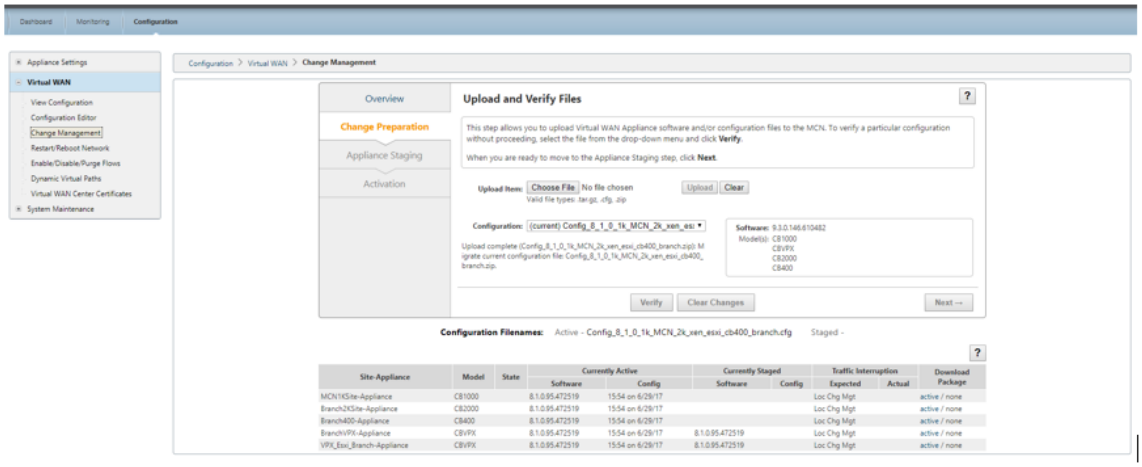
> 注意：
>
> 具有运行 9.3.4 或更低版本的工作虚拟 WAN 配置，并且从 MCN 到分支站点的虚拟路径建立了虚拟路径。

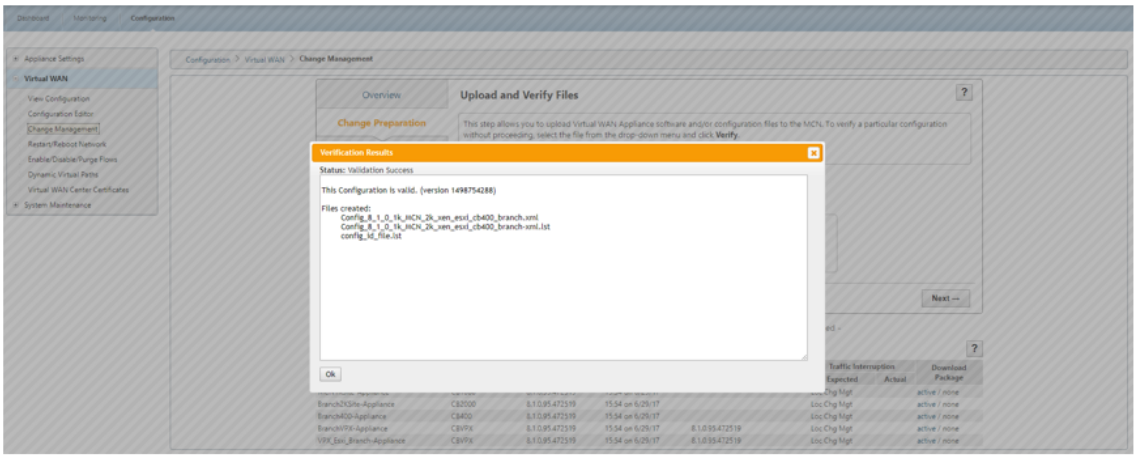
1. 在 MCN 设备上，导航到 配置 > 虚拟 **WAN** > 更改管理。
2. 从 Citrix 下载页面 中获取适用于虚拟 WAN 网络中的所有站点的 *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* 文件。

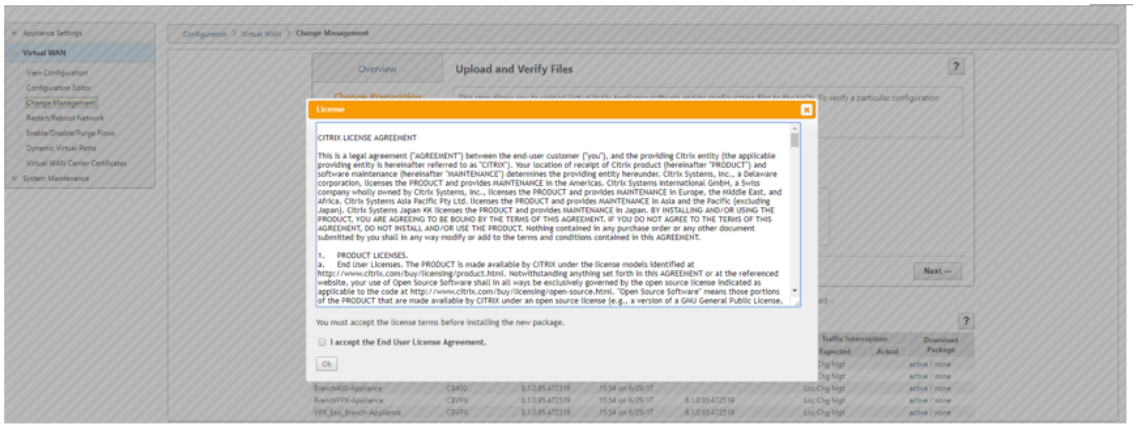
3. 为在必须执行升级的配置文件中定义的分支上载 *cb-vw-<ApplianceModel>-9.3.5.23.tar.gz* 文件。在 SD-WAN Web 界面中为 MCN 设备执行更改管理，并完成更改管理过程。



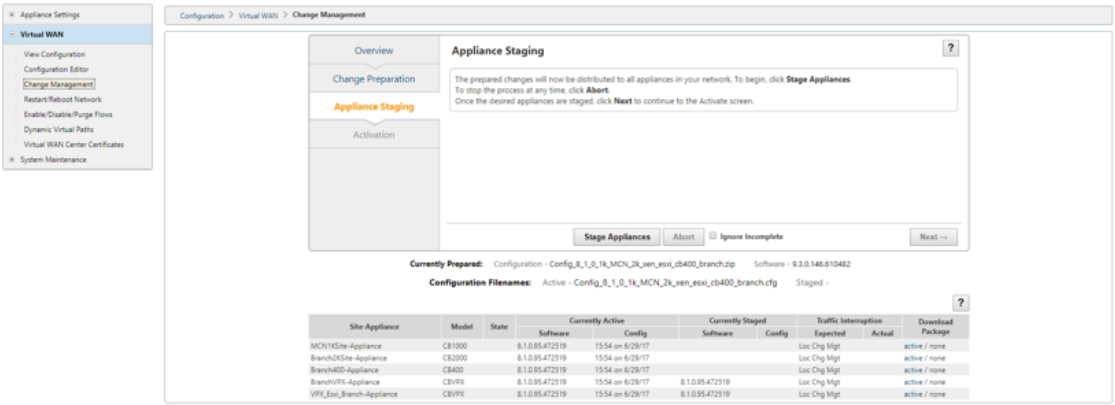
4. 单击下一步以进一步操作。



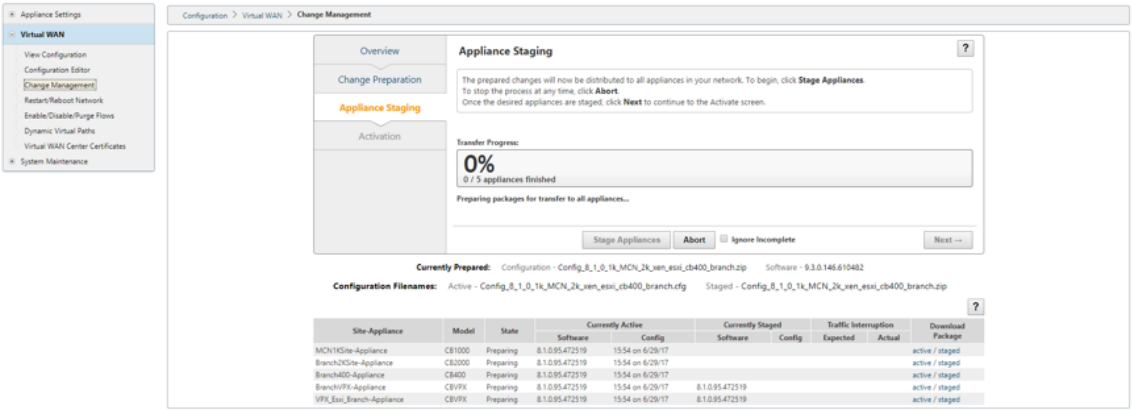


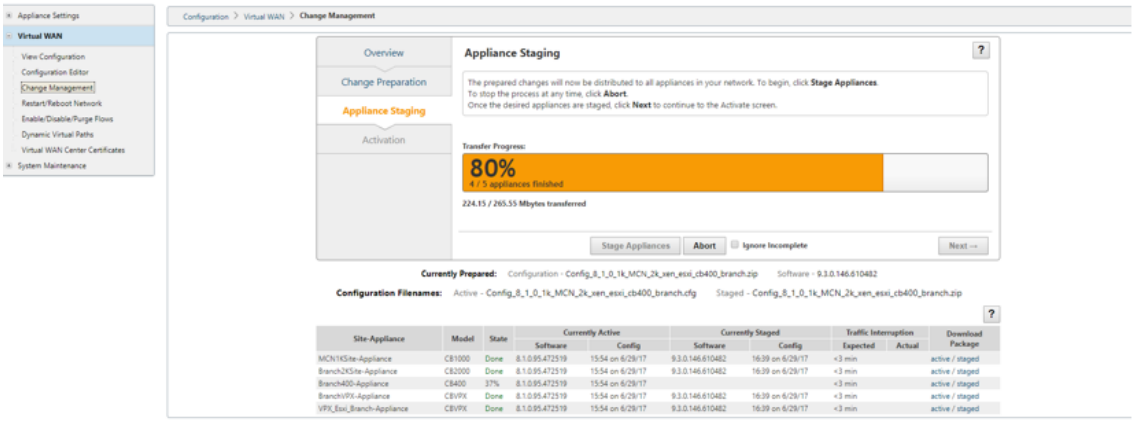


5. 接受许可协议后，您将导航到 设备分段，其中可以通过单击 舞台设备 来暂存设备。

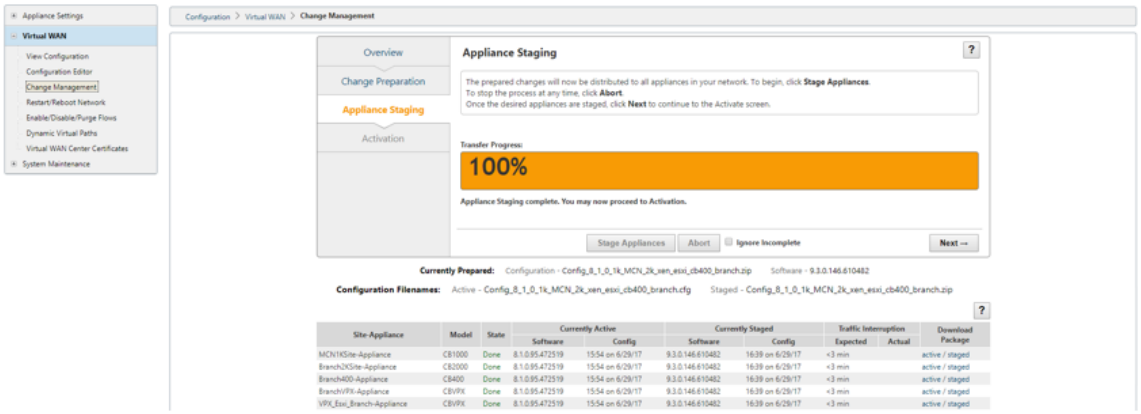


6. 传输进度 状态显示为准备软件包并将其转储到设备中的一部分。

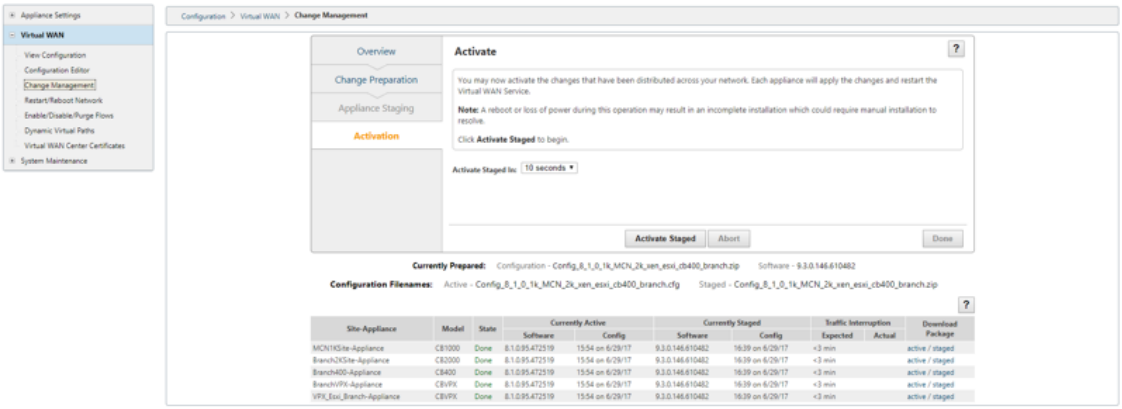


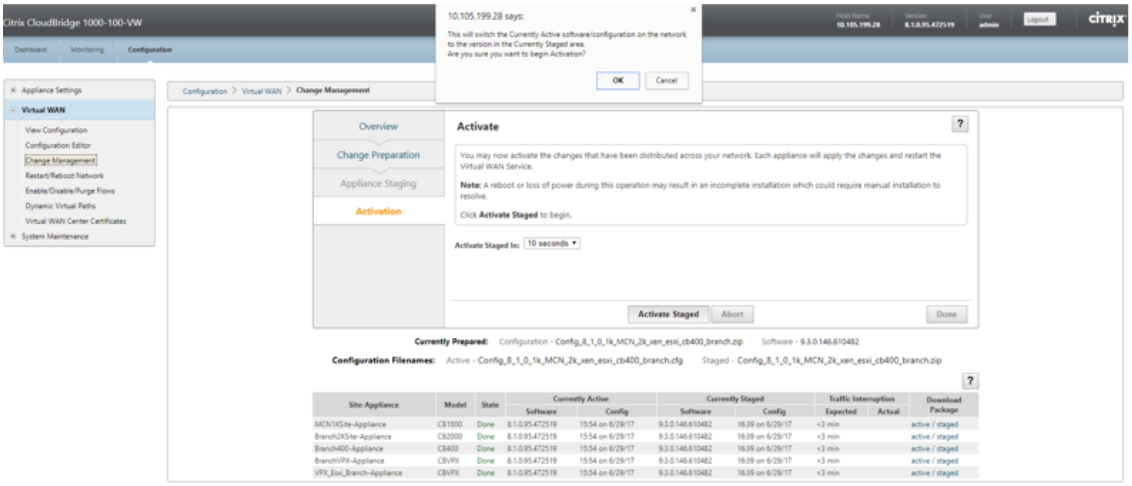


7. 当传输进度显示 100% 时，单击 下一 步，并启用按钮以继续。

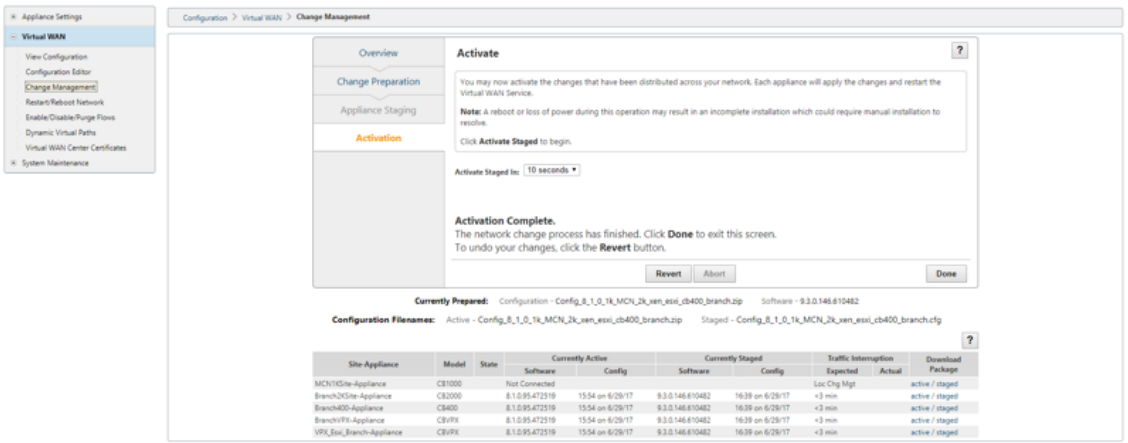


8. 在激活页面中，单击激活暂存以开始激活。





9. 180 秒的激活倒计时完成后单击 完成。

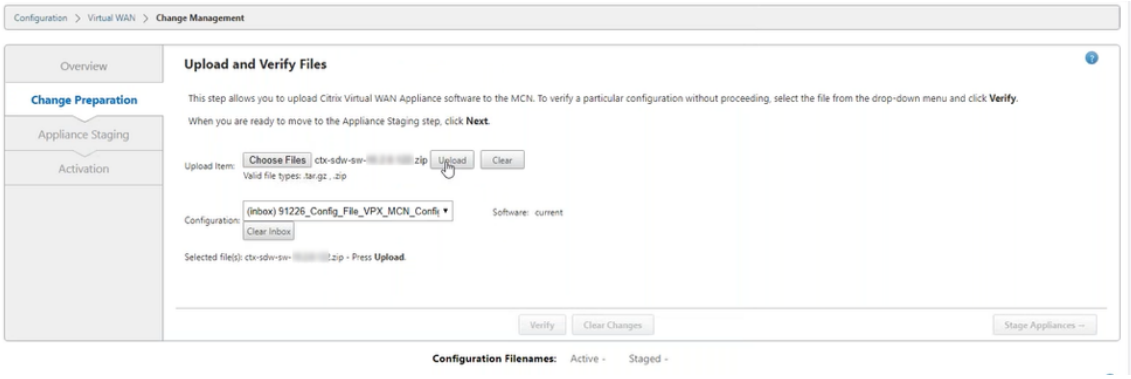


使用正常的虚拟 **WAN** 部署升级到 **11.4**

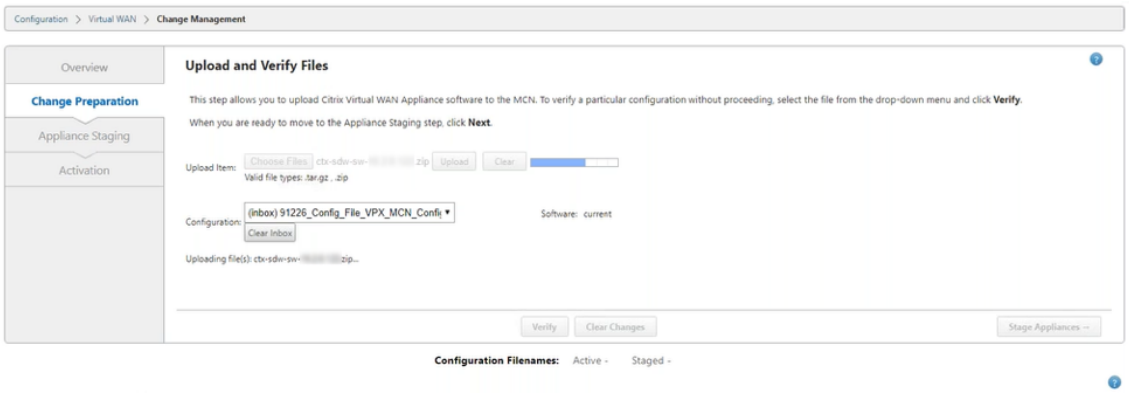
November 1, 2021

1. 在“更改管理”**>** “更改准备”页面中，单击“选择文 件”，然后选择 *ctx-sdw-sw-11.4.0.x.zip* 软件包文件。单击上载。

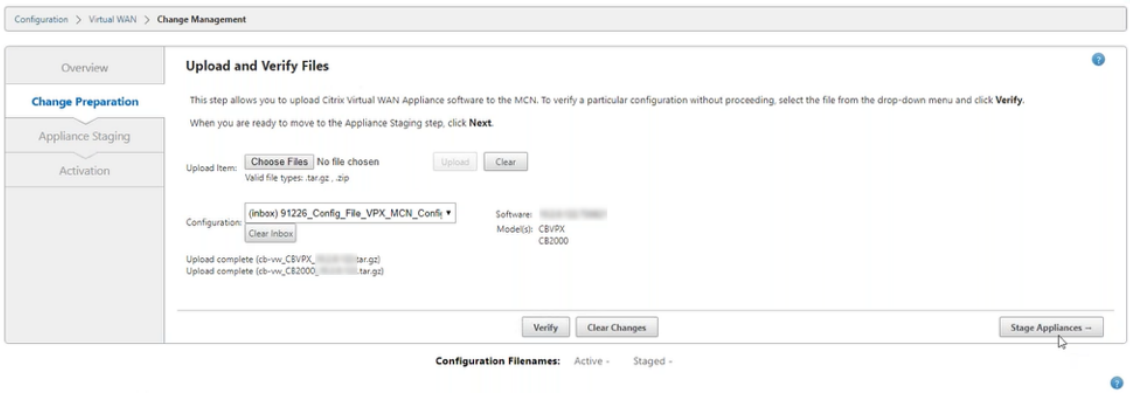
> 注意：
>
> 您可以从下载页面下 载 Citrix SD-WAN 11.4 版软件包。



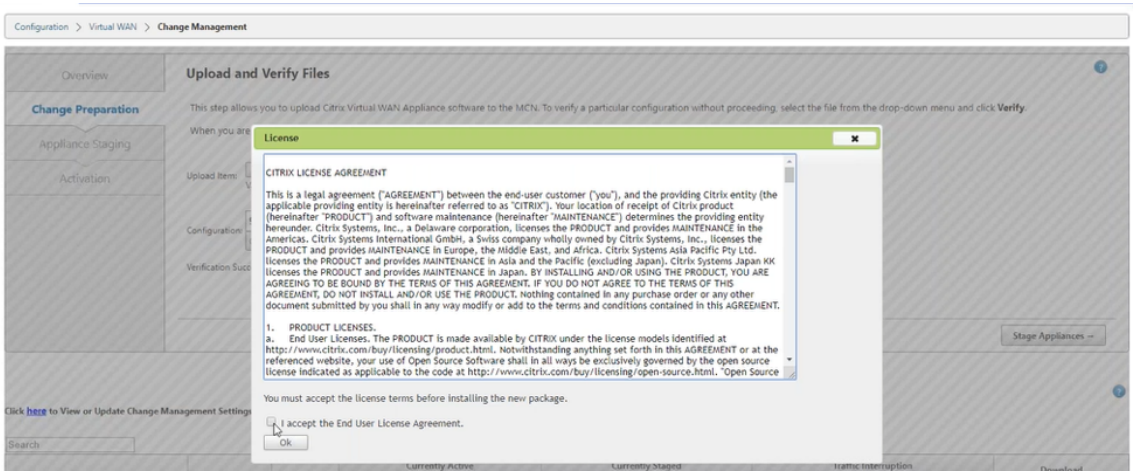
将显示一个进度条，以显示当前上载进度。



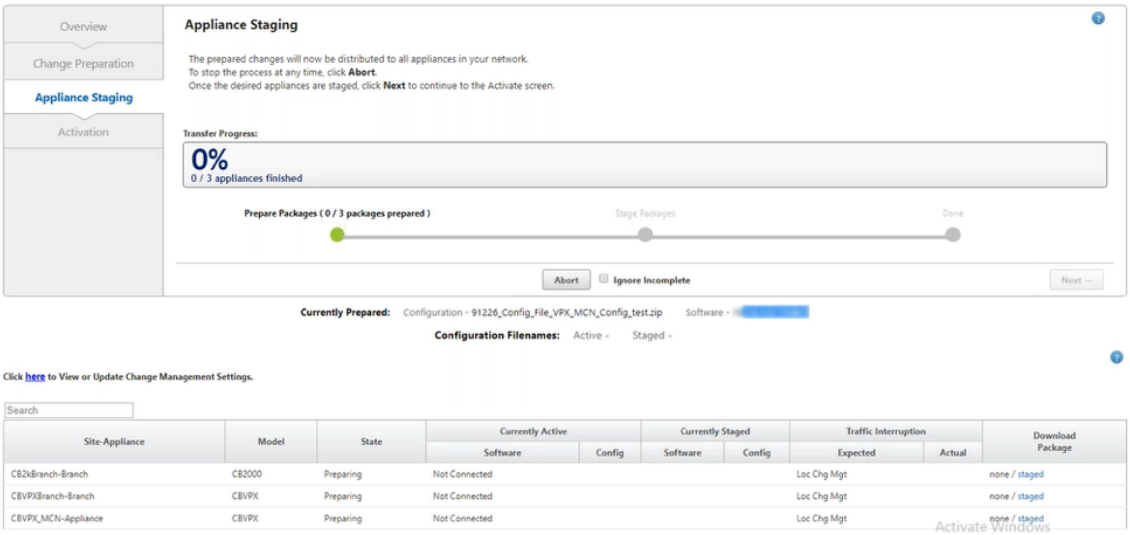
2. 上载过程成功后，将显示相关设备型号。将根据配置文件升级设备。



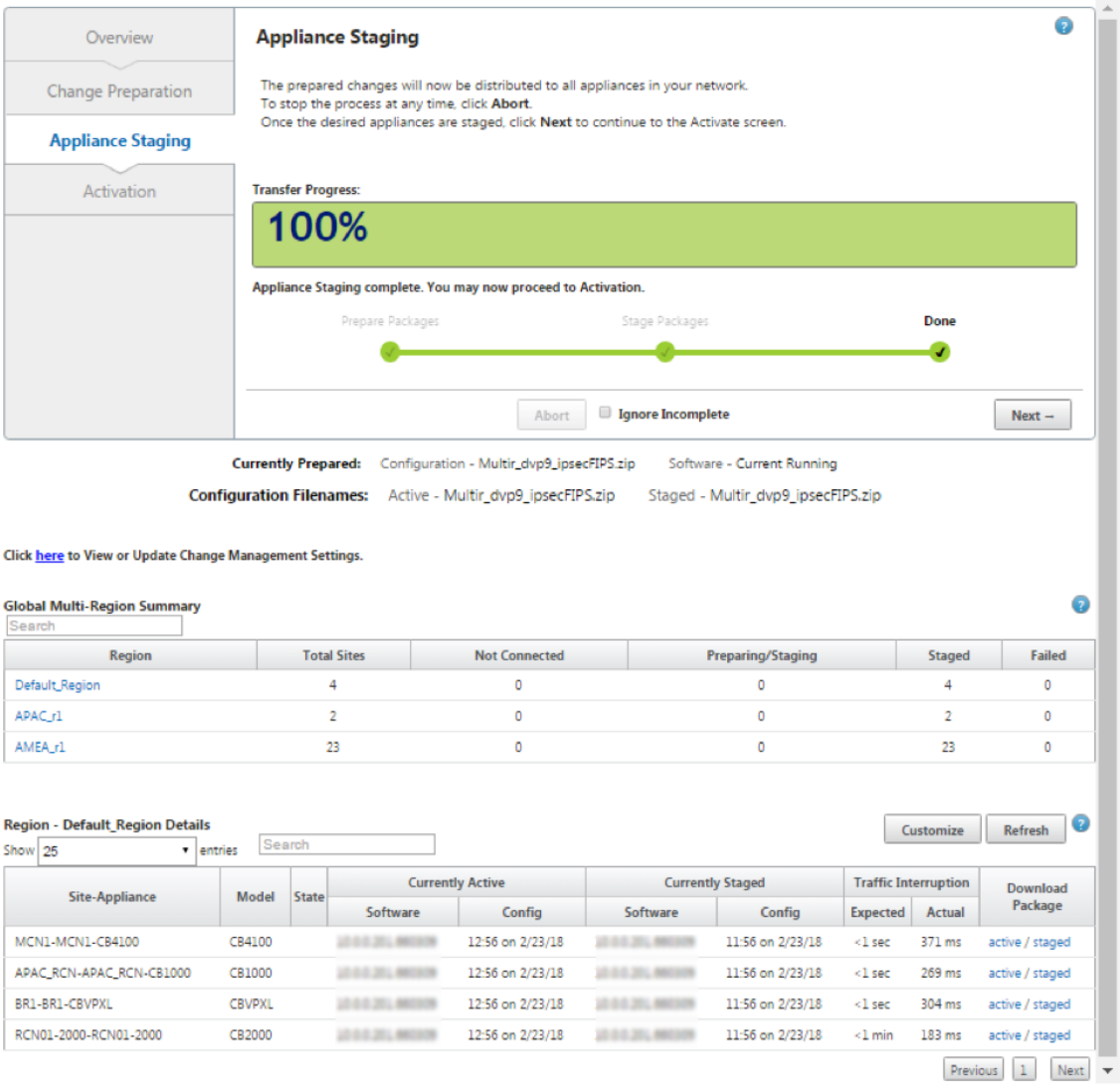
3. 单击 S **tage Appliance** 继续验证配置文件。此时将显示用户接受的许可协议页面。单击 我接受最终用户许可协议，然后单击 确定。



4. 设 备暂存 过程已启动。更改将分发到网络上的所有设备。此时将显示传输进度条并更新站点详细信息表。



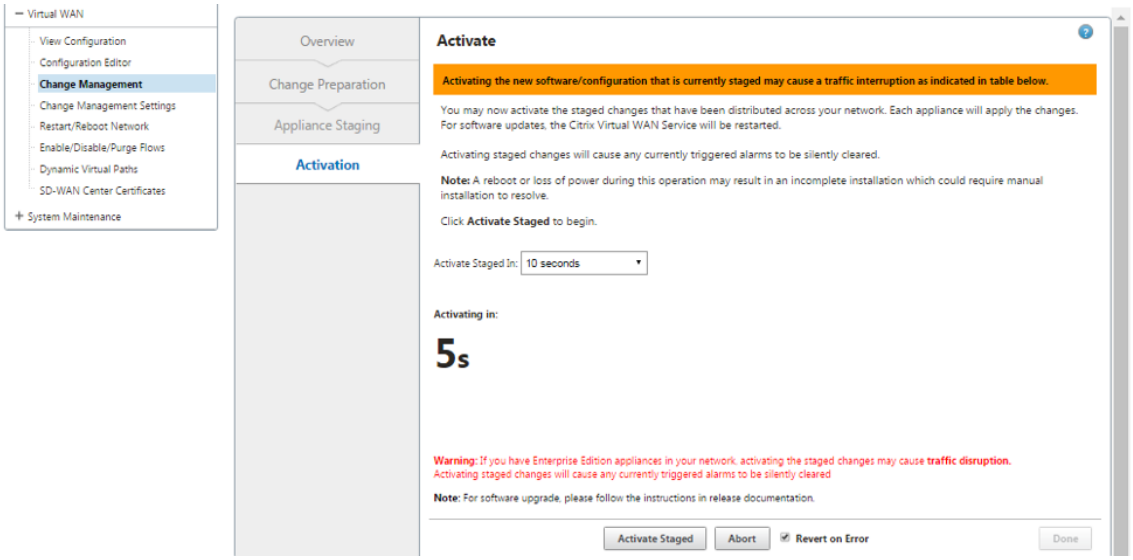
5. 转移进度 100% 完成后，单击“下一 步”继续激活。



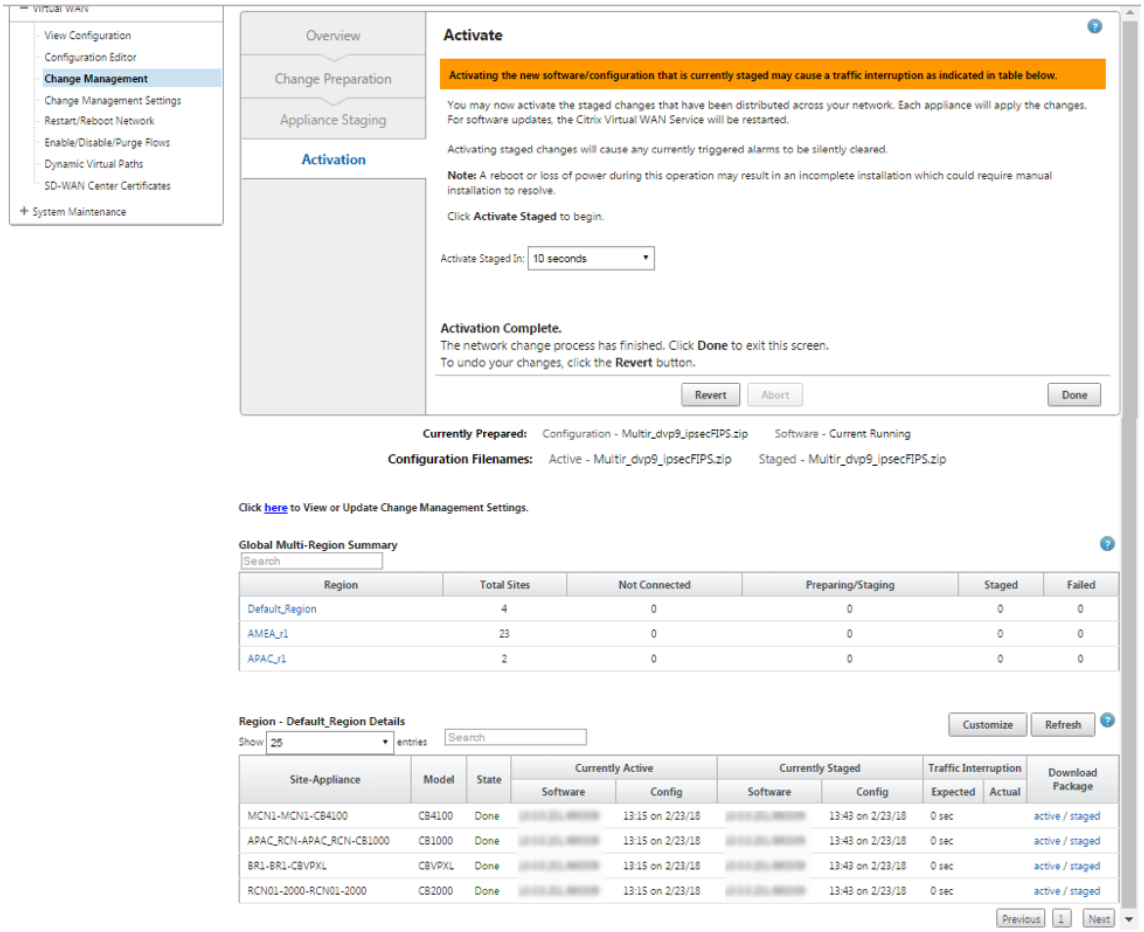
汇总表中显示的软件包配置的各种状态表明以下内容：

- 正 在准备-本地处理以准备要传输到设备的更新包。
- 准备区域软件 包-本地处理以准备要传输到 RCN 的更新包。（如果 RCN 是网络的一部分，则适用）。
- 百分比 -转移到设备的包裹的百分比。
- 打开包装 -远程设备处理以应用更新程序包。
- 转移区域 -包裹正在转移到 RCN。（如果 RCN 是网络的一部分，则适用）。
- 失败 -远程检测到传输不完整。
- 已取消 -在舞台设备期间选中“忽略未完成”时由用户取消
- 不需要 -准备好的暂存包不包含此站点设备名称。
- 未连接 -本地无法看到遥控器的活动软件包信息。

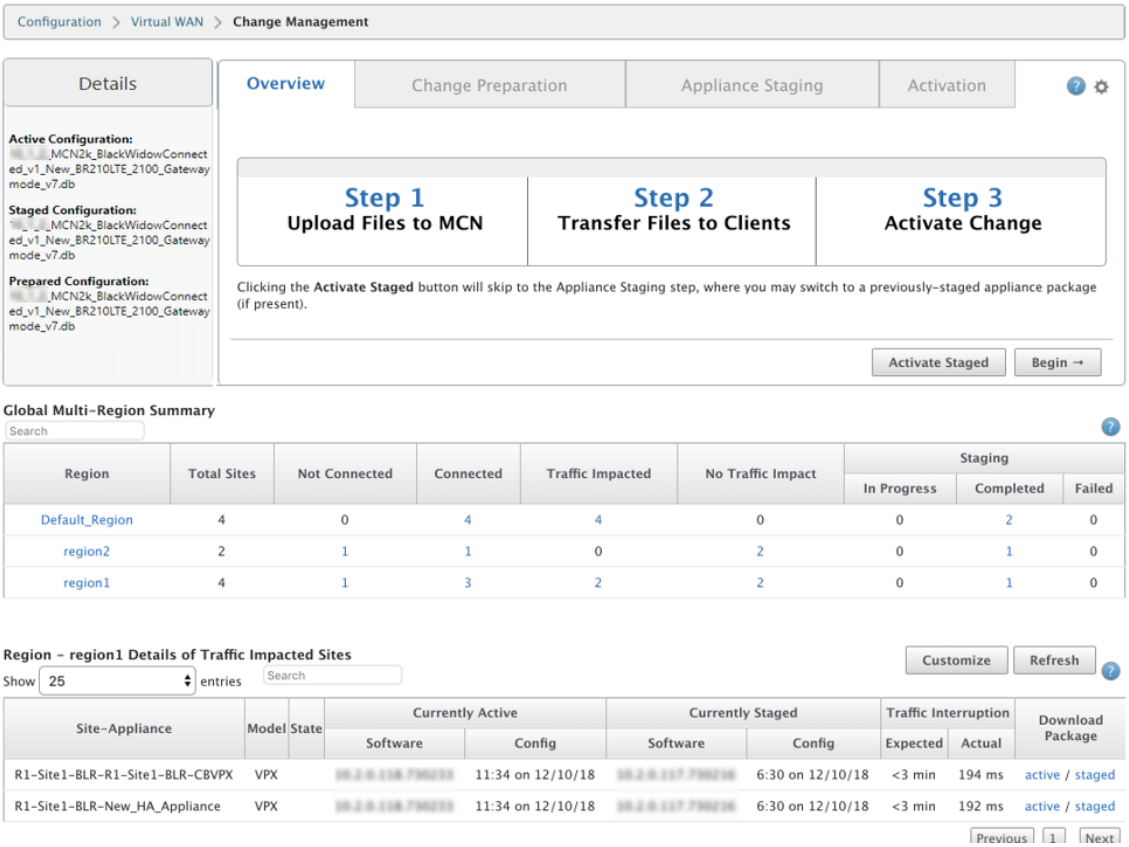
6. 单击 激活暂存 以激活暂存的软件。



7. 倒计时后，一条消息指示激活已完成。单击完成。

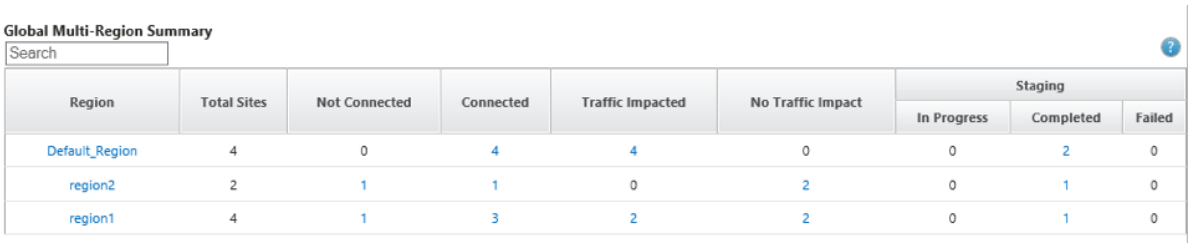


8. 导航到“更改管理”页面以查看转移状态。

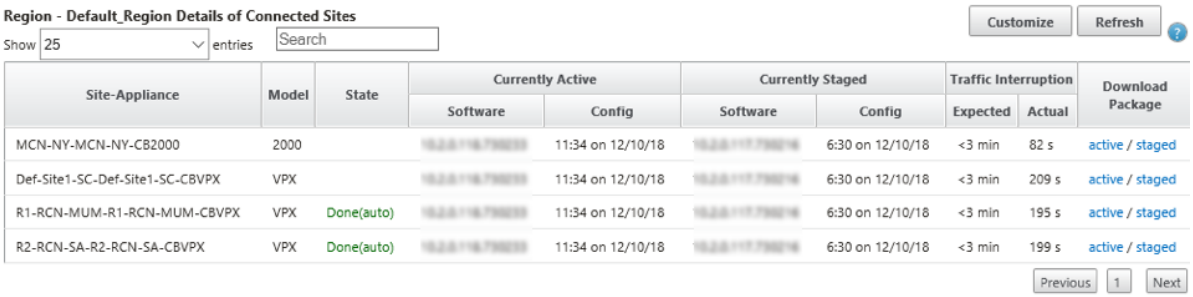


多区域汇总表提供以下详细信息：

- 区域—区 域名称
- 站点总 数-该地区的站点总数。
- 未连接 -区域中未连接的站点总数。
- 已连接 -区域内连接的站点总数。
- 受影响的流量 -区域内流量受到影响的站点总数。
- 无流量影响 -区域内流量不受影响的站点总数。
- 暂存进行中 -本地处理正在尝试为其准备更新包以便在区域中传输的站点总数。
- 暂存已完成-区域中已完成暂存的站点总数。
- 分段失败 -该区域中删除未完成转移的站点总数。



单击 全局多区域摘要 表条目链接以筛选特定于区域的配置报告。



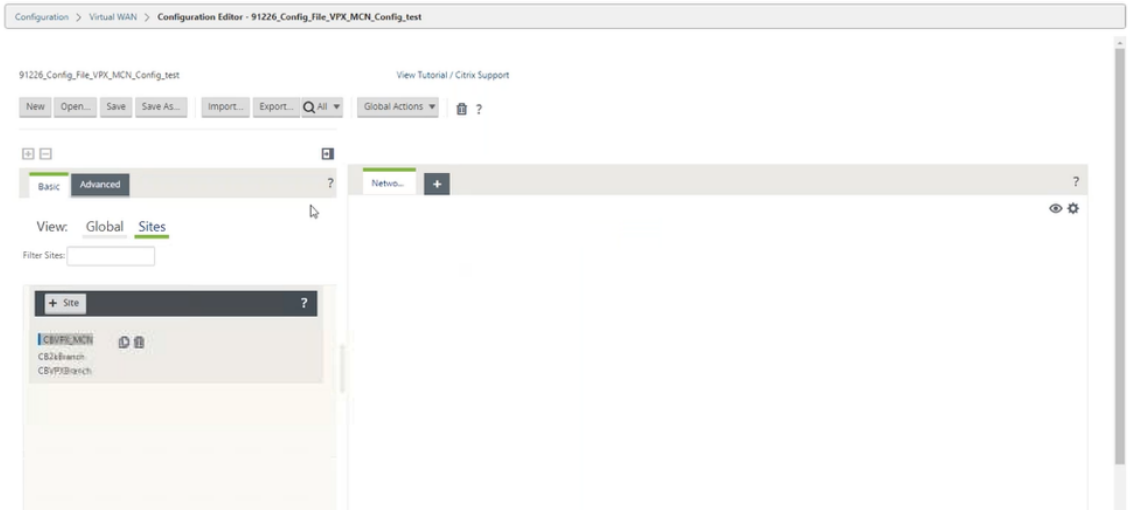
对于多区域部署，在每个 RCN 上导航到“更改管理设置”页面并安排相关组件的安装。默认情况下，MCN/RCN 会根据分支机构上的软件可用性分配每天 21:20:00 尝试安装的计划。有关详细信息，请参阅更 改管理设置

无需部署虚拟广域网即可升级到 **11.4**

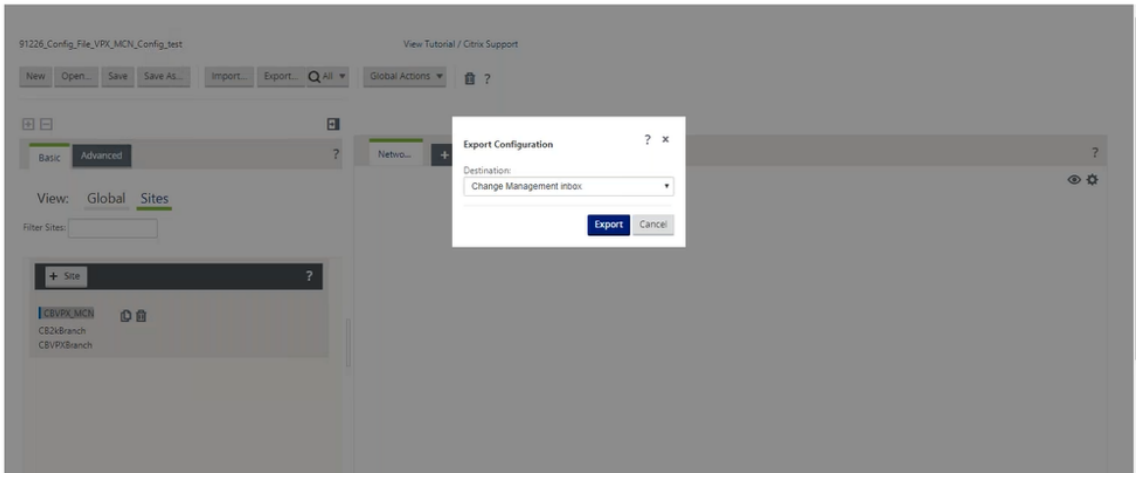
November 1, 2021

> 注意：要配置最新的 11.4 功能，请将 MCN 设备重新设置为 11.4 软件。有关详细信息，请参阅 重新映像 Citrix SD-WAN 设备软件

1. 使用配置 编辑器准备配置，并使用有效名称保存配置。有关详细信息，请参阅 配置 主题。

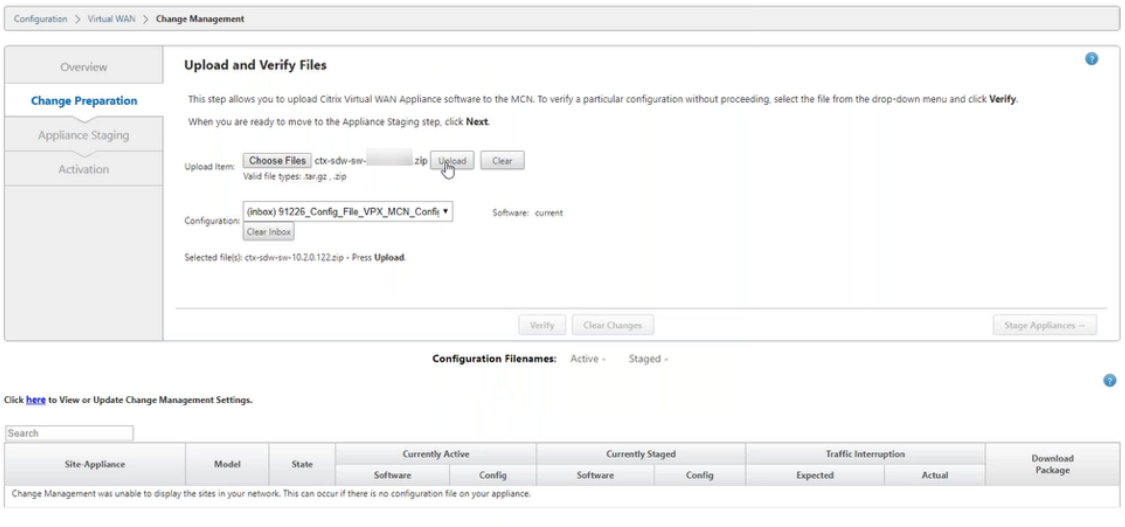


2. 将保存的配置导出到更改管理。单击 导出，然后选择 更改管理收件箱 作为目标。单击导出。

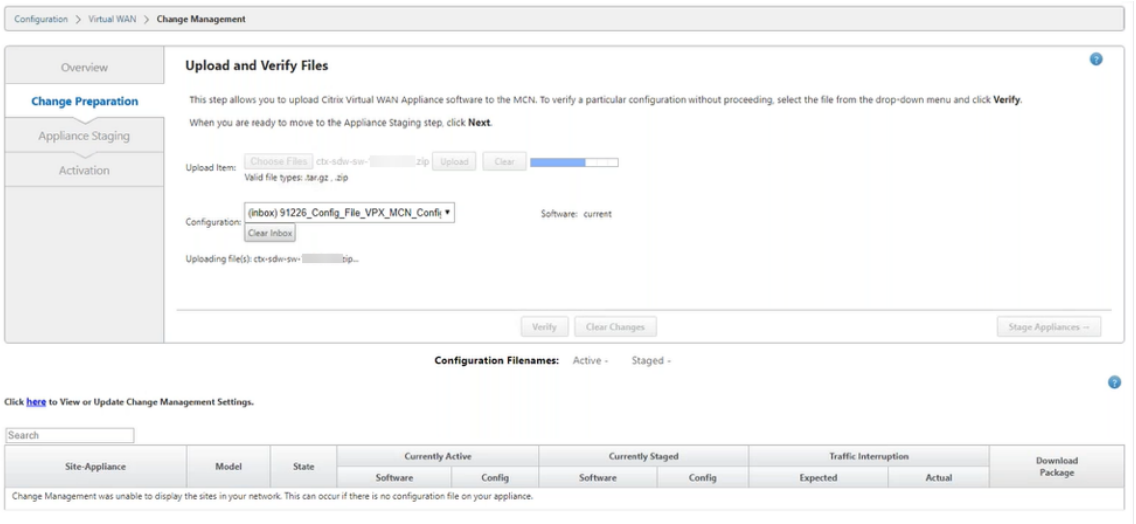


3. 在“更改管理” > “更改准备”页面中，单击“选择文 件”，然后选择 *ctx-sdw-sw-11.4.0.x.zip* 软件包文件。单击上载。

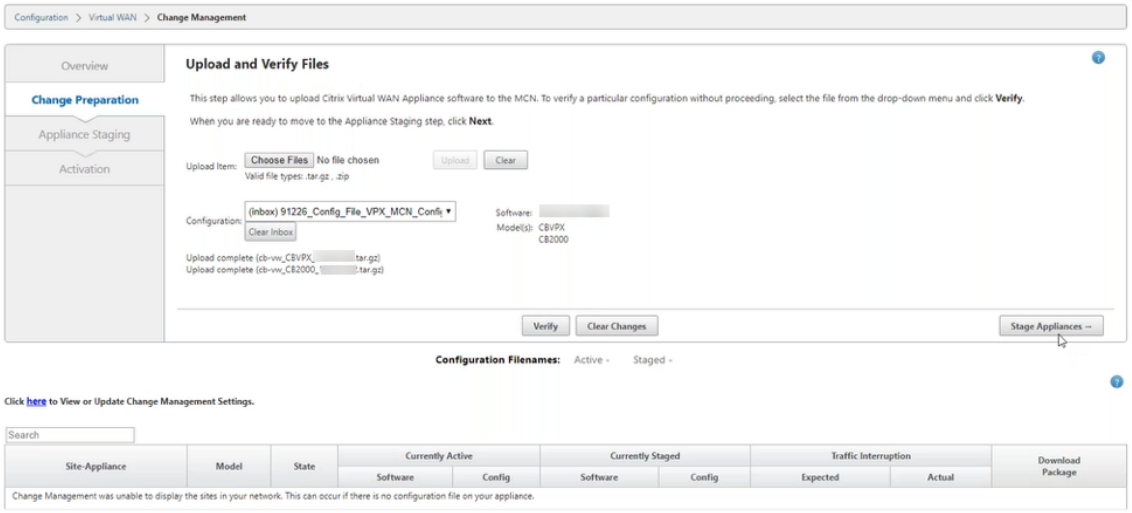
> 注意：
>
> 您可以从下载页面下 载 Citrix SD-WAN 11.4 版软件包。



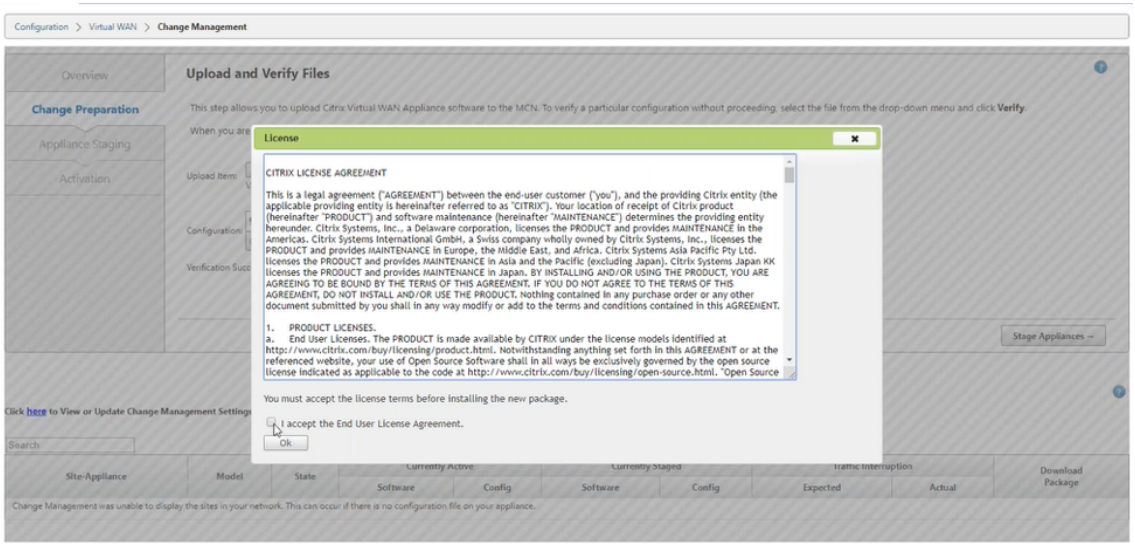
将显示一个进度条，以显示当前上载进度。



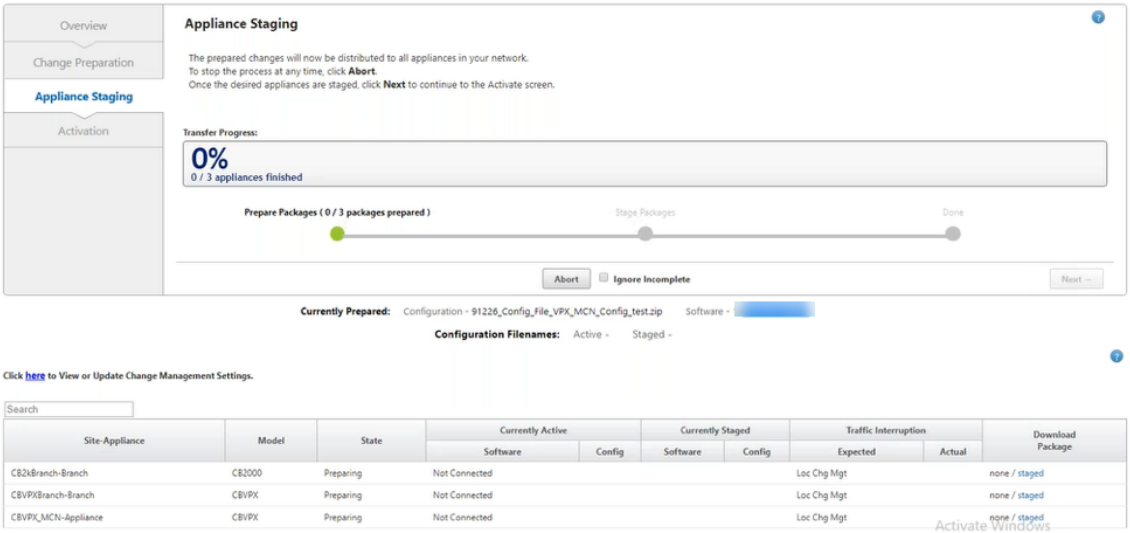
4. 上载过程成功后，将根据包含每个分支平台模型信息的配置文件显示相关模型。



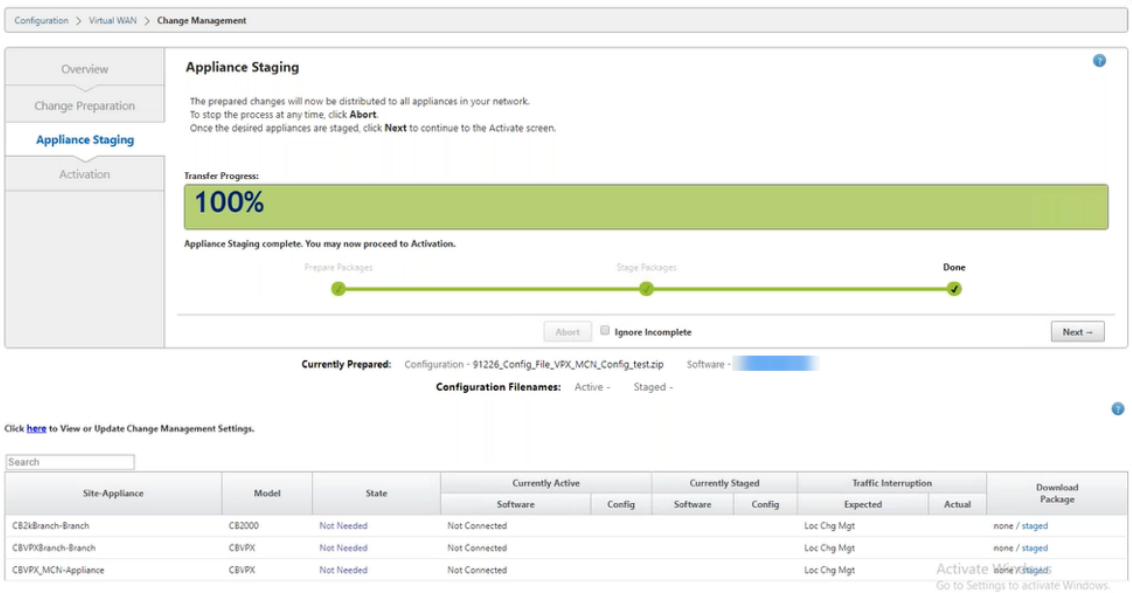
5. 单击 S **tage Appliance** 继续验证配置文件。此时将显示用户接受的许可协议页面。单击 我接受最终用户许可协议，然后单击 确定。



6. 设 备暂存 过程已启动，更改将分发到网络上的所有设备。此时将显示传输进度条并更新站点详细信息表。

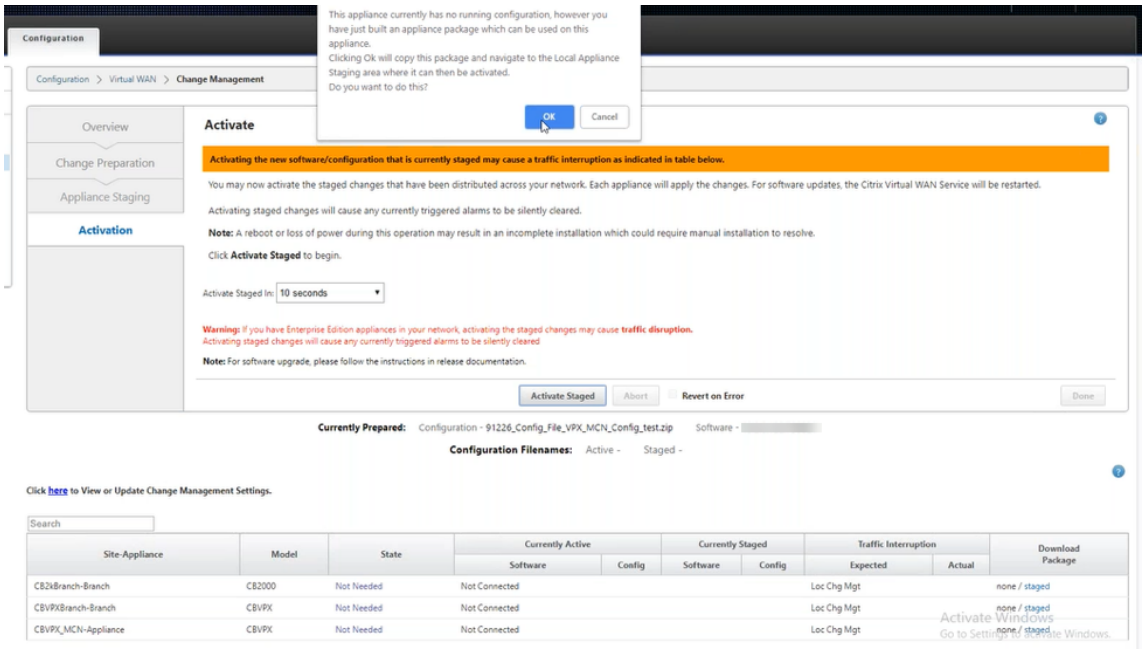


7. 转移进度 100% 完成后，单击“下一 步”继续激活。

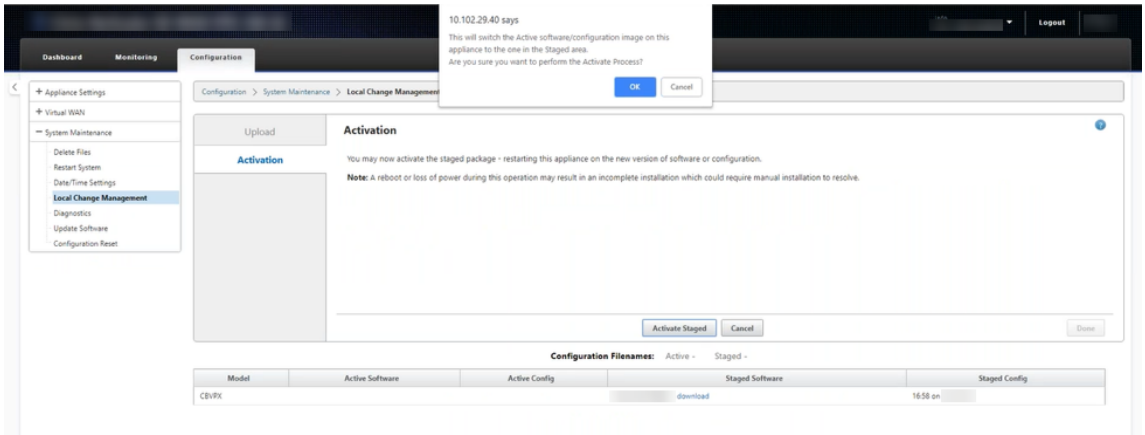


8. 单击激活暂存。将显示用户接受弹出消息，因为这是设备首次暂存。

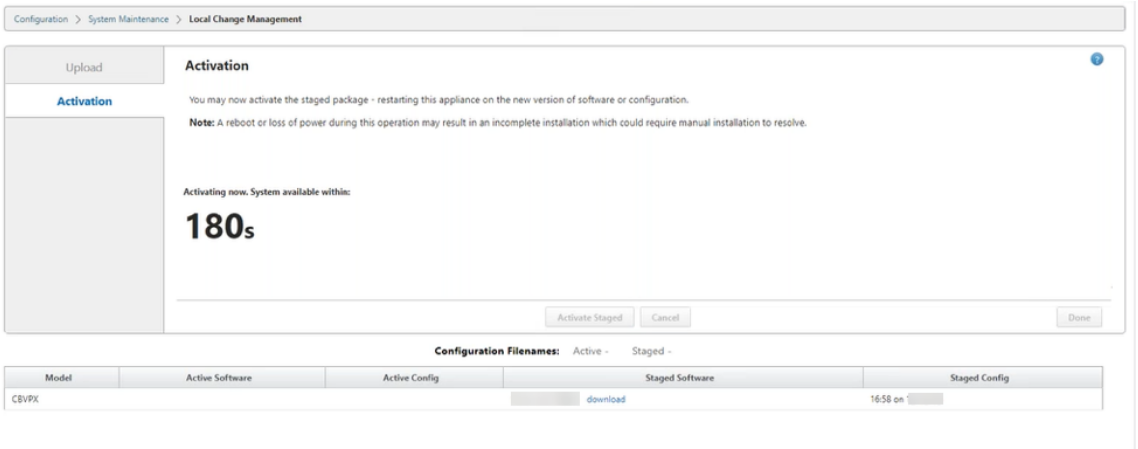
   您将被重定向到 本 地更改管理 页面以激活本地设备。单击“确定”继续。



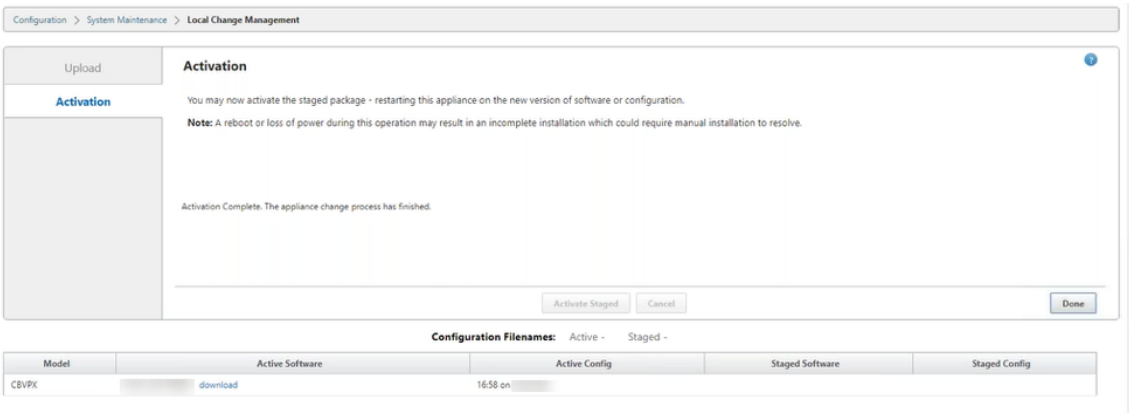
9. 单击在本地变更管理中 激活暂存。此时将显示激活确认消息。单击“确定”。



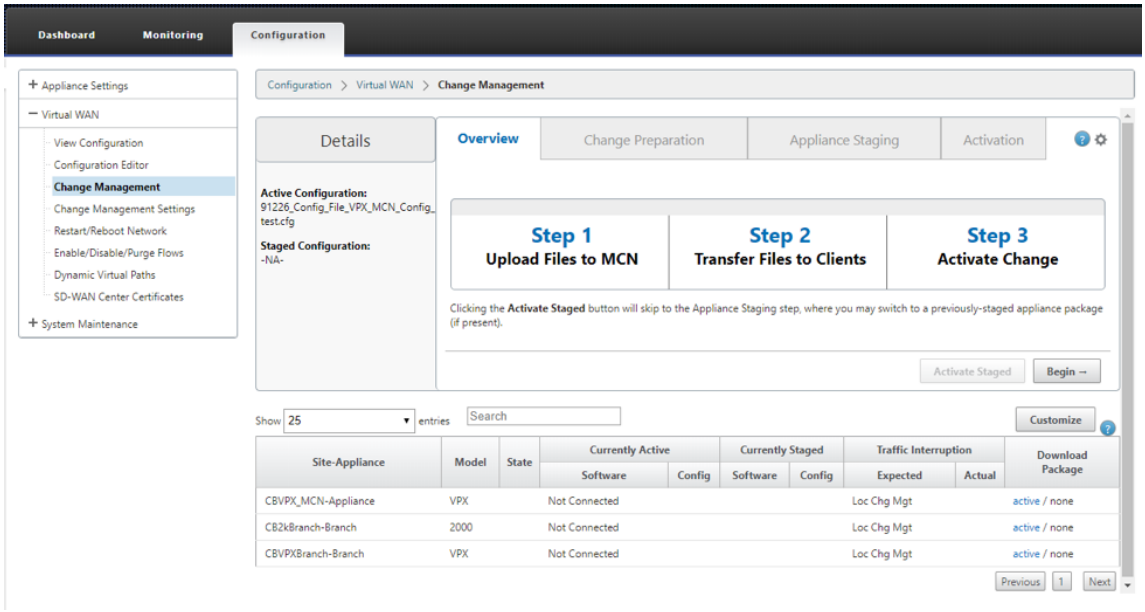
激活以 180 秒的倒计时器开始。



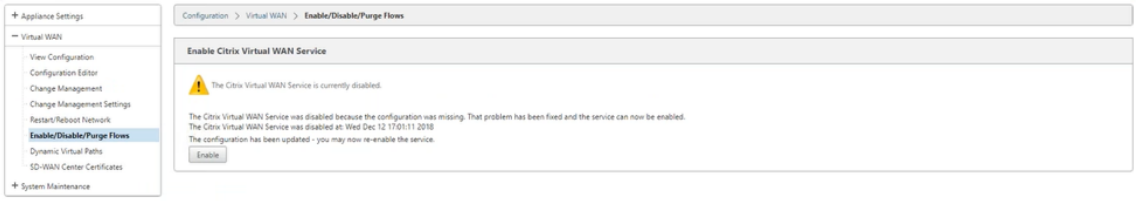
10. 倒计时后，一条消息指示激活已完成。单击 完成，设备将重新启动。



11. 设备重新启动后，导航到“更改管理”页面以下载需要仅通过 Virtual WAN 软件升级引导到网络的相应分支机构的本地更改管理软件包。



12. 在设备上启用 SD-WAN 服务。导航到 虚拟 **WAN >** 启用/禁用/清除流 程，然后单击 启用。



要进一步配置新站点并将其添加到网络中，请按照 配置分支节点 主题中的过程进行操作。

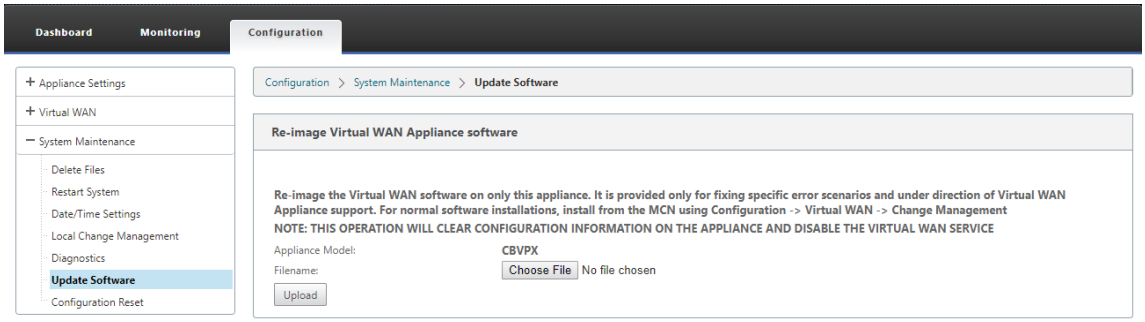
重新映像 **Citrix SD-WAN** 设备软件

June 22, 2021

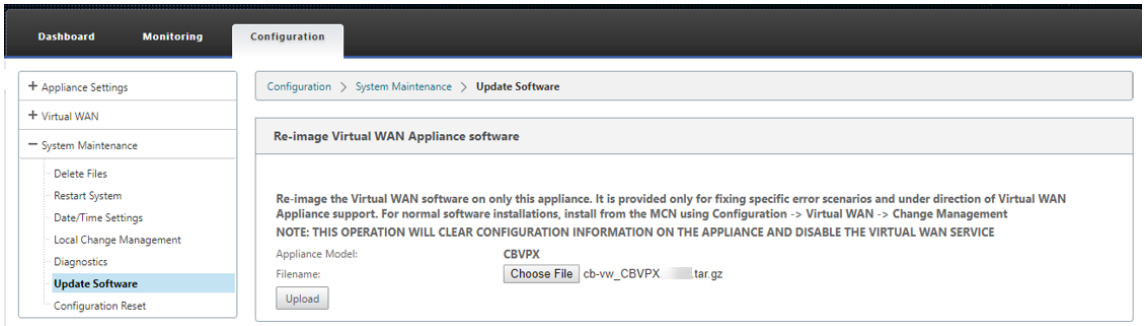
从 Citrix 下载 门户下载所需 Citrix SD-WAN 软件版本和平台的 *.tar.gz* 文件。

要重新映像 Citrix SD-WAN 设备软件，请执行以下操作：

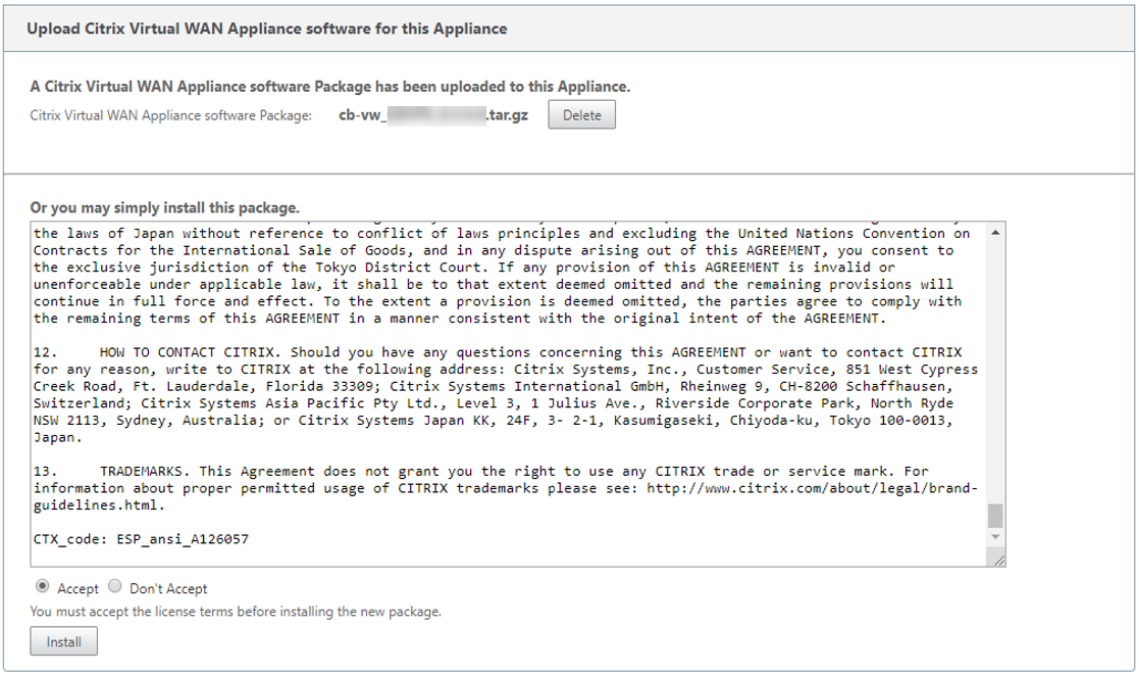
1. 在 SD-WAN 设备 GUI 中，导航到 配置 > 系统维护 > 更新软件。



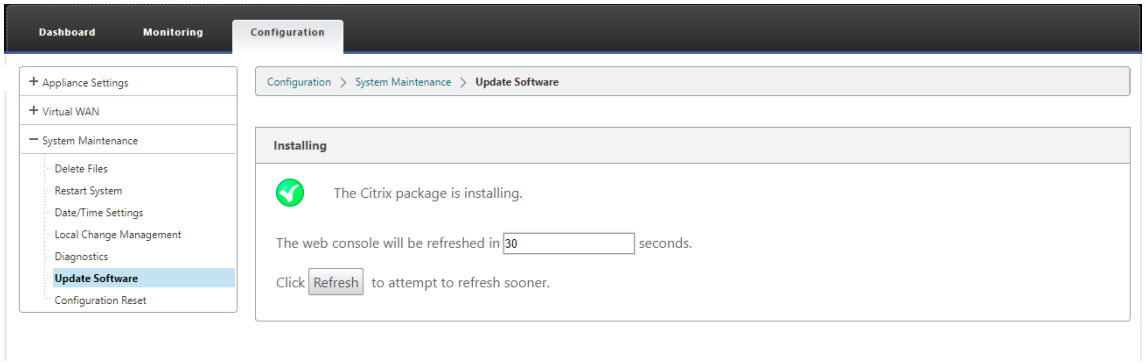
2. 单击 选择文件，然后选择下载的 Citrix SD-WAN 设备软件。单击上载。



3. 阅读并接受许可条款。单击 接受，然后单击 安装。



软件更新大约需要 35 秒，之后设备重新启动。



使用本地更改管理进行部分软件升级

June 22, 2021

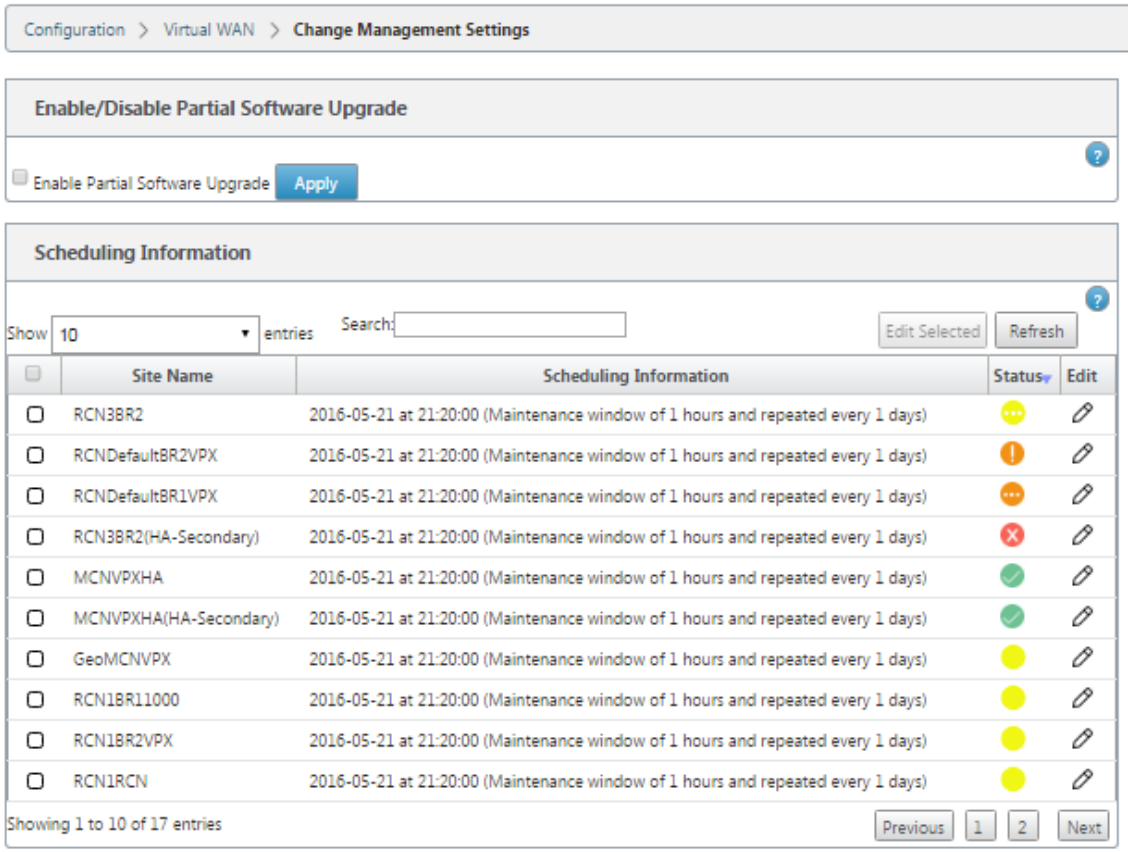
> 重要
>
> 默认情况下，部 分软件升级 选项处于禁用状态。

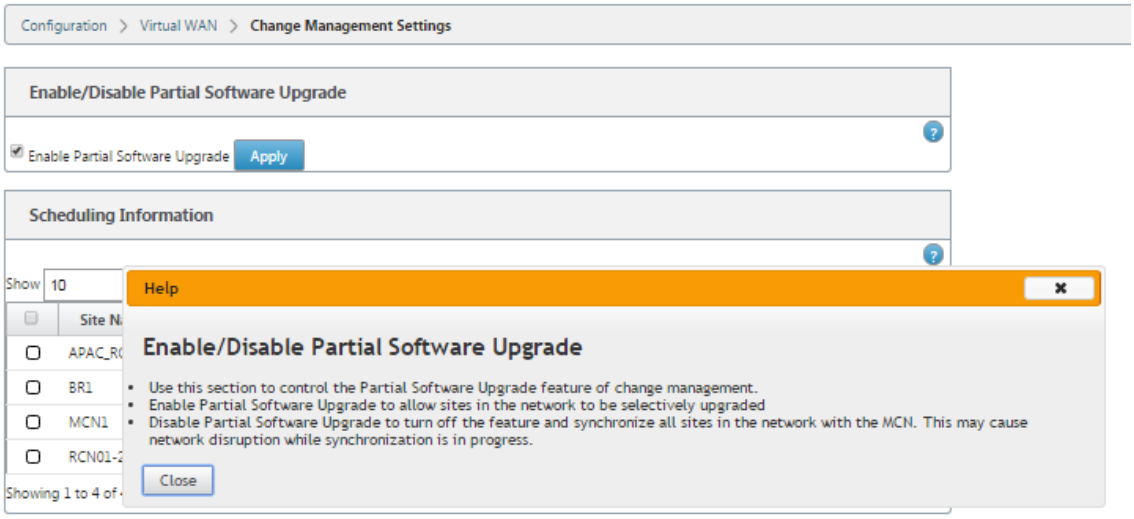
您可以使用 本 地更改管理 选项在客户端站点的子集上安装较新的 SD-WAN 软件发布版本。这是通过部分软件升级功能实现的，该功能允许网络管理员选择性地升级网络中站点上的软件，而无需同时升级所有站点。此功能的一个特定用例是管理员在少数分支站点上测试新软件，然后在网络中的所有站点上安装新软件。

先决条件和要求

在继续执行部分软件升级之前，请查看以下要求：

1. 有一个活动的 SD-WAN 版本 10.0 或更新的软件。单击 启用部分软件升级 复选框。如果取消选中此复选框，则当前在 MCN 设备上运行的软件将应用到运行活动虚拟路径的分支机构。





2. 使用 MCN 更改管理 过程暂存新版本的软件，其主要版本号与活动软件相同，配置与活动配置相同。
3. 新软件应与活动软件相同的主要版本软件。次要版本可以是不同的软件版本。
4. 新软件必须首先在 MCN 的所有站点上分级。停止在更改管理的激活暂存步骤。

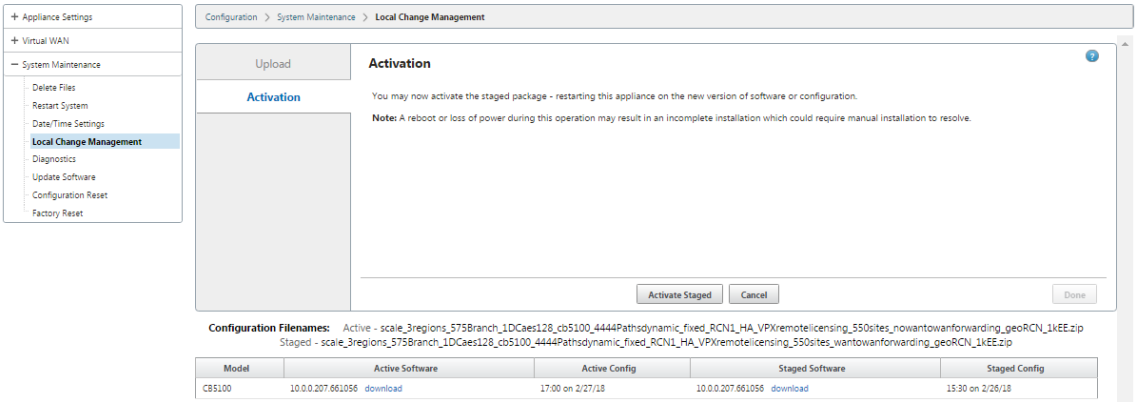
   对于活动站点和部分站点的配置，MCN 和分支站点上的软件必须相同。不可能在部分升级的站点上启用不同的功能集。继续到各个站点以执行 本地更改管理。有关高可用性部署，请参阅以下说明。

要执行部分 **SD-WAN** 软件升级：

在两种情况下，您可以在分支节点上执行部分 SD-WAN 软件升级：高可用性模式和非高可用性模式。

升级没有高可用性模式的分支节点

1. 在 Citrix SD-WAN Web 管理界面中，导航到需要通过部分站点升级过程进行升级的分支站点。
2. 打开 本地变更管理。单击下一步。
3. 单击激活暂存。现在，每个分支站点都将安装新的软件版本。



在高可用性模式下升级分支节点

1. 在 SD-WAN Web 管理界面中，导航到需要通过 部分站点升级 升级的分支站点。
2. 禁用备用设备上的服务。
3. 在主设备上，打开 本地更改管理。
4. 单击激活暂存。此设备现在将使用新的软件版本进行安装。
5. 在备用设备上，打开 本地更改管理。
6. 单击激活暂存。备用设备现在将使用新的软件版本进行安装。
7. 主设备和备用设备完成激活过程后，在备用设备上启用服务。

升级网络

准备好使网络同步时，导航到 MCN 网络更改管理屏幕，然后单击激活暂存。

通过 USB 将 WANOP 转换到 Premium Edition

June 22, 2021

> 注意
>
> 只有 SD-WAN 1000 和 2000 WANOP 设备可以转换为 SD-WAN Premium Edition 设备。

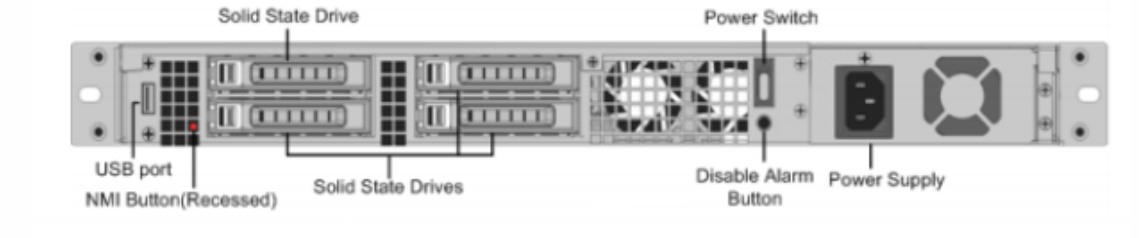
准备工作

- 确保您仅转换 1000 台设备，而不是转换 1000 台设备。1000 WS 设备不支持转换到 SD-WAN 高级（企业）版设备。
- 确保您拥有登录到现有 *Dom-0 - root/nsroot* 的默认凭据。

升级过程

转换过程分为两个步骤，涉及以下步骤：

- 将封闭的 USB 记忆棒插入 Citrix SD-WAN 设备。
- 验证串行控制台是否已连接并继续转换过程。



如何使用 USB 记忆棒进行转换

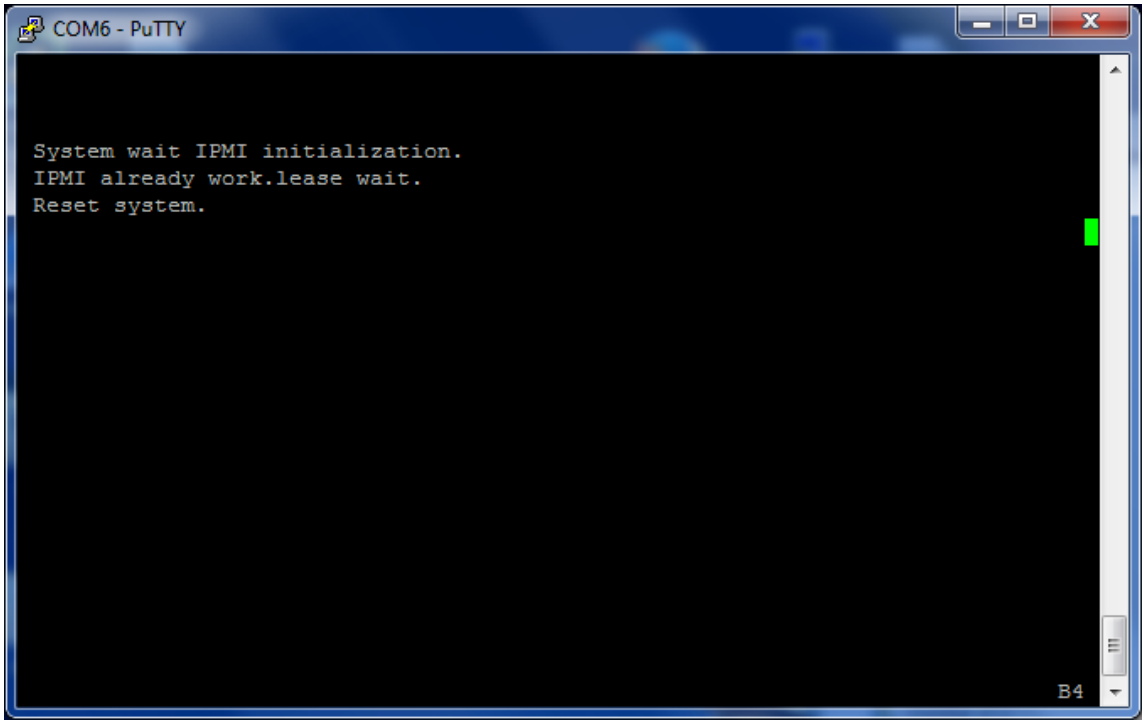
使用 USB 记忆棒升级设备：

1. 将封闭的 USB 记忆棒插入 Citrix SD-WAN 设备。
2. 连接到设备的串行控制台。
3. 重新启动设备。
4. 在引导过程中，当您看到光标在屏幕上移动时，请执行以下操作：
   a) 按住 **ESC** 键。
   b) 按住 **SHIFT** 键。

c) 按数字 **1** 键 (SHIFT +1 = !) 并释放所有密钥。

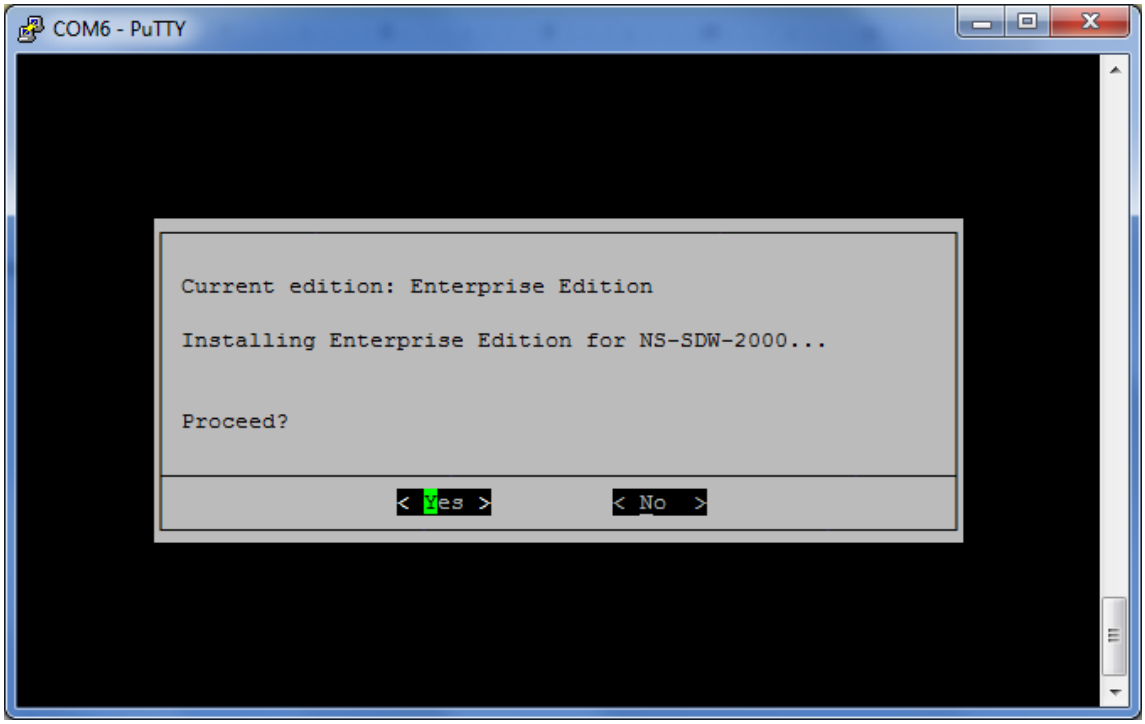
d) 重复步骤 a、b 和 c，直到光标停止移动。

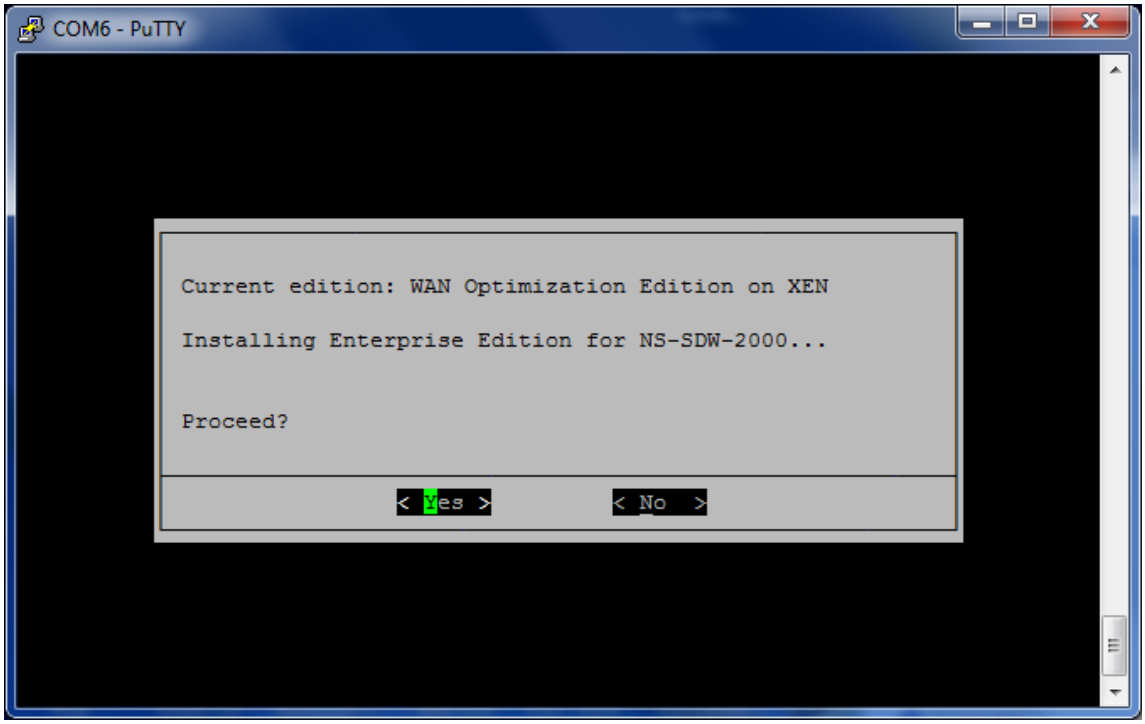
> 注意
>
> 上述步骤应在设备重新启动过程中执行。按键笔划应该发生在 BIOS 后期阶段，如步骤 4 所述。



5. 加载 BIOS 时，请选择外部 USB 驱动器，例如，PNY USB 2.0 FD 1100 启动设备。如果您订购了外部 USB 驱动器，则由 Citrix 发货。

   如果平台支持多个版本，例如 1000 和 2000，则需要选择要使用的平台版本。因此，请先选择高级（企业）版，然后再确认。





6. 出现提示时，选择 **Enterprise Edition** 软件升级选项。
7. 升级过程在 20-30 分钟内完成。系统在 1-2 分钟后重新启动，并显示登录提示。对于 1000 平台版本，升级过程大约需要一个小时，因为更新内部 USB 驱动器本身需要大约半小时。
8. 程序完成后拔下 USB 记忆棒。

引用

- 有关 Citrix SD-WAN 产品的许可，请参阅以下网址的支持链接：http://support.citrix.com/article/ctx131110
- 有关 Citrix SD-WAN 的文档和发行说明信息，请参阅；</en-us/citrix-sd-wan.html>。

将 **Standard Edition** 转换为 **Premium Edition**

June 22, 2021

> 重要
>
> 在版本 10.1 中，平台版本“Enterprise”更名为“Premium”。

要执行从标准版到高级（企业版）版的平台转换，请执行以下操作：

1. 在本地导出配置。
2. 从 更改管理 页面下载 活动包。
3. 使用从 系统维护 > 更新软件 **>** 重映虚拟 **WAN** 设备软件 ** 中下载的软件包升级设备 **。
4. 单击选择文件以提供 *cb-vw_CB1000_x.x.x.x.tar.gz* 文件。其中 x.x.x.x 是 SD-WAN 软件发布版本。
5. 单击上载。选择 接受，然后单击 安装 继续。
6. 安装高级（企业）版许可证。

7. 使用上述步骤 2 中下载的活动包对设备执行 本地更改管理。

以下是 WAN 优化配置的条件：

1. 如果站点角色是 MCN，则 WAN 优化配置仅进行：
   - 软件升级是使用.zip 软件包 (SSUP) 完成的
   - 许可证是 PE
   - 虚拟 WAN 服务已启用
2. 如果站点角色是客户端，则 WAN 优化设置仅进行：
   - 软件升级是使用.zip 软件包 (SSUP) 完成的
   - 虚拟 WAN 服务已启用
   - 许可证是 PE
   - 虚拟路径由 MCN 形成
3. 要立即配置 WAN 优化，请从相应站点的“更改管理设置”页面中将维护时段值设置为 0。

USB 重新映像实用程序

June 22, 2021

SD-WAN USB 重映像实用程序允许通过从可引导的 USB 盘安装干净的出厂映像来重新调整硬件用途。Citrix 提供了一个带有预加载 SD-WAN 软件映像的 USB 棒现场可更换单元 (FRU)。使用 USB FRU 将设备重新映像到所需支持的版本（SE/PE/AE）。使用的设备许可证/配置决定了设备版本。

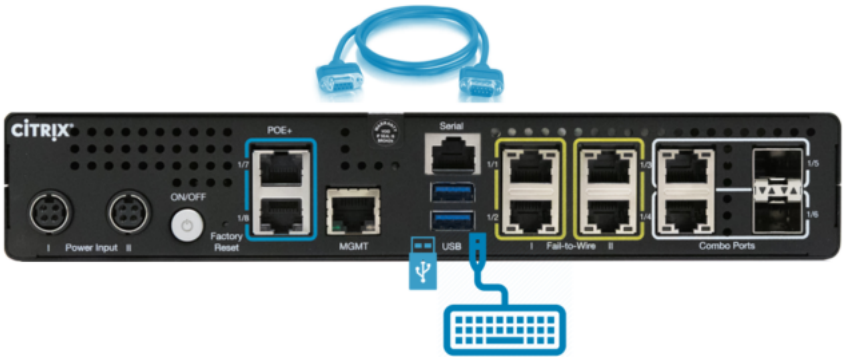
下表提供了有关可用 USB FRU 映像以及 SD-WAN 设备支持的版本的详细信息。

设备	USB FRU 图像	支持的版本
Citrix SD-WAN 110	11.1.1.39	SE
Citrix SD-WAN 210	10.2.7.17	SE, AE
Citrix SD-WAN 410	10.2.3.32	SE
Citrix SD-WAN 1100	10.2.7.17	SE, PE, AE
Citrix SD-WAN 2100	10.2.7.17	硒, PE
Citrix SD-WAN 4100	10.2.7.17	SE
Citrix SD-WAN 5100	10.2.7.17	硒, PE
Citrix SD-WAN 6100	10.2.7.17	硒, PE

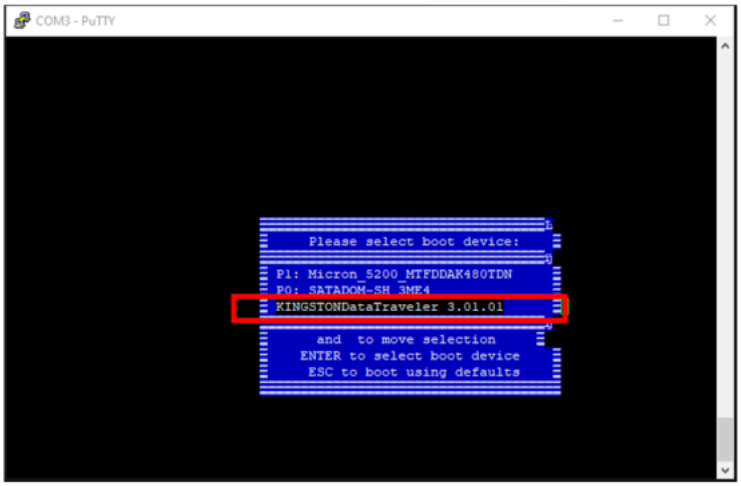
要执行 USB 重映像，请执行以下操作：

1. 将 Citrix 提供的 U 盘插入设备的其中一个 USB 端口。
2. 将 USB 键盘连接到另一个 USB 端口。

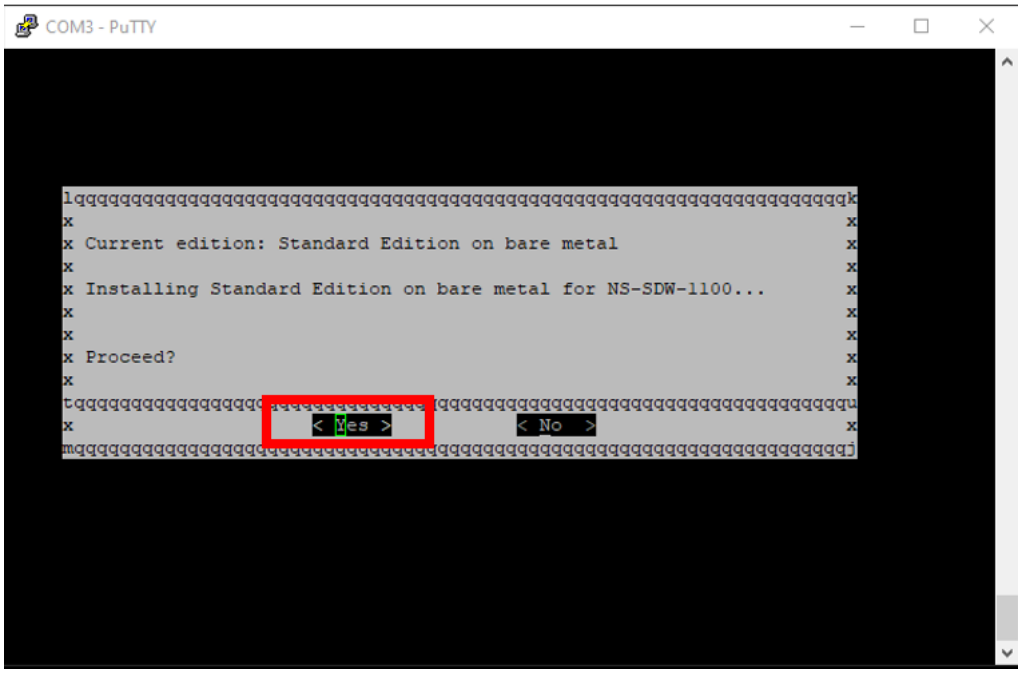
> 提示
>
> 如果设备上有单个 USB 端口，请使用 USB 拆分器同时连接 U 盘和 USB 键盘。



3. 以管理员身份登录串行控制台，并通过 CLI 发出重新启动设备命令。
4. 启动时连续按 USB 连接键盘上的 **F11** 键，或通过串行控制台连接按 **SHFT+ESC+1** 。
5. 从启动设备菜单中选择 USB 驱动器，然后按 Enter 键。



6. 根据平台支持的版本的不同，屏幕会出现，请求允许继续安装。选择是。



> 注意
>
> 对于 PE 和 AE 重新映像，设备可能会以标准版的形式显示在 GUI 中，直到完成相应的操作系统和 PE/AE 许可证安装。

安装需要 30 分钟才能完成。在重新映像过程中，请勿关闭设备电源。它可能会重新启动多次。

7. 默认情况下，出厂映像启用了 DHCP。所有平台上的默认管理 IP 地址是 192.168.100.1。使用它来访问 SD-WAN GUI。

   您还可以通过发出以下命令从串行控制台手动配置管理 IP：

   发出命令 *management_ip*

   发出命令 *set interface 192.168.100.1 255.255.255.0 192.168.100.254*

   发出命令 *apply*

8. 默认情况下，软件将升级到 SE。根据需要安装 PE 或 AE 许可证，具体取决于设备支持的版本。

   > 注意
   >
   > 您只能通过 SD-WAN Orchestrator 配置和管理自动曝光功能。有关详细信息，请参阅边缘安全。

Citrix SD-WAN 许可证选项

June 22, 2021

有四个 Citrix SD-WAN 版本，每个版本都具有不同的 SD-WAN 功能集或子集。您安装的许可证类型决定了平台版本-标准版、WANOP 版、高级版和高级版装置。

> 注意
>
> 安装和应用许可证时，请确保您的特定设备支持要启用的 SD-WAN 设备版本，并且您具有正确的可用软件版本。

Citrix SD-WAN 平台软件支持

下表说明了每个可用 SD-WAN 软件版本支持哪些 Citrix SD-WAN 平台。

> 注意
>
> 在版本 10.2 中，企业平台版将更名为 高级 版。

版本	广域网优化版	Standard Edition	Premium Edition	高级版
版本 7.x	是	否	否	否
版本 8.x	否	是	否	否
版本 9.0、9.1、9.2、9.3	是	是	是	否
版本 10.0、10.1、10.2	是	是	是	否
版本 11.0、11.1	是	是	是	否
版本 11.2	是	是	是	是
版本 11.3	是	是	是	是

要查看 Citrix SD-WAN 版本 11.3 中支持的所有设备型号，请参阅 Citrix SD-WAN 数据表。

必须先获取并注册 Citrix SD-WAN 软件许可证，然后才能下载软件。有关获取 SD-WAN 软件许可证的说明，请与 Citrix 客户支持联系。有关在您的设备上上载和安装许可证文件的说明，请参阅该部分上载和安装 SD-WAN 软件许可证文件。在安装许可证之前，必须先设置设备硬件，然后设置设备的日期和时间。

为 SD-WAN 平台版本 Provisioning 许可的许可过程涵盖以下主题：

- 支持的 SD-WAN 许可模型：本地、远程和集中式。
- SD-WAN 设备的远程许可证服务器支持。
- 使用远程许可证服务器的先决条件。

> 注意
>
> 截至 2020 年 11 月 4 日，“Citrix 许可证返回和修改”流程发生了更改。使用此新流程，您无法通过 Citrix.com 上的管理许可证门户和合作伙伴平台上的我的许可工具返回或修改许可证。

> 有关更多信息和使用案例列表，请参阅 知库文章 CTX285157。

本地许可证

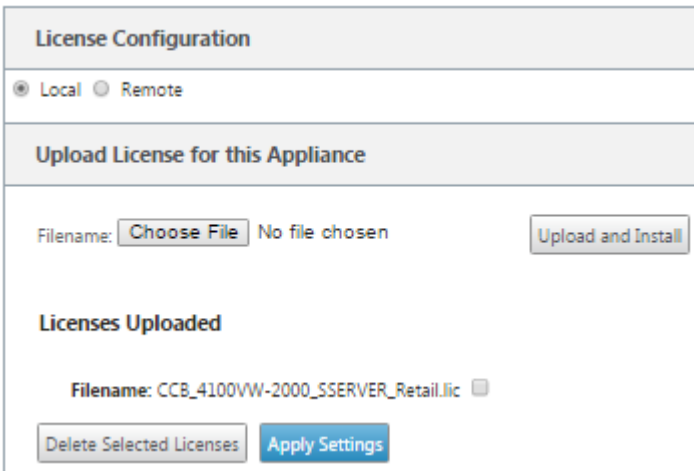
June 22, 2021

使用本地许可证，您需要登录网络中的每个设备并上载许可证文件。即使使用 ZTD 服务，设备也只能使用宽限许可证。您必须上载活动网络连接的许可证文件。许可证文件是根据各个设备的主机 ID 生成的。

您可以使用 SD-WAN Web 管理界面安装和配置 SD-WAN 设备的许可证。

导入在 XenServer/ESXi/Hyper-V 平台上部署的 SD-WAN 设备的许可证：

1. 在 SD-WAN Web 管理界面中，导航到配置 **>** 设备设置 **>** 许可。
2. 选择 **Local**（本地）并上载许可证。单击 **Upload and Install**（上载并安装）。
3. 通过单击 应用设置 来保存您的更改。



远程许可

June 22, 2021

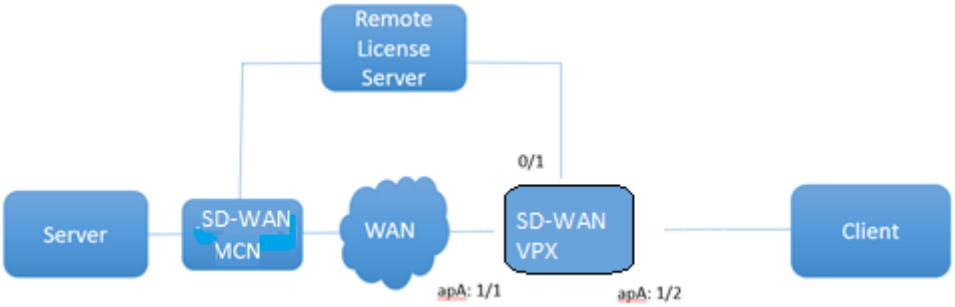
将远程许可证服务器用于 SD-WAN 设备的前提条件。

- 必须为许可证服务器和 SD-WAN 配置 NTP（日期和时间必须同步）
- 建议您使用最新的许可证服务器版本：
  - 发行版：第 9.1 版、第 9.2 版：

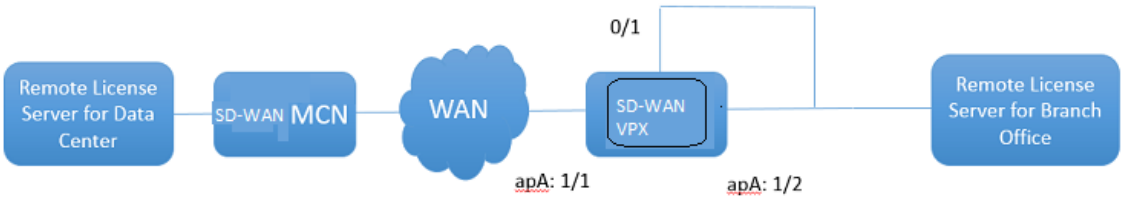
- 发行版 10.0、10.1、10.2、11.0、11.0.1、11.0.2、
- 发行版第 11.0.3 号、第 11.1 号、第 11.2 号

使用案例：

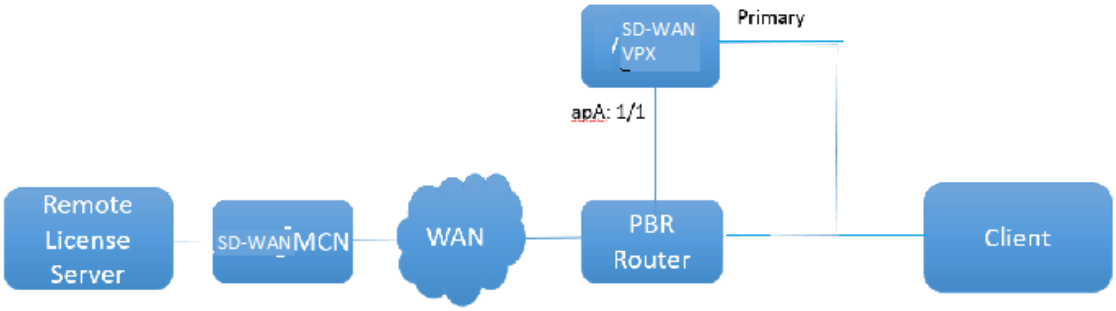
1. 无需使用 data/apA 端口即可通过管理网络访问远程许可证服务器。



2. 分支网络中的远程许可证服务器。

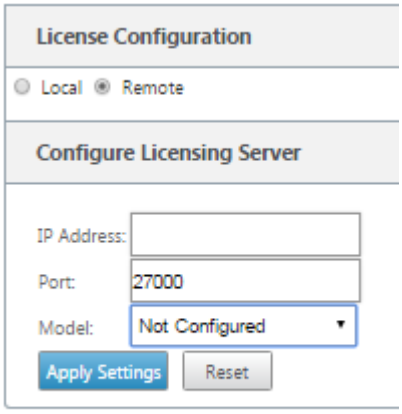


3. SD-WAN VPX-SE-在分支机构部署 PBR。

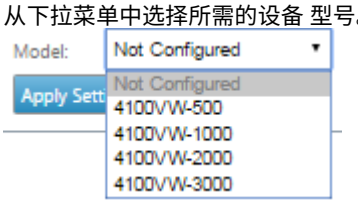


远程许可证：

1. 在 SD-WAN Web 管理界面中，导航到配置 **>** 设备设置 **>** 许可。
2. 选择 远程，然后输入远程服务器 IP 地址详细信息。



3. 从下拉菜单中选择所需的设备 型号。远程许可证服务器的默认端口为 27000。



> 重要
>
> - 如果要使用 SD-WAN Center 安装 SD-WAN 设备的远程许可证，请确保在 SD-WAN Web 管理界面配置编辑器的全局设置中启用 SD-WAN MCN 设备的集中许可。
> - Citrix SD-WAN 中心不支持 IPv6 地址。

集中式许可

June 22, 2021

随着网络部署随着大量网络节点而增长，管理和许可设备变得麻烦。为了简化这一过程，使 SD-WAN 设备的有效登载和简化网络操作，引入了 SD-WAN 网络的集中许可模式。

在新的集中式许可模型中，SD-WAN Center Web 管理界面（SD-WAN 设备管理和报告门户）可为网络中的各个 SD-WAN 设备提供许可服务，而无需登录设备。

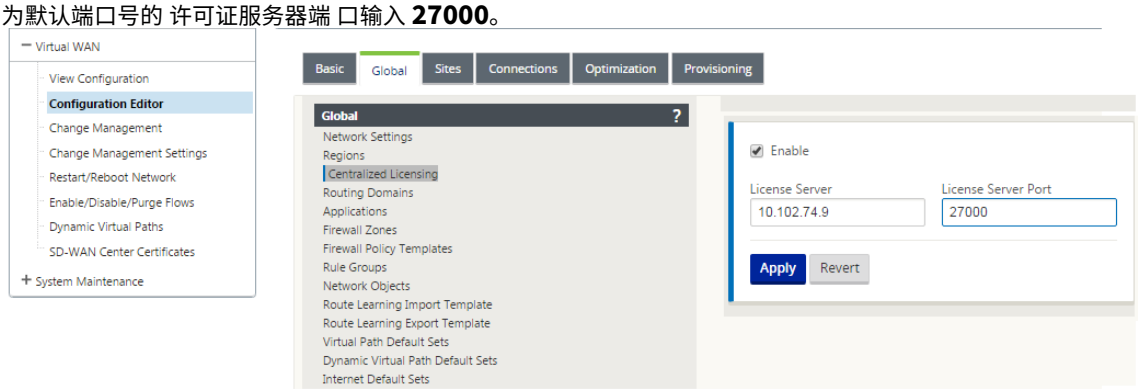
SD-WAN Center IP 地址在 SD-WAN 设备 GUI 中提供了全局 **>** 集中许可。此 IP 地址通过配置包或更新传播到各个设备。当 IP 地址发生更改时，您必须通过更改管理过程来推送它的设备。全局设置可以被本地站点设置覆盖。

可以使用设备型号为站点设置选择许可证带宽。将根据所选许可证审核 WAN 链接带宽。

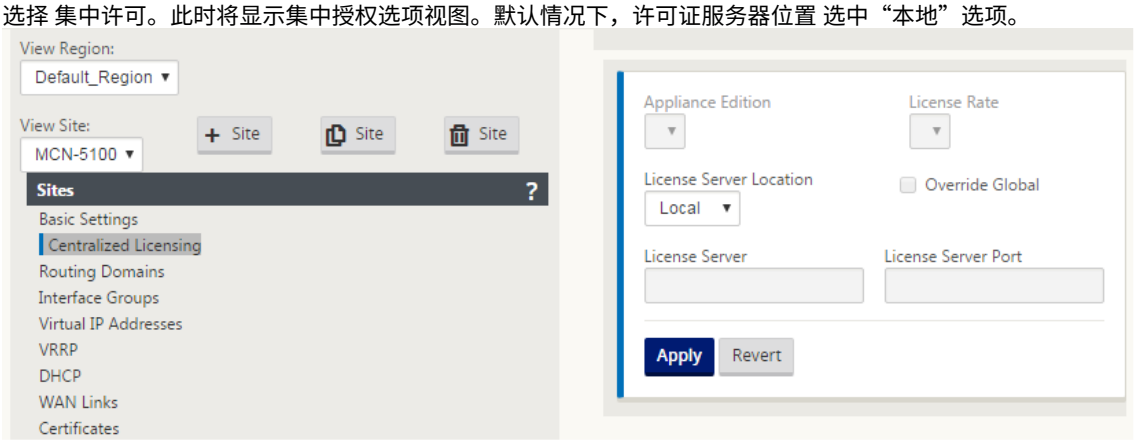
要在 SD-WAN 设备 GUI 中启用集中许可，请执行以下操作：

1. 导航到 配置 > 虚拟广域网 > 配置编辑器。打开现有的虚拟 WAN 配置包或创建配置包。此时将打开配置包。

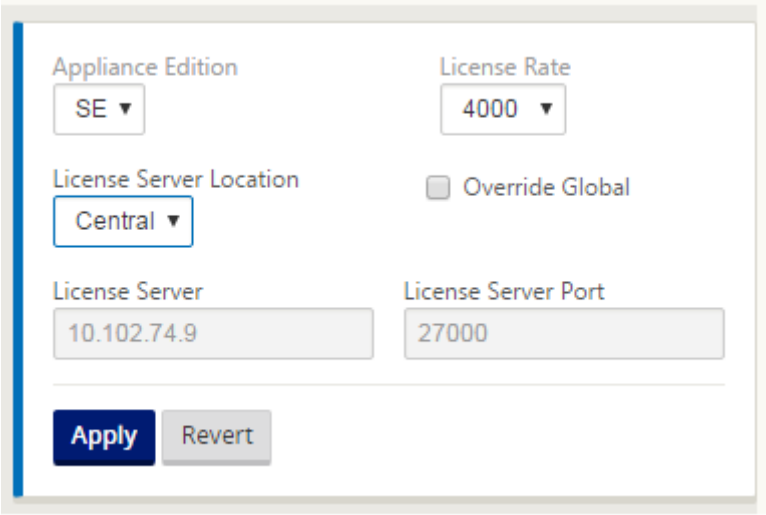
2. 导航到 全局 选项卡。选择 集中许可。Click **Enable**。
3. 输入许可证服务器的 IP 地址，您可以从中下载和管理 SD-WAN 许可证。提供 SD-WAN Center 管理 IP 地址，以便 SD-WAN MCN 或分支设备的配置包可以从 SD-WAN 中心下载许可证。
4. 为默认端口号的 许可证服务器端 口输入 **27000**。



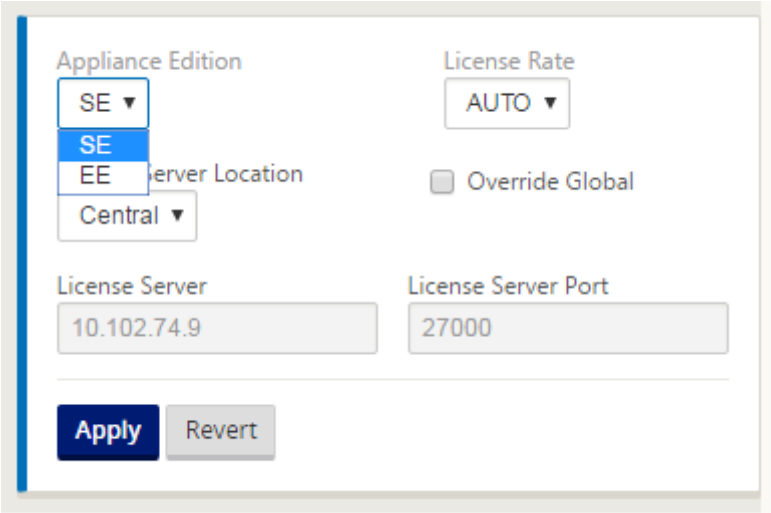
5. 单击应用。
6. 导航到 站点 选项卡。根据要管理集中许可的区域和 站点，在 查看站点 下选择 MCN 或分支站点。
7. 选择 集中许可。此时将显示集中授权选项视图。默认情况下，许可证服务器位置 选中“本地”选项。



8. 单击下拉菜单并选择 **Central** 以更改默认许可证服务器位置。这将显示您在 全局 设置中启用集中许可时为许可证服务器提供的 IP 地址和端口信息。例如,；许可证服务器可以是管理网络中设备的 SD-WAN 中心的 IP 地址。

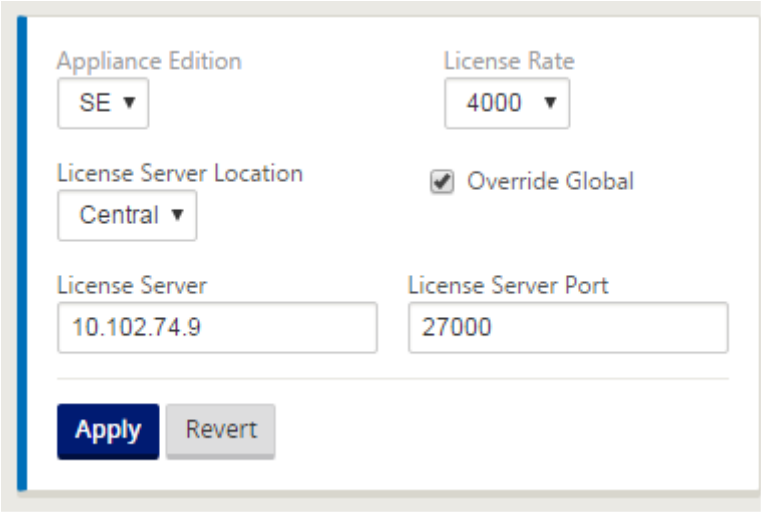


9. 根据要安装的设备选择 设备版本 和 许可费率。单击 应用。



注意：您可以选择覆盖配置的“全局”设置中提供的许可证服务器信息。

10. 选择 覆盖全局 以覆盖全局设置。配置新的许可证服务器 IP 地址。保留默认的许可证服务器端口号；27000。单击应用。



现在，您可以从您配置的许可服务器管理为特定 SD-WAN 设备配置包配置的分支站点和 MCN 站点中的所有节点的许可证。

许可证服务器可以是 SD-WAN Center 管理门户，通过更改管理过程获取从网络配置获得的许可证到站点。

基于带宽分配的许可证：

每个设备都可以选择带宽级别大于或等于配置的带宽的许可证。如果配置的带宽许可证不可用，则会添加设备选择下一个较高带宽许可证的功能。此功能对集中式许可证服务器和远程许可证服务器功能都有效。例如：

- 如果您有三个 410-200 Mbps 的许可证。对于与 410 设备关联的所有带宽分配，您将使用相同的许可证。站点 A（20 Mbps）、站点 B（50 Mbps）和站点 C（200 Mbps）都应该能够使用 410-200 Mbps 的许可证。
- 如果您有一个 410-20 兆位/秒的许可证和 410-200 兆位/秒的许可证。站点 A 配置为消耗 50 Mbps，则站点 A 可以使用 410-200 Mbps 许可证。

许可证宽限期：

从设备中删除许可证文件或许可证配置时允许的宽限期为 30 天。系统日志和电子邮件支持格雷斯警报。

> 注意
>
> 如果选定的许可证速率与配置的 WAN 链接速率不匹配，则设备 GUI 上将显示以下消息以供许可事件使用。
>
> 消息：配置的总允许速率（LAN 到 WAN）NNN（Kbps）不得超过 NNN（Kbps）的两倍，即 NNN（Kbps）
>
> 严重性：警告
>
> 活动：系统日志、电子邮件

管理许可证

June 22, 2021

Citrix SD-WAN 设备许可证通过与远程许可证服务通信来管理，以检查许可证。如果设备已获得许可，网络操作将继续而不会中断。如果设备未获得许可，则 启动 宽限 许可模式。

SD-WAN 设备许可证管理流程：

1. 每个站点都使用 Web 管理界面与远程服务器或 SD-WAN Center 进行通信。此通信 通过检测信号机制以监视连接性和验证许可证状态的检出机制进行。
2. 检测信号每 10-20 分钟通过 TCP 连接发送到许可证服务器，以检查 连接性。
3. 在连续两次检测信号丢失后，设备进入宽限模式。结账方法确定许可证状态。此状态可以是从 SD-WAN 中心发送到设备的“真实”、“格雷”或“拒绝”。每当设备向 SD-WAN Center 提供许可证状态时，它都会签入并签出新的许可证。如果 SD-WAN Center 没有收到两个心跳，则 SD-WAN Center 将分配给该站点的许可证释放到池中。宽限期是 30 天，所以在失去 2 个心跳后，设备 进入宽限期。在这 30 天内，必须恢复通信。恢复后，设备将恢复到正常运行模式。如果未恢复通信，则设备将进入未授权状态，并遵循未许可/许可证到期过程。

MCN 设备的开箱即用许可 (OOB)：

- MCN 设备 将 没有初始宽限期。它需要获得许可才能上来。

客户端设备的开箱即用许可 (OOB)：

- 客户端节点带有或不带 ZTD 功能的 30 天宽限期。
- 该设备已启用 OOB 许可证文件，有效期为 30 天。
- 您有 30 天时间上载许可证文件或通过集中许可服务器获得许可证。
- 如果设备已获得许可，它将正常运行并成为网络的一部分。
- 如果设备未在 30 天内获得许可，则遵循许可证到期程序。

将设备重置为再次拿出 OOB 许可证的唯一方法是执行“重置为出厂状态”。

许可证到期

June 22, 2021

SD-WAN 设备进入 30 天的宽限期，您必须在许可证到期后上载许可证。

在宽限期内，所有操作正常运行。如果许可证未及时上载（到期后 30 天），虚拟广域网服务将被禁用。

集中式许可具有一个日志文件，用于跟踪宽限期、未许可、许可、通信状态和故障的运行情况。

在 SD-WAN 设备 GUI 中，在诊断下，SD-WAN Center 与其他站点的 MCN 连接测试功能可用。这可用于测试每个设备是否可以到达许可服务器。站点、许可证状态和状态表可用于管理和跟踪许可证。

宽限期：

1. 为开箱即用的客户端节点提供 30 天宽限期。通知表明设备处于开箱即用模式，需要有效的许可证。此选项使用宽限许可证文件。

2. 许可证到期：许可证到期后，将提供 30 天的宽限期。通知表明宽限期的原因是许可证到期，需要续订。
3. 丢失与 SD-WAN Center 的通信：2 心跳失后，设备进入宽限模式 30 天。通知表示宽限期的原因是通信失败。

配置

November 1, 2021

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。

SD-WAN 设备配置包括以下内容：

配置 MCN：MCN 充当初始系统配置和任何后续配置更改的分发点。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。

配置分支：添加分支站点的过程类似于创建和配置 MCN 站点。但是，某些配置步骤和设置对于分支站点确实略有不同。此外，添加初始分支站点后，对于具有相同设备型号的站点，您可以使用 克隆（复制）功能简化添加和配置这些站点的过程。与创建 MCN 站点一样，要设置分支站点，必须使用 MCN 设备上管理 Web 界面中的 配置编辑器。仅当接口设置为 MCN 控制台模式时，配置编辑器 才可用。

配置 MCN 和分支站点之间的虚拟路径：在 MCN 和每个客户端（分支）站点之间配置虚拟路径服务。为此，您可以使用配置编 辑器的“连接”部分配置树中提供的配置表单和设置。

启用和配置 WAN 优化：本节提供了有关为您的虚拟 WAN 启用和配置 SD-WAN 高级（企业）版 WAN 优化功能的分步说明。为此，您可以使用 MCN 上 Web 管理界面的 配置编辑器 中的 优化 部分窗体。

> 注意
>
> Citrix SD-WAN Orchestrator 服务不支持 IPv6 地址。

Citrix SD-WAN 设备的以下功能支持 Citrix SD-WAN 11.3 版本中的 IPv6 地址：

- 管理平面功能
  - 管理接口
  - RADIUS 服务器
  - TACACS+ 服务器
  - SMTP 服务器
  - Syslog 服务器
  - HTTP 服务器
  - DNS 服务器
  - 应用程序流程/IPFix

  - SNMP
  - 远程许可
  - 集中式许可
  - NTP 服务器
  - 允许列表
  - SD-WAN 设备的新用户界面
  - 诊断

> 注意
>
> ：使用管理 IPv6 地址配置上述列出的功能后，如果在“装置设置” > “网络适配器”下禁用 IPv6 协议，则这些功能将无法按预期工作。

- 数据平面功能
  - 静态路由
  - 通过 IPv6 WAN 链接的互联网服务
  - 通过 IPv6 WAN 链接的内联网服务
  - 路由器广告
  - DHCP 客户端
  - DHCP 服务器/中继
  - 应用程序 QoS
  - 防火墙
  - 带内管理
  - 高可用性
  - IP 规则
  - 通过 LTE 链接支持 IPv6

> 注意
>
> - Citrix Citrix SD-WAN 1000 SE /PE、Citrix SD-WAN 2000 SE /PE 和 Citrix SD-WAN 4000 SE 设备上不支持 IPv6 地址。
> - 以下配置不支持 IPv6 地址：
> - Dynamic Routing (OSPF/BGP)
> - Virtual Router redundancy protocol
> - Premium edition or Two-Box support
> - Cloud direct
> - VNF/3rd Party Firewall
> - Netflow
> - Header compression for IPv6 packets
> - Application Routing

> - Office-365 support
> - Prefix delegation group

初始设置

September 26, 2023

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.

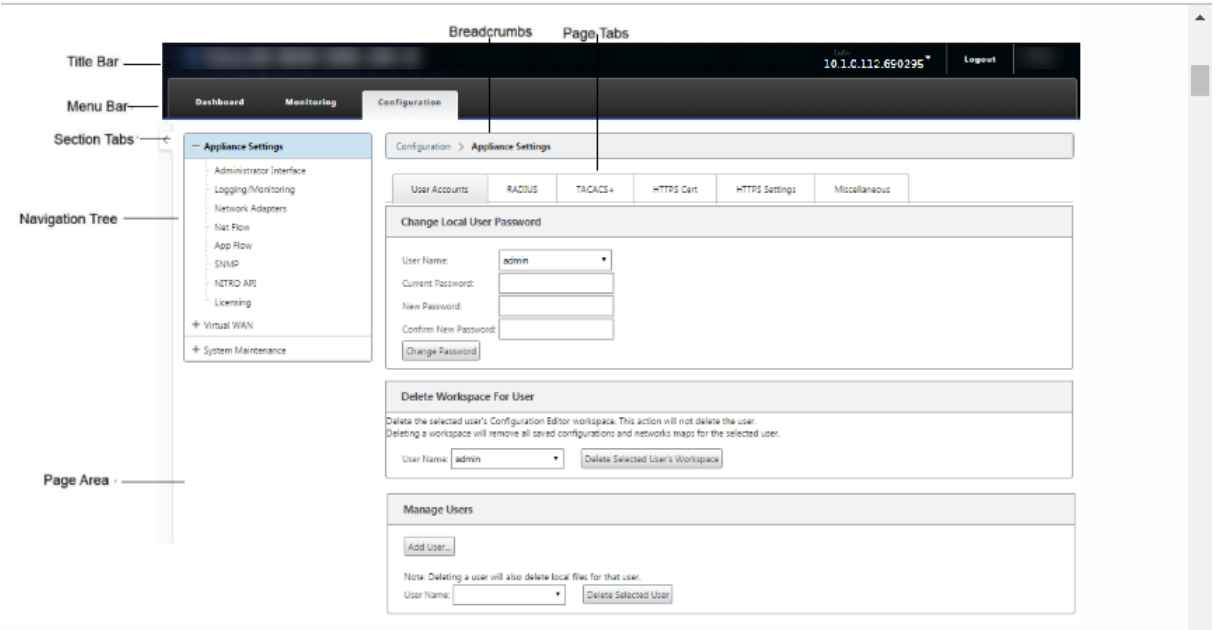
Web 界面 (UI) 布局概述

June 22, 2021

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线图。还提供了配置编辑器和更改管理向导的具体导航说明。

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—显示设备型号、设备的主机 IP 地址、设备上当前运行的软件包的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 区域 选项卡可显示该区域的导航树。
- 导航树—导航树位于主菜单栏下方的左侧窗格中。这将显示部分的导航树。单击部分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。
- 痕迹导航—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窗体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（如 更改管理 向导），选项卡位于页面区域的左窗格中，导航树和页面工作区之间。
- 页面区域大小调整—对于某些页面，您可以增加或缩小页面区域（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。

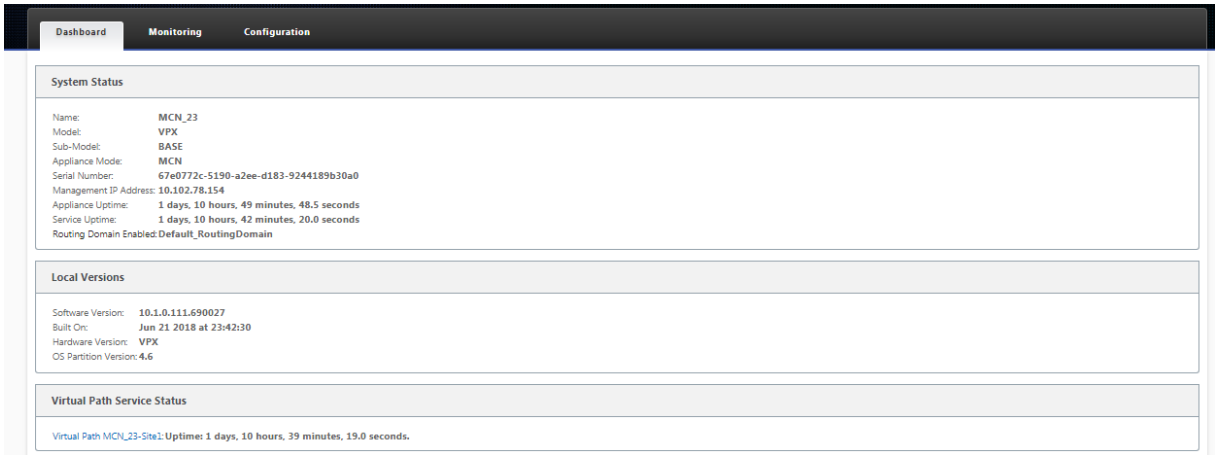
Web 管理界面控制板

单击 控制板 部分选项卡以显示本地设备的基本信息。

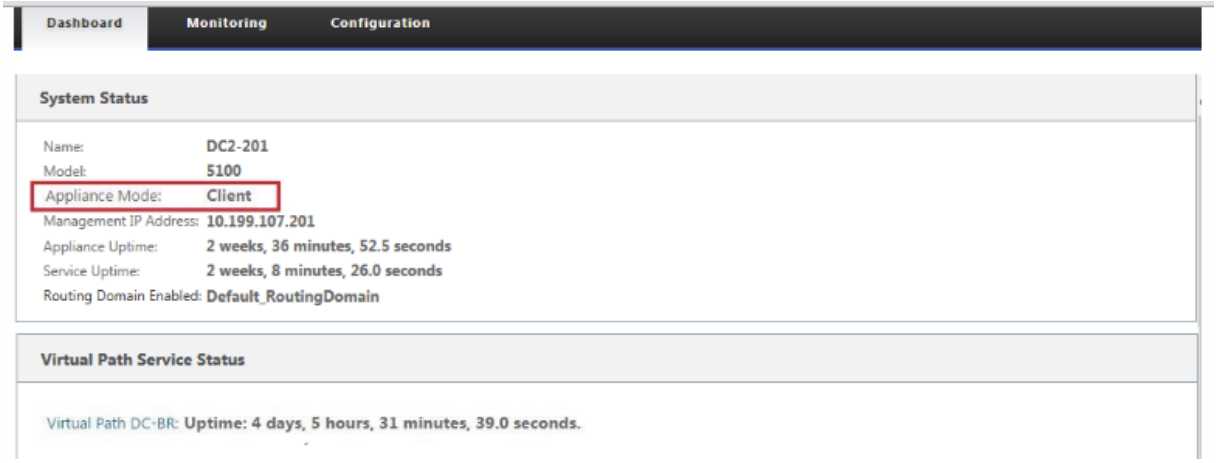
控制面板 页面显示设备的以下基本信息：

- 系统状态
- 虚拟路径服务状态
- 本地设备软件包版本信息

下图显示了主控节点 (MCN) 设备 控制板 显示示示例。



下图显示了客户端设备控制板显示示示例。



配置编辑器

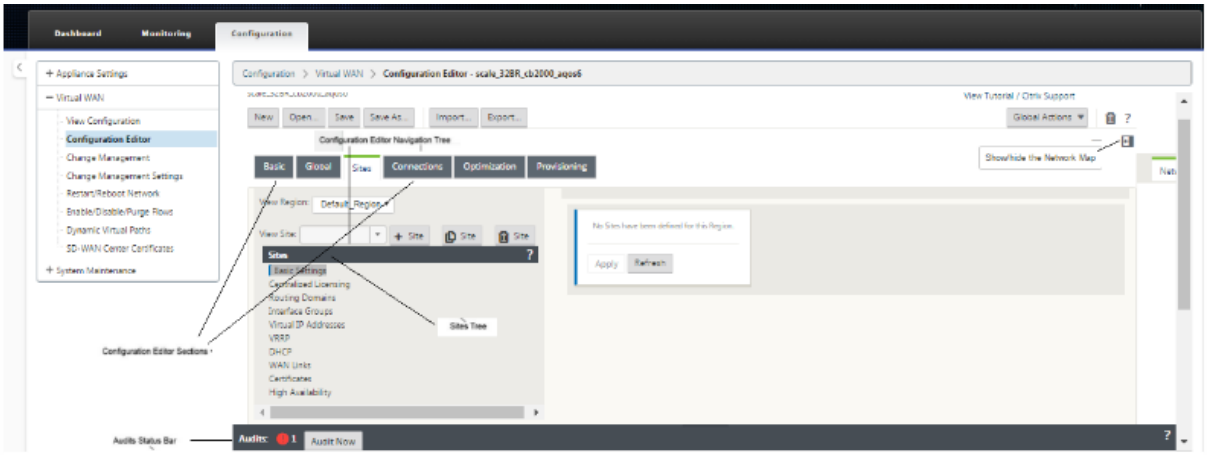
通过配置编辑器，您可以添加和配置虚拟 WAN 设备站点、连接、优化和 Provisioning 备，以及创建和定义虚拟 WAN 配置。

仅当 Web 管理界面处于 MCN 控制台模式时，配置编辑器才可用。默认情况下，新设备上的 Web 界面设置为客户端模式。您必须将模式设置更改为 MCN 控制台，然后才能访问配置编辑器。有关说明，请参阅将管理 Web 界面切换到 MCN 控制台模式。

要导航到 配置编辑器，请执行以下操作：

1. 登录到 MCN 应用程序上的 Web 管理界面。1. 选择配置选项卡。1. 在导航树中，单击树中 虚拟 **WAN** 分支旁边的 **+**。这将显示虚拟 **WAN** 类别的可用页面。1. 在树的虚拟 WAN 分支中，选择 配置编辑器。

   下图概述了 配置编辑器的基本导航和页面元素，以及用于标识它们的术语。



下面介绍了本指南中引用的主要 配置编辑器 导航元素：

- 配置编辑器菜单栏 -这位于页面区域的顶部，正好位于痕迹导航链接的下方。菜单栏包含 配置编辑器 操作的主要活动按钮。此外，菜单栏的最右边缘是用于启动配置编辑器教程的查看教程链接按钮。本教程将引导您完成 配置

编辑器 显示中每个元素的一系列气泡描述。

- 配置编辑器部分树—这是位于配置编辑器页面区域左窗格中的深灰色条的堆栈。每个灰色条表示一个顶层部分。单击某个部分名称以显示该部分的子分支。
- 分段树分支—单击分段树中的分段名称以打开分段分支。每个分支都包含配置类别和表单的一个或多个子分支，而这些分支又可以包含更多子分支和表单。
- 站点树—这列出了已添加到当前在配置编辑器中打开的配置的站点节点。在章节树中。单击站点名称以打开该站点的分支。单击站点以关闭分支。有关导航和使用站点树和配置窗体的详细说明，请参阅以下部分：
  - 设置主控制节点 (MCN) 站点
  - 添加和配置分支站点
- 审核状态栏—这是 配置编辑器 页面底部的深灰色条，跨越管理 Web 界面屏幕的整个宽度。仅当配置编辑器打开时，审核状态栏才可用。状态栏最左侧的审核警报图标（红点或 goldenrod delta）表示当前打开的配置中存在一个或多个错误。单击状态栏以显示该配置的所有未解决审核警报的完整列表。

更改管理向导

更改管理 向导将指导您完成上载、下载、暂存和激活主控制节点 (MCN) 设备和客户端设备上的虚拟广域网软件和配置的过程。更改管理 向导有两个版本，一个用于虚拟 WAN 系统范围（“全局”）变更管理，另一个用于本地变更管理，如下所示：

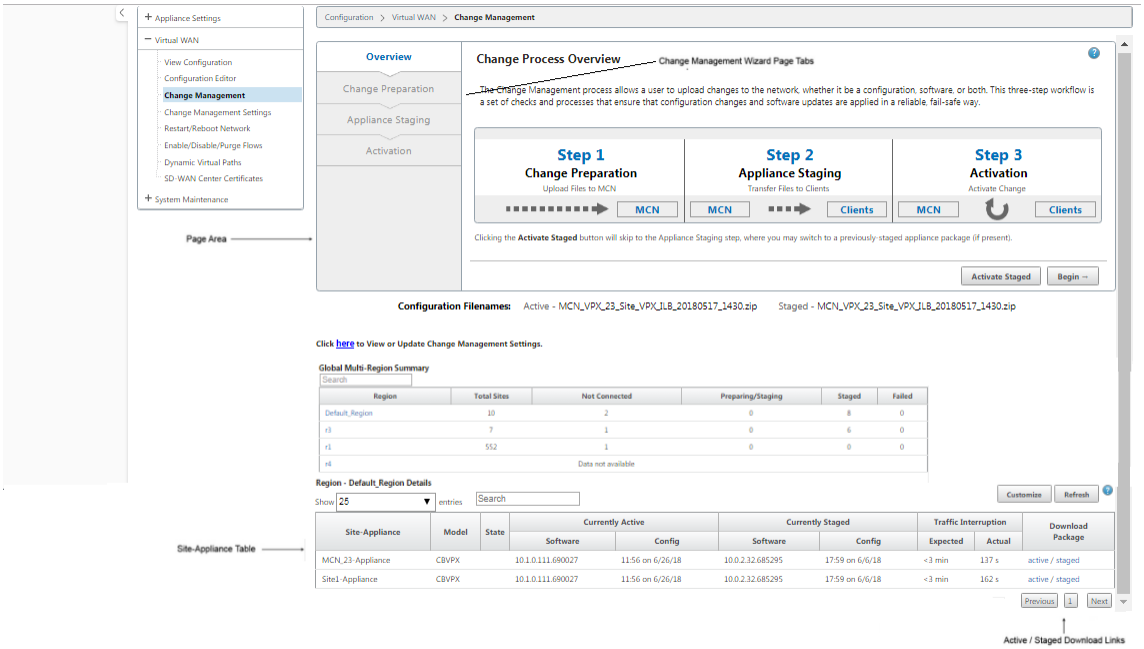
- **MCN**（全局）更改管理向导—**MCN** 全局更改管理 向导是主（主）版本，仅在 MCN 设备 Web 管理界面中提供。使用此选项可生成要为网络中每种类型的虚拟 WAN 设备部署的虚拟 WAN 设备包。您还可以使用向导将配置更改自动传播到虚拟 WAN 中已部署的设备。下面的“使用 MCN 全局更改管理向导”部分提供了基本导航说明。准备 MCN 上的虚拟 WAN 设备包部分提供了使用 MCN 全局 更改管理 向导创建设备包的说明。
- 本地更改管理向导—本地更改管理 向导可在 MCN 和所有客户端节点设备上运行的 Web 管理界面中使用。使用此选项可在要添加到虚拟 WAN 的本地设备上上载、暂存和激活相应的虚拟 WAN 设备包。您还可以使用此向导将更新的设备包专门上载到本地 MCN 或网络中已部署的单个本地虚拟 WAN 设备。

使用 **MCN** 全局更改管理向导

若要打开 MCN 全局 更改管理 向导，请执行以下操作：

1. 登录到 MCN 设备上的 Web 管理界面。
2. 选择 配置 选项卡。在导航树中，单击树中 虚拟 **WAN** 分支旁边的 **+**。
3. 在 虚拟广域网 分支中。选择 更改管理。

   此操作将显示 更改管理 向导的第一页，即 更改流程概览 页，如下图所示。



4. 要启动该向导，请单击开始。

   有关使用向导在设备上上载、暂存和激活 SD-WAN 软件和配置的完整说明，请参阅以下部分：

- 准备 MCN 上的虚拟 WAN 设备包
- 在客户端上安装虚拟 WAN 设备包

更改管理 向导包含以下导航元素：

- 页面区域—这会显示 更改管理 向导的每个页面的窗体、表格和活动按钮。
- 更改管理向导页面选 项卡—页面选项卡位于向导每个页面上页面区域的左窗格中。按照向导过程中相应步骤的顺序列出选项卡。当选项卡处于活动状态时，可以单击该选项卡以返回到向导中的上一个页面。如果选项卡处于活动状态，则名称将以蓝色字体显示。灰色字体表示非活动选项卡。选项卡处于不活动状态，直至完成所有依赖项（之前的步骤），但未出现任何错误。
- 设备-站点表 -这位于向导页面区域的底部，在大多数向导页面上。该表包含有关每个已配置设备站点的信息，以及用于下载该设备型号和站点的活动或暂存设备包的链接。此上下文中的软件包是一个 Zip 文件包，其中包含适用于该设备型号的 SD-WAN 软件包以及指定的配置包。表上方的“配置文件名”部分显示了本地设备上当前活动和暂存包的软件包的软件包名称。
- 主动/分段下载链接—这些链接位于设 备站点 表中每个条目的 下载包 字段（最右侧列）中。单击条目中的链接以下载该设备站点的活动或暂存包。
- 开始—单击 开始 启动 更改管理 向导流程，然后继续进入 更改准备 选项卡页。
- 激活暂存—如果这不是初始部署，并且您希望激活当前暂存的配置，则可以选择直接进行激活步骤。单击 激活暂存 可直接进入激活页面并启动激活当前暂存的配置。

设置设备硬件

June 22, 2021

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 虚拟机时未为 SD-WAN VPX-SE 配置管理 IP 地址，则需要立即执行此操作，如本节所述配置 SD-WAN VPX-SE 的管理 IP 地址。

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 虚拟机时未为 SD-WAN VPX-SE 配置管理 IP 地址，则需要立即执行此操作，如本节所述配置 SD-WAN VPX-SE 的管理 IP 地址。

配置管理 IP 地址

September 26, 2023

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。

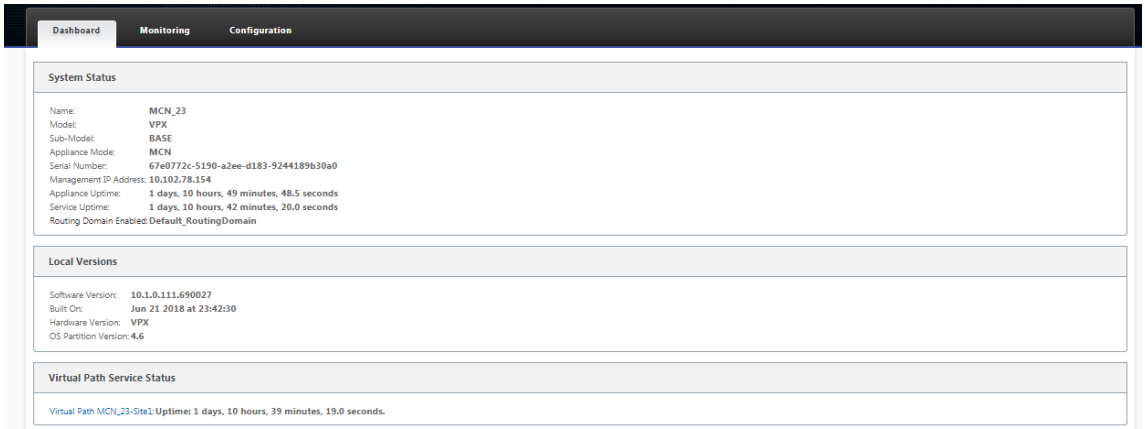
   这将在连接的设备上打开 SD-WAN 管理 Web 界面登录屏幕。

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。



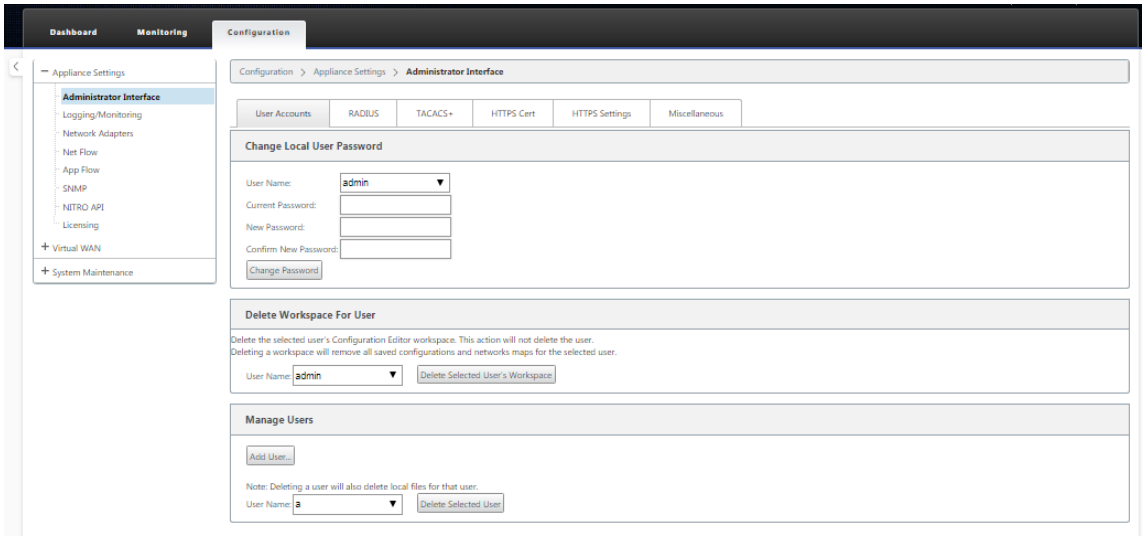
   首次登录设备上的管理 Web 界面时，控制板 会显示警报图标（goldenrod 增量）和警报消息，指示已禁用 SD-WAN 服务，并且尚未安装许可证。目前，您可以忽略此警报。在您安装许可证并完成设备的配置和部署过程后，警报将得到解决。

7. 在主菜单栏中，选择“配置”部分选项卡。

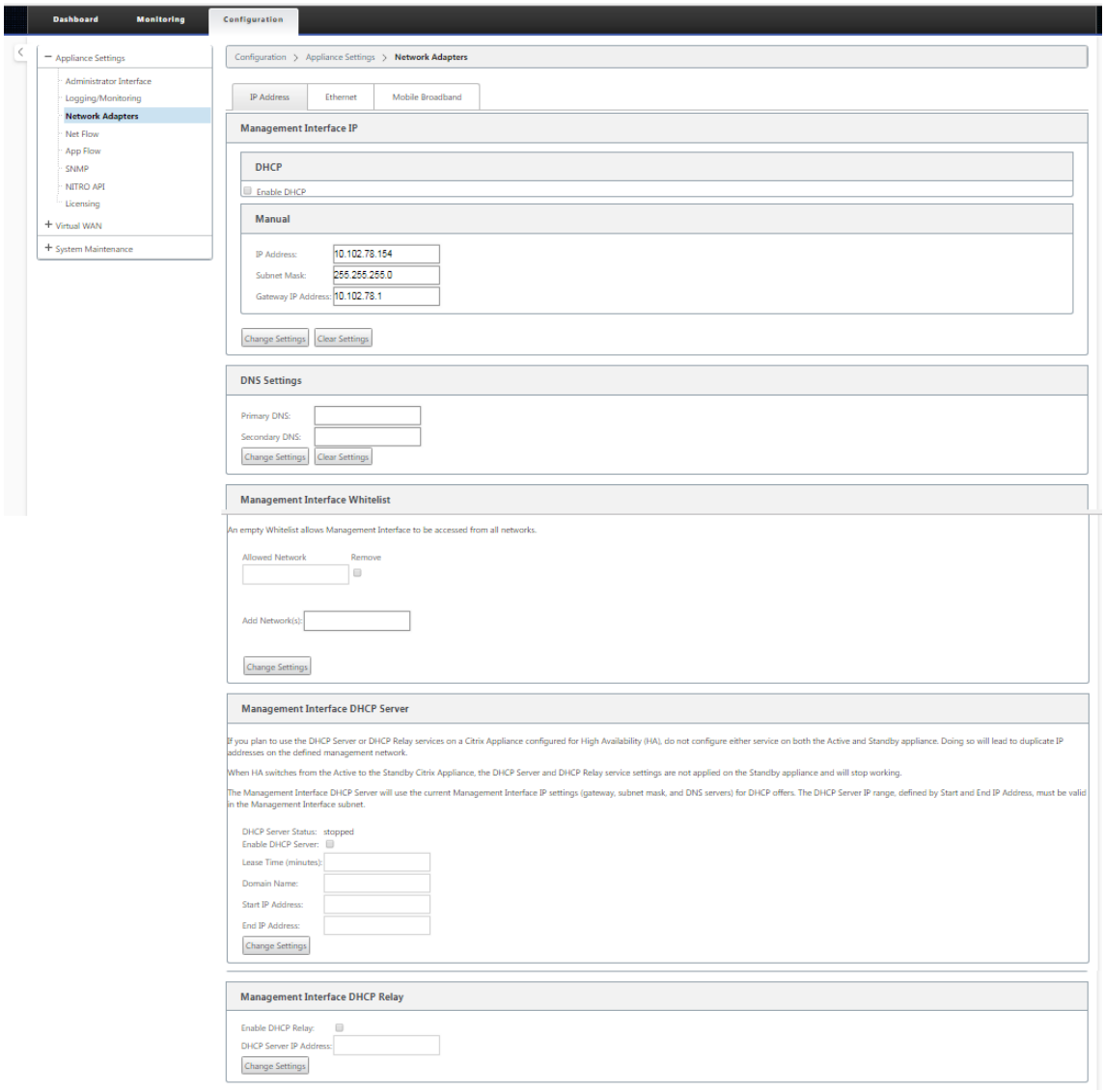
   这将在屏幕的左窗格中显示 配置 导航树。配置 导航树包含以下三个主要分支：

   - 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。

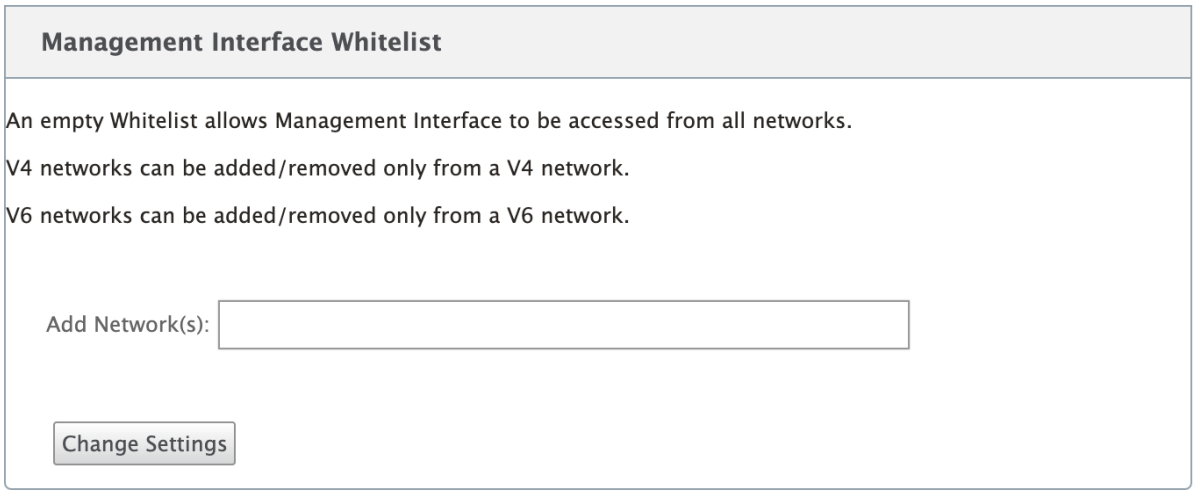
> 提示
>
> 验证连接后，请勿注销管理 Web 界面。您正在使用它来完成后续章节中概述的剩余任务。

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

June 22, 2021

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：

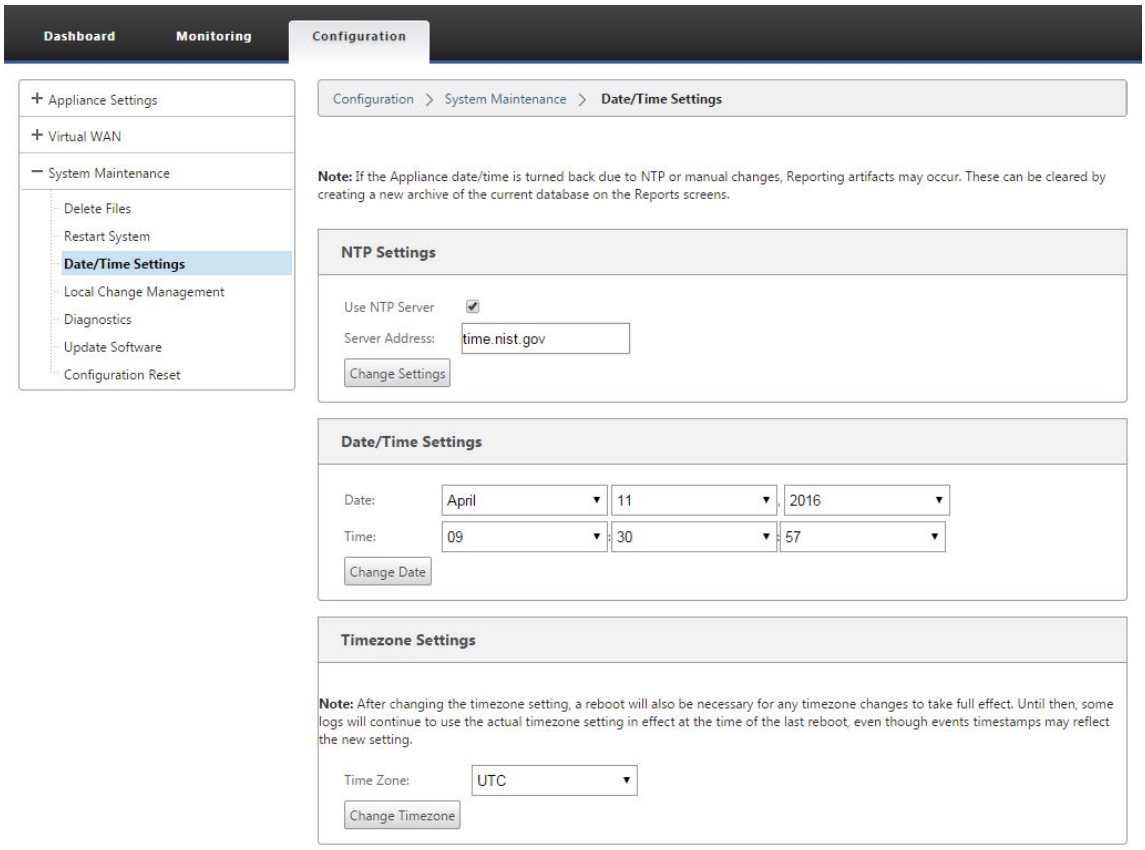
1. 登录到正在配置的设备上的管理 Web 界面。

2. 在主菜单栏中，选择 配置选项卡。

   这将在屏幕左侧窗格中显示 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份、日期 和年份。
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。如果您不想重置超时阈值，则可以直接进入部分上载和安装 SD-WAN 软件许可证文件。

> 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

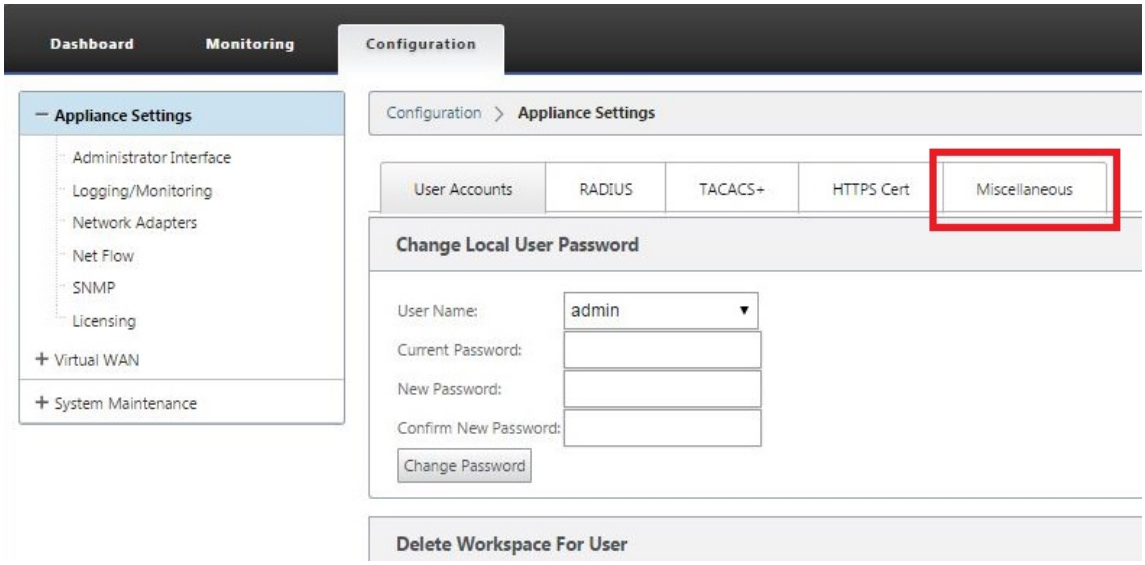
June 22, 2021

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。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：

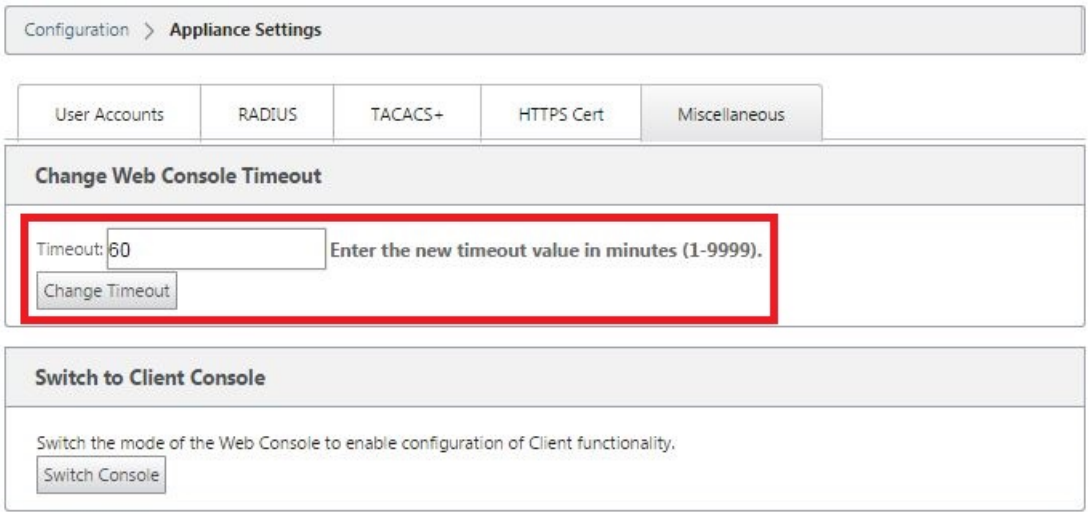
1. 选择 配置 选项卡，然后在导航树中选择 设备设置 分支。

   这将显示 设备设置 页面，默认情况下预先选择 用户帐户 选项卡。



2. 选择 杂项选项卡（最右角）。

   这将显示杂项选项卡页面。



3. 输入控制台 超时 值。

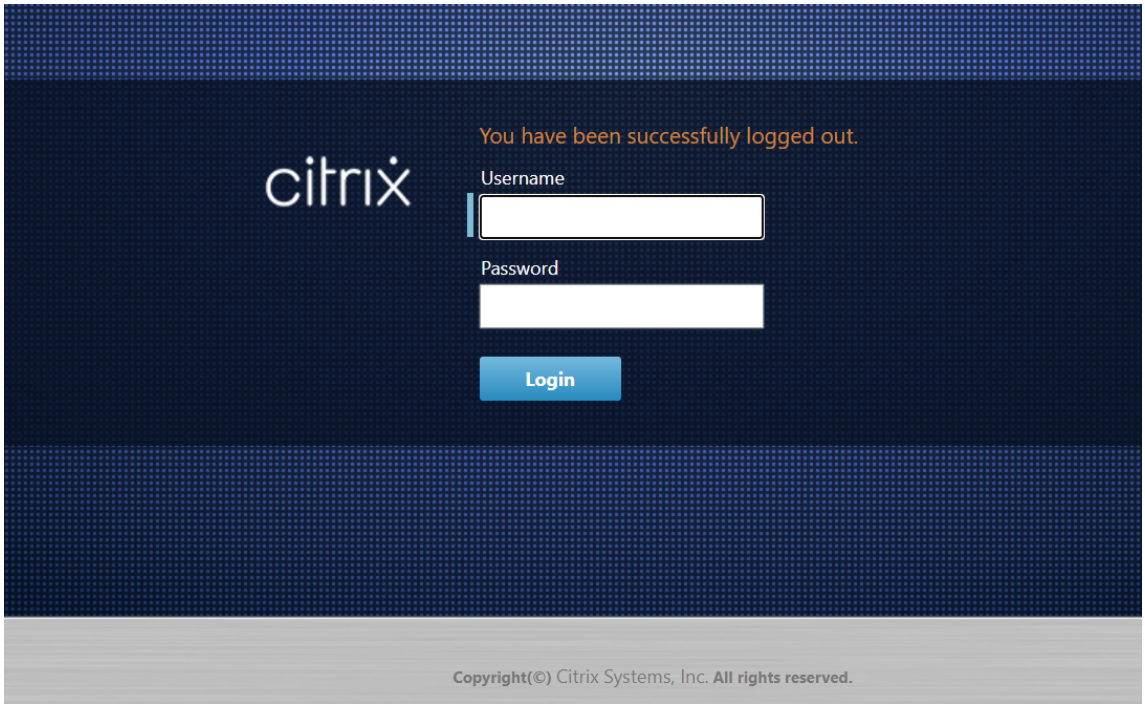
   在更改 **Web** 控制台超时部分的超时字段中，输入较高的值（以分钟为单位），最大值为 9999。默认值为 60，这对于初始配置会话来说太简短。

   > 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

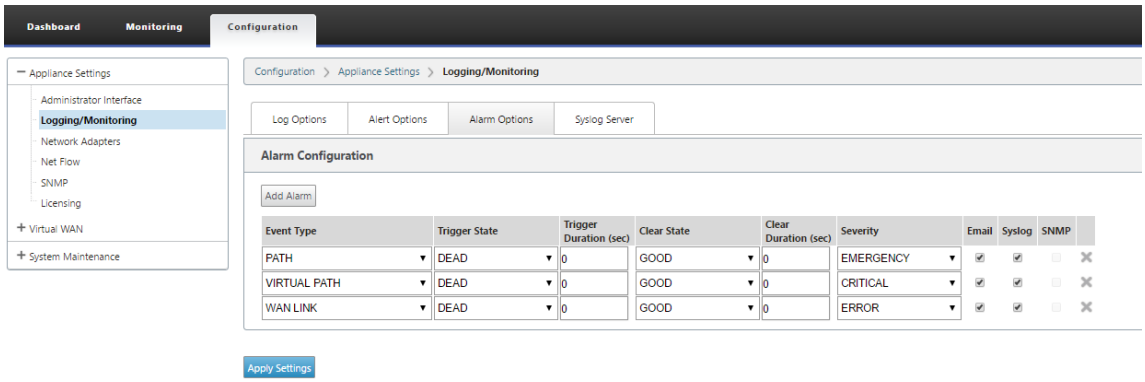
June 22, 2021

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 > 设备设置 > 记录/监视，然后单击警报选项。
2. 单击 添加警报以 添加新警报。



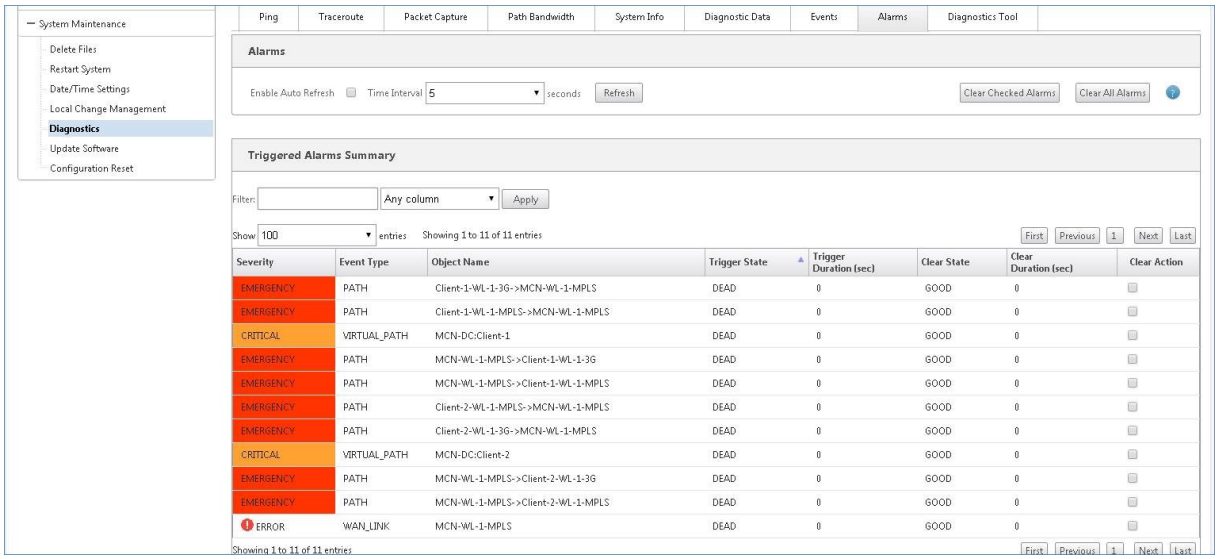
3. 为以下字段选择或输入值：
   - 事件类型：SD-WAN 设备可针对网络中的特定子系统或对象触发警报，这些子系统或对象称为事件类型。可用的事件类型包括 SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL 和 IPSEC_TUNNEL。
   - 触发器状态：为事件类型触发警报的事件状态。可用的 触发状态 选项取决于所选事件类型。
   - 触发器持续时间：这是持续时间（秒），用于确定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：此持续时间（以秒为单位）决定在清除警报之前等待的时长。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，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：通过电子邮件发送事件类型的警报触发器和清除警报。
   - **Syslog**：事件类型的警报触发器和清除警报通过 Syslog 发送。
   - **SNMP**：警报触发器和清除事件类型的警报通过 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 清除已检查的警报。或者，单击 清除所有警报 以清除所有警报。

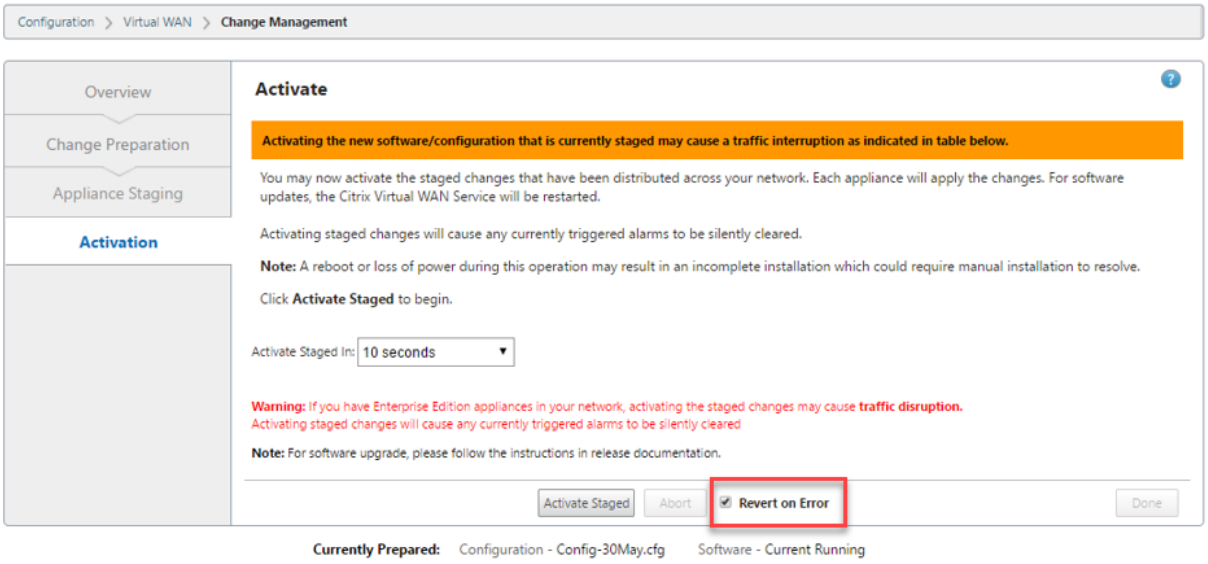
配置回滚

June 22, 2021

配置回滚功能允许 Change Management 系统通过恢复到以前活动的软件/配置来检测以下软件/配置错误并从中恢复：

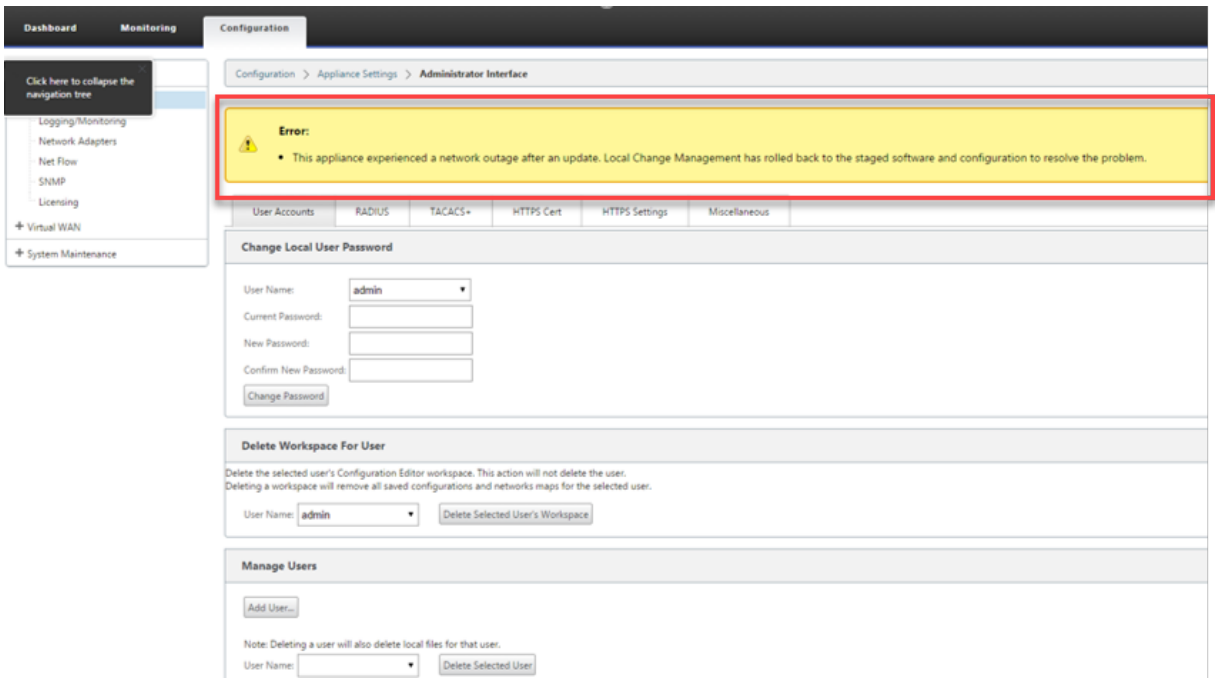
- 软件升级后，虚拟路径已死亡，如果发生软件崩溃，服务将被禁用。
- 进行配置更改后，虚拟路径就会死亡，没有任何软件崩溃。
- 如果 MCN 设备本身的配置导致 MCN 站点出现网络问题，则它不会检测到中断，也不会回滚。但是，网络中的所有其他客户端都会自行回滚，因为他们无法连接到 MCN。

默认情况下，配置回滚功能处于启用状态，要禁用此功能，请清除更改管理向导的激活选项卡中的错误还原选项。



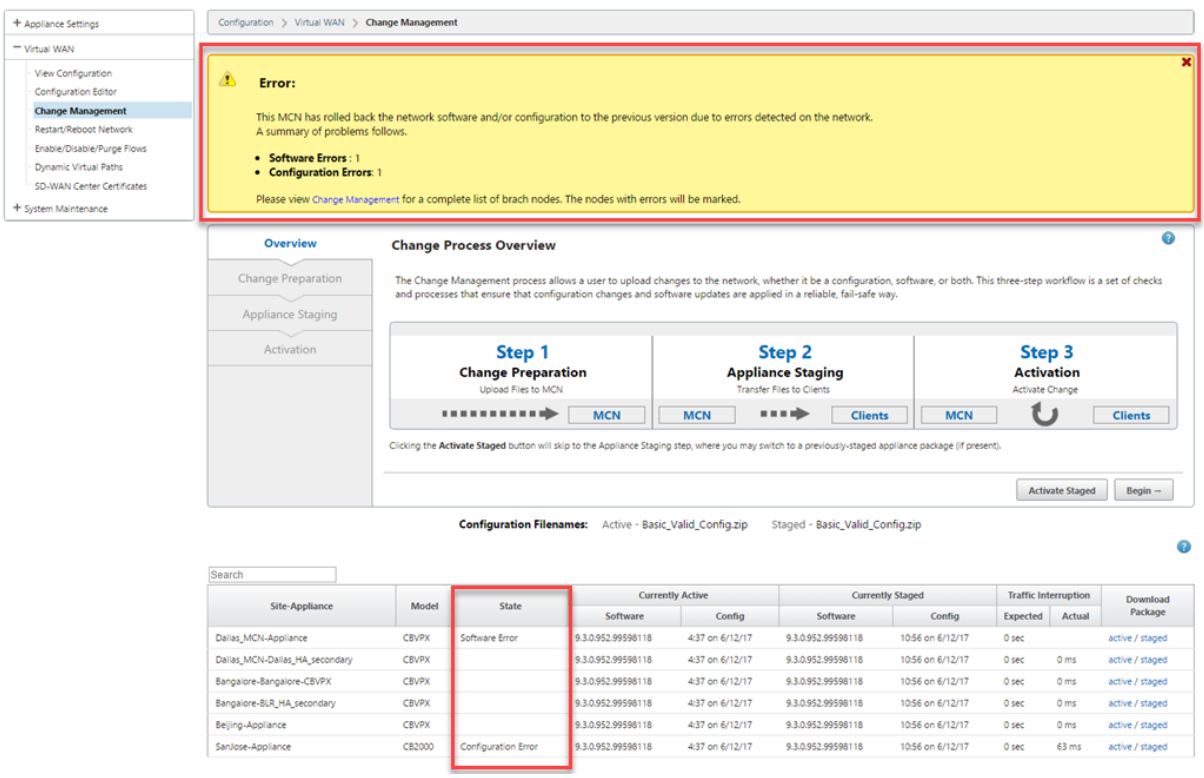
如果从 MCN 激活暂存软件包时，客户端上出现系统配置错误，则客户端将恢复到之前的软件配置，并显示错误消息，如以下屏幕截图所示。

如果检测到设备崩溃，客户端会为 Software_UPDATE 对象生成严重严重性事件；如果检测到网络中断，则会为 CONFIG_UPDATE 对象生成严重性事件。



如果启用了还原错误，则客户端设备将监视自身约 30 分钟。如果软件在 30 分钟内崩溃，或者网络关闭（无法建立到 MCN 的虚拟路径）30 分钟，则会触发回滚。

在 MCN 上，将显示一条错误消息，如以下屏幕截图所示。当客户端重新加入网络时，它会报告遇到的错误类型。错误消息中显示错误数的摘要计数。



在 MCN 的 更改管理 窗口中，您可以看到站点设备的状态，指示该站点是否遇到软件错误或配置错误。

设置主控制节点

June 22, 2021

SD-WAN 主控制节点 **(MCN)** 是虚拟 WAN 中的头端设备。通常，这是部署在企业数据中心的 4000 或 5100 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。

补充 **MCN** 站点部署信息

推荐使用以下知识库支持文章：

- 虚拟 WAN PBR 模式部署步骤 (CTX201577)

  http://support.citrix.com/article/CTX201577

- 虚拟 WAN 网关模式部署步骤 (CTX201576)

  http://support.citrix.com/article/CTX201576

MCN 站点配置过程概述

添加和配置 MCN 站点的步骤如下：

1. 将管理 Web 界面切换到 **MCN** 控制台 模式。
2. 添加 MCN 站点。
3. 为 MCN 站点配置虚拟接口组。
4. 配置 MCN 站点的虚拟 IP 地址。
5. （可选）为站点配置 LAN GRE 隧道。
6. 配置 MCN 站点的 WAN 链接。
7. 配置 MCN 站点的访问接口。
8. 配置 MCN 站点的路由。
9. （可选）为 MCN 站点配置高可用性。
10. （可选）配置虚拟 WAN 安全性和加密。
11. 命名并保存 MCN 站点配置。

以下各节提供了有关这些任务的说明。

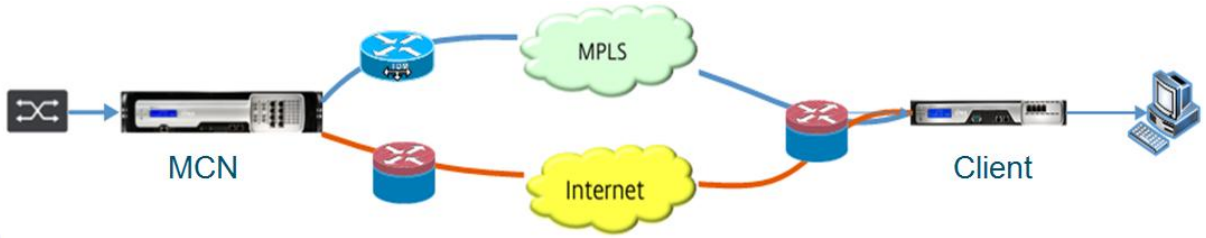
MCN 概述

June 22, 2021

主控制节点 **(MCN)** 是充当虚拟 WAN 主 Controller 的中央虚拟 WAN 设备，也是客户端节点的中央管理点。所有配置活动以及设备包的准备以及将其分发给客户端的工作都在 MCN 上执行。此外，某些虚拟 WAN 监视信息仅在 MCN 上可用。MCN 可以监视整个
虚拟广域网，而客户端节点只能监视其本地内联网，以及与其连接的客户端的一些信息。

MCN 的主要目的是通过位于虚拟 WAN 中的一个或多个客户端节点建立和使用虚拟路径，以进行企业站点到站点的通信。MCN 可以管理和拥有多个客户端节点的虚拟路径。可以有多个 MCN，但在任意给定时间只能激活一个。

下图说明了虚拟 WAN 版部署的 MCN（数据中心）和客户端（分支节点）设备的基本角色和上下文。



切换到 **MCN** 控制台

June 22, 2021

要添加和配置 MCN 站点，必须首先登录到要升级为 MCN 角色的设备上的管理 Web 界面，然后将管理 Web 界面切换到 **MCN** 控制台 模式。**MCN** 控制台 模式允许访问当前连接的管理 Web 界面中的配置编辑器。然后，您可以使用 配置编辑器 添加和配置 MCN 站点。

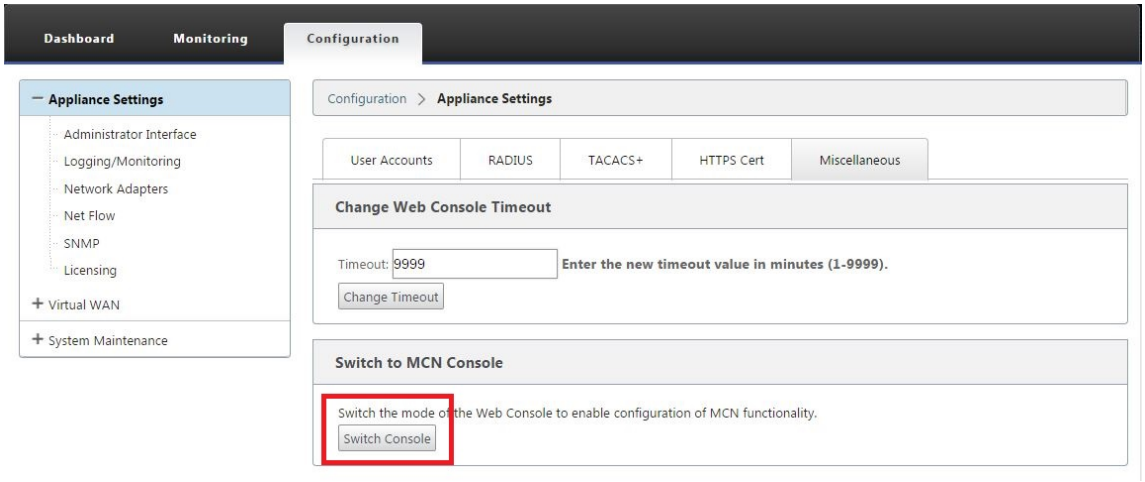
> 注意
>
> 切换到 **MCN** 控制台 模式只会更改管理 Web 接口模式的操作模式，而不会更改设备本身的活动角色。要将设备提升为 MCN 角色，必须首先添加和配置 MCN 站点，然后激活指定 MCN 设备上的配置和软件包。

要将管理 Web 界面切换到 **MCN** 控制台 模式，请执行以下操作：

1. 登录到要配置为 MCN 的设备上的管理 Web 界面。
2. 在管理 Web 界面主屏幕（页面顶部的蓝色栏）的主菜单栏中单击配置。
3. 在导航树（左窗格）中，打开“装置设置”分支，然后单击“管理员界面”。

   这将在中间窗格中显示 管理员界面 页面。
4. 选择杂项选项卡。

   此操作将显示 其他管理 设置 页面。



杂项 选项 卡页面底部是 切换到 **[**客户端 **> MCN** 控制台 部分。本部分包含用于在设备控制台模式之间切换的切换控制台 按钮。

节标题指示当前控制台模式，如下所示：

- 在 客户端控制台 模式（默认）时，部分标题为 切换到 **MCN** 控制台。
- 在 **MCN** 控制台 模式下，部分标题 为切换到客户端控制台。

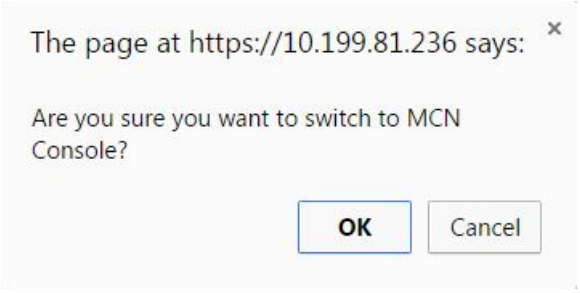
默认情况下，新设备设置为 客户端控制台 模式。

MCN 控制台 模式启用导航树中的 配置编辑器 分支。配置编辑器 仅在 MCN 设备上可用。

> 注意
>
> 继续执行下一步之前，请确保设备仍设置为默认设置（客户端控制台 模式）。部分标题应为：切换到 **MCN** 控制台。

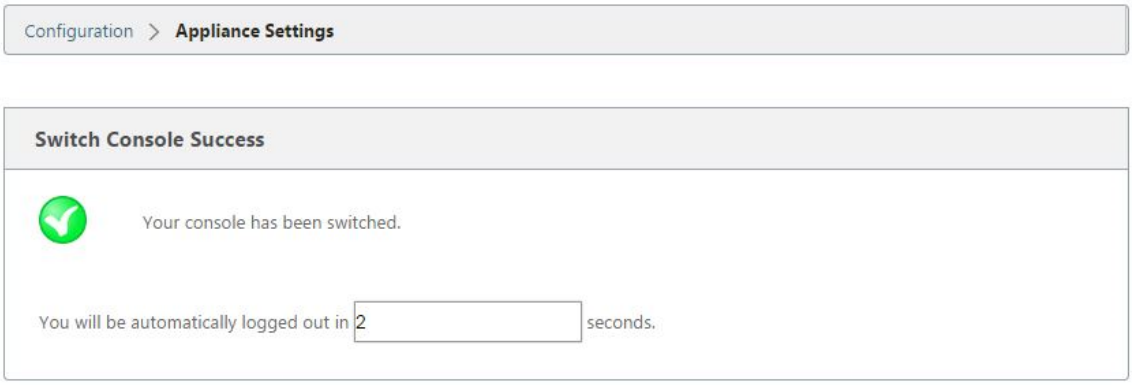
5. 单击 切换模式 将设备模式设置为 **MCN** 控制台 模式。

   此操作将显示一个对话框，提示您确认要切换到 MCN 模式。

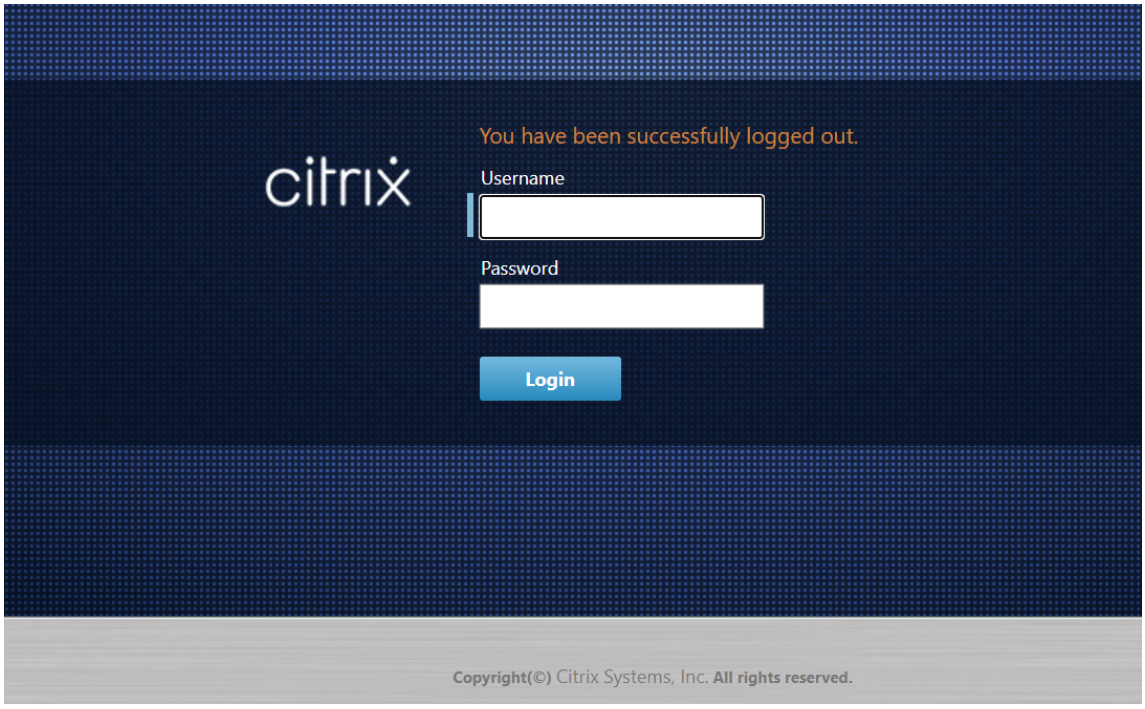


6. 单击确定。

   这会将控制台模式切换到 **MCN** 控制台 模式，并终止当前会话。将显示一条成功消息，以及一个倒计时状态，指示会话终止之前剩余的秒数。



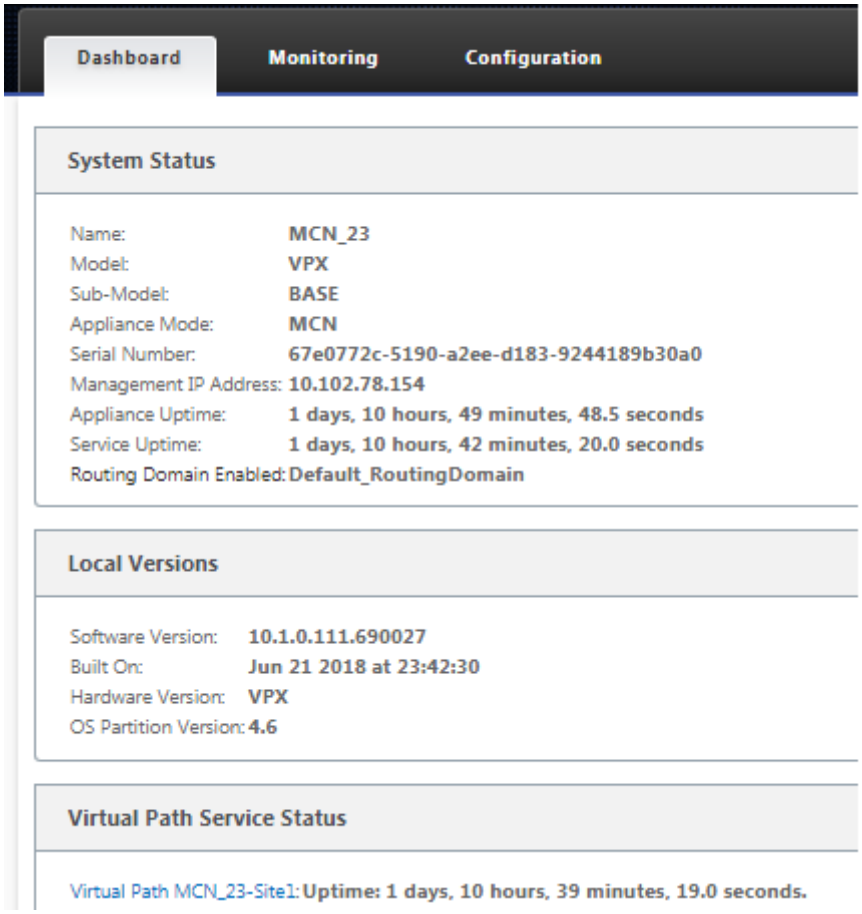
倒计时完成后，会话终止并显示登录页面。



7. 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*

   登录后，显示 控制板，现在指示设备处于 MCN 模式。



下一步是打开新配置并将 MCN 站点添加到站点表，然后开始配置新 MCN 站点。

配置 MCN

June 22, 2021

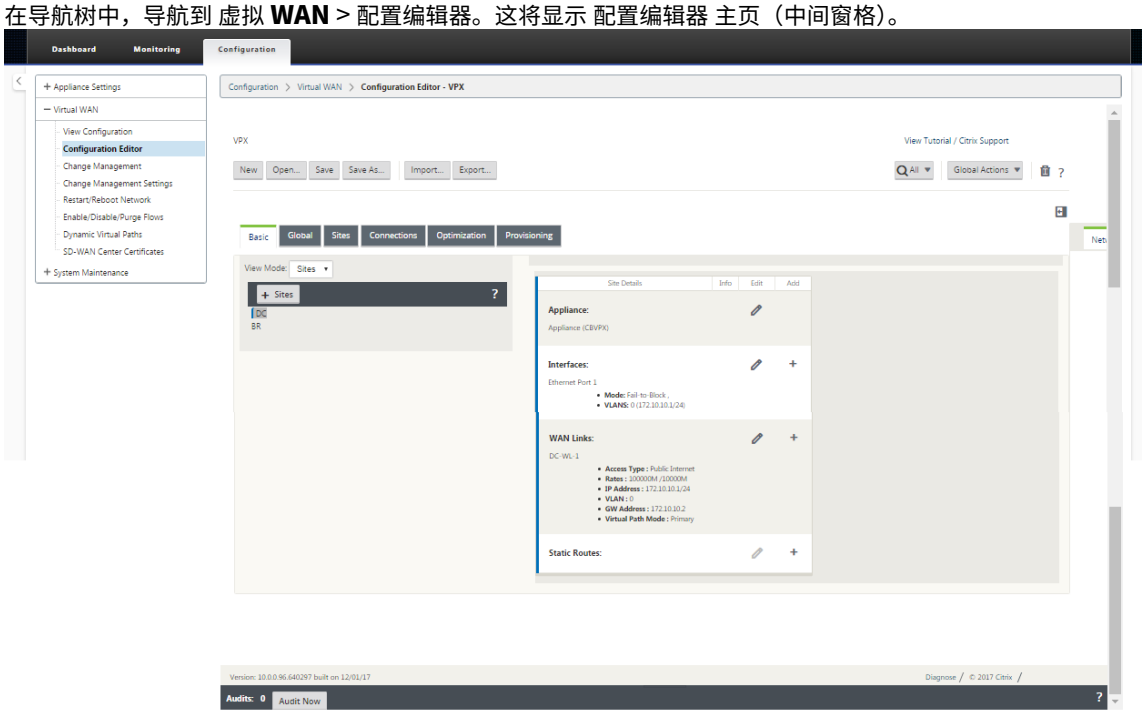
第一步是打开新的配置包，并将 MCN 站点添加到新配置。

> 注意
>
> 配置编辑器 仅在 **MCN** 控制台 模式下可用。如果导航树的 Virtual WAN 分支中 配置编辑器 选项不可用，请参阅将管理 Web 界面切换到 MCN 控制台模式 部分以获取有关更改控制台模式的说明。
>
> 建议您经常或在配置的关键点保存配置包。命名、保存和备份 MCN 站点配置部分中提供了说明。
>
> 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。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

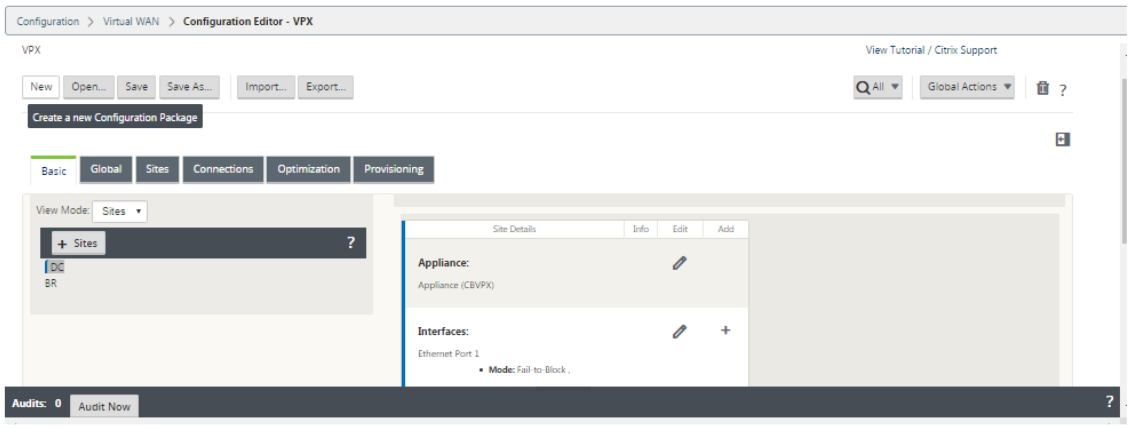
> 会话 超时 间隔设置为较高值。默认值为 60 分钟。最长时间为 9,999 分钟。出于安全原因，您必须在完成这些任务后将其重置为较低的阈值。有关说明，请参阅设置控制台会话超时间隔（可选）

要添加和开始配置 MCN 设备站点，请执行以下操作：

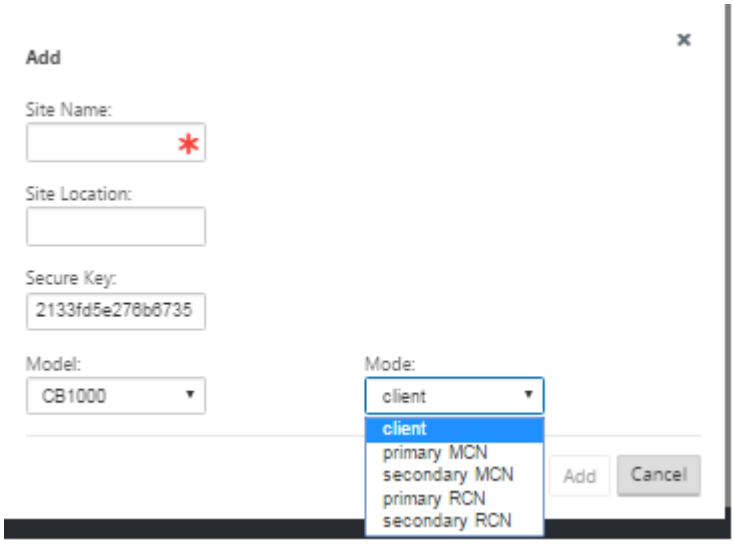
1. 在导航树中，导航到 虚拟 **WAN** > 配置编辑器。这将显示 配置编辑器 主页（中间窗格）。



2. 单击 新建 开始定义新配置。这将显示 新建 配置设置 页面。



3. 单击站点栏中的 **+** 站点以开始添加和配置 MCN 站点。此操作将显示 添加站点 对话框。



4. 输入站点信息。

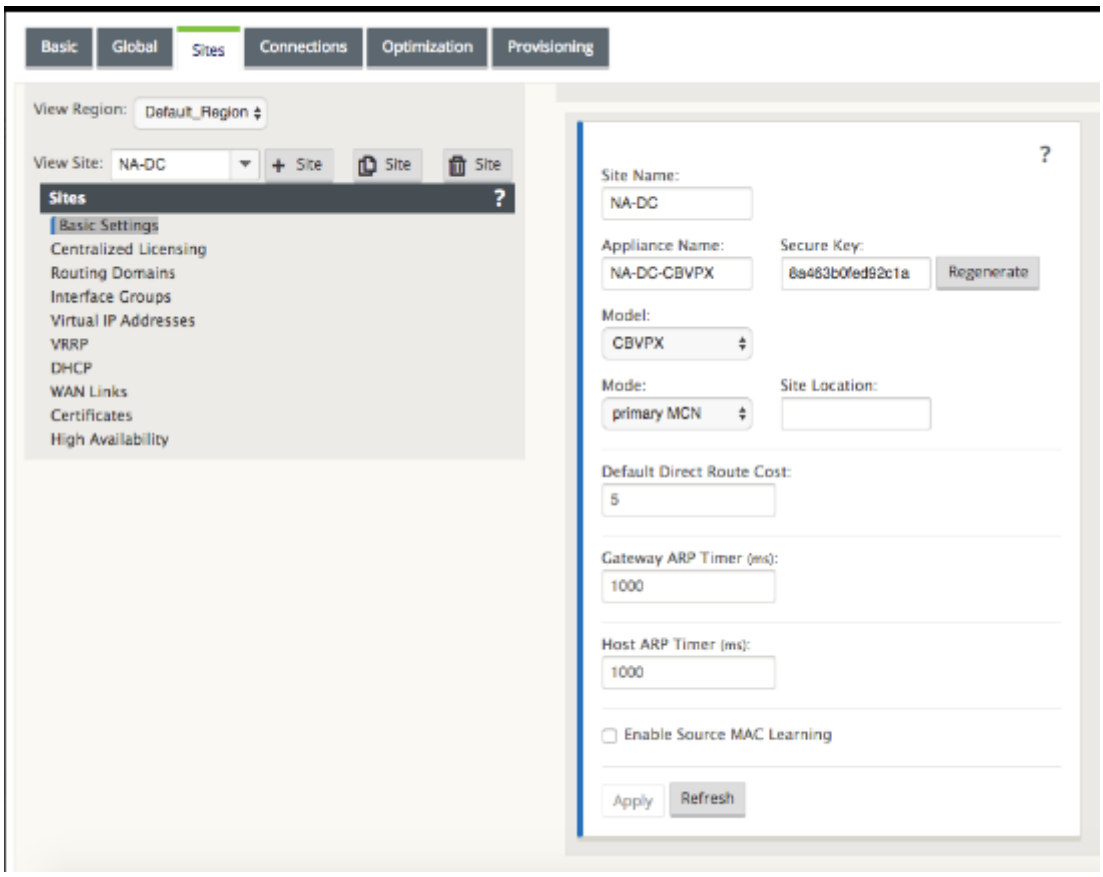
请执行以下操作：

1. 输入 站点名称 和 安全密钥。
2. 选择设备 型号。
3. 选择 模式。
4. 选择 主 **MCN** 作为模式。

> 注意
>
> 模 型 选项菜单列出了受支持的设备型号的通用型号名称。通用名称不包含标准版型号后缀，但与等效的 SD-WAN 设备型号相对应。为此 SD-WAN 设备型号选择相应的型号。（例如，如果这是 SD-WAN 4000-SE 设备，请选择 4000。）
>
> 条目不能包含空格，且必须采用 Linux 格式。

要添加站点：

1. 单击 添加 以添加网站。这会将新站点添加到 站点 树中，并显示新站点的 基本设 置配置窗体。



单击 应用后，将显示审核警告，指示需要进一步操作。红点或金色增量图标表示它出现的部分中出现错误。您可以使用这些警告来识别错误或缺失的配置信息。将光标滚到审核警告图标上，以显示该部分中错误的简短描述。您还可以单击深灰色 审 核状态栏（页面底部）以显示所有未解决审核警告的完整列表。配置过程中，在站点级别添加可配置主机 ARP 计时器 (ms)。当前默认值为 1,000 毫秒。可配置的范围从 1000 毫秒到 18 万毫秒。主机 ARP 定时器配置不适用于管理端口。

2. 输入新站点的基本设置，或接受默认设置。在 Citrix SD-WAN 部署（如网关和单臂）中，当频繁收到 ARP 请求时，访问点会变得过载，影响流量。您现在可以将 ARP 定时器配置为发送具有特定间隔时间的 ARP 请求。时间间隔配置为秒。在 Citrix SD-WAN 设备 GUI 中的 基本设 置 选项卡下配置数据中心站点时，可以配置 ARP 时间间隔。

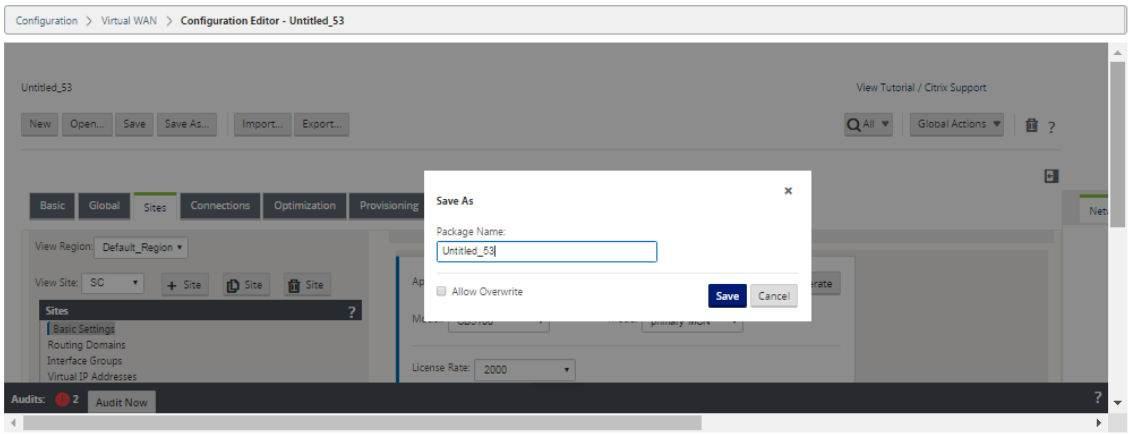
3. （可选，推荐）保存正在进行的配置。

如果您无法在一个会话中完成配置，则可以随时保存配置，以便稍后返回完成配置。配置将保存到本地设备上的 Workspace。要在已保存的配置中继续工作，请单 击 配置编辑器 菜单栏（页面顶部）中的 打开。这将显示一个用于选择要修改的配置的对话框。

> 注意
>
> 作为额外的预防措施，建议您使用另存为（而不是保存），以避免覆盖错误的配置包。

要保存当前配置包，请执行以下操作：

1. 单击 另存为（位于 配置编辑器 中间窗格顶部）。这将打开 另存为 对话框。



2. 输入配置包名称。如果要将配置保存到现有软件包，请务必在保存之前选择 允许覆盖。
3. 单击保存。

如何为 **MCN** 配置接口组

添加新 MCN 站点后，下一步是为站点创建和配置虚拟接口组。

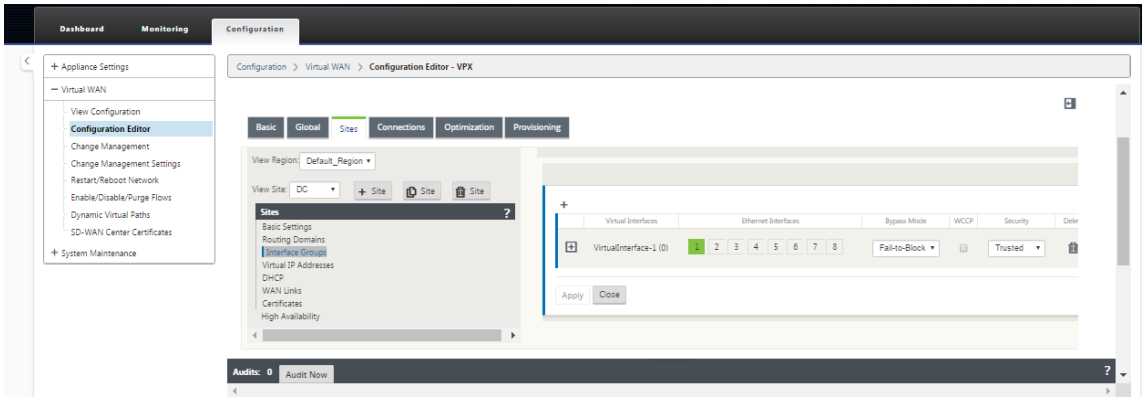
以下是配置虚拟接口组的一些准则：

- 使用最能描述组的逻辑名称。
- 受信任的网络是在防火墙后面受到保护的网络。
- 虚拟接口将接口关联到无法连接 (FTW) 对。
- 单个 WAN 接口不能位于 FTW 对中。
- IPv6 地址在 11.1.0 版本中引入，仅支持不受信任的接口。不受信任的接口是不可路由的，用于虚拟路径流量。

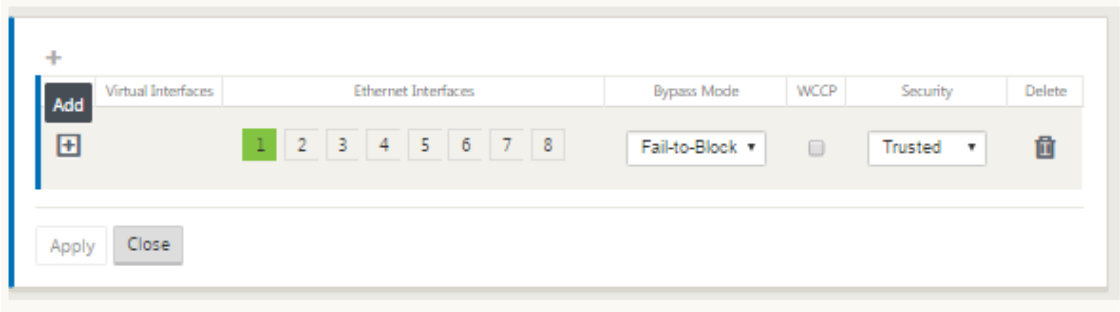
> 注意
>
> 有关配置虚拟接口组的更多准则和信息，请参阅 虚拟路由和转发 部分。

要将虚拟接口组添加到新 MCN 站点，请执行以下操作：

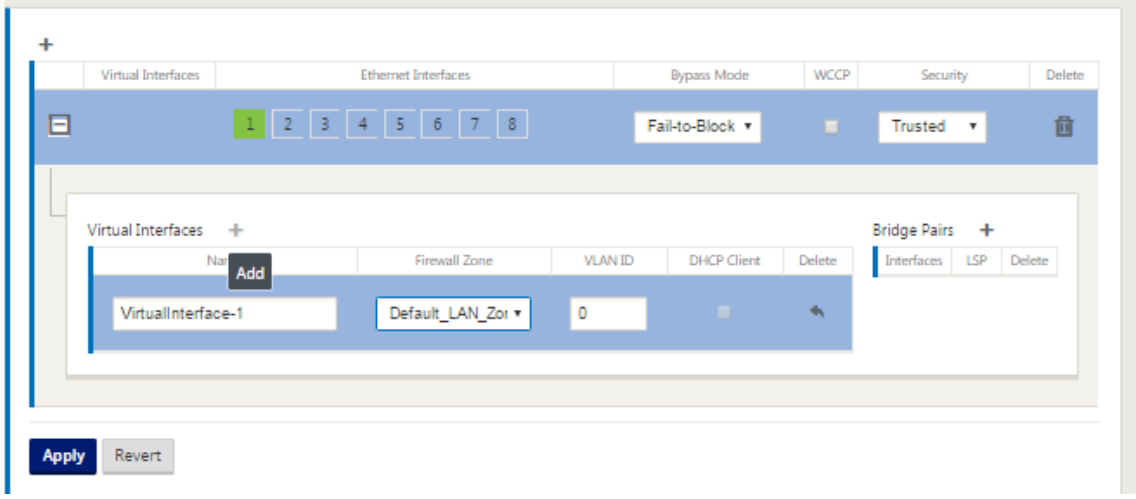
1. 继续在 配置编辑器 的 站 点 视图中，从 查看站点 下拉菜单中选择站 点。这将打开所选站点的配置视图。



2. 单击 **+** 以添加虚拟接口组。这将向表中添加一个新的空白虚拟接口组条目，并将其打开以进行编辑。

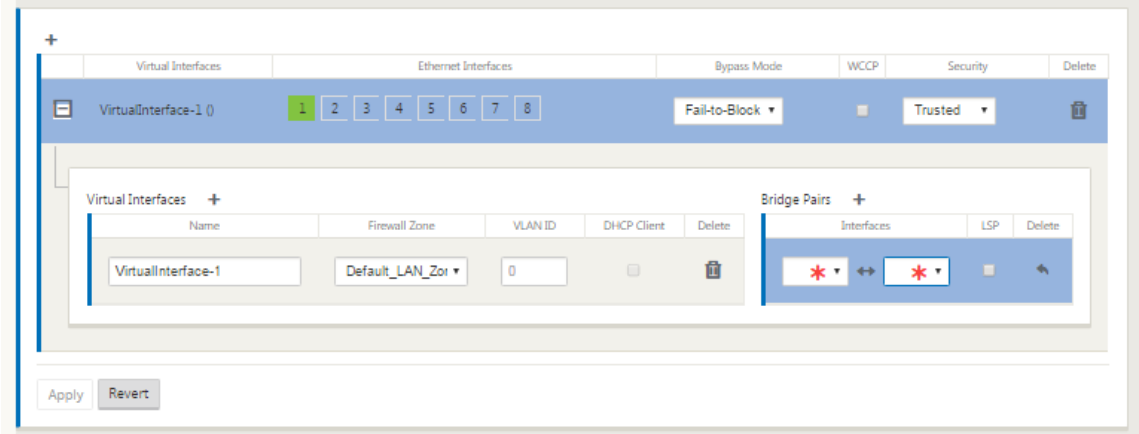


3. 单击虚拟接口右侧的 **+**。这将向表中添加一个新的空白组条目，并将其打开以进行编辑。

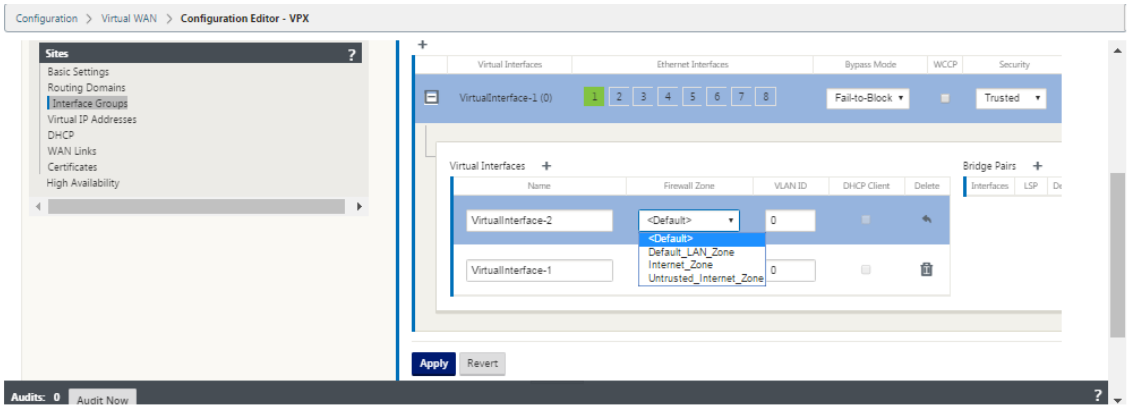


4. 选择要包含在组中的以太网接口。在以太网接口下，单击一个接口以包含/排除该接口。您可以选择要包含在组中的任意数量的接口。

5. 从下拉菜单中选择旁路模式（无默认值）。旁路模式 指定在设备或服务发生故障或重新启动时虚拟接口组中桥接配对接口的行为。选项包括：**Fail-to-Wire** 或 **Fail-to-Block**。
6. 从下拉菜单中选择 安全级别。这指定了虚拟接口组的网络段的安全级别。选项包括：可信或不可信。受信任的区段受防火墙保护（默认为 受信任）。
7. 单击您添加的虚拟接口左边缘的 **+**。这将显示 虚拟接口 表。



8. 单击虚拟接口右侧的 **+**。这将显示 名称、防火墙区域、**VLAN ID**、定向广播、客户端模式 和 无状态地址自动配置 **(SLAAC)**。



9. 输入此虚拟接口组的 名称 和 **VLAN ID**。
   - 名称—这是引用此虚拟接口的名称。
   - 防火墙区域 -从下拉菜单中选择防火墙区域。

- **VLAN ID** —这是用于识别和标记进出虚拟接口的流量的 ID。对原生/未标记的流量使用 0（零）的 ID。
- 客户端模式—从下拉菜单中选择客户端模式。
- 定向广播 -在虚拟接口上，可通过启用复选框将定向广播数据包转发给虚拟 IP 子网。
- **SLAAC** —虚拟接口上的启用 无状态地址自动配置 **(SLAAC)** 复选框允许虚拟接口自动从连接的路由器获取全局 IPv6 地址。打开 **SLAAC** 的虚拟接口不需要配置的虚拟 IP 地址。

  > 注意
  > 只能在不受信任接口的分支站点上启用 SLAAC。

  您可以释放或续订 SLAAC 的 IP 地址。

10. 单击 桥对 右侧的 **+**。这将添加一个新的 桥梁对 条目并将其打开以进行编辑。
11. 从下拉菜单中选择要配对的以太网接口。要添加更多对，请再次单击 桥接对 旁边的 **+**。
12. 单击应用。这将应用您的设置并将新的虚拟接口组添加到表中。在此阶段，您将看到一个黄色的增量审核警报图标，位于新的虚拟接口组条目右侧。这是因为您尚未为站点配置任何虚拟 IP 地址 (VIP)。现在，您可以忽略此警报，因为当您为站点正确配置了 Virtual IP 时，它会自动解决。
13. 要添加更多虚拟接口组，请单击 接口组 分支右侧的 **+** ，然后按上面所示继续操作。

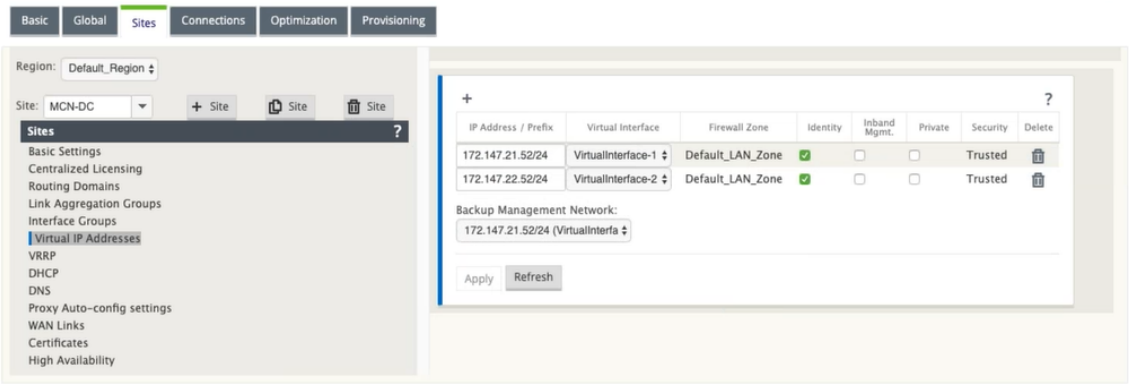
如何为 **MCN** 配置虚拟 **IP** 地址

下一步是为站点配置虚拟 IP 地址，并将其分配给相应的组。

1. 继续在新 MCN 站 点 的 站点 视图中，单击 虚拟 **IP** 地址 左侧的 **+**。这将显示新站点的 虚拟 **IP** 地址 表。
2. 单击 虚拟 **IP** 地址 右侧的 **+** 以 添加地址。这将打开用于添加和配置新虚拟 IP 地址的窗体。
3. 输入 **IP** 地址 / 前缀 信息，然后选择与该地址关联的 虚拟接口。虚拟 IP 地址必须包含完整的主机地址和网络掩码。
4. 为虚拟 IP 地址选择所需的设置，例如防火墙区域、标识、私有和安全。
5. 选择 **Inband Mgmt** 可允许虚拟 IP 地址连接到管理服务，如 Web UI 和 SSH。

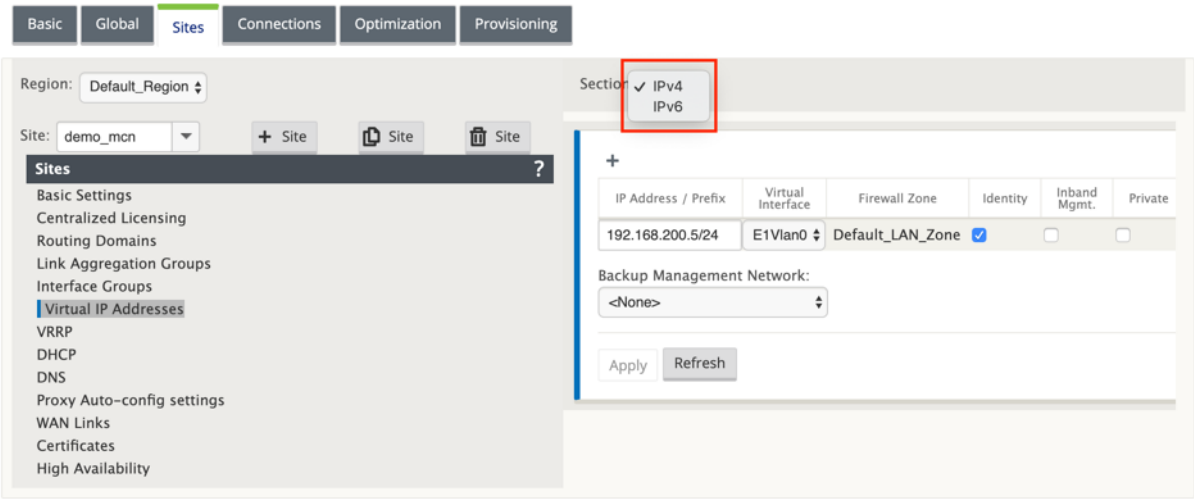
   > 注意：
   >
   > 接口应为安全类型 受信任 且已启用 标识。

6. 选择虚拟 IP 作为 备份管理网络。如果管理端口未配置默认 Gateway，则可以使用虚拟 IP 地址进行管理。



7. 单击应用。这会将地址信息添加到站点，并将其包含在站点 虚拟 **IP** 地址 表中。
8. 要添加更多虚拟 IP 地址，请单击 虚拟 **IP** 地址 右侧的 **+**，然后按照上述步骤继续操作。

从 11.1.0 版本开始，虚拟 **IP** 地址 下有两个子部分：**IPv4** 和 **IPv6** 地址。



限制

- 如果在同一 WAN 链路上配置 IPv4 和 IPv6 接入接口，则只会创建一对路径。
- 如果 IPv6 路径出现故障，则同一 WAN 链路的 IPv4 不会发生回退。
- 11.1.0 版本不支持跟踪 IPv6 地址。
- IPv6 仅支持 SD-WAN 设备之间通过虚拟路径进行通信。不支持互联网和内联网服务。在 11.1.0 版本中不支持管理平面。
- 在 11.1.0 版本中，210 台设备上的 LTE 链路将不支持 IPv6。
- IPv6 不支持 DHCPv6 客户端和服务器。您可以将 SLAAC 配置为自动寻址。

您需要为新创建的不受信任接口添加虚拟 IP 地址，或者如果 SLAAC 是分支站点，则可以启用 SLAAC。添加虚拟 IP 地址：

1. 从“节”下拉菜单中选择 IPv6。

2. 定义以下字段：
3. IP 地址/前缀—提供完整的主机地址和子网掩码。
4. 虚拟接口—从下拉菜单中选择一个关联的虚拟接口。
5. 防火墙区域—虚拟接口的防火墙区域。
6. 本地链路（可选）-如果启用了“链接本地”复选框，则此 IPv6 虚拟 IP 地址可用作虚拟接口的链路本地地址。

> 注意：
> 如果未启用链接本地复选框，装置将自动生成并分配链路本地地址。

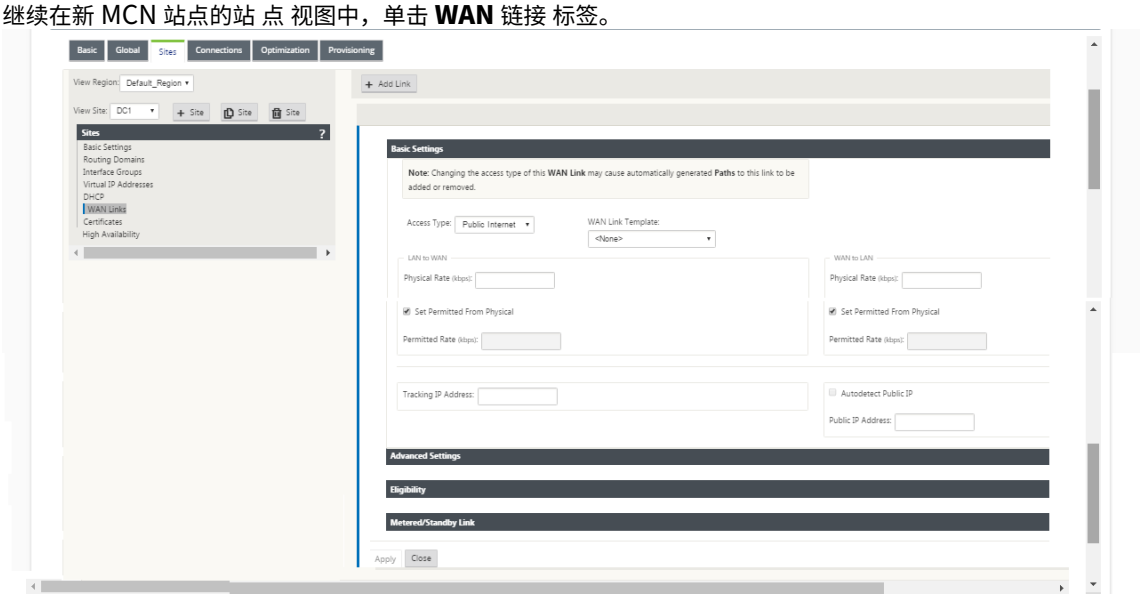
> 注意
> IPv6 支持邻居发现协议 (NDP)。

如果 IPv4 和 IPv6 访问接口都是在本地站点和远程站点上定义的，则只使用 IPv6 地址形成路径。

如何为 **MCN** 配置 **WAN** 链接

下一步是为站点配置 WAN 链接。

1. 继续在新 MCN 站点的站 点 视图中，单击 **WAN** 链接 标签。

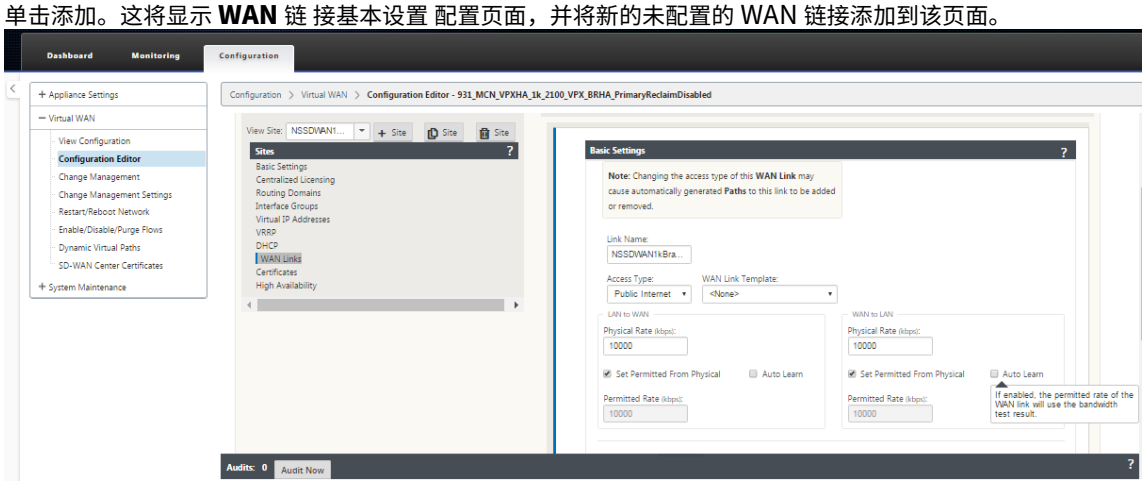


2. 单击 **WAN** 链接右侧的添加链 接以添加新的 WAN 链接。这将打开 添加 对话框。

3. （可选）如果您不想使用默认值，则输入 WAN 链接的名称。默认值为站点名称，附加以下后缀：WL-<number>，其中 <number> 为此站点的 WAN 链接数量，增量为 1。

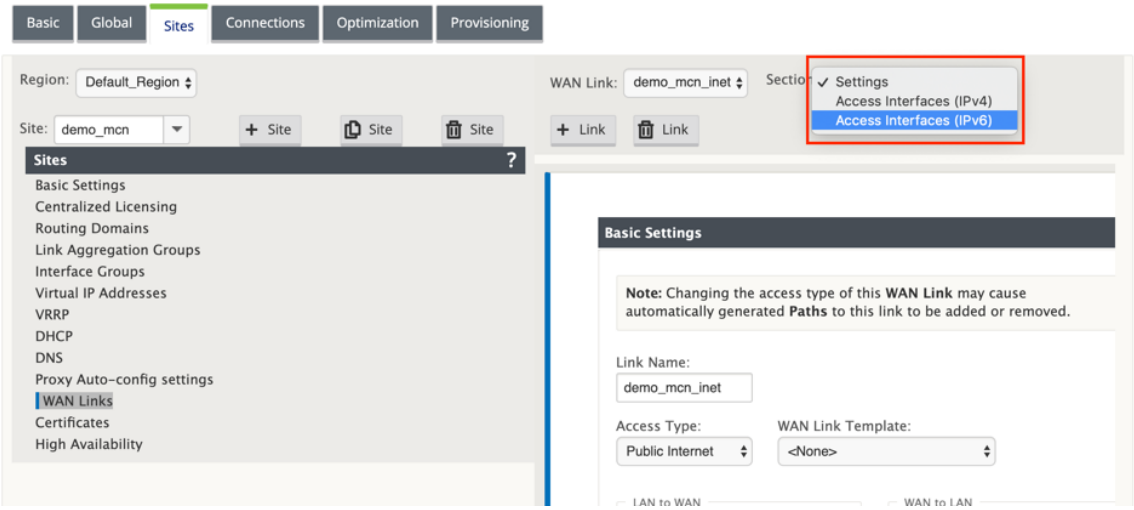
4. 从下拉菜单中选择 访问类型。这些选项是 公共互联网、专用 **Intranet** 或 私有 **MPLS**。

5. 单击添加。这将显示 **WAN** 链 接基本设置 配置页面，并将新的未配置的 WAN 链接添加到该页面。



当为同一 WAN 链路配置 IPv4 和 IPv6 接入接口时，只有两个站点之间才会形成 IPv6 路径。

1. 从 设置 下拉菜单中选择 访问接口 **(IPv6)** 。

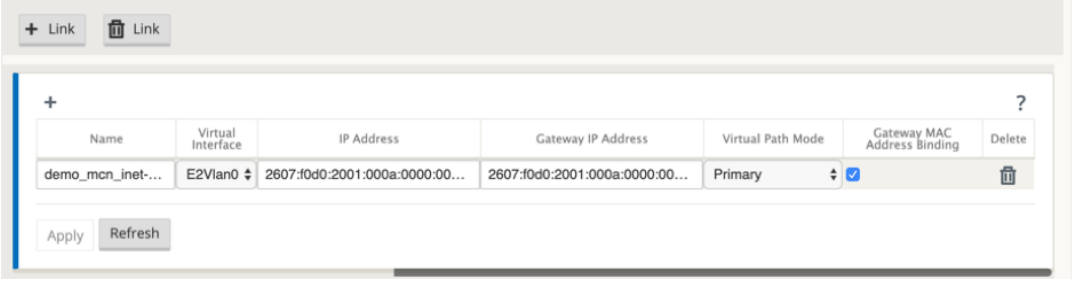


2. 定义以下字段：

- 名称—提供访问接口名称。
- 虚拟接口—选择路由域后，从下拉菜单中选择一个关联的虚拟接口。
- **IP** 地址—为 SD-WAN 上的访问接口终端节点提供静态 IP 地址。
- 网关 **IP** 地址—提供网关路由器的 IP 地址。

  > 注意
  > 如果虚拟设备配置为使用 SLAAC 模式，则无法配置 IP 地址和网关 IP 地址。

- 虚拟路径模式 -从下拉菜单中选择虚拟路径模式，以确定此 WAN 链路上虚拟路径流量的优先级。
- 网关 **MAC** 地址绑定—如果启用了“网关 **MAC** 地址绑定”复选框，则 Internet 或 Intranet 服务收到的数据包的源 MAC 地址必须与网关 MAC 地址匹配。



为 WAN 链路创建 IPv6 接口后，即可使用此接口与互联网服务提供商 (ISP) 进行通信。

> 注意
> 由于初始 IPv6 产品仅提供虚拟路径连接，因此我们无法发送 LAN 端 IPv6 数据包。

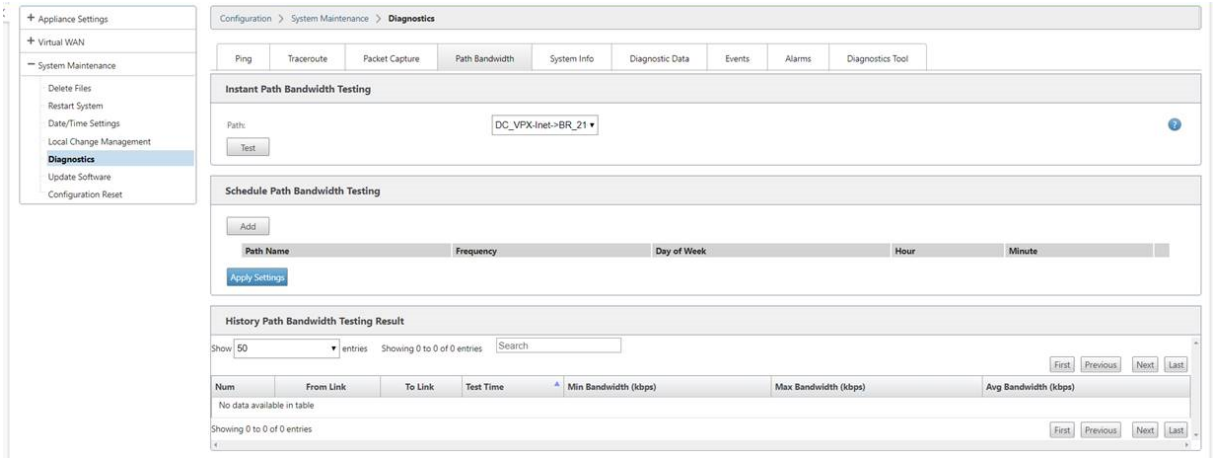
自动学习带宽消耗

自动学习在系统启动时运行，并每五分钟重复一次，直到观察到成功的结果。通过配置编辑器进行任何 WAN 链接配置更改后，自动学习也会运行。

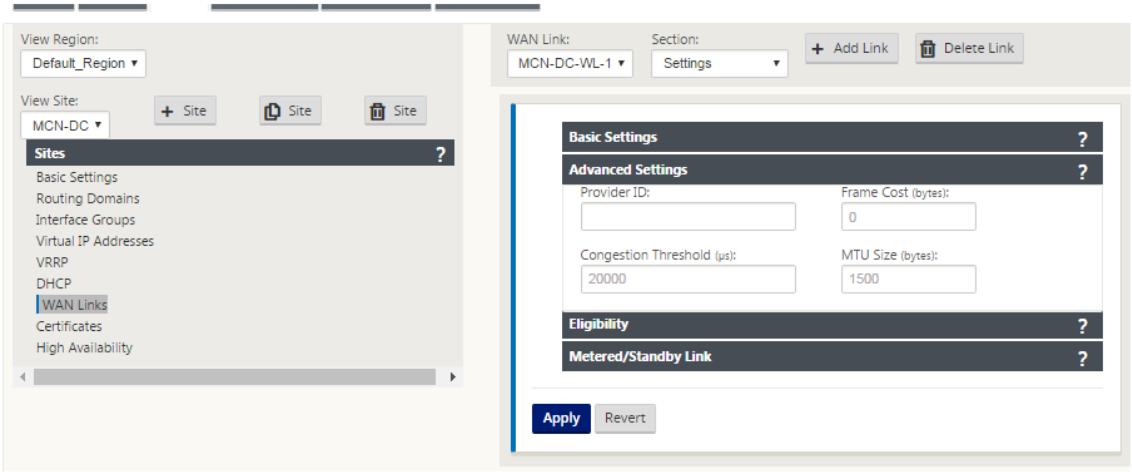
您可以手动执行测试或在 SD-WAN GUI 中安排测试。当测试成功并启用自动学习时，这些测试的结果也应适用于允许的速率。

在大型网络上使用自动学习时，如果配置更改重新启动，则所有站点在 MCN 上同时运行测试，从而导致高带宽使用率导致结果不准确。建议您每天安排一次或两次带宽测试，通常在流量较低的情况下。

> 注意
>
> WAN 链路带宽的自动检测，仅适用于分支机构，不适用于 MCN/RCN。



1. 输入新 WAN 链接的链接详细信息。将局域网配置为 WAN，WAN 配置为 局域网 设置。一些准则如下：
   - 有些互联网链接可能是不对称的。
   - 错误配置允许的速度可能会对该链接的性能产生不利影响
   - 避免使用超过承诺率的突发速度。
   - 对于 Internet WAN 链接，请务必添加公有 IP 地址。
2. 单击灰色的 高级设置 部分栏。这将打开链接的 高级设置 窗体。

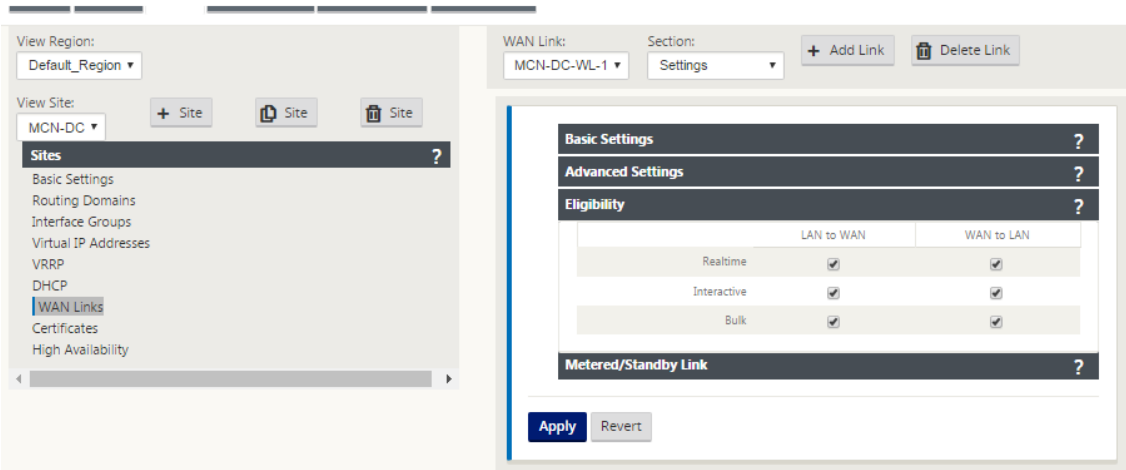


3. 输入链接的 高级设置：

   - 提供商 **ID** —（可选）输入唯一 ID 号 1-100 以指定连接到同一服务提供商的 WAN 链接。在发送重复数据包时，虚拟 WAN 使用提供程序 ID 区分路径。
   - 帧 成本（字节）—输入添加到每个数据包的头部/拖车的大小（以字节为单位）。例如，添加以太网 IPG 或 AAL5 拖车的大小（以字节为单位）。
   - 拥塞 阈值—输入拥塞阈值（以微秒为单位），之后 WAN 链路限制数据包传输，以避免进一步拥塞。
   - MTU 大 小（字节）—输入最大的原始数据包大小（以字节为单位），不包括帧成本。

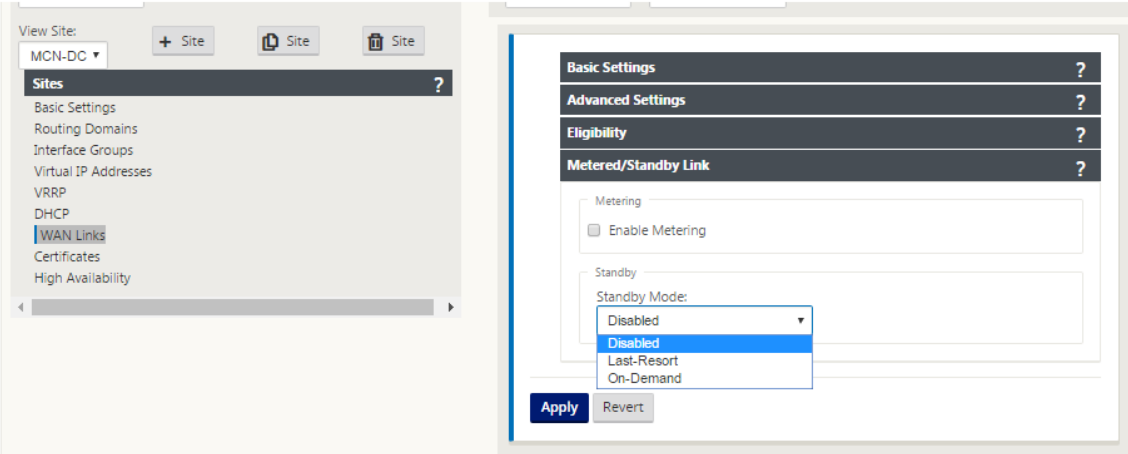
4. 单击灰色 资格 部分栏。这将打开链接的 资格 设置窗体。

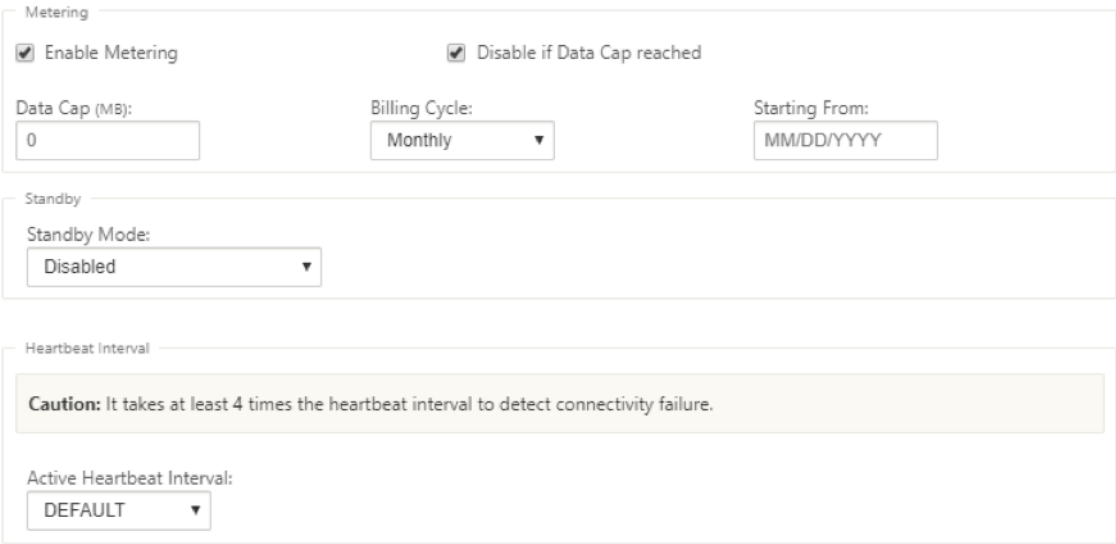
5. 选择链接的 资格 设置。



6. 单击灰色 计量链接 部分栏。这将打开链接的 按计费链接 设置 窗体。

7. （可选）选择 启用计量 以为此链接启用计量。这将显示 启用计量 设置 字段。





8. 配置链接的计量设置。输入以下命令：

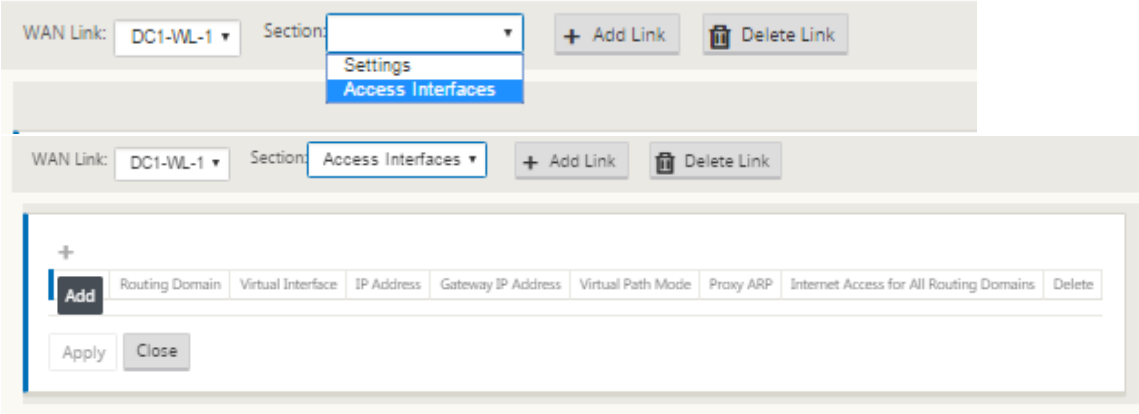
- 数据 上限 **(MB)** —输入链接的数据上限分配（以兆字节为单位）。
- 账单 周期—从下拉菜单中选择每 月或每周。
- 开 始—输入计费周期的开始日期。
- 设置 最后手段—选择此选项可在所有其他可用链接发生故障时将此链接作为最后手段的链接。在正常 WAN 条件下，Virtual WAN 仅通过计费链接发送最小流量，用于检查链接状态。但是，如果发生故障，SD-WAN 可以使用活动按计费链接作为转发生产流量的最后手段。

单击应用。这会将您指定的设置应用到新的 WAN 链接。

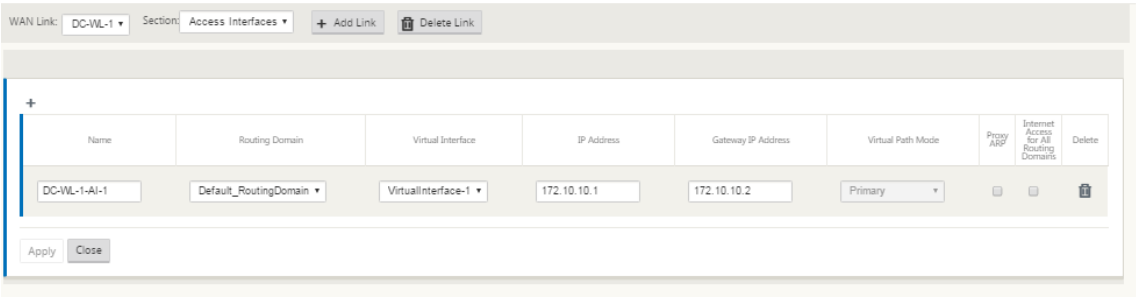
下一步是为新的 WAN 链接配置访问接口。访问接口由虚拟接口、WAN 端点 IP 地址、网关 IP 地址和虚拟路径模式组成，共同定义为特定 WAN 链接的接口。每个 WAN 链接必须至少有一个访问接口。

如何配置访问接口：

1. 在链 接的 **WAN** 链接配置页面中选择访问接口。这将打开站点的访问接口视图。



2. 单击 **+** 以添加界面。这会向表格中添加一个空条目，并将其打开以进行编辑。输入链 接的访问界面 设置。每个 WAN 链接必须至少有一个访问接口。



3. 输入以下命令：

- 名称—这是引用此访问接口的名称。输入新访问接口的名称，或接受默认值。默认设置使用以下命名约定：WAN_link_name-AI-number：其中 *wan_link_Name* 是您要与此接口关联的 WAN 链接的名称，数字是当前为此链接配置的访问接口数量，增加 1。

> 注意
>
> 如果名称显示为截断，您可以将光标放在字段中，然后单击并按住鼠标向右或向左滚动以查看截断部分。

- 虚拟接口—这是此访问接口使用的虚拟接口。从为此分支站点配置的虚拟接口下拉菜单中选择一个条目。
- 路由域 -要为访问接口选择的路由域。
- **IP** 地址—这是访问接口终结点从设备到 WAN 的 IP 地址。
- **Gateway IP** 地址—这是网关路由器的 IP 地址。
- 虚拟路径模式—指定此 WAN 链接上虚拟路径流量的优先级。选项包括：主要、次要或排除。如果设置为 排除，则此访问接口仅用于 Internet 和 Intranet 流量。
- 代理 **ARP** —选中要启用的复选框。如果启用，则当 Gateway 关无法访问时，虚拟 WAN 设备会回复针对网关 IP 地址的 ARP 请求。

1. 单击应用。

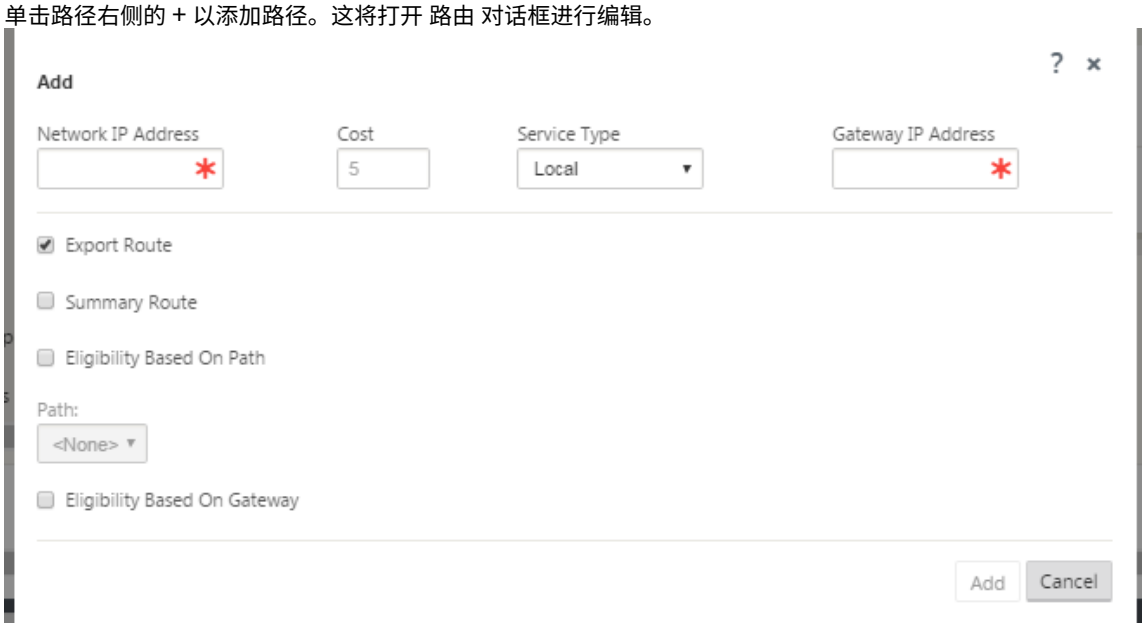
您现在已完成配置新的 WAN 链接。重复这些步骤以添加和配置站点的更多 WAN 链接。

下一步是添加和配置站点的路由。

如何为 **MCN** 配置路由

要添加和配置站点的路由，请执行以下操作：

1. 单击新 MCN 站点的 连接 视图，然后选择 路由。这将显示站点的 路径 视图。
2. 单击路径右侧的 + 以添加路径。这将打开 路由 对话框进行编辑。



3. 输入新路径的路径配置信息。输入以下命令：

- 网络 **IP** 地址—输入 网络 **IP** 地址。
- 成本—输入 1 到 15 之间的权重，以确定此路径的路径优先级。成本较低的路径优先于成本较高的路径。默认值为 5。
- 服务类型—从此字段的下拉菜单中选择路径的服务类型。
  - 虚拟路径—此服务管理跨虚拟路径的流量。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。这是通过不断测量和适应不断变化的应用需求和广域网条件来实现的。SD-WAN 设备根据每个路径测量网络。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。此类型的流量未封装。在拥堵期间，SD-WAN 通过相对于虚拟路径的速率限制互联网流量，主动管理带宽，并根据管理员建立的 SD-WAN 配置管理 Intranet 流量。
  - **Intranet** —此服务管理尚未定义为跨虚拟路径传输的企业 Intranet 流量。与互联网流量一样，它仍然是未封装的，SD-WAN 通过在拥塞期间限制此流量相对于其他服务类型的速率来管理带宽。在某些情况下，

如果为虚拟路径上的 Intranet 回退配置，则通常由虚拟路径传输的流量可能会被视为 Intranet 通信，以保持网络可靠性。

- 直通—此服务管理要通过虚拟 WAN 传递的流量。定向到直通服务的流量包括广播、ARP 和其他非 IPv4 流量，以及虚拟 WAN 设备本地子网、配置的子网或网络管理员应用的规则上的流量。SD-WAN 不会延迟、形状或修改此流量。因此，必须确保直通流量不会消耗 SD-WAN 设备配置为用于其他服务的 WAN 链接上的大量资源。
- 本地—此服务管理不匹配其他服务的站点的本地 IP 流量。SD-WAN 忽略来源和发往本地路由的流量。
- **GRE** 隧道—这项服务管理注定于 GRE 隧道的 IP 流量, 并匹配在现场配置的局域网 GRE 隧道. GRE 隧道功能允许您配置 SD-WAN 设备以终止局域网上的 GRE 隧道。对于具有服务类型 GRE 隧道的路由，Gateway 必须位于本地 GRE 隧道的隧道子网之一。
- 局域网 **IPsec** 隧道—此服务管理发往 IPsec 隧道的 IP 流量。
- 国际路由 -此服务允许站点内的路由域之间或不同站点之间的路由泄漏。这样就不需要边缘路由器来处理路由泄漏。

- 网关 **IP** 地址—输入此路由的 网关 **IP** 地址。
- 资格 -基于路径（复选框）-（可选）如果启用，则选定路径关闭时路由不会接收流量。
- 路径—指定用于确定路径资格的路径。

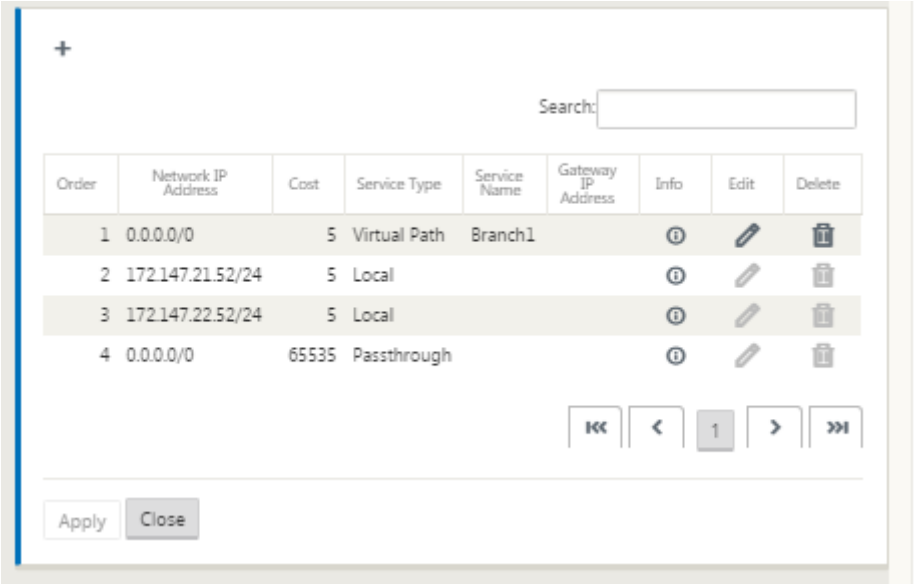
根据 服务类型，将显示以下设置：

服务类型	服务类型设置
虚拟路径	下一跳站点—这表示虚拟路径数据包被定向到的远程站点。
Internet	导出路由：启用/禁用将路由导出到其他连接站点，基于路径的资格
内联网	导出路线、Intranet 服务、基于路径的资格、基于隧道的资格
直通	基于路径的资格
本地	导出路线、总结路线、基于路径的资格
GRE 隧道	导出路线、基于路径的资格、基于网关的资格
IPsec 隧道	导出路线、基于路径的资格、IPsec 隧道、基于隧道的资格
放弃	出口路线、汇总路线
国际路由	国际路由域服务

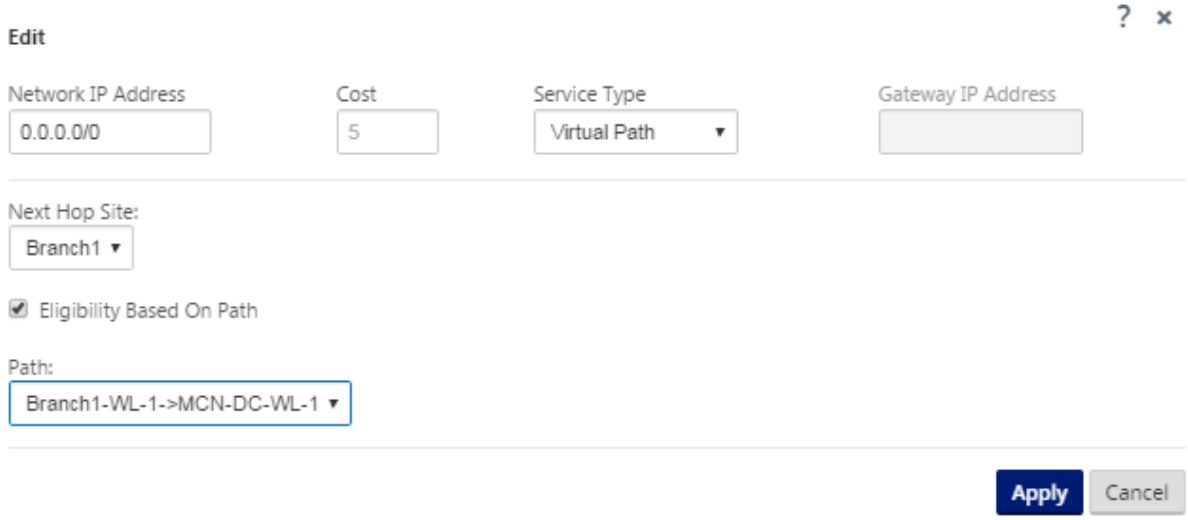
1. 单击应用。

> 注意
>
> 单击 应用后，可能会显示审核警告，指示需要进一步操作。红点或金色增量图标表示它出现的部分中出现错误。您

> 可以使用这些警告来识别错误或缺失的配置信息。将光标滚到审核警告图标上，以显示该部分中错误的简短描述。您还可以单击深灰色 审 核状态栏（页面底部）以显示所有审核警告的完整列表。



您还可以编辑配置的路由，如下所示。



要为网站添加更多路线，请单击 路线 分支右侧的 **+**，然后按上述操作。

您现在已完成输入新 MCN 站点的主要配置信息。以下两部分提供了有关更多可选步骤的说明：

- 为 MCN 站点配置高可用性 (HA)（可选）。
- 启用和配置虚拟 WAN 安全和加密（可选）。

如果您现在不想配置这些功能，您可以直接进入命名、保存和备份 MCN 站点配置。

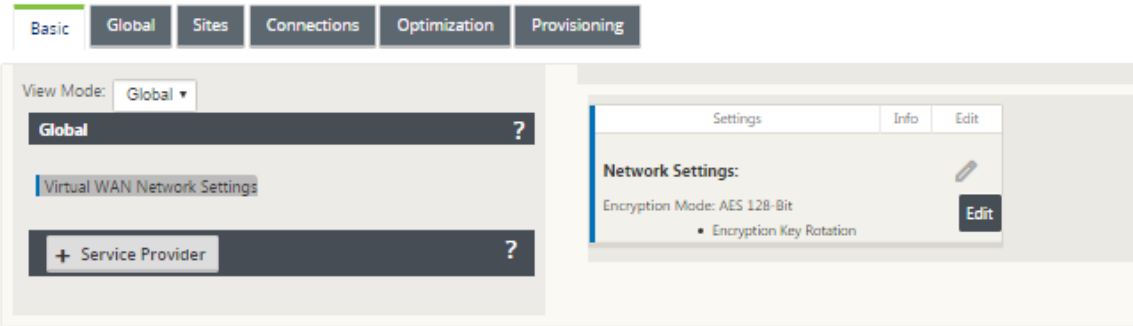
启用和配置虚拟 **WAN** 安全和加密（可选）

June 22, 2021

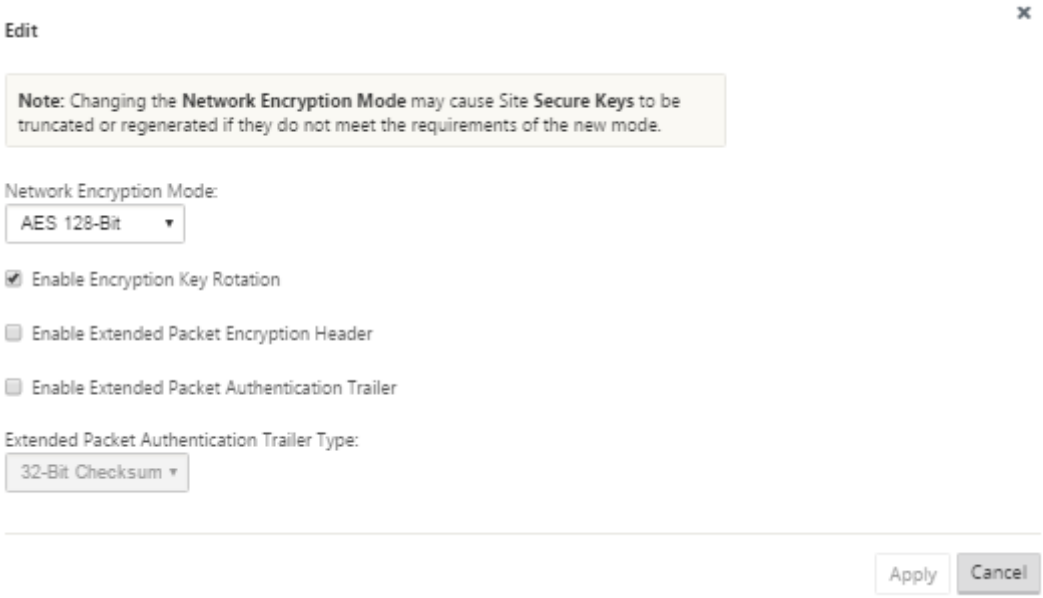
要启用和配置虚拟 WAN 安全性和加密，请执行以下操作：

> 注意
>
> 启用虚拟 WAN 安全性和加密是可选的。

1. 导航到 配置编辑器 中的 基本 选项卡，从 查看 模式选择 全局。将显示虚拟网络设置配置窗体。



2. 单击 编辑（铅笔图标）以启用对表单的编辑。



3. 输入您的全局安全设置。这些选项如下所示：

   - 网络加密模式—这是用于加密路径的加密算法。从下拉菜单中选择以下选项之一：**AES 128** 位 或 **AES 256** 位。
   - 启用加密密钥轮换：启用后，加密密钥将按 10-15 分钟的间隔轮换。

- 启用扩展数据包加密标头：启用后，16 字节的加密计数器会在加密流量的前置添加，以作为初始化矢量，并随机化数据包加密。
- 启用扩展数据包身份验证拖车：启用后，将在加密流量的内容附加身份验证代码，以验证邮件是否未经更改传递。
- 扩展数据包身份验证拖车类型：这是用于验证数据包内容的拖车类型。从下拉菜单中选择以下选项之一：**32** 位校验和或 **SHA-256**。

4. 单击 应用 以将您的设置应用于配置。

这完成了 MCN 站点的配置。下一步是命名并保存新 MCN 站点配置（可选，但建议使用），如以下部分所述。

> 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。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，建议您经常或在配置的关键点保存配置包。

配置辅助 **MCN**

November 1, 2021

您可以将站点配置为辅助 MCN 以支持 MCN 冗余。辅助 MCN 持续监视主 MCN 的运行状况。如果主 MCN 发生故障，则辅助 MCN 代表 MCN 的角色。要创建辅助 MCN，请在 模式 选项中添加新站点时选择辅助 MCN。您可以手动配置虚拟接口、虚拟 IP、WAN 链接和其他设置。同样，您也可以配置辅助 RCN。

> 注意
>
> 请勿将辅助 MCN 配置与高可用性配置混淆。在辅助 MCN 配置中，位于不同地理位置的分支/客户端站点被配置为辅助 MCN 以启用灾难恢复。在 HA 配置中，将两台设备配置为相同的子网或地理位置，以确保容错。有关配置高可用性配置的信息，请参阅 高可用性部署。

您可以根据使用情况、带宽要求和要支持的站点数量为辅助 MCN 选择设备型号。

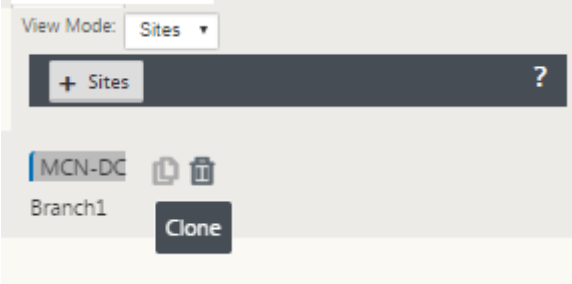
主 MCN 至辅助 MCN 切换发生在主 MCN 处于非活动状态 15 秒后。无法为辅助 MCN 配置主回收，主回收会在主设备重新开启并保持计时器过期后自动执行主回收。

配置辅助 MCN 的最佳方法是克隆现有 MCN，因为它保留了大部分 MCN 配置。克隆站点时，将复制站点的整套配置设置，并在单个窗体屏幕中显示。然后，您可以根据要求快速轻松地修改设置。

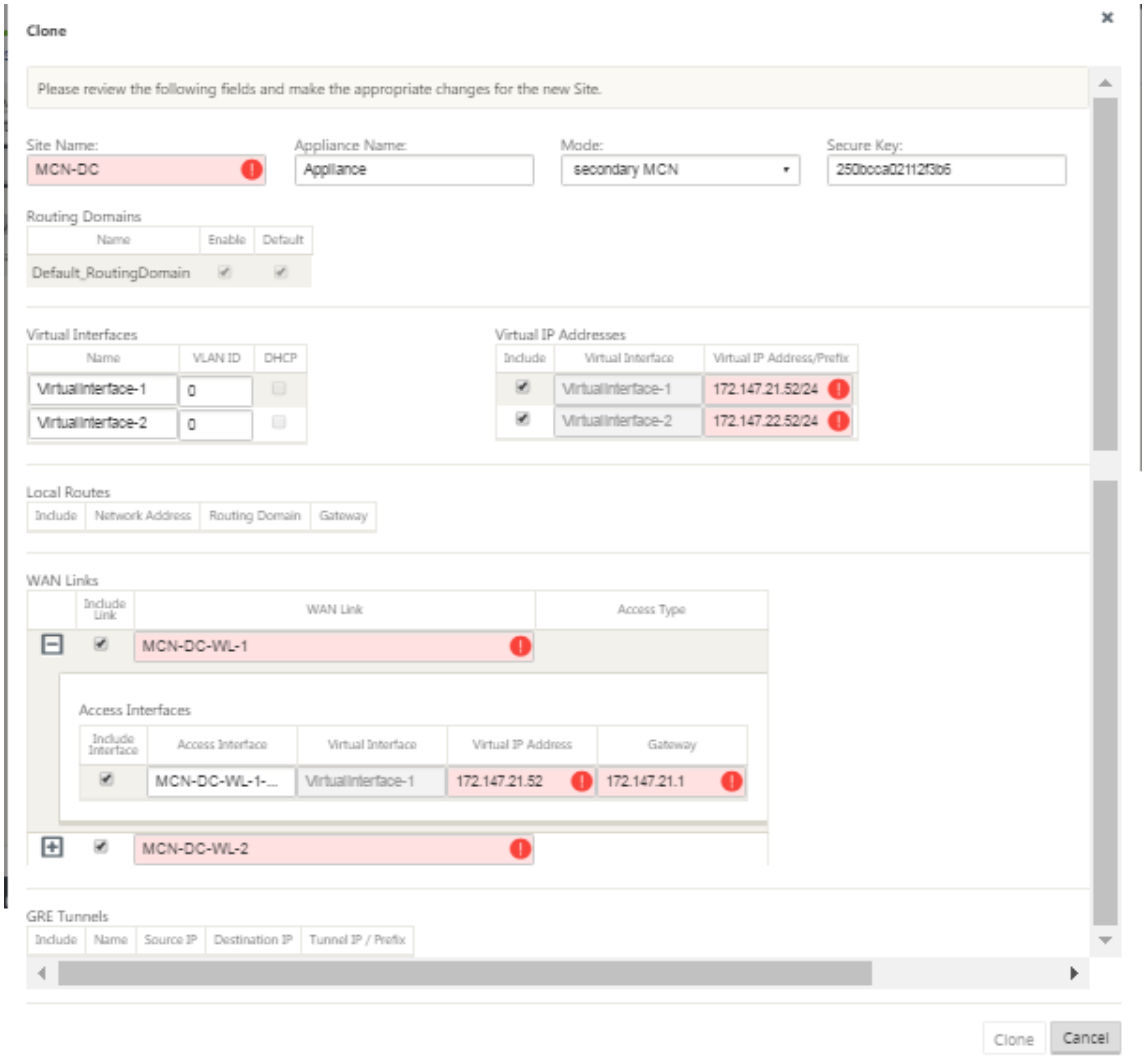
> 注意
>
> 您可以克隆 MCN 以创建辅助 MCN 或分支站点。您只能配置一个辅助 MCN。

要克隆 **MCN** 站点并创建辅助 **MCN**，请执行以下操作：

1. 在配置编辑器中，导航到 基本 > 站点，然后单击 MCN 站点的克隆图标。



2. 输入新站点的配置参数设置。



> 注意：
>
> 带有审核警报图标（红点）的高亮显示字段表示必需的参数设置，该参数设置必须具有与当前设置不同的值。

3. 在 模 式字段中，选择 辅助 **MCN**。解决所有审核提醒。

4. 单击 克隆 以创建辅助 MCN 站点。

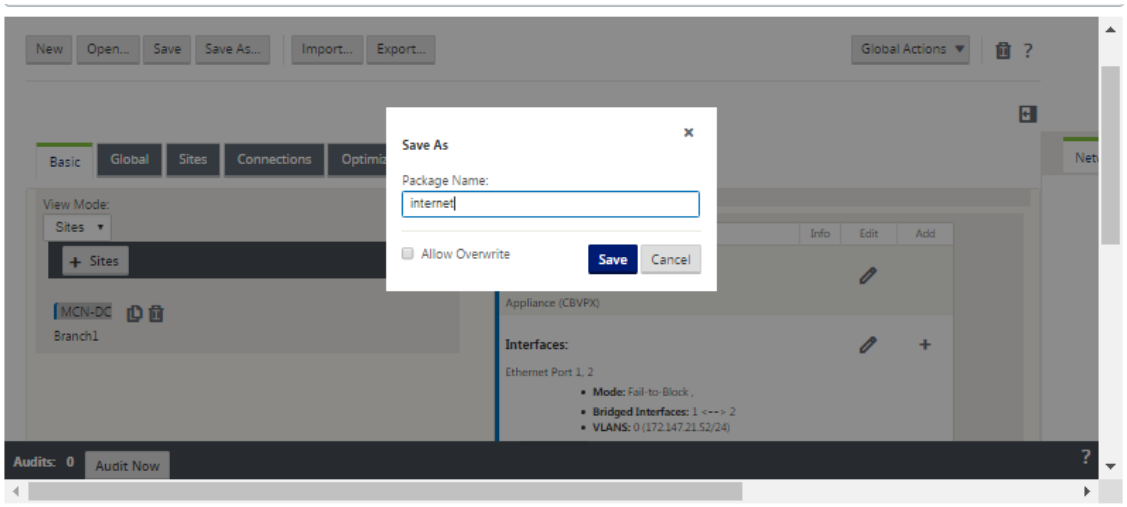
管理 MCN 配置

June 22, 2021

下一步是命名并保存新的配置，也将其视为配置包。此步骤在配置中是可选的，但建议使用此步骤。配置包将保存到本地设备上的 Workspace。然后，您注销管理 Web 界面，然后继续配置过程。但是，如果您注销，则应在恢复时重新打开保存的配置。下面提供了打开已保存配置的说明。

> 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。您应该重新登录到系统，并从头开始重复配置过程。因此，建议您经常或在配置的关键点保存配置包。
> 提示：
>
> 作为额外的预防措施，建议您使用“另存为”而不是“保存”来避免覆盖错误的配置包。

1. 单击 另存为（位于 配置编辑器 中间窗格顶部）。此时将打开 另存为 对话框。



2. 键入配置包名称。

> 注意
>
> 如果要将配置保存到现有配置包中，请务必在保存之前选择 允许覆盖。

3. 单击保存。

> 注意

> 保存配置文件后，您可以注销管理 Web 界面，然后继续配置过程。但是，如果您注销，则应在恢复时重新打开保存的配置。说明在将保存的配置包加载到配置编辑器中部分中提供。

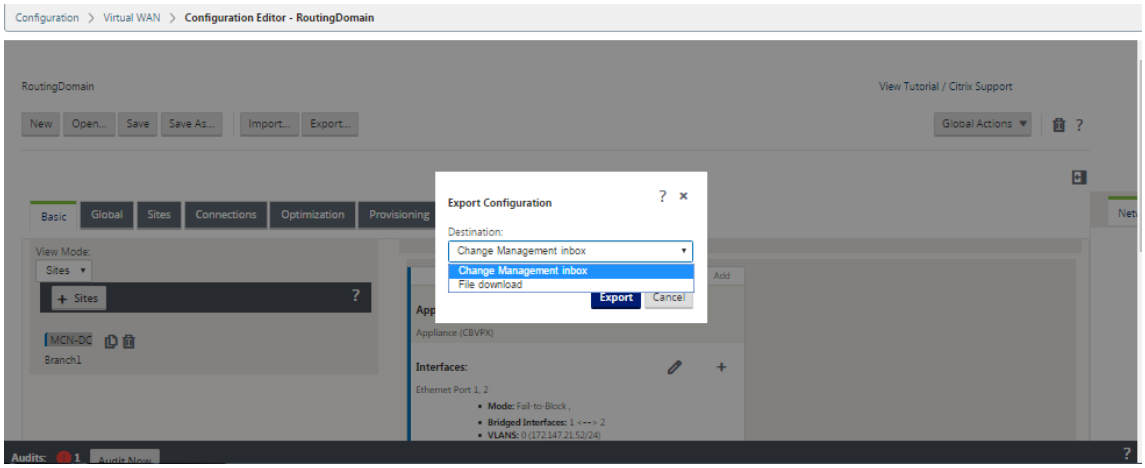
您现在已完成 MCN 站点配置，并创建了新的 SD-WAN 配置包。您现在可以添加和配置分支站点。设置分支站点中提供了说明] (/en-us/citrix-sd-wan/current-release/configuration/setup-branch-nodes.html)。

导出配置包的备份副本

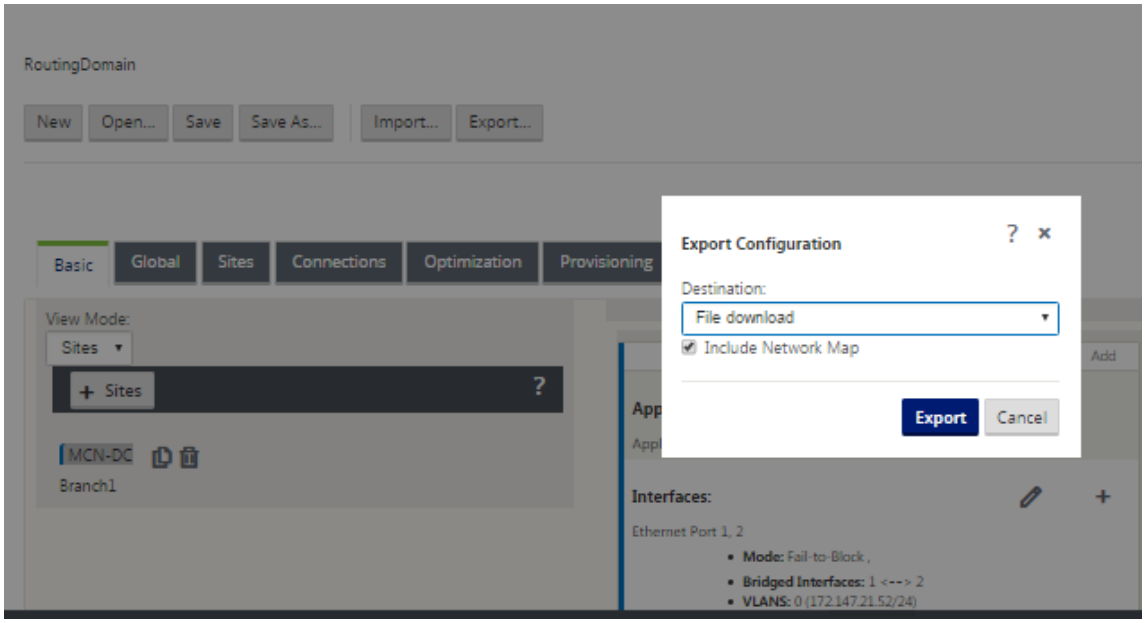
除了将正在进行的配置保存到设备 Workspace 之外，建议您还定期将配预配份到本地电脑。

要将当前配置包导出到电脑，请执行以下操作：

1. 单击导出。这将显示 导出配置 对话框。



2. 从 目标：下拉菜单中选择文件下载。这将显示默认情况下选择的包括网络映射 选项。



3. 接受默认值，然后单击 导出。这包括配置包中的 网络映射 信息，并打开一个文件浏览器，用于指定用于保存配置的名称和位置。

4. 导航到电脑上的保存位置，然后单击 保存。这样会将配置包保存到您的电脑中。

> 注意
>
> 要恢复备份的配置包，您可以使用 导 入 操作从电脑导入该软件包并将其加载到 配置编辑器 中。然后，您可以将导入的软件包保存到管理 Web 界面 Workspace 以供将来使用。

导入备份的配置包

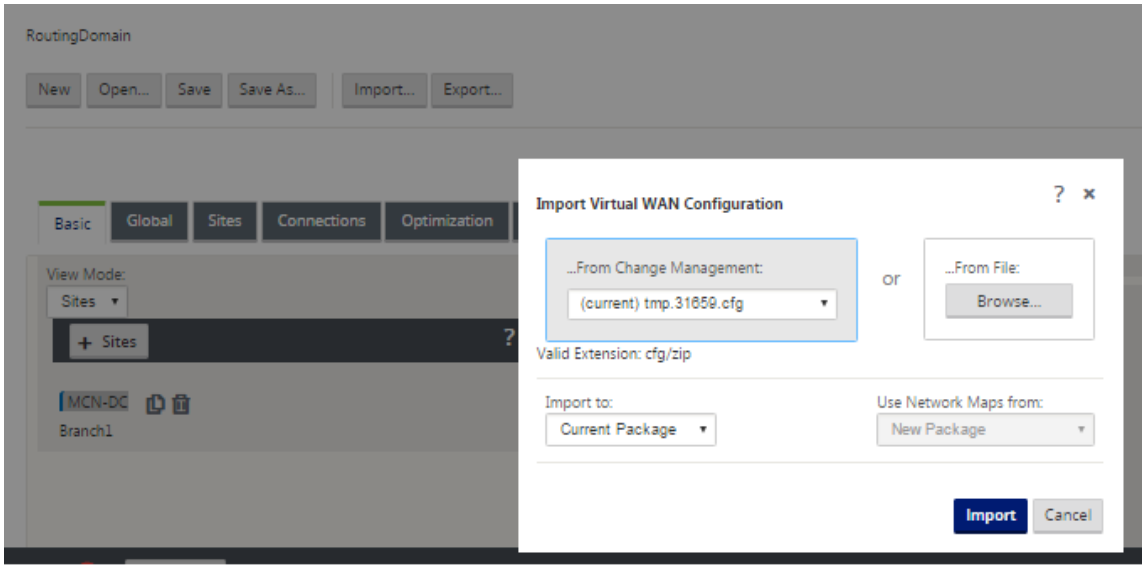
有时，您可能希望恢复到早期版本的配置包。如果您已将早期版本的副本保存到本地电脑，则可以将其导回配置编辑器中，然后将其打开进行编辑。如果这不是初始部署，您还可以从当前 MCN 上的全局更改管理收件箱中导入现有的配置包。下文提供了这两种程序的说明。

要导入配置包，请执行以下操作：

1. 打开 配置编辑器。

2. 在 配置编辑器 菜单栏中，单击 导入。

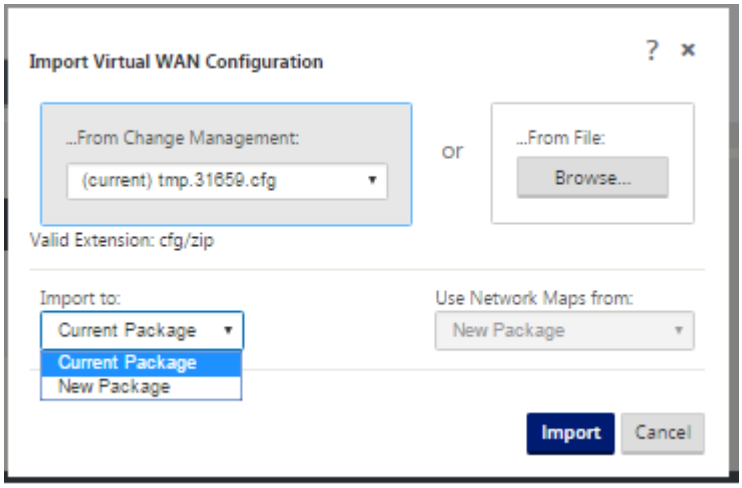
   此时将显示 导入虚拟 **WAN** 配置 对话框。



3. 选择要从中导入包的位置。

   - 从更改管理导入配置包：从更改管 理 下拉菜单（左上角）中选择该包。
   - 要从本地电脑导入配置包：单击 浏览 以在本地电脑上打开文件浏览器。选择文件并单击 确定。

4. 选择导入目的地（如果适用）。如果配置编辑器中已经打开了配置包，则导入到**:** 下拉菜单将可用。



选择以下选项之一：

当前包—选择此选项可将当前打开的配置包的内容替换为导入的包的内容，并保留打开的包的名称。但是，当前软件包的保存版本的内容不会被覆盖，直到您显式保存已更改的软件包。如果使用 另存为保 存软件包，请选择允许覆盖 以启用覆盖以前版本的覆盖。

- 新建包—选择此选项可打开一个新的空白配置包，并使用导入的包的内容填充它。新软件包自动使用与导入的软件包相同的名称。

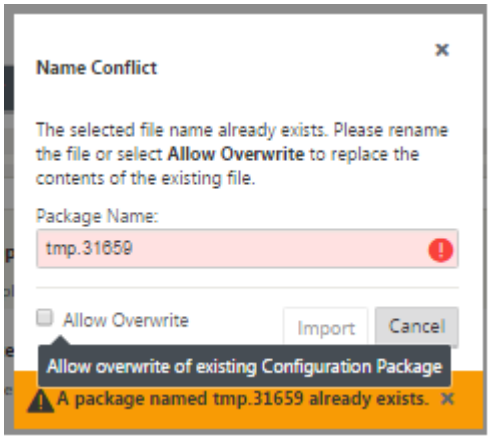
5. 指定要包含的网络映射（如果适用）。如果配置 编辑器中已打开配置包，则 使用网络映射发件人**:** 下拉菜单可用。

选择以下选项之一：

- 当前包—这将保留当前在配置编辑器中可用的包中配置的网络映射，并丢弃导入包中的所有网络映射。
- 新建包—这将使用导入包中的网络映射（如果有）替换当前打开的包中当前配置的网络映射。
- 两个 软件 包—这包括来自当前和导入的软件包的所有网络映射。

6. 单击导入。导入的文件将根据您的规格加载到 配置编辑器中。

> 注意
>
> 如果 Workspace 作区中存在同名的包，则会显示 名称冲突 对话框。



要指定要用于导入的软件包的名称，请执行以下操作之一：

- 在 包名称 字段中键入其他名称 以重命名新包并启用 导 入 按钮。导入的软件包将使用指定名称加载到 配置编辑器 中。包名称现在保存到您的 Workspace，但包内容会保存到您的工作区，直到您显式保存包。
- 选择 允许覆盖 以确认您要保留现有名称并启用覆盖已保存包的内容。但是，当前软件包的保存版本的内容不会被覆盖，直到您显式保存已更改的软件包。

这也会启用 名称冲突 对话框中的 导入 按钮。单击 导入 以完成导入操作。

加载已保存的配置包

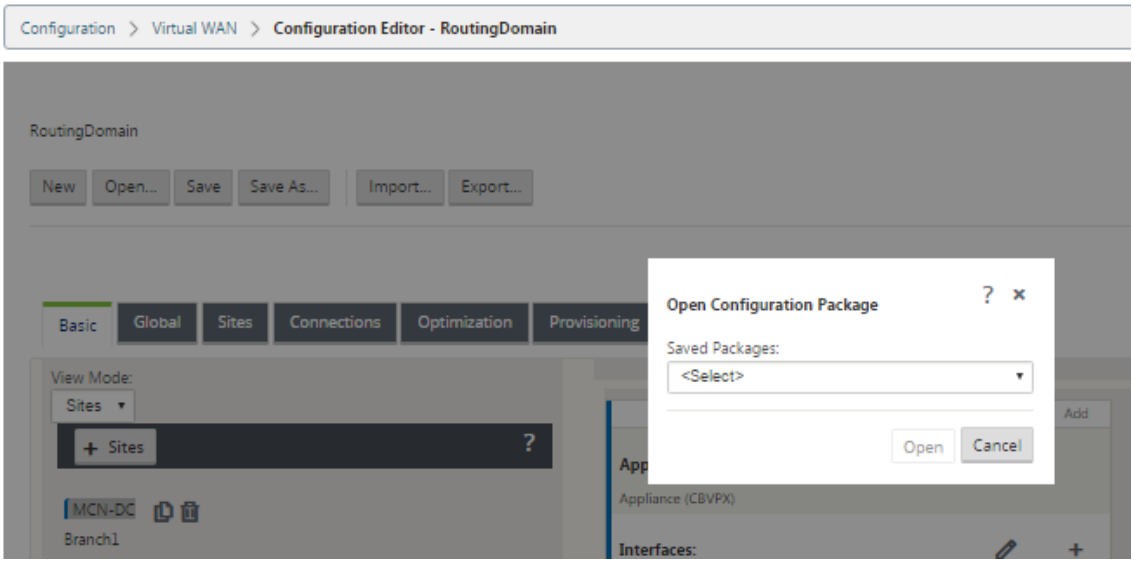
要恢复对已保存的配置包的工作，必须先打开该包并将其加载到 配置编辑器中。

要加载已保存的配置包，请执行以下操作：

1. 重新登录管理 Web 界面，然后导航到 配置编辑器。这将打开新会话的 配置编辑器 主页。

   如果您已重新登录管理 Web 界面，则 配置编辑器 最初会打开新会话，但未加载任何配置包。您可以启动新配置（新建）、打开现有保存的配置（打开）或导入（导入），然后打 开（打开）先前备份到本地 PC 的配置。

2. 单击打开。此时将显示 打开配置包 对话框。



3. 从 保存的软件包下拉菜单中选择要打开的软件包。

> 注意
>
> 如果您打开了 配置编辑器，则可能需要几秒钟或一两分钟才能填充 保存的包 菜单，具体取决于您保存到 Workspace 的配置数量。如果是这样，在此期间，保存的包 菜单字段可能会显示消息 无保存的包。如果出现这种情况，请单击 取消 以关闭该对话框，等待片刻，然后再次单击 打开 以重新打开该对话框。

4. 单击打开。

> 注意
>
> 此操作将打开指定的配置包并将其加载到 配置编辑器 中以进行编辑。这不会将所选配置转储或激活到本地设备。

重命名站点

如果在配置编辑器中更改 MCN 站点的名称，则必须将重命名站点的配置应用到 MCN 和 SD-WAN 网络。根据 MCN 角色以及是否启用或禁用高可用性，以下方案适用于重命名站点时 SD-WAN 网络配置。

- MCN
- 具有高可用性的 MCN
- GEO
- 具有高可用性的 GEO
- RCN
- 具有高可用性的 RCN

重命名 **MCN** 站点

重命名 MCN 后，您必须使用重命名的站点加载新配置。

要为重命名站点上载新配置，请执行以下操作：

1. 从 MCN, 舞台网络与新配置.
2. 下载重命名的 MCN 的分段配置包。
3. 导航到 MCN 的 本地更改管理 页面。
   a) 上载之前下载的软件包。
   b) 处理完成 后，单击 下一步。
   c) 单击激活。

> 注意
>
> 步骤 3 (c) 完成后，更改管理过程会自动激活网络中设备（节点）的暂存软件。

以高可用性重命名 **MCN** 站点

重命名已启用高可用性的 MCN 后，您必须加载新配置。

1. 从 MCN, 舞台网络与新配置.
2. 下载具有新名称的活动和高可用性 MCN 设备的分段配置包。
3. 禁用备用 MCN 设备上的服务。
4. 导航到活动 MCN 的 本地更改管理 页面。
   a) 上载之前下载的软件包。
   b) 处理完成后，单击 下一步。
   c) 单击激活。
   d) 对于高可用性禁用的备用 MCN 设备，重复步骤 i、ii、iii、iv。
   e) 在备用 MCN 设备上启用服务。

> 注意
>
> 步骤 4 (c) 完成后，更改管理过程会自动激活网络中设备的暂存软件。

重命名 **GEO** 站点

要为已重命名的 GEO 站点上载新配置，请执行以下操作：

1. 从 MCN，具有包含已重命名的 GEO 站点的新配置的阶段网络。
2. 从 MCN 中，下载重命名的 GEO 站点的临时配置包。
3. 在 **MCN** 上，选择为网络激活暂存。这将停用重命名的站点，并且该站点将变为不可用。
4. 导航到 GEO 站点上的 本地更改管理 页面。

a) 上载之前下载的软件包。

b) 完成处理程序包时，单击 下一步。

c) 单击激活。

以高可用性重命名 **GEO** 站点

要上载已重命名的 GEO 站点且具有高可用性的新配置，请执行以下操作：

1. 从 MCN，具有包含已重命名的 GEO 站点的新配置的阶段网络。
2. 从 MCN 中，为具有重命名的 GEO 站点的活动和高可用性设备下载临时配置包。
3. 在 **MCN** 上，选择为网络激活暂存。这将禁用重命名的站点，并且站点变得不可用。
4. 导航到活动的 GEO 设备。

   a) 转到本地更改管理页面。
   b) 上载之前下载的软件包。
   c) 完成处理程序包时，单击 下一步。
   d) 单击激活。
   e) 对备用设备重复步骤 a、b、c 和 d。

重命名 **RCN** 网站

要使用重命名的 RCN 站点上载新配置，请执行以下操作：

1. 从 MCN，具有包含已重命名的 RCN 站点的新配置的阶段网络。
2. 从 MCN，下载重命名的 RCN 站点的临时包。
3. 在 **MCN** 上，选择为网络激活暂存。这将禁用重命名的 RCN 站点，并且区域站点在 MCN 上变得不可用。RCN 站点和区域中的分支机构相互通信，但在步骤 4 完成之前，区域无法与 MCN 通信（除非有未重命名的 GEO RCN）。
4. 导航至 RCN 的本地更改管理页面：

   a) 上载之前下载的软件包。
   b) 包处理完成后，单击 下一步。
   c) 单击激活。

> 注意
>
> 区域中的分支需要一段时间才可用，因为区域暂存在直到步骤 4 (c) 完成后才会发生。RCN 的变更管理流程管理区域分段。

以高可用性重命名 **RCN** 站点

上载启用了重命名 RCN 站点且具有高可用性的新配置。

1. 从 MCN，具有包含已重命名的 RCN 站点的新配置的阶段网络。
2. 从 MCN 下载具有重命名 RCN 站点的活动和高可用性设备的临时包。这将禁用重命名的 RCN 站点，并且区域站点在 MCN 上变得不可用。RCN 站点和区域中的分支机构相互通信，但在步骤 4 完成之前，区域无法与 MCN 通信（除非有未重命名的 GEO RCN）。
3. 在 **MCN** 上，选择 为网络激活暂存。
4. 禁用备用 RCN 设备上的服务。
5. 导航到活动 RCN 的 本地更改管理 页面：
   a) 上载之前下载的软件包。
   b) 完成处理程序包时，单击 下一步。
   c) 单击激活。
   d) 对已禁用的备用 RCN 设备重复步骤 a、b 和 c。
6. 在备用 RCN 设备上启用服务。

重命名 **GEO RCN** 网站

要使用已重命名的 GEO RCN 站点上载新配置，请执行以下操作：

1. 从 MCN, 舞台网络与重命名的 GEO RCN 站点的新配置.
2. 从 MCN，下载重命名的 GEO RCN 站点的临时包。
3. 在 **MCN** 上，选择为网络激活暂存。这将禁用重命名的站点，并且站点变得不可用。如果主 RCN 处于联机状态，则在重命名 GEO RCN 站点时，该区域将保持连接到网络。
4. 导航至 GEO RCN 的 本地更改管理 页面：
   a) 上载之前下载的软件包。
   b) 完成处理程序包时，单击 下一步。
   c) 单击激活。

以高可用性重命名 **GEO RCN** 站点

1. 从 MCN, 舞台网络与重命名的 GEO RCN 站点的新配置.
2. 从 MCN 中，为已重命名的 GEO RCN 站点下载活动和高可用性设备 的临时包。
3. 在 **MCN** 上，选择为网络激活暂存。这将禁用重命名的站点，并且站点变得不可用。如果主 RCN 处于联机状态，则在重命名 GEO RCN 站点时，该区域将保持连接到网络。

4. 导航到活动的 GEO RCN 的 本地更改管理 页面：

   a) 上载之前下载的软件包。
   b) 完成处理程序包时，单击 下一步。
   c) 单击激活。
   d) 为备用设备重复步骤 a、带 c。

设置分支节点

June 22, 2021

本章提供有关添加和配置分支站点的说明。添加分支站点的过程与创建和配置 MCN 站点非常相似。但是，某些配置步骤和设置对于分支站点确实略有不同。此外，添加初始分支站点后，对于具有相同设备型号的站点，您可以使用 克隆（重复）功能简化添加和配置这些站点的过程。

与创建 MCN 站点以设置分支站点一样，您必须在 MCN 设备上的管理 Web 界面中使用配置编辑器。仅当接口设 置为 MCN 控制台模式时，配置编辑器 才可用。

补充分支站点部署信息

除了本指南之外，还推荐使用以下 知识库支持文章：

- 虚拟 WAN PBR 模式部署步骤 (CTX201577)

  http://support.citrix.com/article/CTX201577

- 虚拟 WAN 网关模式部署步骤 (CTX201576)

  http://support.citrix.com/article/CTX201576

分支站点配置过程概述

完成此过程的步骤如下：

1. 添加分支站点。
2. 为分支站点配置虚拟接口组。
3. 配置分支站点的虚拟 IP 地址。
4. （可选）为分支站点配置 LAN GRE 隧道。
5. 配置分支站点的 WAN 链接。
6. 配置分支站点的路由。

7. （可选）为分支站点配置高可用性。
8. （可选）克隆新分支站点以创建和配置其他站点。

> 注意
>
> 克隆站点是可选的。对于原始站点和克隆站点，Virtual WAN 设备模型必须相同。您无法更改克隆的指定设备型号。如果站点的设备型号不同，则必须手动添加站点。

9. 解决任何配置审核警报。
10. 保存完成的配置。

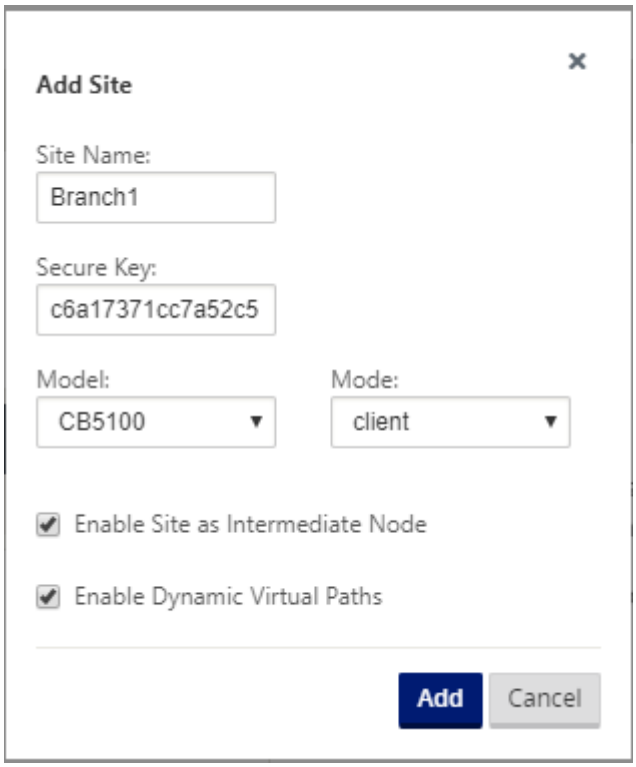
配置分支节点

June 22, 2021

要将新分支站点添加到站点表并开始配置站点，请执行以下操作：

> 注意
>
> 如果您在创建和保存新配置包后退出 MCN，则需要重新登录并重新打开配置，然后才能继续。为此，请单击配置编辑器菜单栏（页面顶部区域）中的打开。这将显示一个用于选择要更改的配置的对话框。

1. 继续在配置编辑器中，单击站点栏中的添加以开始添加和配置新的分支站点。此时将显示添加站点对话框。

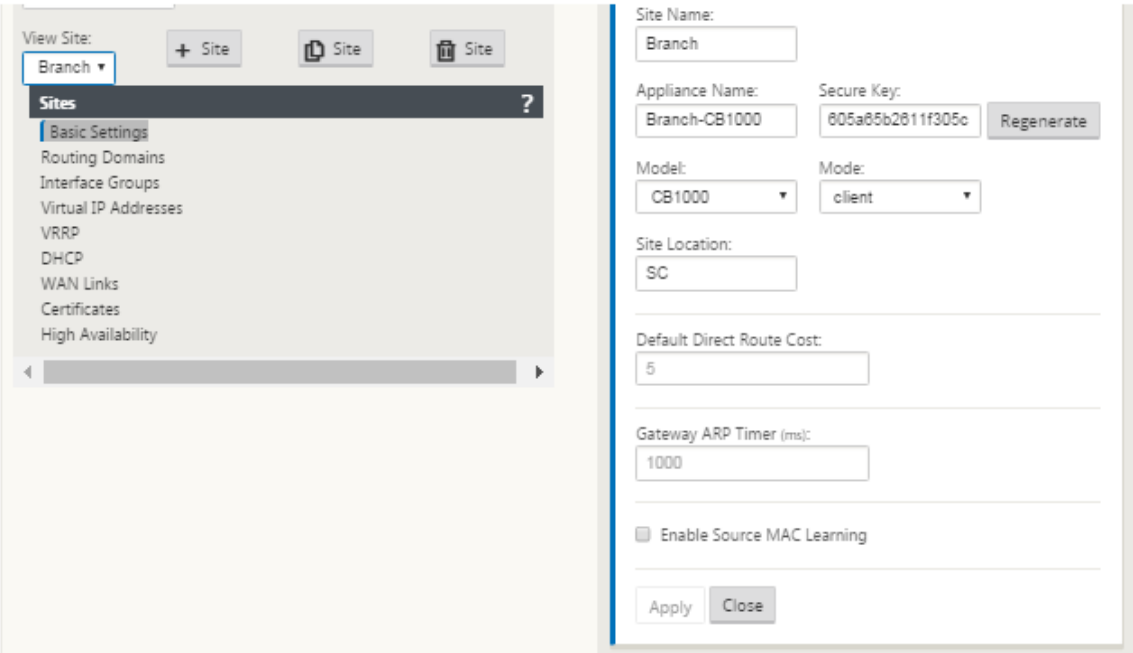


2. 键入以下站点信息。

> 注意
>
> 条目不能包含空格，且必须采用 Linux 格式。

- 站点名称—键入站点的名称。
- 设备名称—键入要分配给设备的名称。
- 安全密钥—这是一个 8-32 位的十六进制密钥，用于 SD-WAN 设备中的加密和成员身份验证。默认情况下，此字段预填充自动生成的安全密钥。接受默认值或键入自定义键入十六进制格式。
- 型号—从下拉菜单中选择设备型号。
- 模式—选择客户端作为模式。

3. 单击 添加 以添加网站。新站点将添加到站点树中，并打开站点的基本设置配置窗体。



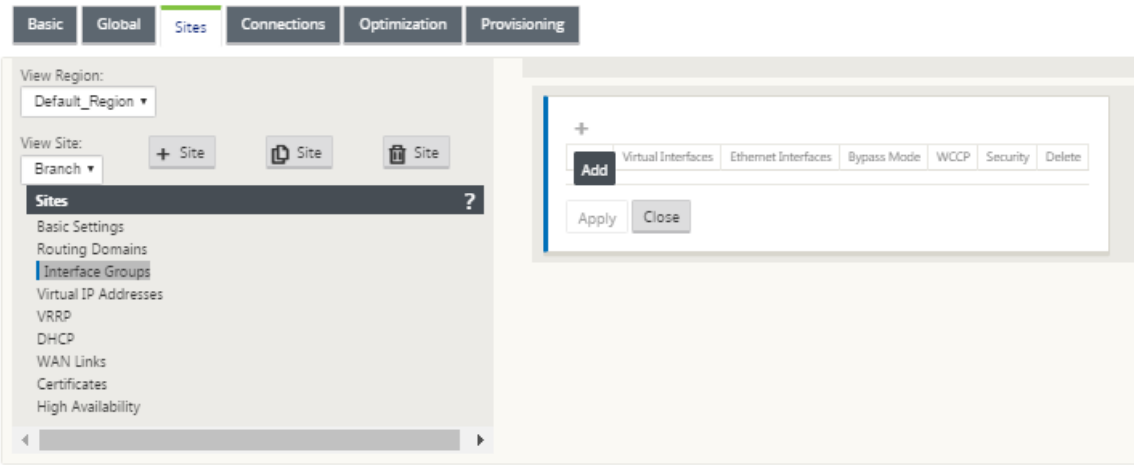
4. 键入网站的基本设置，然后单击应用。

   下一步是为新分支站点添加和配置接口组。

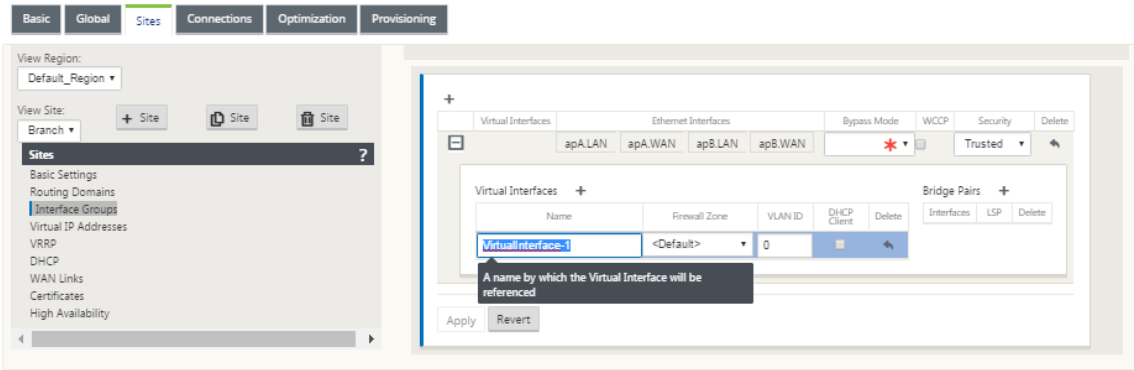
如何为分支配置接口组

要将接口组添加到新的分支站点，请执行以下操作：

1. 继续在 配置编辑器 的“站 点”视图中，从“站点”下拉菜单中选择分支 站 点。这将打开所选站点的配置视图。



2. 单击 **+** 以添加虚拟接口组。将向表中添加一个新的空白虚拟 接口组条目并打开以供编辑。
3. 单击虚拟接口右侧的 **+**。将向表中添加一个新的空白组条目并打开以进行编辑。



4. 选择要包含在组中的以太网接口。

   在以太网接口下，单击一个接口以包含/排除该接口。您可以选择要包含在组中的任意数量的接口。

5. 从下拉菜单中选择旁路模式（无默认值）。

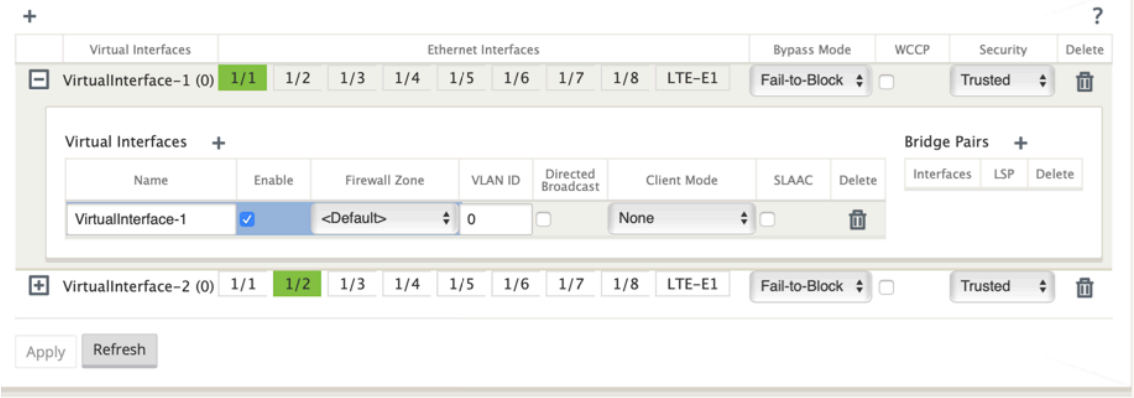
   旁路模式 指定在设备或服务发生故障或重新启动时虚拟接口组中桥接配对接口的行为。选项包括：**Fail-to-Wire** 或 **Fail-to-Block**。

6. 从下拉菜单中选择 安全级别。

   这指定了虚拟接口组的网络段的安全级别。选项包括：可信或不可信。受信任的区段受防火墙保护（默认为 受信

任)。

7. 单击您添加的虚拟接口左边缘的 **+**。这将显示 虚拟接口 表。



8. 单击虚拟接口右侧的 **+**。此时将显示 名称、防火墙区域 和 **VLAN ID ID** 。
9. 键入此虚拟接口组的 名称 和 **VLAN ID**。
   - **Name** —引用此虚拟接口的名称。
   - 启用 -默认情况下，所有虚拟接口都选中 启 用复选框。如果要禁用虚拟接口，请清除 启 用复选框。

     > 注意
     >
     > – 仅当 WAN 链接访问接口未使用虚拟接口时，禁用虚拟接口的选项才可用。如果 WAN 链路访问接口使用虚拟接口，则默认情况下该复选框处于只读状态并选中。
     > – 在配置其他功能以及已启用的虚拟接口时，禁用的虚拟接口也会列出，但 **WAN** 链接的访问接口下除外。即使选择禁用的虚拟接口，也不考虑虚拟接口，也不会影响网络配置。

   - 防火墙区域 -从下拉菜单中选择防火墙区域。
   - **VLAN ID** —用于识别和标记进出虚拟接口的流量的 ID。对原生/未标记的流量使用 0（零）的 ID。
10. 单击 桥对 右侧的 **+**。将添加一个新的 桥接对 条目并打开以进行编辑。
11. 从下拉菜单中选择要配对的以太网接口。要添加更多对，请再次单击 桥接对 旁边的 **+**。
12. 单击应用。您的设置将应用并添加到表的新虚拟接口组中。

    > 注意
    >
    > 在此阶段，您将看到一个黄色的增量审核警报图标，位于新的虚拟接口组条目右侧。这是因为您尚未为站点配置任何虚拟 IP 地址 (VIP)。现在，您可以忽略此警报，因为当您为站点正确配置了 Virtual IP 时，它会自动解决。

13. 要添加更多虚拟接口组，请单击 接口组 分支右侧的 **+** ，然后按上述操作。

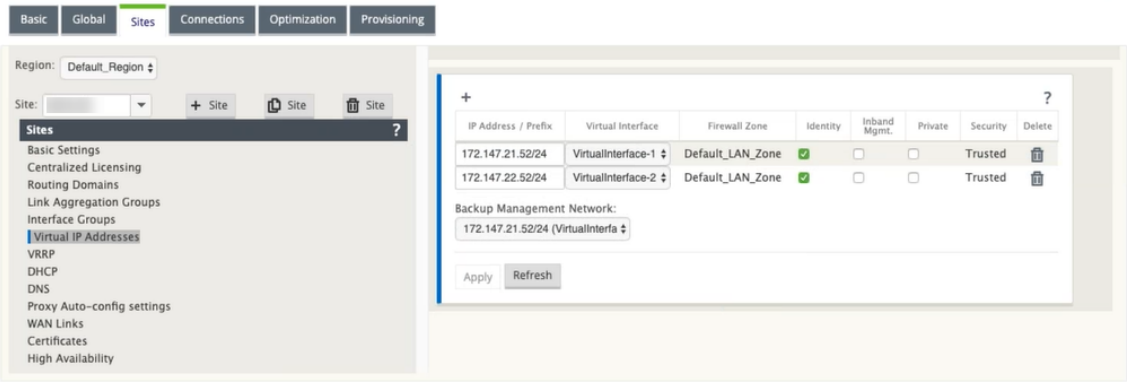
如何为分支站点配置虚拟 **IP** 地址

下一步是为站点配置虚拟 IP 地址，并将其分配给相应的组。

1. 继续在新分支站点的站 点 视图中，单击 虚拟 **IP** 地址 左侧的 **+**。这将显示新站点的 虚拟 **IP** 地址 表。
2. 单击 虚拟 **IP** 地址 右侧的 **+** 以 添加地址。此时将显示用于添加和配置新虚拟 IP 地址的窗体。
3. 键入 **IP** 地址 / 前缀 信息，然后选择与该地址关联的 虚拟接口。虚拟 IP 地址必须包含完整的主机地址和网络掩码。
4. 为虚拟 IP 地址选择所需的设置，例如防火墙区域、标识、私有和安全。
5. 选择 **Inband Mgmt** 可允许虚拟 IP 地址连接到管理服务，如 Web UI 和 SSH。

   > 注意：
   >
   > 接口必须为“受信任”且已启用 身份 的安全类型。

6. 选择虚拟 IP 作为 备份管理网络。如果管理端口未配置默认 Gateway，则可以使用虚拟 IP 地址进行管理。

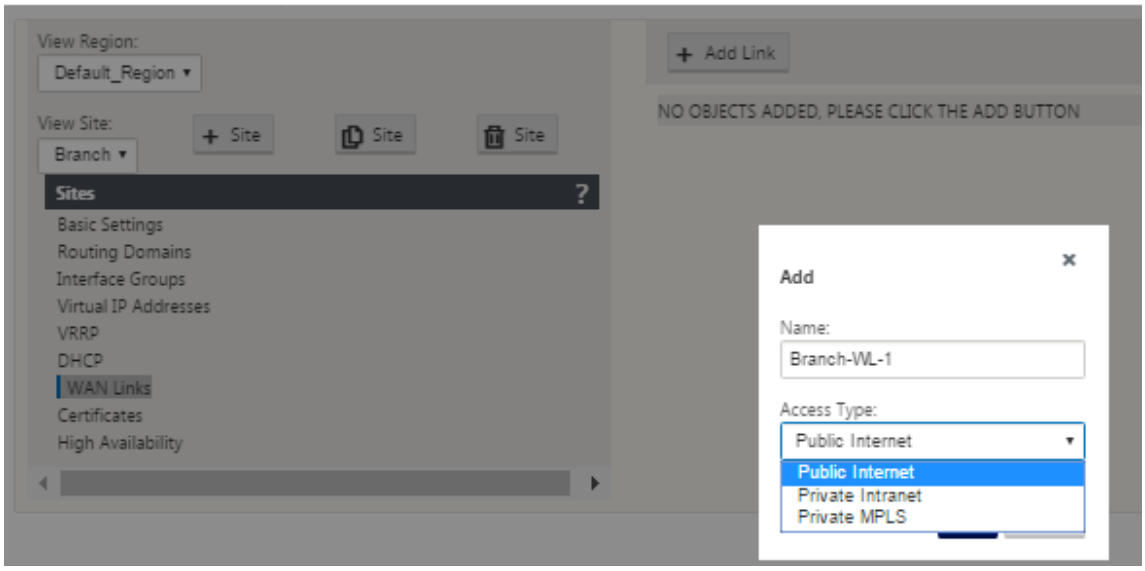


7. 单击应用。将添加到站点的地址信息，并将其包含在站点 虚拟 **IP** 地址 表中。
8. 要添加更多虚拟 IP 地址，请单击 虚拟 **IP** 地址 右侧的 **+**，然后按照上述步骤继续操作。

如何为分支配置 **WAN** 链接

下一步是为站点配置 WAN 链接。

1. 继续在新分支站点的站 点 视图中，单击 **WAN** 链接 标签。
2. 单击 **WAN** 链接右侧的添加链 接以添加新的 WAN 链接。此时将显示 添加 对话框。



3. （可选）如果您不想使用默认值，请键入 WAN 链接的名称。

   默认值为站点名称，附有以下后缀：

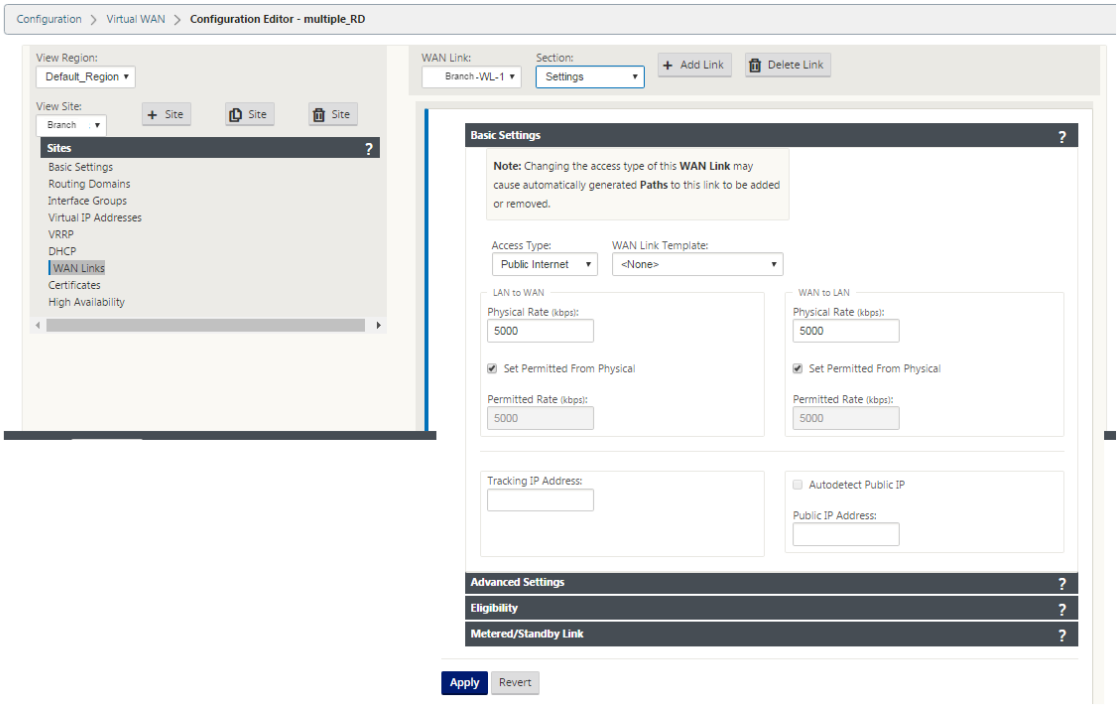
   -WL-<number>

   其中 <number> 为此站点的 WAN 链接的数量，增量为 1。

4. 从下拉菜单中选择 访问类型。

   这些选项是 公共 **Internet**、专用 **Intranet** 或 专 用多协议标签交换。

5. 单击添加。此时将显示 **WAN** 链 接基本设置配置页面，并将新的未配置 WAN 链接添加到该页面。

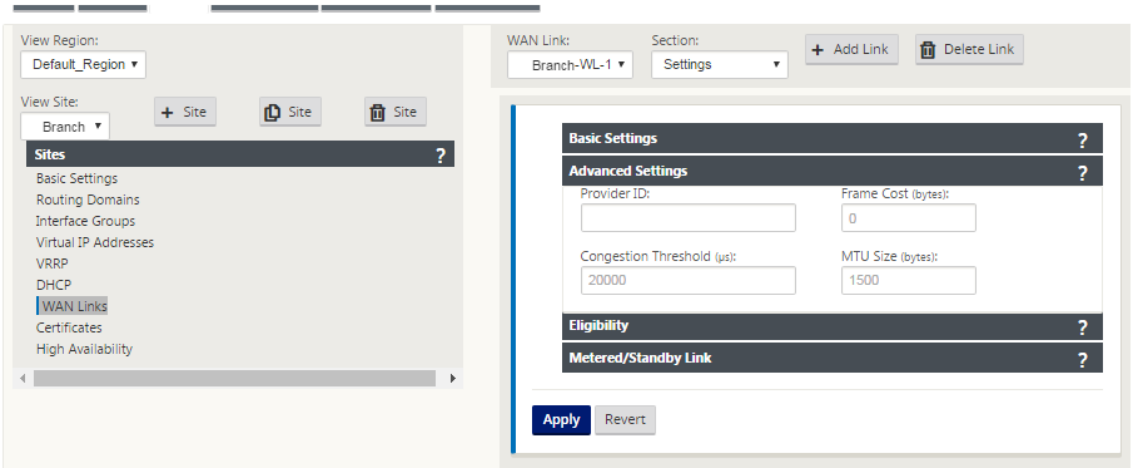


6. 键入新 WAN 链接的链接详细信息。将局域网配置为 WAN，WAN 配置为 局域网 设置。

   一些准则如下：

   - 有些互联网链接可能是不对称的。错误配置允许的速度可能会对该链接的性能产生不利影响。
   - 避免使用超过承诺率的突发速度。
   - 对于 Internet WAN 链接，请务必添加公有 IP 地址。

7. 单击灰色的 高级设置 部分栏。这将打开链接的 高级设置 窗体。

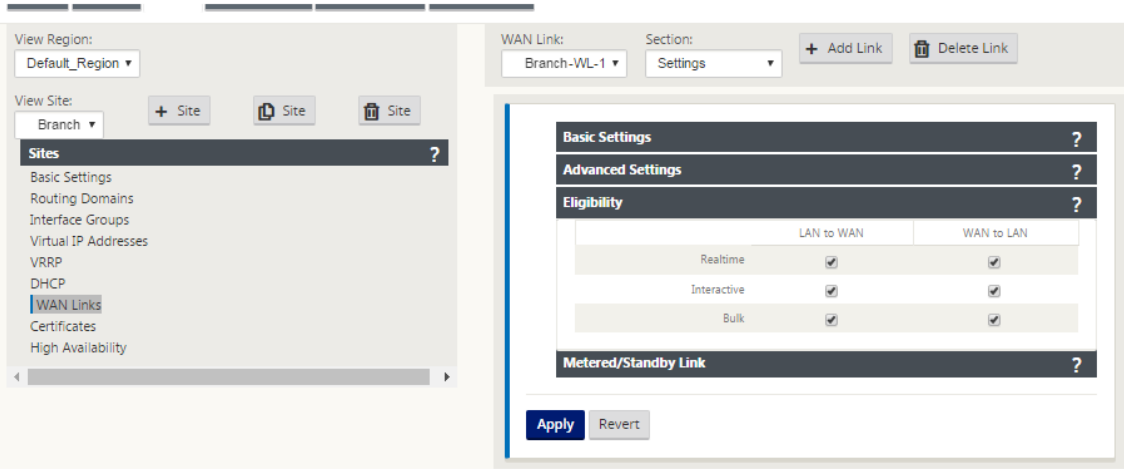


8. 键入链接的 高级设置。

   - 提供程序 **ID** —（可选）键入唯一 ID 号 1-100 以指定连接到同一服务提供程序的 WAN 链接。在发送重复数据包时，虚拟 WAN 使用提供程序 ID 区分路径。
   - 帧成本（字节）—键入添加到每个数据包的头/拖车的大小（以字节为单位）。例如，添加以太网 IPG 或 AAL5 拖车的大小（以字节为单位）。
   - 拥塞阈值—键入拥塞阈值（以微秒为单位），之后 WAN 链路限制数据包传输，以避免进一步拥塞。
   - **MTU** 大小（字节）—键入最大的原始数据包大小（以字节为单位），不包括帧成本。

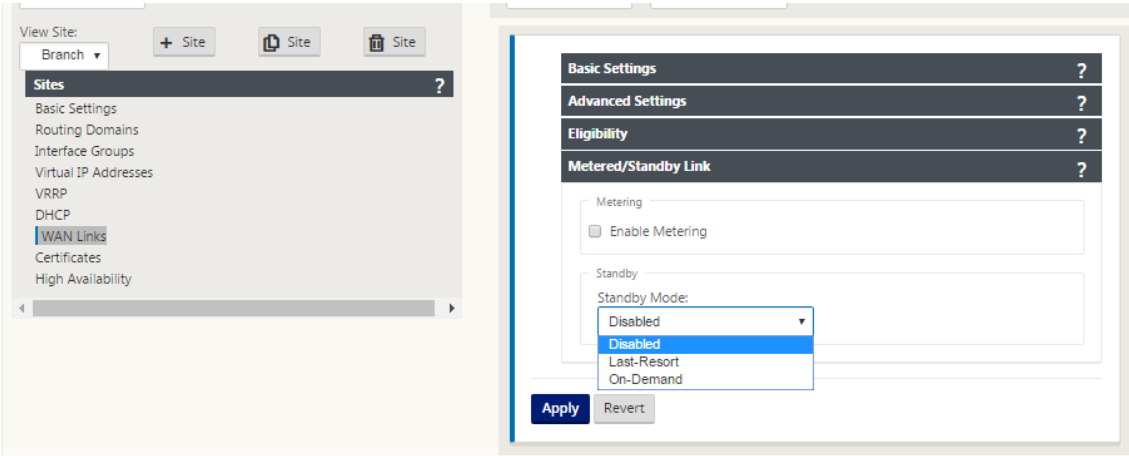
9. 单击灰色 资格 部分栏。这将打开链接的 资格 设置窗体。

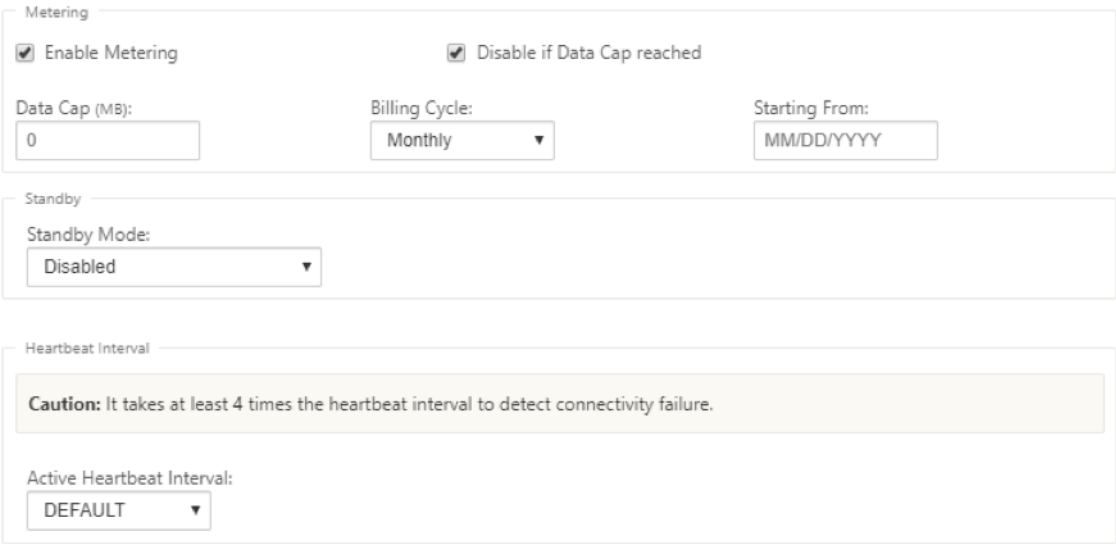
10. 选择链接的 资格 设置。



11. 单击灰色 计量链接 部分栏。这将打开链接的 按计费链接 设置 窗体。

12. （可选）选择 启用计量 以为此链接启用计量。这将显示 启用计量 设置 字段。





13. 配置链接的计量设置。键入以下命令：

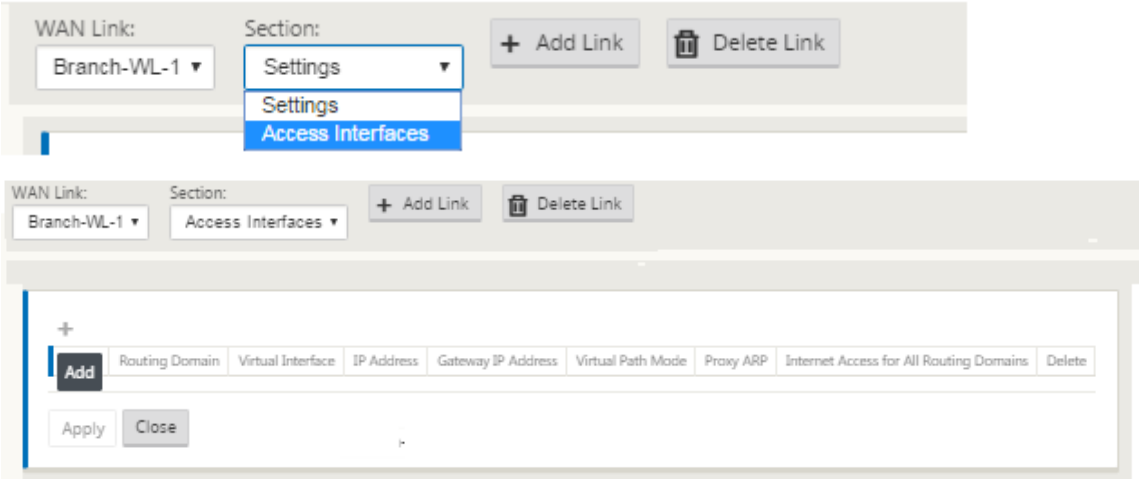
    - 数据上限 **(MB)** —键入链接的数据上限分配（以 MB 为单位）。
    - 账单周期—从下拉菜单中选择每月或每周。
    - 开始 -键入计费周期的开始日期。
    - 设置最后手段—选择此选项可在所有其他可用链接失败时启用此链接作为最后手段的链接。在正常 WAN 条件下，Virtual WAN 仅通过计费链接发送最小流量，用于检查链接状态。但是，如果发生故障，SD-WAN 可以使用活动按计费链接作为转发生产流量的最后手段。

14. 单击应用。这会将您指定的设置应用到新的 WAN 链接。

    下一步是为新的 WAN 链接配置访问接口。访问接口由虚拟接口、WAN 端点 IP 地址、网关 IP 地址和虚拟路径模式组成，共同定义为特定 WAN 链接的接口。每个 WAN 链接必须至少有一个访问接口。

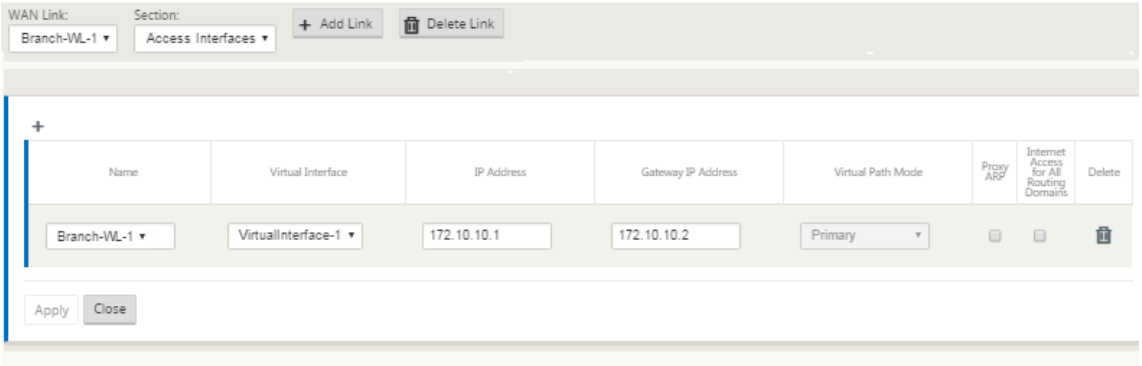
    > 注意
    >
    > 添加了一个通过考虑远程带宽自动配置共享的选项来配置 WAN 链接。使用远程带宽设 Provisioning 置配选项使拥有大型网络和不同带宽配置的用户能够以动态方式管理数据中心站点的带宽配置。

15. 在链 接的 **WAN** 链接配置页面中选择访问接口。这将打开站点的访问接口视图。



16. 单击 **+** 以添加界面。表中的空白条目将添加并打开以进行编辑。键入链 接的访问界面 设置。

    > 注意
    >
    > 每个 WAN 链接必须至少有一个访问接口。



17. 键入以下命令：

    - 名称：这是引用此访问接口的名称。键入新访问接口的名称，或接受默认值。默认设置使用以下命名约定：

      WAN_link_name-AI-number

      其中 *Wan_link_Name* 是您要与此接口关联的 WAN 链路的名称，数量是当前为此链路配置的访问接口数量，增加 1。

    > 注意
    >
    > 如果名称显示为截断，您可以将光标放在字段中，然后单击并按住鼠标向右或向左滚动以查看截断部分。

    - 虚拟接口—此访问接口使用的虚拟接口。从为此分支站点配置的虚拟接口下拉菜单中选择一个条目。
    - **IP** 地址—访问接口终结点从设备到 WAN 的 IP 地址。
    - **Gateway IP** 地址 -这是网关路由器的 IP 地址。
    - 虚拟路径模式—此 WAN 链接上虚拟路径流量的优先级。选项包括：主要、次要或排除。如果设置为 排除，则此访问接口仅用于 Internet 和 Intranet 流量。
    - 代理 **ARP** —选中要启用的复选框。如果启用，则当 Gateway 关无法访问时，虚拟 WAN 设备会回复针对网关 IP 地址的 ARP 请求。

18. 单击应用。

    您现在已完成配置新的 WAN 链接。重复这些步骤以添加和配置站点的额外 WAN 链接。

    下一步是添加和配置站点的路由。

如何为分支配置路由

要添加和配置站点的路由，请执行以下操作：

1. 单击新分支站点的 连接 视图，然后选择 路由。这将显示站点的 路径 视图。
2. 单击路径右侧的 + 以添加路径。这将打开 路由 对话框进行编辑。

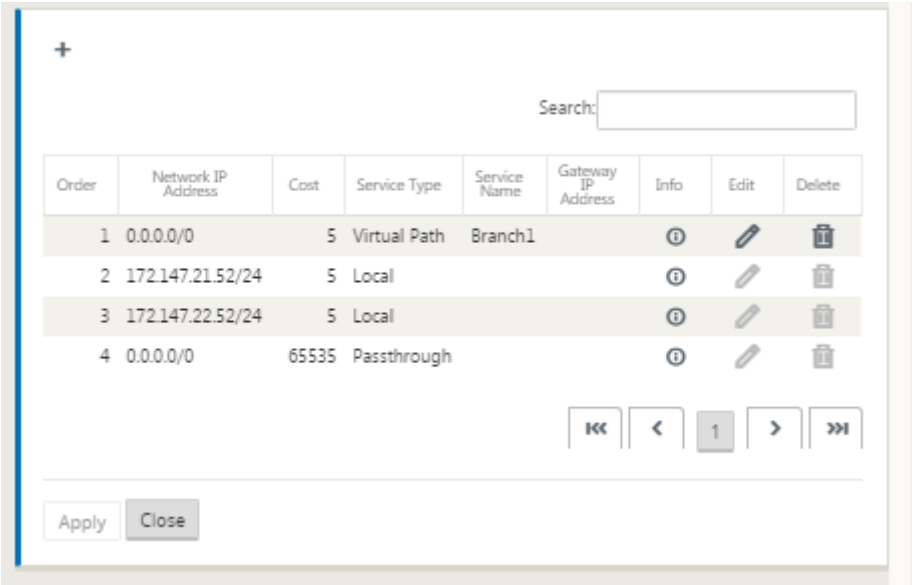
3. 键入新路径的路径配置信息。

   - 网络 **IP** 地址—键入网络 IP 地址。
   - 成本—键入 1 到 15 之间的权重，用于确定此路径的路径优先级。成本较低的路径优先于成本较高的路径。默认值为 5。
   - 服务类型—从此字段的下拉菜单中选择路径的服务类型。这些选项如下所示：
     - 虚拟路径—此服务管理跨虚拟路径的流量。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。这是通过不断测量和适应不断变化的应用需求和广域网条件来实现的。SD-WAN 设备根据每个路径测量网络。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。此类型的流量未封装。在拥堵期间，SD-WAN 通过相对于虚拟路径的速率限制互联网流量，主动管理带宽，并根据管理员建立的 SD-WAN 配置管理 Intranet 流量。
     - **Intranet** —此服务管理尚未定义为跨虚拟路径传输的企业 Intranet 流量。与互联网流量一样，它仍然是未封装的，SD-WAN 通过在拥塞期间限制此流量相对于其他服务类型的速率来管理带宽。在某些情况下，如果为虚拟路径上的 Intranet 回退配置，则通常使用虚拟路径传输的流量可以被视为 Intranet 通信，以保持网络可靠性。
     - 直通—此服务管理要通过虚拟 WAN 传递的流量。定向到直通服务的流量包括广播、ARP 和其他非 IPv4 流量，以及虚拟 WAN 设备本地子网、配置的子网或网络管理员应用的规则上的流量。SD-WAN 不会延迟、形状或更改此流量。因此，必须确保直通流量不会消耗 SD-WAN 设备配置为用于其他服务的 WAN 链接上的大量资源。
     - 本地—此服务管理不匹配其他服务的站点的本地 IP 流量。SD-WAN 忽略来源和发往本地路由的流量。

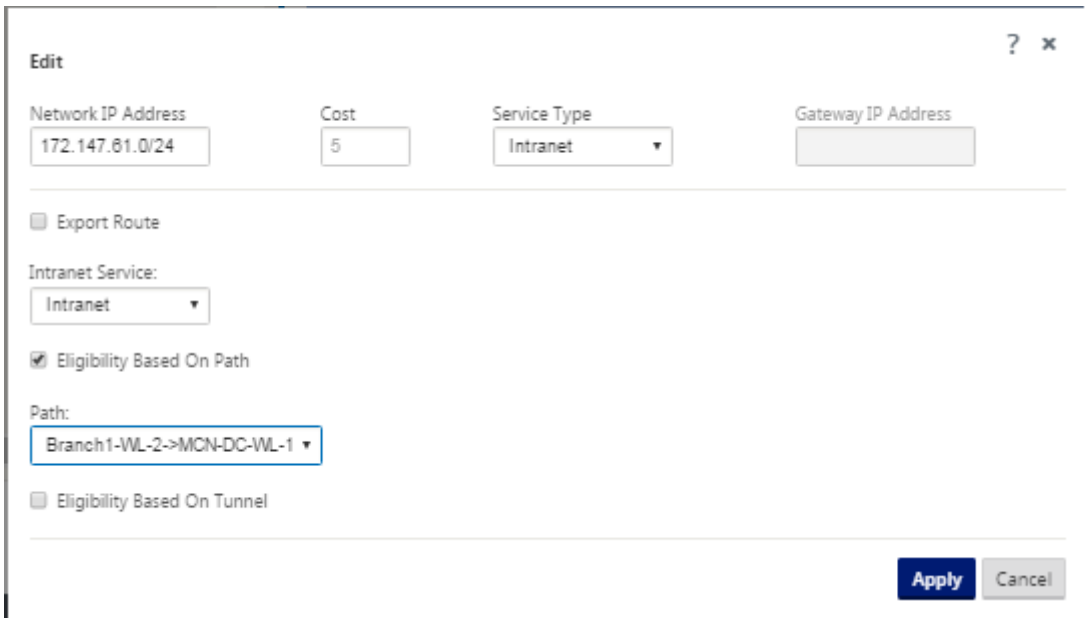
  - **GRE** 隧道—这项服务管理注定于 GRE 隧道的 IP 流量，并匹配在现场配置的局域网 GRE 隧道. GRE 隧道功能使您能够配置 SD-WAN 设备以结束局域网上的 GRE 隧道。对于具有服务类型 GRE 隧道的路由，Gateway 必须位于本地 GRE 隧道的隧道子网之一。
  - 局域网 **IPsec** 隧道—此服务管理发往 IPsec 隧道的 IP 流量。
  - 国际路由 -此服务允许站点内的路由域之间或不同站点之间的路由泄漏。这样就不需要边缘路由器来处理路由泄漏。
- 网关 **IP** 地址—键入此路由的网关 IP 地址。
- 基于路径的资格（复选框）-（可选）如果启用，则选定路径关闭时路由不会接收流量。
- 路径—指定用于确定路径资格的路径。

4. 单击应用。

> 注意
>
> 单击 应用后，可能会显示审核警告，指示需要进一步操作。红点或金色增量图标表示它出现的部分中出现错误。您可以使用这些警告来识别错误或缺失的配置信息。将光标滚到审核警告图标上，以显示该部分中错误的简短描述。您还可以单击深灰色 审 核状态栏（页面底部）以显示所有审核警告的完整列表。



您还可以编辑配置的路由，如下所示。



您现在已完成配置客户端站点所需的步骤。在继续下一阶段部署之前，您还可以选择完成一些额外的可选步骤。下面列出了这些步骤和指向说明的链接。如果您现在不想配置这些功能，您可以直接进入准备 MCN 上的 SD-WAN 设备包。

可选步骤如下：

- 配置高可用性—高可用性是一种配置，其中一个站点上的两个虚拟 WAN 设备在主动/备用伙伴关系容量中提供服务，以实现冗余目的。如果您没有为此站点实施高可用性，则可以跳过此步骤。有关说明，请参阅为分支站点配置高可用性（高可用性）（可选）。
- 克隆新分支站点 -您可以选择克隆您配置的分支站点，并将其用作添加另一个站点的模板。原始站点和克隆的设备型号必须相同。相关说明，请参阅克隆分支站点（可选）。
- 配置 **WAN** 优化—如果 Citrix SD-WAN 虚拟 WAN 许可证包含 WAN 优化功能，则可以选择启用这些功能并将其添加到配置中。为此，您必须在 配置编辑器 中完成 优化 部分，并保存更改的配置。

保存配置

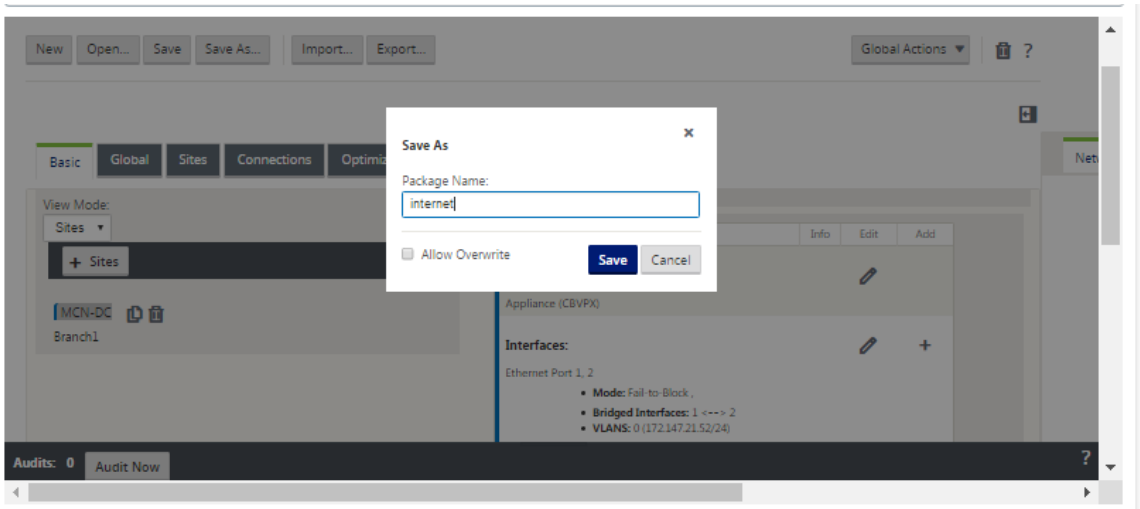
下一步是保存已完成的 站点 配置。配置将保存到本地设备上的 Workspace。

> 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。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，建议您经常或在配置的关键点保存配置包。
> 注意
>
> 作为额外的预防措施，建议您使用另存为而非保存，以避免覆盖错误的配置包。
> 保存配置文件
> 后，您可以选择退出管理 Web 界面，然后继续配置过程。但是，如果您注销，则需要在恢复时重新打开保存的配

> 置。说明在配置 **MCN** 下的部分中提供；将保存的配置包加载到配置编辑器中。

要保存当前配置包，请执行以下操作：

1. 单击 另存为（位于 配置编辑器 中间窗格顶部）。这将打开 另存为 对话框。



2. 键入配置包名称。单击保存。

> 注意
>
> 如果要将配置保存到现有配置包中，请务必在保存之前选择 允许覆盖。

下一步是配置 MCN 与客户端站点之间的虚拟路径和虚拟路径服务。说明在配置 MCN 与客户端站点之间的虚拟路径服务中提供。

重命名分支站点

重命名分支站点后，您需要将新的配置包上传到网络。

1. 从 MCN，具有包含重命名分支站点的新配置的阶段网络。
2. 下载重命名的分支站点的临时包。
3. 在 **MCN** 上，选择激活暂存网络。这将禁用重命名的站点，并且站点变得不可用。
4. 导航到分支 本地更改管理 页面。
5. 上载之前下载的软件包。单击 下一步，然后单击 激活。

以高可用性重命名分支站点

要在重命名启用高可用性的分支站点后上传新配置，请执行以下操作：

1. 从 MCN，具有包含已重命名的分支站点的新配置的阶段网络。
2. 为具有重命名分支站点的活动和高可用性设备下载临时包。
3. 在 **MCN** 上，选择为网络激活暂存。这将禁用重命名的站点，并且站点变得不可用。
4. 导航到分支处的活动设备。转到 本地变更管理 页面。
5. 上载之前下载的软件包。单击 下一步，然后单击 激活。
6. 对备用设备重复步骤 4 (a) 和 4 (b)。

克隆分支站点（可选）

June 22, 2021

本节提供了克隆新分支站点的说明，以便用作添加更多分支站点的部分模板。

> 注意
>
> 克隆站点是可选的。对于原始站点和克隆站点，Virtual WAN 设备模型必须相同。您无法更改克隆的指定设备型号。如果站点的设备型号不同，则必须按照前面部分中的说明手动添加站点。

克隆站点简化了添加和配置更多分支节点的过程。克隆站点时，将复制站点的整个配置设置集并显示在单个窗体页面中。然后，您可以根据新站点的要求修改设置。可以保留某些原始设置（如果适用）。但是，大多数设置对于每个站点都必须是唯一的。

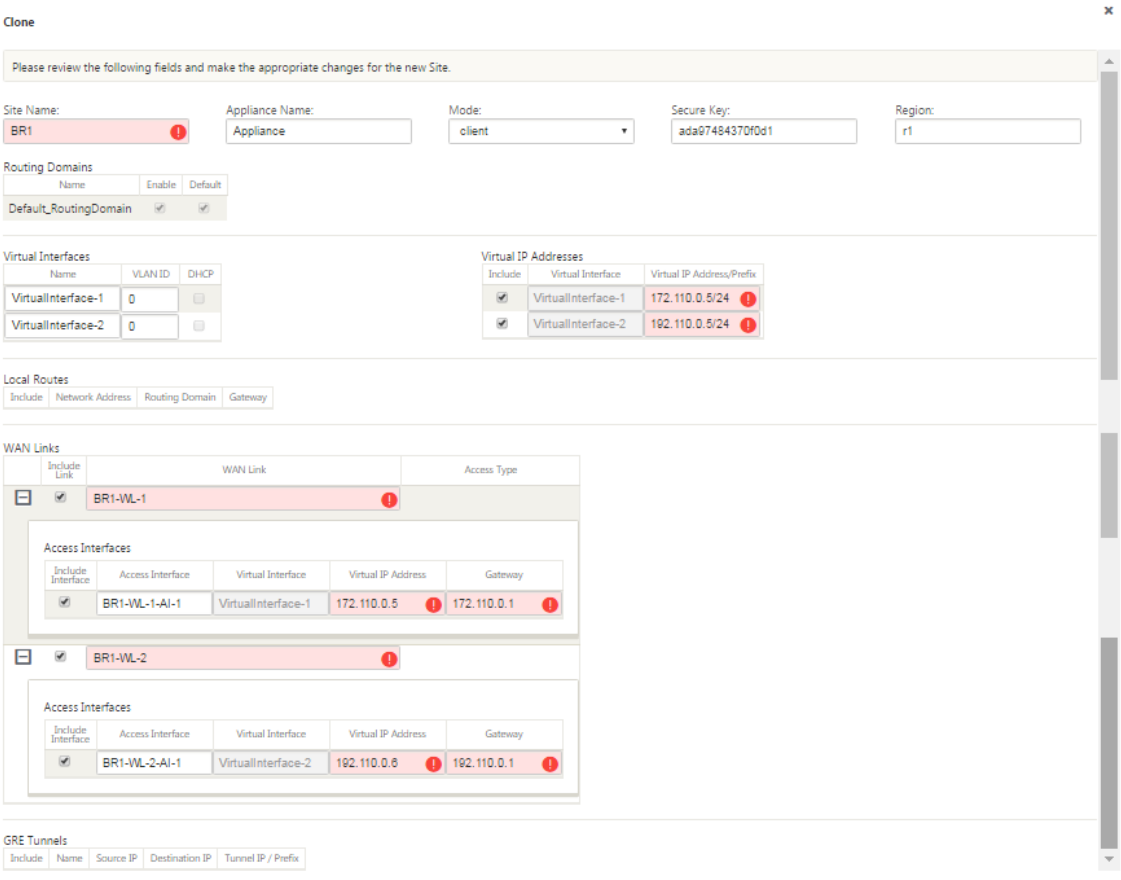
要克隆站点，请执行以下操作：

1. 在配置编辑器的站点树（中间窗格）中，单击要复制的分支站点。

   这将在站点树中打开该站点分支，并显示克隆按钮（双页图标）和“删除”按钮（垃圾桶图标）。

2. 单击树中分支站点名称右侧的克隆图标。

   这将打开克隆站点配置页。



3. 输入新站点的配置参数设置。

   带有审核警报图标（红点）的粉红色字段表示必需的参数设置，该设置的值必须与原始克隆站点的设置不同。通常，此值必须是唯一的。

   > 提示
   >
   > 要进一步简化克隆过程，请在命名克隆时使用一致的预定义命名约定。

4. 解决任何审计提醒。

   要诊断错误，请将光标滚动到 审核警报 图标（红点或金色增量）上，以显示该特定警报的气泡帮助。

5. 单击 克隆（最右角）创建站 点 并将其添加到 站点 表中。

   > 注意
   >
   > 在您输入所有必需值之前，克隆 按钮将保持不可用，并且新站点配置无错误。

6. （可选。）保存对配置的更改。

   > 注意

> 作为额外的预防措施，建议您使用另存为（而不是保存），以避免覆盖错误的配置包。请务必在保存到现有配置之前选择允许覆盖，否则您的更改不会保存。

对要添加的每个分支站点重复此步骤。

添加完所有站点后，下一步是检查审核警报的配置，并根据需要进行更正或添加。

审核分支配置

June 22, 2021

项目旁边的审核警报图标（红点或金色增量）表示该项目的配置错误或缺少参数信息。图标旁边的数字表示该警示的关联错误数。要查看特定警示的气泡帮助，请将光标滚到警示图标上。这将显示该警示标记的特定错误的简要描述。您必须解决配置中的所有审核警报，否则您将无法在稍后部署过程中验证、暂停和激活配置包。

解决所有审核警报（如果有），完成配置的 站点 阶段。下一步是保存已完成的 站点 配置。

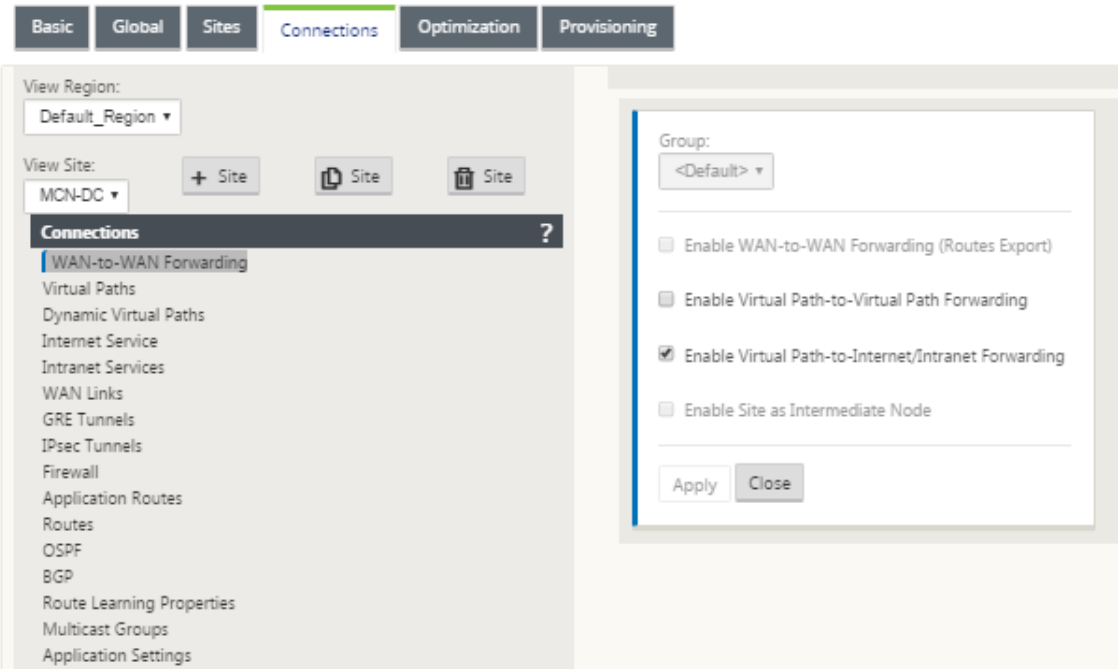
配置 **MCN** 与客户端站点之间的虚拟路径服务

June 22, 2021

下一步是在 MCN 和每个客户端（分支）站点之间配置虚拟路径服务。为此，您可以使用配置 编辑器的连接部分配置树中可用的配置窗体和设置。

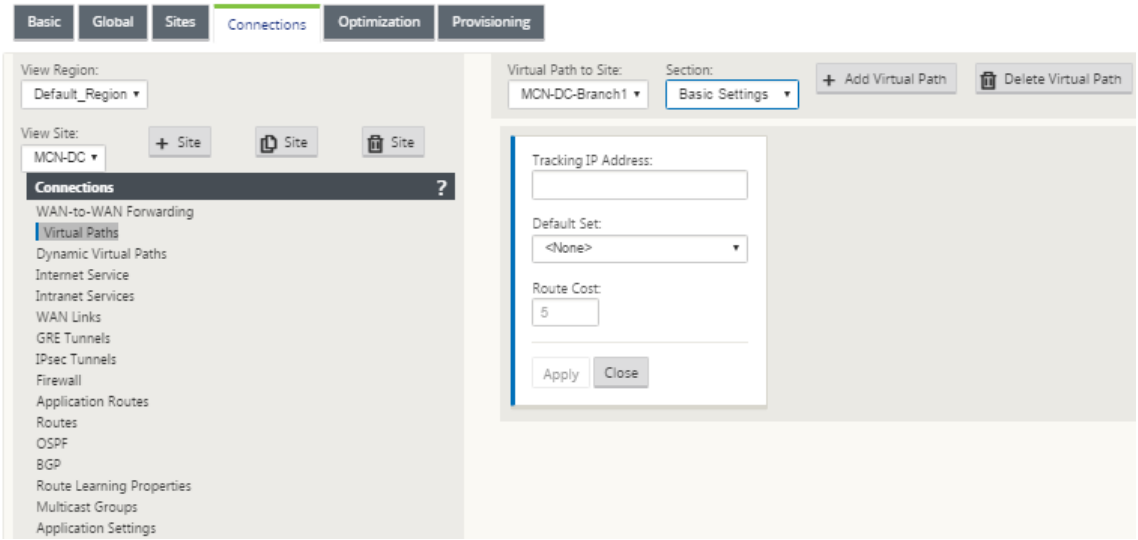
要在 MCN 与客户端站点之间配置虚拟路径服务，请执行以下操作：

1. 继续在 配置编辑器中，单击 连接选项卡。这将显示 连接 部分配置树。
2. 从 连 接 部分页面的 查看站点 下拉菜单中选择 **MCN**。这将在 连接 配置中打开 MCN 站点。

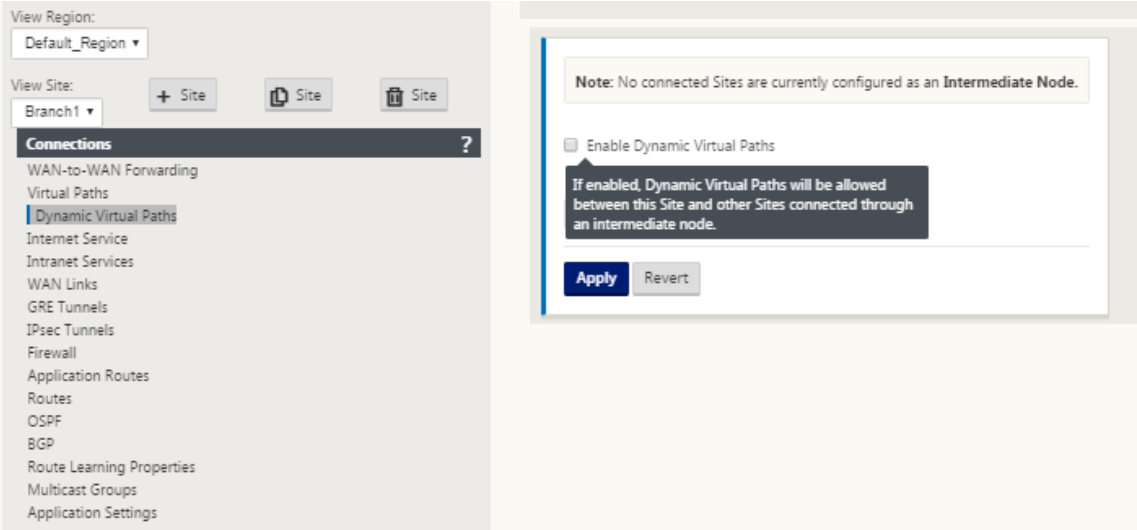


> 注意
>
> WAN 到 WAN 转发组仅在区域内受支持，而不是跨区域。您可以使用区域分离网络，而不是依赖 WAN 到 WAN 转发组。

3. 单击 虚拟路径。这将打开 MCN 站点的 虚拟路径配置 部分（子分支）。本节提供了用于在 MCN 和每个虚拟 WAN 客户端站点之间配置虚拟路径服务的设置和窗体。下图显示了 MCN 站点的示例虚拟路径部分。



下图显示了分支站点的示例 动态虚拟路径 部分。



动 态虚拟路径 部分允许配置以下内容：

- 动态 虚拟路径—（可选）此部分中的设置允许您启用和禁用动态虚拟路径，并设置站点允许的最大动态虚拟路径。动态虚拟路径是基于配置的阈值在站点之间直接建立的虚拟路径。阈值通常基于这些站点之间发生的流量。只有在达到指定阈值后，动态虚拟路径才能运行。正常操作不需要动态虚拟路径，因此配置此部分是可选的。
- **<MCN_Site_Name>**_<**Branch_Site_Name**> —系统最初会自动添加 MCN 与客户端站点之间的静态虚拟路径，因为需要此虚拟路径。路径的名称使用以下格式：

  <MCN_Site_Name>_<Branch_Site_Name>

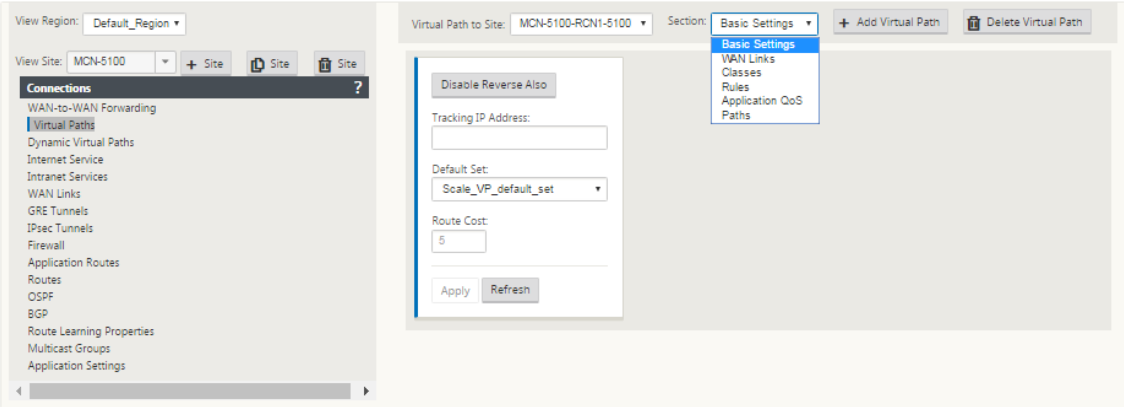
  其中，

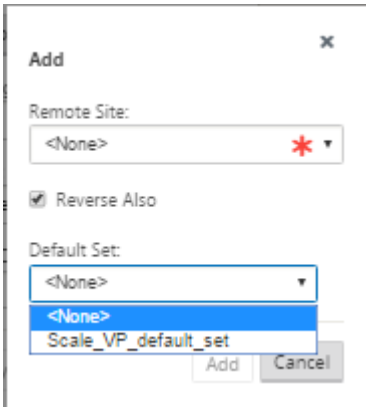
  MCN_Site_Name 是此虚拟广域网的 MCN 的名称。

  Branch_Site_Name 是当前配置包中标识的客户端站点的名称。

用户可配置的默认设置最初将应用于静态虚拟路径，如 连接 配置树的 虚拟路径 **>** 默认集 部分中定义的那样。但是，您可以自定义或添加到定义的 默认集，还可以自定义特定站点和虚拟路径的配置。

> 注意
>
> 要为站点添加更多静态虚拟路径，必须手动执行此操作。步骤中包含手动添加静态虚拟路径的说明，如下所示。



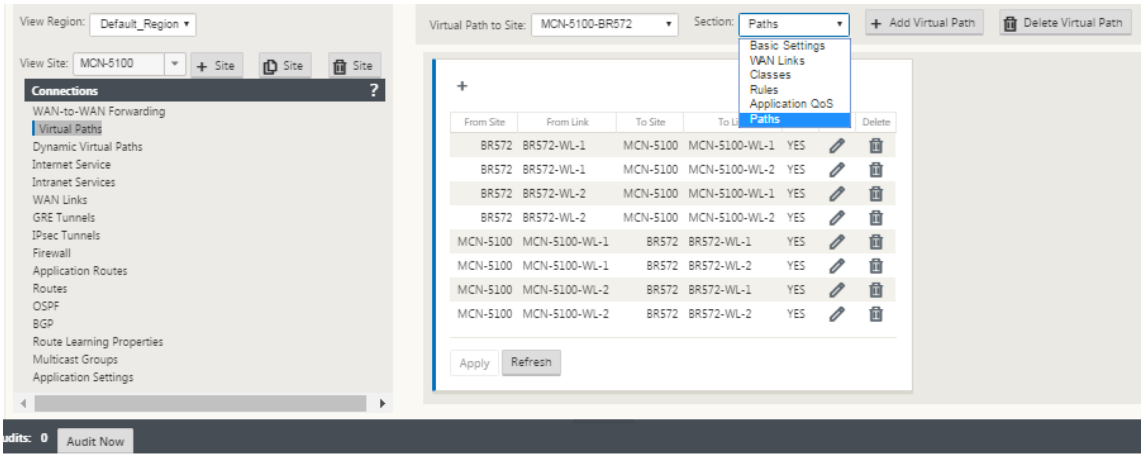


4. 单击 虚拟路径 部分中静态虚拟路径名称旁边的 **+** 添加虚拟路径。这显示了静态虚拟路径的更多配置：

   a) 远程 站 点—此部分使您能够从远程站点的角度查看和配置 虚拟路径 设置。您可以根据此特定虚拟路径的需要查看、自定义和添加 类 或 规则。您还可以根据需要将虚拟路径添加到远程站点。
   b) 反向同时- 启用后，类和规则将在两个站点上镜像虚拟路径。
   c) 默认设置 -用于填充站点上虚拟路径的规则和类的虚拟路径默认设置的名称。

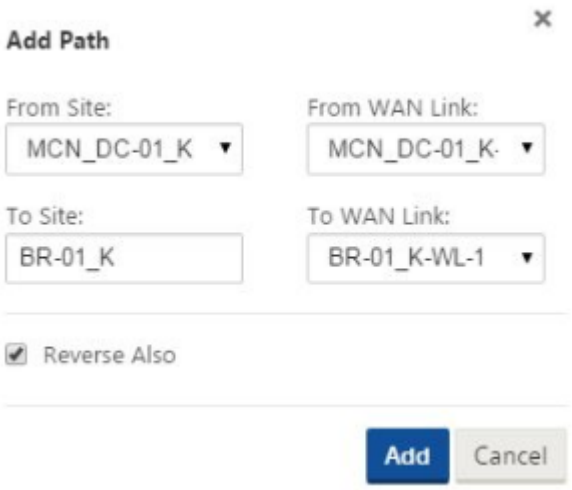
   下图显示了 MCN 静态虚拟路径分支和子分支的示例。

5. 从“节”下拉菜单中选择“路径”。



6. 单击 路径 表上方的 **+** （添加）。

   这将显示 添加路径 对话框（配置窗体）。



7. 指定新虚拟路径的源站点和目标站点信息。

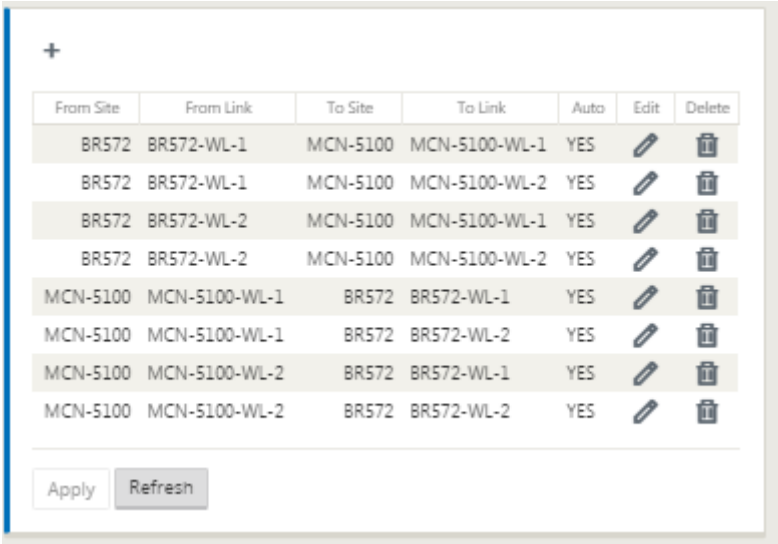
8. 从可用的下拉菜单中指定以下内容：

   > 注意
   >
   > 根据为站点配置 WAN 链接的方式，某些字段是只读的。可配置的字段提供可用选择的下拉菜单。

   - 来自站点—这是虚拟路径的源站点。对于所需的静态虚拟路径，默认情况下将其配置为 MCN 站点。
   - 从 **WAN** 链接—这是虚拟路径的源 WAN 链接。
   - 到站点—这是虚拟路径的目标站点。
   - 到 **WAN** 链接—这是虚拟路径的目标 WAN 链接。

9. 单击添加。

   这将在 连接 **>** 虚拟路径 树中将配置的虚拟路径 添加到 MCN 和关联的客户端站点。这也会自动打开虚拟 路径 的从站点（在本例中为 MCN）的路径设置配置窗体。



From Site	From Link	To Site	To Link	Auto	Edit	Delete
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-1	MCN-5100	MCN-5100-WL-2	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-1	YES		
BR572	BR572-WL-2	MCN-5100	MCN-5100-WL-2	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-1	BR572	BR572-WL-2	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-1	YES		
MCN-5100	MCN-5100-WL-2	BR572	BR572-WL-2	YES		

Apply Refresh

10. 单击 MCN-客户端虚拟路径标签右侧的编辑（铅笔图标）。这将打开虚拟路径服务配置窗体进行编辑。
11. 配置虚拟路径的设置，或接受默认设置。

    路 径 配置窗体包含以下设置：

    - 从站点 部分：
      - 站点—这是虚拟路径的源站点。对于所需的静态虚拟路径，默认情况下将其配置为 MCN 站点。
      - **WAN** 链接—这是虚拟路径的源 WAN 链接。
    - 至站点 部分：
      - 站点—这是虚拟路径的目标站点。
      - **WAN** 链接—这是虚拟路径的目标 WAN 链接。
    - 同时反向 -选中此复选框可为此虚拟路径启用反向。如果启用，系统会自动在配置路径的相反方向构建虚拟路径，使用与原始路径配置相同的 WAN 链接。
    - **IP DSCP** 标记—从下拉菜单中选择一个标记。这将指定要在 IP 标头中为通过此虚拟路径传输的流量设置的 DSCP 标记。
    - 启用加密—选中此复选框可启用对沿此虚拟路径发送的数据包的加密。
    - 不良损失敏感—从下拉菜单中选择一个设置。选项包括：
      - 启用—（默认）如果启用，路径由于丢失而被标记为 **BAD**，并且将导致路径评分损失。
      - 禁用 -当带宽损失
        不能容忍时，禁用坏损失敏感 可能很有用。
      - 自定义—选择 自定义 以指定将路径标记为 坏 所需的时间内损失百分比。选择此选项将显示以下更多设置：

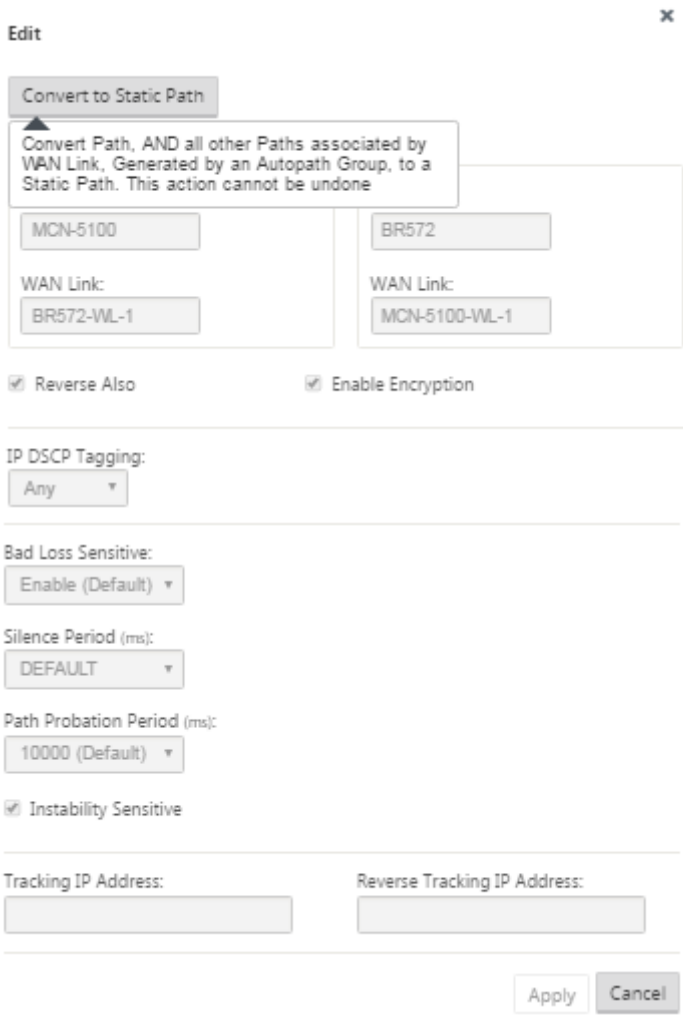
    * 损失百分比 **(%)** —指定在指定时间内测量的路径标记为 BAD 之前的损失阈值百分比。默认情况下，百分比基于最近收到的 200 个数据包。
    * 随时间变化 **(ms)** —指定测量数据包丢失的时间段（以毫秒为单位）。从该字段的下拉菜单中选择一个介于 100 到 2000 之间的选项。

  - 静默周期 **(ms)** —指定路径状态从 好 转为 坏 之前的持续时间（以毫秒为单位）。

  默认值为 150 毫秒。从此字段的下拉菜单中选择一个介于 150 到 1000 之间的选项。

  - 路径试用期 **(ms)** —指定路径从 BAD 转换到好之前的等待时间（以毫秒为单位）。从此字段的下拉菜单中选择介于 500 到 60000 之间的选项。默认值为 10,000 毫秒。
  - 不稳定敏感—选中此复选框以启用。如果启用，则路径评分算法中会考虑由于 **BAD** 路径状态和其他延迟峰值而产生的延迟惩罚。
  - 跟踪 **IP** 地址—在虚拟路径上输入可以 ping 以确定路径状态的虚拟 IP 地址。
  - 反向跟踪 **IP** 地址—如果为虚拟路径启用了 反 向，请在路径上输入可以 ping 的虚拟 IP 地址以确定反向路径的状态。

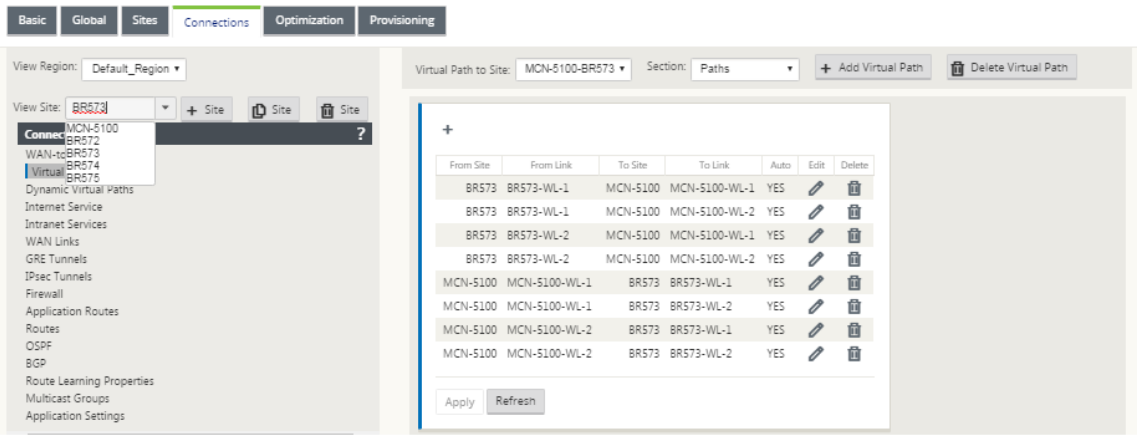
12. 单击应用。这表明 MCN 和客户端 站点之间的两个新的 从站点 和 到站点 虚拟路径已添加到 路径 表中。



13. 对要连接到 MCN 的每个分支重复上述步骤。

    接下来，您可以选择自定义客户端站点的虚拟路径配置，以及添加和配置客户端之间的更多路径。下面的其余步骤中提供了说明。

14. 从 查看站点 下拉菜单中选择客户端站点 分支。此时将打开 连 接 树中的客户端站点分支的配置。

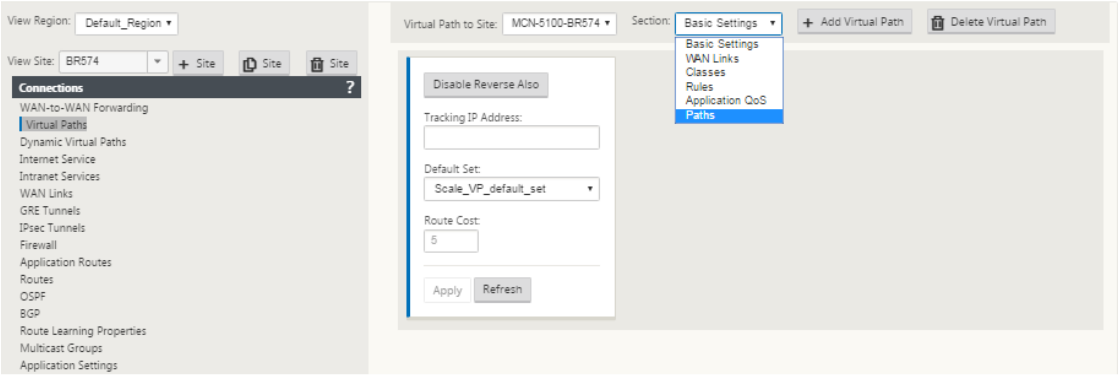


15. 导航到要配置的任何客户端站点虚拟路 径 的路径设置配置窗体。

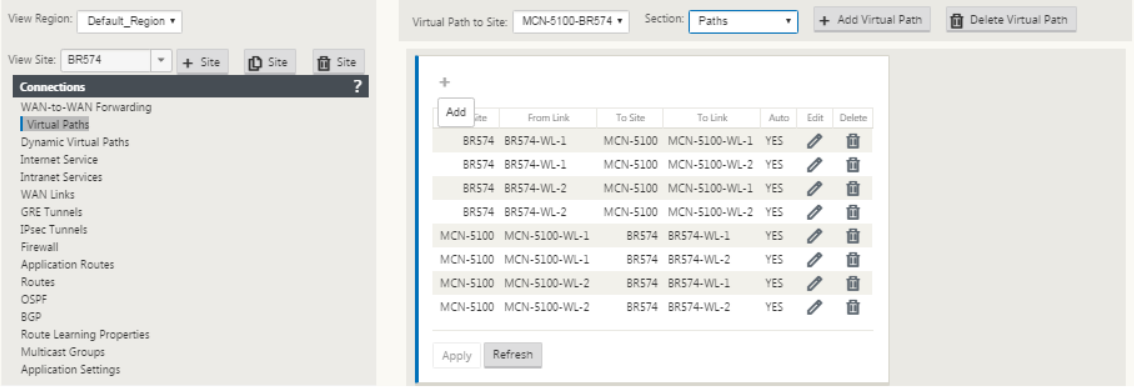
    要导航到客户端站点的 路径 设置窗体，请执行以下操作：

16. 从客户端站点的分支页面的 部 分选项卡中选择 路径。

    下图显示了前面步骤中添加的新 从站点 路 径的示例路径 设置窗体。



17. 为要自定义的每个路径配置设置。按照与配置 MCN 站点的虚拟路径相同的步骤操作。



这完成了客户端站点和 MCN 之间的虚拟路径的基本配置。

> 注意
>
> 有关配置编辑器的连接或预配部分中的更多设置的信息，请参阅“管理 Web 界面联机帮助”，了解这些部分的信息。如果您当前不想配置这些设置，可以继续执行以下所示的相应步骤。

下一步取决于您为部署激活的 SD-WAN 版许可证，如下所示：

- **SD-WAN** 高级（企业）版—高级（企业）版包括全套 WAN 优化功能。如果您想为您的网站配置 WAN 优化，请继续主启用和配置 WAN 优化题。否则，您可以直接前往在客户端上安装 SD-WAN 设备包。
- **SD-WAN** 版本—此版本不包括 WAN 优化功能。您现在可以直接前往在客户端上安装 SD-WAN 设备包。

部署 MCN 配置

June 22, 2021

下一步是准备 SD-WAN 设备包以分发到客户端节点。这涉及以下两个过程：

1. 将配置包导出到更改管理。

   必须先将已完成的配置包从配置编辑器导出到 MCN 上的全局更改管理暂存收件箱，才能生成设备包。执行更改管理部分中提供了说明。

2. 生成和暂存设备包。

   将新配置包添加到 更改管理 收件箱后，可以生成和暂存设备包。为此，您将使用 MCN 上的 管理 **Web** 界面中的更改 管理向导。说明在部分 [将配置部署到分支。] 中提供 (/en-us/citrix-sd-wan/current-release/configuration/deploy-mcn-configuration/perform-mcn-change-management.html)

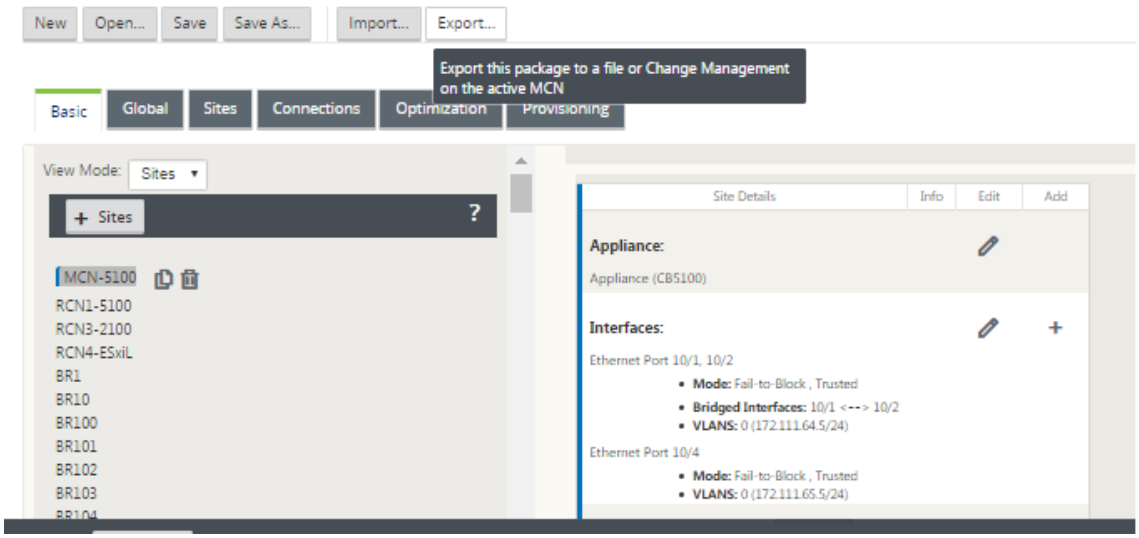
执行 MCN 更改管理

June 22, 2021

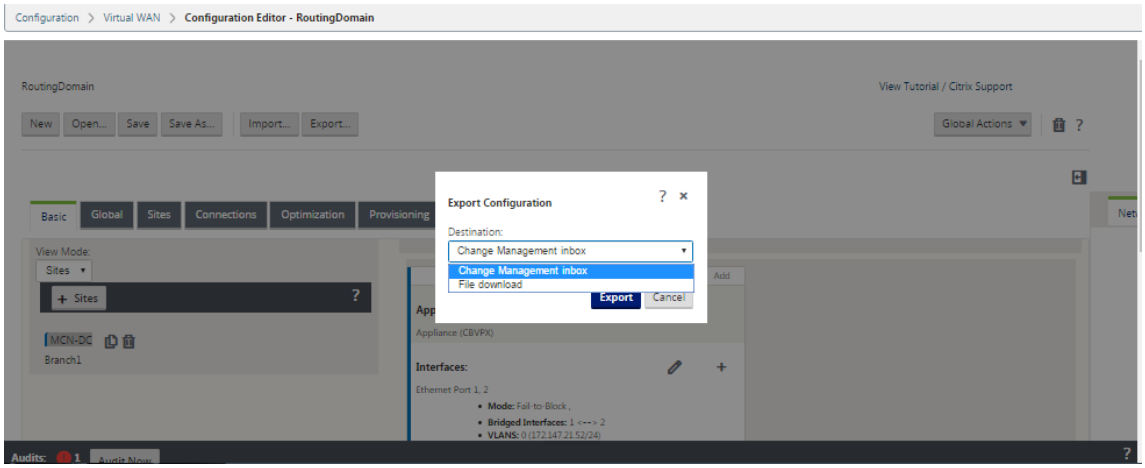
必须先将已完成的配置包导出到管理 Web 界面 更改管 理系统，然后才能生成设备包。

要将配置包导出到 更改管理，请执行以下操作：

1. 在 配置编辑器 页面中，单击 导出（在页面顶部）。



   这将打开 导出配置 对话框。



2. 选择 更改管理 收件箱 作为导出目标。使用 目标 字段中的下拉菜单进行选择。
3. 单击导出。

导出操作完成后，页面顶部将显示绿色成功状态消息。

> 提示
>
> 您可以单击成功消息中的蓝色 更改管理 链接，直接转到 更改管理向导的 更改准备—上载和验证文件 页面（第二页）。您需要导航到此页面才能执行配置过程中的下一步。但是，成功消息仅显示几秒钟，之后您必须使用导航树打开向导，然后逐步转到此页面。说明将在下一节中提供。

您现在可以将 SD-WAN 软件包上载到 MCN 设备，并准备将设备包分发到客户端节点。

将配置部署到分支机构

June 22, 2021

使用配置编辑器准备配置并将配置包导出到更改管理收件箱后，下一步是准备 SD-WAN 设备包以分发到客户端节点。使用 MCN 上的 管理 **Web** 界面中的更改 管理向导。

每个 SD-WAN 设备型号都有不同的 SD-WAN 软件包。设备包由特定型号的软件包组成，该软件包与要部署的配置包捆绑在一起。因此，必须为网络中的每个设备型号准备和生成不同的设备包。

> 注意
>
> 如果您尚未将所需的 SD-WAN 软件包下载到连接到您的网络的 PC 上，现在就可以这样做了。有关获取和下载软件的信息，请参阅获取 SD-WAN 软件包

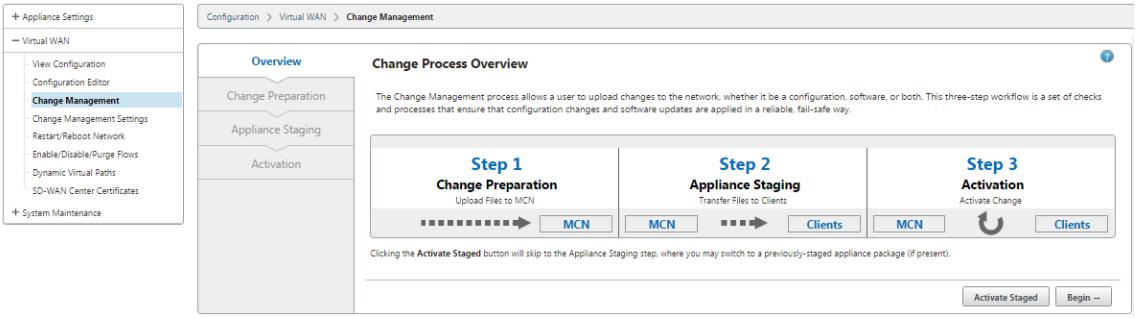
要将软件包和配置上载并安装到 MCN，请执行以下操作：

1. 登录到 MCN 设备上的管理 Web 界面。

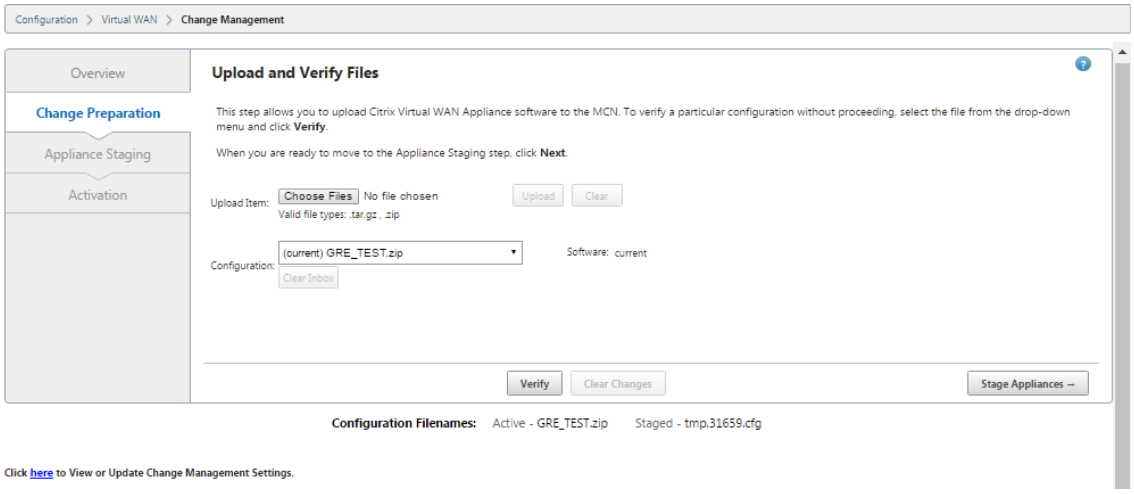
> 注意
>
> 您正在将之前下载的软件包上载到连接的 PC。为方便起见，您可能需要使用同一台 PC 再次连接到 MCN。

2. 选择 配置 选项卡。

3. 在左窗格中，打开 虚拟 **WAN** 部分，然后选择 更改管理。将显示 更改管理 向导的第一页，更改流程概览 页。



4. 单击 开始。更改准备 页面，用于上载和验证是否显示指定的配置和软件包。



5. 上载网络所需的每个 SD-WAN 软件包。
   对于要部署的每个 SD-WAN 软件包，请执行以下操作：

   a) 单击 上载商品 字段 旁边的 选择文件。这将打开一个文件浏览器，用于选择要上载的 SD-WAN 软件包。

   b) 选择 SD-WAN 软件包，然后单 击确定。

   c) 导航到之前下载到本地 PC 的 SD-WAN 软件包，然后选择要上载的软件包。

   d) 单击上传。

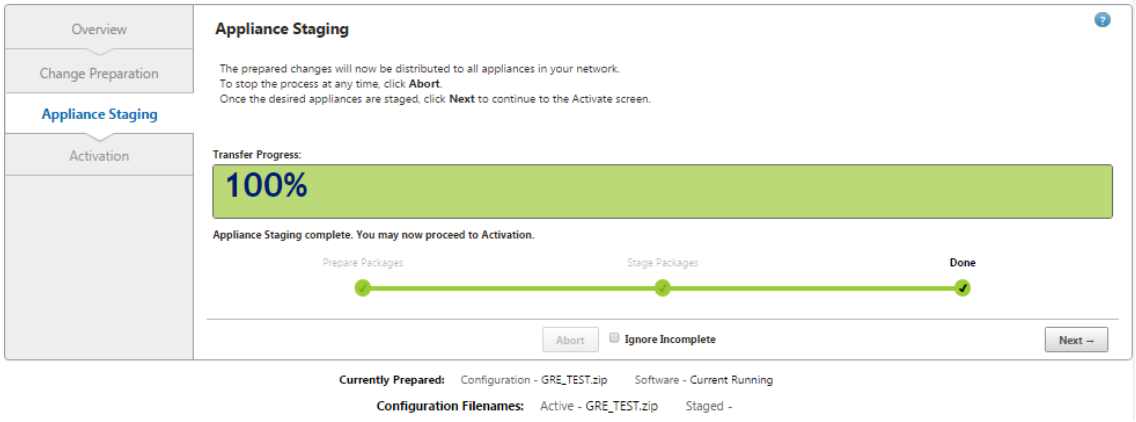
   e) 为您的网络所需的每个 SD-WAN 软件包重复步骤 (i) 至 (iii)。

6. 在 配置 字段下拉菜单中，选择刚导出到 更改管理 的新配置包。

7. 单击 舞台设备。设备分段启动以下操作：

- 将选定的软件包和配置传输到 MCN。
- 为在所选配置中标识的每个设备型号生成一个设备包。
- 将新设备软件包添加到 站点设备 表中的可用软件包列表中。
- 在 MCN 上分阶段新配置和适当的软件包。

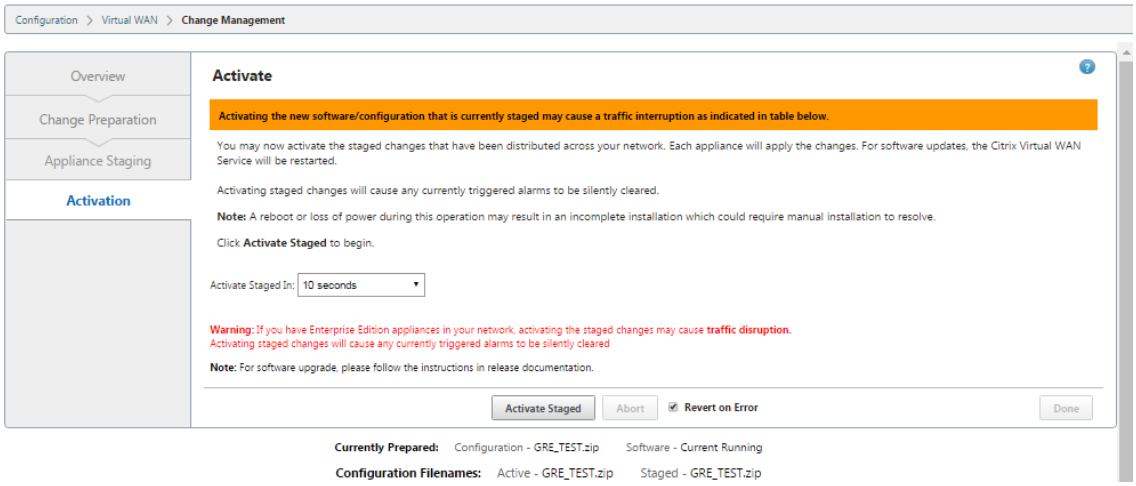
8. 单击下一步。此操作将进入 设 备暂存 页面。



分段操作完成后，将使用新暂存的设备包信息填充站点设备 表。**

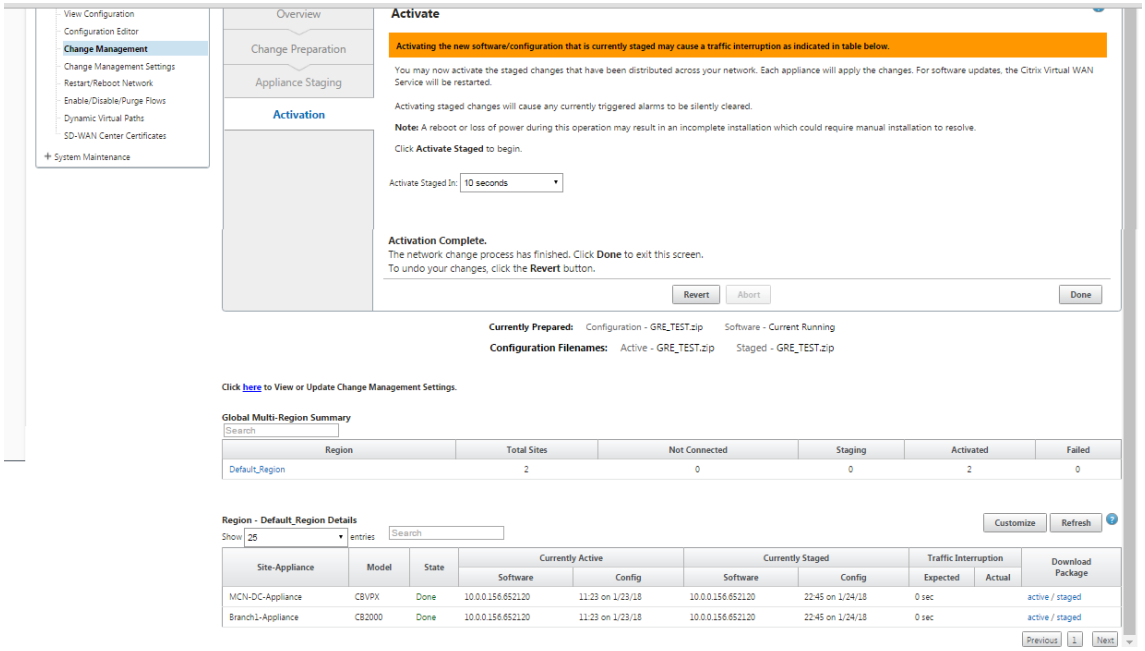
> 注意
>
> 如果这是初始部署，则现在仅更新 MCN 并暂存。如果您正在更新现有部署，并且虚拟路径已在已部署站点之间运行，则此操作还会将相应的设备包分发到已部署的客户端节点，并在这些节点上启动分段。但是，如果要向现有 Virtual WAN 部署添加新客户端节点，则仍然必须在每个新客户端上手动上载、暂存和激活相应的设备包，如本过程中的其余步骤所述。
>
> 如果站点在变更管理页面中显示为 未连接，则在暂存过程中将其标记为失败，进度条完成为 100%。一旦 未连接 的站点恢复在线并连接，MCN 会自动更正它。

9. 选择 还原错误 可在 遇到某些错误时恢复到以前的应用程序包。有关详细信息，请参阅配置回滚。
10. 单击激活暂存。



此时，结果和后续步骤将有所不同，具体取决于这是初始配置还是您正在更新或替换现有配置，如下所示：

- 如果要更新或更改现有部署的配置。
  - 如果这不是初始配置，则会激活 MCN 设备上的新配置和相应的设备包。然后，相应的设备包会分发到 SD-WAN 中的每个客户端并在其上自动激活。这可能需要几秒钟才能完成。



激活完成后，将显示 激活完 成 状态消息，并启用 完 成 按钮。此外，配置文件名状态行（在表上方）现在会在活动字段中显示新激活的软件包的名称。

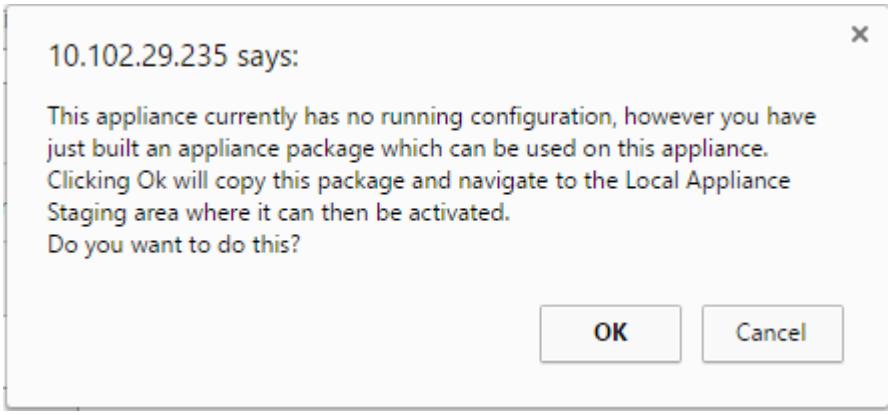
11. 单击 ** 完成并继续执行以下操作之一：

    - 如果您没有向 SD-WAN 添加任何新节点，这将完成 SD-WAN 中新设备包的准备、分发和激活。您可以直接进行启用虚拟广域网服务。

- 如果要向 SD-WAN 添加新的客户端节点，请继续
  将客户端设备连接到您的网络.
- 如果您正在激活初始配置，则此时不会激活新的配置包，并且您必须执行更多步骤。下一步是将配置包复制到本地设备分段区域，以准备在 MCN 上暂存和激活配置包。

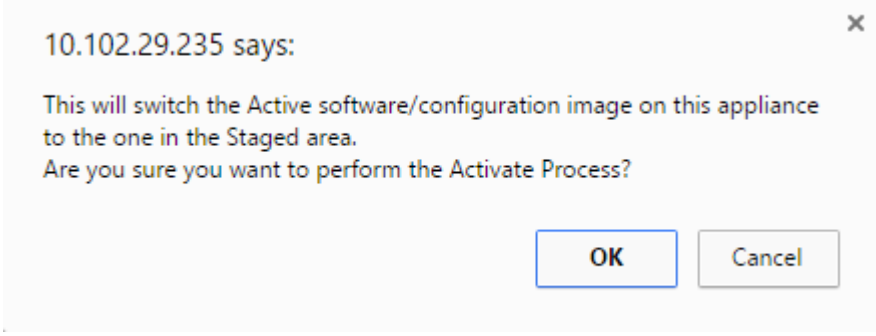
请执行以下操作：

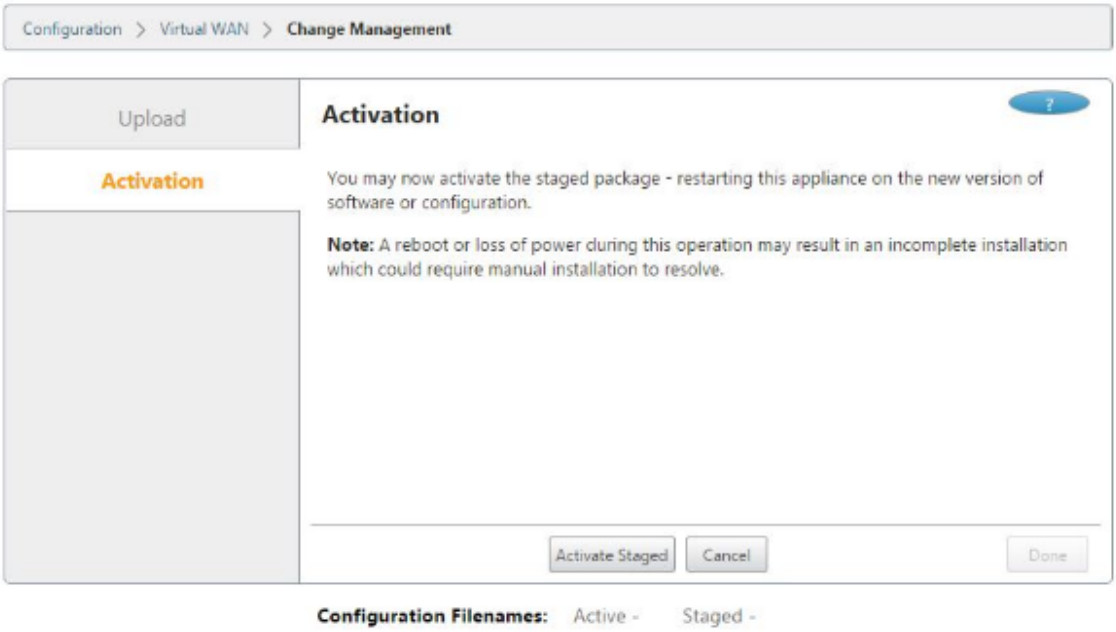
12. 单击激活暂存后，将显示以下消息。



13. 单击 **OK**（确定）。
14. 单击激活暂存。

    这将显示一个对话框，要求您确认激活操作。





15. 单击 **OK**（确定）。

    这将启动暂存配置包的激活。此过程需要几秒钟，在此期间显示进度状态消息。

    激活完成后，将显示一条状态消息，指出激活已完成，并启用 完 成 按钮。

16. 单击完成。此操作将进入管理 Web 界面 控制板 页面，您可以在其中查看激活结果。

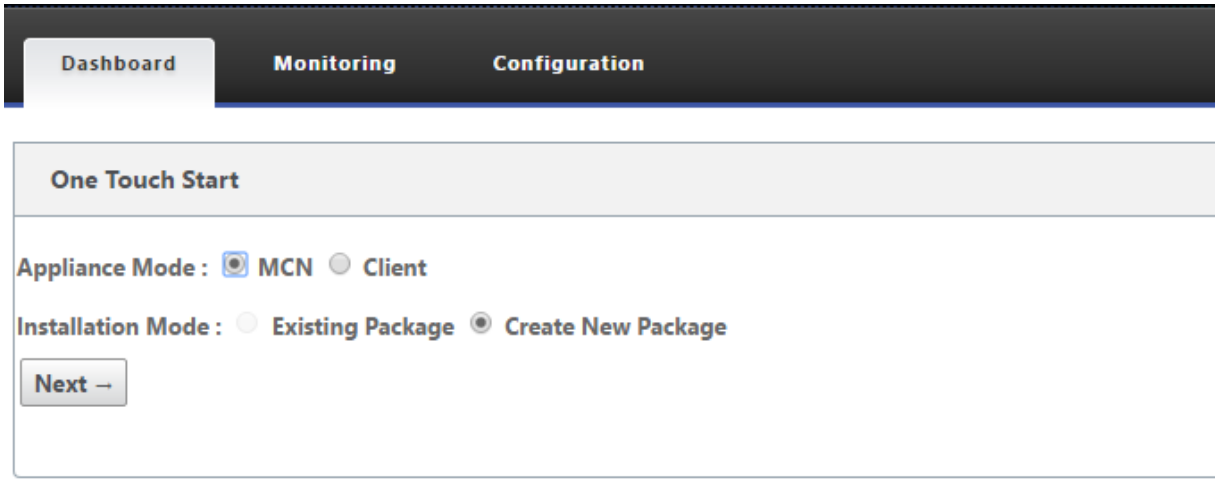
您 现在已完成 MCN 上 SD-WAN 设备包的准备工作。继续 (/en-us/citrix-sd-wan/current-release/configuration/connecting-client-appliances-to-network.html) 将客户端设备连接到您的网络。

> 提示
>
> 更改管理 向导允许您搜索站点设备表。这允许您在具有多个站点的大型网络上查找站点并下载所需的分段配置。您还可以搜索错误状态，例如：失败 或 未连接。这会为您提供该状态下所有站点的列表。

一键启动

June 22, 2021

一旦触摸启动，您可以在首次启动时轻松快速地将 SD-WAN 设备配置为客户端。
设备首次启动时会显示一键启动选项。



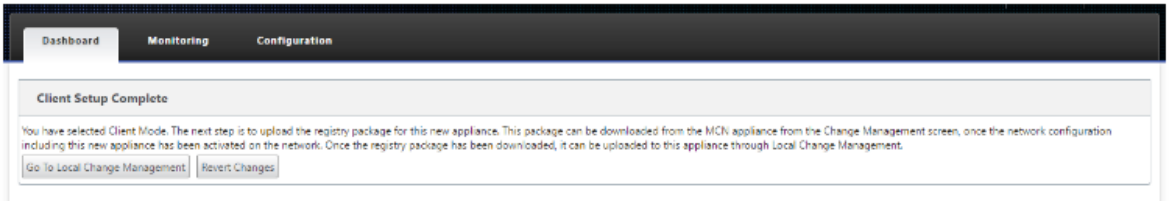
> 注意
>
> 要将 SD-WAN 设备配置为 MCN，请使用配置 编辑器创建配置或导入现有配置。有关详细信息，请参阅在 MCN 上准备 SD-WAN 设备包。

要使用现有配置文件将 SD-WAN 设备配置为客户端，请执行以下操作：

1. 选择 客户端 作为设备模式。
2. 选择 现有软件包 安装模式。管理员必须定期保存 MCN 的配置，才能使用 MCN 的现有软件包。
3. 单击 选择文件 以从本地计算机中选择配置包。
4. 单击上载并安装。

要使用本地更改管理将 SD-WAN 设备配置为客户端，请执行以下操作：

1. 选择 客户端 作为设备模式。
2. 选择 创建新包 以使用本地更改管理为此设备上载配置包。可以从更改管理屏幕中从 MCN 设备下载该软件包。
3. 单击下一步。
4. 单击 转到本地更改管理。



按照主题中的步骤操作在客户端上安装 SD-WAN 设备包。

将客户端设备连接到您的网络

November 1, 2021

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。

在客户端上安装 **SD-WAN** 设备包

June 22, 2021

准备好设备包并连接 MCN，并且分支站点管理员已将其各自的客户端设备连接到 LAN 和 WAN 后，下一步是在每个客户端上上载并激活相应的 SD-WAN 设备包。更改管理向导将指导您完成此过程。

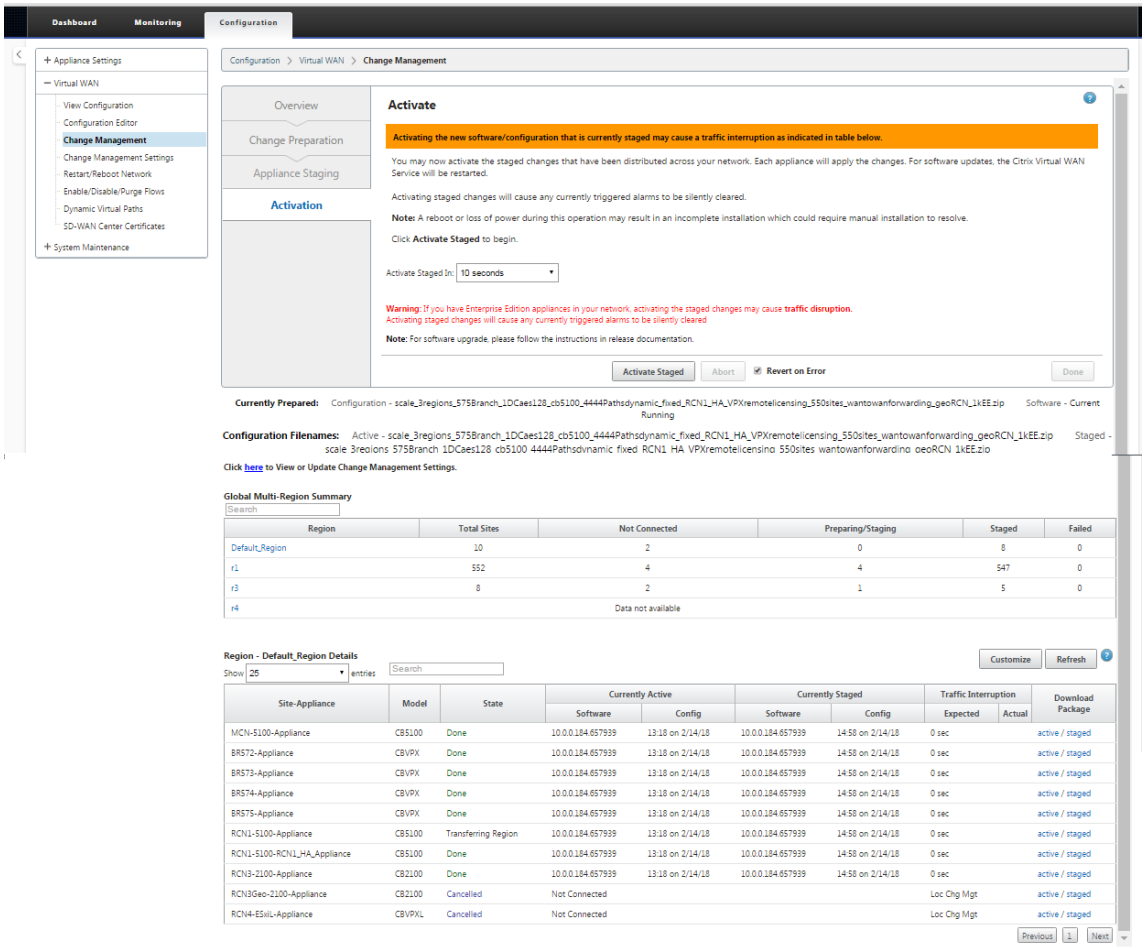
要在客户端设备上安装和激活软件和配置，请执行以下操作

1. 在连接的 PC 上，打开浏览器并登录到 MCN 设备管理 Web 界面。

   在浏览器地址字段中输入 MCN 的管理 IP 地址。这将显示 MCN 设备的 管理 Web 界面 控制板 页面。

2. 选择 配置 选项卡。在左侧的导航窗格中，选择 虚拟 **WAN** ，然后选择 更改管理。

   此操作将显示 更改流程概览 页面（更改管理 向导的第一页）。



在此页面底部，您可以看到 一个列出各个站点和设备的表格。在 下载包 列中表格的最右侧，是 活动（如果可用）和 暂存一个 ppliance 软件包的链接。

> 注意
>
> 如果这是初始安装，则 活动 链接尚不可用，并将替换为纯文本标记 无。

3. 单击要下载的程序包的 暂 存 链接。

   在 站点设备 表中，找到站点设备的条目，然后单击该条目的 下载包 列中的 暂存 链接。将显示用于选择下载位置（在本地 PC 上）的文件浏览器。

4. 选择下载位置，然后单击 确定。

5. （可选。）下载完成后，请注销 MCN 管理 Web 界面。

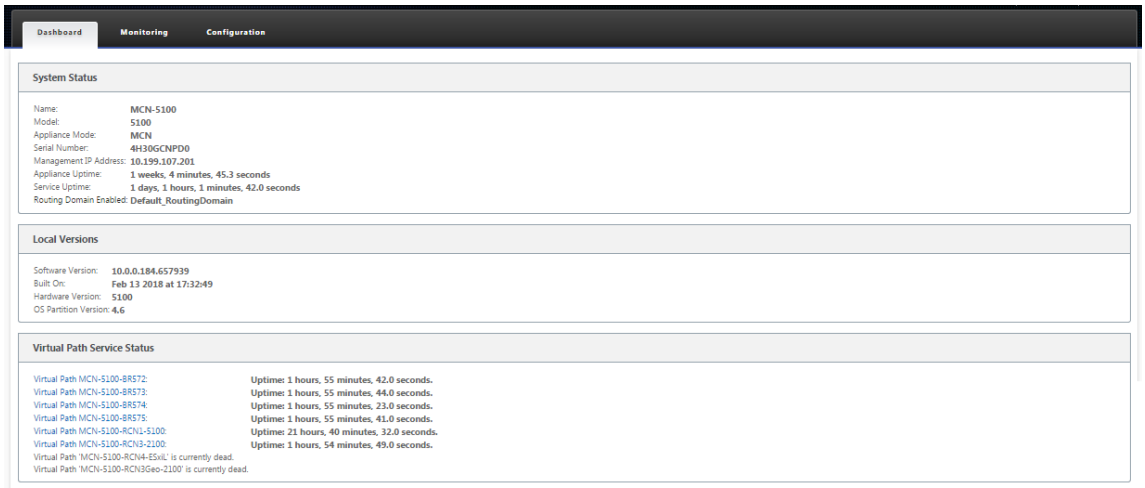
6. 打开浏览器，然后输入要将设备包.zip 文件上载到的客户端的 IP 地址。

> 注意
>
> 请忽略 管理 Web 界面的任何浏览器证书警告。

这将打开客户端设备上的 Citrix SD-WAN 管理 Web 界面登录屏幕。

7. 输入管理员用户名和密码，然后单击 登录。默认的管理员用户名是 *admin*。默认密码是 密码。

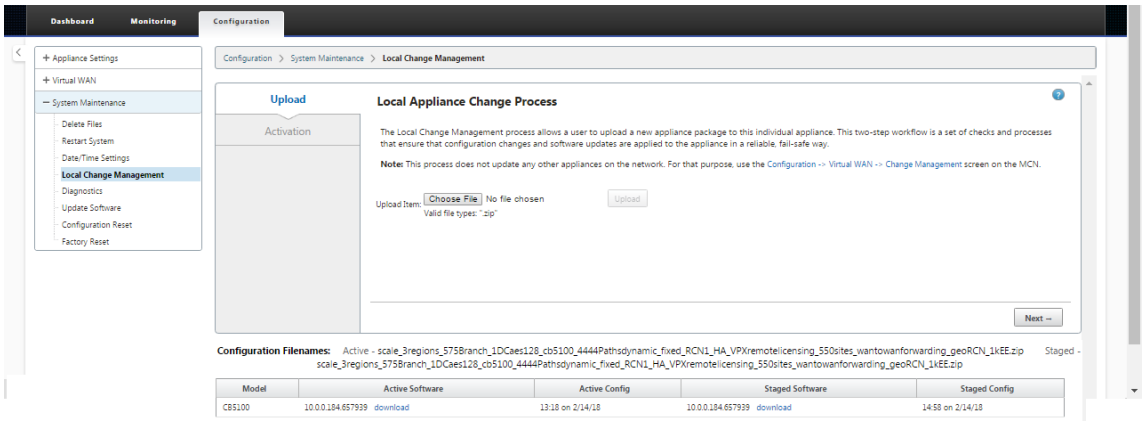
   这将显示客户端设备的 管理 Web 界面控制面 板 页面。



> 注意
>
> 如果这是初始安装，或者如果您暂时禁用了此设备上的虚拟 WAN 服务，则 可以看到 一个 goldenrod 审核警报图标，其中显示一条状态消息，指示虚拟 WAN 服务处于非活动状态或禁用状态。您现在可以忽略此警报。在完成安装后手动启动服务之前，警报将保留在 控制板 页面上。

8. 选择 配置 选项卡。
9. 在导航树（左窗格）中打开 系统维护 分支，然后选择 本地更改管理。

   此操作将显示用于 上载设备包的 本地设备更改流程上载 页面。

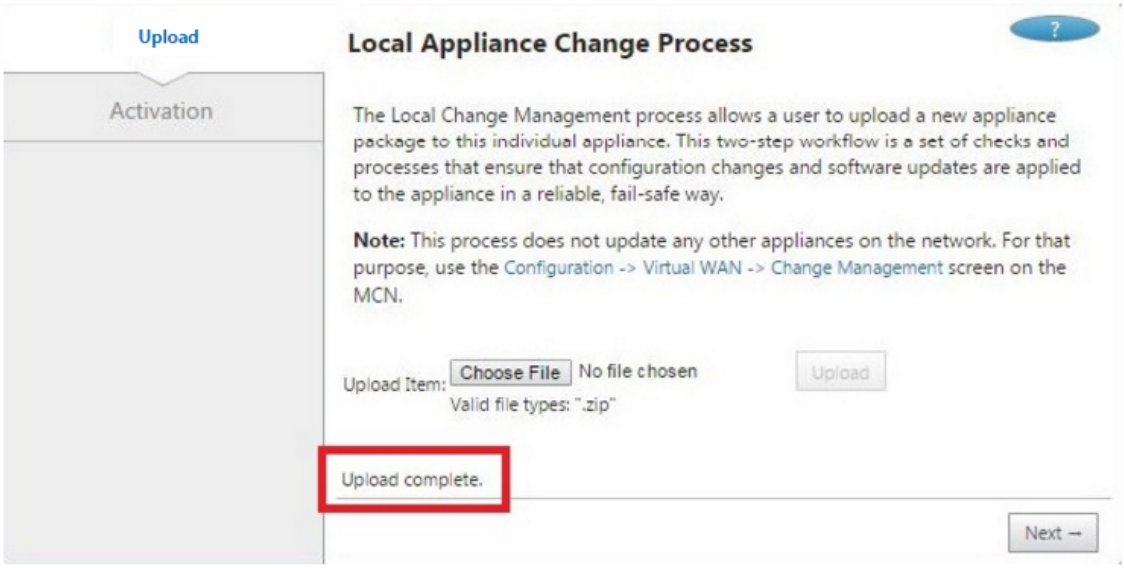


10. 单击 上载商品 标签旁边的 选择文件。

    这将打开一个文件浏览器，用于选择要上载到客户端的设备包。

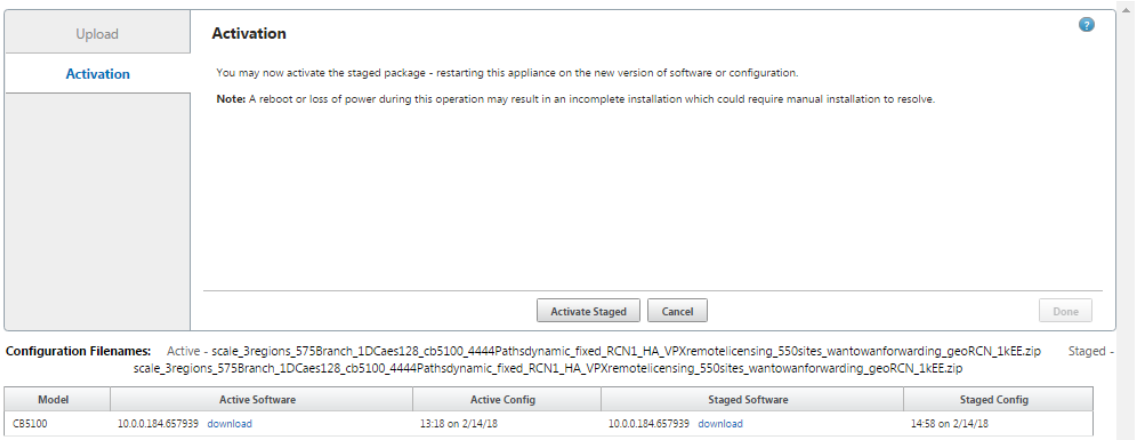
11. 导航到刚从 MCN 下载的 SD-WAN 设备包 zip 文件，选择该文件，然后单 击 确定。
12. 单击上载。

    上载过程需要几秒钟才能完成。完成后，将显示状态消息（页面左侧中间），指出 上载已完成。



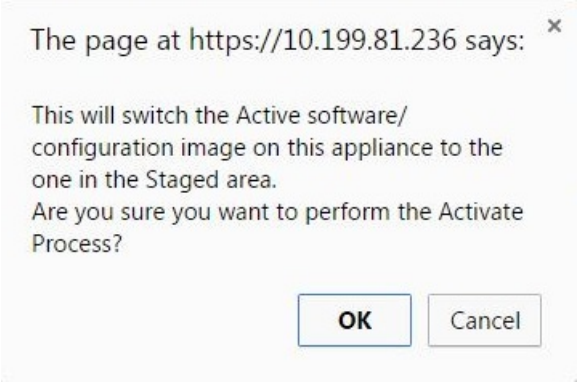
13. 单击下一步。

此操作会上载指定的软件包，并显示 本地更改管理 激活 页面。



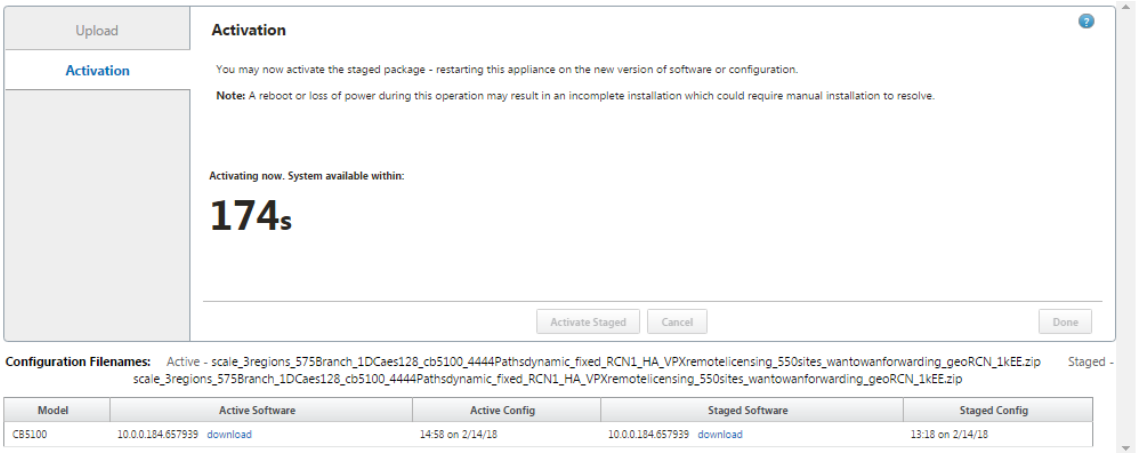
14. 单击激活暂存。

这将显示一个对话框，提示您确认激活操作。

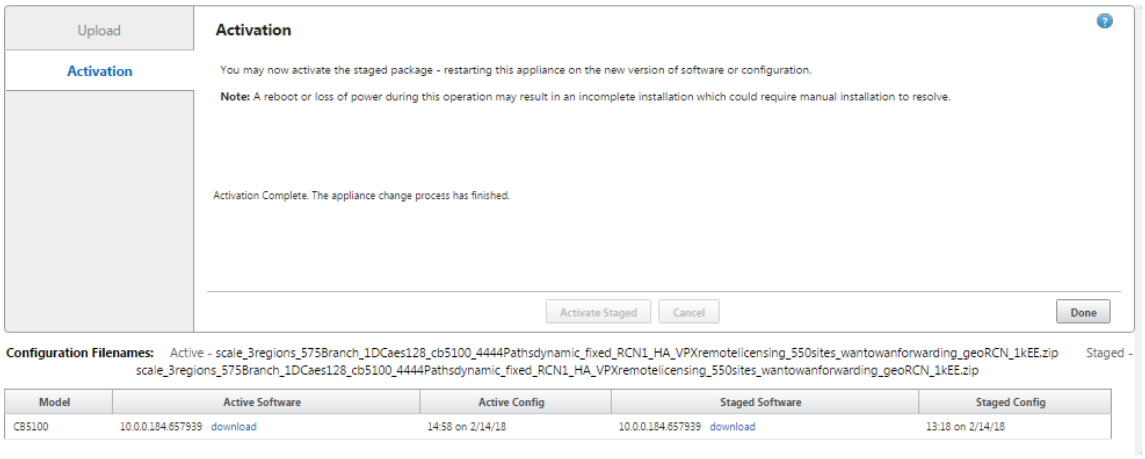


15. 单击确定。

这会激活新安装的软件包，如果这不是初始部署，则会在客户端设备上启动虚拟 WAN 服务。此过程需要几秒钟，在此期间显示进度状态消息。



激活完成后，将显示一条状态消息，指出 激活已完成，并且 完成 按钮将变为可用。

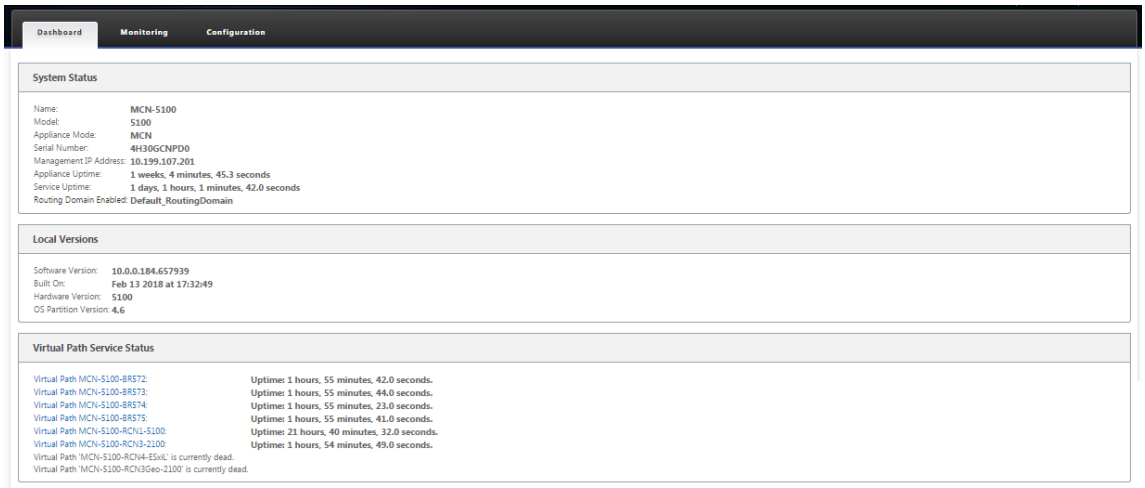


16. 单击 完成 退出向导并查看激活结果。

    激活完成后，单击 激活 页面上的 完 成以返回管理 Web 界面 控制板 页面。

    如果这不是初始部署，此页面现在应显示软件包的当前活动版本、操作系统分区和 虚拟路径状态的更新信息。如果这是初始安装，则会出现一个 goldenrod 审核警报图标，以及一条状态消息，指示虚拟广域网服务处于非活动状态或禁用状态。在这种情况下，您必须手动启用该服务，如中所述启用虚拟广域网服务。

    下图显示了显示警报图标和状态消息的客户端 控制板 示例页面。



完成初始 SD-WAN 部署的最后一步是启用虚拟 WAN 服务。启用虚拟广域网服务部分中提供了说明。

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

June 22, 2021

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。

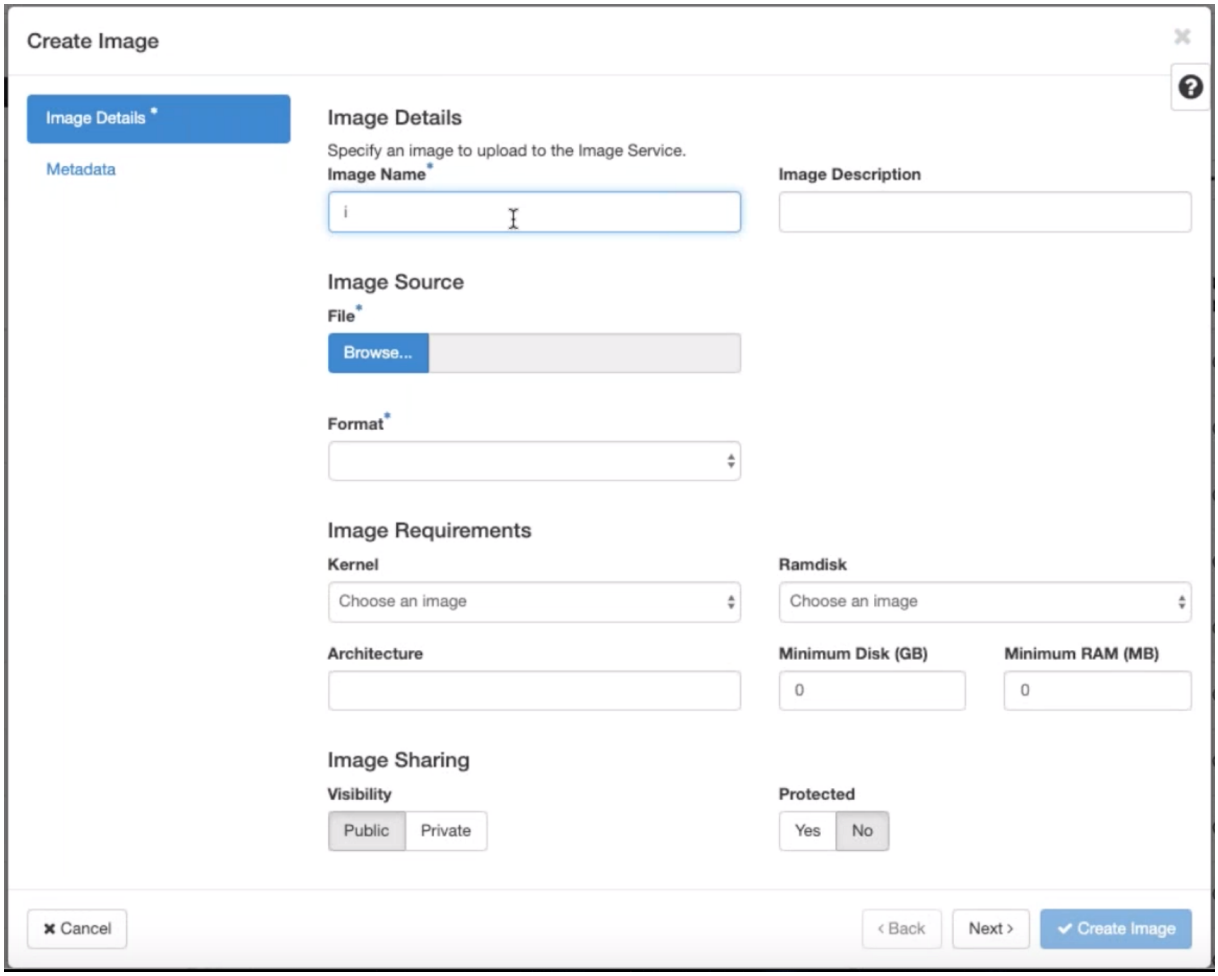
对于 OpenStack 中的 SD-WAN 实例，是用户提供的管理 IP、DNS 和序列号所需的输入。Cloudinit 脚本将解析这些输入并使用给定的信息置备实例。

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。

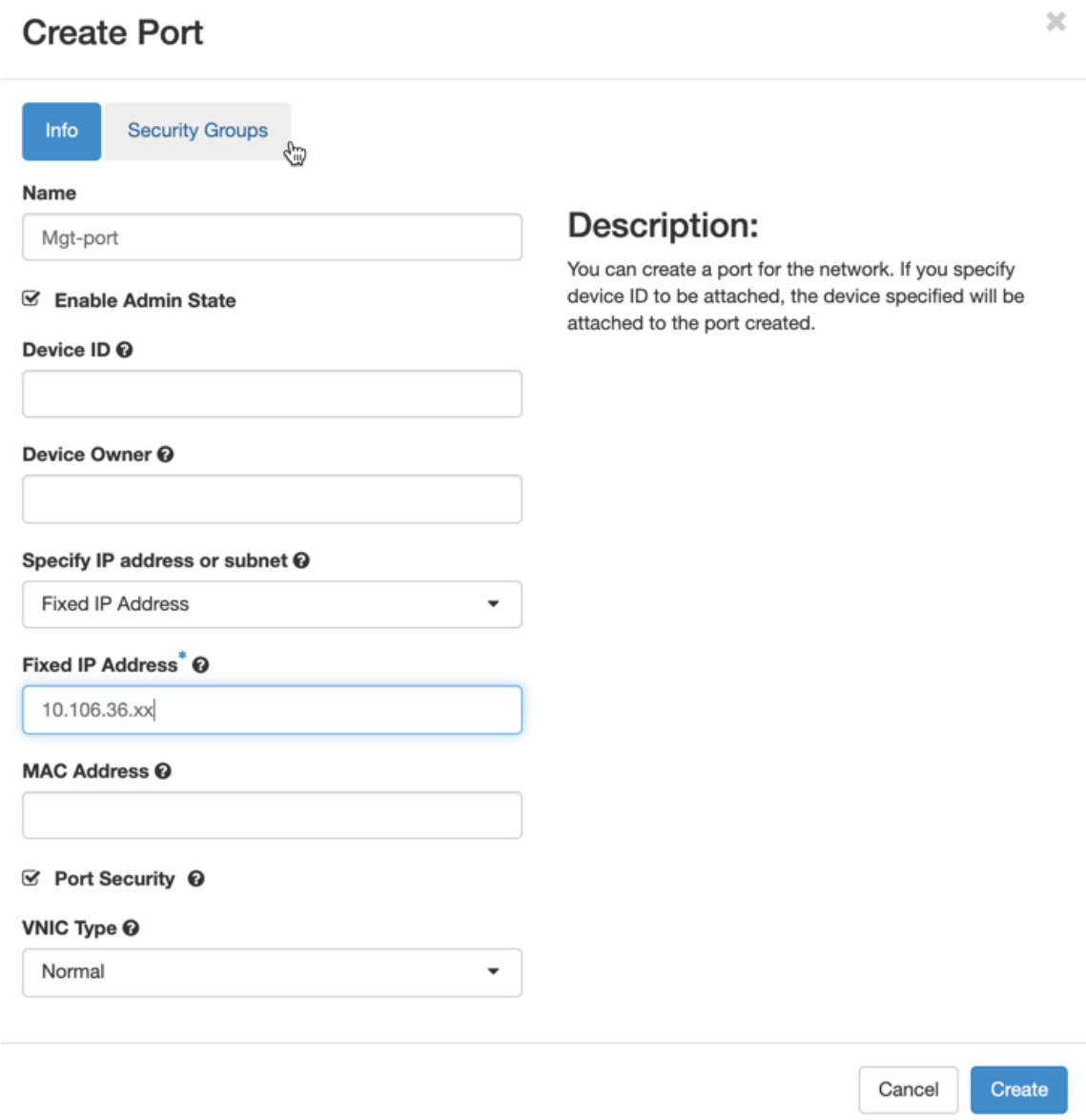


- 图片名称 -提供图像名称。
- 图片描述—添加图片描述。
- 文件 -从本地驱动器浏览 kvm.qcow2 映像文件并将其选中。
- 格式—从下拉列表中选择 QCOW2 —QEMU 模拟器磁盘格式。

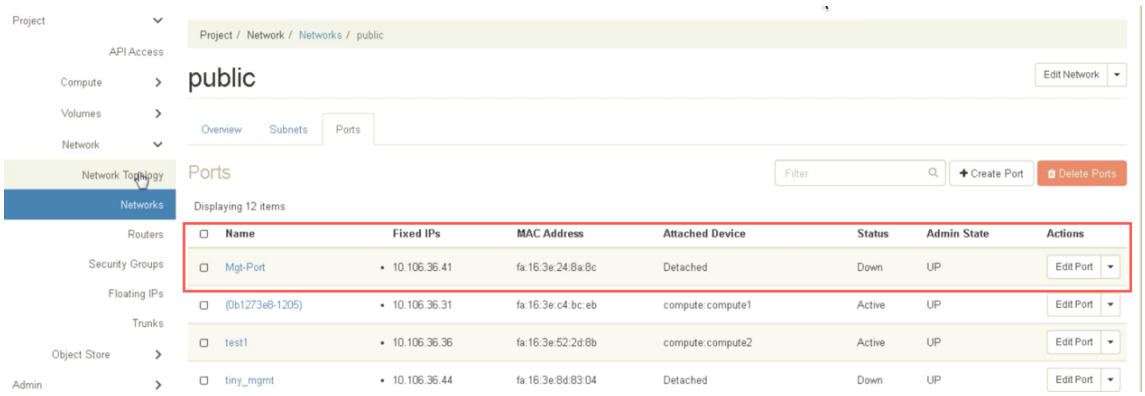
单击创建映像。

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



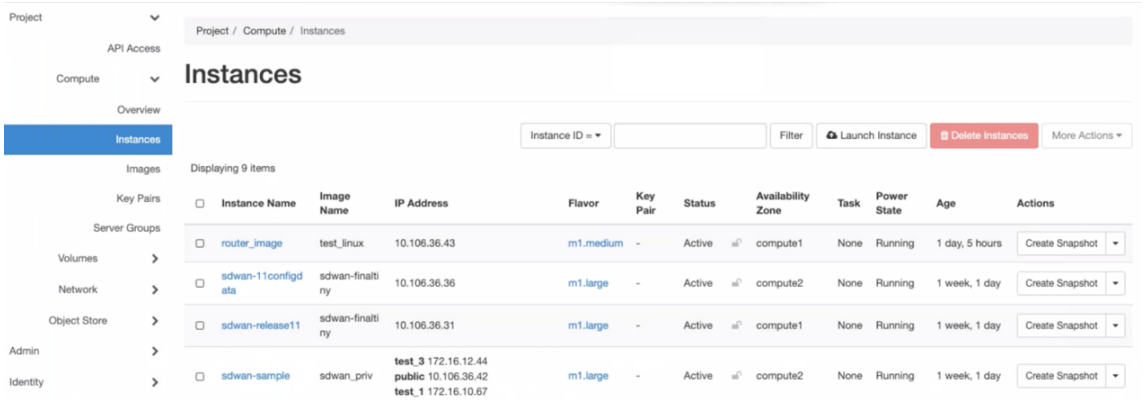
如果选择 固定 **IP** 地址，则必须为新端口提供子网 IP 地址。



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。

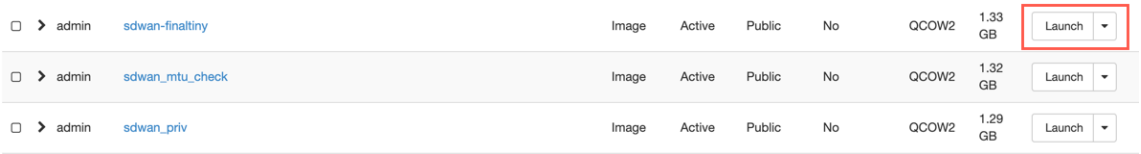
3. 登录 OpenStack 并配置实例。



4. 下载 **kvm.qcow2.gz** 文件并解压它。

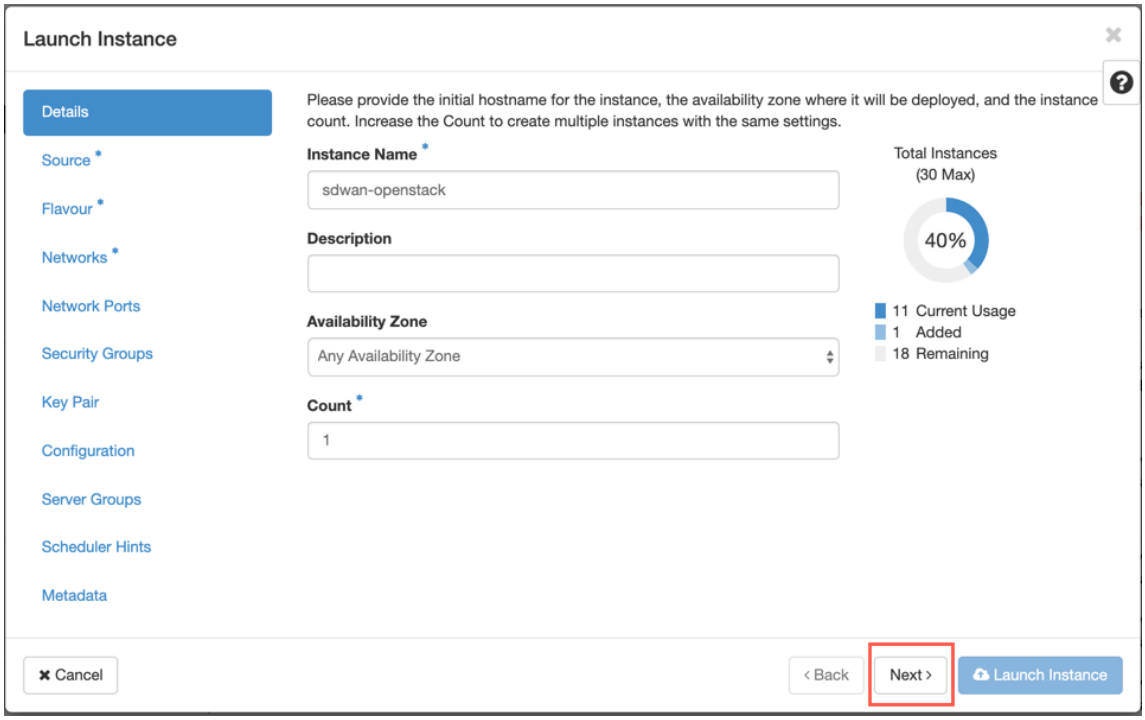
5. 转到 实例，然后单击 启动实例。

> 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。

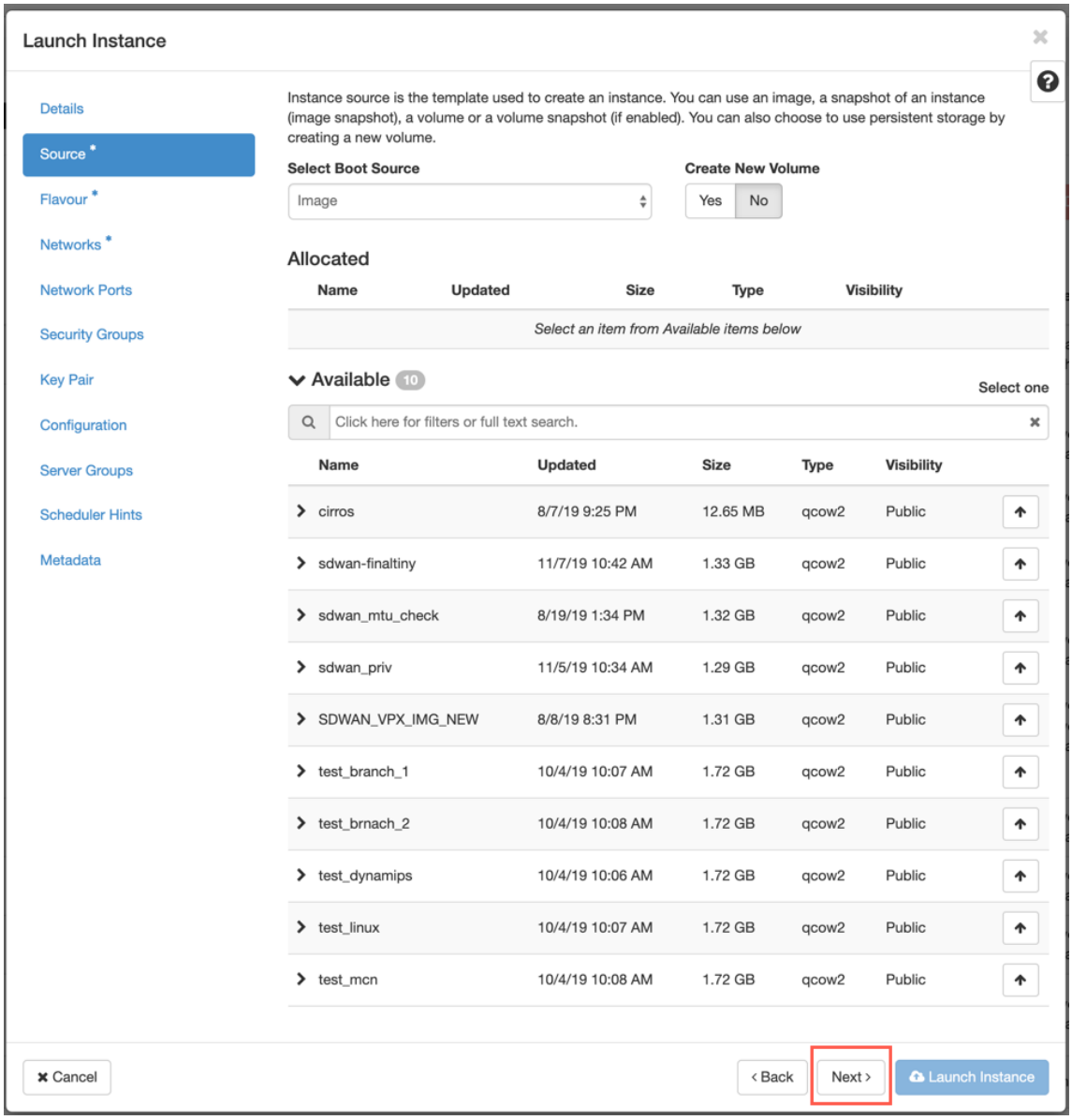


6. 在 详细 信息选项卡下，提供以下信息：

   - 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。



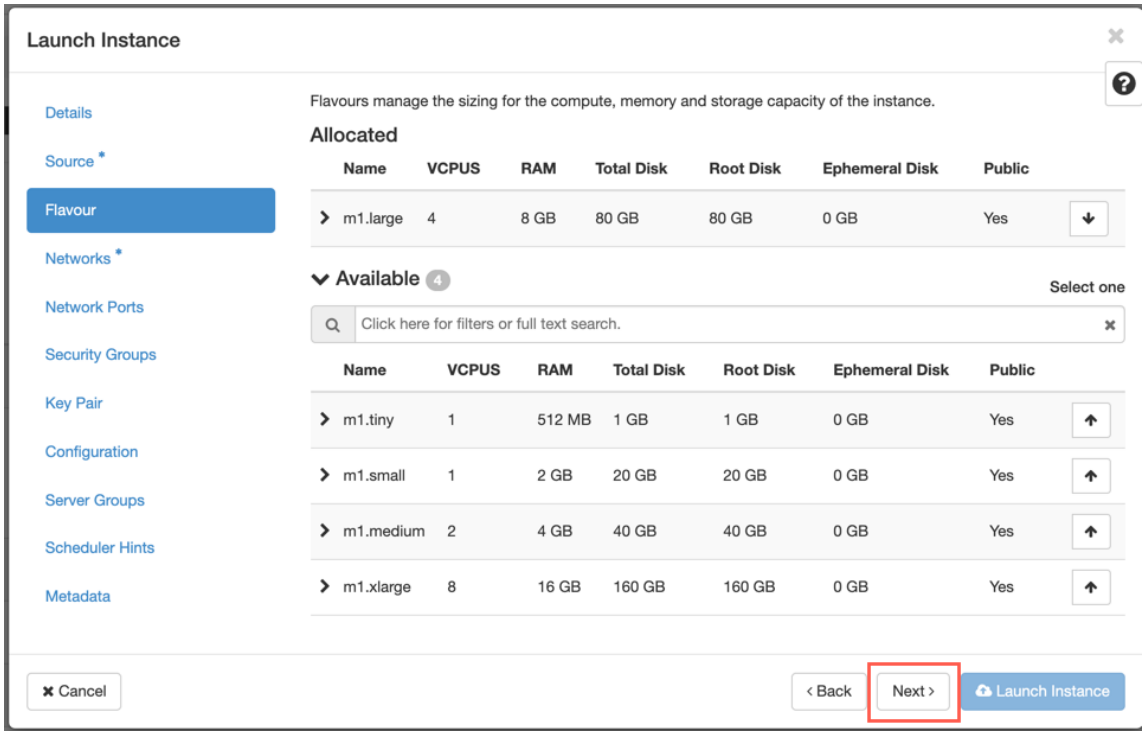
7. 在 源 选项卡中，在 创建新卷 下选择 否，然后单击下一步。实例源是用于创建实例的模板。



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。

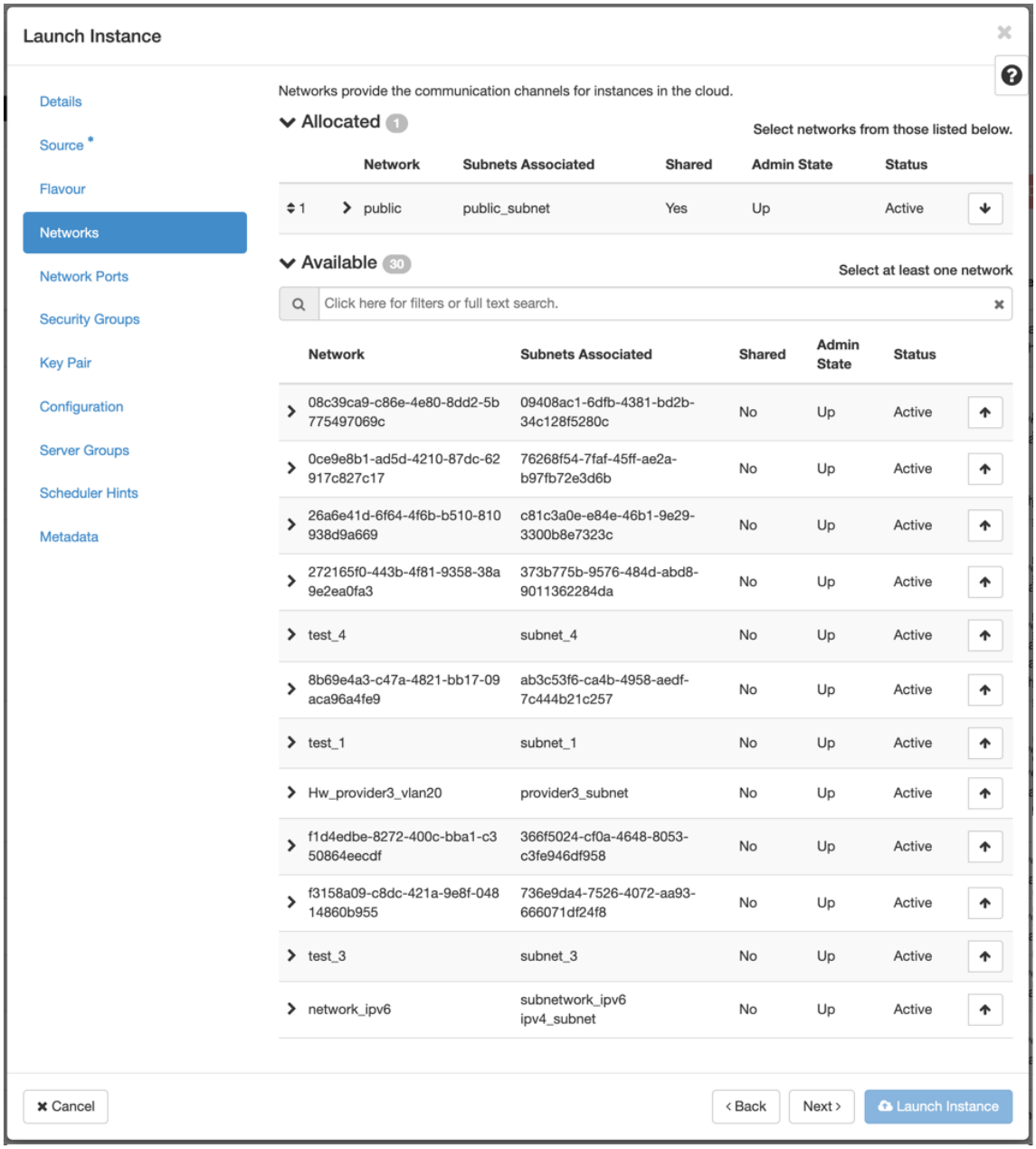
> 注意
>
> 您选择的风格必须有足够的资源来支持您尝试创建的实例类型。没有为您的实例提供足够资源的样式会在可用表中标识一个黄色警告图标。

管理员负责创建和管理风味。单击要分配的箭头（右侧）。



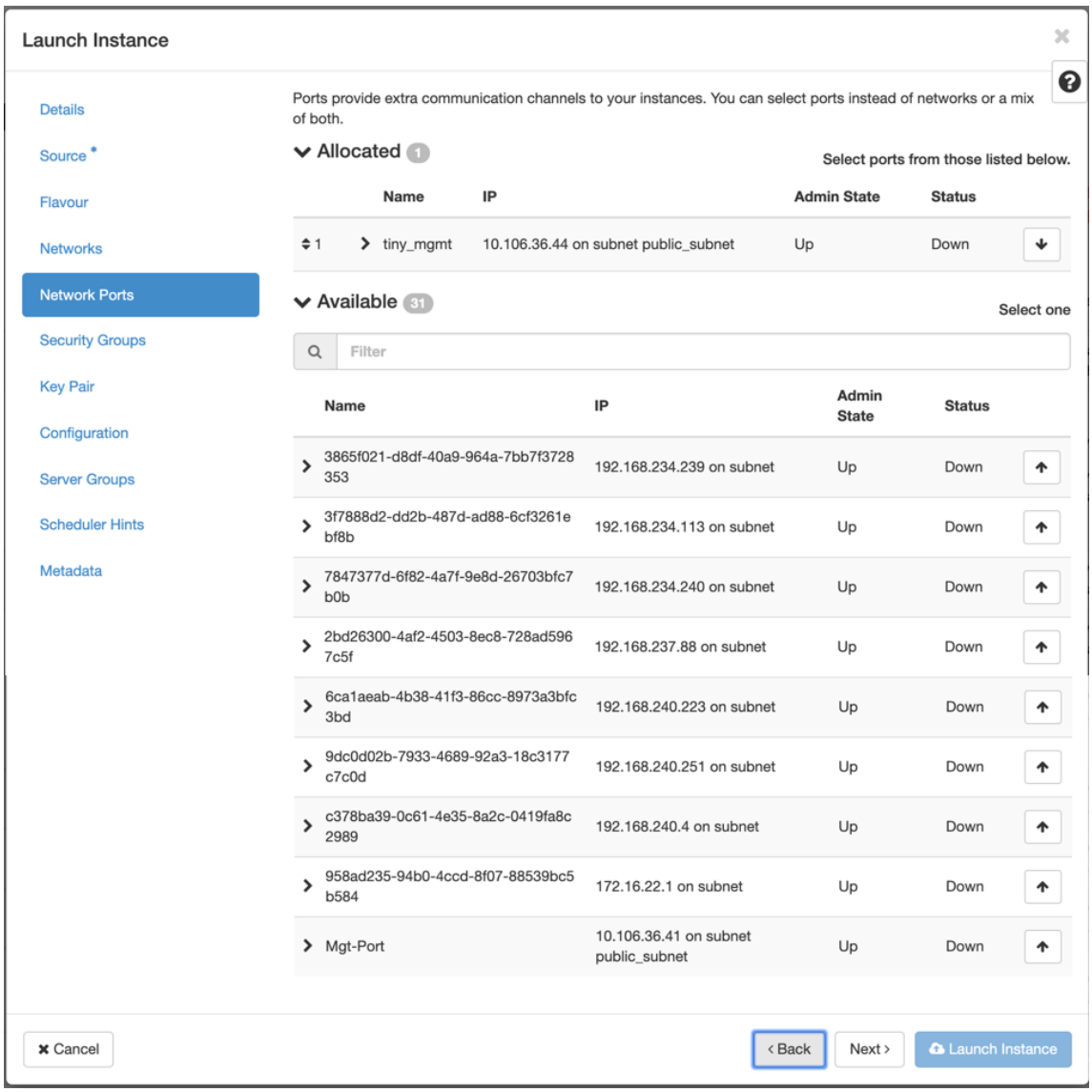
9. 选择网络，然后单击 下一步。网络为实例提供通信通道。

> 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。



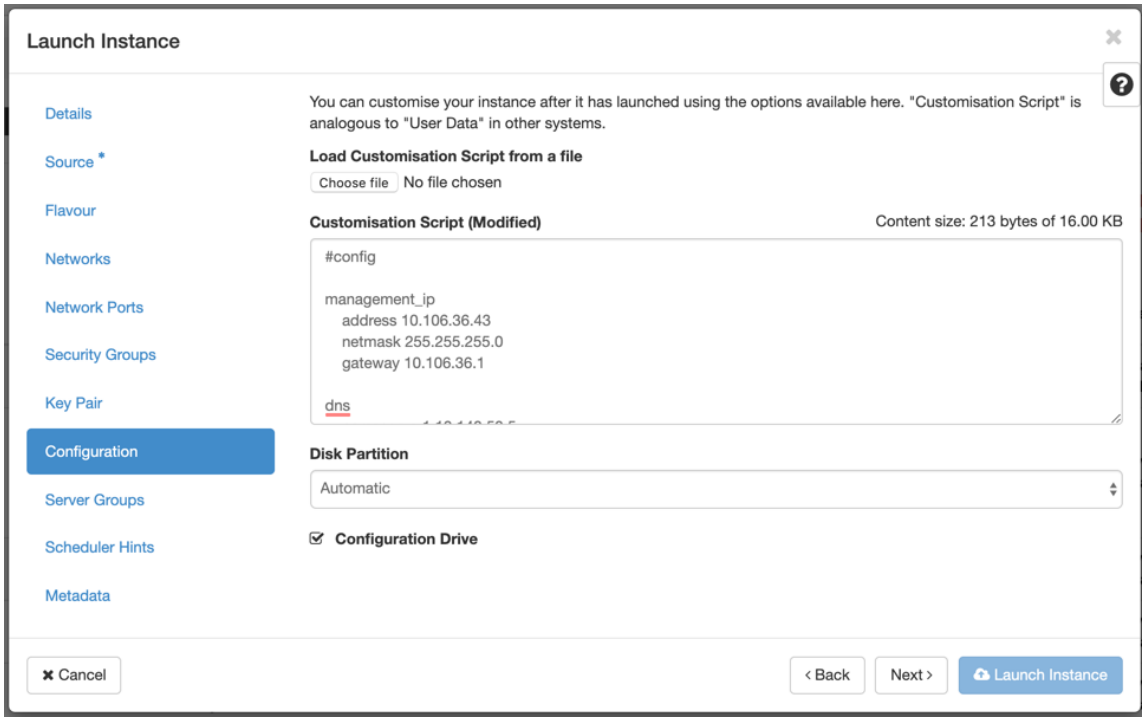
10. 为实例选择网络端口，然后单击 下一步。网络端口为实例提供额外的通信通道。

> 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 26, 2023

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。

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。

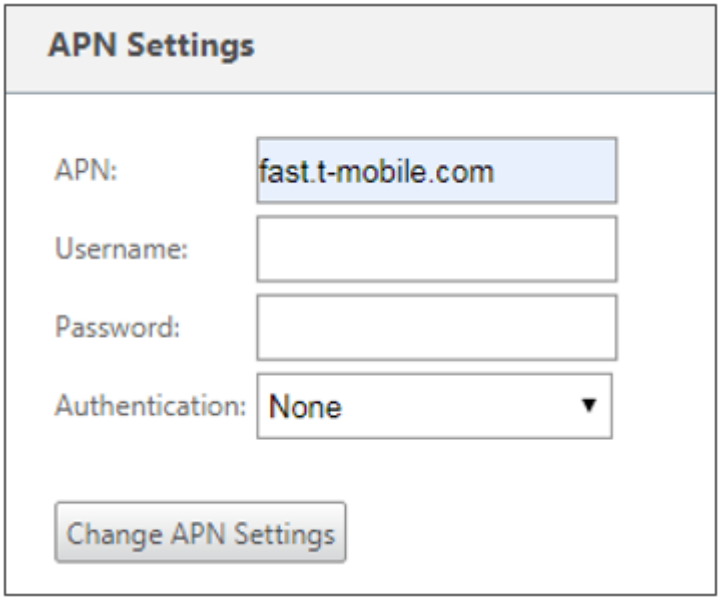
   > 注意：
   > 仅支持标准或 2FF SIM 卡（15x25 毫米）。

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。

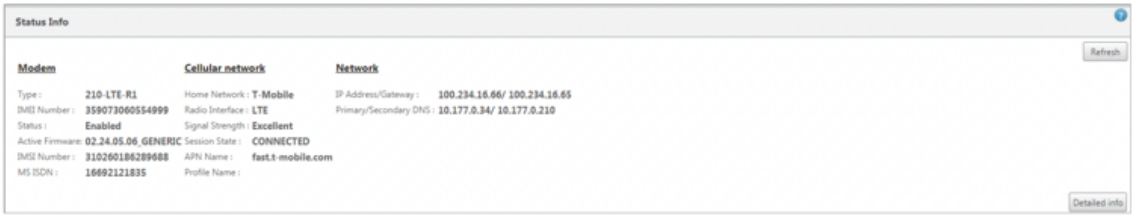
4. 配置 APN 设置。在 SD-WAN GUI 中，导航到 配置 > 设备设置 > 网络适配器 > 移动宽带 > **APN** 设置。

> 注意：
> 从承运人处获取 APN 信息。



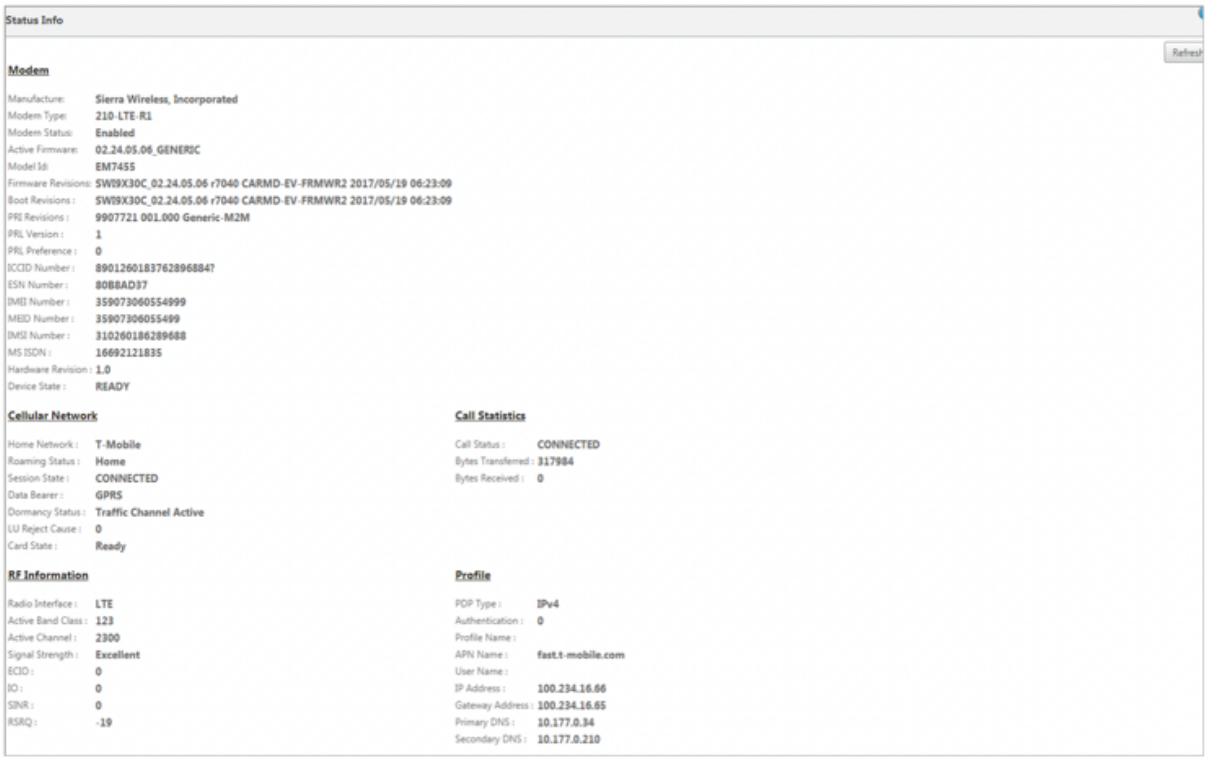
5. 输入承运人提供的 **APN**、用户名、密码 和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。
6. 单击 更改 **APN** 设置。
7. 在 SD-WAN 设备 GUI 中，导航到 配置 > 装置设置 > 网络适配器 > 移动宽带。

   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：

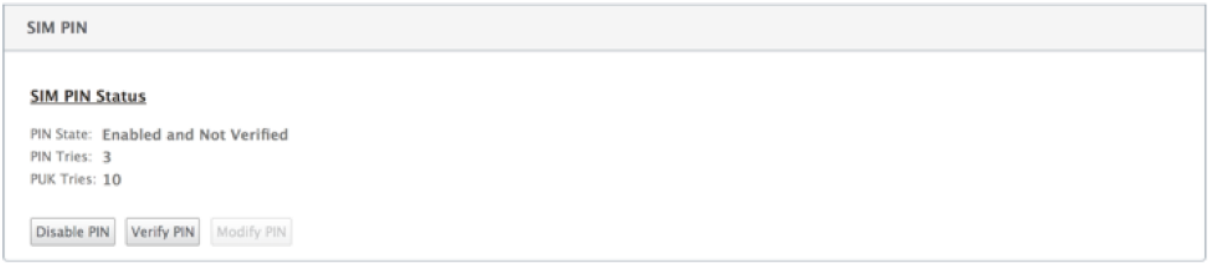
- 操作模式：显示调制解调器状态。
- 活动 **SIM** 卡：在任何给定时间，只能有一个 SIM 卡处于活动状态。显示当前处于活动状态的 SIM 卡。
- 卡状态：存在表示 SIM 卡已正确插入。
- 信号强度：信号强度的质量-优秀、良好、公平、差或无信号。
- 家庭网络：插入的 SIM 卡的运营商。
- **APN** 名称：LTE 调制解调器使用的接入点名称。
- 会话状态：已连接表示设备已加入网络。如果会话状态已 断开连接，请在启用数据计划时向运营商核实帐户是否已激活。



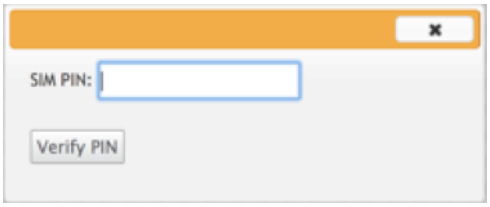
SIM PIN

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 卡。您可以从运营商处获取 SIM PIN。

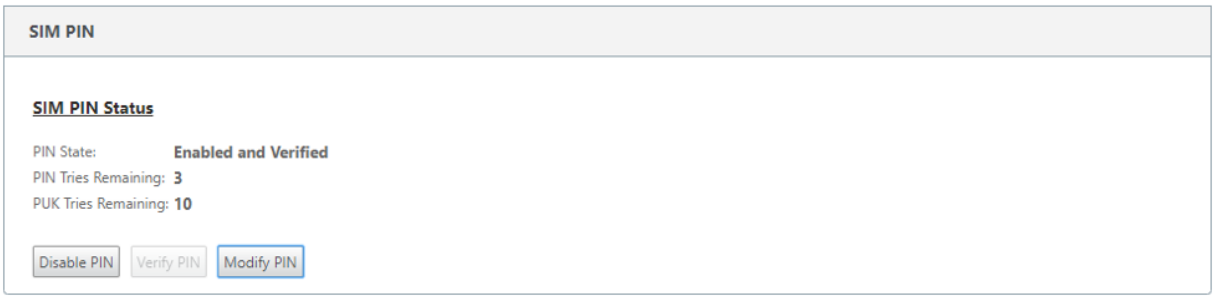
要执行 SIM PIN 操作，请导航到配置 **>** 设备设置 **>** 网络适配器 **>** 移动宽带 **> SIM PIN**。



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

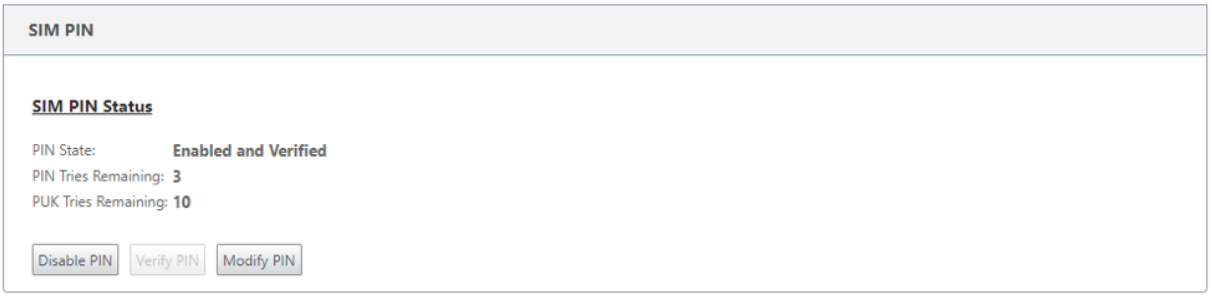


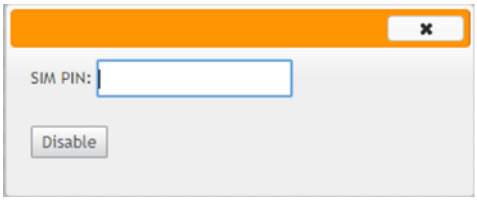
状态更改为 已启用 和 已验证。



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。

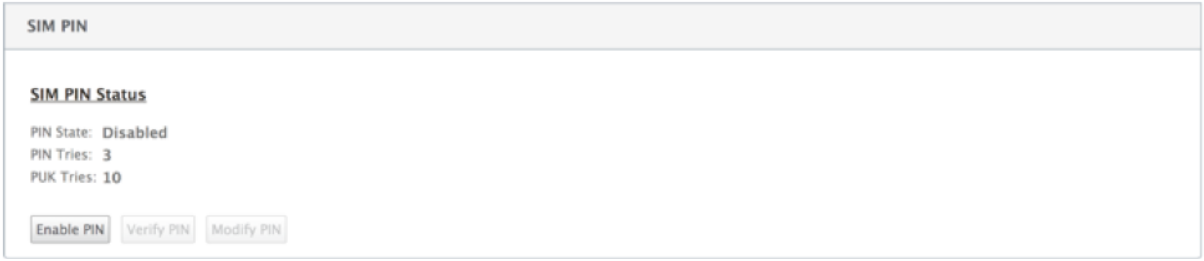




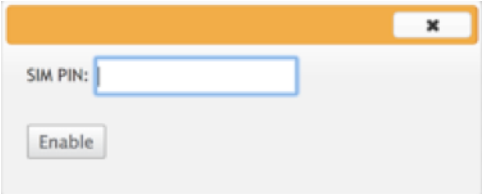
单击 禁用 **PIN**。输入 **SIM PIN** 码，然后单击 禁用。

启用 **SIM PIN**

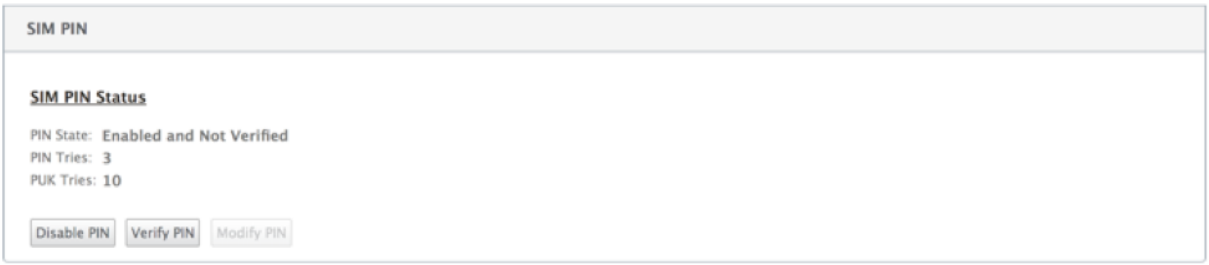
可以为禁用了 SIM PIN 的 SIM 启用 SIM PIN。



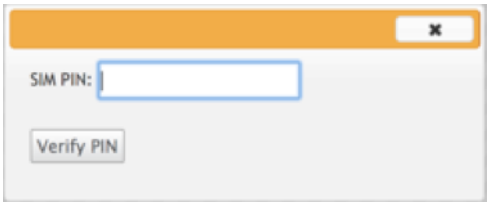
单击 启用 **PIN**。输入运营商提供的 SIM PIN，然后单击启用。



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。



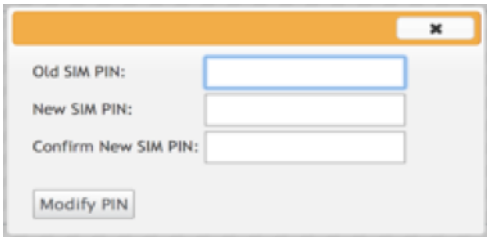
单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。



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。

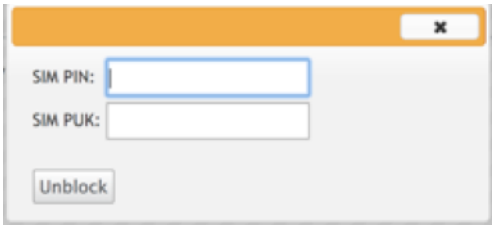
单击 修改 **PIN**。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 修改 **PIN**。



取消阻止 **SIM** 卡

如果您忘记了 SIM 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。输入从运营商处获得的 **SIM PIN** 和 **SIM PUK** ，然后单击取 消封锁。

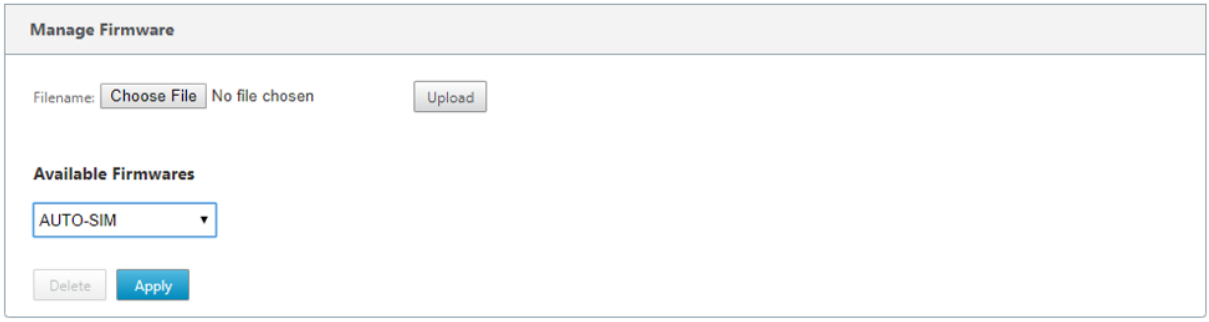


> 注意：
> SIM 卡被永久阻止，并且 10 次 PUK 尝试失败，同时解除阻止 SIM 卡。请联系运营商以获取新的 SIM 卡。

管理固件

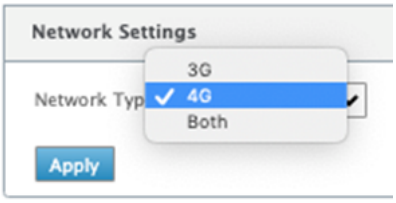
每个启用了 LTE 的设备都将拥有一组可用固件。您可以从现有的固件列表中选择或上载固件并应用它。

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

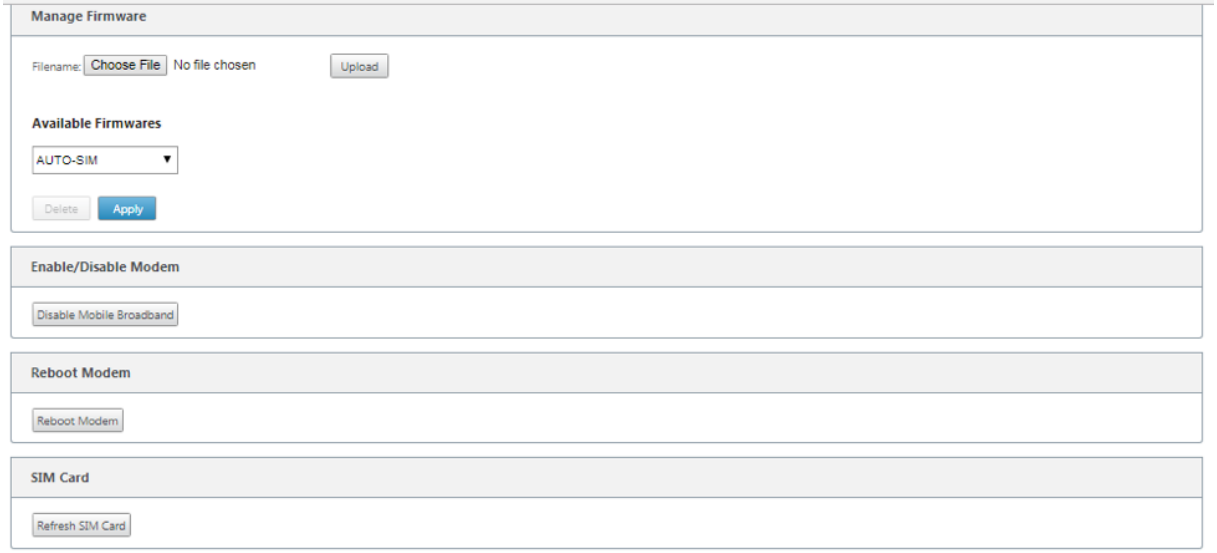
根据您使用 LTE 功能的意图启用/禁用调制解调器。默认情况下，LTE 调制解调器处于启用状态。

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。



可以使用 Citrix SD-WAN Center 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。

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 **>help**。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。

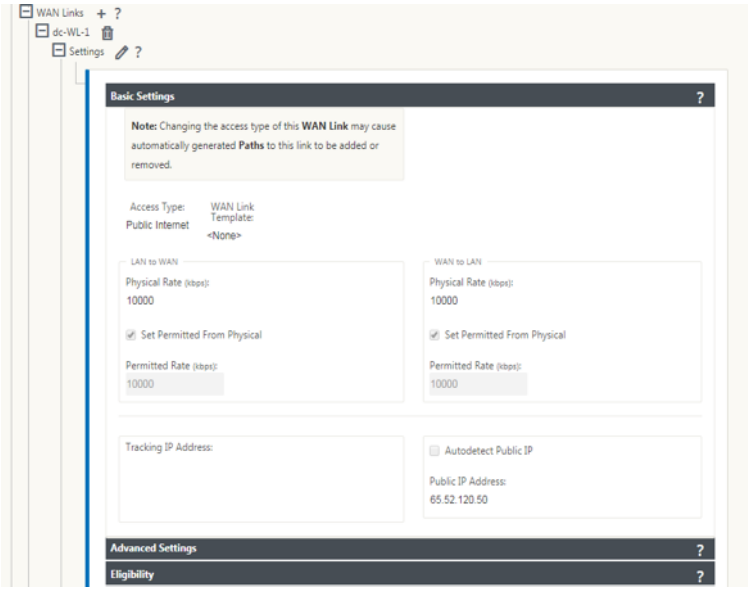
命令	说明
Help {lte>help}	列出可用 LTE 命令和参数
Status {lte>status}	显示 LTE 连接状态
Show {lte>show}	显示 LTE 设置
Disable {lte>disable}	禁用 LTE 调制解调器
Enable {lte>enable}	启用 LTE 调制解调器
Apn {lte>apn}	配置 APN 设置信息
SIM-关闭电源、打开、重置 > {lte> sim-关机、打开、重置}	关闭 SIM 卡、打开 SIM 卡电源、刷新 SIM 卡
SIM PIN {lte>sim-pin}	关闭 SIM 卡、打开 SIM 卡电源、刷新 SIM 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
应用-FW\ <gw\ > {lte\ > 应用-fw}	应用特定于运营商的固件

为 **LTE** 配置 **MCN**

您不能将 210-LTE 设备配置为 MCN。但是，要使 MCN 与 LTE 分支设备配合使用，请在 MCN 设备上执行以下配置。

要配置 MCN，请执行以下操作：

1. 登录到 SD-WAN 设备 GUI。转到配置编辑器。完成 MCN 站点的配置，请参阅 配置 MCN。
2. 确保提供可路由的公有 IP 地址作为 WAN 链接配置的一部分。您不必为客户端设备配置公有 IP 地址。

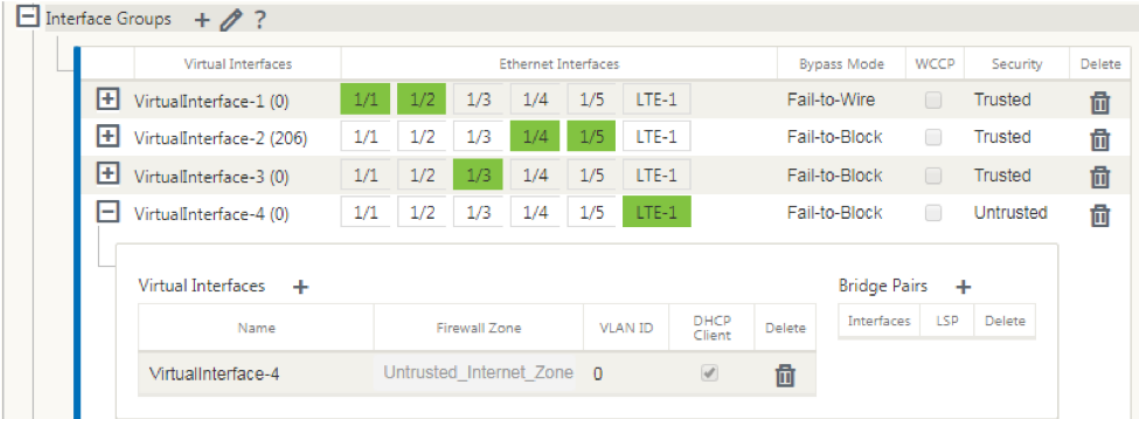


为 **LTE** 配置分支

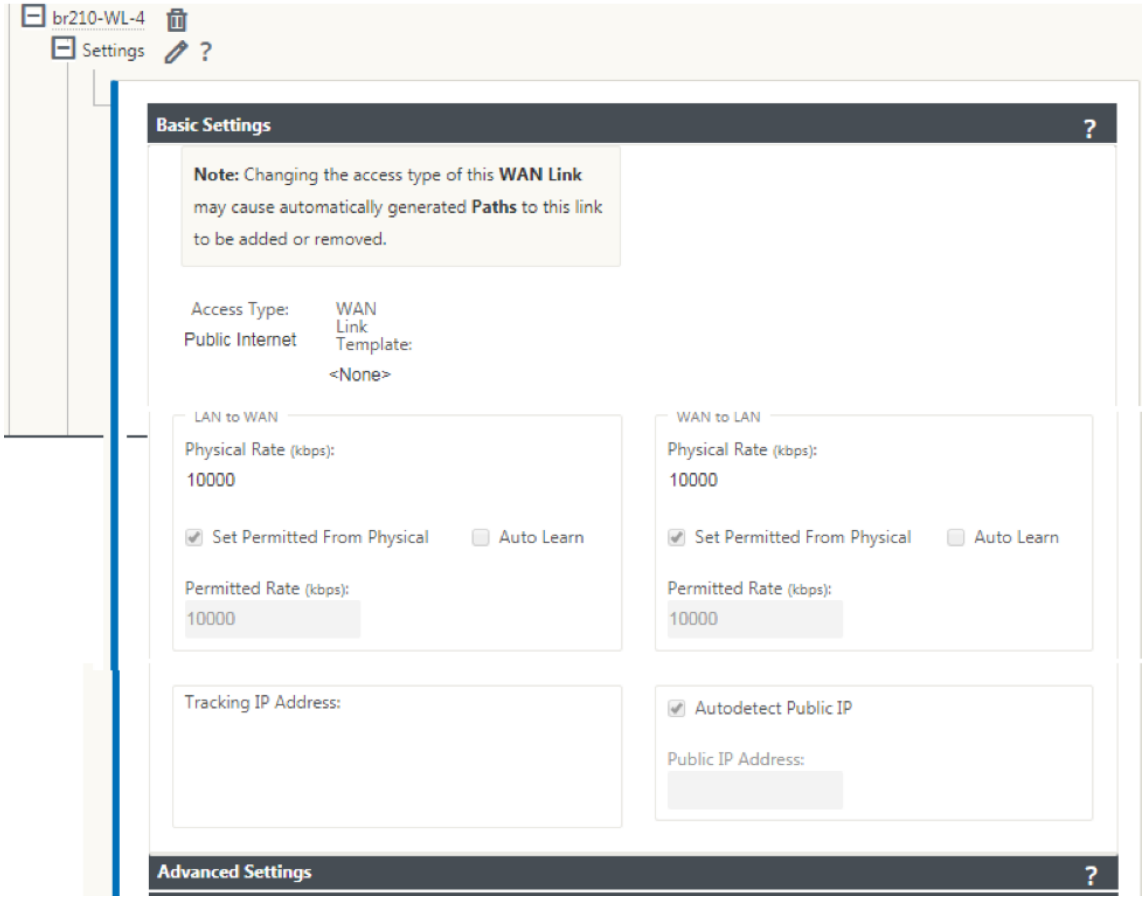
要将 210-SE LTE 设备配置为分支站点，请执行以下操作：

1. 在 SD-WAN 设备 GUI 中，转到配置编辑器。请参阅 配置分支。

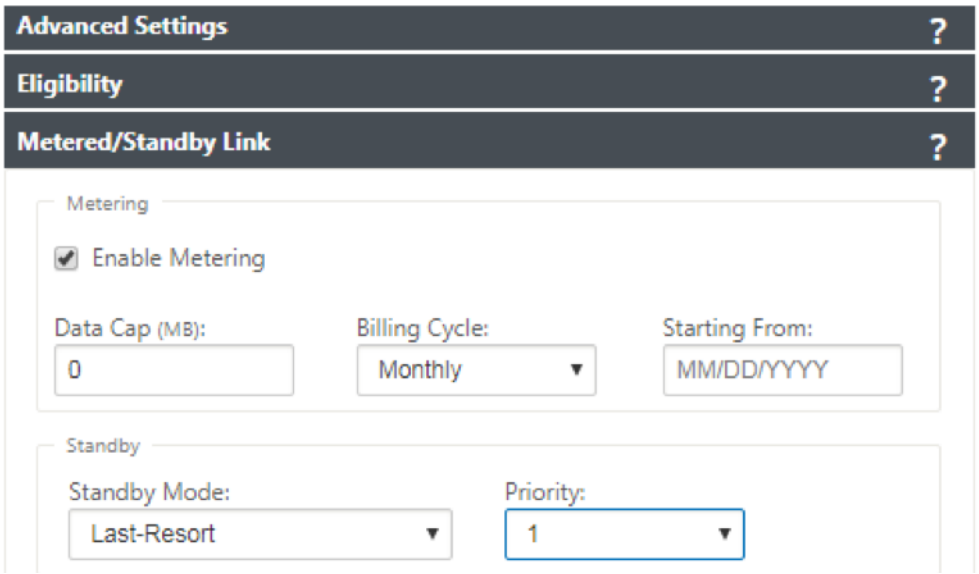
   - 创建接口组。
   - 通过选择以下选项，为 LTE 适配器创建最多一个虚拟接口和一个接口组以配置 WAN 链接：
     - 以太网接口—LTE 1
     - 安全性—不受信任（默认）
     - DHCP 客户端-已启用（默认）



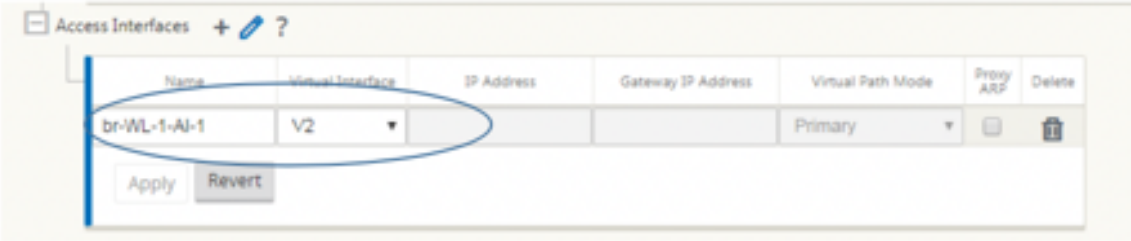
2. 使用为 LTE 接口创建的虚拟接口配置 WAN 链接时，启用 WAN 链接配置的 自动检测公共 **IP** 。



3. 默认情况下，当您尝试使用 LTE 接口配置 WAN 链接时，WAN 链接被标记为按流量计费的链接和最后手段待机模式。如有必要，您可以更改这些默认设置。



无需配置 WAN 链接的访问接口的 IP 地址和 Gateway 地址，因为它通过 DHCP 从运营商接收该信息。



4. 完成 210-SE LTE 设备所需的其余分支配置。请参阅 配置分支。
5. 通过上载 SD-WAN 软件来执行更改管理。请参阅 变更管理过程。
6. 通过本地更改管理过程激活配置。执行变更管理时，系统会激活配置并应用所需的配置。

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 接口定义的互联网服务。

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。

您可以使用 SD-WAN Center GUI 为零接触部署服务部署和配置 210-SE LTE 设备。

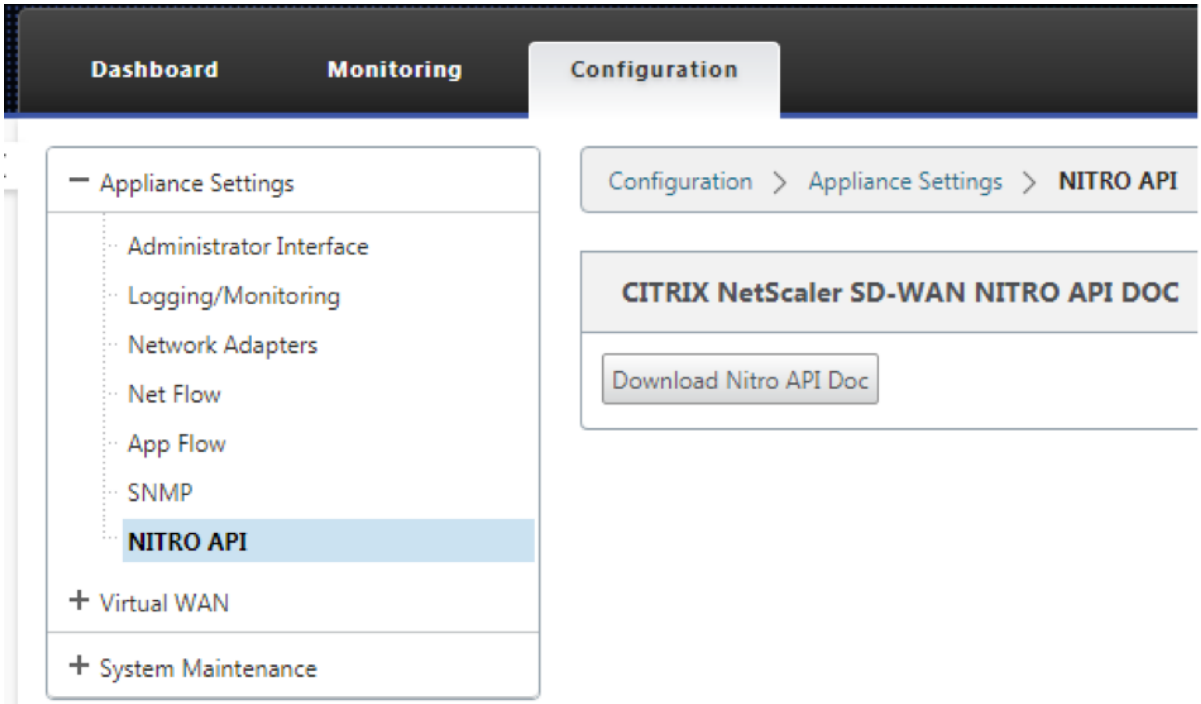
有关使用 SD-WAN Center 部署和配置 210-SE LTE 设备的更多信息，请参阅零接触部署过程 。

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

November 1, 2021

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。

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。

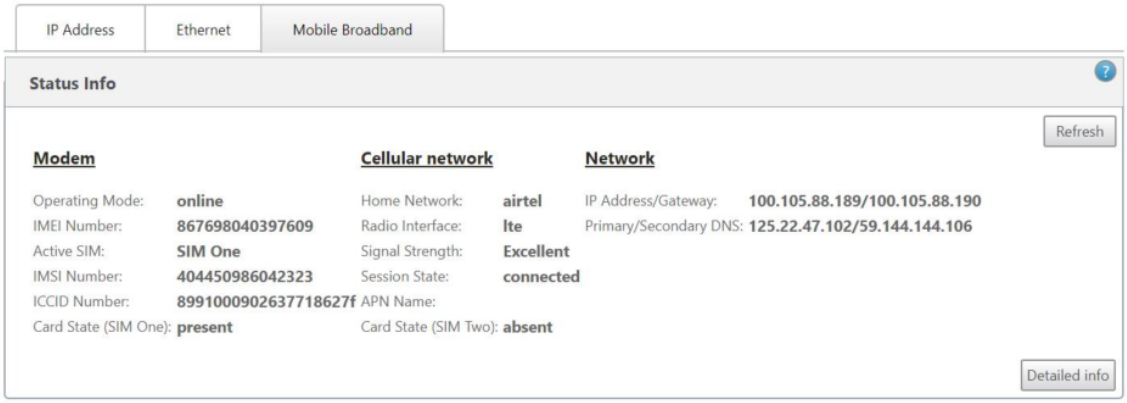
   > 注意
   >
   > 从运营商处获取 APN 信息。

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：

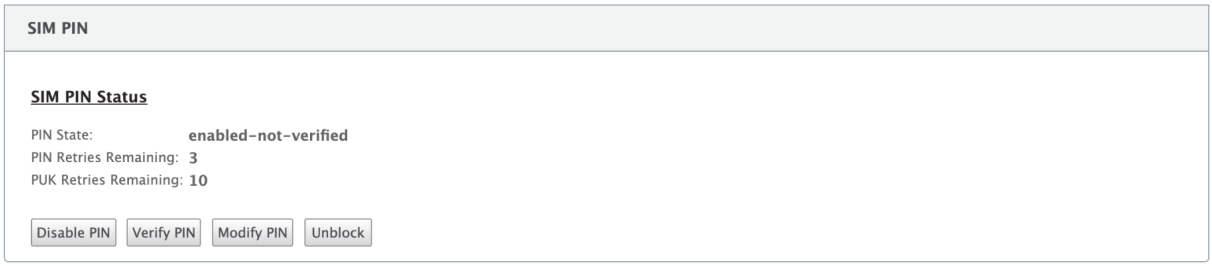
- 首选 **SIM One**：如果插入了两张 SIM 卡，则在启动时，LTE 调制解调器会使用 SIM One（如果可用）。LTE 调制解调器启动并运行时，它将使用当时可用的 SIM 卡（SIM 卡 1 或 SIM 卡 2）。它会继续使用它，直到 SIM 处于活动状态。
- 首选 **SIM 2**：如果插入两个 SIM 卡，则在启动时 LTE 调制解调器使用 SIM Two（如果可用）。LTE 调制解调器启动并运行时，它将使用当时可用的 SIM 卡（SIM 卡 1 或 SIM 卡 2）。它会继续使用它，直到 SIM 处于活动状态。
- **SIM One**：无论两个 SIM 卡插槽的 SIM 状态如何，都只使用 SIM One。SIM 卡一始终处于活动状态。
- **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

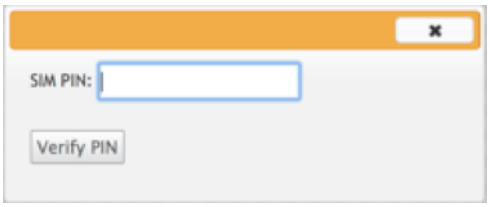
如果您插入了使用 PIN 锁定的 SIM 卡，则 SIM 卡状态为 启用未验证 状态。在使用 SIM 卡进行验证之前，您无法使用 SIM 卡。您可以从运营商处获取 SIM PIN。

> 注意
>
> SIM 卡 PIN 码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**。



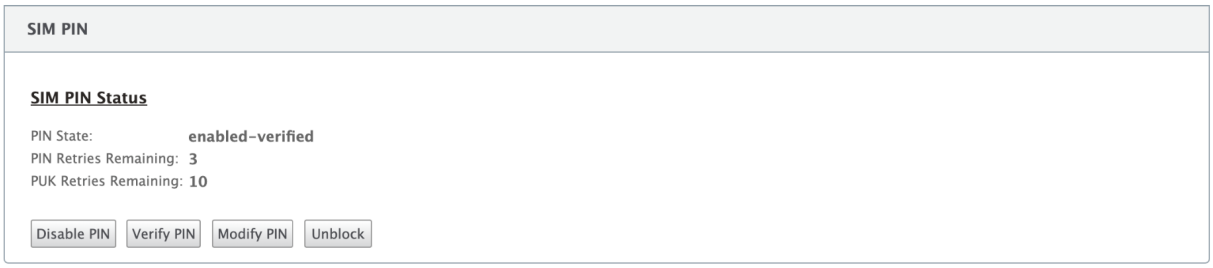
单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。



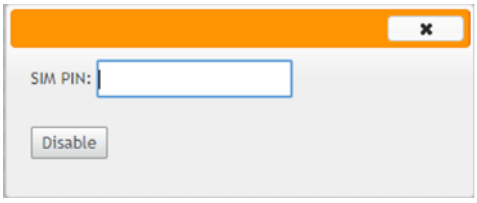
状态变为已 启用验证。

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。

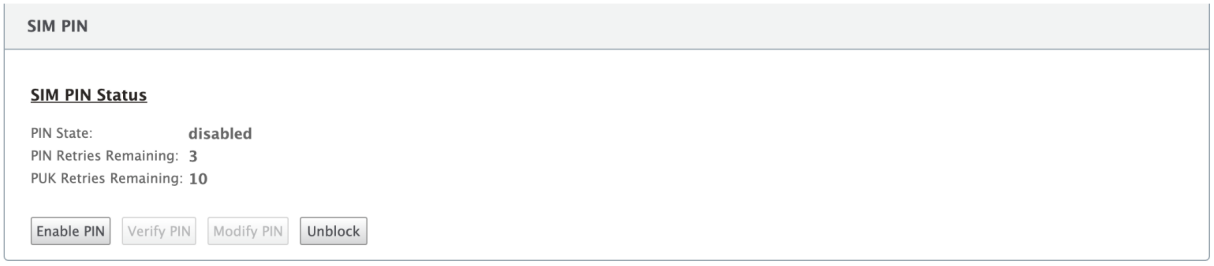


单击 禁用 **PIN**。输入 **SIM PIN** 码，然后单击 禁用。

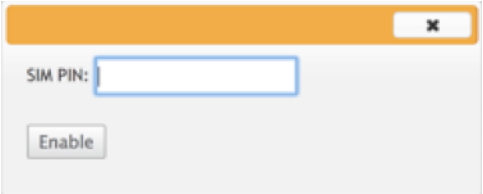


启用 **SIM PIN**

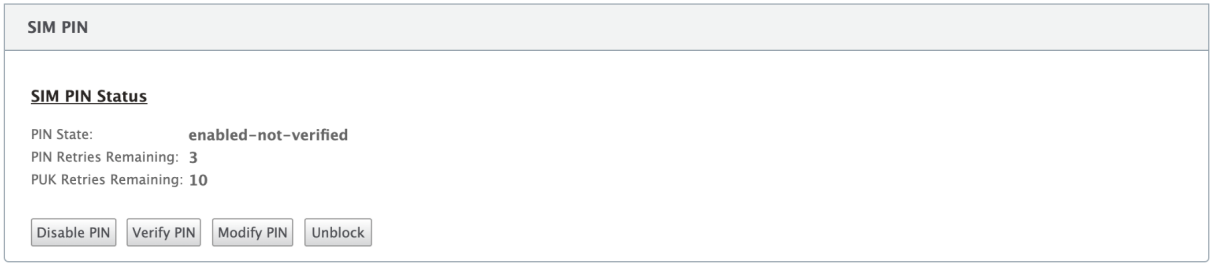
可以为禁用了 SIM PIN 的 SIM 启用 SIM PIN。



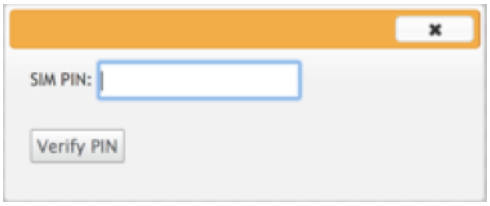
单击 启用 **PIN**。输入运营商提供的 SIM PIN，然后单击启用。



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。



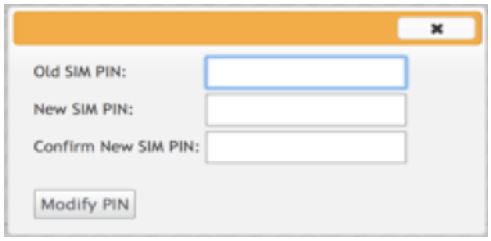
单击 验证 **PIN**。输入运营商提供的 SIM PIN，然后单击 验证 **PIN** 码。



修改 **SIM PIN**

PIN 处于 启用验证 状态后，您可以选择更改 PIN。

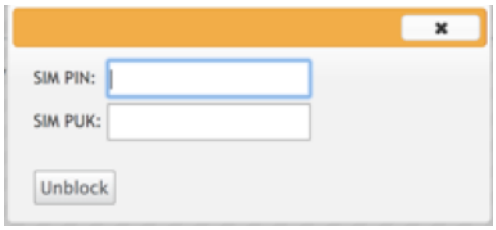
单击 修改 **PIN**。输入运营商提供的 SIM PIN。输入新的 SIM PIN 并进行确认。单击 修改 **PIN**。



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

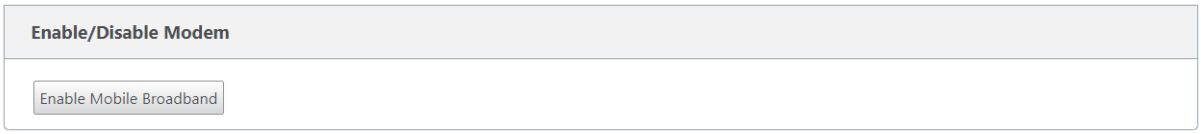
您可以在支持内部 LTE 调制解调器的 Citrix SD-WAN 设备上选择移动网络。支持的网络包括 3G、4G 或两者。

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。

可以使用 Citrix SD-WAN Center 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。

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 **>help**。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
Help {lte>help}	列出可用 LTE 命令和参数
Status {lte>status}	显示 LTE 连接状态
Show {lte>show}	显示 LTE 设置
Disable {lte>disable}	禁用 LTE 调制解调器
Enable {lte>enable}	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
选择 [1l2] [1l2] {lte> 选择 [1l2] [1l2]}	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
Reboot {lte>reboot}	重新启动 LTE 调制解调器

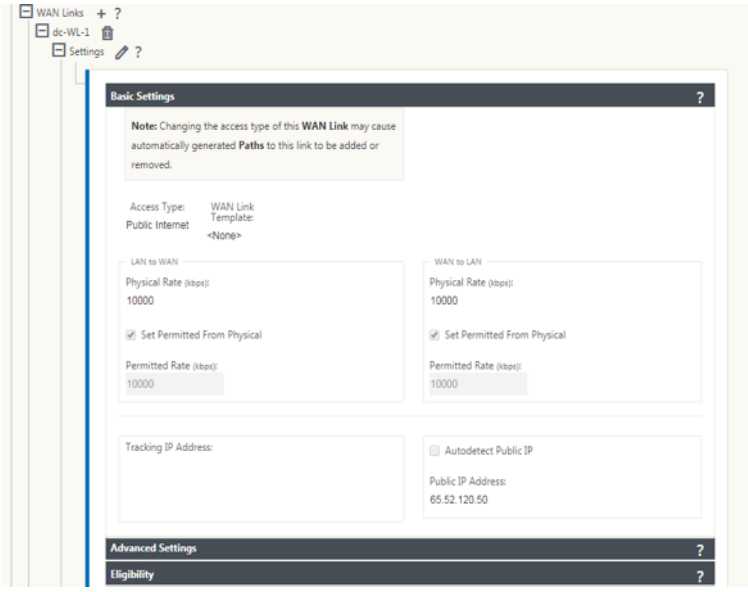
> 注意
>
> 110-LTE-WiFi 设备不支持与固件相关的操作。

为 **LTE** 配置 **MCN**

您不能将 110 轻型 WiFi 设备配置为 MCN。但是，要使 MCN 与 LTE 分支设备配合使用，请在 MCN 设备上执行以下配置。

要配置 MCN，请执行以下操作：

1. 登录到 SD-WAN 设备 GUI。转到配置编辑器。完成 MCN 站点的配置，请参阅 配置 MCN。
2. 确保在 WAN 链接配置中提供可路由的公有 IP 地址。您不必为客户端设备配置公有 IP 地址。

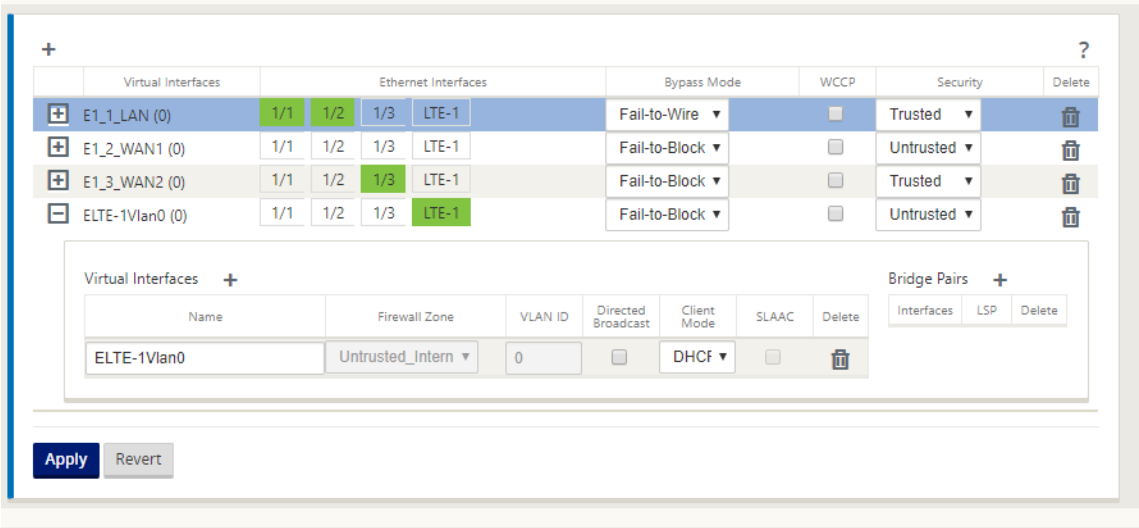


为 **LTE** 配置分支

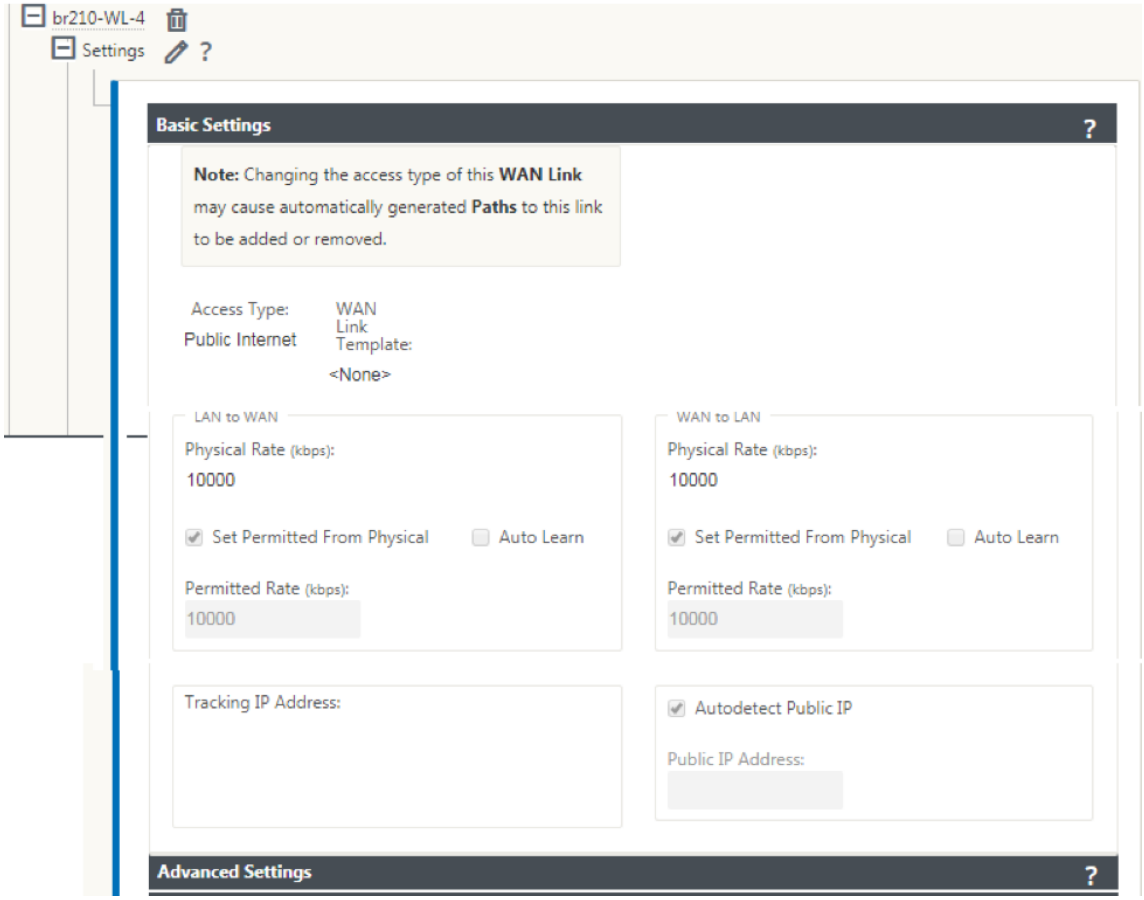
要将 110-LTE-WiFi 设备配置为分支站点，请执行以下操作：

1. 在 SD-WAN 设备 GUI 中，转到配置编辑器。请参阅 配置分支。

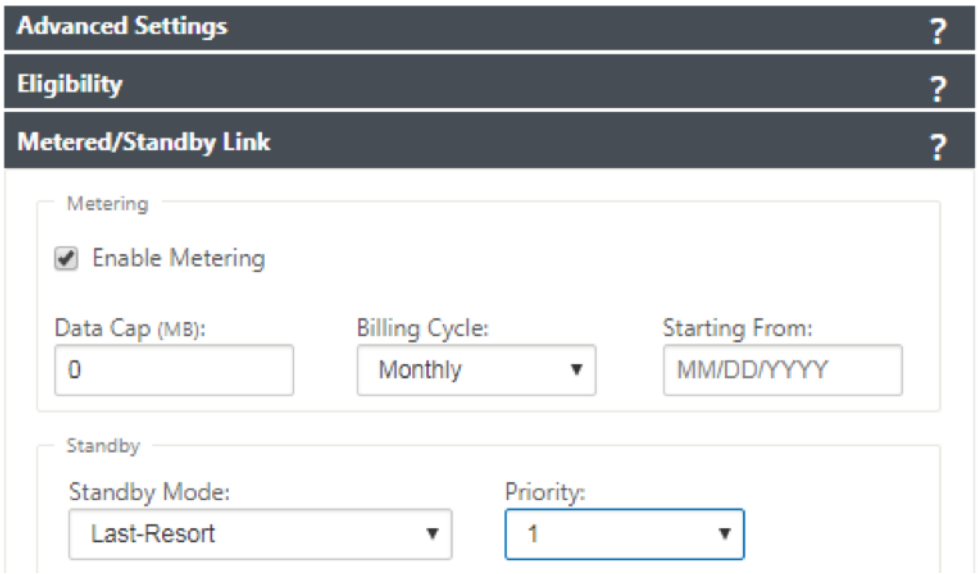
   - 创建接口组。
   - 通过选择以下选项，为 LTE 适配器创建最多一个虚拟接口和一个接口组以配置 WAN 链接：
     - 以太网接口—LTE 1
     - 安全性—不受信任（默认）
     - DHCP 客户端-已启用（默认）



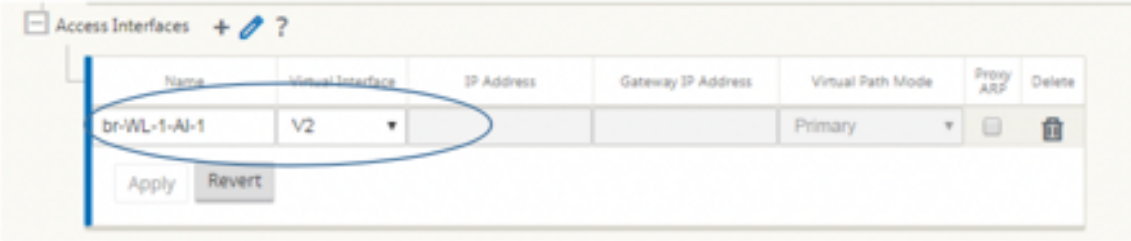
2. 使用为 LTE 接口创建的虚拟接口配置 WAN 链接时，启用 WAN 链接配置的 自动检测公共 **IP** 。



3. 默认情况下，当您尝试使用 LTE 接口配置 WAN 链接时，WAN 链接被标记为按流量计费的链接和最后手段待机模式。如有必要，您可以更改这些默认设置。



无需配置 WAN 链接的访问接口的 IP 地址和 Gateway 地址，因为它通过 DHCP 从运营商接收该信息。



4. 完成 110-LTE-WiFi 设备所需的其余分支配置。请参阅 配置分支。
5. 通过上载 SD-WAN 软件来执行更改管理。请参阅 变更管理过程。
6. 通过本地更改管理过程激活配置。执行变更管理时，系统会激活配置并应用所需的配置。

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 接口定义的互联网服务。

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。

您可以使用 SD-WAN Center GUI 为零接触部署服务部署和配置 110-LTE-WiFi 设备。

有关使用 SD-WAN Center 部署和配置 110-LTE-WiFi 设备的更多信息，请参阅零接触部署过程 。

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

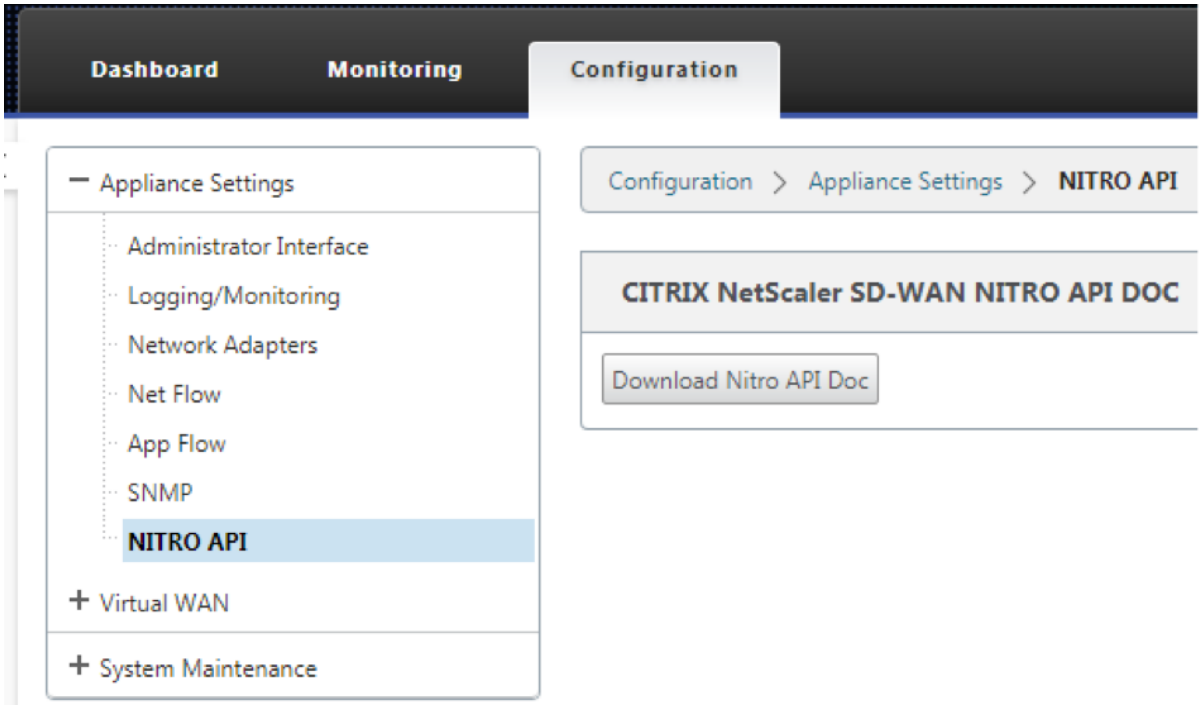
不受支持的平台

以下 SD-WAN 设备不支持第 0 天配置和第 N 天管理：

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

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

November 1, 2021

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 /AE
- 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 /PE /AE
- Citrix SD-WAN 2100 SE /PE

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。

以下设备不支持外部 USB 调制解调器：

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

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

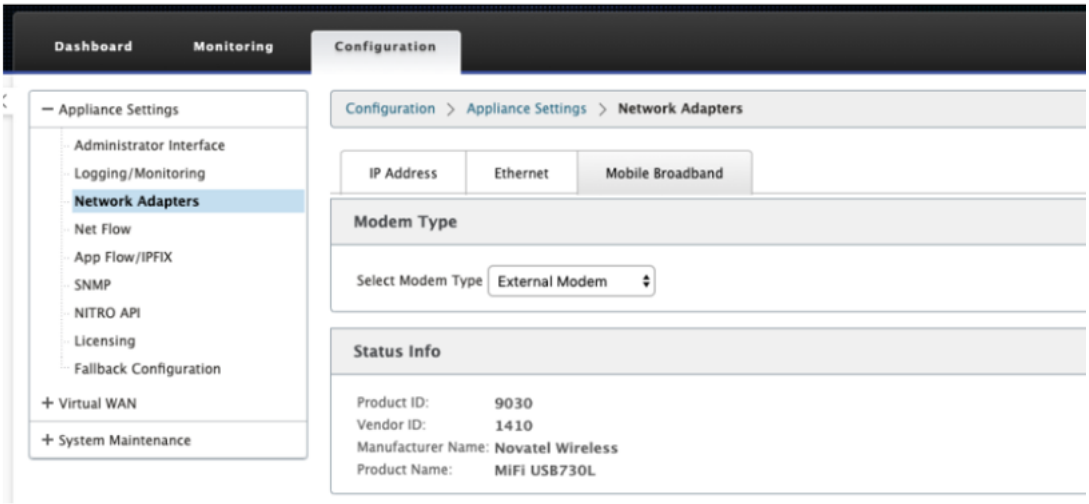
根据无线运营商提供的指南启用和测试 USB 调制解调器。

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，并确保互联网正常工作，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

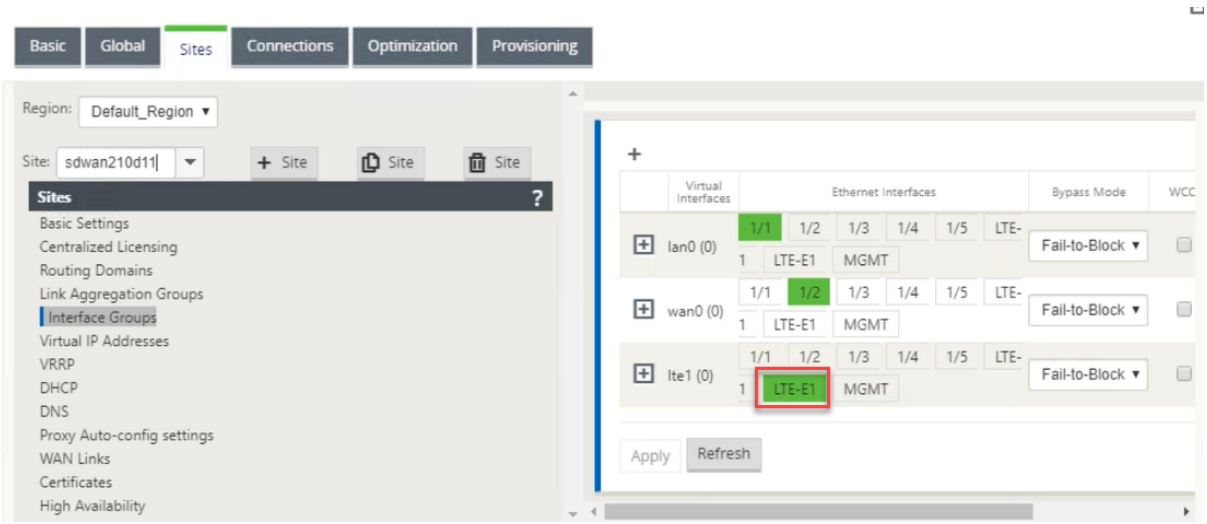
CDC 以太网和 MBIM /NCM 外部调制解调器支持的操作：

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

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。

配置外部 **USB** 调制解调器

要配置外部 USB 调制解调器，请在配置编辑器中导航到站点，选择一个站点，然后单击 接口组。外部 USB 调制解调器接口 LTE-E1 可供配置。有关为 LTE 配置分支的更多信息，请参阅 为 LTE 配置分支。



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 接口定义的互联网服务。

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。

使用 SD-WAN 中心 GUI 为零接触部署服务部署和配置设备。有关更多信息，请参阅 零接触部署。
有关通过 SD-WAN Orchestrator 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。

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

June 22, 2021

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
- 利用高级版设备仅提供 WAN 优化服务
- 双盒模式
- 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 标准和高级（企业）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

June 22, 2021

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互联网。
- 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互联网连接的网桥对绕过 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：

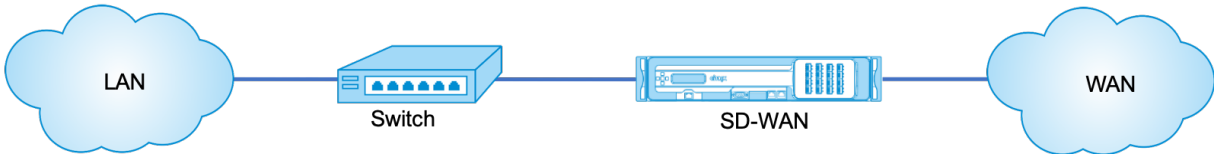
- 必须适当注意将定义的 WAN 链路的 SD-WAN 逻辑 VIP 明确地映射到正确的物理接口（否则，这可能会导致 WAN 指标评估和 WAN 路径选择中出现不良问题）。
- 要知道所有流量是通过 SD-WAN 还是仅通过特定流量转移，需要进行适当的设计考虑。
- 这意味着 SD-WAN 必须专门用于自身的一些带宽份额，这些带宽必须在接口上设置，以便 SD-WAN 的容量不会被其他非 SD-WAN 流量使用，从而导致不良后果。
  - 如果 SD-WAN 链路容量定义不正确，则可能会出现带宽记帐问题和拥塞问题。
- 如果设计不当，如果 SD-WAN 路由数据中心和分支 VIP 导出到前端，并且如果路由受到到 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

June 22, 2021

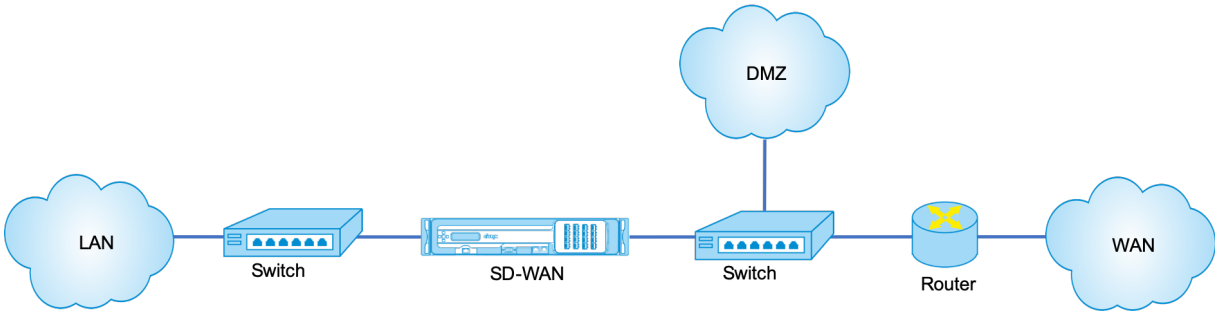
Gateway 模式将 SD-WAN 设备置于路径中（双臂部署），并且需要对现有网络基础结构进行更改，以使 SD-WAN 设备成为该站点整个 LAN 网络的默认网关。Gateway mode used for new networks and router replacement. 网关模式允许 SD-WAN 设备：

- 查看进出 WAN 的所有流量
- 执行本地路由



> 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。

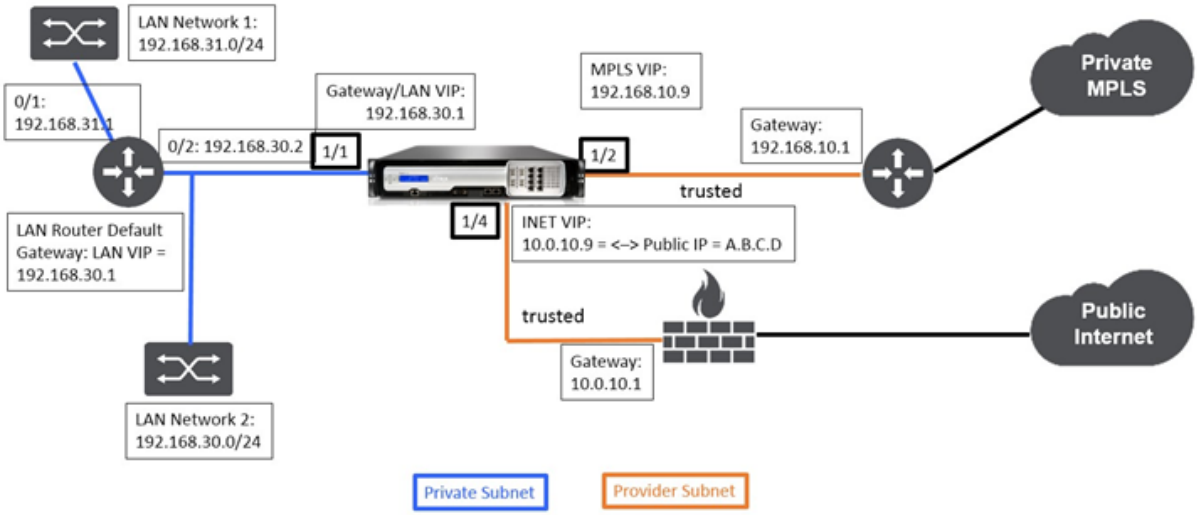


本文提供了在示例网络设置中在网关模式下配置 SD-WAN 设备的分步过程。还介绍了内联部署，以便分支端完成配置。如果删除了内联设备，网络可以继续运行，但如果删除网关设备，则会失去所有访问权限。

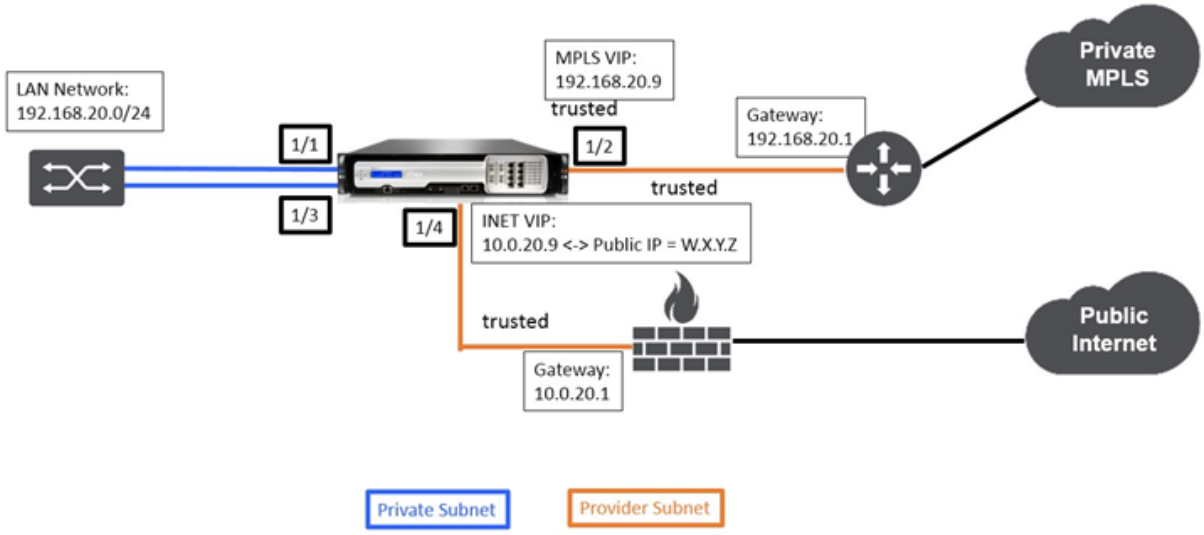
拓扑

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



部署所需资源

下面介绍了部署要求和相关信息，以帮助您构建配置。

站点名称	数据中心站点	分支机构
设备名称	A_DC1	A_BR1
管理知识产权	172.30.2.10/24	172.30.2.20/24
安全密钥	如果有	如果有
模型/版本	4000	2000
模式	网关	内联
拓扑	2 x 广域网路径	2 x 广域网路径
VIP 地址	192.168.10.9/24 –MPLS，10.0.10.9/24 –Internet（公共 IP – A.B.C.D），192.168.30.1/24 - LAN	192.168.20.9/24 - MPLS，10.0.20.9/24 –Internet（公共 IP – W.X.Y.Z）
网关 MPLS	192.168.10.1	192.168.20.1
网关 Internet	10.0.10.1	10.0.20.1
链接速度	MPLS –100 Mbps，Internet –20 Mbps	MPLS –10 Mbps，Internet –2 Mbps
路由	网络 IP 地址-192.168.31.0/24，服务类型-本地，网关 IP 地址-192.168.30.2	如果有

站点名称	数据中心站点	分支机构
VLAN	如果有	如果有

配置先决条件

- 将 SD-WAN 设备启用为主控制节点。
- 配置仅在 SD-WAN 设备的主控制节点 (MCN) 上完成。

要将设备启用为主控制节点，请执行以下操作：

1. 在 SD-WAN Web 管理界面中，导航到 配置 **>** 设备设置 > 管理 员界面 > 杂项选项卡 > 切换控制台。

   > 注意
   >
   > 如果显示“切换到客户端控制台”，则说明设备已处于 MCN 模式。SD-WAN 网络中只能有一个活动的 MCN。

2. 通过导航到配置 > 虚拟 **WAN** > 配置编辑器启动配置。单击“新建”开始配置。

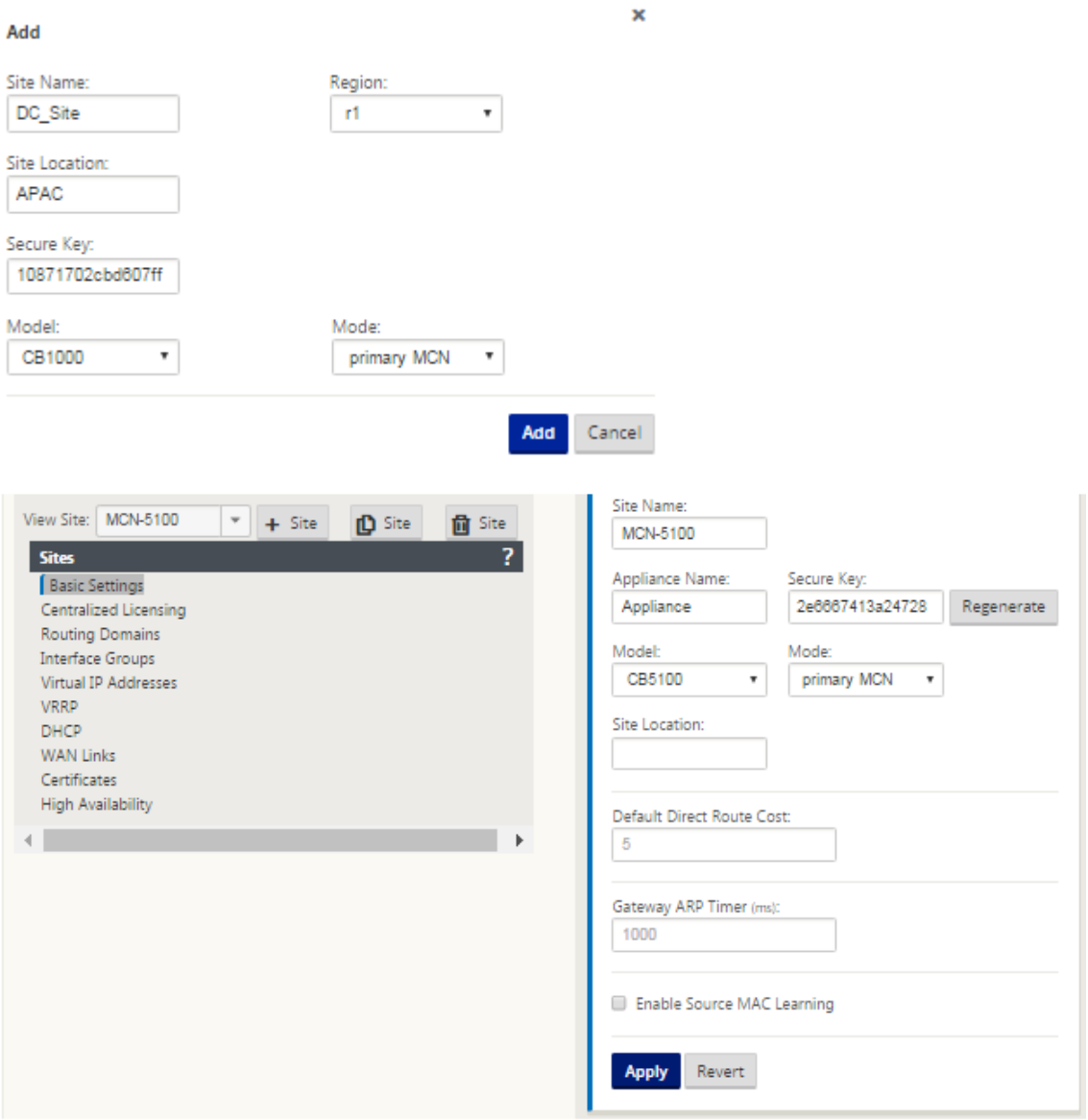
数据中心站点 **Gateway** 模式配置

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。

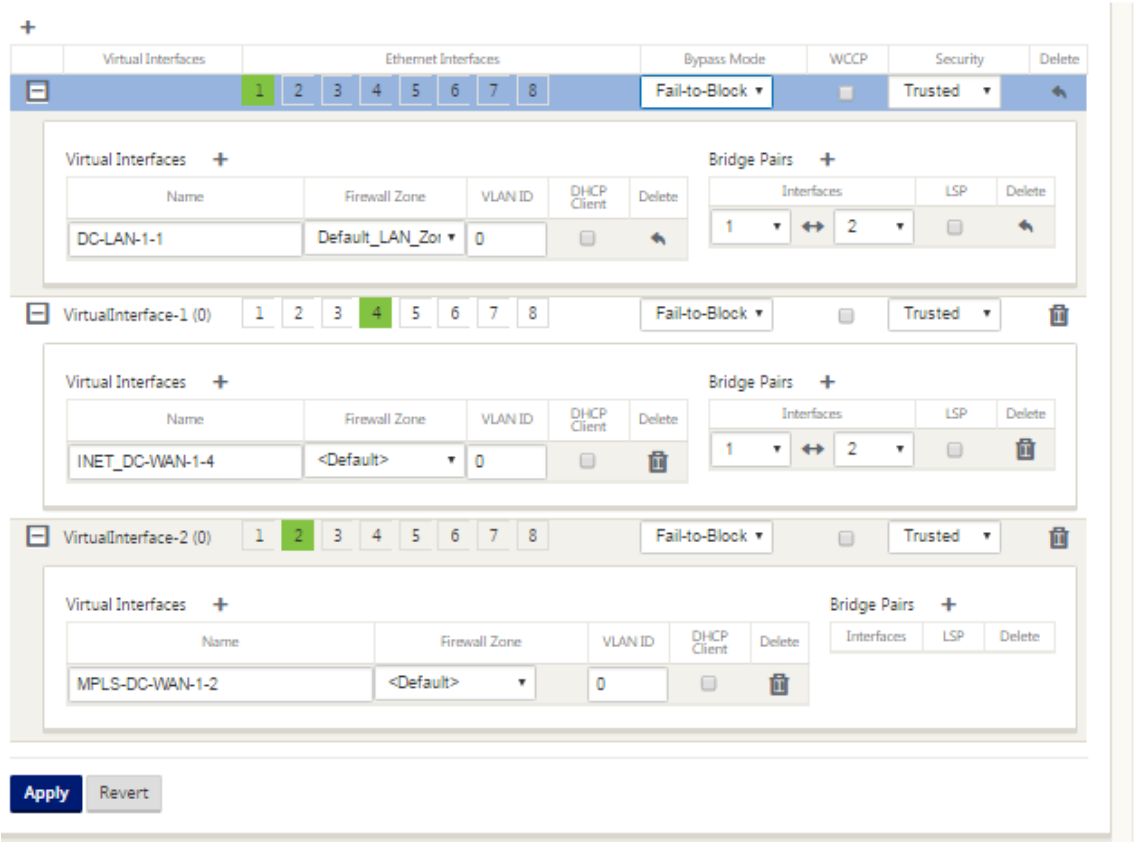
创建 **DC** 站点

1. 导航到 配置编辑器 > 站点，然后单击 **+** 添加 按钮。
2. 填充字段，如下所示。
3. 保留默认设置，除非要求更改。



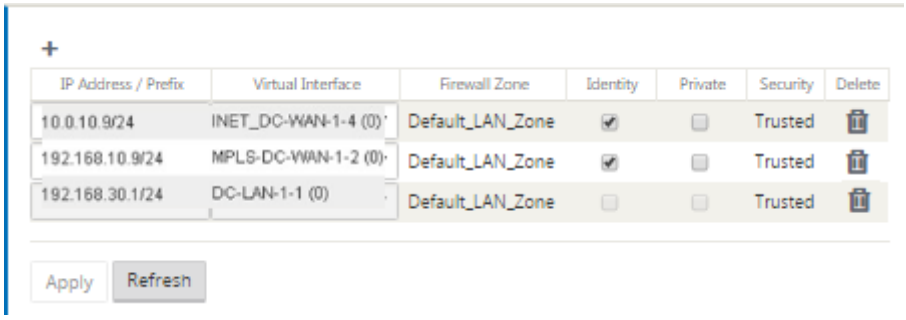
基于连接的以太网接口配置接口组

1. 在 配置编辑器中，导航到 站点 > 查看站 点 > [站点名称] > 界面组。单击 + 以 添加要使用的接口。对于网关模式，为每个接口组分配一个以太网接口。
2. 旁路模式设置为 故障到阻塞，因为每个虚拟接口只使用一个以太网/物理接口。也没有桥梁对。
3. 在此示例中，创建了三个接口组，一个面向 LAN，另外两个面向每个相应的 WAN 链接。请参阅上面的示例 “DC 网关模式” 拓扑并填充接口组字段，如下所示。



为每个虚拟接口创建虚拟 **IP (VIP)** 地址

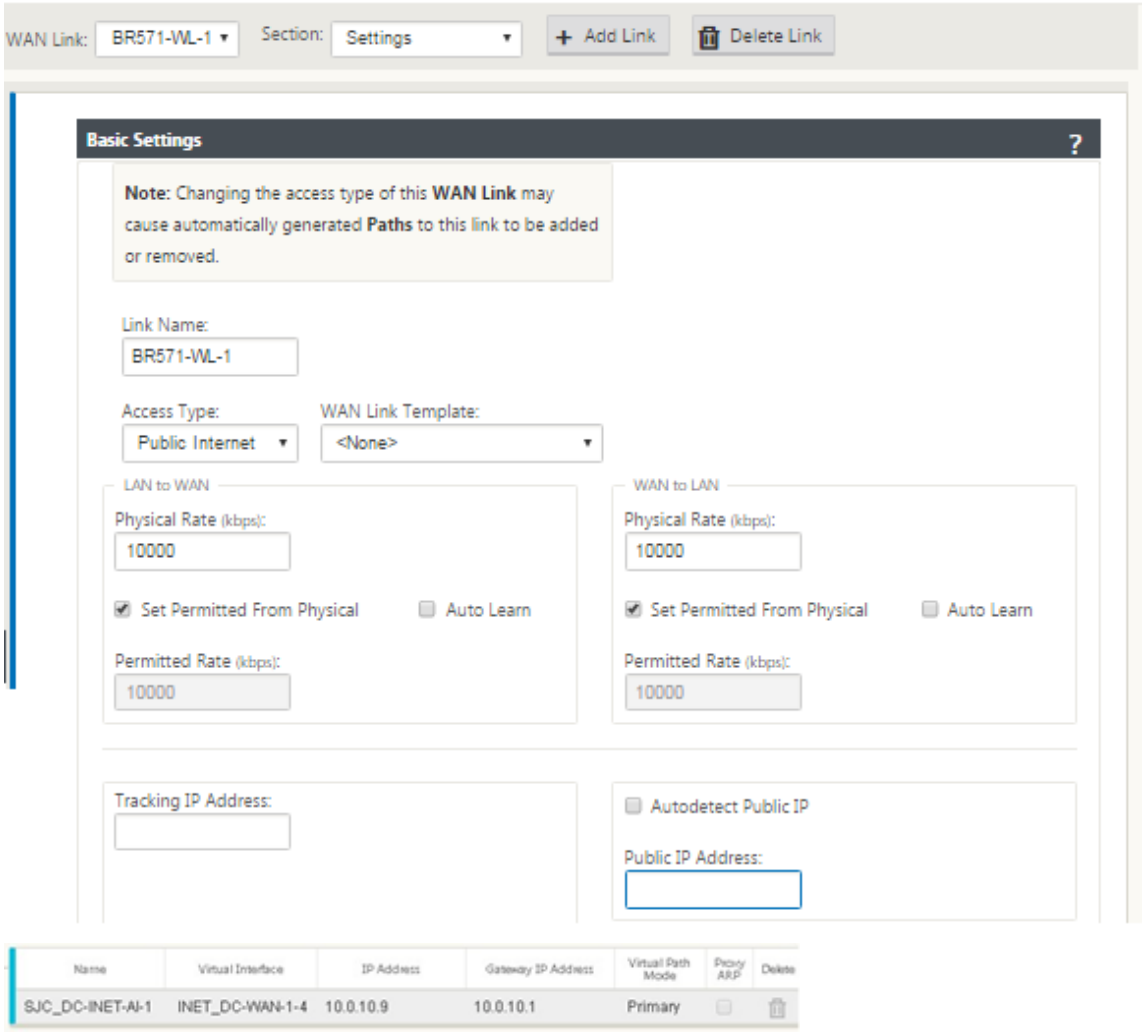
1. 在适当的子网上为每个 WAN 链接创建 VIP。VIP 用于虚拟 WAN 环境中的两个 SD-WAN 设备之间的通信。
2. 创建一个虚拟 IP 地址，用作 LAN 网络的网关地址。



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：

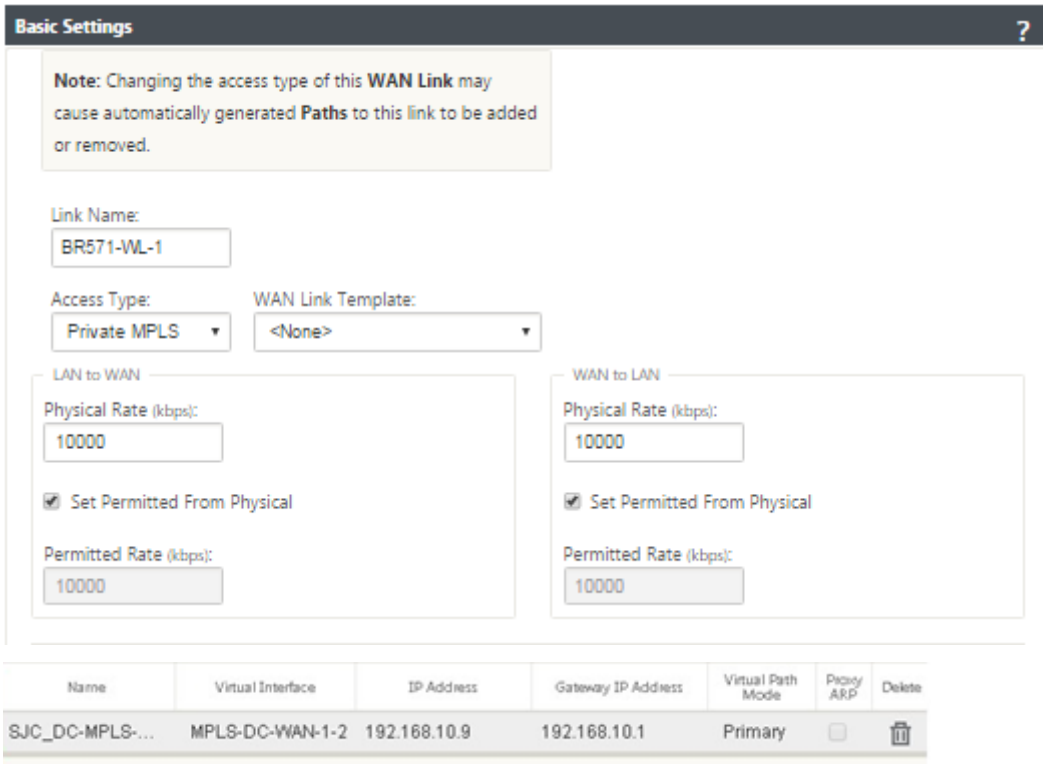
1. 导航到 **WAN** 链接，单击 **+** 添加链接 按钮为 Internet 链接添加 WAN 链接。
2. 填充互联网链接详细信息，包括提供的公有 IP 地址，如下所示。无法为配置为 MCN 的 SD-WAN 设备选择自动检测 公有 **IP**。
3. 从部分下拉菜单导航到 访问界面，然后单击 **+** 添加按钮以添 加特定于 Internet 链接的界面详细信息。

4. 填充 IP 和 Gateway 地址的访问接口，如下所示。



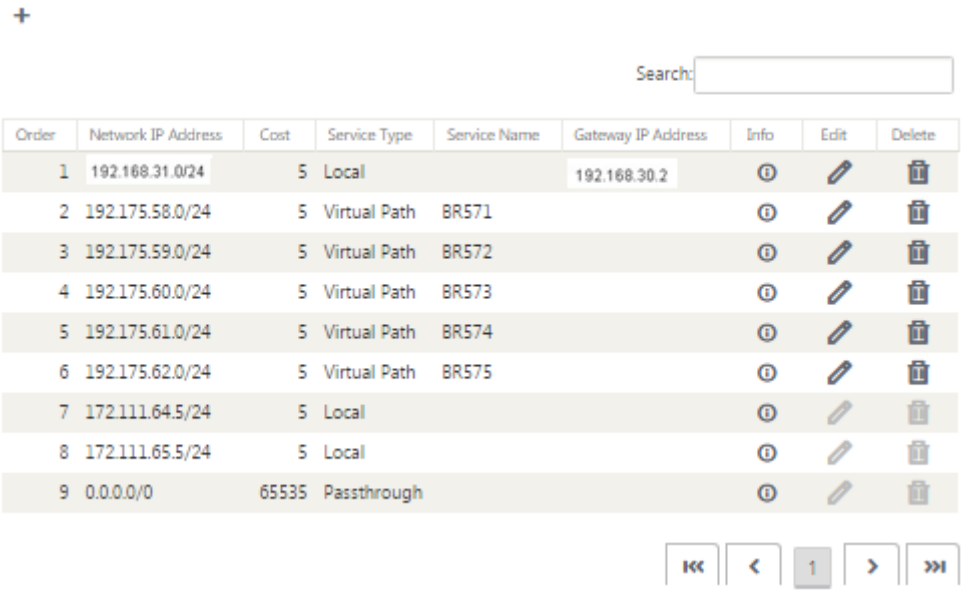
创建 **MPLS** 链接

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 访问界面，单击 **+** 按钮以添加 MPLS 链接特定的界面详细信息。
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。上面显示的直流局域网示例拓扑具有额外的局域网子网，该子网为 **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。



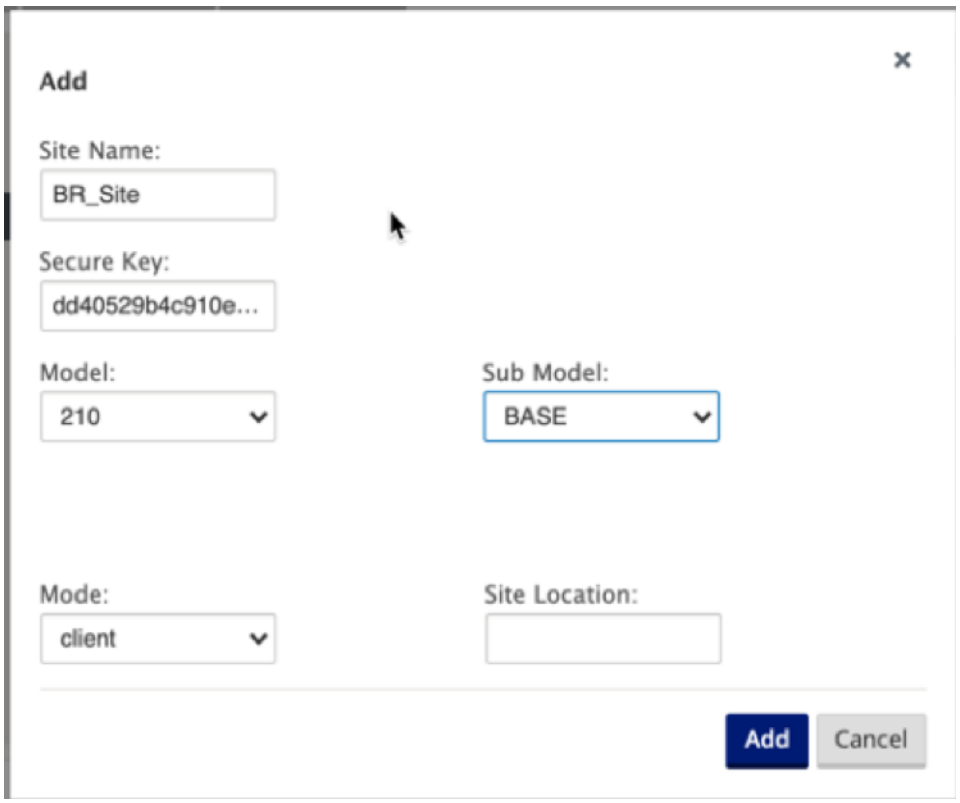
分支站点内联部署配置

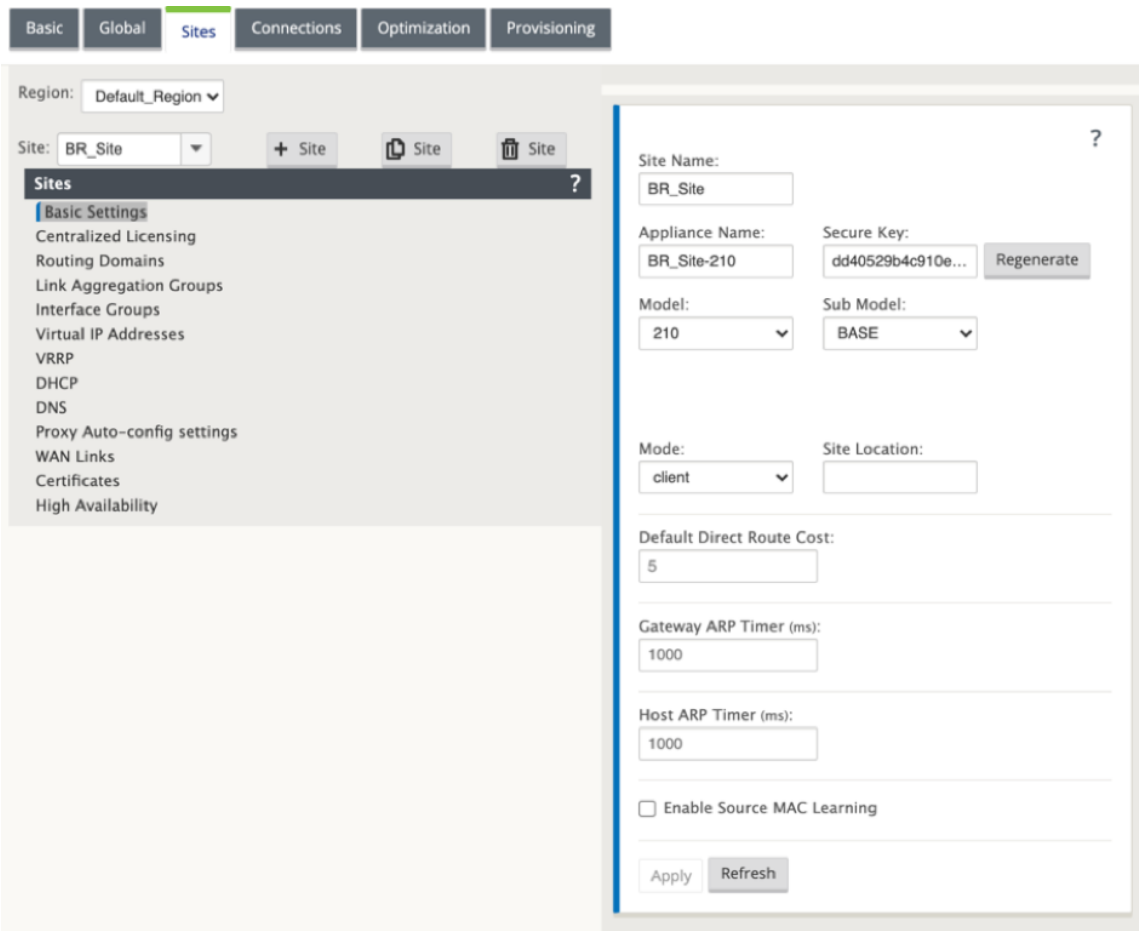
以下是为内联部署配置分支站点的高级配置步骤：

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。

创建分支站点

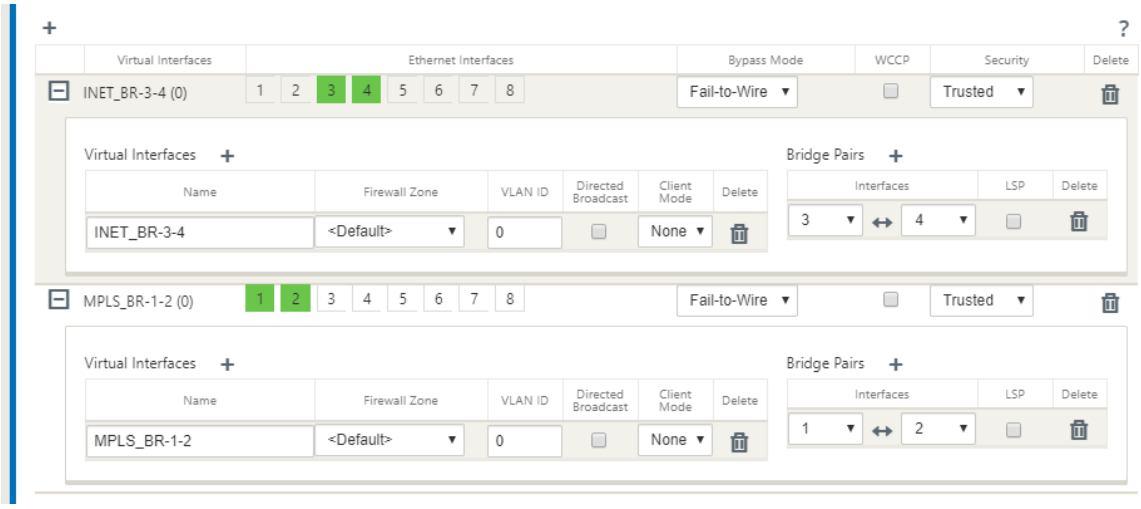
1. 导航到 配置编辑器 > 站点，然后单击“**+**”添加 按钮。
2. 填充字段，如下所示。
3. 保留默认设置，除非要求更改。





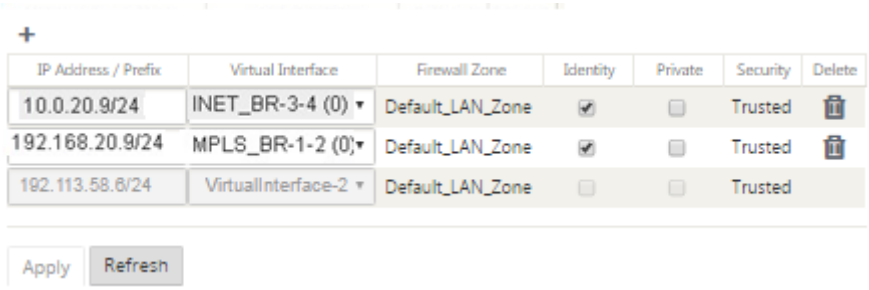
基于连接的以太网接口填充接口组

1. 在 配置编辑器中，导航到 站点 > 查看站 点 > **[**客户端站点名称**]** > 界面组。单击 **+** 以 添加要使用的接口。对于内联模式，为每个接口组分配两个以太网接口。
2. 旁路模式设置为 故障到线，网桥对是使用两个以太网接口创建的。
3. 请参阅上述示例 远程站点内联模式 拓扑并填充接口组字段，如下所示。



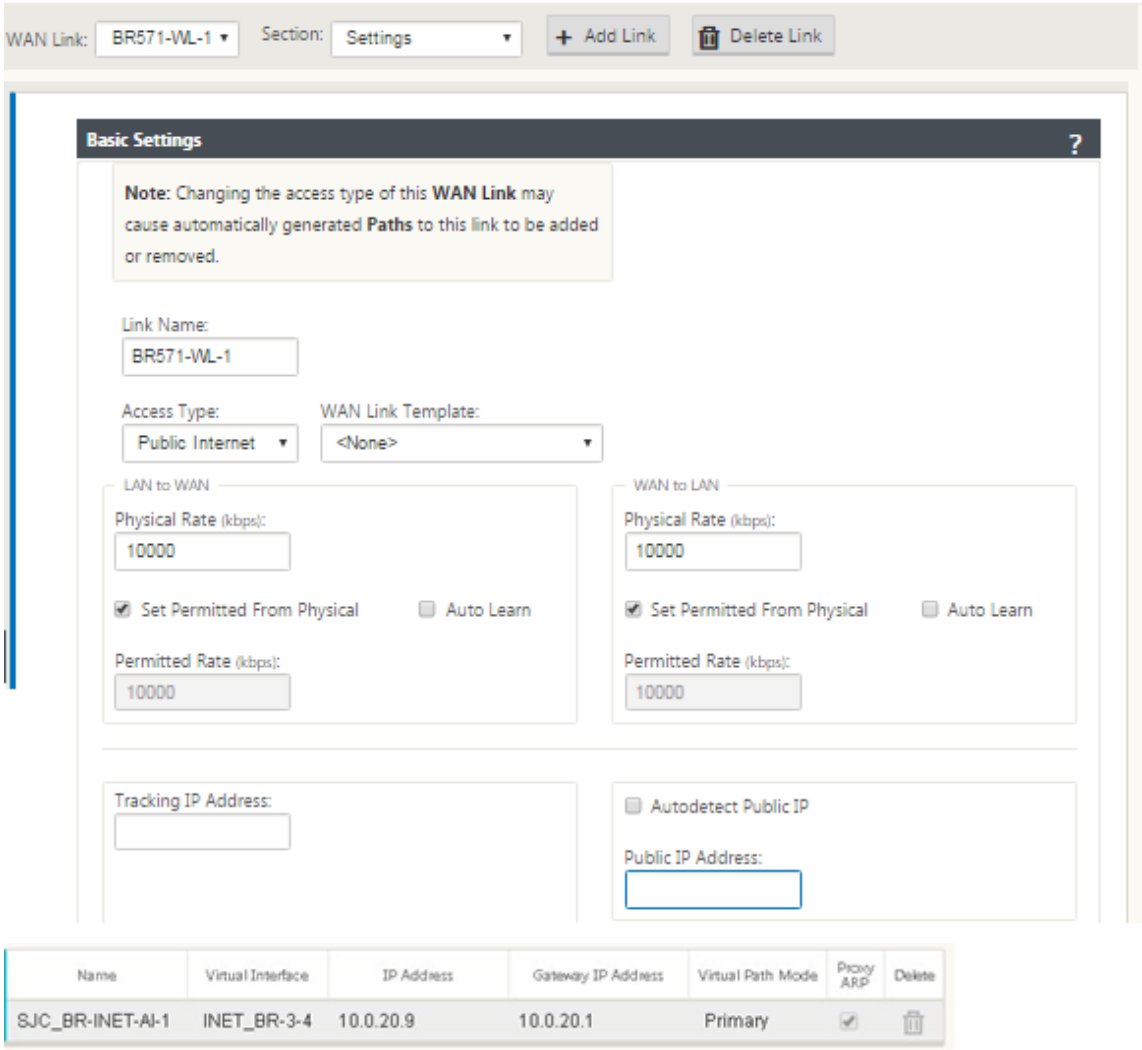
为每个虚拟接口创建虚拟 **IP (VIP)** 地址

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。



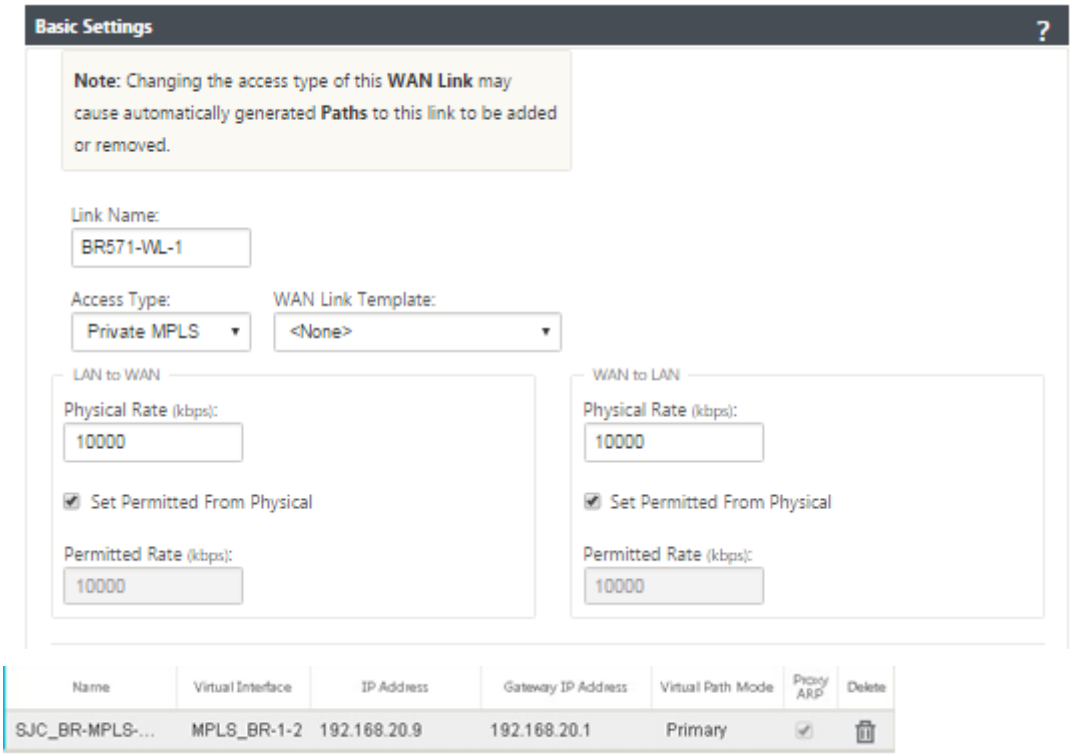
要使用 Internet 链路根据物理速率而不是突发速度填充 WAN 链路，请执行以下操作：

1. 导航到 **WAN** 链接，单击 **+** 按钮为 Internet 链接添加 WAN 链接。
2. 填充互联网链接详细信息，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。



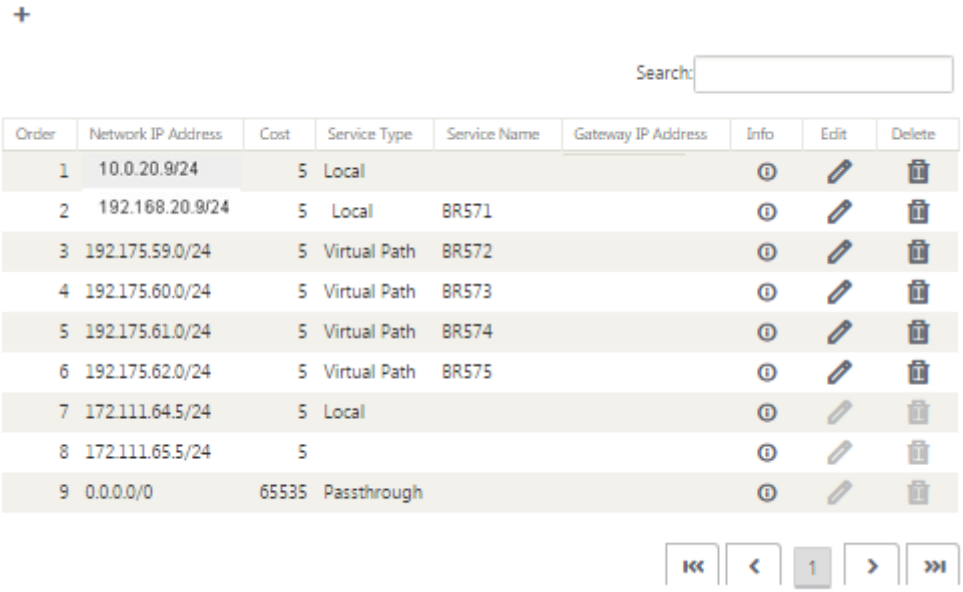
创建 **MPLS** 链接

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

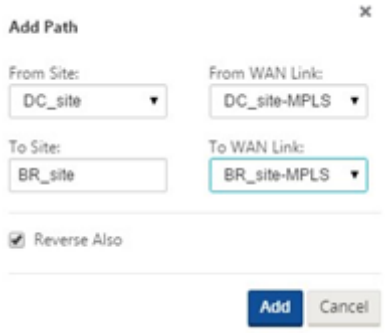
路由是基于上述配置自动创建的。如果有更多的子网特定于此远程分支机构，则需要添加特定的路由，以确定哪个 Gateway 将流量引导到达这些后端子网。



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。



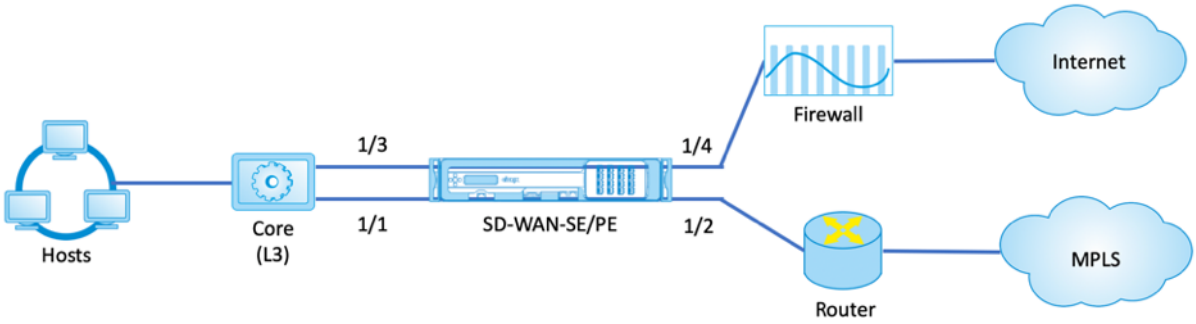
完成上述所有步骤后，继续准备 SD-WAN 设备包。

内联模式

June 22, 2021

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。



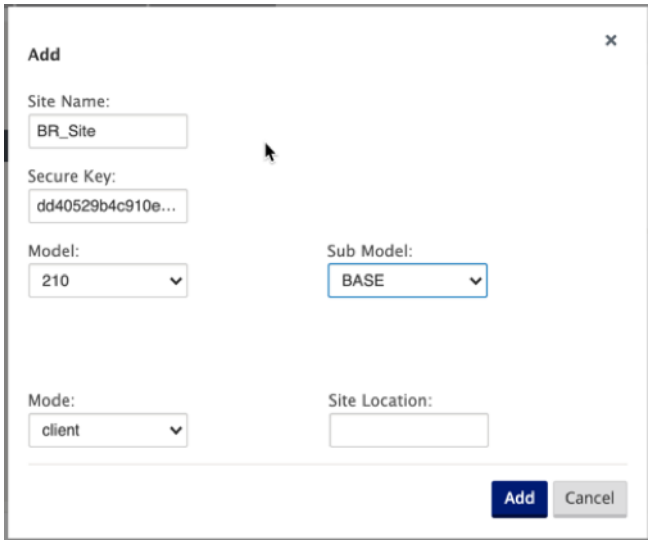
分支站点内联部署配置

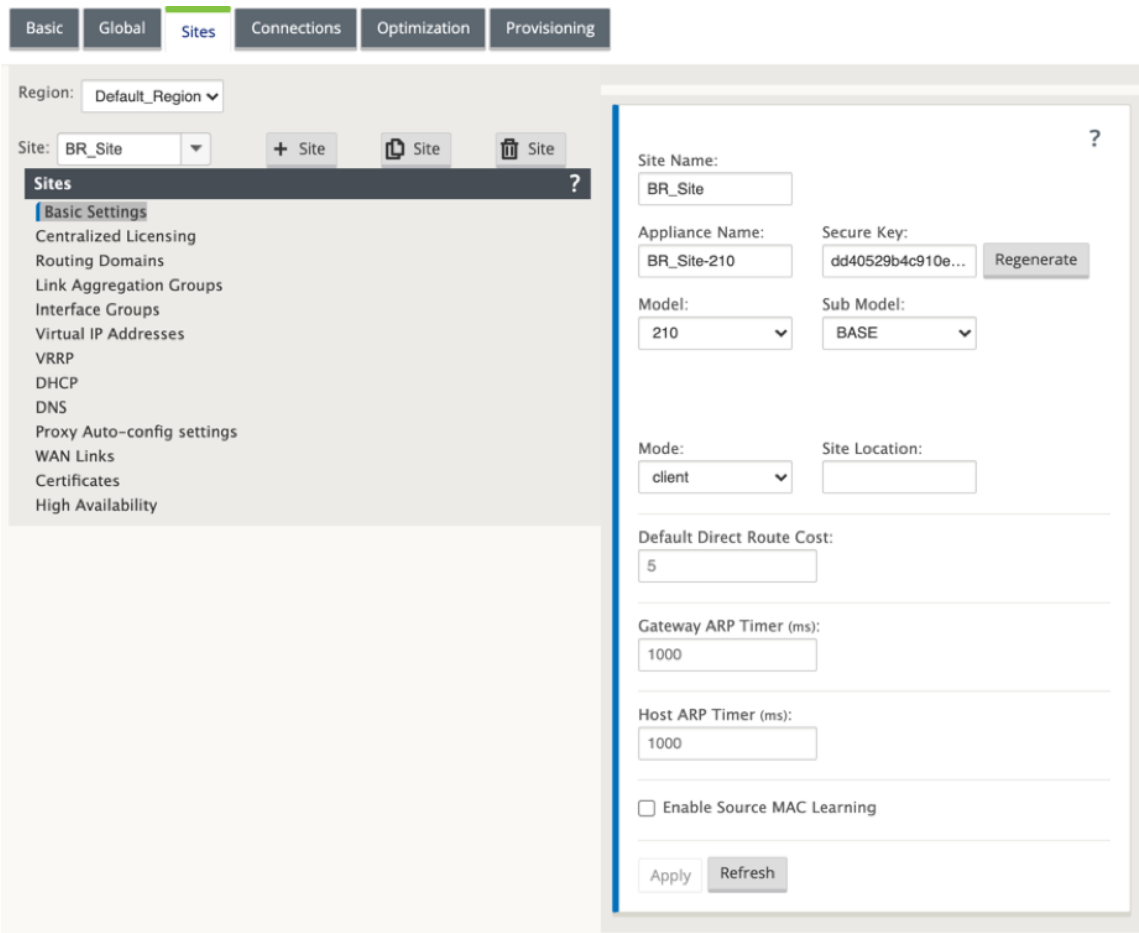
以下是为内联部署配置分支站点的高级配置步骤：

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。

创建分支站点

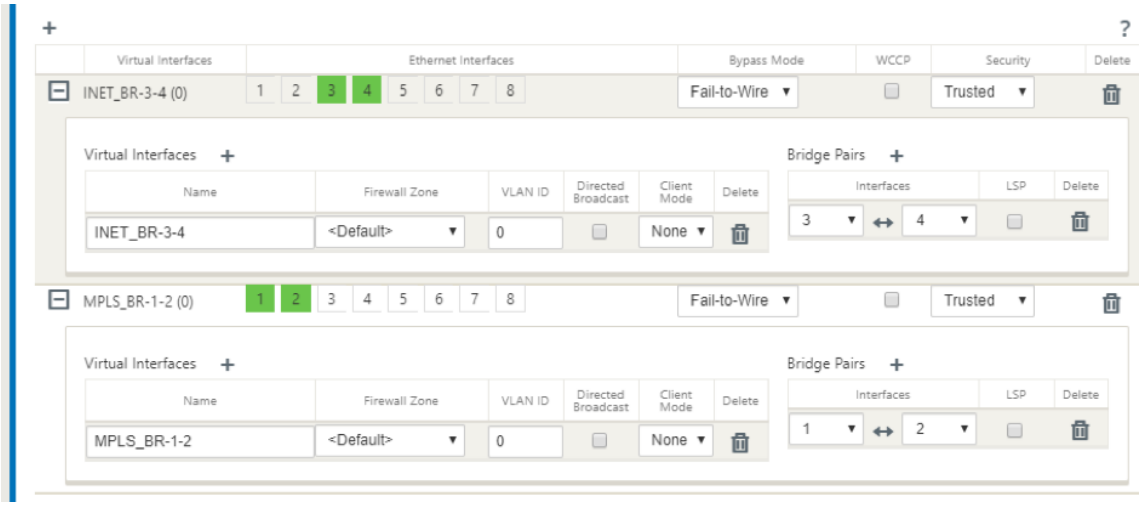
1. 导航到配置编辑器 **>** 站点，然后单击 **+** 添加按钮。
2. 保留默认设置，除非要求更改。





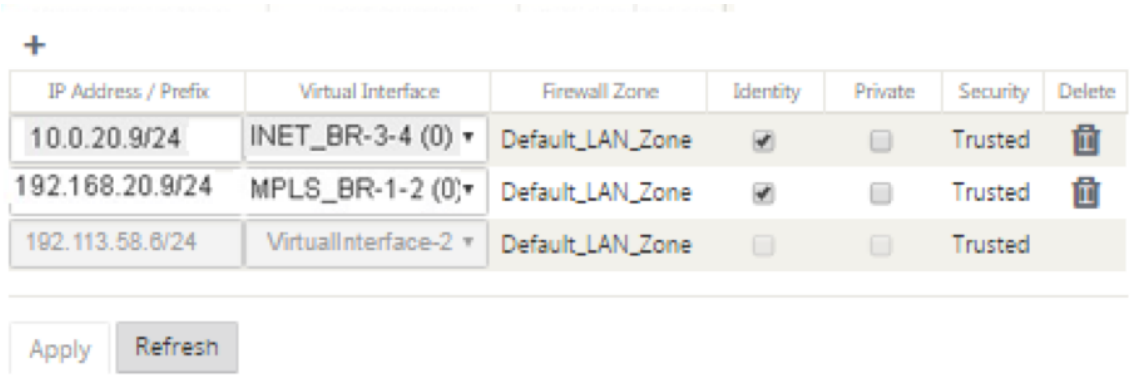
基于连接的以太网接口填充接口组

1. 在配置编辑器中，导航到 站点 **>** 查看站点 **> [**客户端站点名称**] >** 接口组。单击 **+** 以 添加要使用的接口。对于内联模式，为每个接口组分配两个以太网接口。
2. 旁路模式设置为 故障到线，网桥对是使用两个以太网接口创建的。
3. 请参阅上面的示例拓扑并填充接口组字段，如下所示。



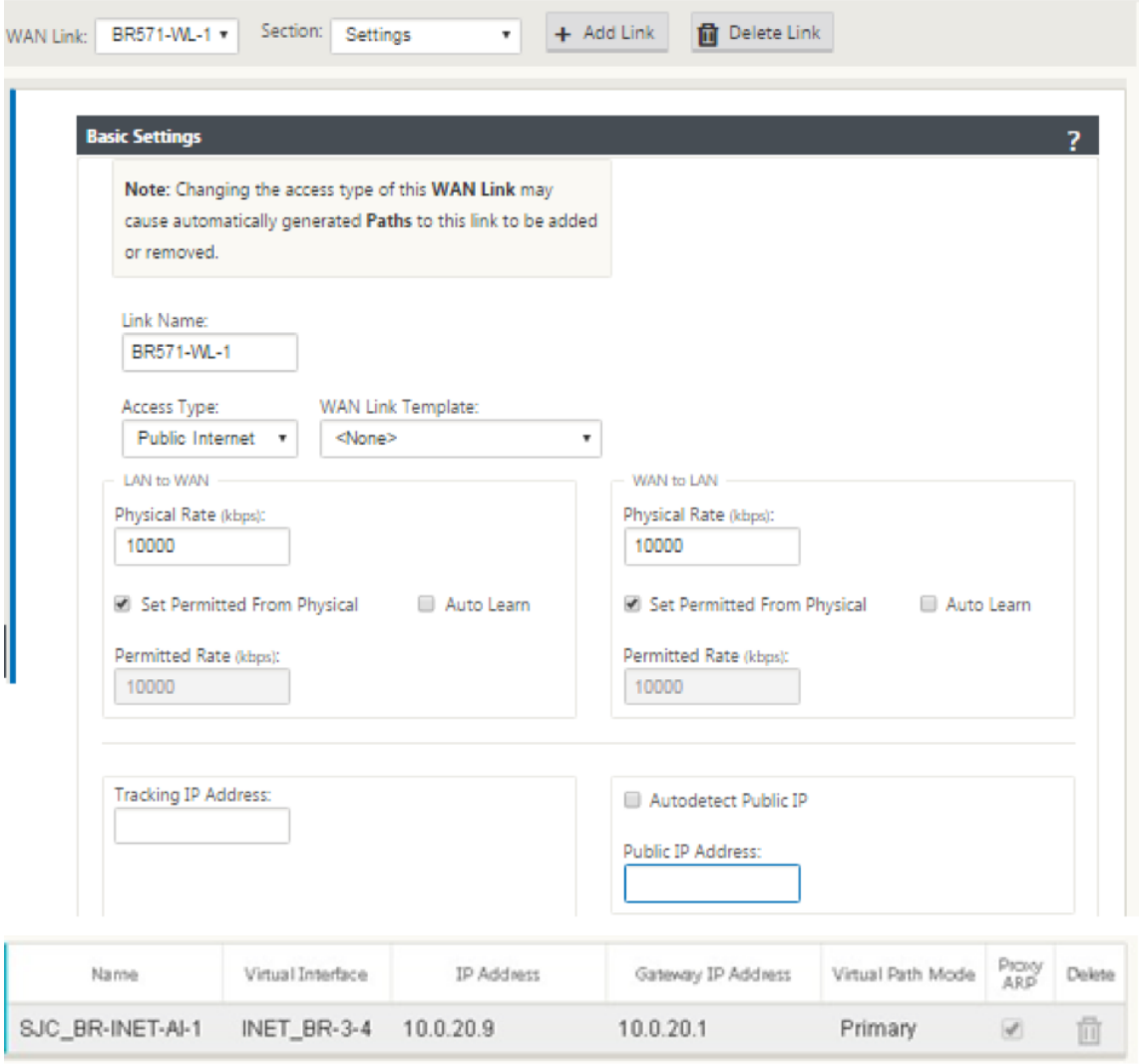
为每个虚拟接口创建虚拟 **IP (VIP)** 地址

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。



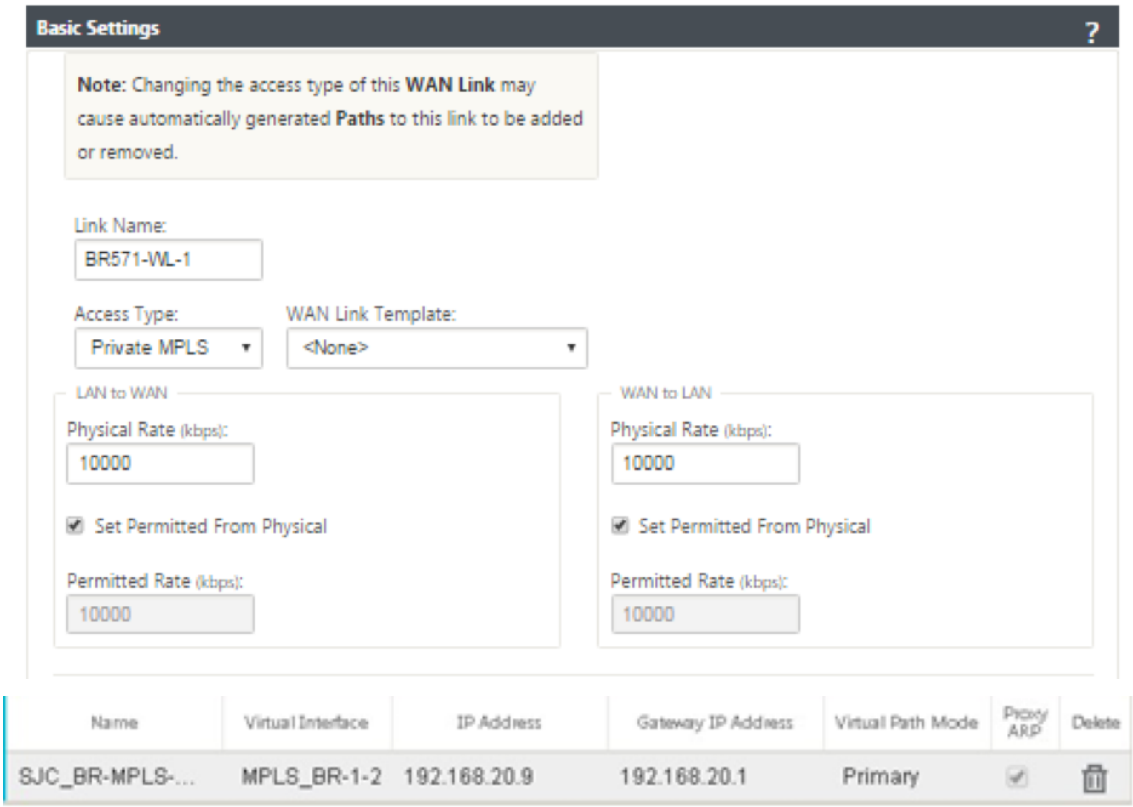
使用 **Internet** 链接基于物理速率而不是突发速度填充 **WAN** 链接

1. 导航到 **WAN** 链接，单击 **+** 按钮为 Internet 链接添加 WAN 链接。
2. 填充互联网链接详细信息，包括自动检测公有 IP 地址，如下所示。
3. 导航到 访问接口，单击 **+** 按钮添加特定于 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。



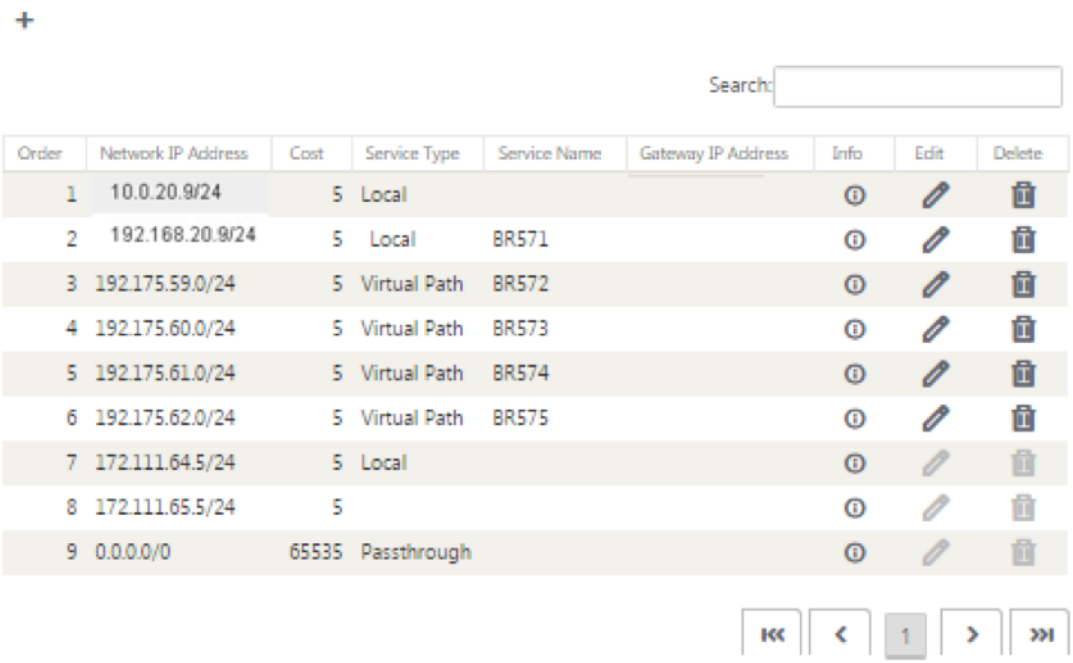
创建 **MPLS** 链接

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。



虚拟内联模式

November 1, 2021

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：

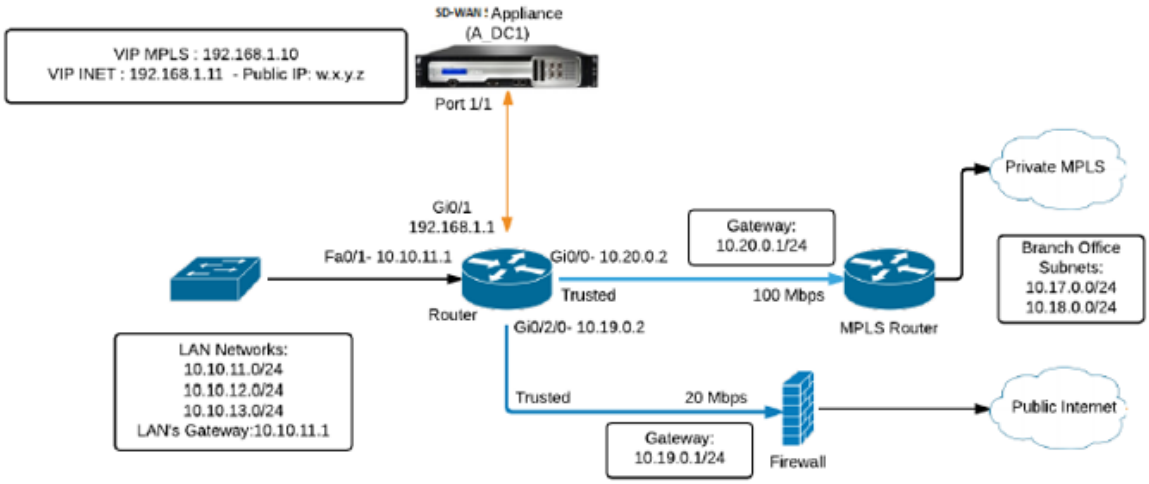
- 本地和远程站点的准确网络图，包括：

  - 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。

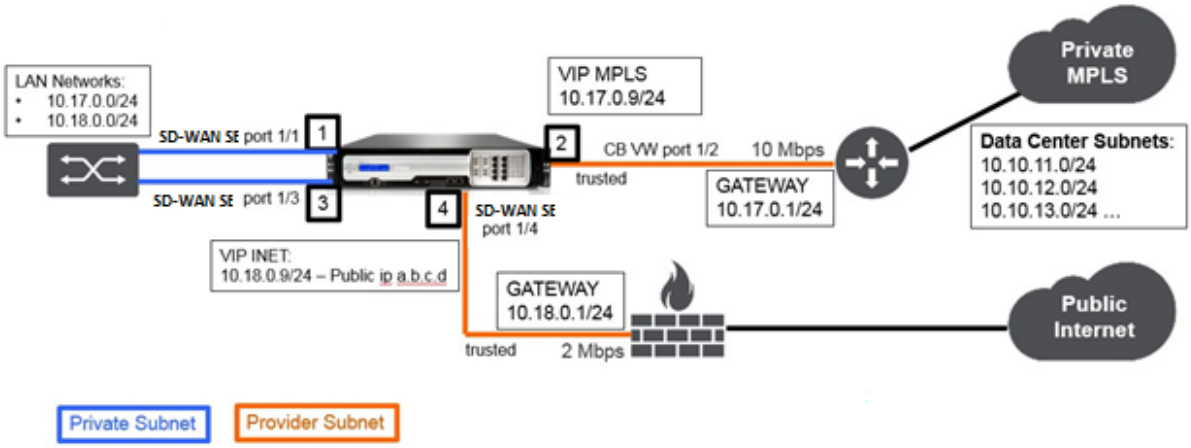
- 部署表

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



分支拓扑-内联模式



站点名称	数据中心站点	分支机构
设备名称	SJC-DC	SJC-BR

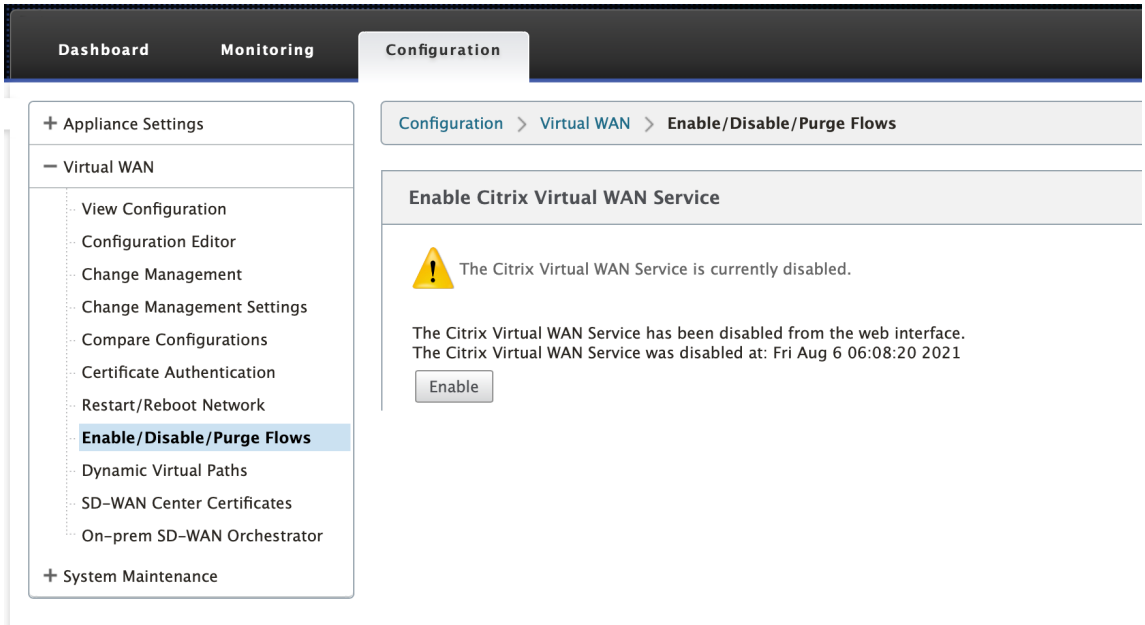
站点名称	数据中心站点	分支机构
管理知识产权	172.30.2.10/24	172.30.2.20/24
安全密钥	如果有	如果有
模型/版本	4000	2000
模式	虚拟内联模式	内联
拓扑	2 x 广域网路径	2 x 广域网路径
VIP 地址	192.168.1.10/24 —MPLS，192.168.2.10/24 —Internet，公共 IP w.x.y.z	10.17.0.9/24 - MPLS，10.18.0.9/24 –Internet，公共 IP a.b.c.d
网关 MPLS	10.20.0.1	10.17.0.1
网关 Internet	10.19.0.1	10.18.0.1
链接速度	MPLS –100 Mbps，Internet –20 Mbps	MPLS –10 Mbps，Internet –2 Mbps
路由	需要在 SD-WAN SE 设备上添加路由，了解如何通过任何物理接口访问 LAN 子网（10.10.11.0/24、10.10.12.0/24、10.10.13.0/24 等）：Gi0/1-192.168.1.1, 配置 **>** 虚拟 **WAN >** 配置编辑器 **> SJC_DC\ >** 路由。在本示例中，使用了接口 192.168.1.1：- 不适用地址：10.10.13.0/24、10.10.12.0/24、10.10.11.0/24，- 服务类型：本地，- 网关 IP 地址：192.168.1.1	未添加其他路线
VLAN	MPLS-VLAN 10、Internet - VLAN 20	无（默认值 0）

必备条件

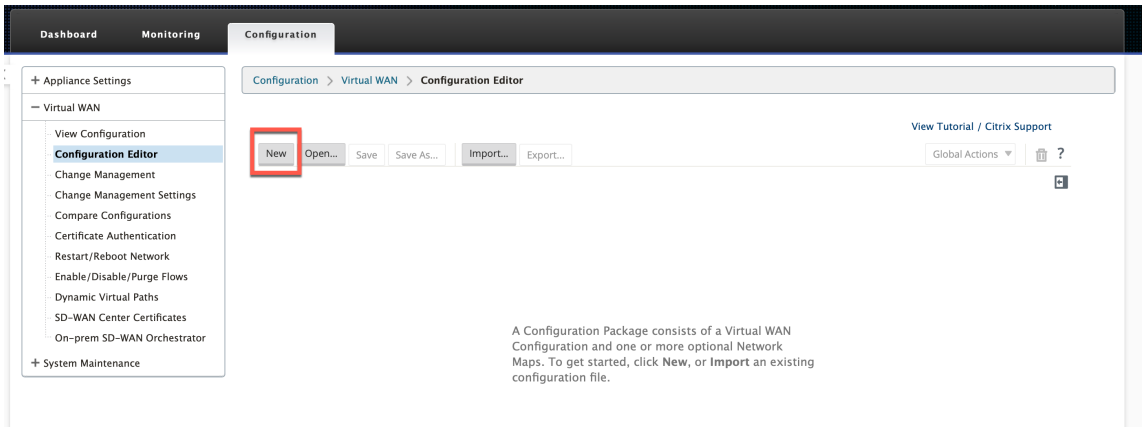
1. 在 SD-WAN 设备 **Web** 管理界面中，导航到配置 **>** 装置设置 **>** 管理员界面 **>** 其他选项卡，然后单击 切换控制台。

   > 注意：
   >
   > 如果显示 切换到客户端控制台，则表示设备已处于 MCN 模式。SD-WAN 网络中必须只有一个活动的 MCN。

2. 导航到 配置 **>** 虚拟 **WAN >** 启用/禁用/清除流 程，然后单击 启 用 **Citrix Virtual WAN** 服务 部分中的启用。



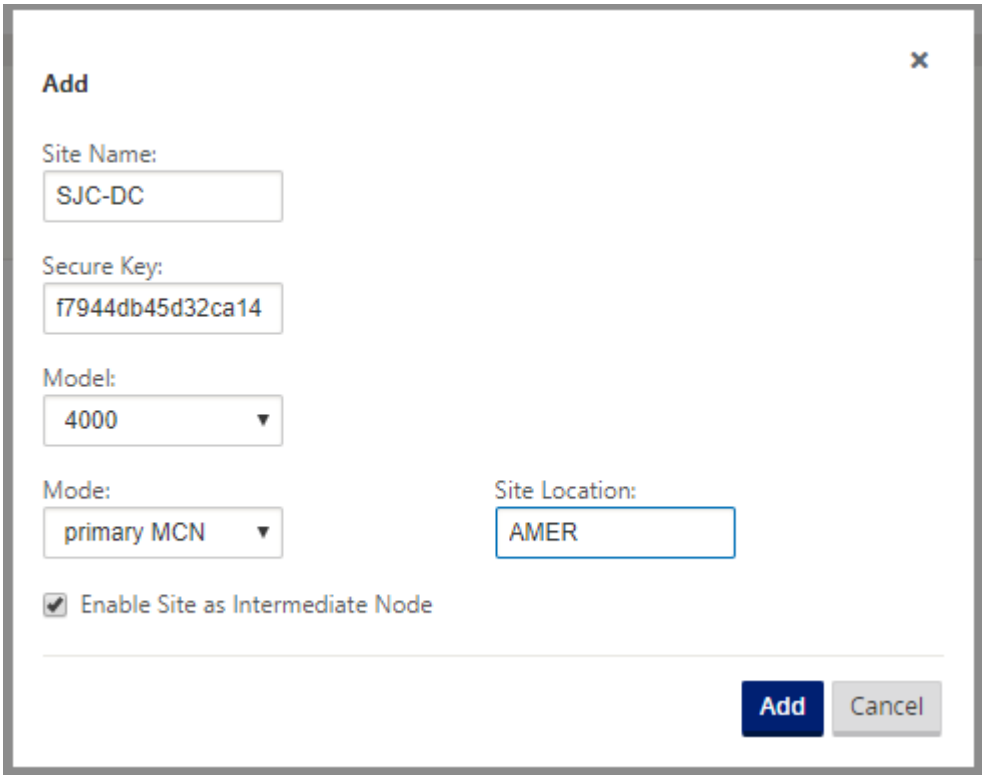
3. 通过导航到配置 **>** 虚拟 **WAN >** 配置编辑器来开始配置。单击“新建”开始配置。单击“新 建”将创建一个初始配置文件，其文件名为 **Untitled_1** 。您可以稍后使用“另存为”按钮重命名文件（可 [选] ）。



数据中心站点-虚拟内联模式配置

创建数据中心站点

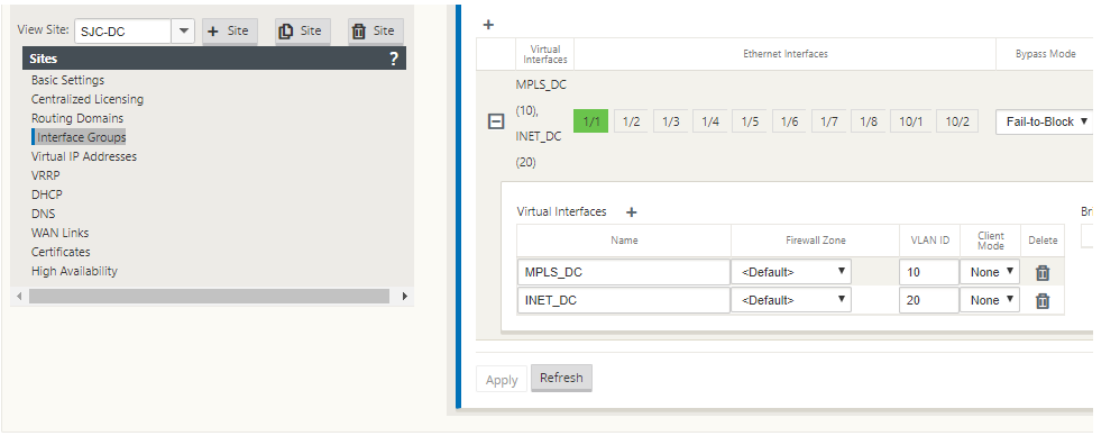
1. 导航到配置 **>** 虚拟 **WAN >** 配置编辑器 **>** 站点，然后单击 **+** 站点。
2. 输入站点名称和位置。从型号下拉列表中选择设备 型号，从 模式 下拉列表中选择 主 **MCN** 。
3. 单击添加。



基于连接的以太网接口配置接口组

在虚拟内联模式配置中，只使用一个以太网接口，即连接上游路由器的接口，提供路由策略含义（Example-Interface 1/5）。由于每个虚拟接口只使用一个以太网/物理接口，所以将旁路模式设置为故障阻止 (FTB)。另外，没有桥对。

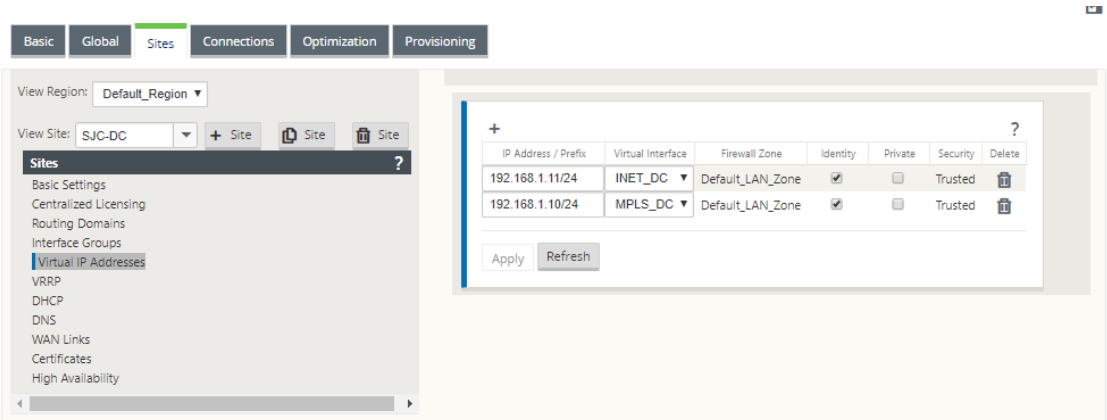
1. 在 配置编辑器中，导航到 站 **[**点 **>** 站点名称**] >** 界面组。单击 **+** 以 添加要使用的接口。
2. 选择连接到上游路由器的以太网接口，然后单击虚拟接口旁边的 **+** 。为 MPLS 和 INTERNET 链接添加虚拟接口。根据示例拓扑，添加以下内容：
   - 在 **VLAN 10** 上配置了虚拟接口 **MPLS**
   - **VLAN 20** 上配置的虚 拟接口 互联网
3. 从 旁路模式 下拉列表中选择 失败阻止。单击应用。



为每个虚拟接口创建虚拟 **IP** 地址

在适当的子网上为每个 WAN 链路创建虚拟 IP (VIP) 地址。VIP 用于虚拟 WAN 环境中的两个 SD-WAN 设备之间的通信。

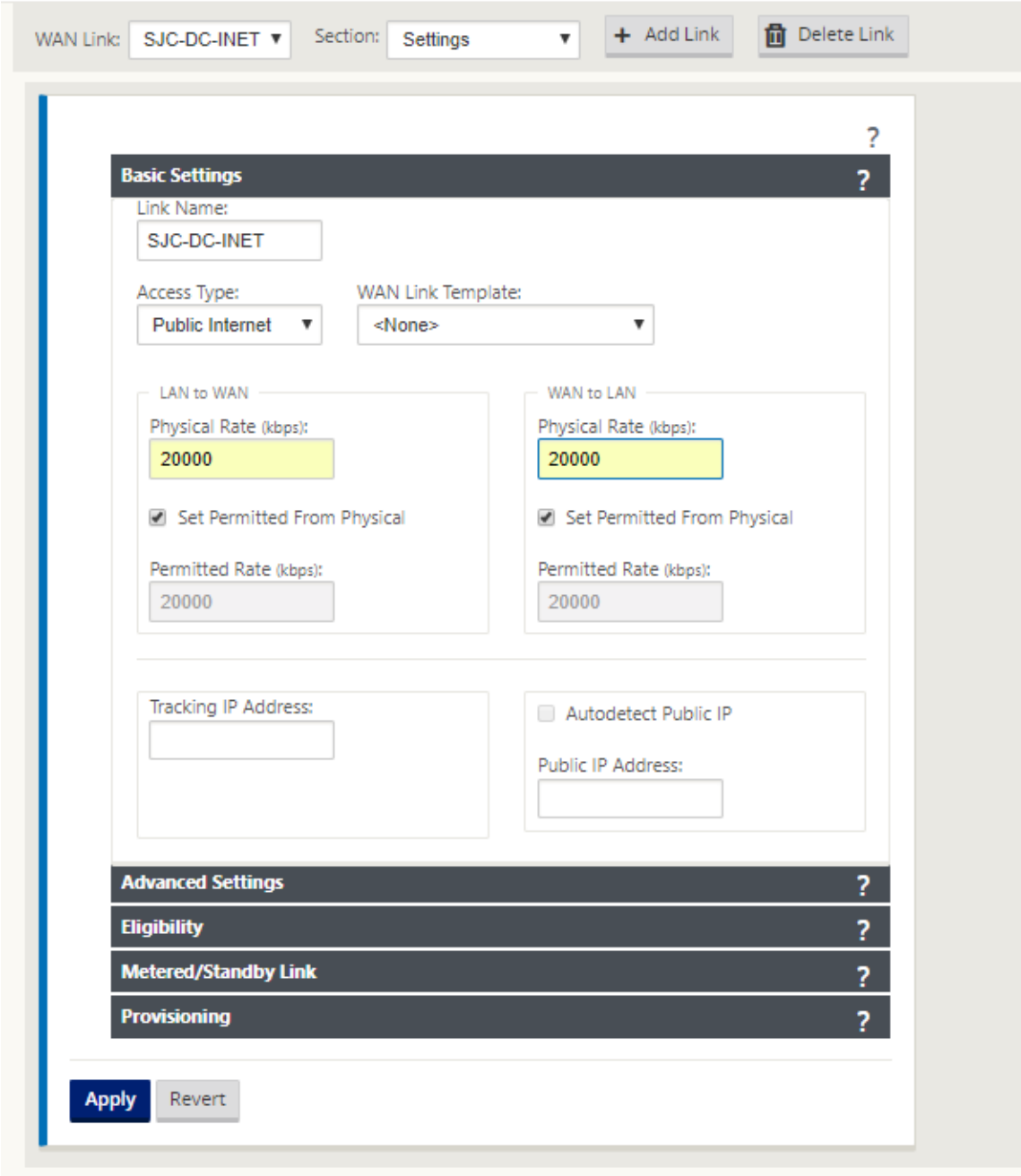
1. 在配置编辑器中，导航到 站点 **>** [点 **>** 站点名称] **>** 虚拟 **IP** 地址。单击 **+** 创建 VIP。
2. 输入 IP 地址/前缀，然后为 MPLS 和互联网选择相应的虚拟接口。
3. 单击应用。



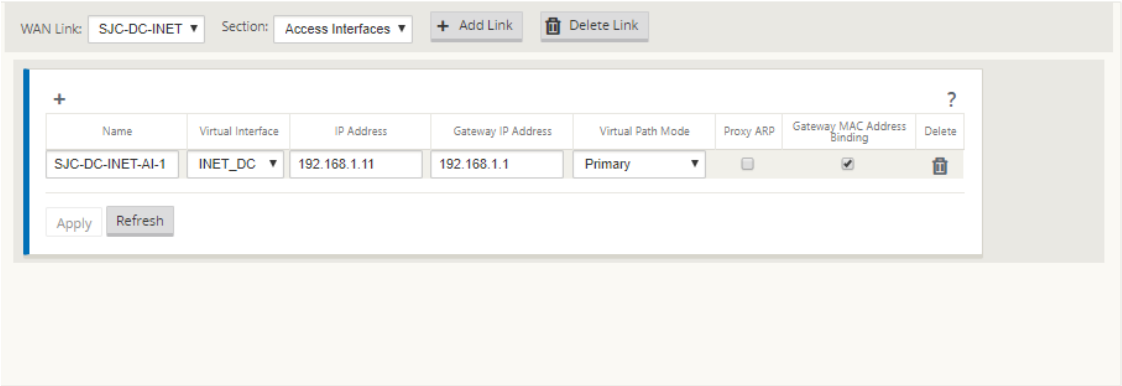
创建互联网广域网链接

根据物理速率而不是突发速度创建 Internet WAN 链接。

1. 在配置编辑器中，导航到站点 **>** [点 **>** 站点名称] **> WAN** 链接，然后单击 **+** 链接。输入名称，然后选择访问类型为公共 **Internet**。单击添加。
2. 输入实际费率。不要选中 自动检测公共 **IP** 复选框。对于配置为 MCN 的 SD-WAN 设备，无法选中 自动检测公共 **IP** 复选框。

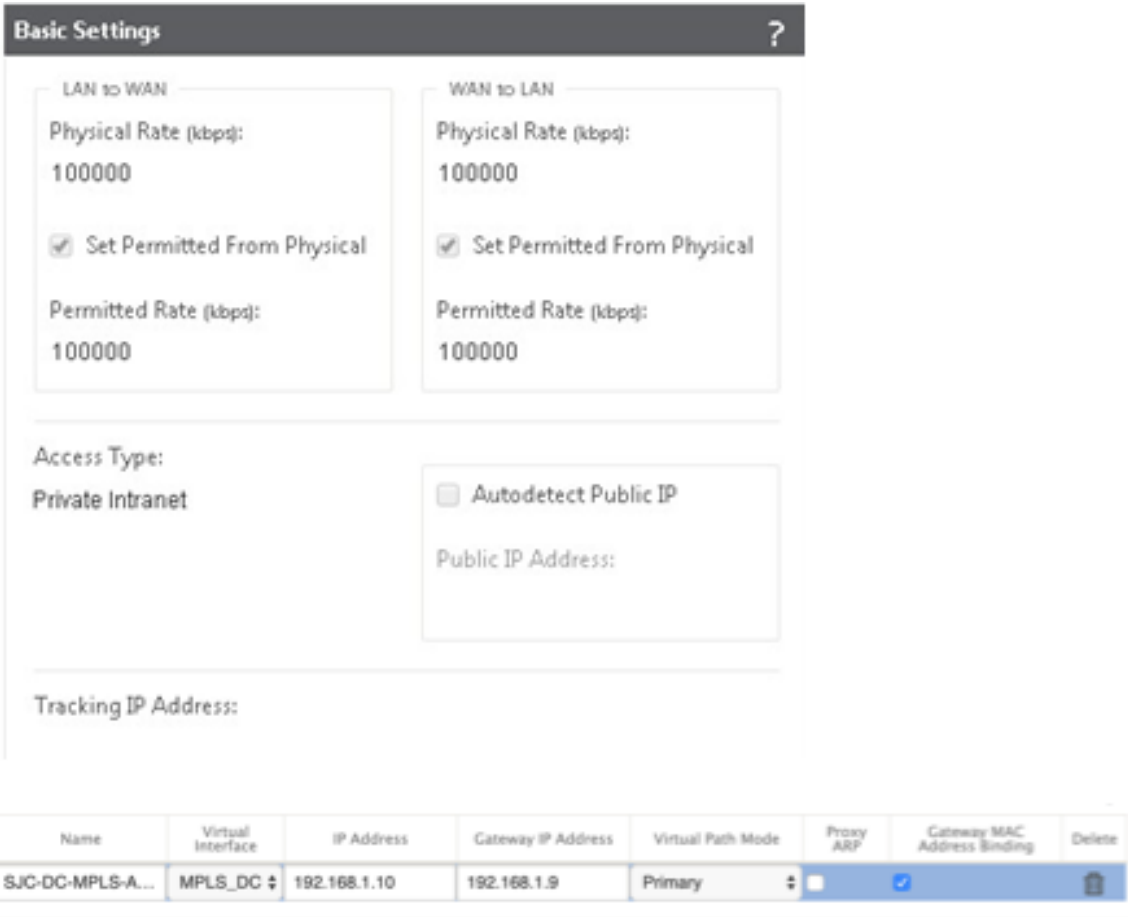


3. 从 部分 下拉列表中选择 访问接口，然后单击 **+** 按钮以添加特定于 Internet 链接的接口详细信息。
4. 输入互联网 WAN 虚拟 IP 地址和网关地址。对于少于两个以太网接口，不会检查代理 ARP 。
5. 单击应用。

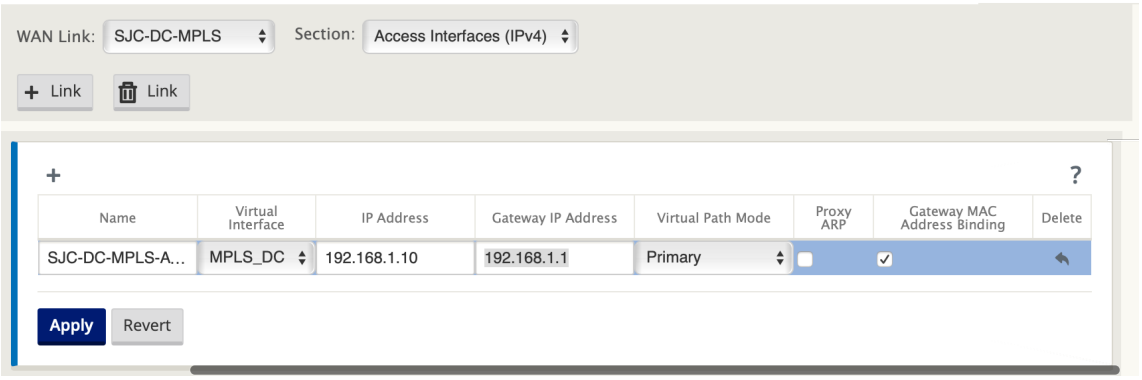


创建 **MPLS** 链接

1. 在“站点”[点 **>** 站点名称] **>** “**WAN** 链接”页面中，从“部分”下拉列表中选择“设置”。单击 **+** 链接 按钮添加适用于 MPLS 的 WAN 链接。
2. 输入 MPLS WAN Link 名称，然后选择 访问类型 作为 专用内联网。单击添加。
3. 输入实际费率和其他详细信息。单击应用。



4. 从 部分 下拉列表中选择 访问接口，然后单击 **+** 按钮以添加特定于 MPLS 链接的接口详细信息。
5. 输入 MPLS 虚拟 IP 地址和网关地址。对于少于两个以太网接口，不会检查代理 ARP 。
6. 单击应用。



填充路线

在数据中心方面，在 SD-WAN 设备上添加关于如何通过任何物理接口到达局域网子网(10.10.11.0/24、10.10.12.0/24、10.10.13.0/24 等）的路由。

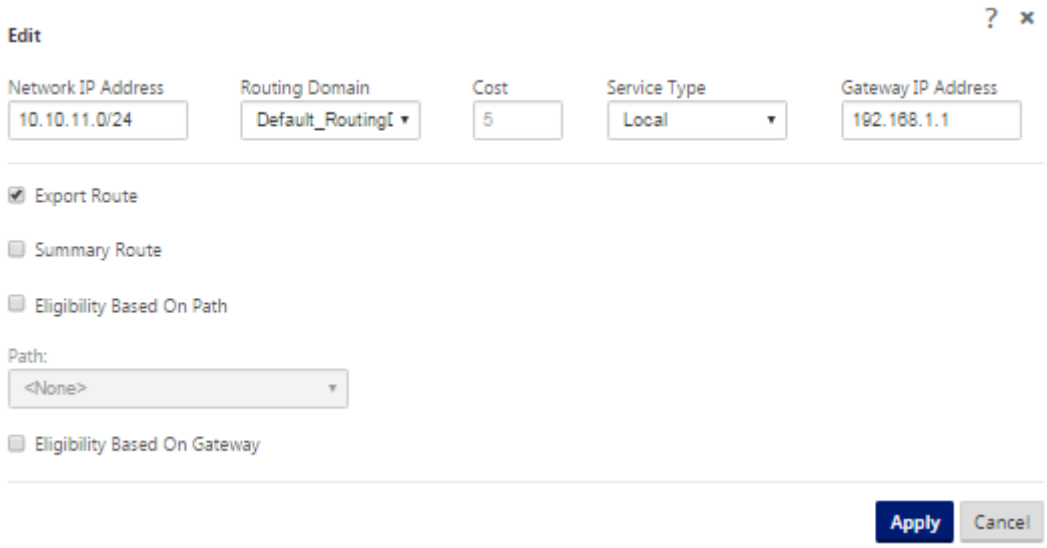
0/1/0.1 –VLAN 10 上的 192.168.1.1

0/1/0.2 –VLAN 20 上的 192.168.2.1

在本例中，使用接口 192.168.1.1。

在 配置编辑器中，导航到 连接 **>** 路由，然后单击 **+** 添加路由。

输入 网络 **IP** 地址、开 销和网 关地址。单击添加。

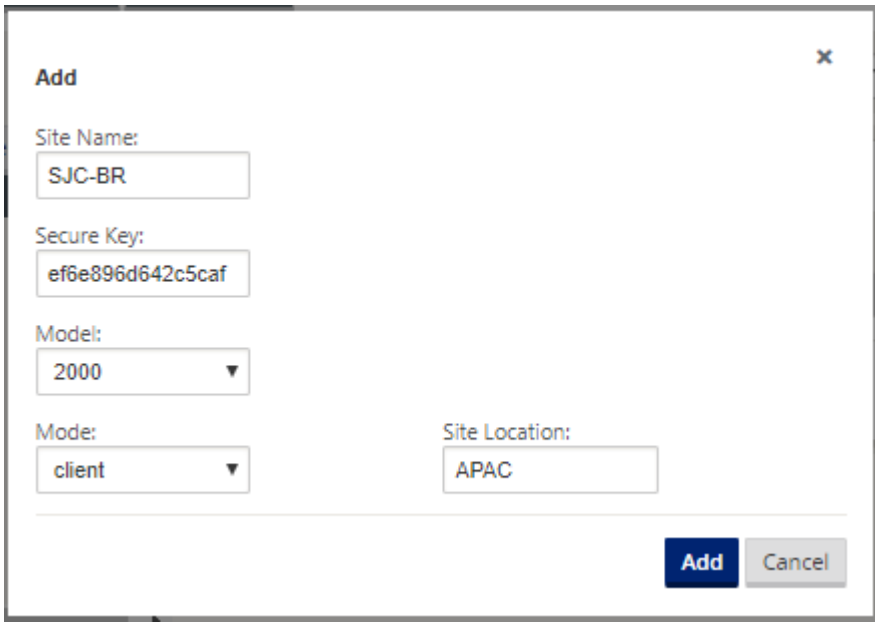


Order	Network IP Address	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.10.13.0/24	5	Local		192.168.1.1			
2	10.10.12.0/24	5	Local	BR571	192.168.1.1			
3	10.10.11.0/24	5	Local	BR572	192.168.1.1			
4	192.175.60.0/24	5	Virtual Path	BR573				
5	192.175.61.0/24	5	Virtual Path	BR574				
6	192.175.62.0/24	5	Virtual Path	BR575				
7	172.111.64.5/24	5	Local					

分支站点内联部署配置

创建分支站点

1. 导航到 配置编辑器 **>** 站 点，然后单击 **+** 站点。
2. 输入站点名称和位置。从型号下拉列表中选择设备 型号，从 模式 下拉列表中选择 客户端。
3. 单击添加。

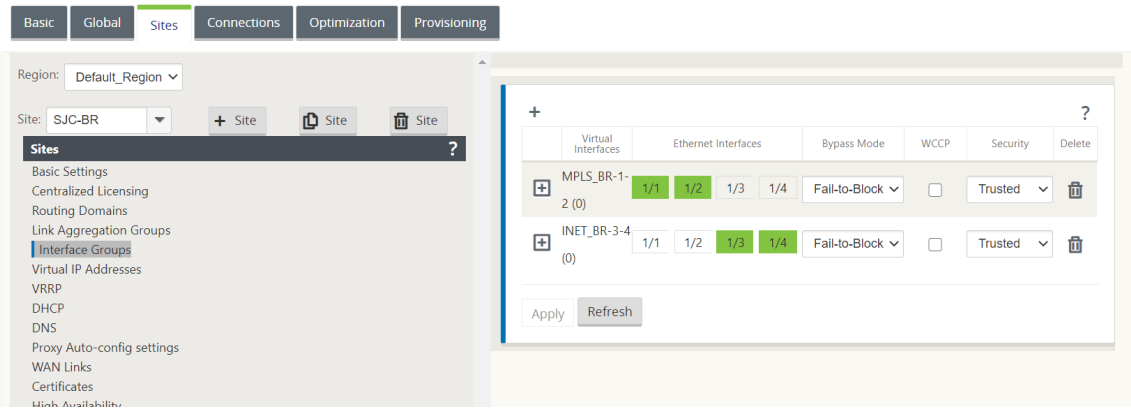


基于连接的以太网接口配置接口组

1. 在 配置编辑器中，导航到 站点 **>** **[**客户端站点名称**]** **>** 接口组。单击 **+** 以 添加要使用的接口。对于内联模式配置，使用四个以太网接口；接口对 1/3、1/4 和接口对 1/1 和 1/2。

2. 将 旁路模式 设置为故障连接，因为每个虚拟接口使用两个以太网/物理接口。有两个桥对。
3. 单击 虚拟接口 旁边的 **+** ，然后使用 Internet 和 MPLS 链接根据物理速率而不是突发速度填充 WAN 链接。
   - 在 网桥对 **1/3** 和 **1/4** 上配置了虚拟接口 **INTERNET**
   - 在网桥对 1/1 和 1/2 上配置的虚拟接口 **MPLS** 。
4. 单击 网桥对 旁边的 **+** ，然后通过选择适当的接口来创建网桥对。

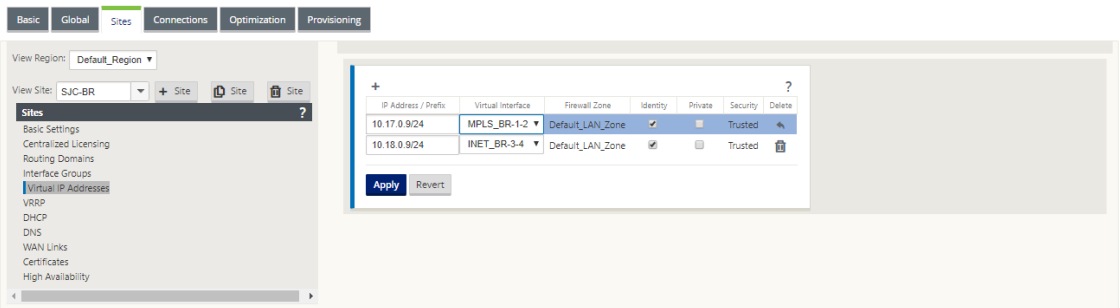
   请参阅 先决条件 部 分下的分支拓扑—串联模式 拓扑图，然后填充接口组。



为每个虚拟接口创建虚拟 **IP (VIP)** 地址

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。

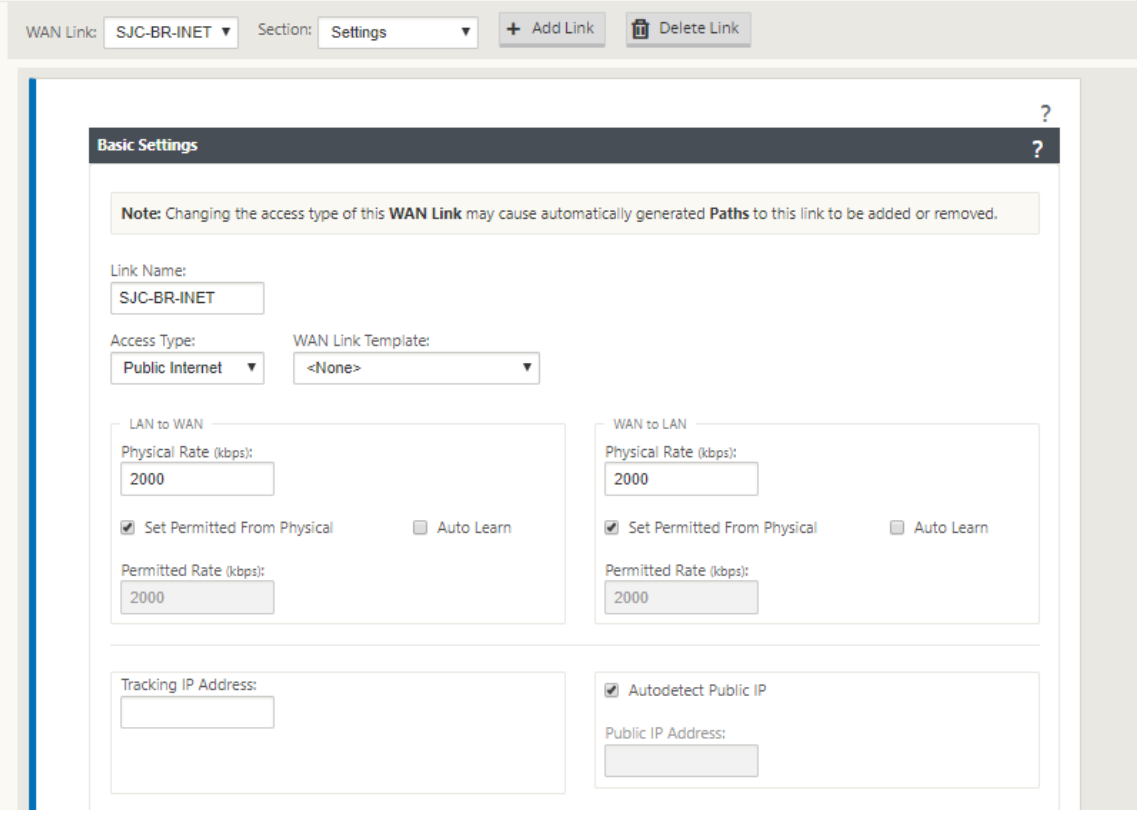
1. 在配置编辑器中，导航到 站点 **>** [点 **>** 站点名称] **>** 虚拟 **IP** 地址。单击 **+** 创建 VIP。
2. 输入 IP 地址/前缀，然后为 MPLS 和互联网选择相应的虚拟接口。
3. 单击应用。

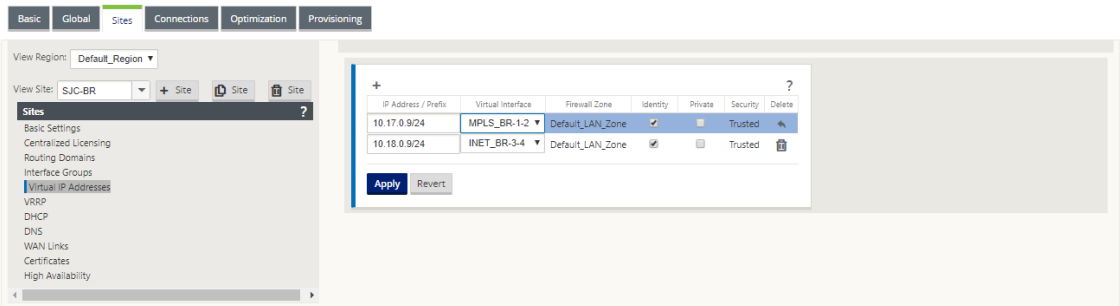


创建互联网广域网链接

使用 Internet 链接基于物理速率而不是突发速度填充 WAN 链接

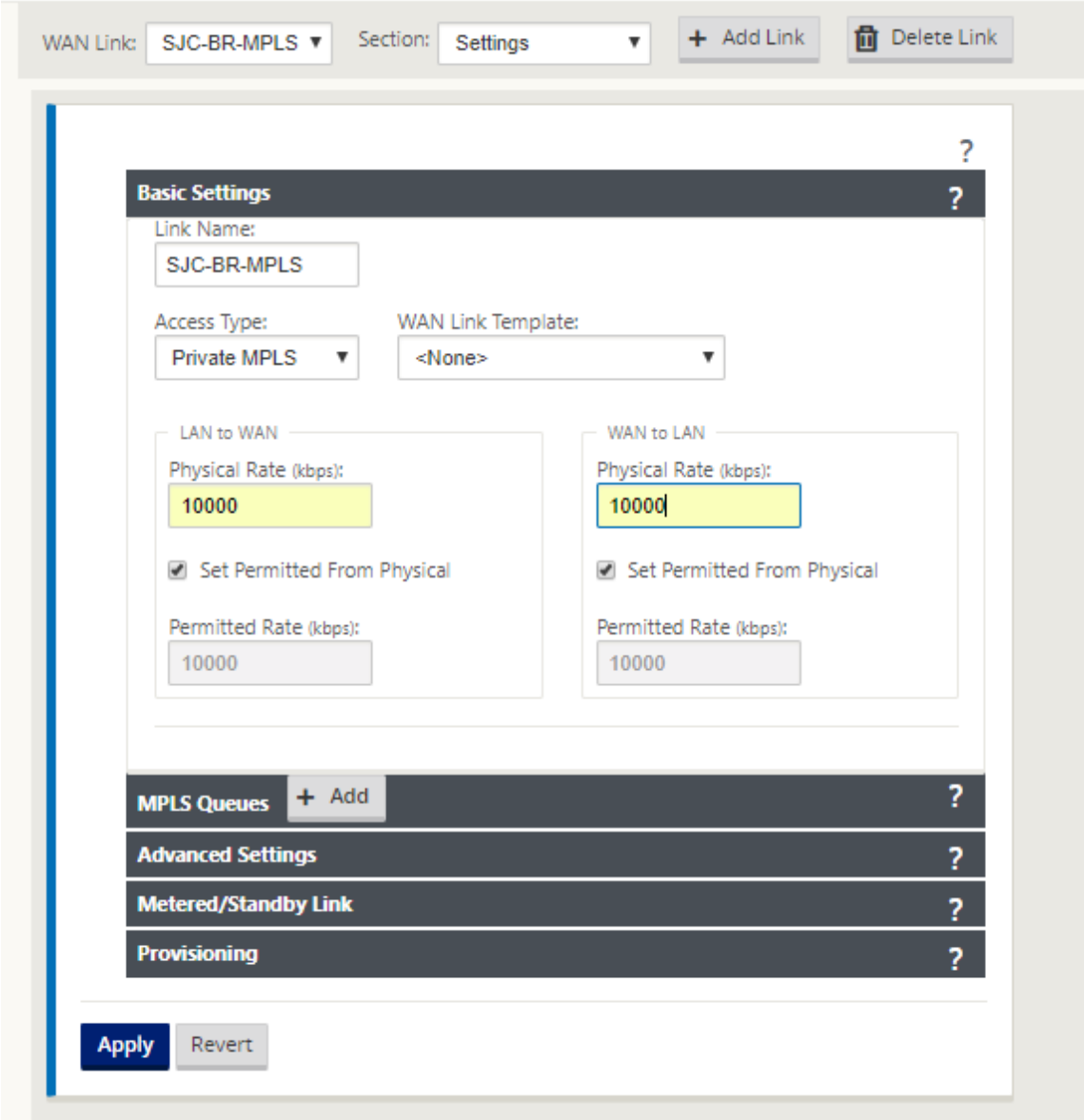
1. 导航到 **WAN** 链接，单击 **+** 链接 按钮为 Internet 链接添加 WAN 链接。输入名称，然后选择访问类型为公共 **Internet**。单击添加。
2. 填充 Internet 链接详细信息，然后选中 自动检测公共 **IP** 地址 复选框。
3. 从“部分”下拉列表中选择“访问接口”，然后单击 **+** 以添加特定于 Internet 链接的接口详细信息。
4. 输入互联网 WAN 虚拟 IP 地址和网关地址。对于少于两个以太网接口，不会检查代理 ARP 。



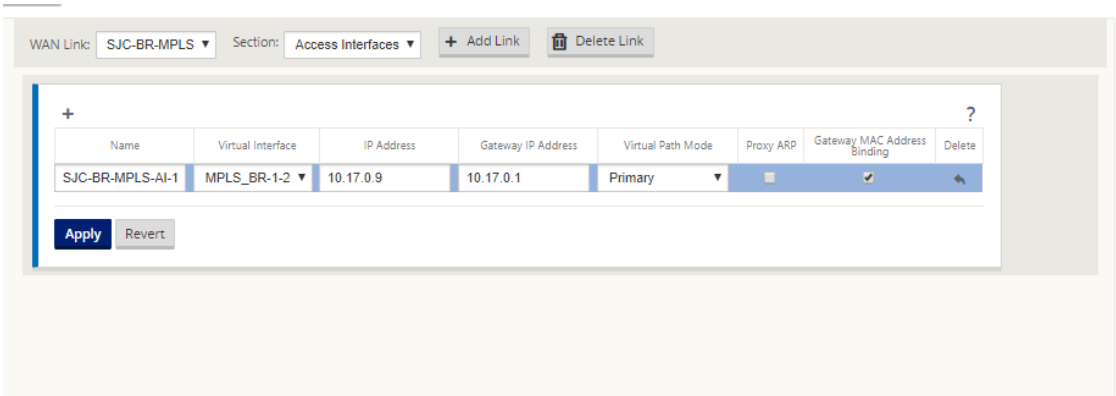


创建 **MPLS WAN** 链接

1. 导航到 **WAN** 链接，然后从 部分 下拉列表中选择 设置。单击 **+** 链接 按钮为 MPLS 链接添加 WAN 链接。
2. 输入 MPLS WAN Link 名称和其他详细信息。选择 访问类型 作为 专用 **Intranet**。



3. 从 部分 下拉列表中选择 访问接口，然后单击 **+** 按钮以添加特定于 MPLS 链接的接口详细信息。
4. 输入 MPLS 虚拟 IP 地址和网关地址。对于少于两个以太网接口，不会检查代理 ARP 。

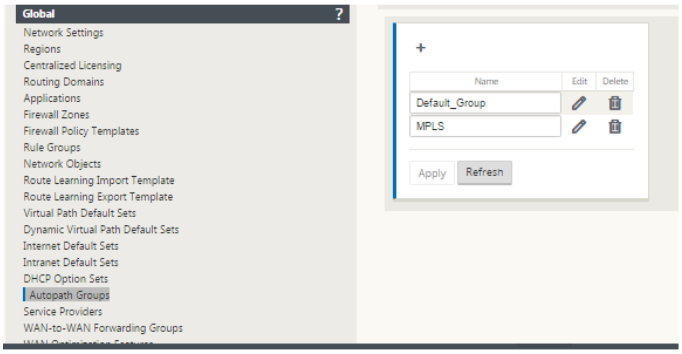


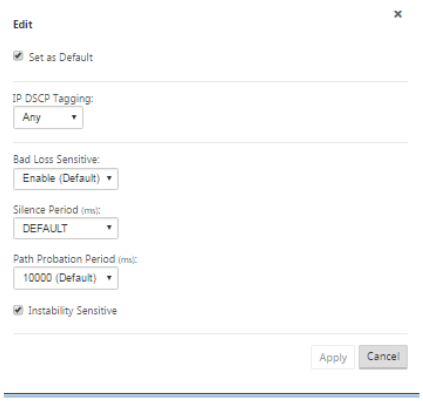
填充路线

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

创建自动分析组

1. 在 配置编辑器中，导航到 全局 **>** 自动分析组。单击 **+**。
2. 输入名称，然后单击“应用”。
3. 根据需要配置 Autopath 组，然后单击 应用。





4. 导航到“连接” **>** “**WAN** 链接”。从 WAN 链接下拉列表中选择 Internet **WAN** 链 接，从 部分 下拉列表中选择虚拟路径。
5. 选中 使用 复选框，然后从相应站点（数据中心和分支机构）的 Intranet WAN 链接的 **Autopath Group** 复选框中选择新创建的自动分析组。

   没有两个自动分析组可以标记为默认值。如果标记，将导致审计错误。

为访问类型为 私有 **Intranet** 的 WAN 链接手动添加虚拟路径后，虚拟路径将填充在 路径下。

完成上述所有步骤后，继续 准备 SD-WAN 设备包。

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

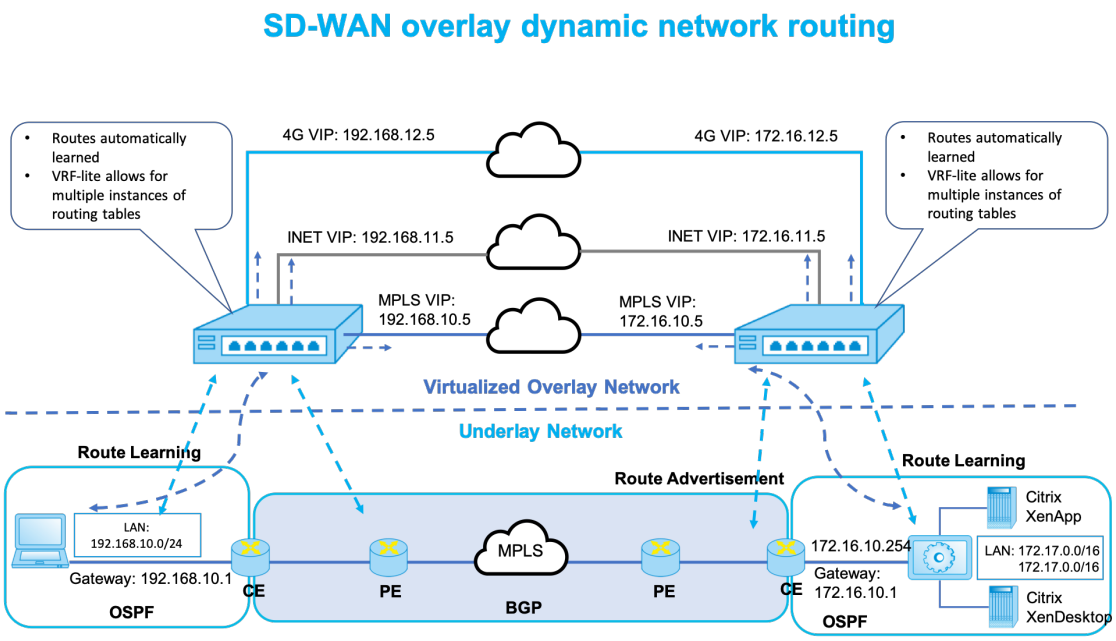
June 22, 2021

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 路径隧道。
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
- 互联网-互联网流量
- 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。



仅使用 **Premium (Enterprise) Edition** 的 **WAN** 优化

June 22, 2021

SD-WAN 高级（企业）版设备除了 WAN 虚拟化外，还包含功能齐全的 WAN 优化功能。某些客户更愿意在迁移到 SD-WAN 服务之前实施 WAN 优化功能。此部署使用案例提供了利用高级版设备来利用 WAN 优化服务的步骤。

Citrix SD-WAN 产品平台版本包括以下设备：

- SD-WAN：SD-WAN 标准版设备
- 高级（企业级）：SD-WAN 高级版设备
- WANOP: SD-WANOP 版设备

要将高级（企业）版设备集成到现有的分布式 WANOP 网络中，可以将 DC 站点上的 SD-WAN（物理或虚拟）设备配置为 MCN。SD-WAN 设备管理网络的所有配置。在分支站点和 DC 站点的 MCN 之间建立虚拟路径。此虚拟路径仅用于在设备之间发送控制流量。在分支设备上，数据流量将作为 Intranet 服务进行处理。Intranet 流量未封装，并通过现有 WAN 链接进行遍历以达到 DC 站点。DC 站点的 WANOP 设备应位于流量路径中，以提供端到端流量优化。

对于头端没有 SD-WAN 硬件设备的客户站点，HA 对中的 VPX 设备（两个虚拟 WAN VPX）可以在单臂模式下用作 MCN。对于单臂模式，需要第三方路由器上的 PBR 规则才能将流量重定向到 SD-WAN 设备。

本文档假定 DC 站点设备部署在 HA 模式下进行冗余。此部署不强制使用 HA 模式。

必备条件

- 在 DC 站点以 HA 模式部署的一对 WANOP 设备和一对 SD-WAN 设备。
- 分支机构站点的高级版设备。

网络拓扑

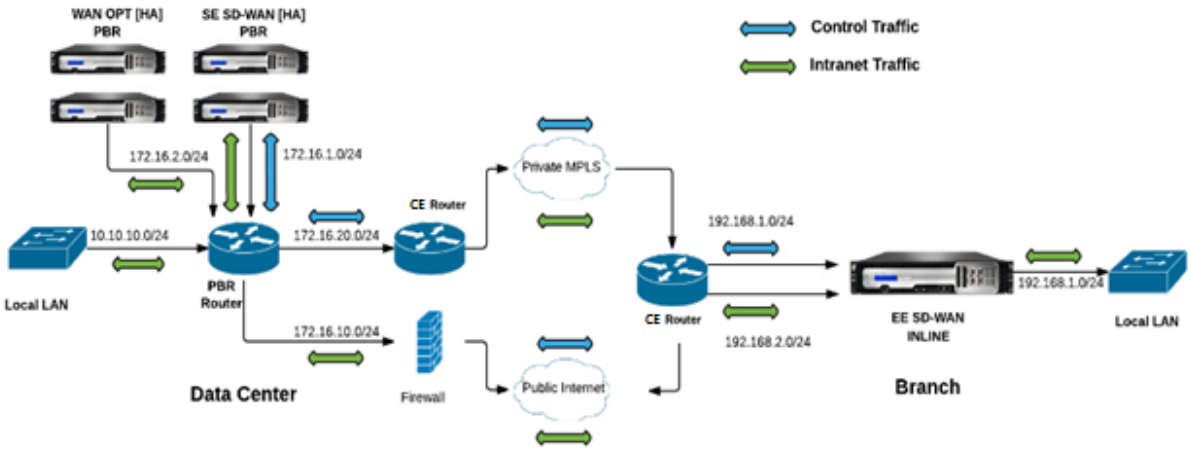
SD-WAN 标准版和 **PBR** 部署中的 **WANOP** 设备：

在下图中，DC 站点的 SD-WAN SE 和 WAN OP 设备均以单臂模式部署。SD-WAN 设备支持 PBR 部署，而 WANOP 设备支持 PBR 和 WCCP。PBR 路由器将从 DC 站点的 WAN 接收的控制流量（虚拟路径流量）重定向到 SD-WAN 设备。数据流量由 PBR 路由器重定向到 WAN 优化设备。

广域网至直流局域网的流量：

- CE（客户边缘）路由器-> PBR 路由器-> SD-WAN-> PBR 路由器-> 局域网
- CE（客户边缘）路由器-> PBR 路由器-> 广域网 OPT-> PBR 路由器-> 局域网

相同的交通流是在相反的方向。



PBR 模式下的 **SD-WAN** 标准版和内联部署中的 **WANOP**：

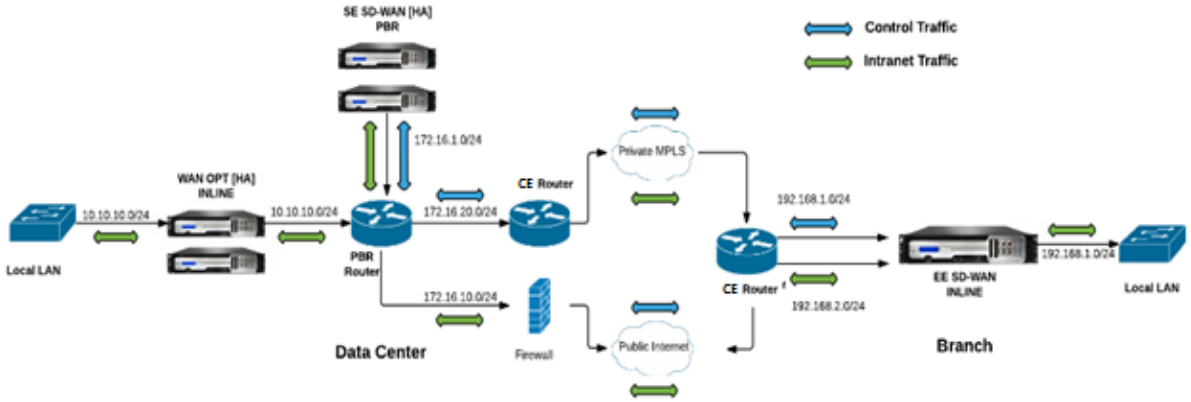
在下图中，DC 站点的 SD-WAN 设备以单臂模式部署，而 WANOP 设备则以内联模式部署。

PBR 路由器将从 DC 站点的 WAN 接收的控制流量（虚拟路径流量）重定向到 SD-WAN 设备。数据流量由 PBR 路由器转发到 WAN 优化设备（内联）。

广域网至直流局域网的流量：

- CE（客户边缘）路由器-> PBR 路由器-> SD-WAN-> PBR 路由器-> 局域网
- CE（客户边缘）路由器-> PBR 路由器-> 广域网 OPT-> 局域网

相同的交通流是在相反的方向。



配置步骤

1. 在 DC [MCN] 配置 SD-WAN 设备以在 DC 和分支站点之间建立虚拟路径。

   看到配置 MCN 和客户端之间的虚拟路径服务了

2. 在 DC 站点配置 Intranet 服务。

   a) 在 MCN（DC 站点）上，转到 配置 **>** 虚拟广域网 **>** 配置编辑器 **>** 连接 **>** 站点 **(DC) > Intranet** 服务。单击 **[+** 符号以**]** 添加 Intranet 服务。

   b) 为 **Intranet** 服务选择一个或多个 WAN 链接，然后单击 应用。

   c) 导航到同一 站点 **(DC)** 下的路由，单击 **[+** 符号以**]** 符号以添加成本低于 5 的远程网络，然后选择 添加。

   例如，在成本为 4 的网络 **IP** 地址字段中输入 **192.168.1.0/24**，然后选择服务类型 **Intranet**。

   > 注意
   >
   > 每个站点的成本应小于 5，以便优先使用 Intranet 路由。

3. 在分支站点上配置 Intranet 服务。

   a) 在分支站点上重复上述步 骤 **2** 中的子步骤 a 到 c。

   例如，-在成本 4 的网络 IP 地址字段中输入 **172.16.1.0/24** ，然后选择作为 **Intranet** 的 服务类型。

4. 执行 更改管理 以将配置上载并分发到分支站点。

   请参阅导出配置包和更改管理

   默认情况下，流量通过虚拟路径从分支机构发送到 DC。

   > 注意
   >
   > 应将 PBR 路由器配置为根据提供的部署步骤重定向流量。

   有关配置 WAN 优化的详细信息，请参阅：启用配置 WAN-优化。

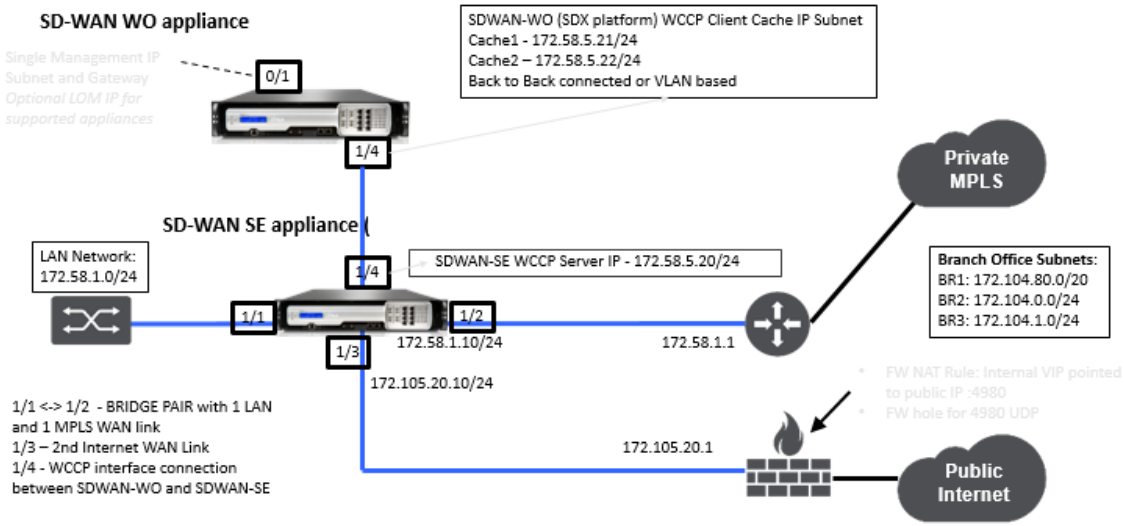
双盒模式

June 22, 2021

两箱模式是一种基于 WCCP 的单臂部署，SD-WAN SE 设备充当 WCCP 路由器，SDWAN-WANOP（4000/5000）设备充当 WCCP 客户端，帮助建立 WCCP 融合。这样，到达 SD-WAN SE 设备的所有面向虚拟路径/Intranet 服务的 TCP 数据包都会重定向到 SDWAN-WANOP 设备，通过为客户流量提供 SD-WAN SE 和 WANOP 优势，从而实现优化优势。

仅在以下设备型号上支持双盒模式：

- SD-WAN SE 设备–4000、4100 和 5100
- SD-WAN WANOP 设备–4000、4100、5000 和 5100



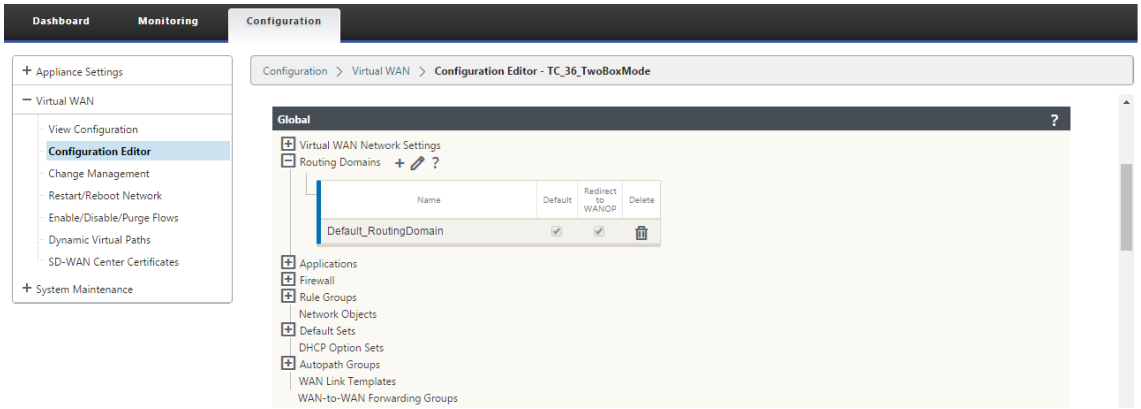
> 注意
>
> 启用双盒模式时，无法访问高可用性和 WCCP 部署模式。但是，这些部署模式可供用户管理。
>
> 重要
>
> - 虽然启用两盒模式时禁用旧版 WCCP 部署，但只能从 WCCP 监视页面验证服务组融合。双盒模式的监视部分下没有单独的 GUI 页面。
> - 如果在标准版设备上运行的 WCCP 进程在短时间间隔内重新启动多次，例如，一分钟内 3 次，则服务组将自动关闭。在这种情况下，要在 WANOP 设备上获得 WCCP 融合，请在 WANOP 设备 Web GUI 中重新启用 WCCP 功能。
> - 当 WCCP 配置或与标准版设备上的配置相关的 WAN 优化发生更改时，外部 WANOP 设备将重新启动。例如，在配置编辑器接口组中启用/禁用 WCCP 复选框，然后是更改管理过程，也会重新启动 WANOP 设备。
>
> 注意

> 另外，在实现双盒模式时需要注意以下几点：
>
> - 当选择路由域从配置编辑器重定向到 WANOP 设备时，应将其添加到已启用 WCCP 的接口组中。
> - 同样的路由域的流量也应该在合作伙伴站点上选择。例如，**MCN** > **Branch01** 观察 WAN 优化优势。
> - 如果在启用 WCCP 的接口组中选择了路由域，则包含桥接接口的另一个接口组应配置相同的路由域。只有在启用 WCCP 的接口组配置了路由域时，传输具有 WAN 优化优势的端到端流量是不够的。

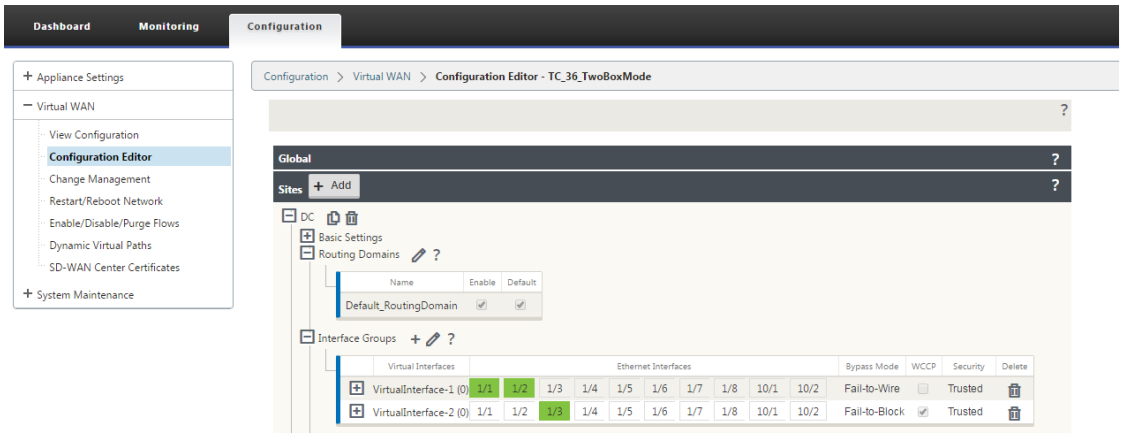
Citrix SD-WAN 标准版

要在 DC 或分支站点的标准版设备中配置双盒模式解决方案，请执行以下操作：

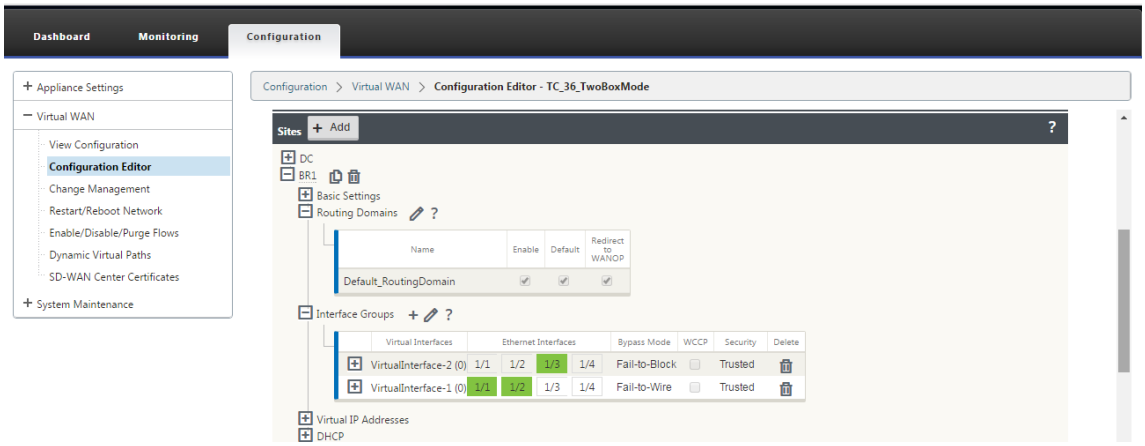
1. 在 SD-WAN SE Web 管理界面中，转到 配置 > 虚拟 **WAN** > 配置编辑器。打开现有配置包或创建包。
2. 在所选配置包中，转到 高级 选项卡以查看配置详细信息。
3. 打开 全局 设置并展开 路由域 以查看 重定向到 **WANOP** 复选框已启用。



4. 展开 DC 以在界面 组设置下为虚拟接口 启用 **WCCP** ，该设备指示启用了哪个虚拟网络接口。



5. 展开 站点 **+** 添加 以查看分支路由域和接口组设置。在分支站点下，为路由域启用 重定向到 **WANOP** 复选框。

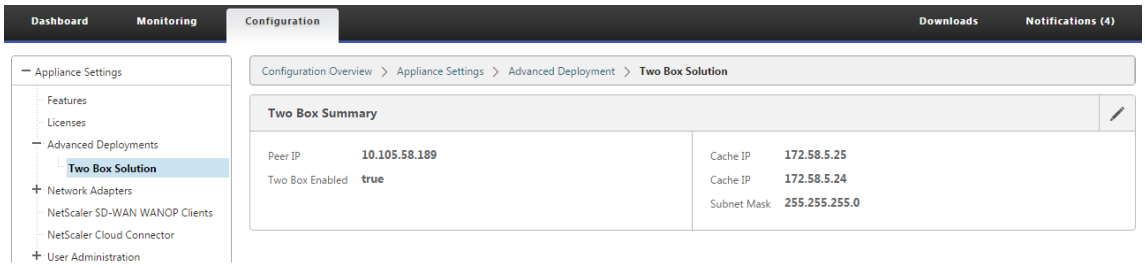


> 注意
>
> 只有那些只配置了一个以太网接口的虚拟网络接口才能启用 WCCP 侦听器。不要在桥接对上启用 WCCP 侦听器。它旨在在 SD-WAN SE 和 SD-WAN WANOP 设备之间的一个 ARM 接口上启用。

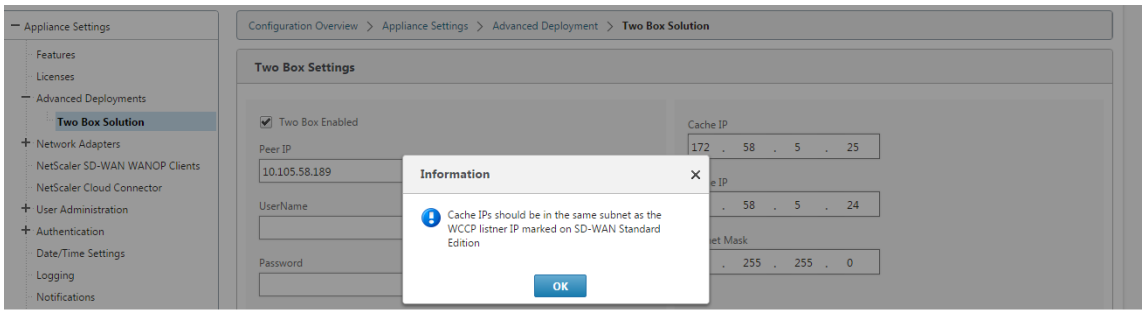
Citrix SD-WAN ANOP 配置

要在 SD-WAN WANOP 设备 Web GUI 中配置双框部署模式，请执行以下操作：

1. 在 SD-WAN WANOP Web 管理界面中，转到配置 > 设备设置 > 高级部署 > 双盒解决方案。



2. 单击编辑图标以编辑双盒模式设置。将显示有关 缓存 **IP** 的信息对话框。单击确定。



3. 启用双盒已启用复选框。
4. 输入对等 **IP**。对等 IP 是 SD-WAN 标准版设备 IP 地址。
5. 输入用户凭据，然后单击应用。

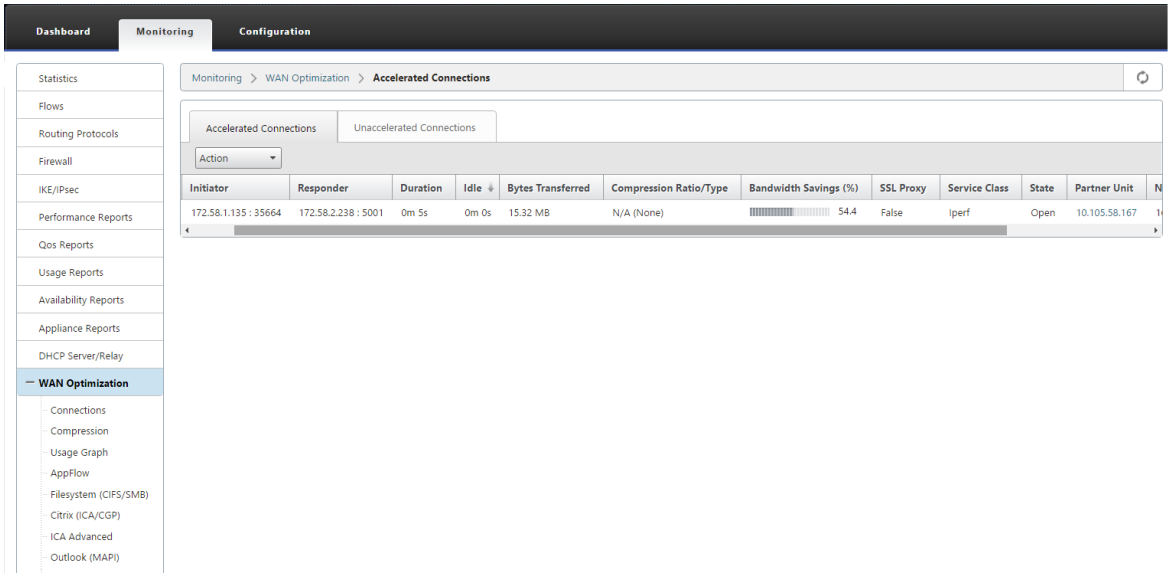
两箱模式配置和可管理性

以下是部署时需要考虑的两个盒子模式配置和可管理性点中的一些：

- 下面提到的 SD-WAN WANOP 配置可以从 SD-WAN SE 配置编辑器配置为统一窗格
  - 服务类别
  - 应用程序分类器
  - 功能
  - 系统调整

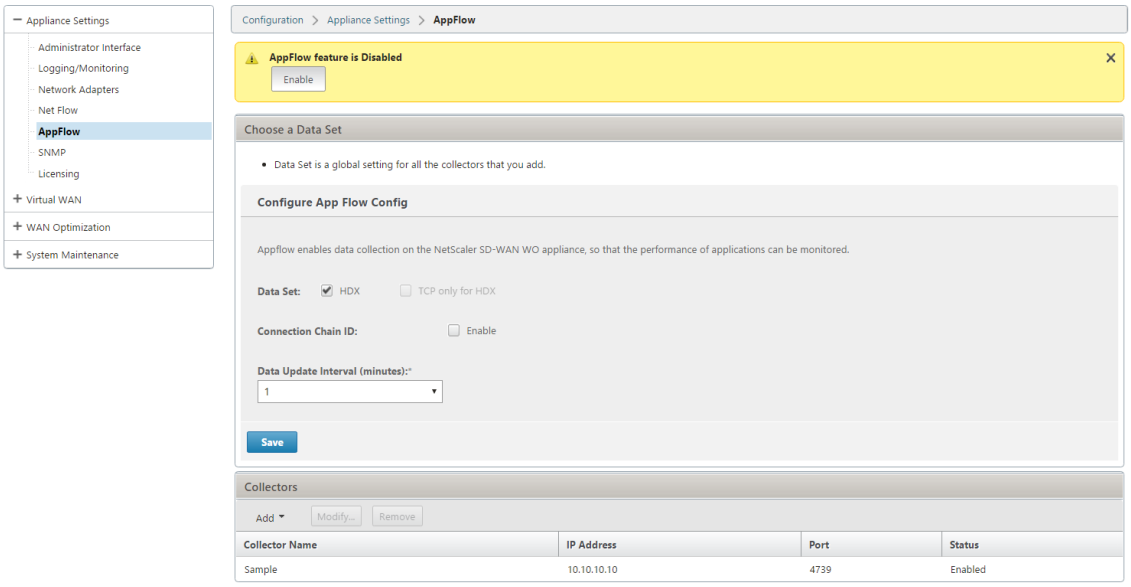
监视

您可以直接使用 SD-WAN SE 设备的 Web UI 的“监视”页面监视 SD-WAN WANOP 流量。这样可以在处理数据流量时对 SDWAN-SE 和 SDWAN-WO 设备进行单个窗格监视。您可以在 SDWAN-SE UI 的 WAN 优化节点下查看连接详细信息、安全合作伙伴详细信息等。



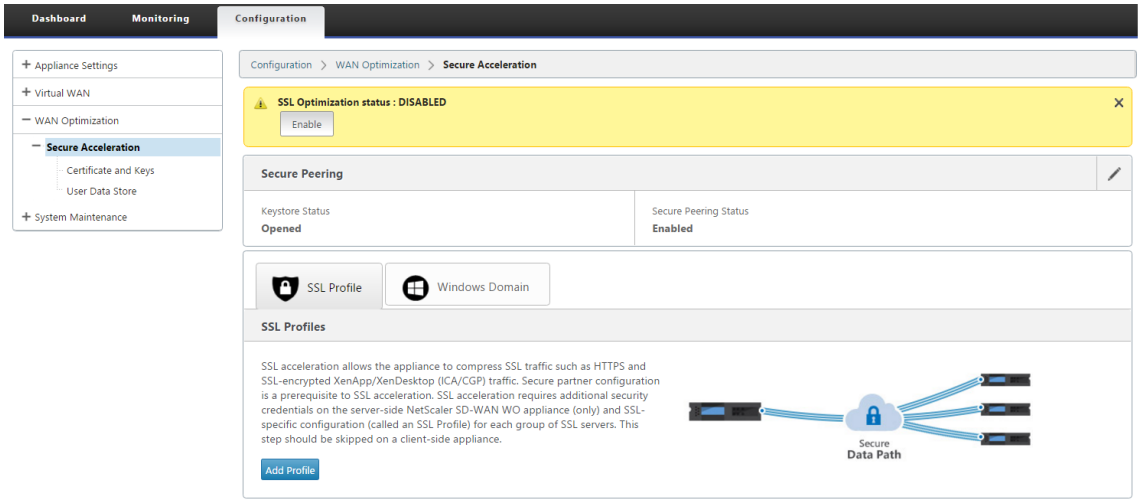
配置

您可以直接从 SDWAN-SE 配置 页面在 **APPFLOW** 节点下配置 **APPFLOW**。这使 SDWAN-SE 能够充当配置 APPFLOW 和其他数据处理配置属性（如服务类、应用程序分类器）的单个窗格。在 SDWAN-SE 上完成的配置反映了 SDWAN-WO 配置，保持了无缝的 APPFLOW 功能支持。



Citrix Application Delivery Management (ADM) 已发现 SD-WANOP，如果在双盒模式下使用，则应隔离并且在关闭此模式之前不使用 Citrix ADM 进行配置。这是因为 WANOP 用于流量处理的配置由 SD-WAN SE 设备在双盒模式下进行管理。

高级优化或安全加速应直接在 SDWAN-SE 设备上配置，就像我们在 SDWAN-WO 设备上配置的那样。这有助于维护配置的单个窗格，如域加入或安全加速/SSL 配置文件创建高级优化或 SSL 代理。



- 应单独管理 SD-WAN SE 和 SD-WAN WANOP 设备的许可。
- 每个 SD-WAN SE 和 SD-WAN WANOP 设备的软件升级应该使用各自的软件包进行单独管理。例如，对于 SD-WAN SE 和升级 UPG SD-WAN WANOP.
- 应通过 WCCP 部署模式在 SD-WAN SE 和外部 WANOP 设备之间配置数据路径集成。
  - 在数据路径级别，通过 WANOP 和 SE 之间的数据路径集成，在单臂模式下提供 WCCP 和虚拟广域网功能，从而获得优化优势。

统一配置和监视

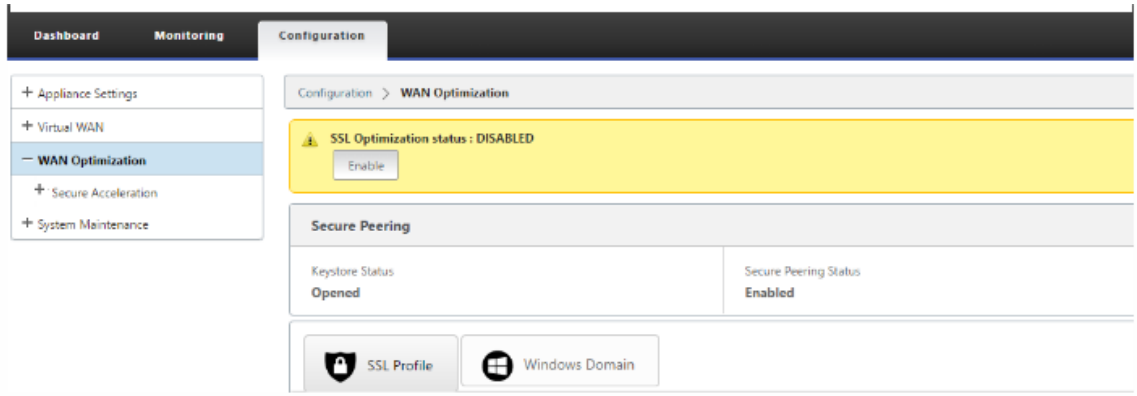
启用 SD-WAN SE 和 SDWAN-WANOP 设备的两个盒子模式时，可以查看 SD-WAN SE 设备中的配置，类似于查看 SD-WAN-EE 设备中的两个盒子配置的方式。

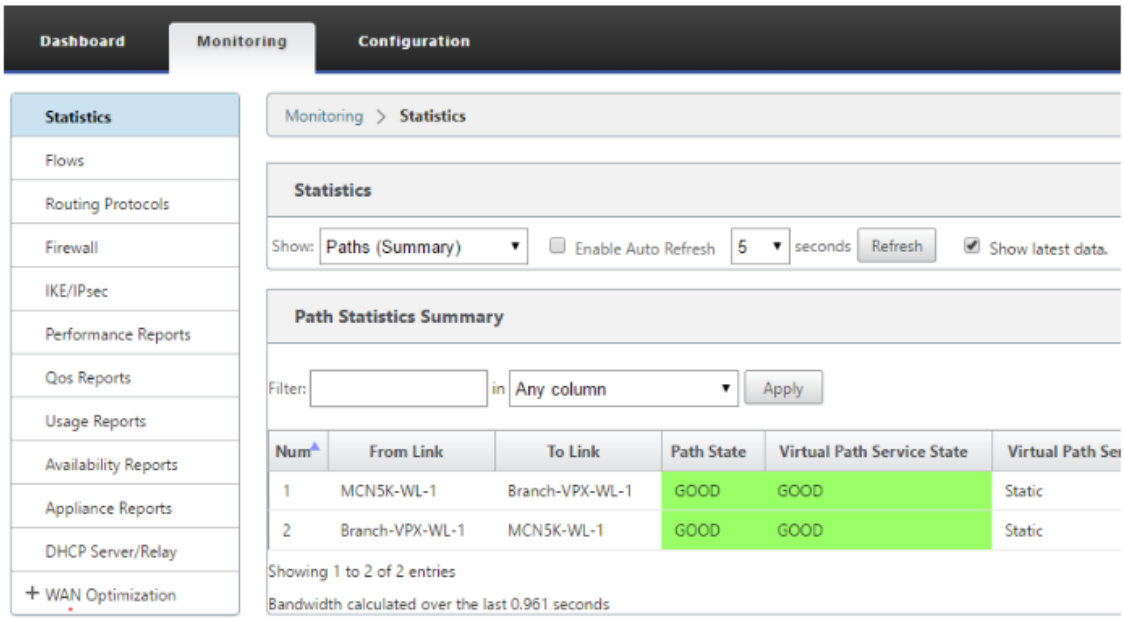
1. 转到 配置 > 虚拟广域网 **>** 广域网优化
2. 配置 > 设备设置下的 AppFlow 节点
3. 配置下的 WAN 优化节点。

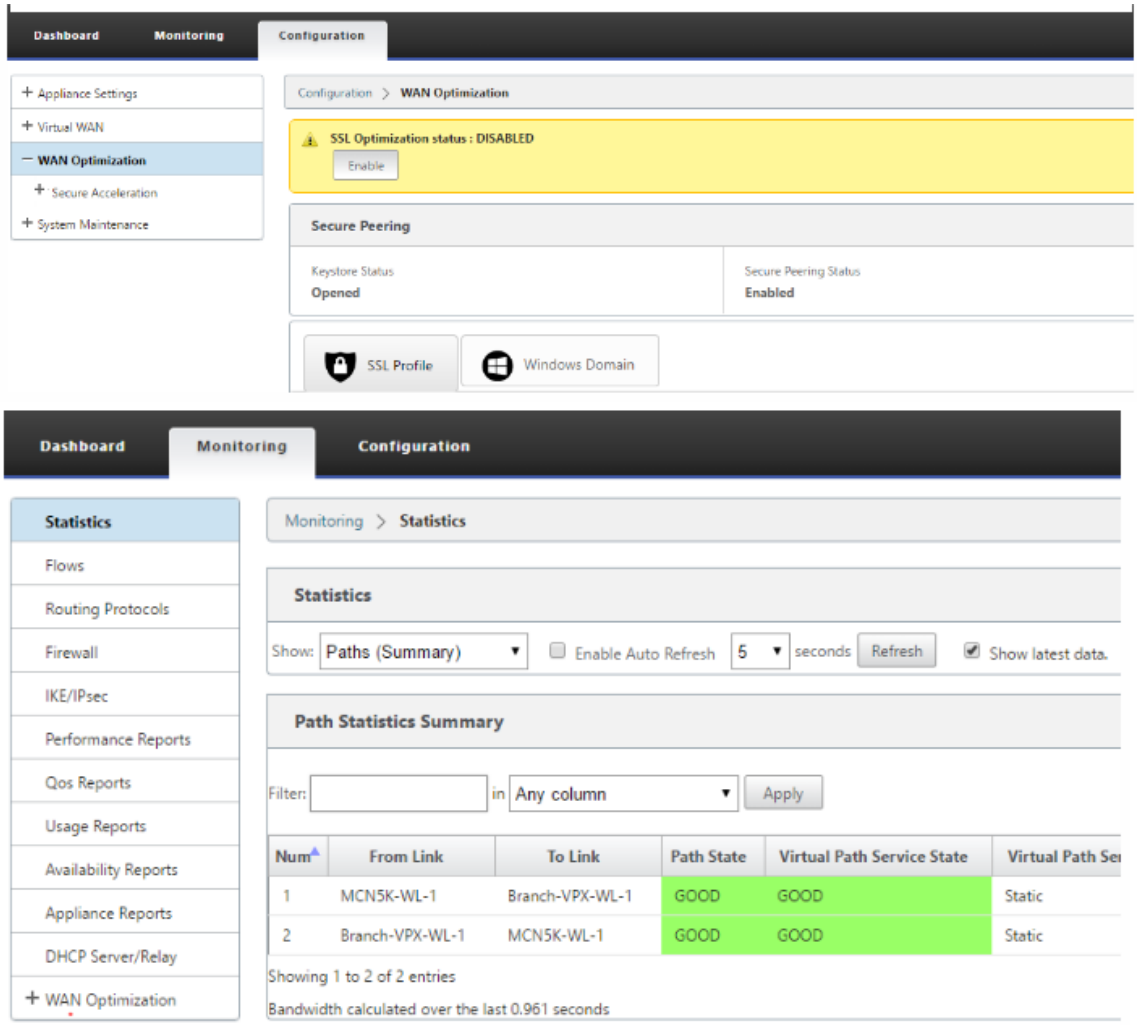
   此信息将从 SD-WAN WANOP 设备重定向，该设备与 SD-WAN SE 设备处于双盒模式。

   与 WANOP 相关的配置，如 SSL 加速和 AppFlow 现在可以从 SD-WAN SE 网页 GUI 执行。

   现在可以在监视 > **WAN** 优化下的 SD-WAN SE Web GUI 中监视与流量相关的统计信息，例如连接、压缩、CIFS/SMB、ICA Advanced、MAPI 和合作伙伴，类似 SD-WAN Premium (Enterprise) 版设备。







双盒模式下 **SD-WANOP** 设备的管理 **IP** 地址变更

要在两箱模式下更改 SDWAN-WANOP 设备的管理 IP 地址，请执行以下操作：

1. 在 SD-WAN SE 设备上执行命令 清除同步。它确保清除 SD-WAN WANOP IP 地址信息以进行 GUI 重定向。
2. 禁用并启用 SD-WAN WANOP 设备上的双盒模式配置。SD-WANOP 设备的新 IP 地址（已更改的 IP）被发送到 SD-WAN SE。新更改的 IP 地址将显示在 URL 重定向页面中。

管理 IP 地址用于对等 IP 地址配置。

在 **SD-WAN WANOP** 设备上禁用两个盒子模式

若要从双盒模式中禁用 SD-WAN WANOP 和 SD-WAN SE 设备或解耦，请执行以下操作：

1. 从 SD-WAN WANOP 设备禁用双盒模式。

2. 它预计会看到 SD-WAN WANOP 设备两个盒式模式页面在 SD-WAN SE Web GUI 中。要清除这些页面，请执行命 令：清除同步。

高可用性

November 1, 2021

本主题介绍 SD-WAN 设备（标准版和高级（企业版）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：

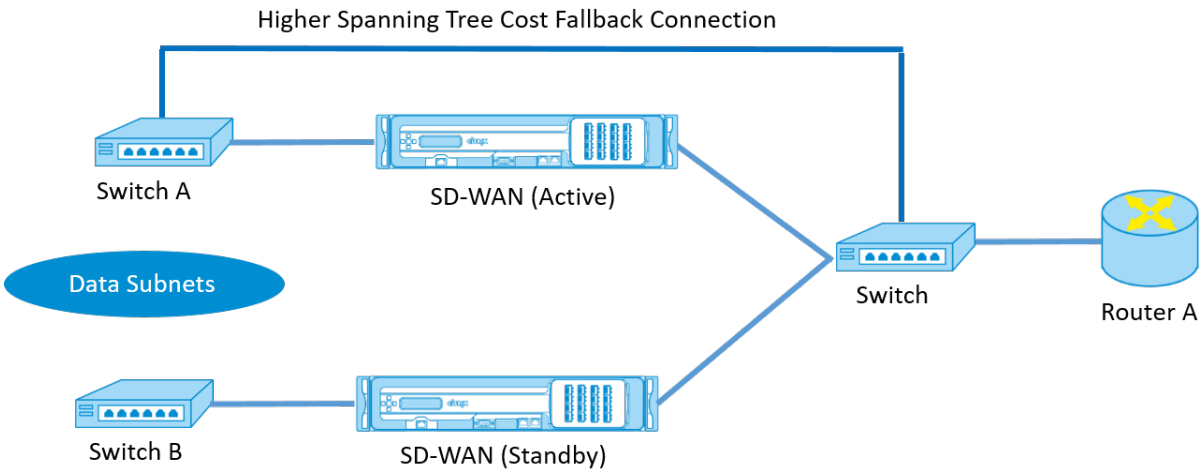
  只要 SD-WAN 设备之一处于活动状态，即使虚拟路径处于关闭状态，活动流量也会流动。SD-WAN 设备将流量重定向回路由器，作为内部网流量。但是，如果两个活动/备用 SD-WAN 设备都变为非活动状态，路由器会尝试将流量重定向到设备。如果下一台设备无法访问，则可以在路由器上配置 IP SLA 监视以禁用 PBR。它允许路由器回退以执行路由查找并适当转发数据包。

并行内联高可用性模式：

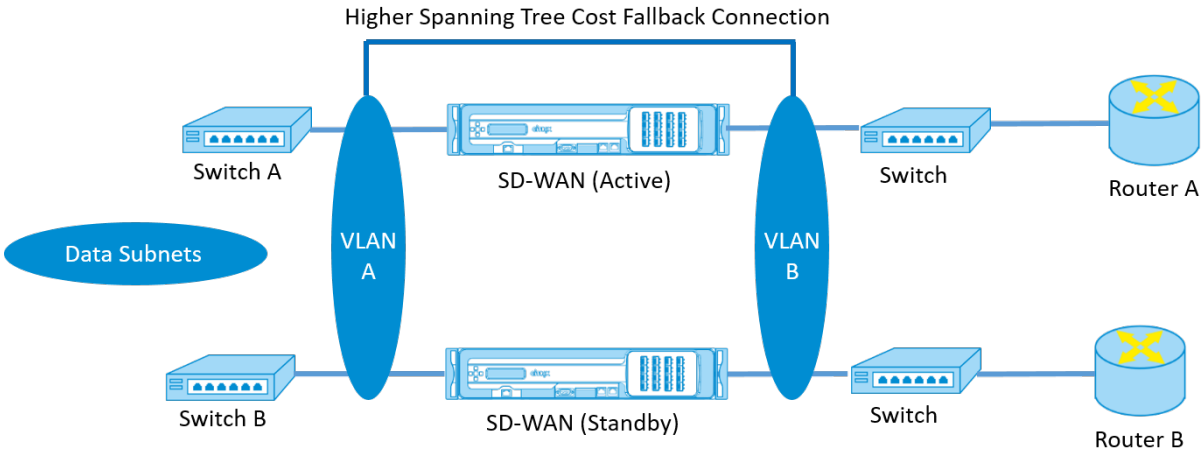
在并行内联高可用性模式下，SD-WAN 设备彼此并行部署，并与数据路径内联。只使用通过活动设备的一个路径。请注意，绕过接口组被配置为故障到块，以避免故障转移过程中的桥接环路。

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。



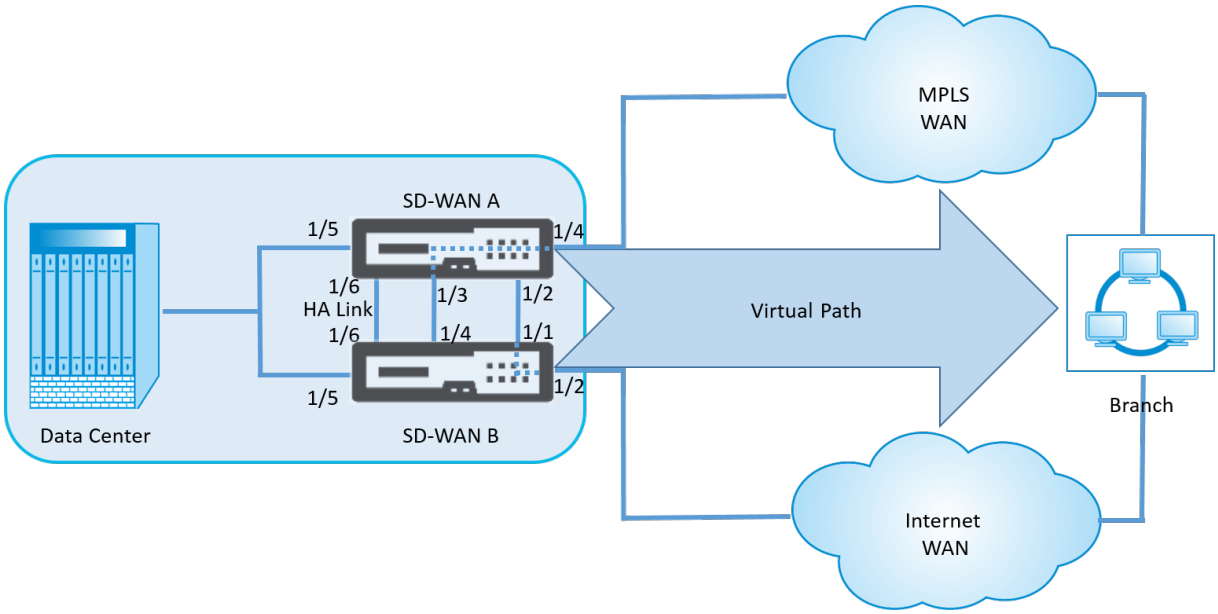
故障到线模式：

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。



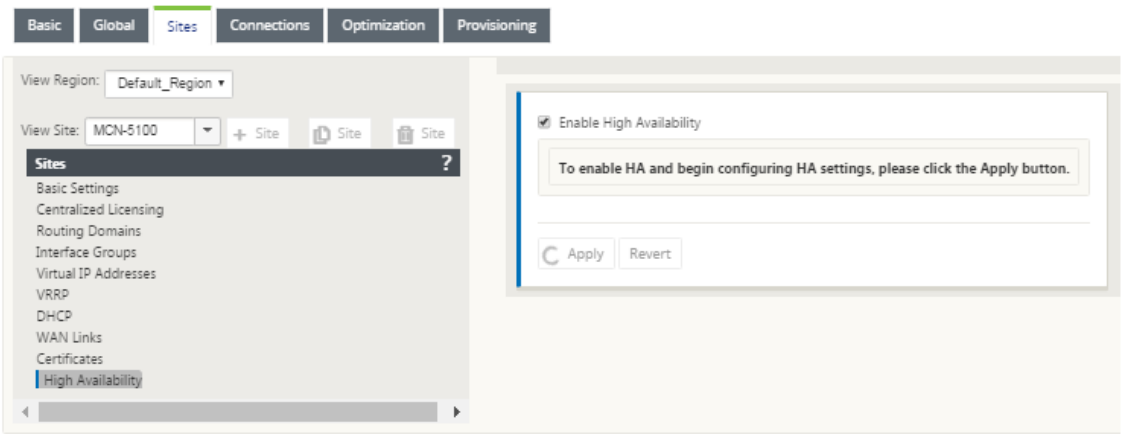
对于转发大量流量的数据中心或站点，建议使用 One-Arm 高可用性配置或并行内联高可用性配置，以最大限度地减少故障转移期间的干扰。

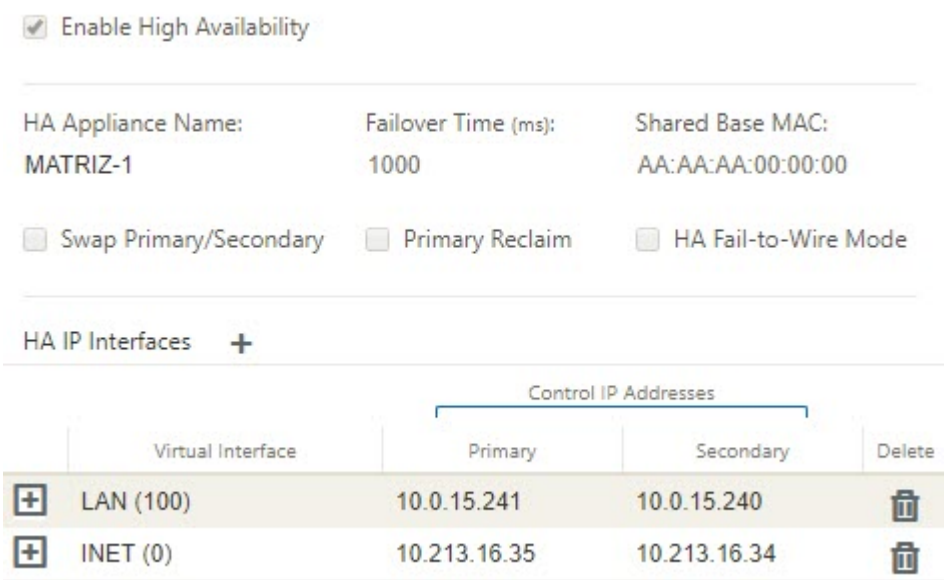
如果在故障转移期间可以接受最小的服务损失，则故障到线高可用性模式是更好的解决方案。故障到线高可用性模式可防止设备故障，并行内联高可用性可防止所有故障。在所有情况下，高可用性对于在系统故障期间保持 SD-WAN 网络的连续性都很有价值。

配置高可用性

要配置高可用性：

1. 在配置编辑器中，导航到 站点 **>** 站点名称 > 高可用性。选择启用高可用性，然后单击应用。





2. 键入以下参数的值：

   - 高可用性设备名称：高可用性（辅助）设备的名称。
   - 故障转移时间：与主设备的联系丢失后，备用设备变为活动状态之前的等待时间（以毫秒为单位）。
   - 共享基本 **MAC**：高可用性对设备的共享 MAC 地址。发生故障转移时，辅助设备具有与发生故障的主设备相同的虚拟 MAC 地址。
   - 交换主设备/辅助设备：选择此选项后，如果高可用性对中的两个设备同时出现，则辅助设备将成为主设备，并优先。

- 主要回收：选中此选项后，指定的主设备将在故障切换事件发生后重新启动时回收控制权。
- 高可用性故障到线模式：选择此选项可启用故障到线高可用性部署模式。

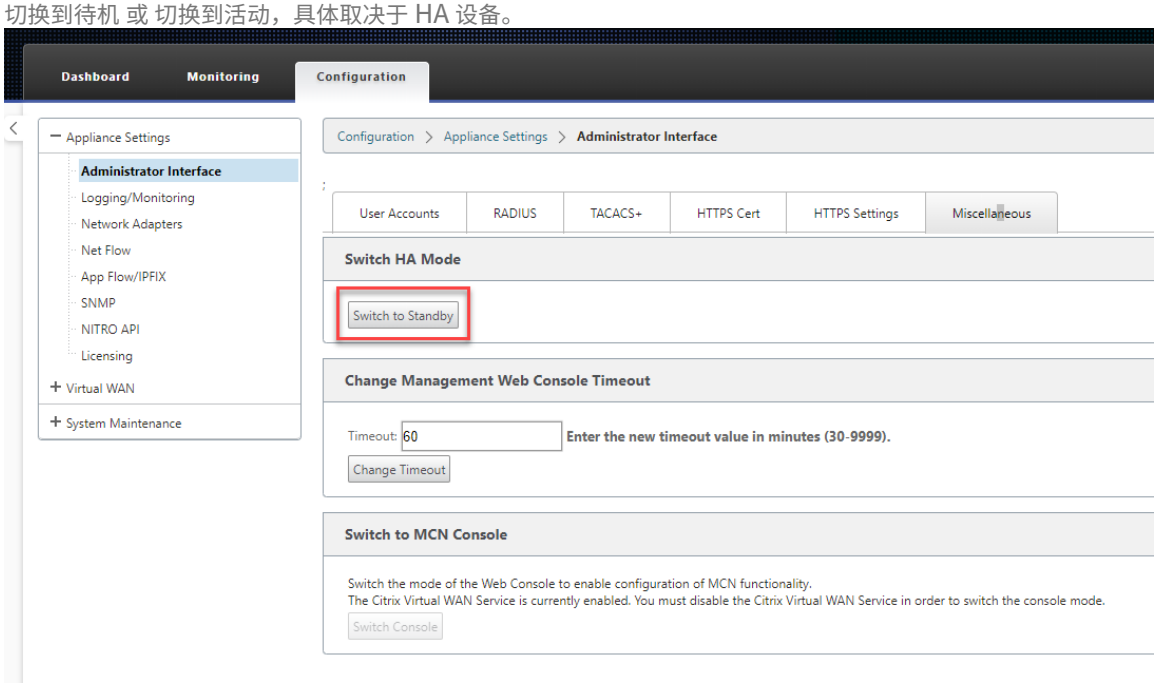
> 注意
>
> 对于虚拟机管理程序和基于云的平台，请选择 禁用 **Shared Base MAC** 选项以禁用共享虚拟 MAC 地址。
>
> 对于基于 Hypervisor 的平台，请确保在虚拟机管理程序上启用混杂模式，以允许从高可用性共享 MAC 地址进行数据包采购。如果未启用混杂模式，则可以启用“禁用共享基础 **MAC** ”选项。

单击 高可用性 **IP** 接口旁边的 + 以配置接口组。键入以下参数的值：

- 虚拟接口—用于高可用性对中设备之间的通信的虚拟接口。它监视活动设备的可达性。对于单臂高可用性模式，只需要一个接口组。
- 主设备 - 主设备的唯一虚拟 IP 地址。辅助设备使用主虚拟 IP 地址与主设备进行通信。
- 辅助 - 辅助设备的唯一虚拟 IP 地址。主设备使用辅助虚拟 IP 地址与辅助设备通信。

单击新的 高可用性 **IP** 接口 条目左侧的 **+**。在“外部 跟踪 **IP** 地址”字段中，键入响应 ARP 请求的外部设备的 IP 地址以确定主装置的状态，然后单击应 用。

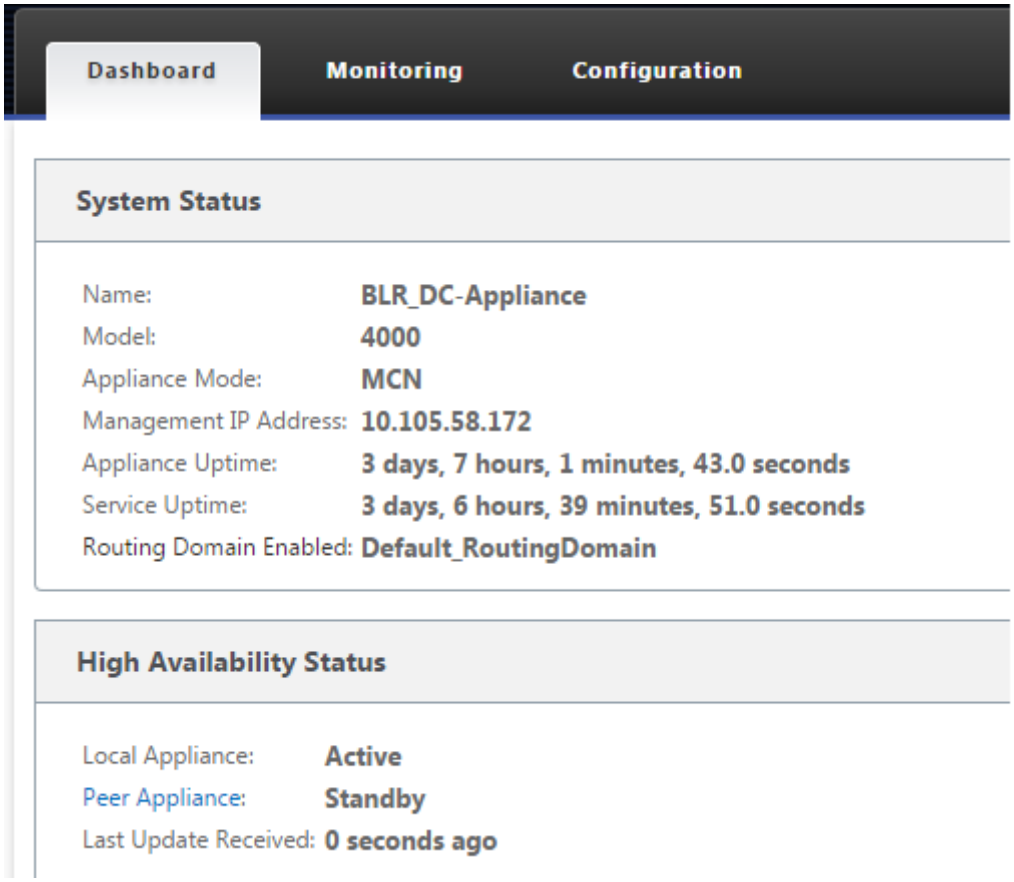
> 注意：
>
> 您还可以从设备手动触发 HA 切换。导航到 配置 > 装置设置 > 管理员界面 > 其他。在 切换 HA 模式 部分中，单击 切换到待机 或 切换到活动，具体取决于 HA 设备。

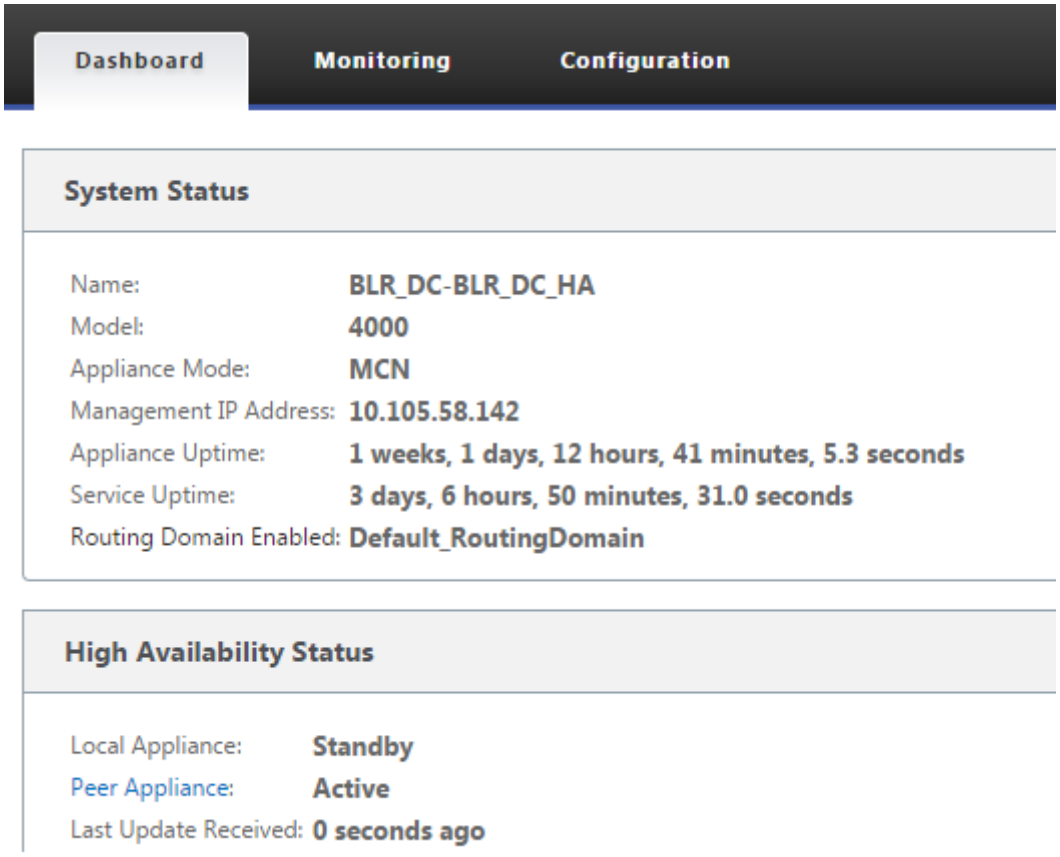


监视

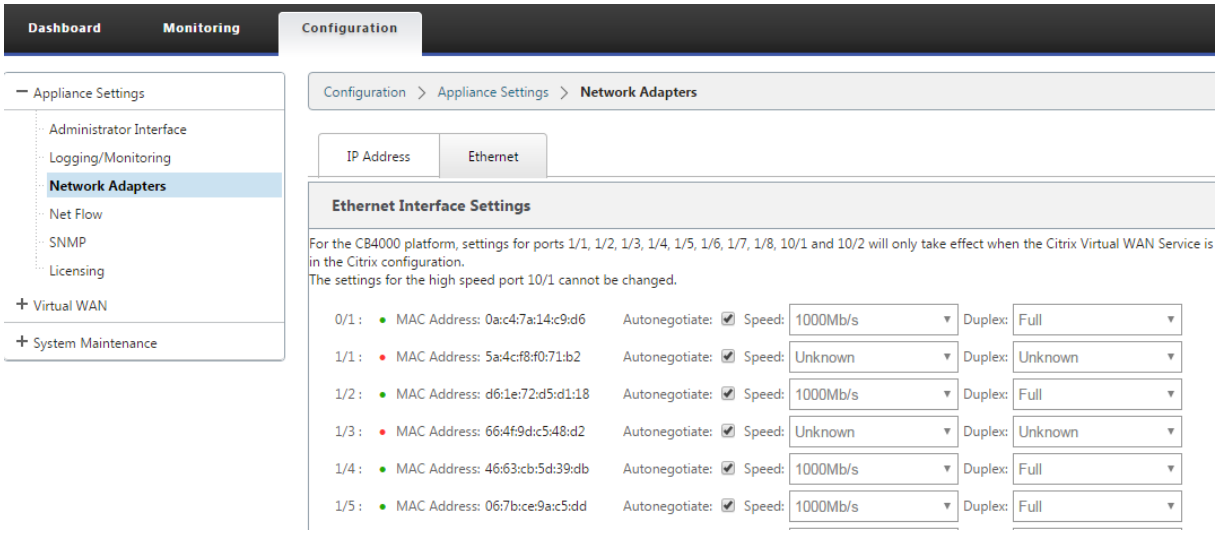
要监视高可用性配置，请执行以下操作：

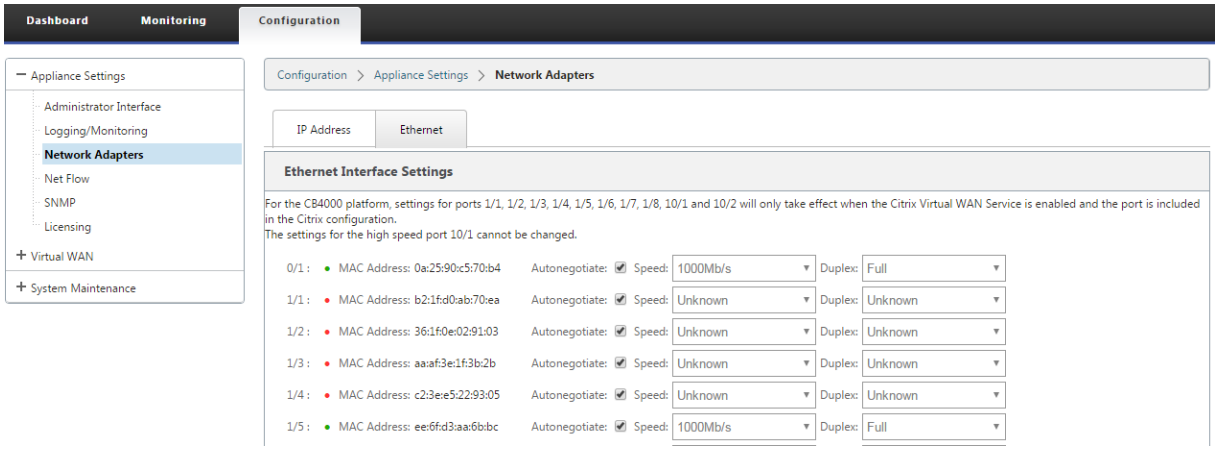
登录到已实现高可用性的活动和备用设备的 SD-WAN Web 管理界面。在 控制板 选项卡下查看高可用性状态。





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。

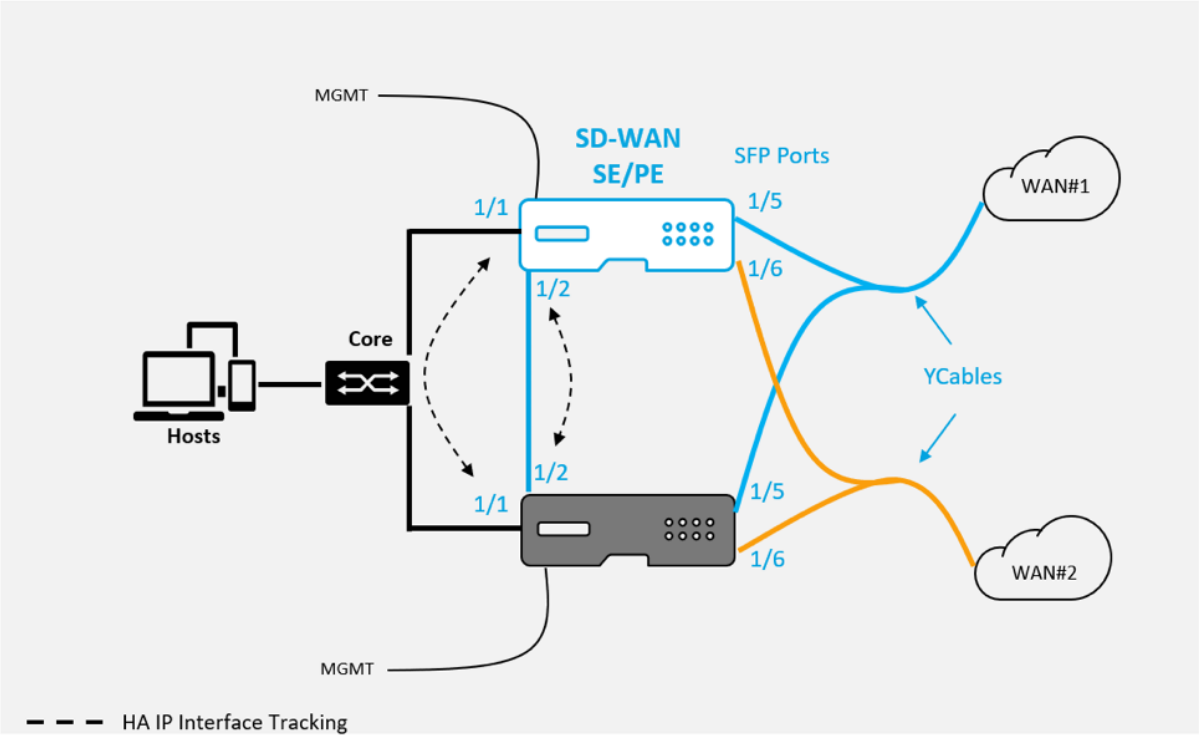
使用光纤 Y 电缆实现边缘模式高可用性

September 26, 2023

> 注意：在 10.2 版本 2 中，此功能仅适用于 1100 SE/PE 设备。

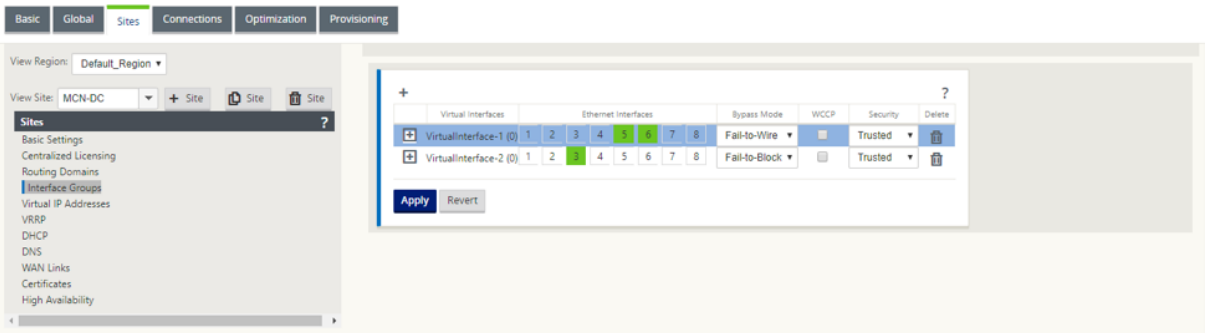
以下过程介绍了在边缘模式中部署的 1100 SE/PE 设备上启用高可用性 (HA) 的步骤，其中 WAN 链路服务提供商的切换是光纤。
1100 设备上的可用小型可插拔 (SFP) 端口可与光纤 Y 电缆一起使用，以实现边缘模式部署的高可用性功能。
在 1100 SE/PE 设备上，分离器电缆分离端连接到两台 1100 台设备的光纤端口，这两台设备采用 HA 对配置。

光纤 Y 型电缆有三端。一端连接到提供程序的光纤切换，另外两端连接到在 HA 对中部署的两台 1100 SE/PE 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。



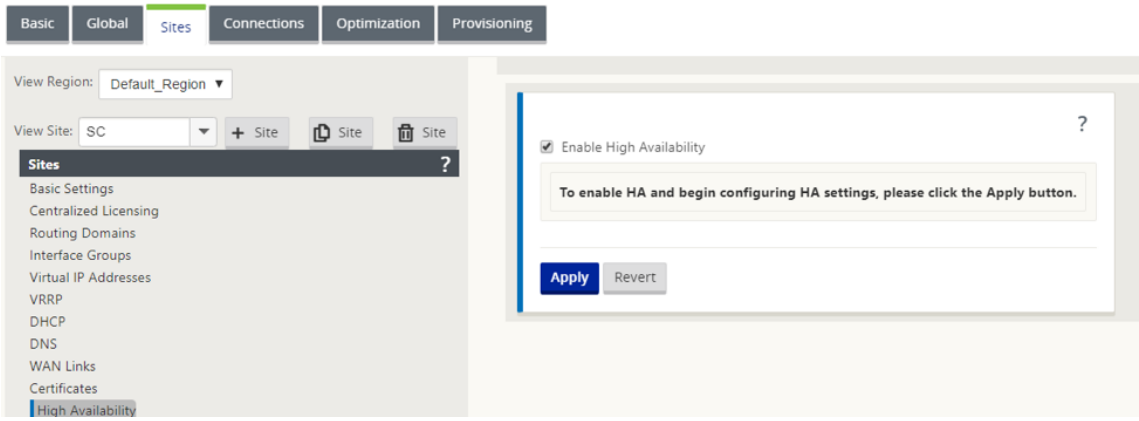
必备条件：

1. 在 1100 SE/PE 设备上，1/5 和 1/6 端口是 SFP 端口。将 Y 电缆的分离器端连接到 HA 对中的两个设备上的任何一个端口，请参阅1100 SE了解更多信息。
2. 将 SFP 端口添加到 SD-WAN 设备配置。配置 SFP 端口与配置任何网络接口端口相同。有关详细信息，请参阅如何配置接口组。将 1/5 或 1/6 端口添加到配置允许您启用 Y 型电缆支持功能。

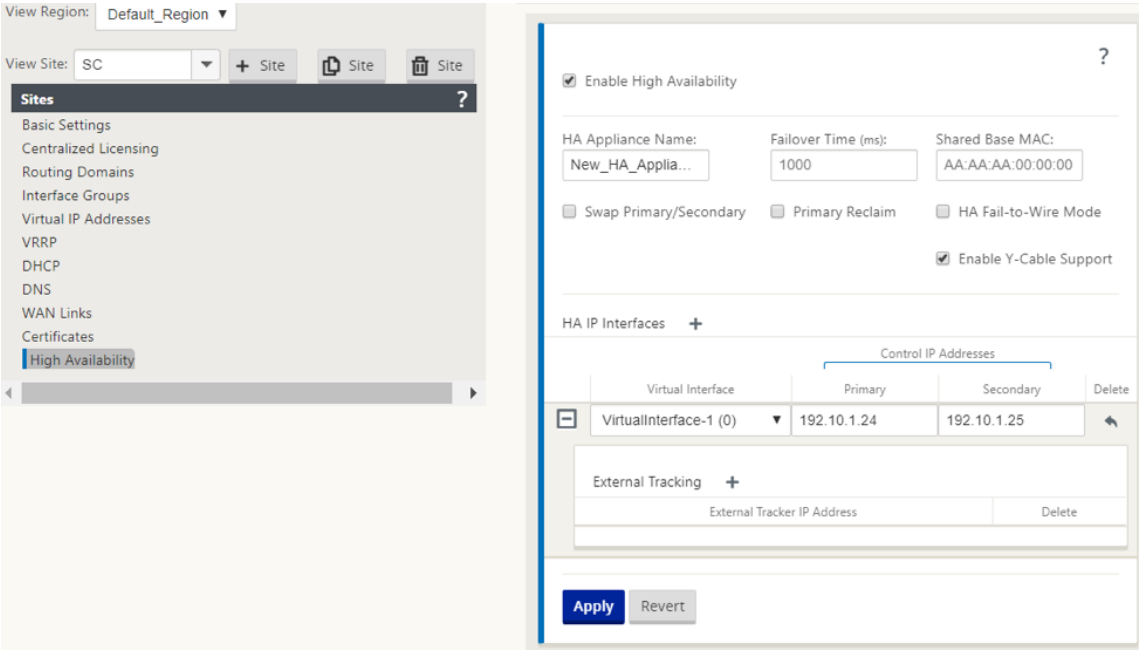


要使用 Y 型电缆实现高可用性：

1. 在 1100 SE/PE 设备 GUI 中，导航到 配置 > 虚拟广域网 > 配置编辑器 > 站点。单击 启用高可用性。



2. 单击 启用 **Y** 型电缆支持。
3. 添加 HA IP 接口，除了连接到 Y 型电缆的接口（例如 1/1 局域网接口，或 1/2 直接连接的接口）。启用 Y 电缆功能后，SFP 端口无法用于 HA IP 接口。



4. 应用、暂停和激活配置。

限制：

- 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

November 1, 2021

> 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 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition（需要重新创建映像)
> - SD-WAN 1000 企业版（高级版）（需要重新映像）
> - SD-WAN 1100 标准版
> - SD-WAN 1100 Premium (Enterprise) Edition
> - SD-WAN 2000 标准版（需要重新映像）
> - SD-WAN 2000 企业版（高级版（需要重新映像）
> - SD-WAN 2100 Enterprise Edition (Premium 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互联网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。

零接触部署云服务与后端 Citrix 服务安全地通信，托管已购买零接触功能设备（例如 SD-WAN 410-SE、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。

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：

- 使用 Citrix SD-WAN Center 网络配置工具创建配置，或从主控制节点 (MCN) SD-WAN 设备导入配置
- Citrix Cloud 登录为新站点节点部署启动零接触部署服务。

  > 注意
  >
  > 如果您的 SD-WAN Center 通过代理服务器连接到 Internet，则必须在 SD-WAN Center 上配置代理服务器设置。有关详细信息，请参阅零接触部署的代理服务器设置。

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

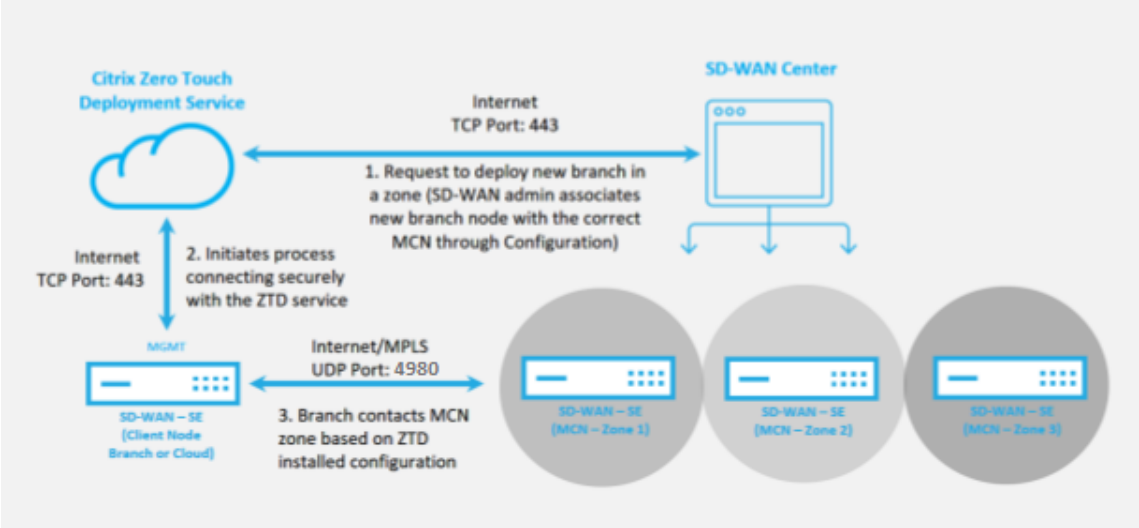
- 如有必要，请将防火墙设置为从 SD-WAN Center 向 FQDN ***sdwanzt.citrixnetworkapi.net*** 出站通信。

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互联网。
- 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。

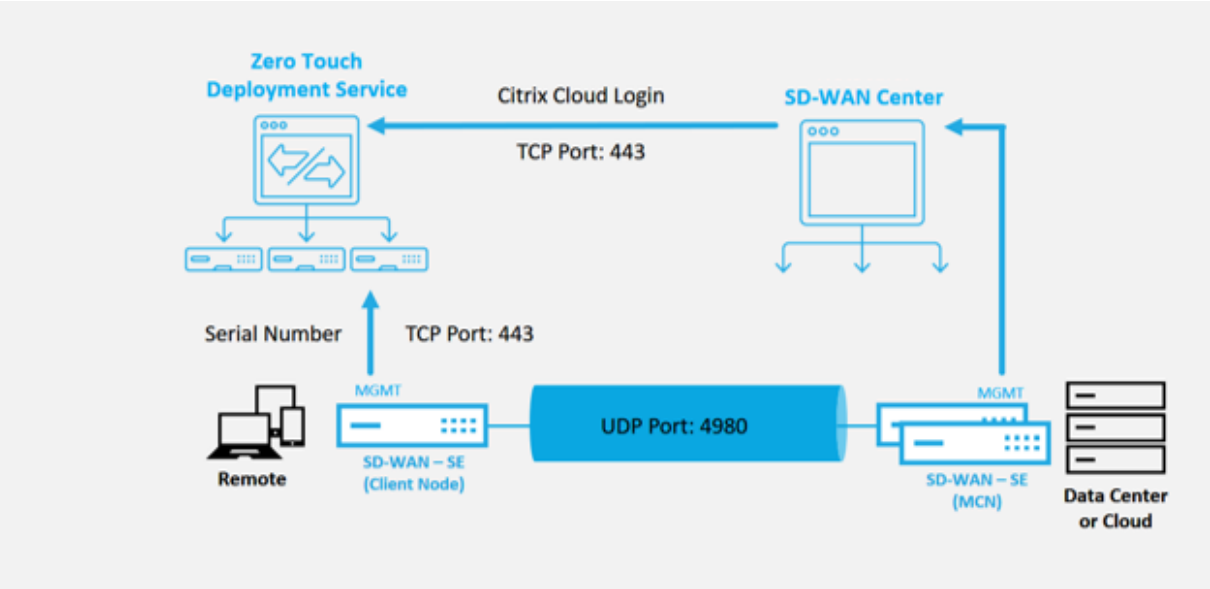
> 注意
>
> 每种型号的接口布局都有所不同，因此请参考有关识别数据和管理端口的文档。



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)。
- 主动运行 SD-WAN 中心，通过虚拟路径连接到 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）。
- 在端口 443 上直接管理或通过代理服务器管理到 Internet 网络连接（SD-WAN Center 和 SD-WAN 设备）。
- （可选）在客户端模式下，至少有一台主动运行在分支机构的 SD-WAN 设备，并且有效的虚拟路径可以连接到 MCN，以帮助验证在现有底层网络中成功建立的路径。

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：

零接触部署服务与 SD-WAN Center 结合使用，以提供更易于部署的分支机构 SD-WAN 设备。SD-WAN 中心配置并用作 SD-WAN 标准和企业（高级）版设备的中央管理工具。要使用零接触部署服务（或零接触部署云服务），管理员必须首先在环境中部署第一台 SD-WAN 设备，然后将 SD-WAN Center 配置并部署为中心管理点。当 SD-WAN 中心（9.1 版或更高版本）在端口 443 上连接到公共互联网的情况下安装时，SD-WAN Center 会自动启动云服务并安装必要的组件，以解锁零接触部署功能，并在 GUI 中提供零接触部署选项 SD-WAN 中心。在 SD-WAN 中心软件中默认情况下，零接触部署不可用。这样做的目的是确保在允许管理员启动任何涉及零接触部署的现场活动之前，底层网络上存在适当的初步组件。

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。由于 SD-WAN Center 能够与零接触部署服务进行通信，GUI 将在“配置”选项卡下显示零接触部署选项。登录零接触服务会验证与特定 SD-WAN 环境关联的客户 ID，并注册 SD-WAN 中心，此外还可解锁帐户以进一步验证零接触部署设备部署的身份。

然后，使用 SD-WAN Center 中的网络配置工具，SD-WAN 管理员将需要使用模板或克隆站点功能来构建 SD-WAN 配置以添加新站点。SD-WAN 中心使用新配置，为新添加的站点启动零接触部署的部署。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。

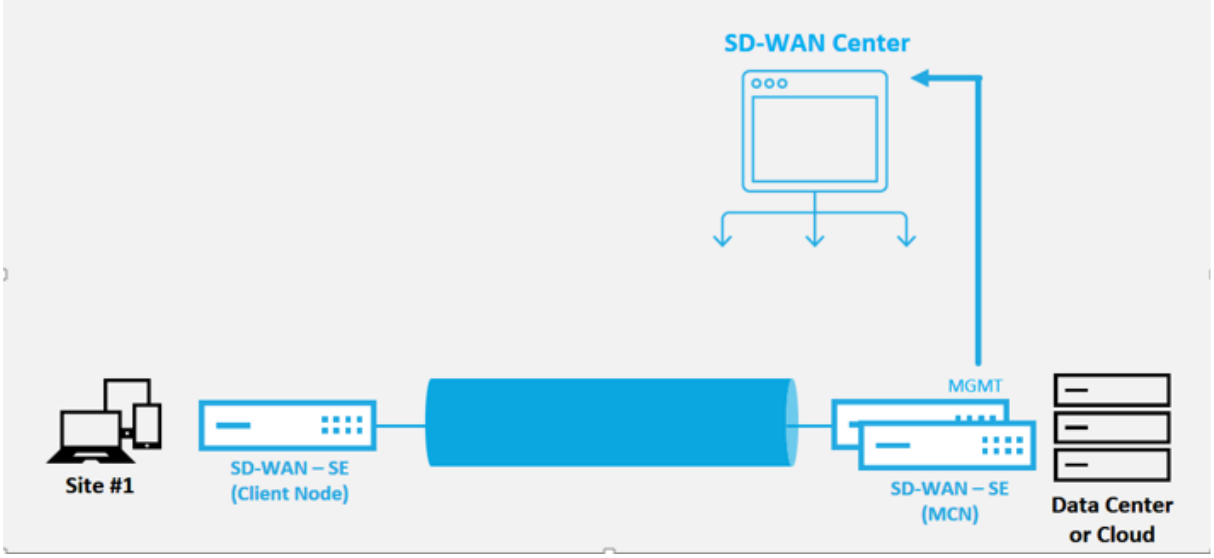
- 通过验证序列号对分支设备进行身份验证。
- 验证 SD-WAN 管理员是否使用 SD-WAN 中心接受该站点进行零接触部署。
- 从 SD-WAN Center 拉出目标设备特定的配置文件。
- 将特定于目标设备的配置文件推送到分支设备。
- 在分支设备上安装配置文件。
- 将任何丢失的 SD-WAN 软件组件或所需更新推送到分支设备。
- 推送一个临时 10 Mbps 许可证文件，以确认与分支设备建立的虚拟路径。
- 在分支设备上启用 SD-WAN 服务。

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。

零接触部署设备过程

以下过程详细介绍了使用零接触部署服务部署新站点所需的步骤。有一个正在运行的 MCN 和一个客户端节点已经在与 SD-WAN Center 进行正常通信，并建立虚拟路径来确认整个底层网络的连接。要启动零接触部署，SD-WAN 管理员需要执行以下步骤：



如何配置零接触部署服务

SD-WAN Center 可以接受来自新连接的设备的请求以加入 SD-WAN Enterprise 网络。请求通过零接触部署服务转发到 Web 界面。设备连接到服务后，将下载配置和软件升级软件包。

配置工作流程：

- 访问 **SD-WAN Center** > 创建新站点配置 或导入现有配置并保存。
- 登录到 Citrix Cloud 以启用零接触部署服务。“零接触部署”菜单选项现在显示在 SD-WAN 中心 Web 管理界面中。
- 在 SD-WAN Center 中，导航到 配置 > 零接触部署 **>** 部署新站点。
- 选择一个设备，单击 启用，然后单击部署。
- 安装程序会收到激活电子邮件 > 输入序列号 > 激 活 > 设备已成功部署。

要配置零接触部署服务，请执行以下操作：

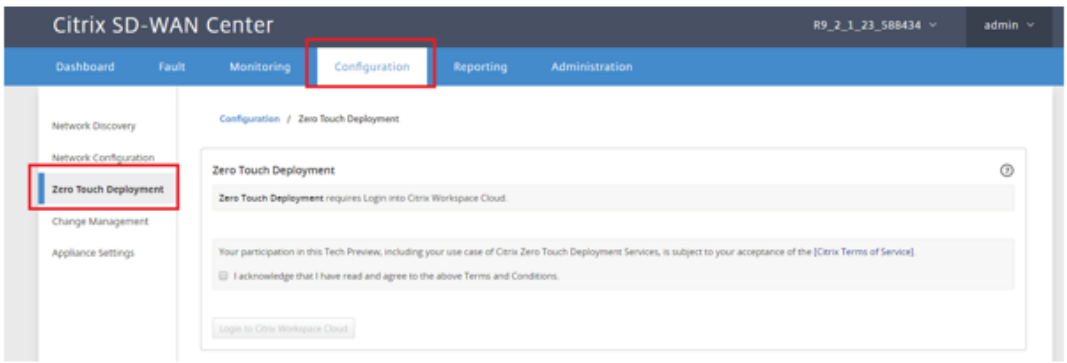
1. 使用启用的零接触部署功能安装 SD-WAN Center：

   a) 使用 DHCP 分配的 IP 地址安装 SD-WAN 中心。

   b) 验证 SD-WAN Center 是否分配了正确的管理 IP 地址和网络 DNS 地址，并通过管理网络与公用 Internet 建立连接。

   c) 将 SD-WAN 中心升级到最新的 SD-WAN 软件版本。

   d) 通过适当的互联网连接，SD-WAN Center 将启动零接触部署云服务，并自动下载并安装特定于零接触部署的任何固件更新，如果此 Call Home 过程失败，则 GUI 中将不可用以下零接触部署选项。

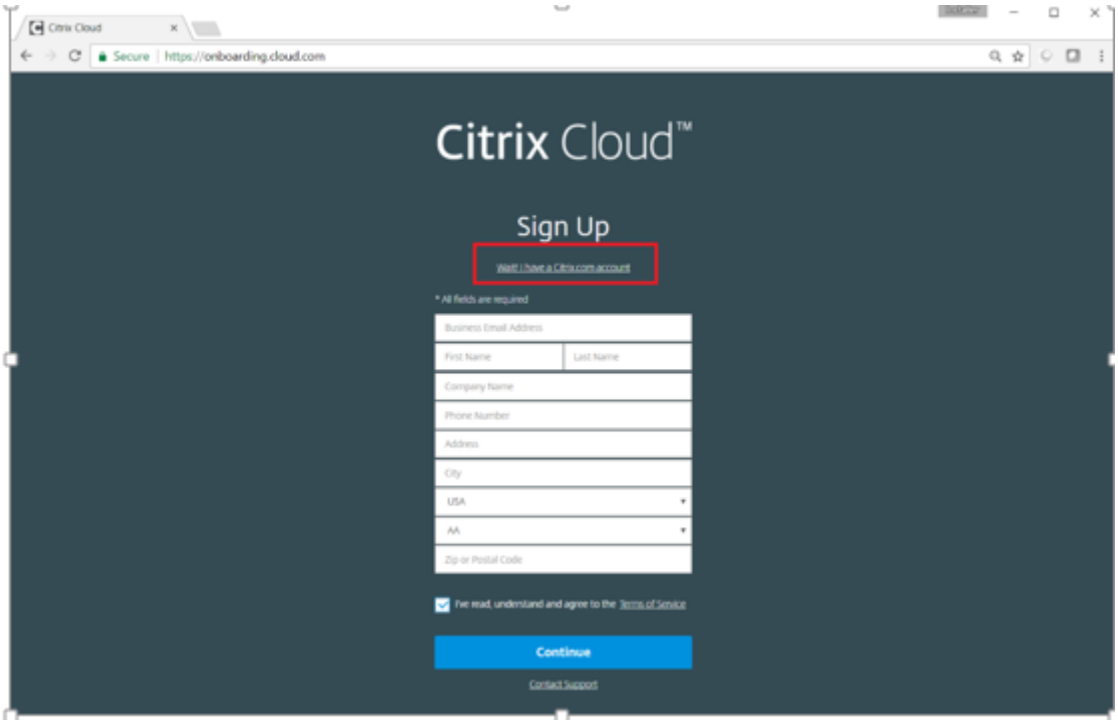


   e) 阅读条款和条件，然后选择 我确认我已阅读并同意上述条款和条件。

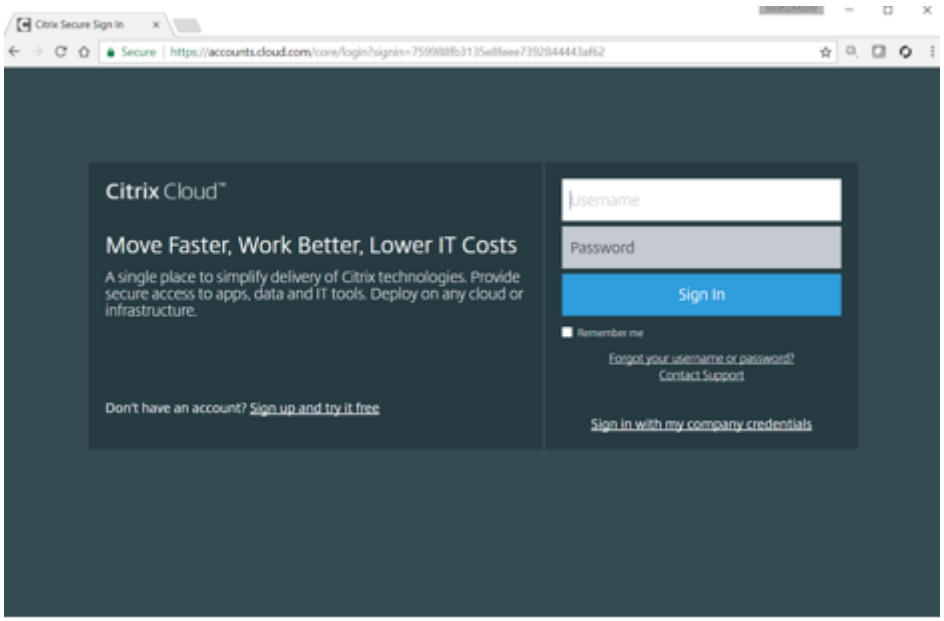
   f) 如果已创建 Citrix Cloud 帐户，请单击登录 **Citrix Workspace** 云按钮。

   g) 登录 Citrix Cloud 帐户，在收到以下成功登录消息后，请不要关闭此窗口，此过程需要约 **20** 秒才能刷新 **SD-WAN CENTER GUI**。窗口完成后必须自行关闭。

2. 要创建 Cloud Login 帐户，请按照以下步骤操作：打开网络浏览器进入 https://onboarding.cloud.com
3. 点击“等待”的链接，我有一个 **Citrix.com** 帐户。



4. 使用现有 Citrix 帐户登录。



5. 登录到 SD-WAN 中心零接触部署页面后，您可能会注意到没有站点可用于零接触部署，原因如下：

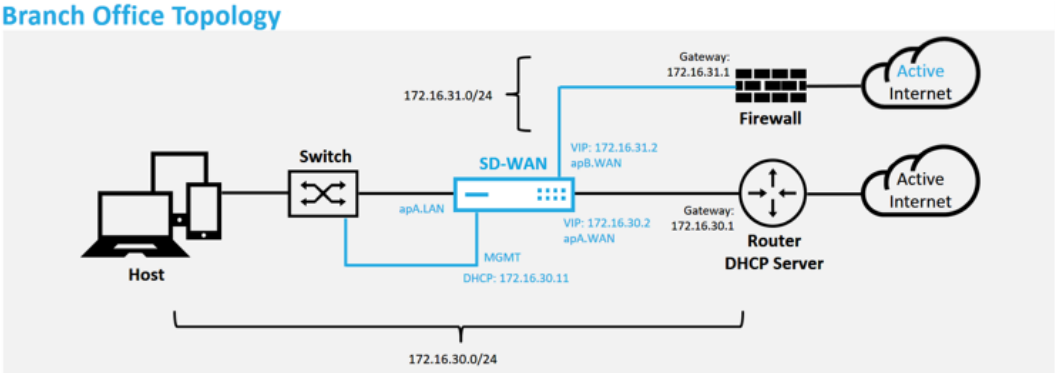
   - 尚未从 配置 下拉菜单中选择活动配置
   - 当前活动配置的所有站点都已部署
   - 配置不是使用 SD-WAN Center 建立的，而是在 MCN 上可用的配置编辑器
   - 站点未在引用零触摸功能设备的配置中构建（例如 410-SE、21000-SE、云 VPX）

6. 更新配置，以使用 **ZTD** 功能的 **SD** 设备 (使用 SD-WAN Center 网络配置）添加新远程站点。

   如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。必须使用以下过程添加针对零接触部署的新站点。

   a) 通过首先列出新站点的详细信息（即设备型号、接口组使用情况、虚拟 IP 地址、带宽与带宽及其各自的网关），为 SD-WAN 设备部署设计新站点。

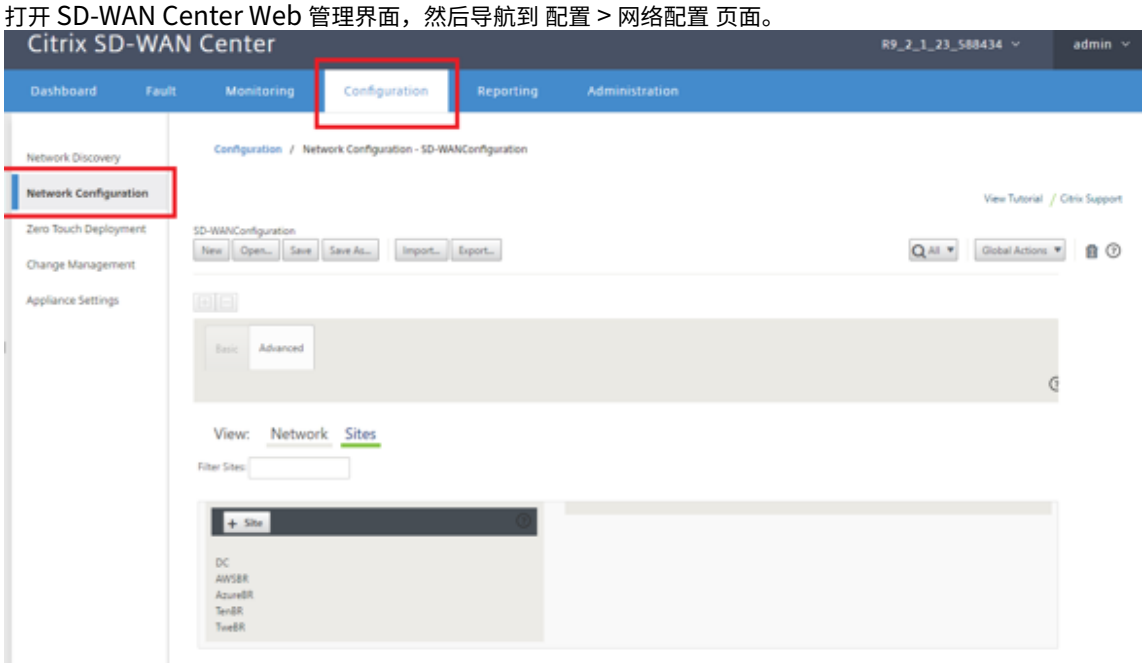
   > 重要
   >
   > 您可能会注意到任何已选择 VPX 作为模型的站点节点也会被列出，但当前零接触部署支持仅适用于 AWS VPX 实例。
   >
   > 注意
   >
   > - 请务必使用 Citrix SD-WAN Center 支持的 Web 浏览器
   > - 确保在 Citrix Workspace 登录期间 Web 浏览器未阻止任何弹出窗口



这是分支机构站点的部署示例，SD 设备物理上部署在 172.16.30.0/24 网络中的现有 MPLS WAN 链接的路径中，并通过将现有备份链接启用为“活动”状态并将其终止而使用现有备份链接。WAN 链接直接连接到不同子网 172.16.31.0/24 上的 SD-WAN 设备。

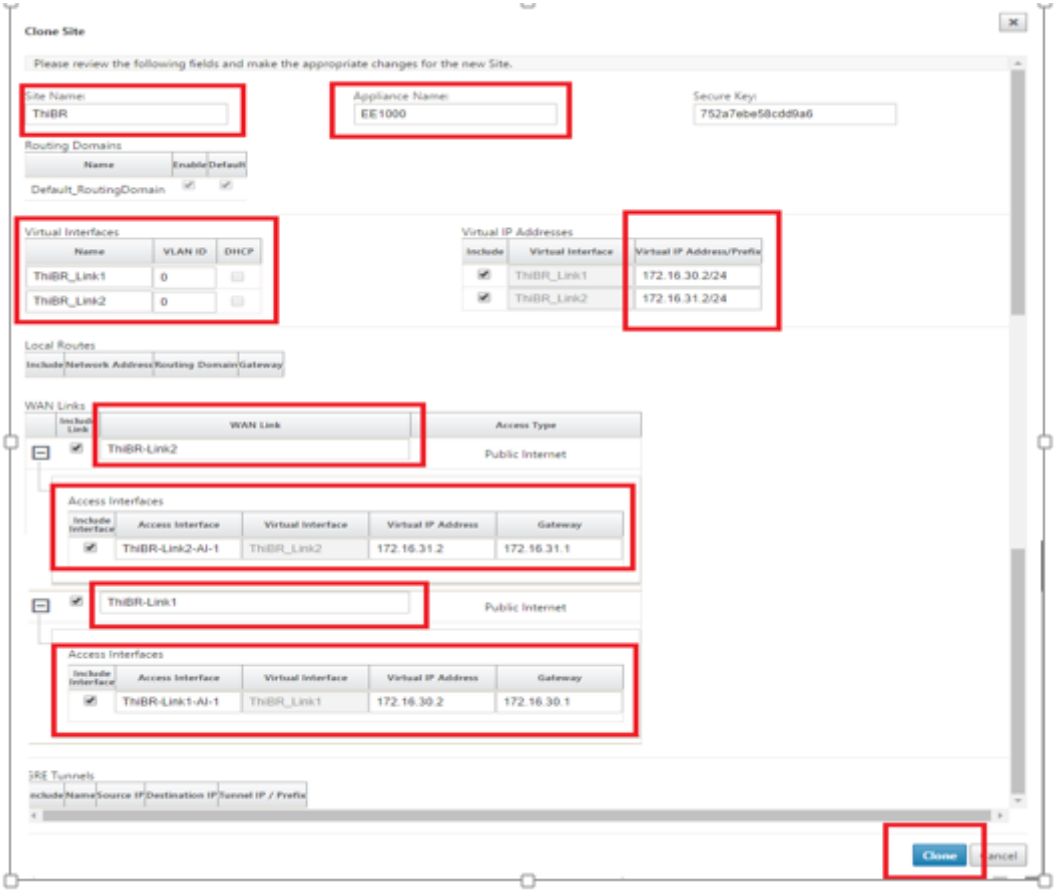
> 注意
>
> SD-WAN 设备可自动分配默认 IP 地址 192.168.100.1/16。默认启用 DHCP 后，网络中的 DHCP 服务器可能会在与默认值重叠的子网中为设备提供第二个 IP 地址。这可能会导致设备上的路由问题，即设备可能无法连接到零接触部署 Cloud Service。将 DHCP 服务器配置为分配在 192.168.0.0/16 范围内的 IP 地址。
>
> 有各种不同的部署模式可用于在网络中放置 SD-WAN 产品。在上面的示例中，将在现有网络基础结构的顶部将 SD-WAN 部署为覆盖。对于新站点，SD-WAN 管理员可以选择在边缘或网关模式部署 SD-WAN，从而无需使用 WAN 边缘路由器和防火墙，并将边缘路由和防火墙的网络需求整合到 SD-WAN 解决方案中。

7. 打开 SD-WAN Center Web 管理界面，然后导航到 配置 > 网络配置 页面。

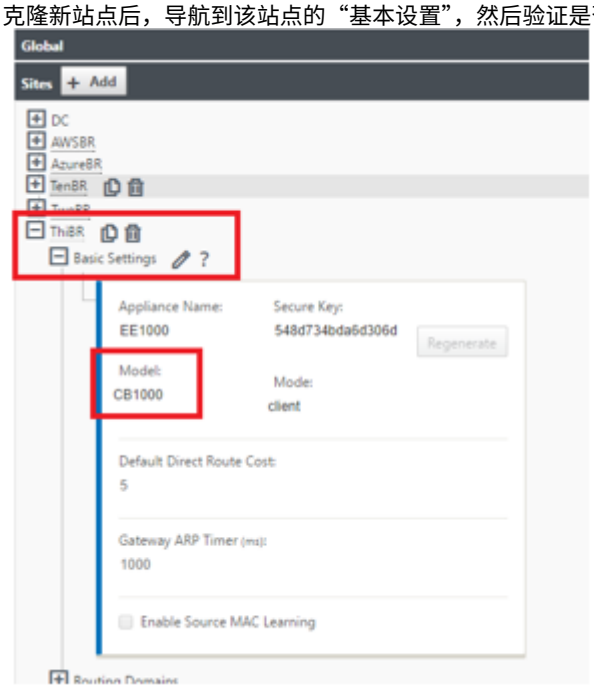


8. 确保已有工作配置，或者从 MCN 导入配置。
9. 导航到 高级 选项卡以创建站点。
10. 打开 站点 磁贴以显示当前配置的站点。
11. 使用任何现有站点的克隆功能快速构建新站点的配置。

12. 填充为此新分支站点设计的拓扑中的所有必填字段



13. 克隆新站点后，导航到该站点的“基本设置”，然后验证是否正确选择了支持零接触服务的 SD-WAN 型号。

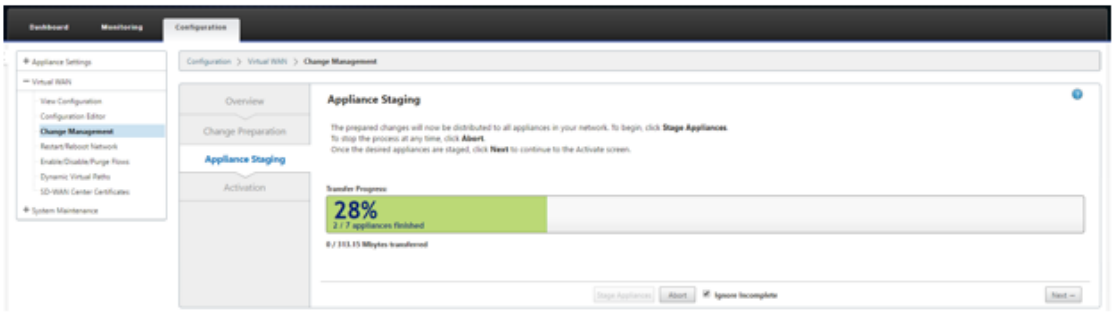


可以更新站点的 SD-WAN 模型，但请注意，可能需要重新定义接口组，因为更新后的设备的接口布局可能比用

于克隆的布局更新。

14. 在 SD-WAN Center 上保存新配置，然后使用“导出到 更改管理收件箱”选项使用“更改管理”推送配置。

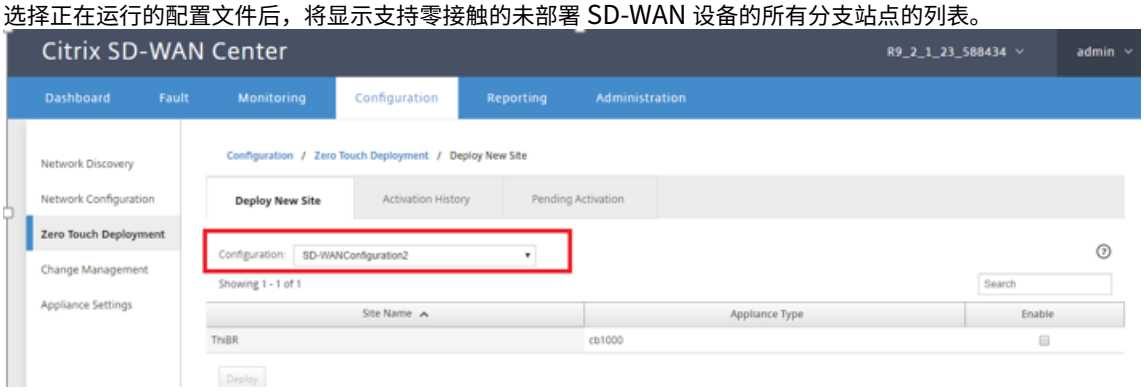
15. 按照变更管理过程正确暂存新配置，这样可以使现有的 SD-WAN 设备知道要通过零接触部署的新站点，您必须使用“忽略不完整”选项来跳过尝试将配置推送到仍然必须通过的新站点的尝试零接触部署工作流程。



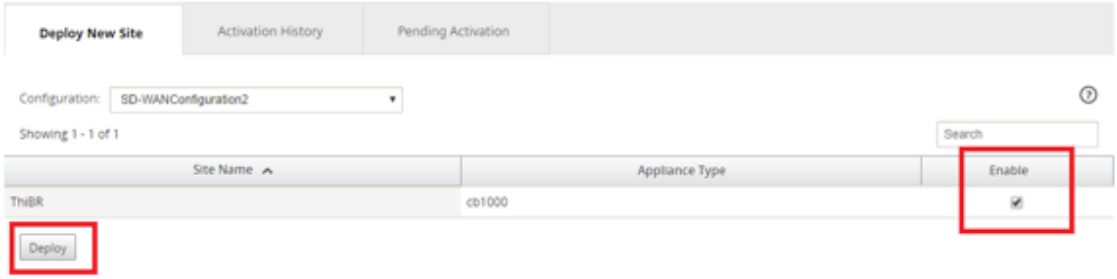
16. 导航回 SD-WAN Center 零接触部署页面，在运行新的活动配置的情况下，将有新站点可供部署。

17. 在零接触部署页面的“部 署新站点”选项卡下，选择正在运行的网络配置文件

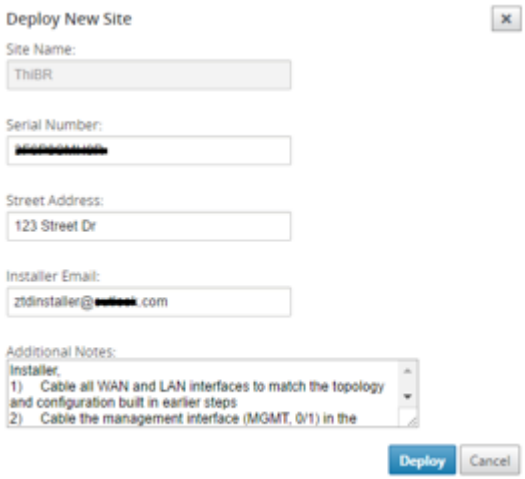
18. 选择正在运行的配置文件后，将显示支持零接触的未部署 SD-WAN 设备的所有分支站点的列表。



19. 选择要为零接触服务配置的分支站点，单击 启用，然后单击 部署。



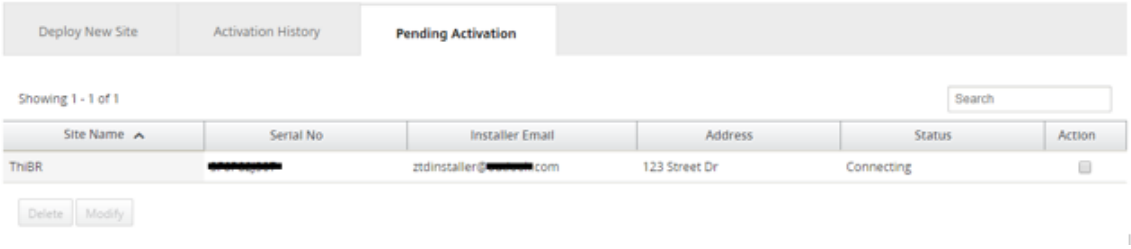
20. 此时将显示部署新站点弹出窗口，在此窗口中，管理员可以提供序列号、分支站点街道地址、安装程序电子邮件地址以及其他备忘录（如有必要）。



> 注意
>
> “序列号”条目字段为可选字段，如果填充了此字段，则会导致安装程序负责在现场活动中进行更改。
>
> > - 如果填充了序列号字段—安装程序不需要在使用部署站点命令生成的激活 URL 中输入序列号
> >
> > - 如果序列号字段保留为黑色—安装程序将负责在将设备的序列号更正到使用部署站点命令生成的激活 URL 中

21. 单击部署按钮后，将显示一条消息，指出“站点配置已部署”。此操作将触发 SD-WAN 中心（该中心先前注册到零接触部署云服务）共享此特定站点的配置，以便在零接触部署云服务中存储。

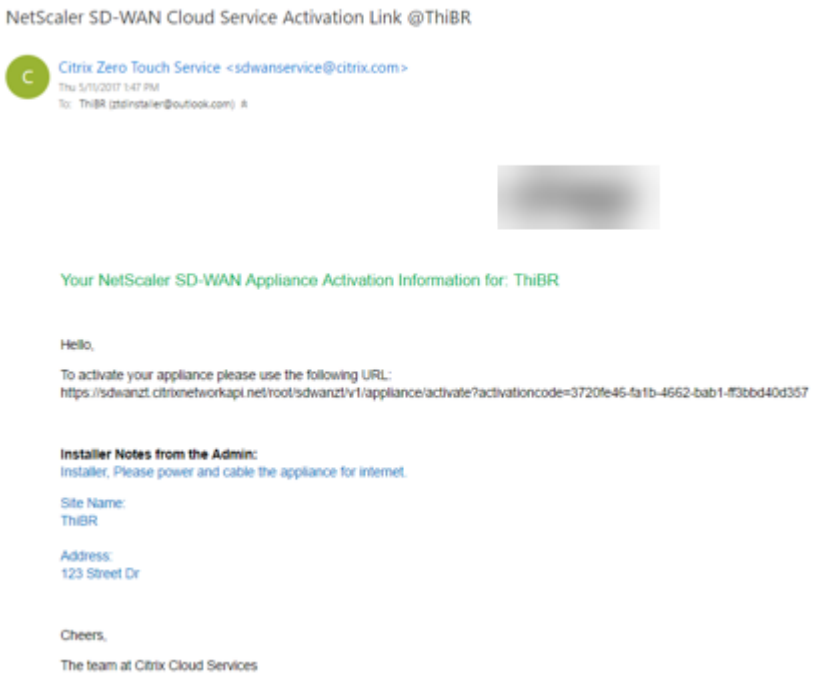
22. 导航到“挂起的激活”选项卡，确认已成功填充分支站点信息，并将其设置为待执行的安装程序活动状态。



> 注意
>
> 如果信息不正确，则可以选择处于“挂起激活”状态的零接触部署来删除或修改。如果从“挂起的激活”页面中删除了一个站点，该站点将可以在部署新站点选项卡页面中部署。选择将分支站点从挂起的激活中删除后，发送到安装程序的激活链接将失效。
>
> 如果 SD-WAN 管理员未填充序列号字段，则状态字段指示“等待安装程序”而不是“正在连接”。

23. 下一系列活动由现场安装程序执行。

    a) 安装程序验证 SD-WAN 管理员在部署站点时使用的电子邮件地址的邮箱。



b) 在互联网浏览器窗口中打开零接触部署激活 URL(例如 `https://sdwanzt.citrixnetworkapi.net`)。

c) 如果 SD-WAN 管理员未在部署站点步骤中预填充序列号，则安装程序将负责找到物理设备上的序列号，并手动将序列号输入到激活 URL 中，然后单击激活按钮。

d) 如果管理员预填充序列号信息，激活 URL 将一直准备执行下一个步骤。

e) 安装程序的物理位置必须在现场，以执行以下操作：

- 连接所有 WAN 和 LAN 接口，使其与之前步骤中构建的拓扑和配置相匹配。

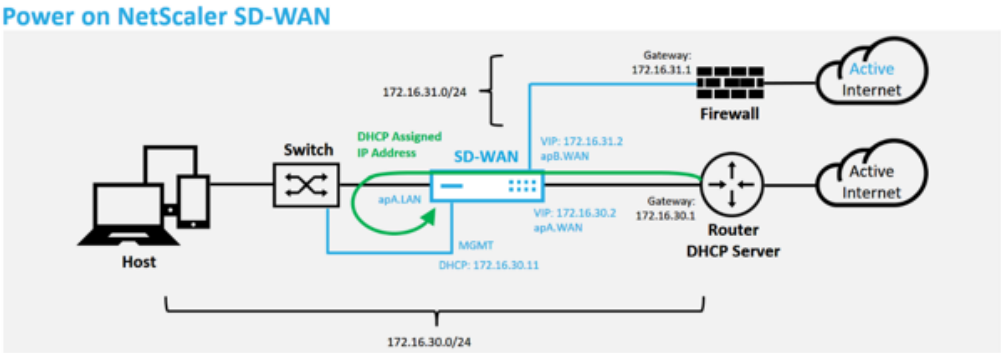
- 在网络中提供 DHCP IP 地址和通过 DNS 将 FQDN 连接到 IP 地址解析的网络段中的管理接口（MGMT、0/1）电缆。
- 电源线 SD-WAN 设备。
- 打开设备的电源开关。

> 注意
>
> 连接电源线时，大多数设备将自动启动。某些设备可能必须使用设备前面的电源开关打开电源，其他设备可能在设备背面安装了电源开关。某些电源开关需要按住电源按钮，直到设备通电。

24. 下一系列步骤通过零接触部署服务的帮助自动完成，但需要使用以下必备条件。

    - 分支设备必须打开电源
    - DHCP 必须在现有网络中可用，以分配管理和 DNS IP 地址
    - 任何 DHCP 分配的 IP 地址都需要连接到互联网并能够解析 FQDN
    - 只要满足其他先决条件，就可以手动配置 IP 分配

    a) 设备从网络 DHCP 服务器获取 IP 地址，在此示例中，拓扑通过出厂默认状态设备的跳过数据接口实现。

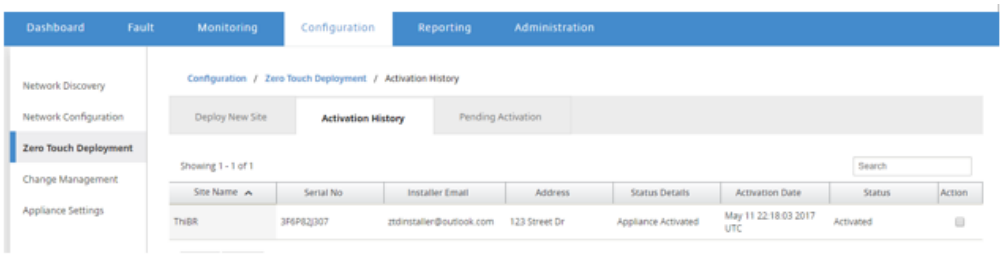


    b) 当设备从底层网络 DHCP 服务器获取 Web 管理和 DNS IP 地址时，设备将启动零接触部署服务并下载任何与零接触部署相关的软件更新。

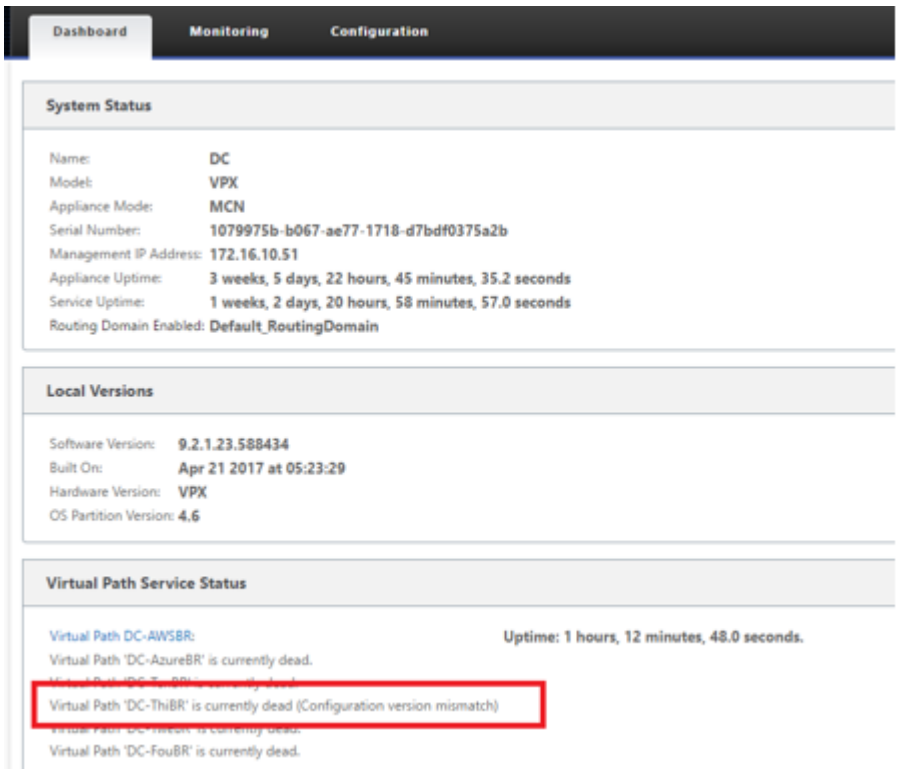
    c) 成功连接到零接触部署云服务后，部署过程会自动执行以下操作：

        - 下载 SD-WAN 中心之前存储的配置文件
        - 将配置应用于本地设备
        - 下载并安装临时 10 MB 许可证文件
        - 下载并安装任何软件更新（如有需要）
        - 激活 SD-WAN 服务

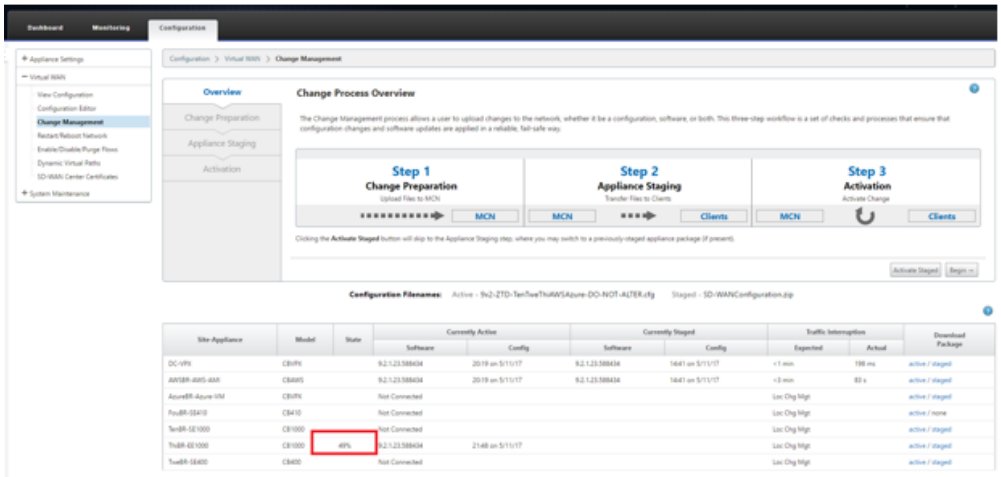
d) 进一步确认可以在 SD-WAN Center Web 管理界面中完成，在激活历史记录选项卡中，“零点触摸部署”菜单显示成功激活的设备。



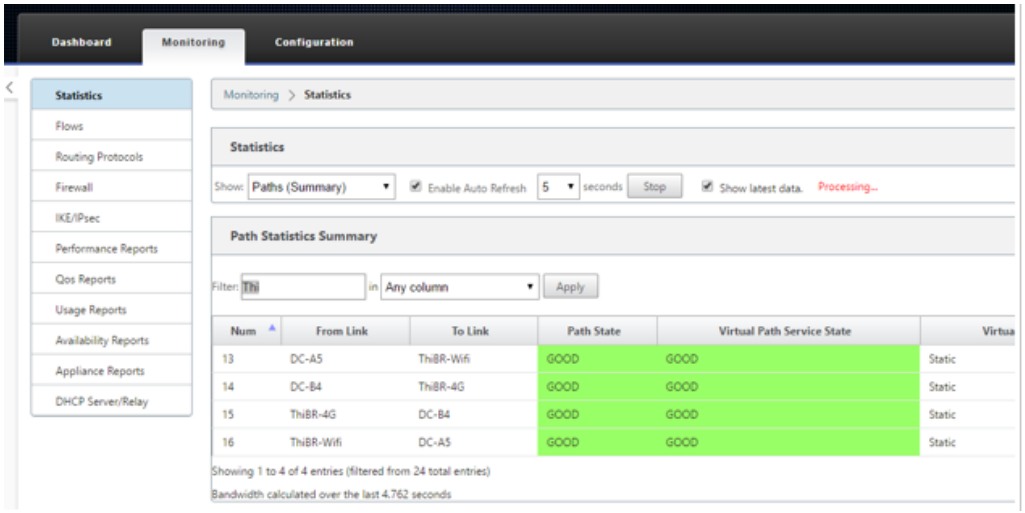
e) 虚拟路径可能不会立即显示为连接状态，因为 MCN 可能不信任从零接触部署云服务传递的配置，并在 MCN 仪表板中报告“配置版本不匹配”。



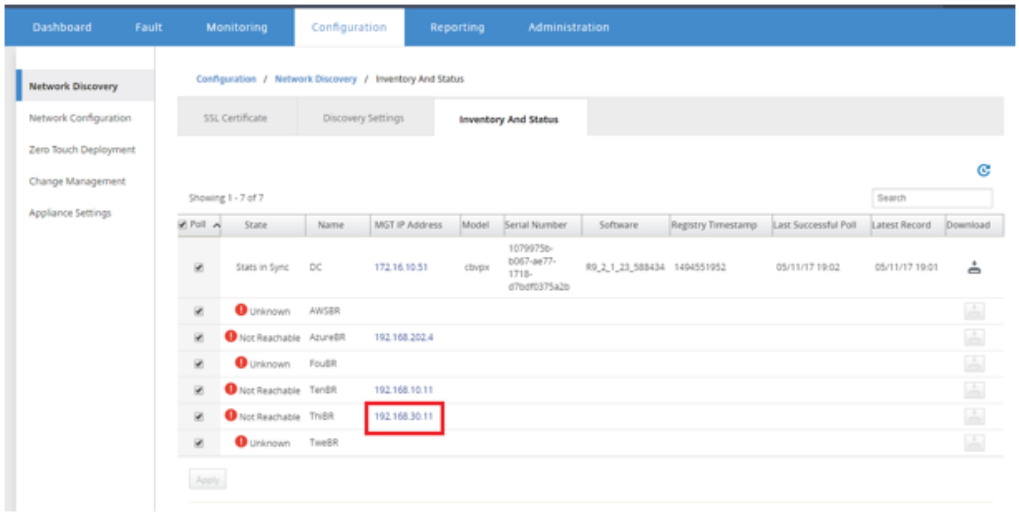
f) 配置将重新传递到新安装的分支机构设备，并在 **MCN** > 配置 > 虚拟 **WAN** > 更改管理 页面上监视状态（此过程可能需要几分钟才能完成）。



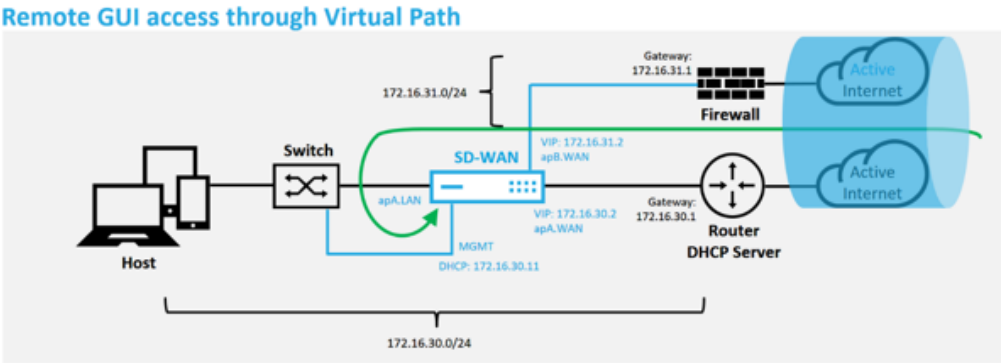
g) SD-WAN 管理员可以监视面向已建立的远程站点虚拟路径的头端 MCN Web 管理页面。



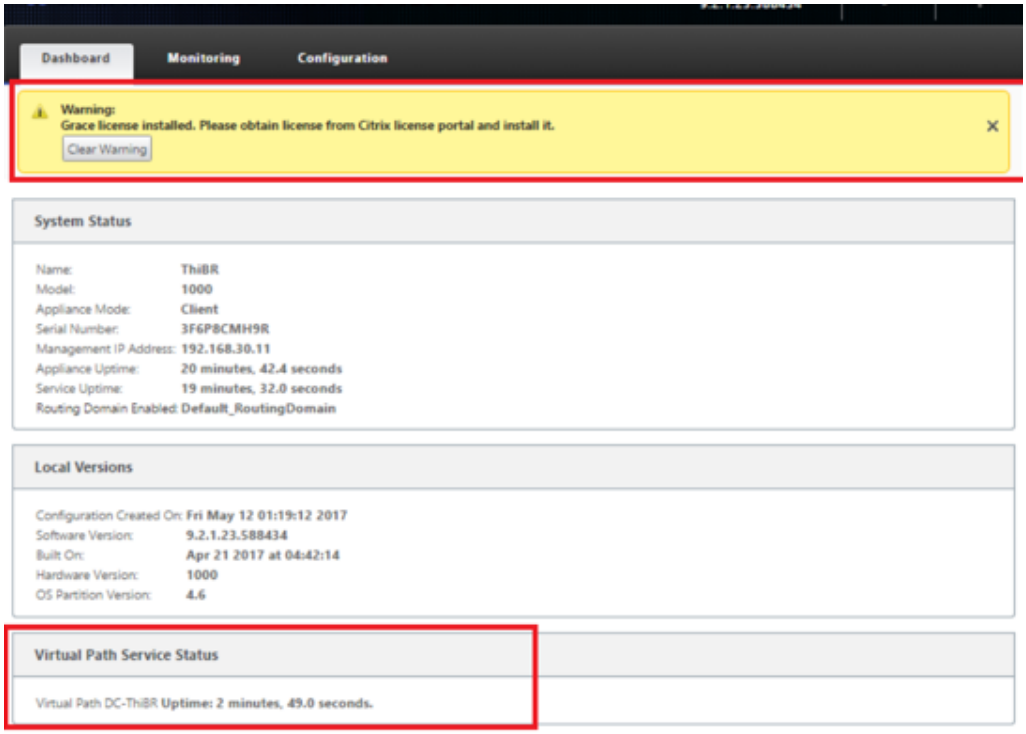
h) SD-WAN Center 还可用于从 配置 **>** 网络发现 **>** 清单和状态页面中识别 **DHCP** 分配的现 场设备的 IP 地址。



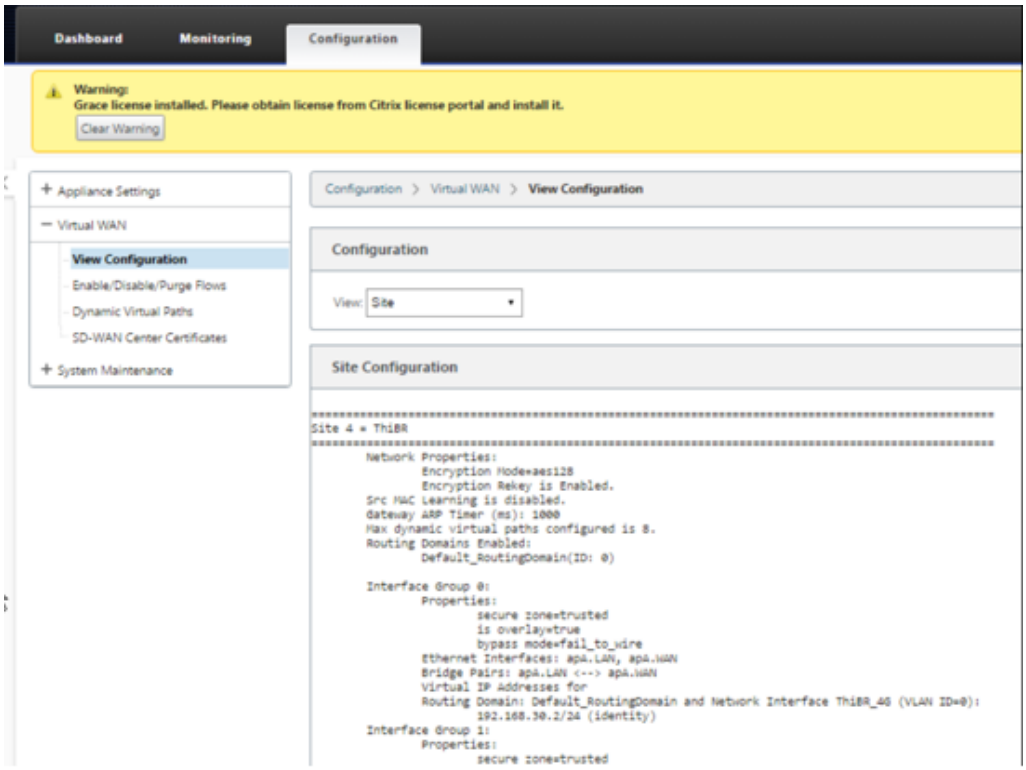
i) 此时，SD-WAN 网络管理员可以使用 SD-WAN 覆盖网络获得对现场设备的 Web 管理访问权限。



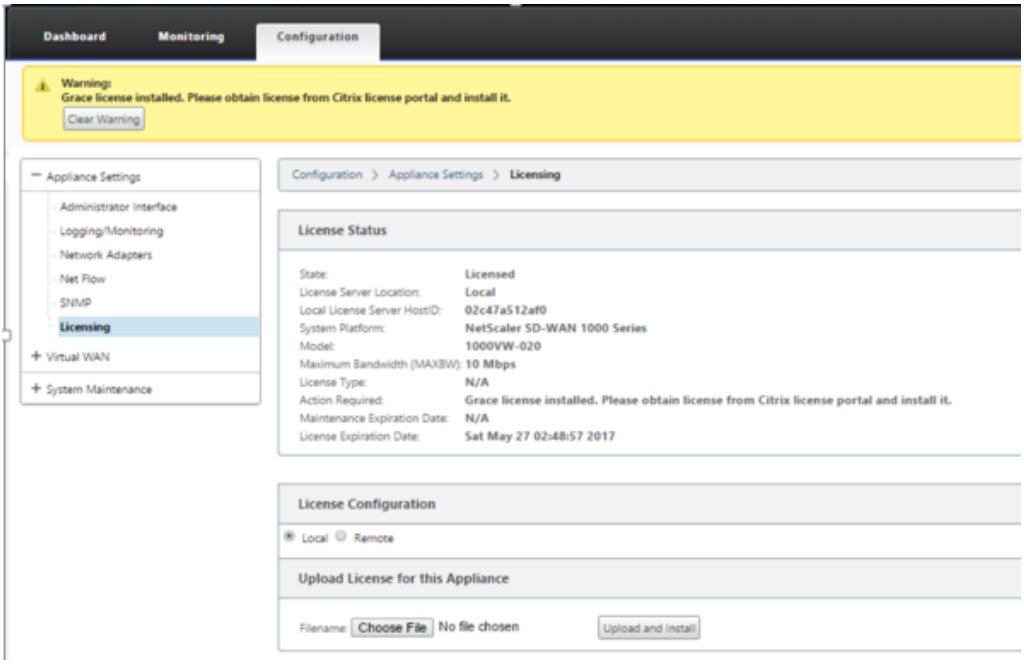
j) 对远程站点设备进行 Web 管理访问指示已使用临时宽限期 10 Mbps 来安装设备，这样可使虚拟路径服务状态报告为活动状态。



k) 可以使用配置 > 虚拟 **WAN**> 查看配置页面对设备配置进行验证。



l) 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。



上载并安装永久许可证文件后，Grace 许可证警告横幅消失，并且在许可证安装过程中不会发生与远程站点的连接丢失（丢弃零 ping）。

本地零接触

June 22, 2021

有关如何部署 SD-WAN 设备和零接触服务的说明，请参阅主题 如何配置零接触部署服务。

AWS

June 22, 2021

以下部分介绍如何在 AWS 环境中部署 ZTD。

在 **AWS** 中部署：

使用 SD-WAN 版本 9.3 时，零接触部署功能已扩展到云实例。部署零接触部署过程四个云实例的过程与零接触服务的设备部署略有不同。

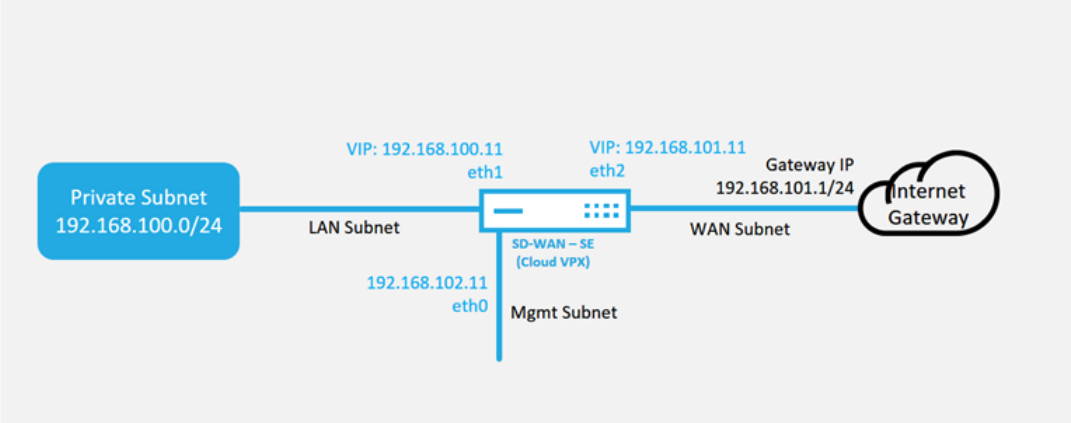
1. 通过使用 SD-WAN Center 网络配置，更新配置以添加具有 ZTD 功能的 SD-WAN 设备的新远程站点。

如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。应使用以下过程添加针对零接触部署的新云节点。

a) 通过首先列出新站点的详细信息（例如，VPX 大小、接口组使用情况、虚拟 IP 地址、WAN 链接以及带宽及其各自的网关），为 SD-WAN 部署设计新站点。

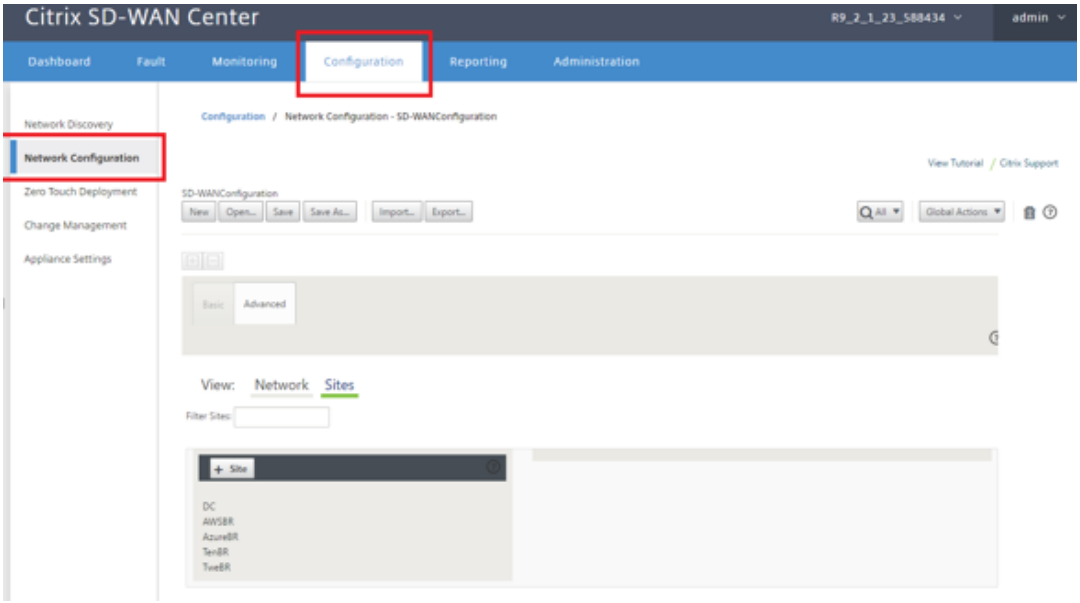
> 注意
>
> - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
> - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
> - SD-WAN VPX 的可用云模板当前被硬设置为获取 VPC 中可用子网的 #.#.#.#.11 IP 地址。

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。

b) 打开 SD-WAN Center Web 管理界面，然后导航到 配置 > 网络配置 页面。

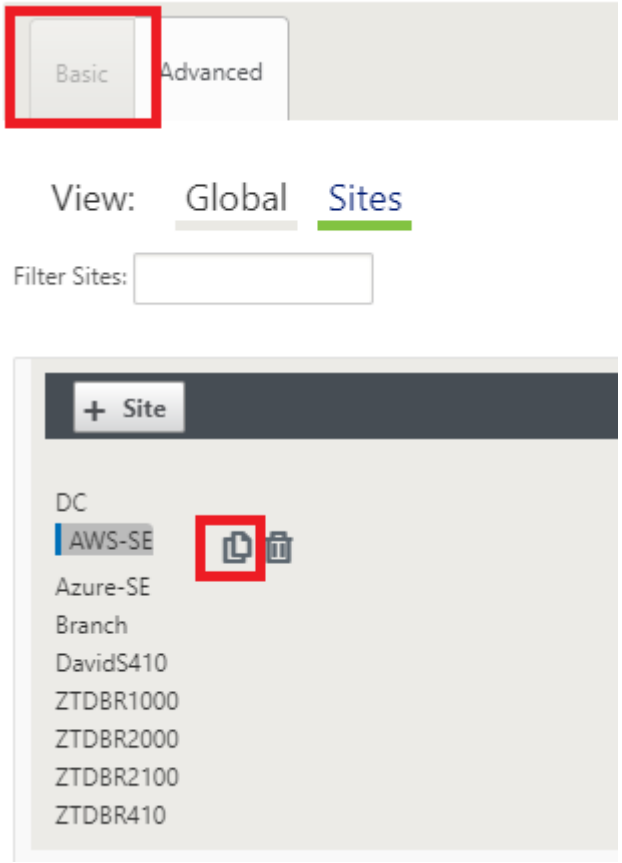


c) 确保已准备好正在运行的配置，或从 MCN 导入配置。

d) 导航到 基本 选项卡以创建新站点。

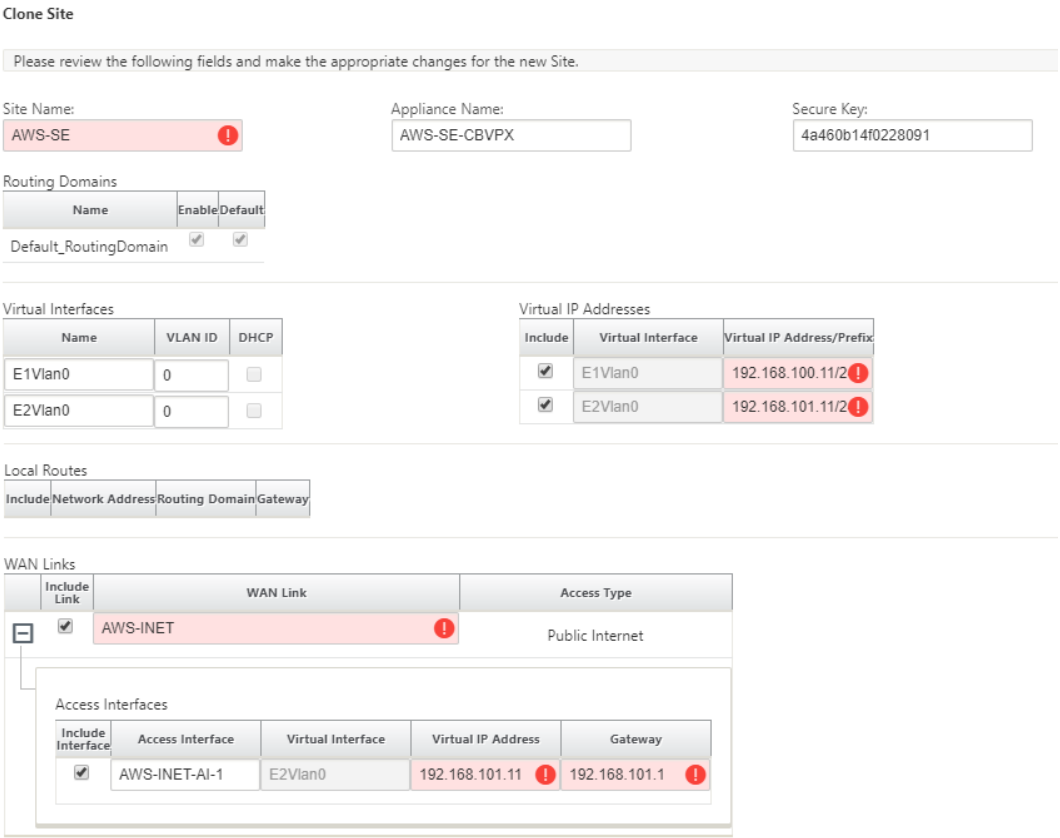
e) 打开 站点 磁贴以显示当前配置的站点。

f) 通过使用任何现有站点的克隆功能，或者手动构建新站点来快速构建新云站点的配置。

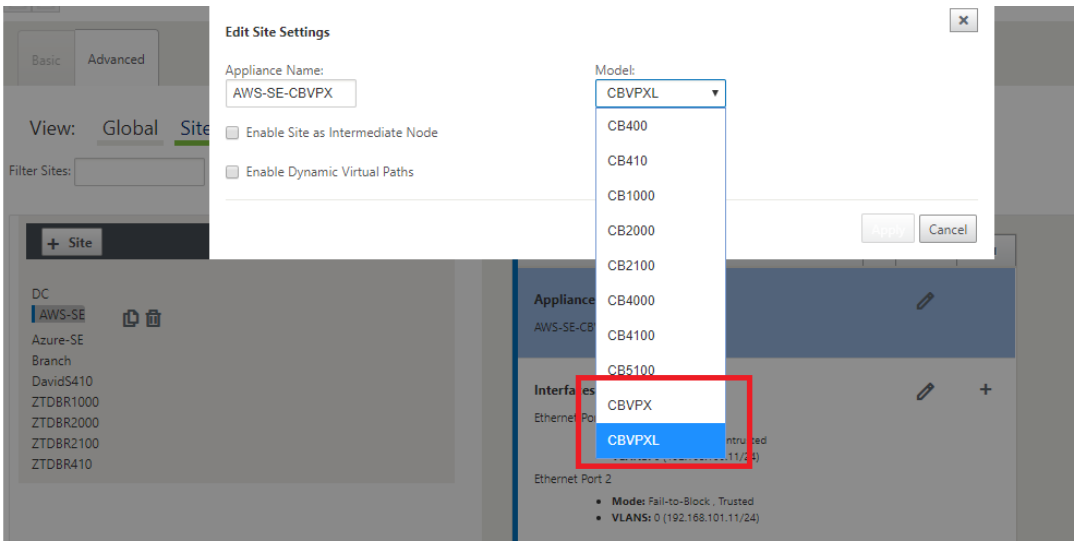


g) 填充之前为此新云站点设计的拓扑中的所有必填字段

请注意，可以将云 ZTD 部署的模板硬设置为对管理、LAN 和 WAN 子网使用 #.#.#.11 IP 地址。如果配置未设置为与每个接口的预期.11 IP 主机地址相匹配，则设备将无法正确建立到云环境网关的 ARP 以及与 MCN 虚拟路径的 IP 连接。

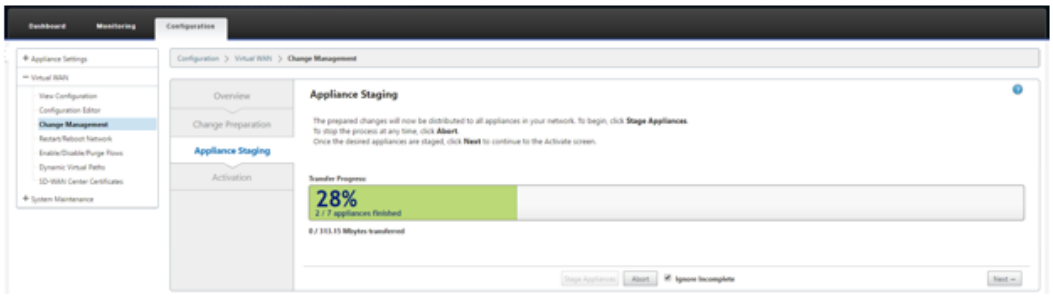


h) 克隆新站点后，导航到该站点的基本设置，并验证是否正确选择了要支持零接触服务的 SD-WAN 的型号。



i) 在 SD-WAN Center 上保存新配置，然后使用“导出到 更改管理收件箱”选项使用“更改管理”推送配置。

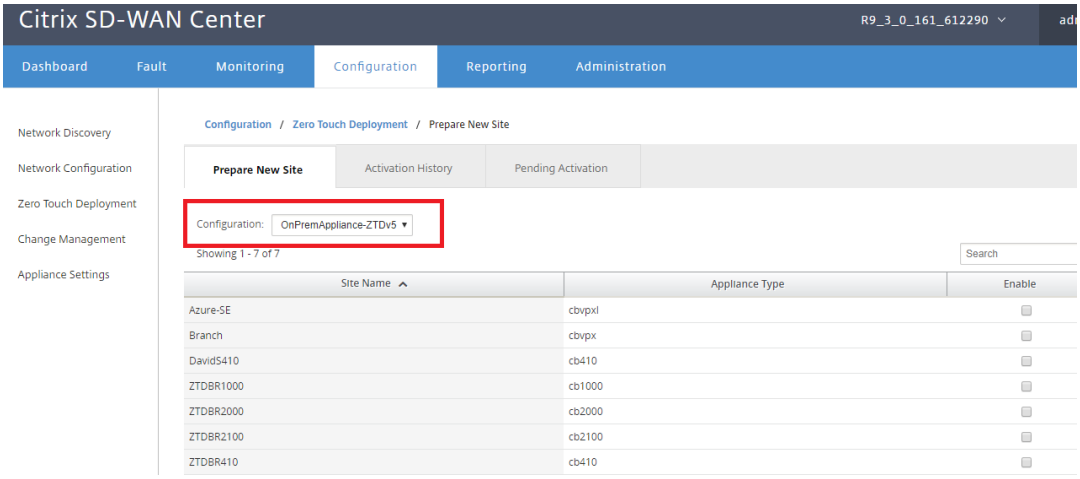
j) 按照“更改管理”过程正确暂存新配置，这使现有 SD-WAN 设备知道要通过零接触部署的新站点，您需要使用“忽略不完整”选项来跳过尝试将配置推送到仍然存在的新站点的尝试需要通过 ZTD 工作流程。



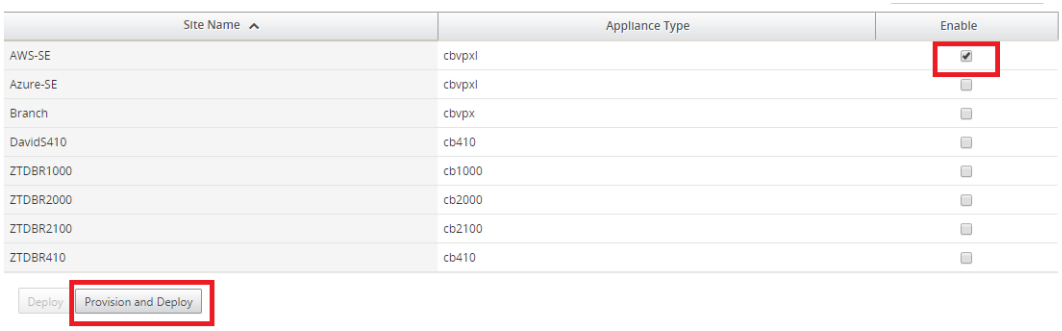
2. 导航回 SD-WAN Center 零接触部署页面，在运行新的活动配置的情况下，将有新站点可供部署。

a) 在零接触部署页面的“部 署新站点”选项卡下，选择正在运行的网络配置文件。

b) 选择运行配置文件后，将显示具有未部署 Citrix SD-WAN 设备且支持零接触的所有分支站点的列表。



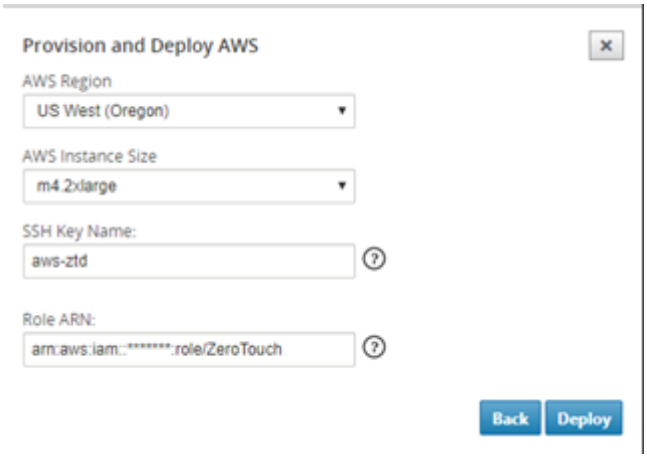
c) 选择要使用零接触服务部署的目标云站点，单击 启用，然后单击 预配和部署。



d) 此时将显示一个弹出窗口，其中 Citrix SD-WAN 管理员可以在零接触的情况下发起部署。

填写可以交付激活 URL 的电子邮件地址，然后选择所需云的提供类型。

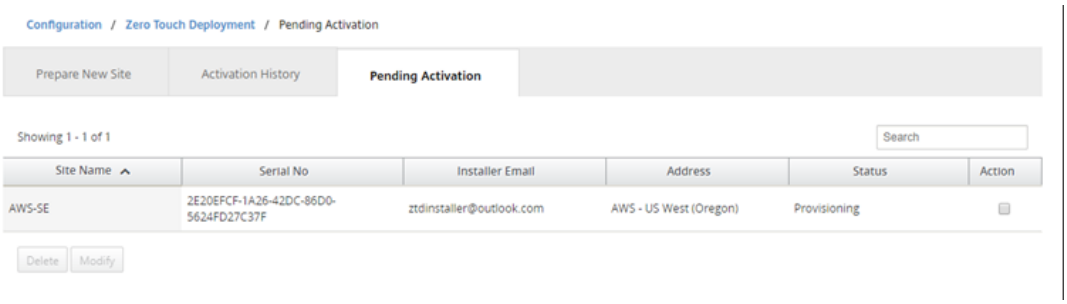
e) 单击下一步后，选择适当的区域（实例大小），相应地填充 SSH 密钥名称和角色 ARN 字段。



> 注意
>
> 请使用帮助链接获取有关如何在云帐户上设置 SSH 密钥和角色 ARN 的指导。此外，请确保所选区域与账户上的可用区域匹配，并且选定的实例大小与 SD-WAN 配置中选定型号的 VPX 或 VPXL 匹配。

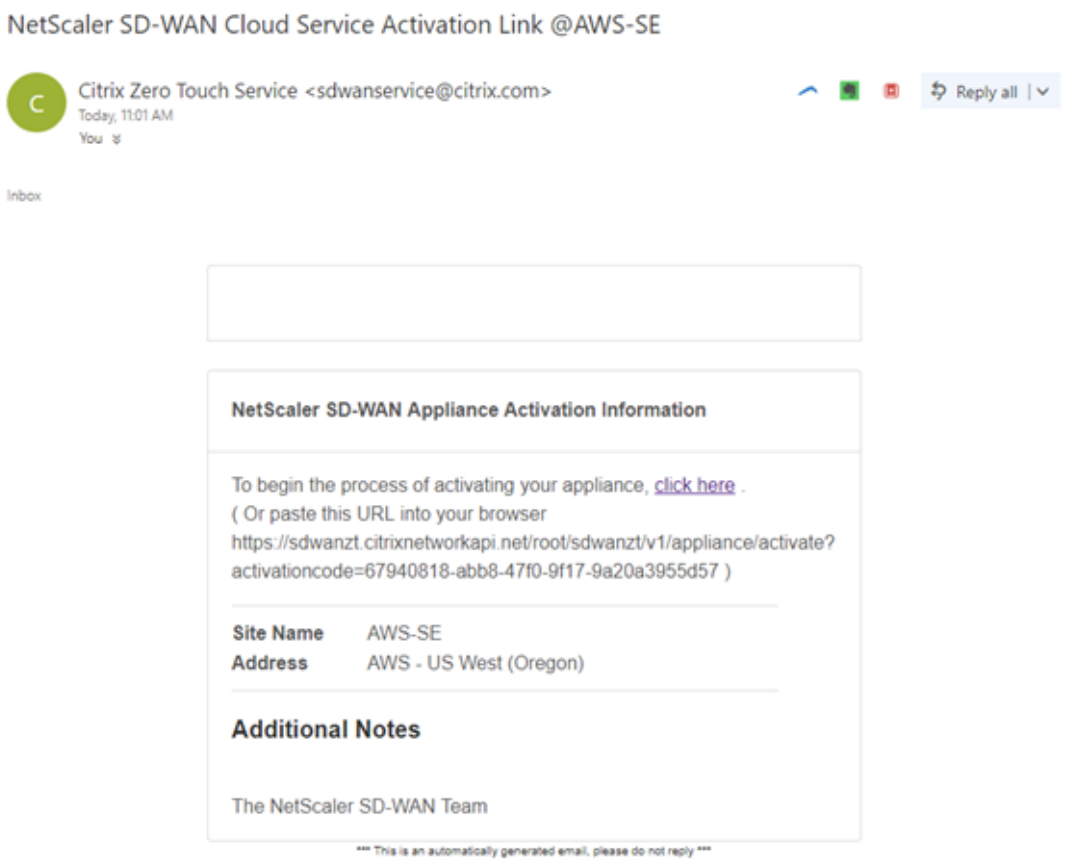
f) 单击部署，触发 SD-WAN Center（以前在 ZTD 云服务中注册），以将此站点的配置临时存储在 ZTD 云服务中。

g) 导航到挂起的激活选项卡，确认站点信息已成功填充并置于预配状态。



3. 以云管理员身份启动零接触部署过程。

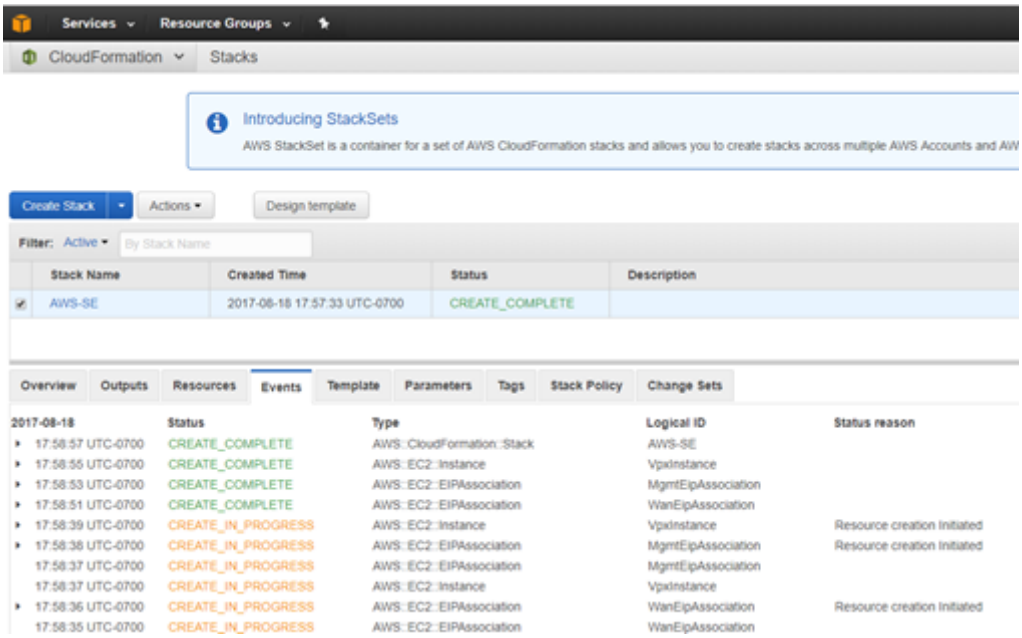
a) 安装程序将需要检查在部署站点时使用 SD-WAN 管理员的电子邮件地址的邮箱。



b) 在互联网浏览器窗口中打开电子邮件中找到的激活 URL（例如;`https://sdwanzt.citrixnetworkapi.net`）。

c) 如果正确输入了 SSH 密钥和角色 ARN，则“零接触部署”服务将立即开始预配 SD-WAN 实例，否则连接错误将立即显示出来。

d) 要在 AWS 控制台上执行其他故障排除，可以使用云组建服务来捕捉预配过程中发生的任何事件。

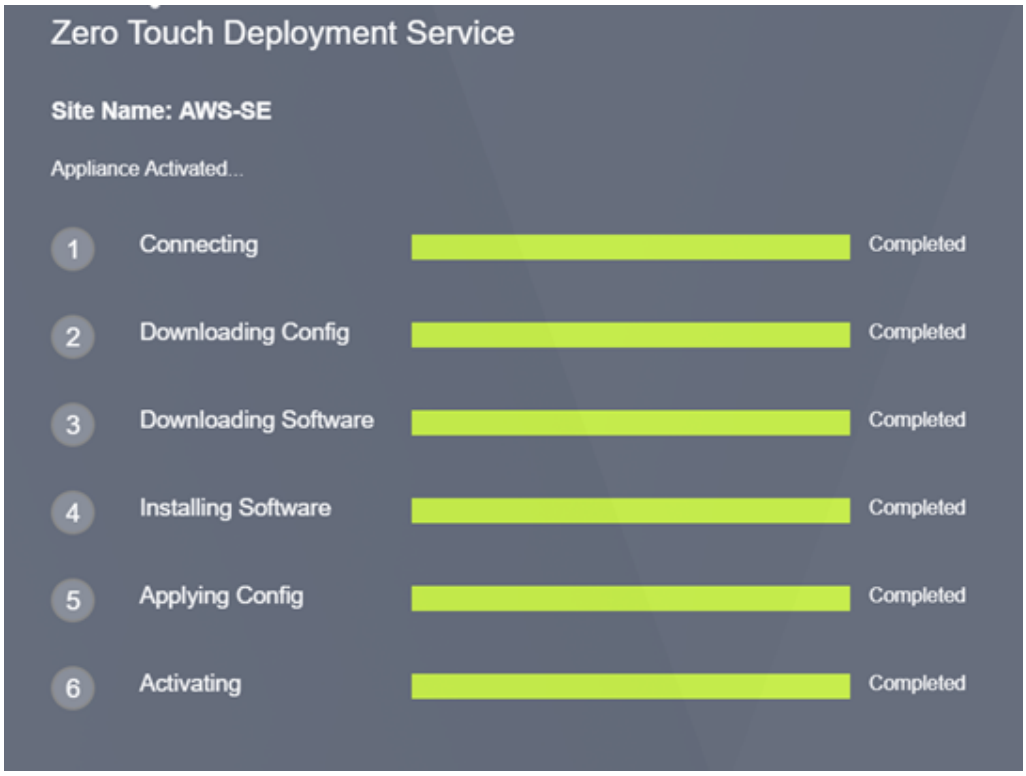


e) 允许预配过程 ~ 8-10 分钟，并在激活后约需要 3-5 分钟来完成。

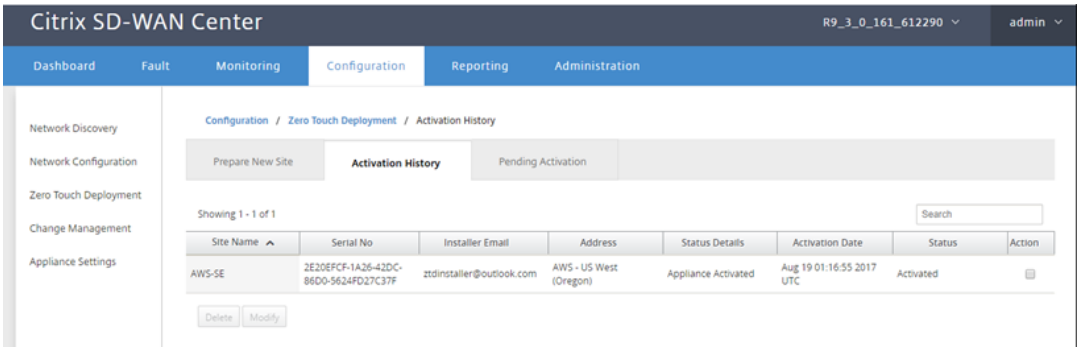
f) 通过将 SD-WAN 实例成功连接到 ZTD 云服务，该服务将自动执行以下操作：

- 下载 SD-WAN 中心之前存储的特定于站点的配置文件

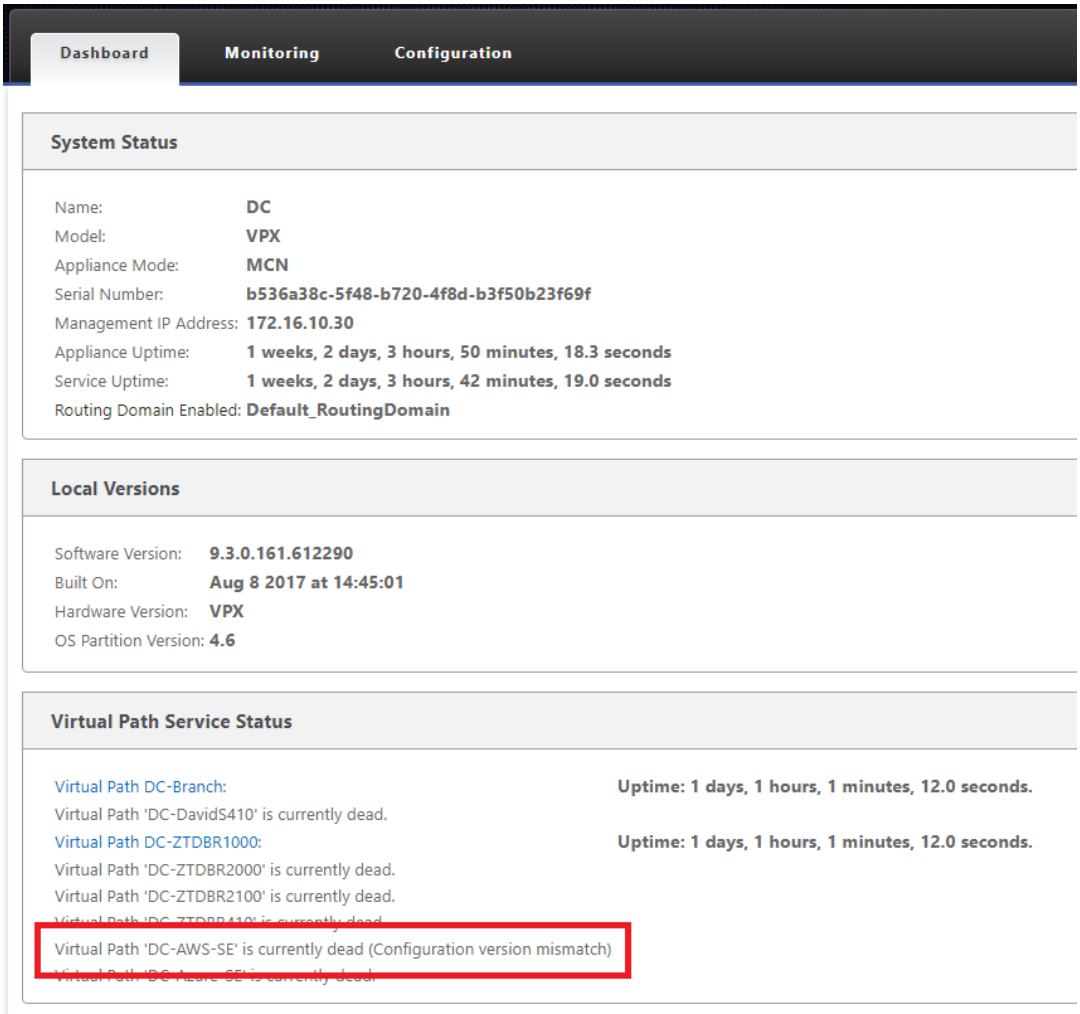
- 将配置应用于本地实例
- 下载并安装临时 10 MB 许可证文件
- 下载并安装任何软件更新（如有需要）
- 激活 SD-WAN 服务



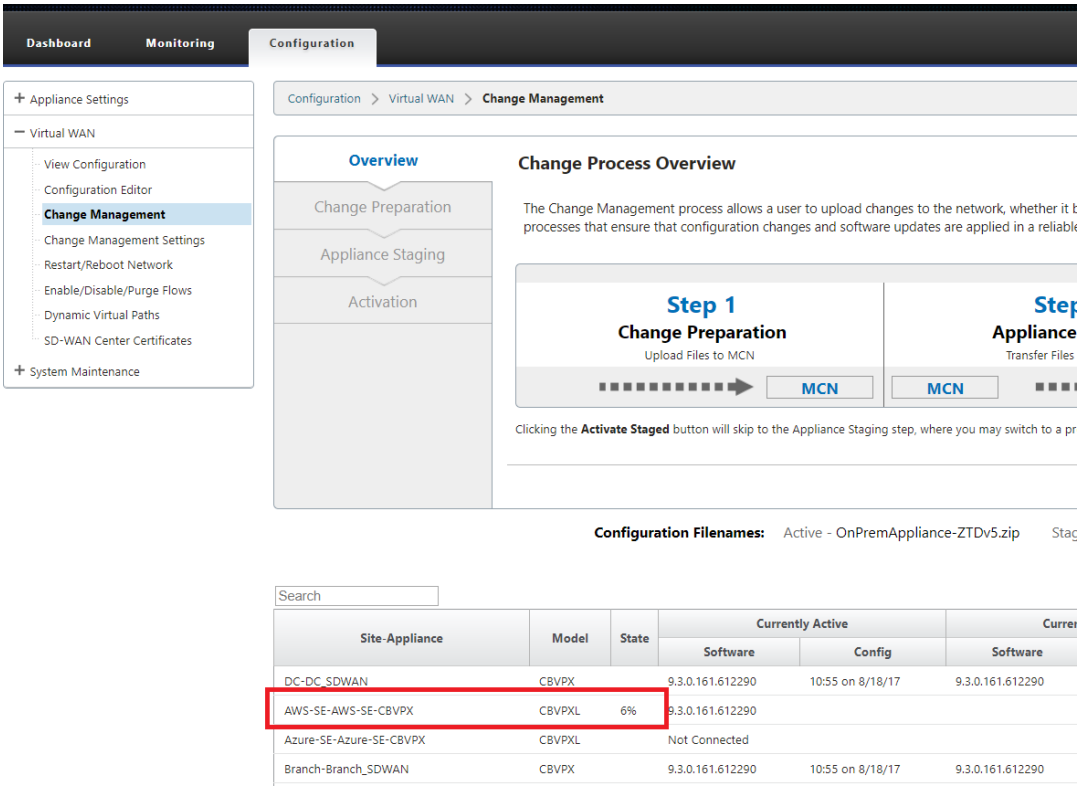
g) 可以在 SD-WAN Center Web 管理界面进一步确认；零接触部署菜单将在 激活历史选项卡中显示已成功激活 的装置。



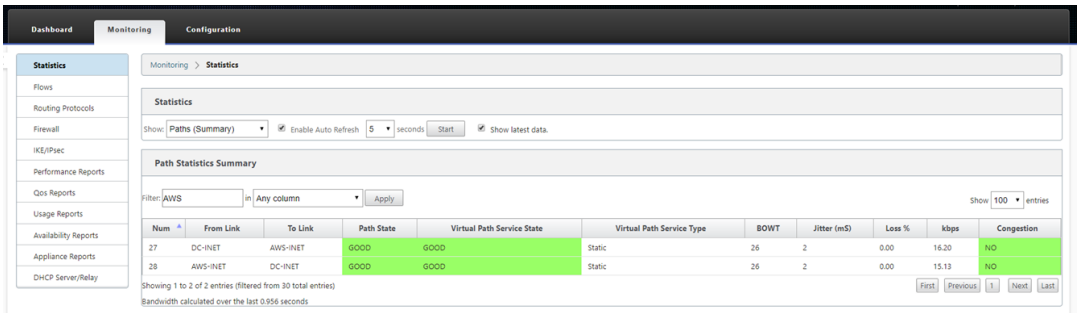
h) 虚拟路径可能不会立即显示在已连接状态下，这是因为 MCN 可能不信任 ZTD Cloud Service 传递的配置，并将在 MCN 控制面板中报告 配置版本不匹 配。



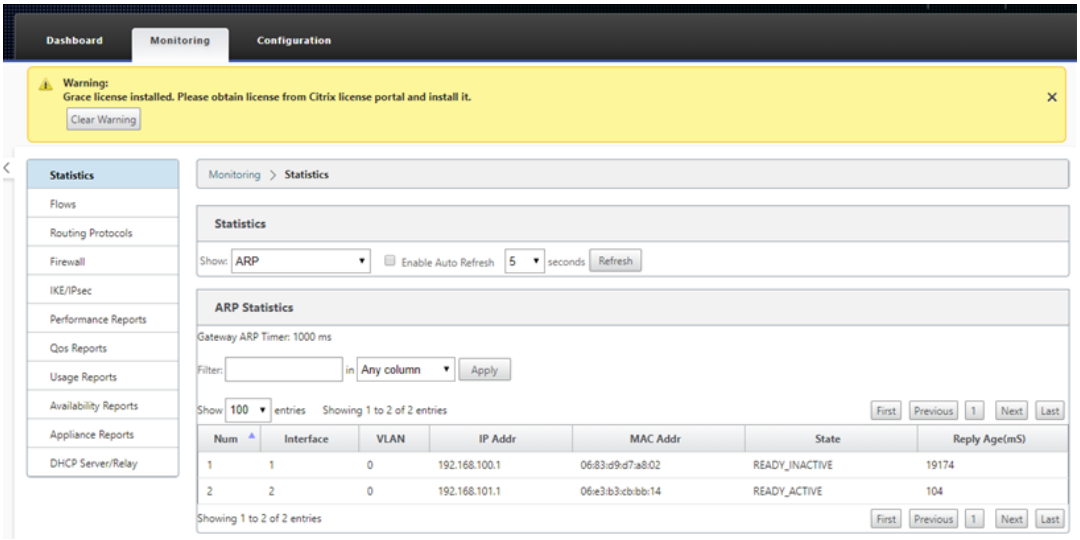
i) 配置将自动重新传递到新安装的分支机构设备，其状态可以在 **MCN** > 配置 > 虚拟广域 网 > 更改管理 页面上进行监视（取决于连接性，此过程可能需要几分钟才能完成）。



j) SD-WAN 管理员可以监视与新添加的云站点建立的虚拟路径有关的头端 MCN Web 管理页面。



k) 如果需要进行故障排除，请使用预配过程中云环境所分配的公用 IP 打开 SD-WAN 实例用户界面，并利用监视 > 统计信息页面中的 ARP 表来确定连接时遇到的任何问题到预期网关，或使用诊断中的跟踪路由和数据包捕获选项。



Azure

June 22, 2021

部署面向云实例的零接触部署过程的过程与设备部署中的过程稍有不同，以实现零接触服务。

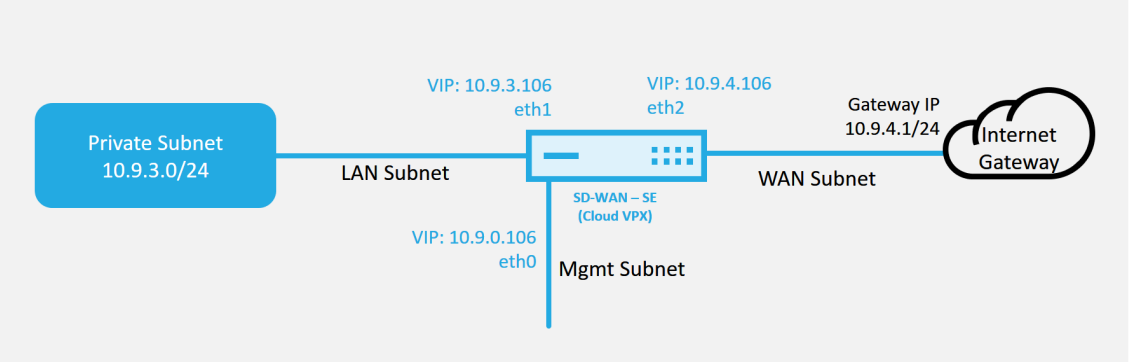
更新配置以使用 SD-WAN Center 网络配置添加具有 ZTD 功能的 SD-WAN 云设备的新远程站点

如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。应使用以下过程添加针对零接触部署的新云节点。

1. 通过首先列出新站点的详细信息（例如，VPX 大小、接口组使用情况、虚拟 IP 地址、WAN 链接以及带宽及其各自的网关），为 SD-WAN 部署设计新站点。

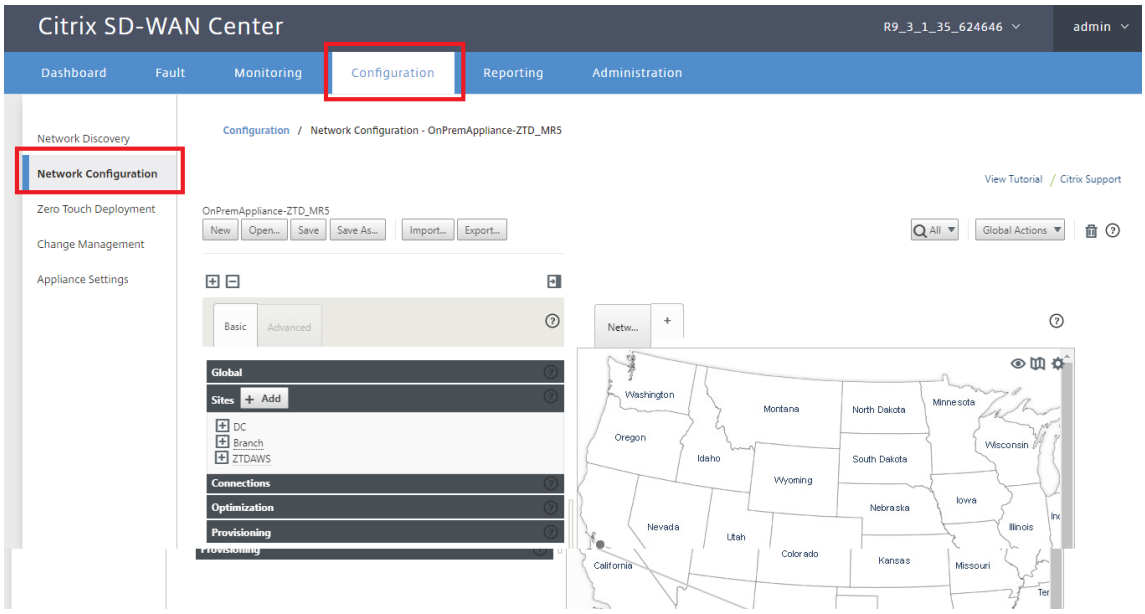
> 注意
>
> - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
> - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
> - 适用于 SD-WAN VPX 的 Azure 云模板当前被硬设置为获取 WAN 的 10.9.4.106 IP、适用于 LAN 的 10.9.3.106 IP 以及管理地址的 10.9.0.16 IP。针对零接触的 Azure 节点的 SD-WAN 配置必须与此布局匹配。
> - 配置中的 Azure 站点名称必须全小写且无特殊字符（例如 ztdazure）。

Azure Cloud Topology with NetScaler SD-WAN

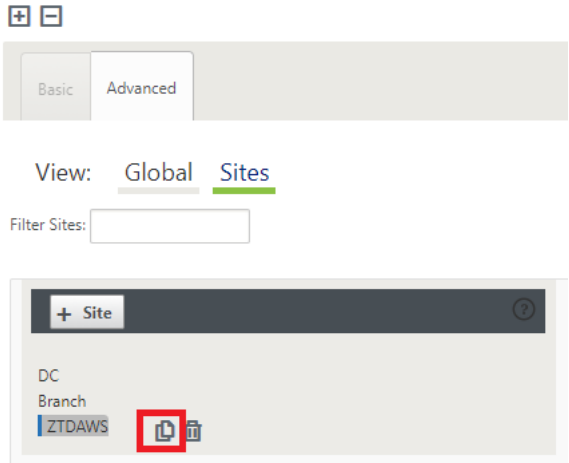


这是 SD-WAN 云部署站点的示例部署，Citrix SD-WAN 设备部署为此云网络中的单个 Internet WAN 链接提供服务的边缘设备。远程站点将能够利用连接到同一 Internet 网关的多个不同 Internet WAN 链路，从而提供从任何 SD-WAN 部署站点到云基础设施的弹性和聚合带宽连接。这样就可以提供经济高效且高度可靠的云连接。

2. 打开 SD-WAN Center Web 管理界面，然后导航到 配置 > 网络配置 页面。



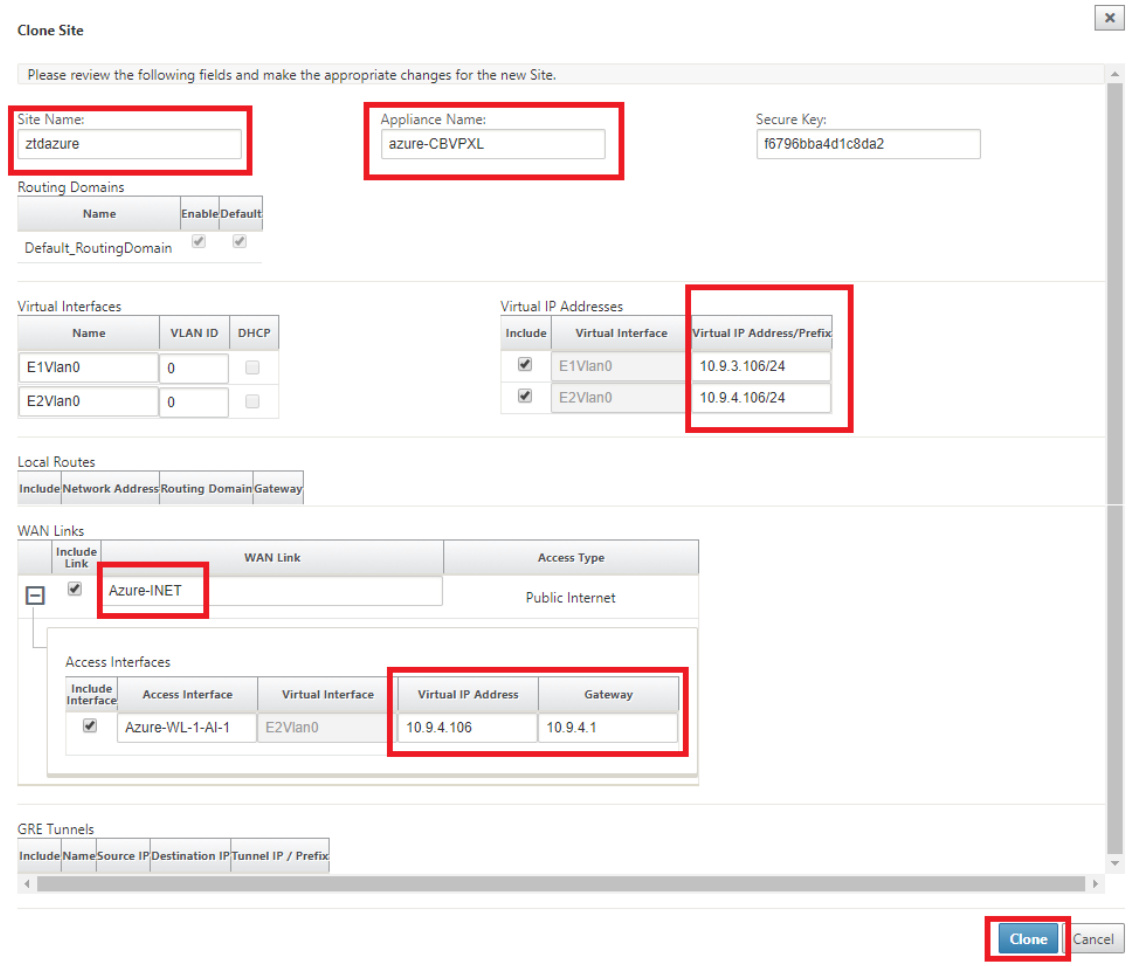
3. 确保已准备好正在运行的配置，或从 MCN 导入配置。
4. 导航到 基本 选项卡以创建新站点。
5. 打开 站点 磁贴以显示当前配置的站点。
6. 通过使用任何现有站点的克隆功能，或者手动构建新站点来快速构建新云站点的配置。



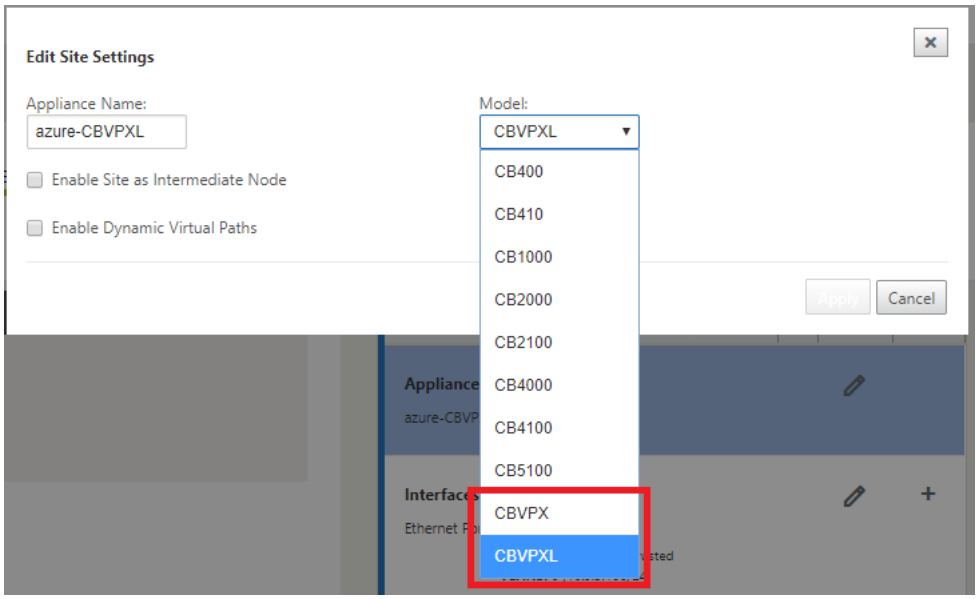
7. 填充之前为此新云站点设计的拓扑中的所有必填字段。

   请注意，适用于 Azure cloud ZTD 部署的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。如果配置未设置为与每个接口的预期 VIP 地址相匹配，则设备将无法正确建立到云环境网关的 ARP 以及与 MCN 虚拟路径的 IP 连接。

   将导入站点名称，使其符合 Azure 预期的要求。站点名称必须全部小写，至少 6 个字符，不含特殊字符，必须确认以下正则表达式 **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $**。

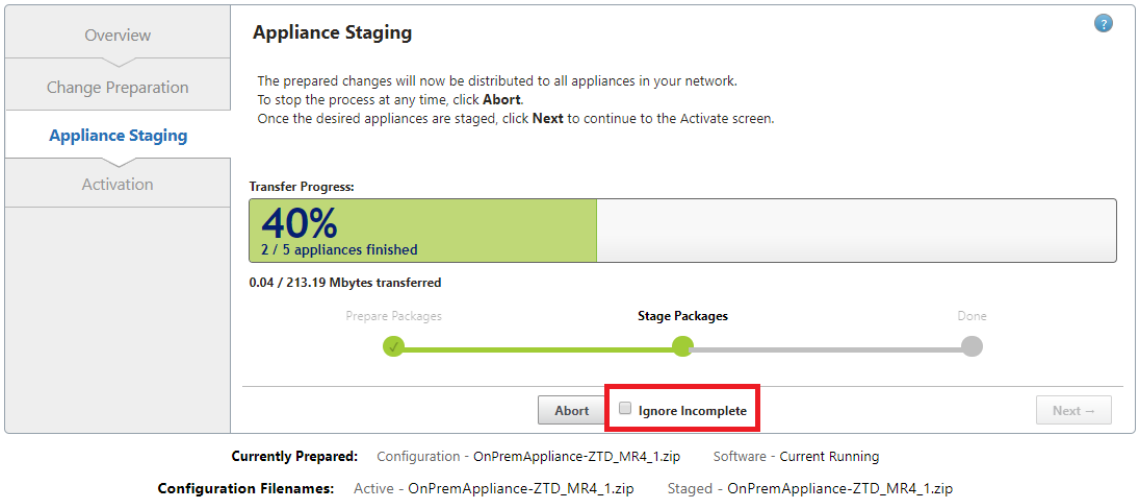


8. 克隆新站点后，导航到该站点的基本设置，并验证是否正确选择了要支持零接触服务的 SD-WAN 的型号。



9. 在 SD-WAN Center 上保存新配置，然后使用“导出到 更改管理收件箱”选项使用“更改管理”推送配置。

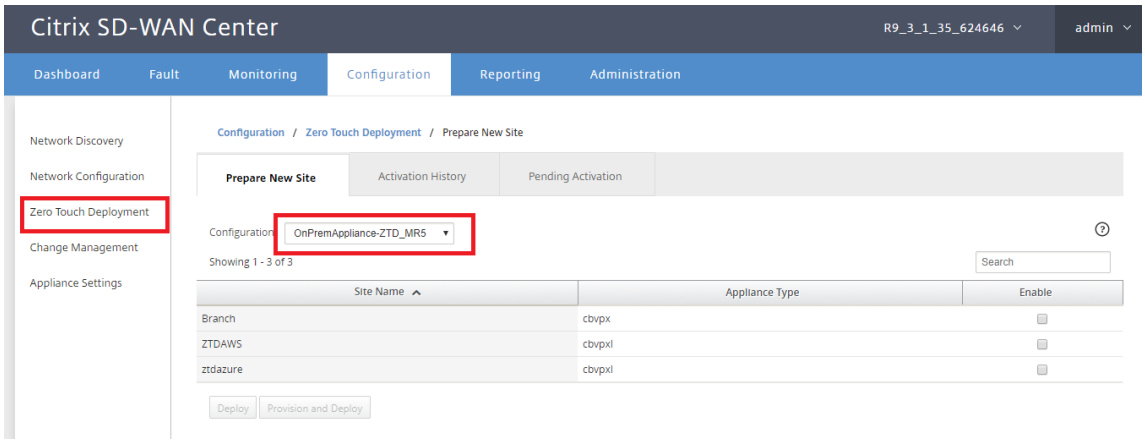
10. 按照“更改管理”过程正确暂存新配置，这使现有 SD-WAN 设备知道要通过零接触部署的新站点，您需要使用“忽略不完整”选项来跳过尝试将配置推送到仍然存在的新站点的尝试需要通过 ZTD 工作流程。



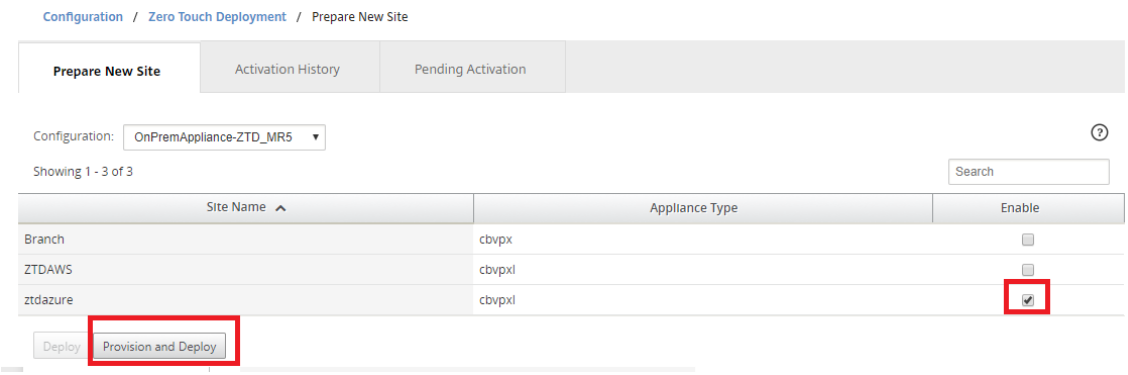
导航到 **SD-WAN Center** 的零接触部署页面，在运行新的活动配置的情况下，新站点将适用于 **SD-WAN Center** 预配和部署 **Azure**（第 **1** 步，共 **2** 步）

1. 在零轻点部署页面上，使用您的 Citrix 帐户凭据进行登录。在“部 署新站点”选项卡下，选择正在运行的网络配置文件。

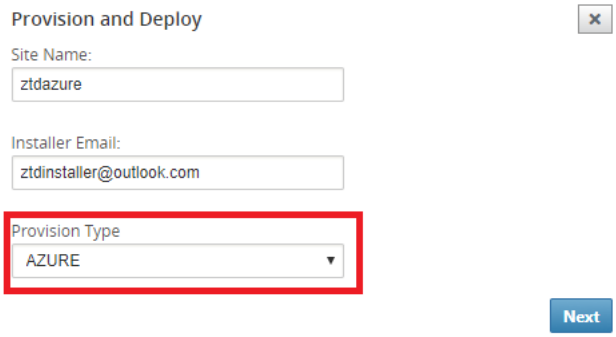
2. 选择运行配置文件后，将显示具有 ZTD 功能的 Citrix SD-WAN 设备的所有分支站点的列表。



3. 选择要使用零接触服务部署的目标云站点，单击 启用，然后单击 预配和部署。

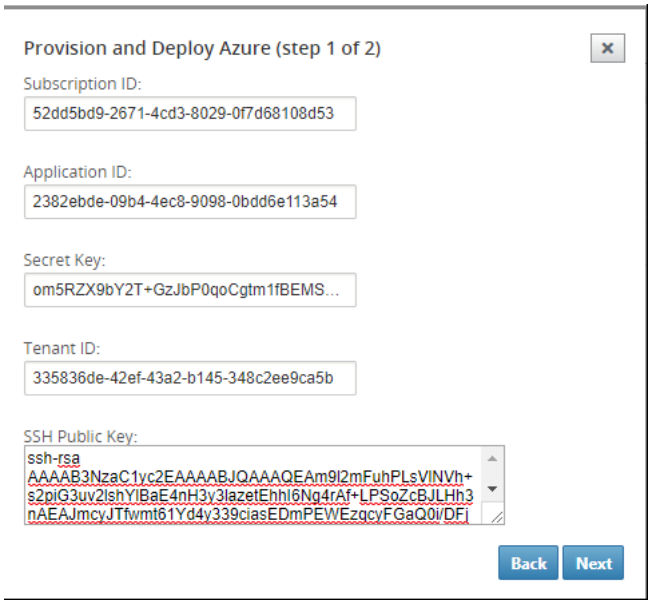


4. 此时将显示一个弹出窗口，其中 Citrix SD-WAN 管理员可以在零接触的情况下发起部署。验证站点名称是否符合 Azure 上的要求（小写，无特殊字符）。在单击下一步之前，填充可以传送激活 URL 的电子邮件地址，然后选择 Azure 作为所需云的预配类型。

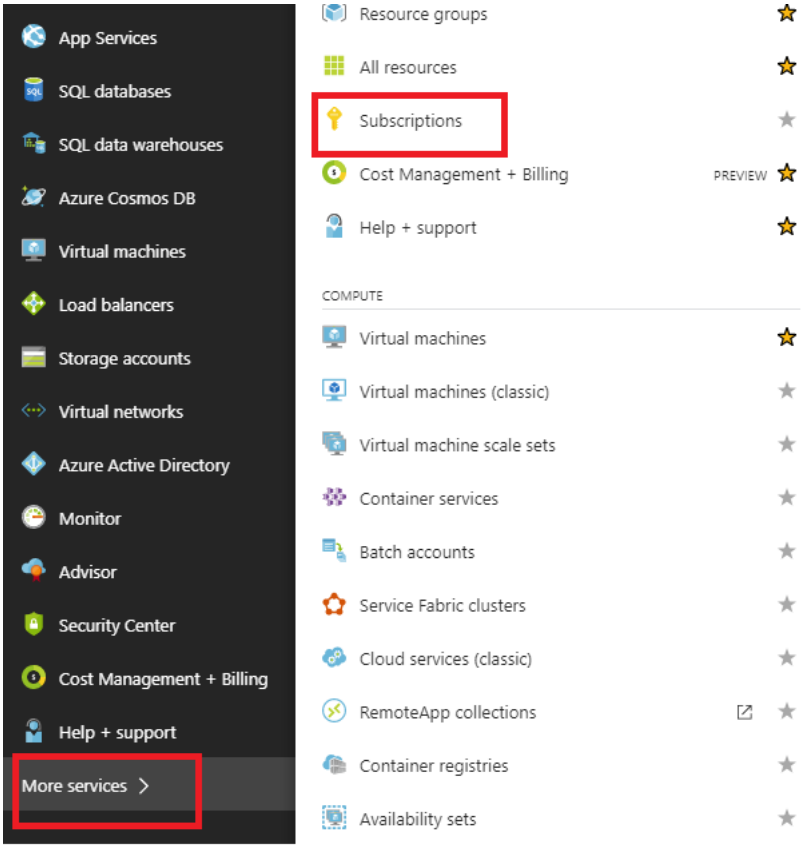


5. 单击下一步后，设置和部署 Azure（步骤 1，共 2 步）窗口将需要从 Azure 帐户获取的输入。

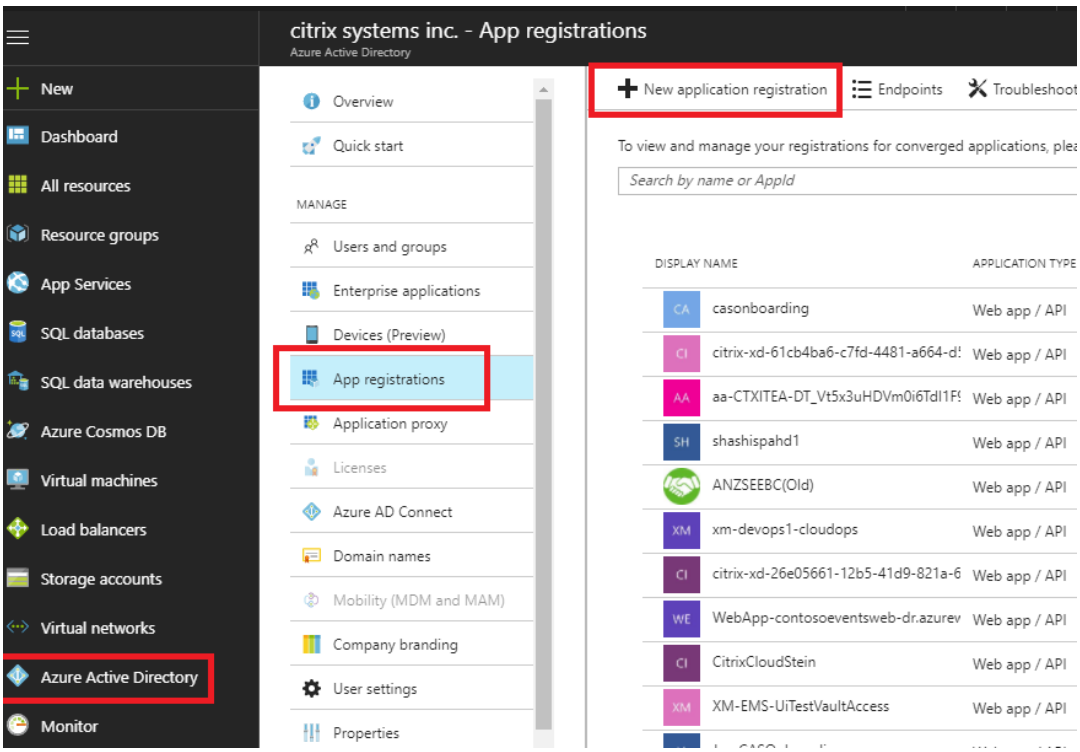
   从您的 Azure 帐户获取信息后，复制并粘贴每个必填字段。以下步骤概述了如何从 Azure 帐户获取所需的订阅 ID、应用程序 ID、密钥和租户 ID，然后单击 下一步继续。



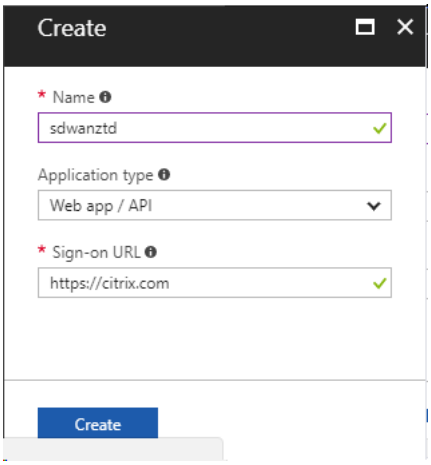
   a) 在 Azure 帐户上，我们可以通过导航到“更多服务”并选择 订阅来识别所需的订阅 ID。



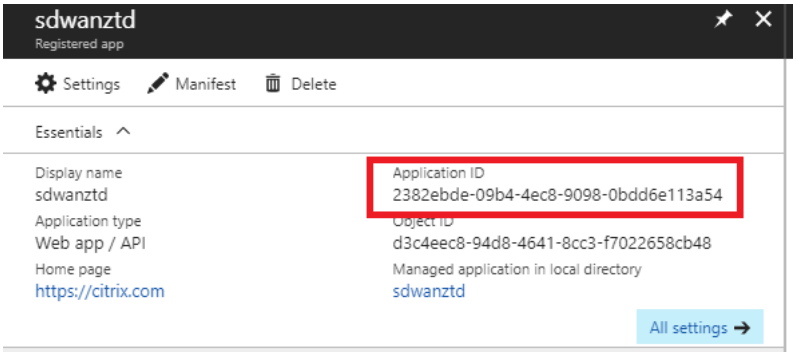
b) 若要标识所需的 * 应用程序 **ID**，请导航到 Azure Active Directory、应用程序注册，然后单击 新建应用程序注册。



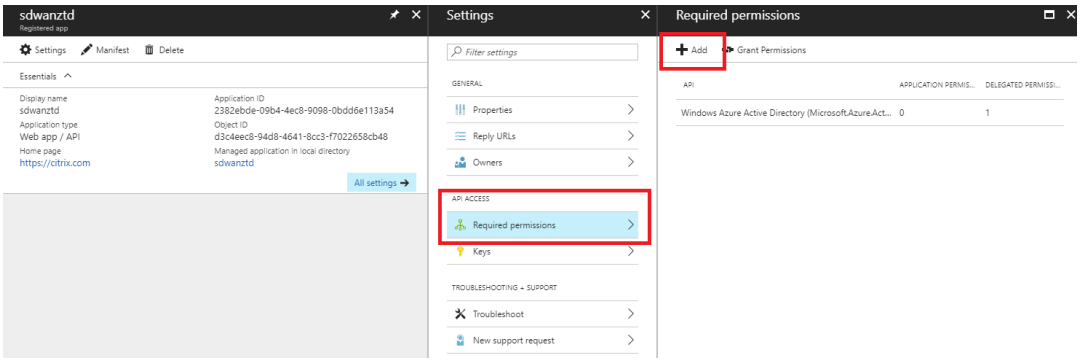
c) 在应用程序注册创建菜单中，输入名称和登录 URL（可以是任何 URL，唯一的要求是必须有效），然后单击创建。



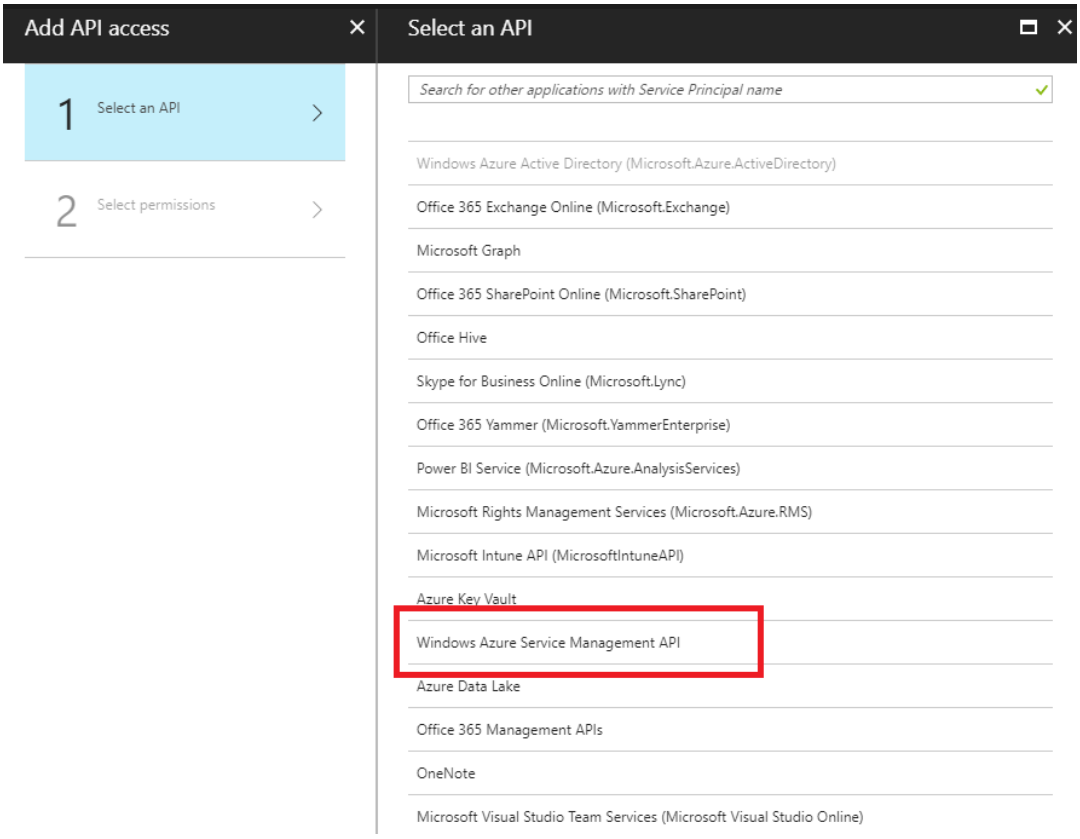
d) 搜索并打开新创建的注册应用程序，并记录应用程序 ID。



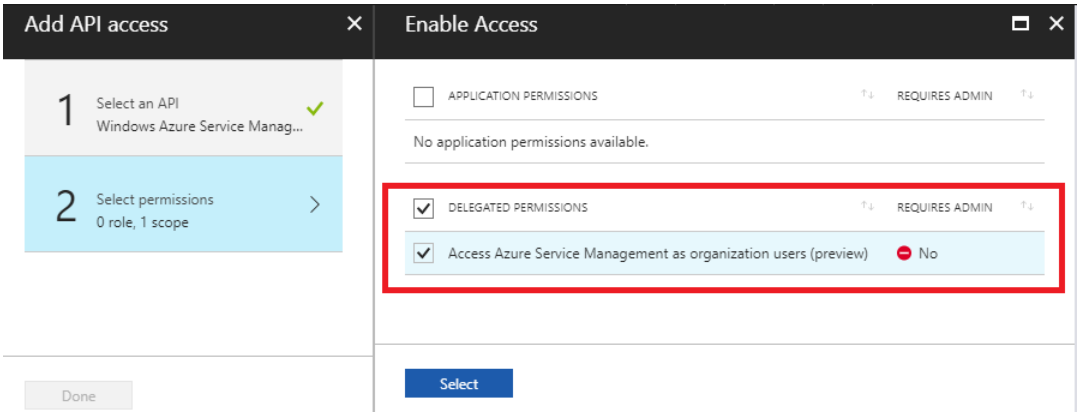
e) 再次打开新创建的注册应用程序，要识别所需的 安全密钥，请在 API 访问下，选择 必需的权限，以允许第三方进行配置和实例。然后选择添加。



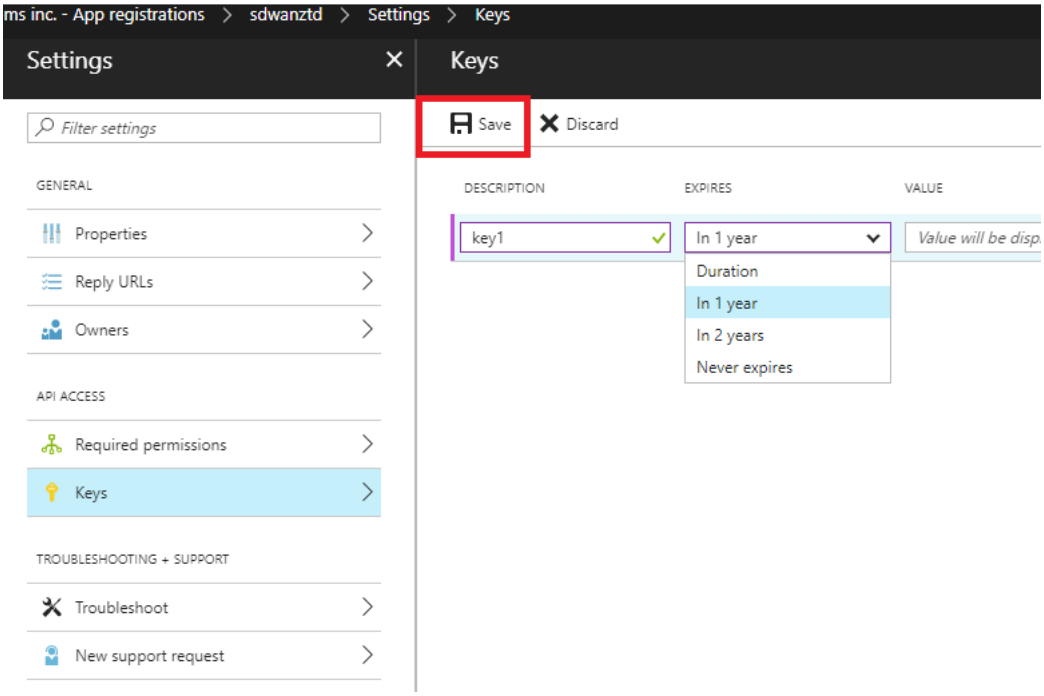
f) 添加所需权限时，选择一个 **API**，然后突出显示 **Windows Azure** 服务管理 **API**。



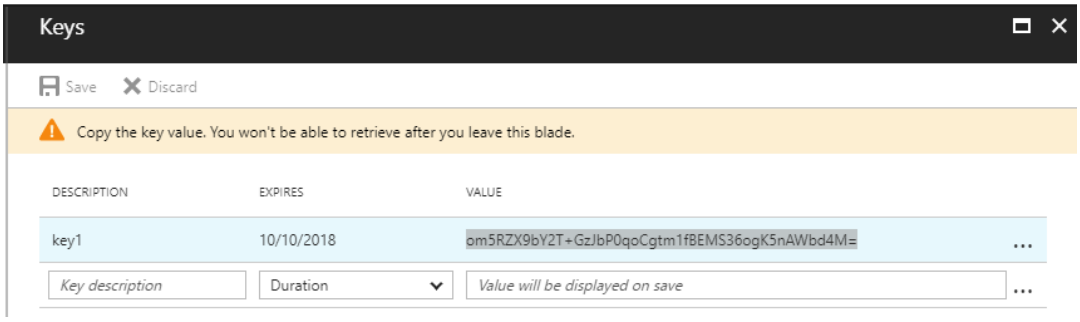
g) 启用委派权限以预配实例，然后单击选择和完成。



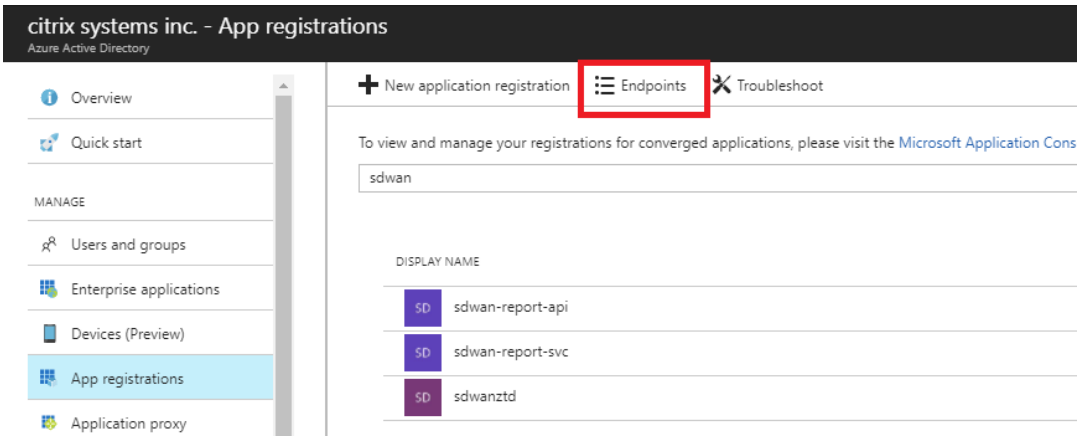
h) 对于此已注册应用程序，在 API Access 下，选择密钥，然后创建私有密钥描述和密钥有效的所需持续时间。然后单击 **Save** ，它将生成一个 私有密钥（该密钥仅在配置过程中需要，在实例可用后可以将其删除）。



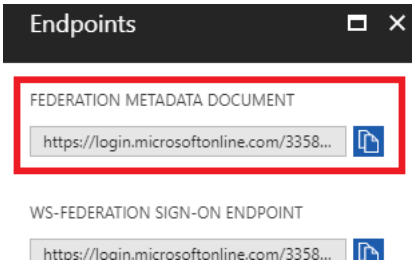
i) 复制并保存密钥（请注意，您以后将无法检索此密钥）。



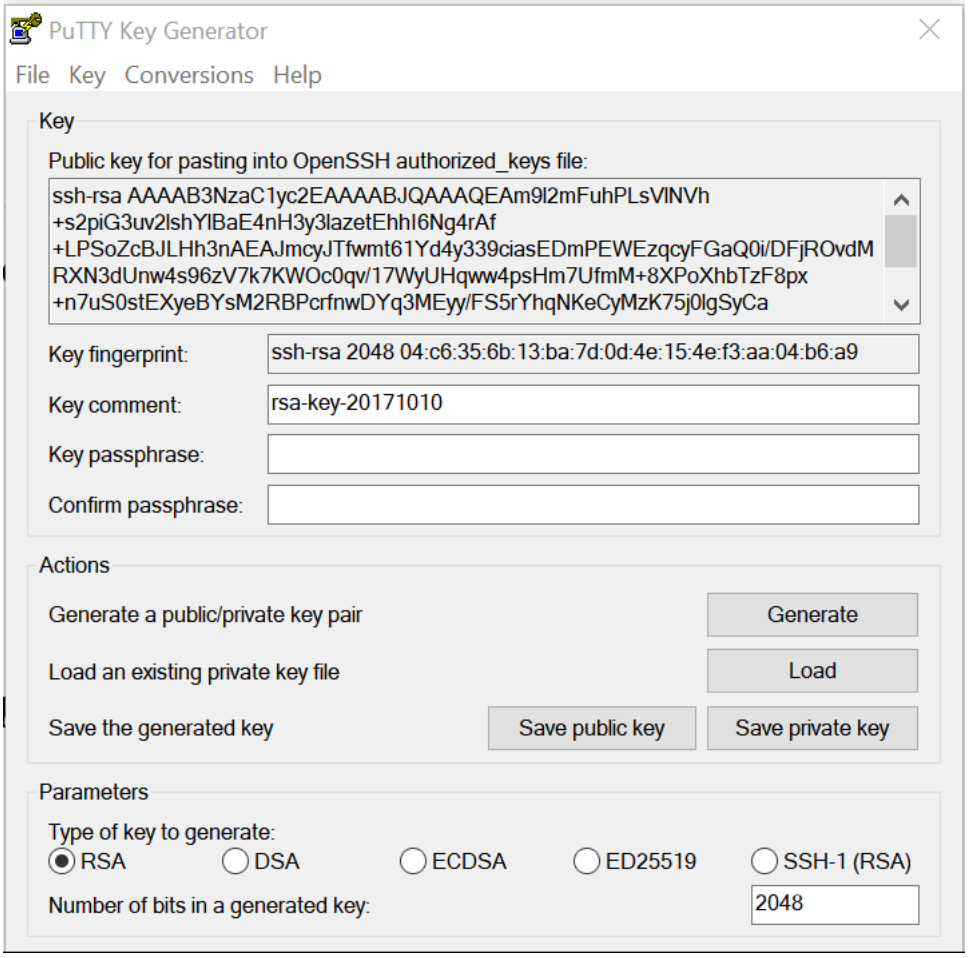
j) 要确定所需的 租户 ***ID***，请导航回应用程序注册窗格，然后选择 终端节点。



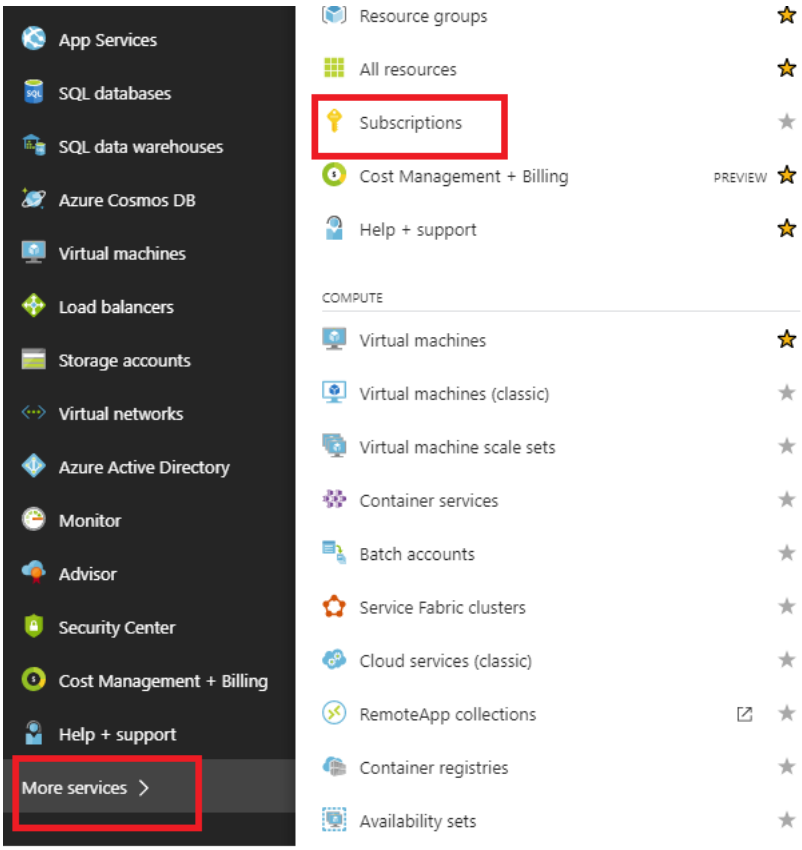
k) 复制 联合元数据文档以标识您的租户 ID（请注意，租户 ID 为 36 个字符的字符串，位于 URL 中的 `online.com/` 和 `/federation` 之间）。



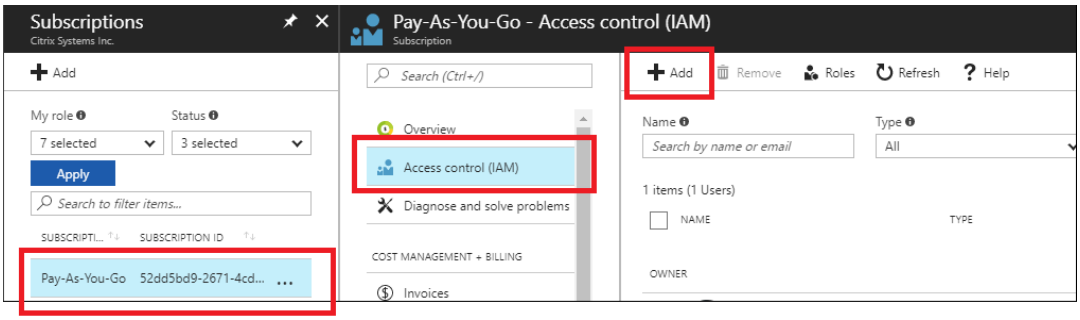
l) 需要的最后一项是 ***SSH*** 公钥。这可以使用腻子密钥生成器或 ssh-keygen 创建，并将用于身份验证，无需使用密码登录。SSH 公钥可以被复制（包括标题 ssh-rsa 和尾随的 rsa 键字符串）。此公钥将通过 SD-WAN 中心输入共享到 Citrix 零接触部署服务。



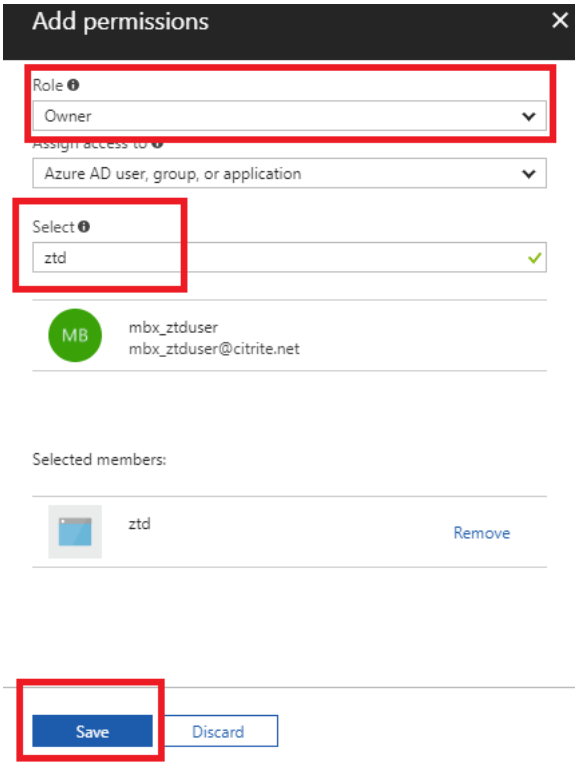
m) 为应用程序分配角色需要执行其他步骤。返回“更多服务”，然后导航到“订阅”。



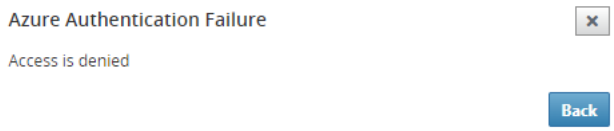
n) 选择活动订阅，然后选择访问控制 **(AIM)**，然后单击添加。



o) 在添加权限窗格中，选择 所有者 角色，将访问权限分配给 **Azure AD** 用户、组或 应用程序，然后在 选择字段 中搜索已注册的应用程序，以允许零接触部署云服务在 Azure 订阅上创建和配置实例。识别应用程序后，选择该应用程序并确保其填充为选定成员，然后单击“保 存”。

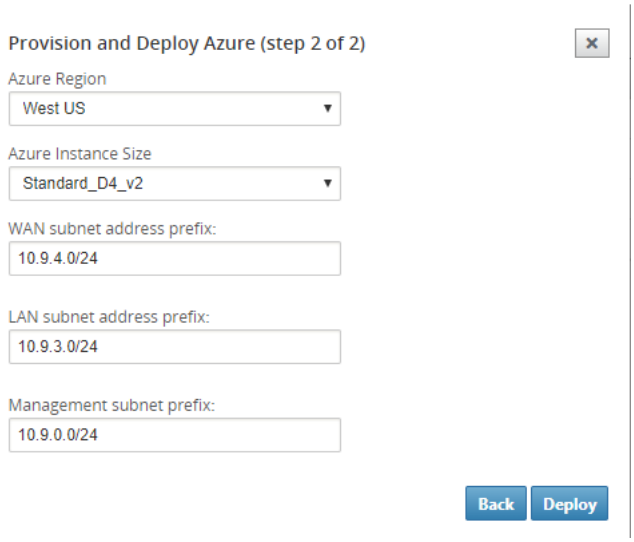


p) 收集所需输入并将其输入到 SD-WAN Center 之后，单击 下一步。如果输入不正确，您将遇到身份验证失败。

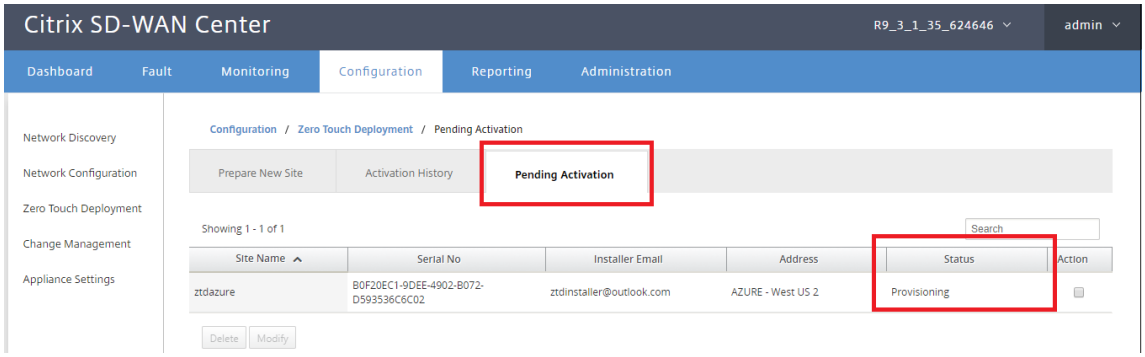


SD-WAN Center 配置和部署 **Azure**（第 **2** 步，共 **2** 步）

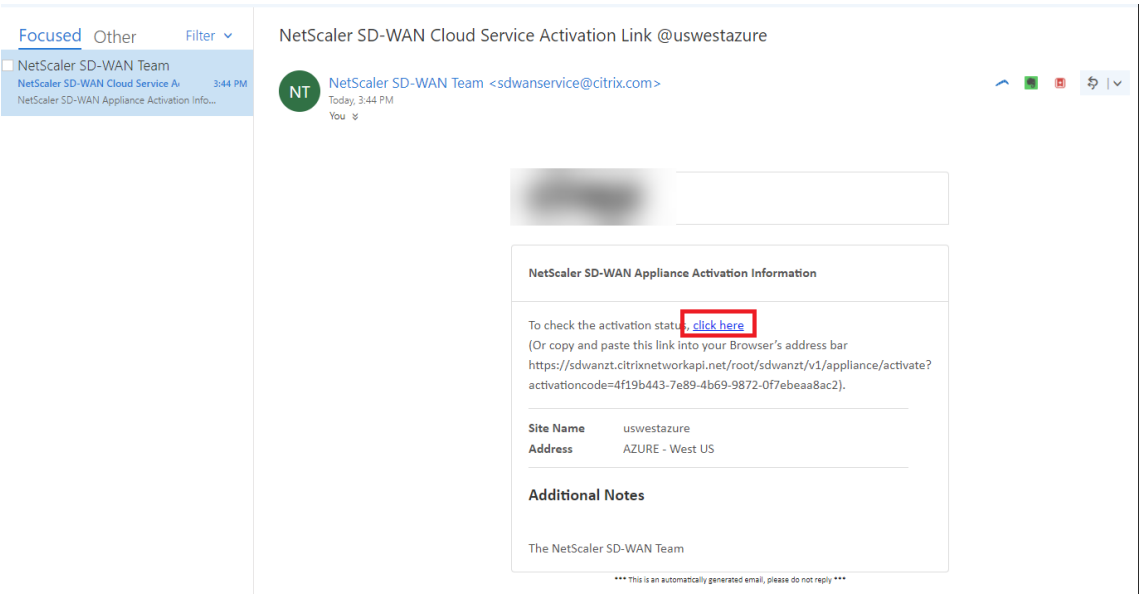
1. Azure 身份验证成功后，填充相应的字段以选择所需的 Azure 区域以及适当的实例大小，然后单击部署。



2. 导航到 SD-WAN Center 中的挂起的激活 选项卡可帮助跟踪部署的当前状态。

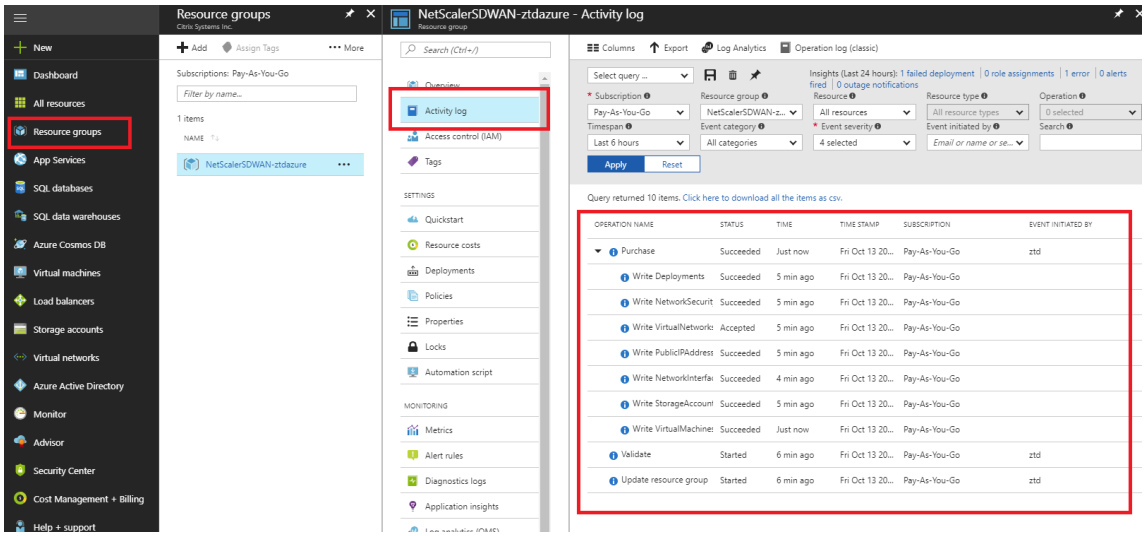


3. 在步骤 1 中，带有激活代码的电子邮件将传送到电子邮件地址输入项，获取电子邮件并打开激活 **URL** 以触发该过程并检查激活状态。

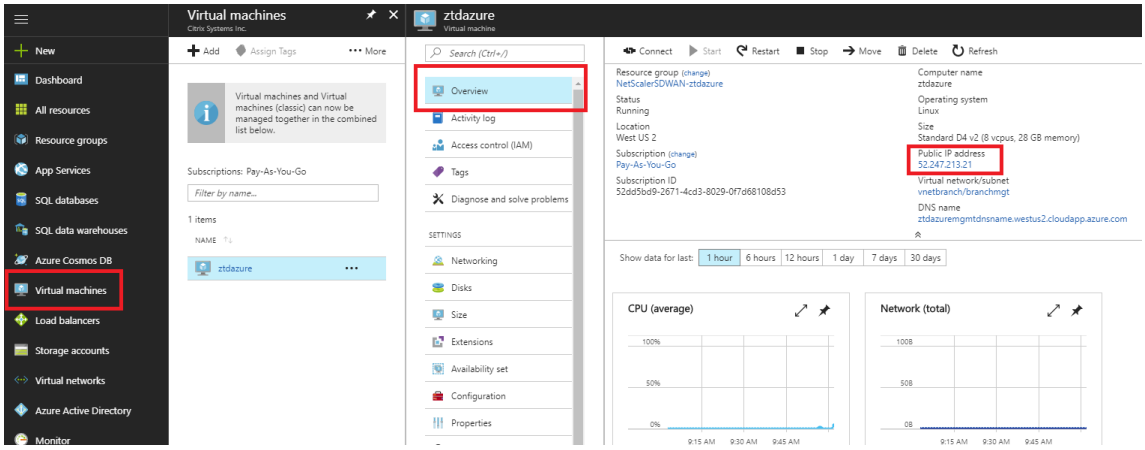


4. 带有激活 URL 的电子邮件将被发送到步骤 1 中输入的电子邮件地址。获取电子邮件并打开 激活 **URL** 以触发流程并检查激活状态。

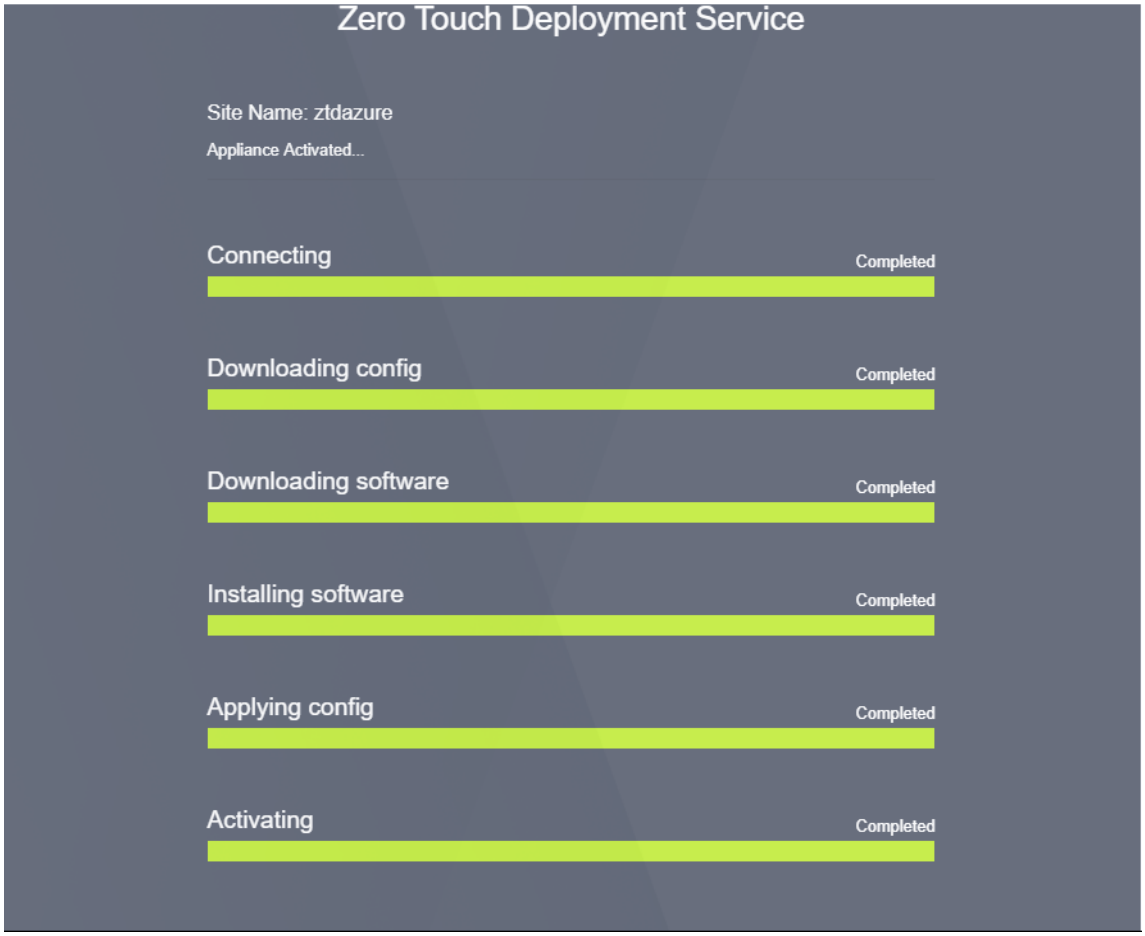
5. 使用 SD-WAN 云服务预配实例需要几分钟时间。你可以在自动创建的 资源组 的 活动日志 下监视 Azure 门户上的活动。Provisioning 的任何问题或错误都将在此处填充，并在激活状态下复制到 SD-WAN 中心。



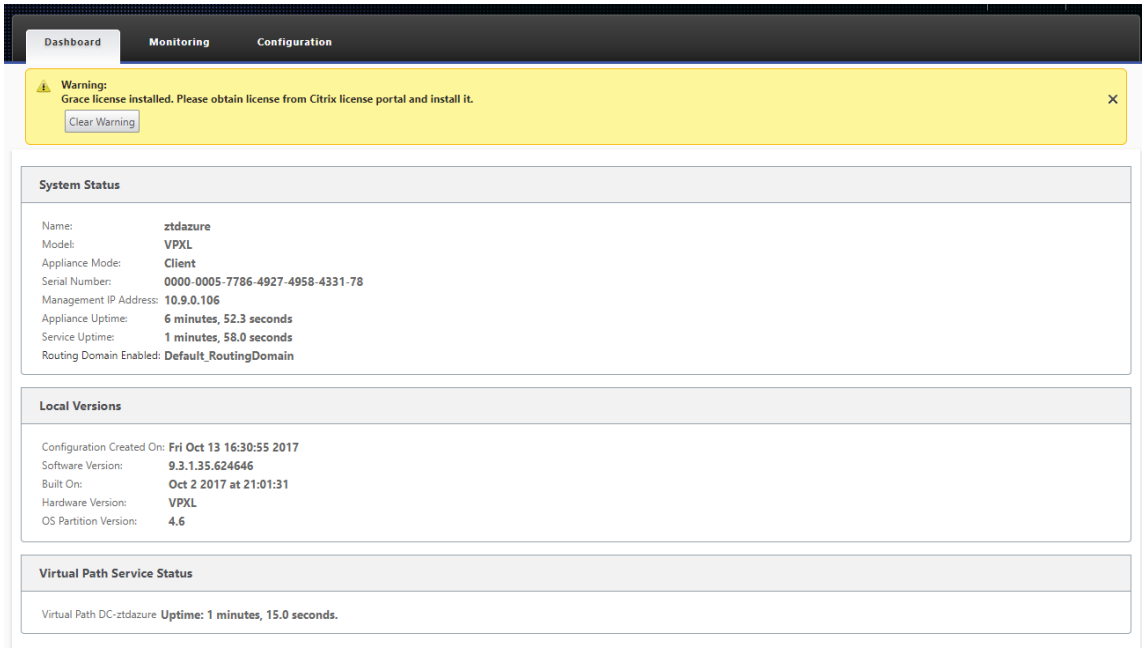
6. 在 Azure 门户中，成功启动的实例将在 虚拟机下提供。要获取分配的公有 IP，请导航到实例的概述。



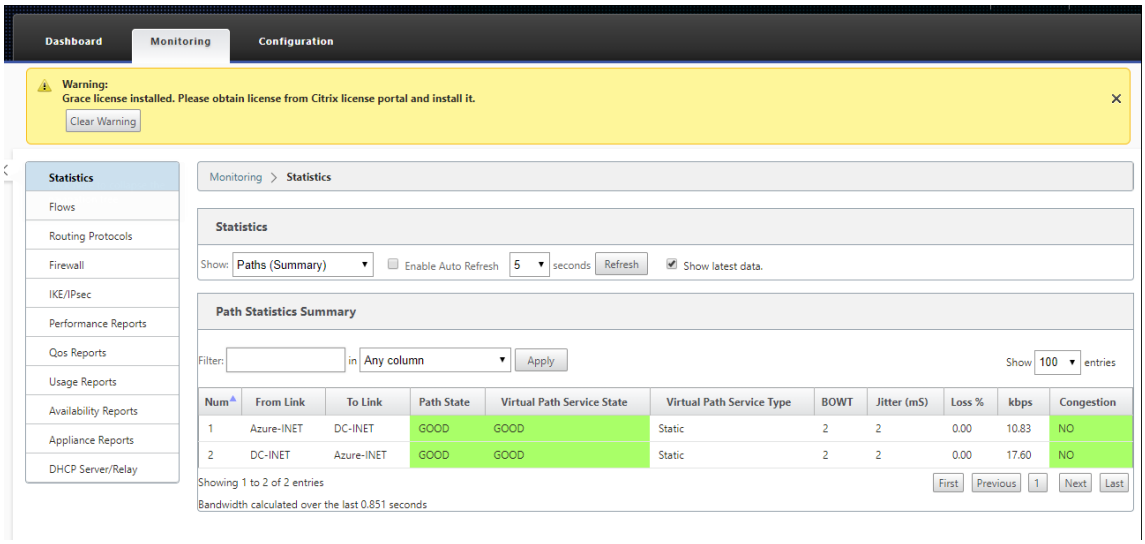
7. 当 VM 处于运行状态时，请在此时间后等待一分钟后，该服务才能完成，并启动下载配置、软件和许可证的过程。



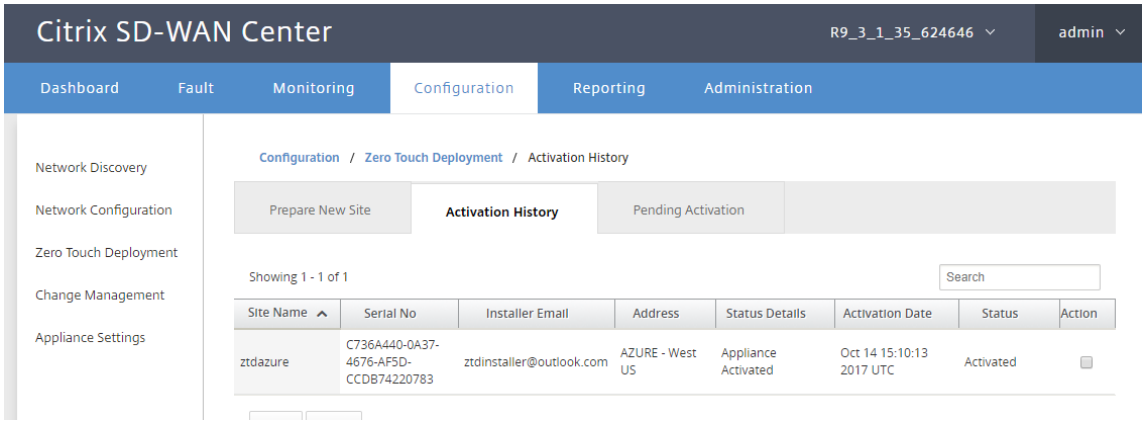
8. 每个 SD-WAN 云服务步骤自动完成后，使用从 Azure 门户获取的公用 IP 登录到 SD-WAN 实例 Web 界面。



9. Citrix SD-WAN 监视统计信息页面将确定从 MCN 到 Azure 中 SD-WAN 实例的成功连接。



10. 此外，还会在 SD-WAN Center 的激活历史记录页面上记录成功的（或失败）预配尝试。



单区域部署

June 22, 2021

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。

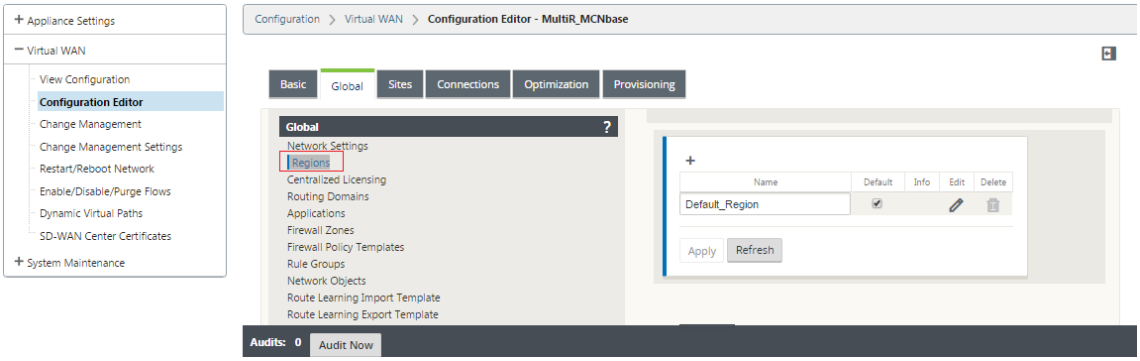
SD-WAN 网络中的单区域部署可以支持小于 550 的网络站点。

您可以在 SD-WAN 设备 GUI 的配置编辑器中配置默认区域。基本编辑器对于仅创建具有 MCN 和客户端 SD-WAN 节点的小型网络非常有用。要使用 MCN、RCN、客户端或高级功能配置多区域网络，请使用配置编辑器中的其他配置选项。

要配置单区域部署：

1. 导航到配置编辑器中的 全局 选项卡。选择 区域。将显示默认区域配置选项。

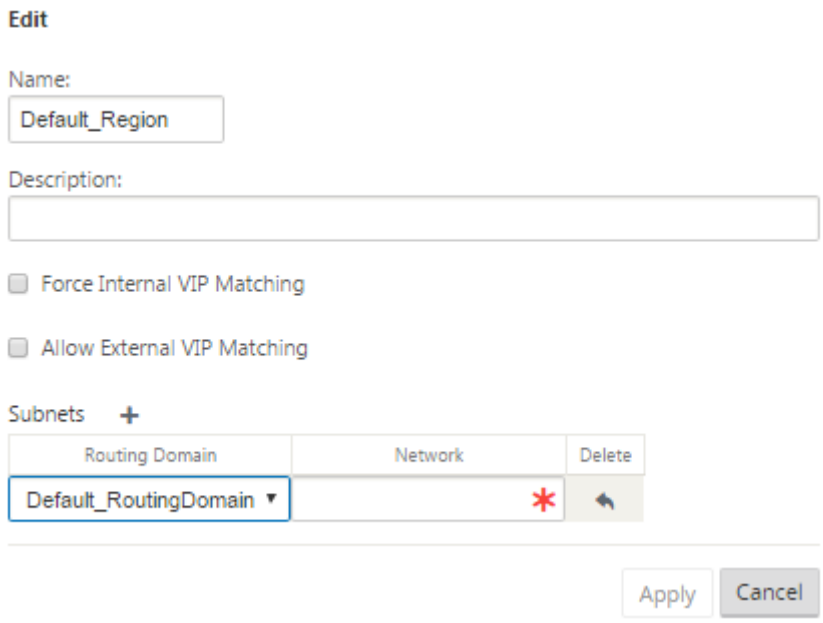
   您可以通过编辑默认区域来更改其名称和描述。



2. 编辑 默认区域 以更改名称并配置子网。
3. 根据您是想要 强制内部 **VIP** 匹配还是允许外部 **VIP** 匹配启用间隔 **VIP** 匹配。

- 强制内部 VIP：启用后，区域中的所有非私有虚拟 IP 地址都被强制匹配配置的子网。
- 允许的外部 VIP-启用后，允许来自其他区域的非私有虚拟 IP 地址与配置的子网匹配。

4. 单击 + 以添加子网。



5. 选择 路由域，输入 网络 地址。单击应用。网络地址是子网的 IP 地址和掩码。

多区域部署

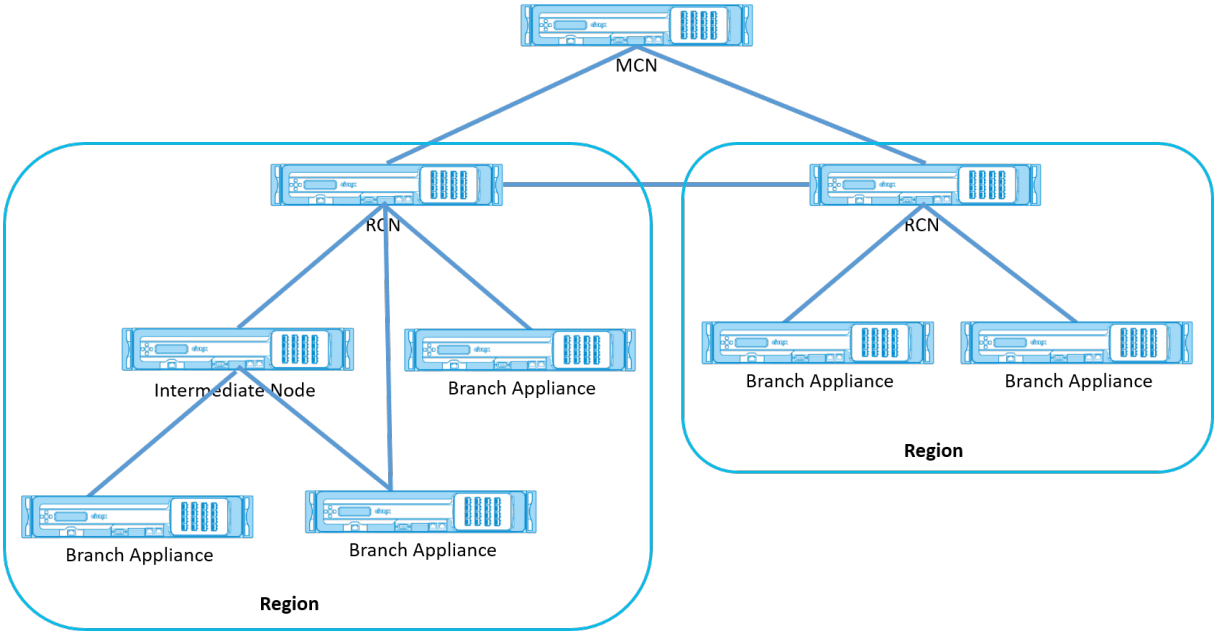
November 1, 2021

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。



下表提供了配置主 MCN/RCN 所支持的平台列表。

> 注意
>
> - 高级版 (PE) 设备以前称为企业版 (EE)。
> - 仅在 SD-WAN 编排器托管的网络中将 Citrix SD-WAN 210 SE 设备用作 MCN。

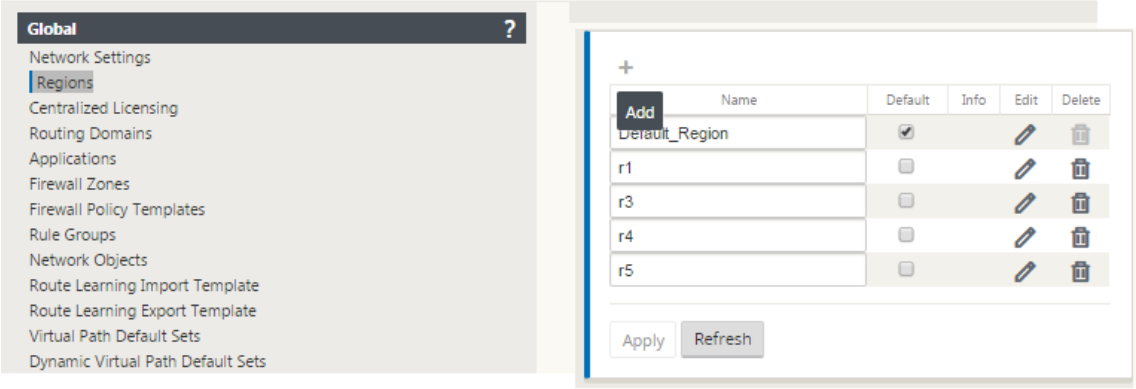
平台版本	小学/中学 MCN	小学/中学 RCN
110-SE	否	否
210-SE	是	是
400-SE	是	否
410-SE	是	否
1000-SE, 1000-PE	是	否
1100-SE, 1100-PE	是	是
VPX-SE、VPXL-SE	是	是
2000-SE, 2100-SE, 2000-PE, 2100-PE, 4000-SE, 4100-SE, 5100-SE, 5100-PE, 6100-SE	是	是

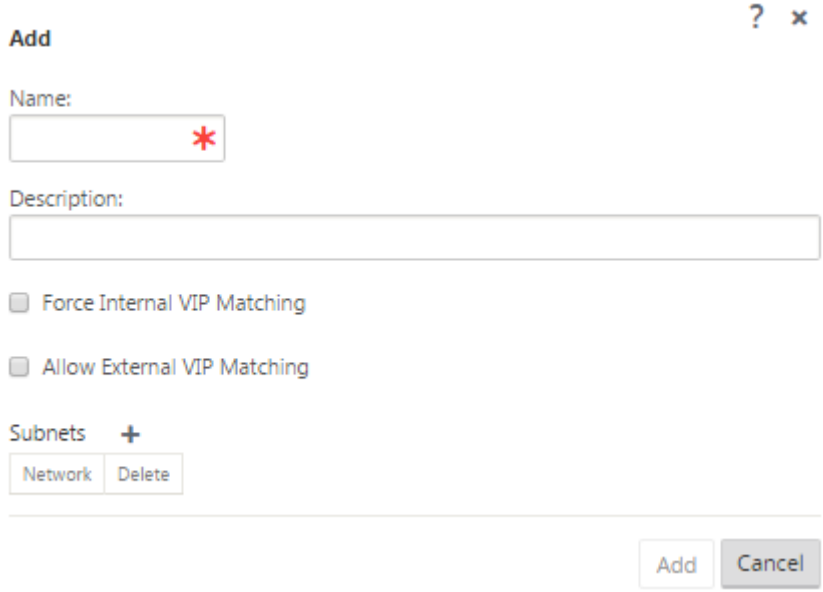
要为 **SD-WAN** 网络配置多区域部署，请执行以下操作：

1. 导航到配置编辑器中的 全局 选项卡。选择 区域。将显示默认区域配置选项。

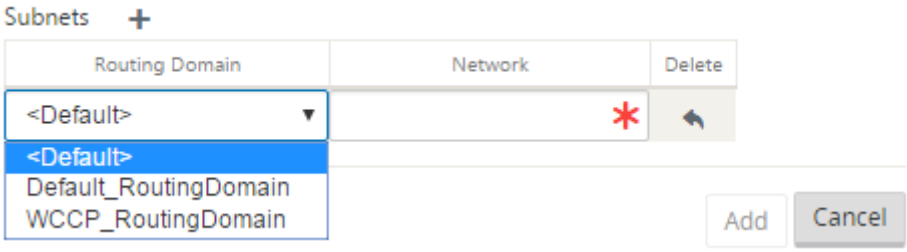
您可以通过编辑默认区域来更改其名称和描述。

2. 单击 **+** 添加以 添加新区域。



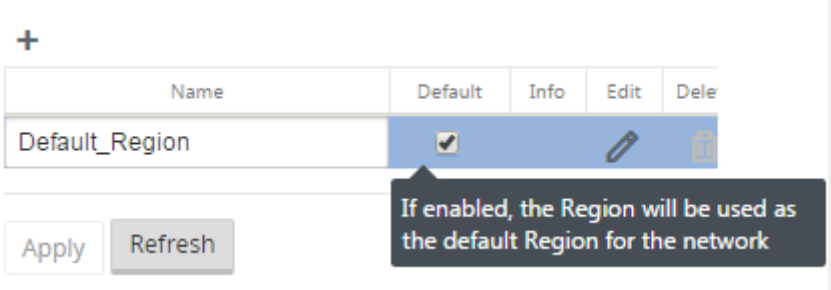


3. 输入区域的名称和描述。
4. 根据您是想要 强制内部 **VIP** 匹配还是允许外部 **VIP** 匹配启用内部 **VIP** 匹配。
   - 强制内部 VIP：启用后，区域中的所有非私有虚拟 IP 地址都被强制匹配配置的子网。
   - 允许的外部 VIP-启用后，允许来自其他区域的非私有虚拟 IP 地址与配置的子网匹配。
5. 单击 + 以添加子网。选择路由域。



6. 输入网 络 地址。单击添加。网络地址是子网的 IP 地址和掩码。新创建的区域将添加到现有的区域列表中。

   您可以选中 默认 复选框以使用所需区域作为默认区域。



> 注意
>
> 您可以将 MCN 克隆到 GEO 或客户端站点。

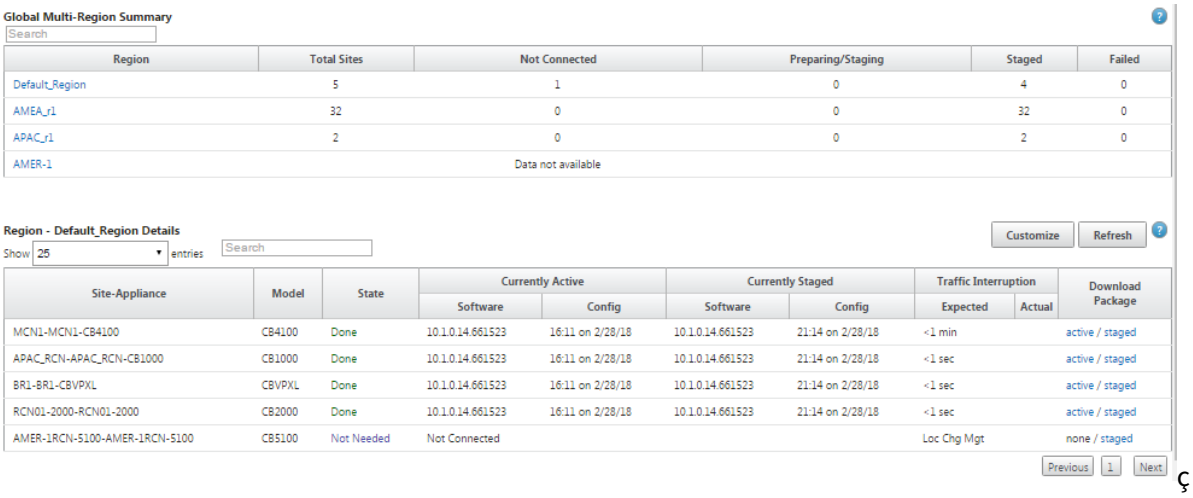
SD-WAN Center 支持多区域部署。有关更多信息，请参阅 SD-WAN Center 多区域部署和报告。

变更管理摘要视图

对在多区域部署中配置的设备执行更改管理过程时，更改管理摘要表将显示在 SD-WAN 设备 GUI 中。

Re **gion** 列显示当前在网络中配置的区域列表。您可以通过在汇总表中选择特定区域的变更管理摘要来查看该摘要。

默认区域摘要：



Global Multi-Region Summary

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - Default_Region Details

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
MCN1-MCN1-CB4100	CB4100	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 min		active / staged
APAC_RCN-APAC_RCN-CB1000	CB1000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
BR1-BR1-CBVPXL	CBVPXL	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
RCN01-2000-RCN01-2000	CB2000	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec		active / staged
AMER-1RCN-5100-AMER-1RCN-5100	CB5100	Not Needed	Not Connected				Loc Chg Mgt		none / staged

区域摘要：

Global Multi-Region Summary

Search

Region	Total Sites	Not Connected	Preparing/Staging	Staged	Failed
Default_Region	5	1	0	4	0
AMEA_r1	32	0	0	32	0
APAC_r1	2	0	0	2	0
AMER-1	Data not available				

Region - AMEA_r1 Details

Show 25 entries Search

Customize Refresh

Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
AMEA_r1_vpx01-AMEA_r1_vpx01	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx02-AMEA_r1_vpx02	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx03-AMEA_r1_vpx03	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx04-AMEA_r1_vpx04	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx05-AMEA_r1_vpx05	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx06-AMEA_r1_vpx06	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx07-AMEA_r1_vpx07	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx08-AMEA_r1_vpx08	CBVPX	Done	10.1.0.14.661523	15:54 on 2/28/18	10.1.0.14.661523	16:11 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx13-AMEA_r1_vpx13	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx14-AMEA_r1_vpx14	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx15-AMEA_r1_vpx15	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx16-AMEA_r1_vpx16	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx17-AMEA_r1_vpx17	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx18-AMEA_r1_vpx18	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx19-AMEA_r1_vpx19	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx20-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx33-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx34-AMEA_r1_vpx20	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx35-vpx35	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx36-vpx36	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx37-vpx37	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx38-vpx38	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx39-vpx39	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx40-vpx40	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged
AMEA_r1_vpx49-vpx49	CBVPX	Done	10.1.0.14.661523	16:11 on 2/28/18	10.1.0.14.661523	21:14 on 2/28/18	<1 sec	0 ms	active / staged

Previous 1 2 Next

> 注意
>
> 在某些情况下，“全局多区域摘要”表中显示的 站点总数 值小于其余列的总和。
>
> 例如，当分支节点未连接时，分支可能被计数两次；一次是“未连接”，一次是“准备/暂存”。

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

June 22, 2021

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。有关详细信息，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

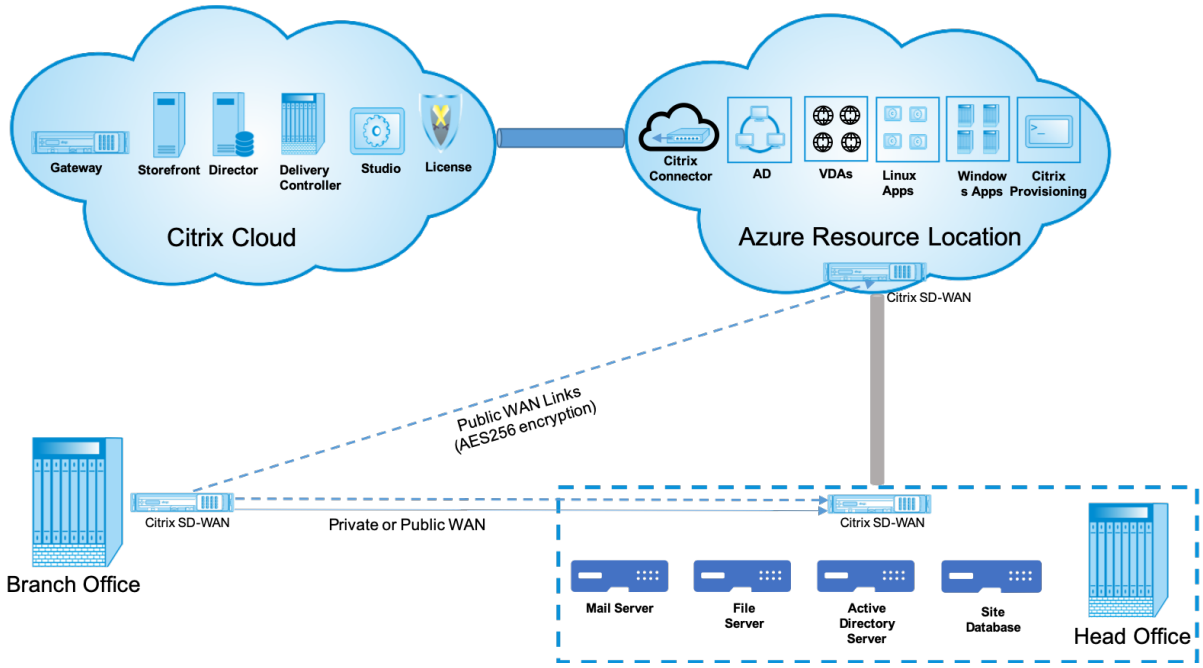
- 通过引导式工作流在 Citrix Virtual Apps and Desktops 中轻松设置 SD-WAN
- 通过先进的 SD-WAN 技术实现始终在线、高性能连接
- 跨所有连接（VDA 到 DC、用户到 VDA、VDA 到云、用户到云）的优势
- 与向数据中心回传流量相比，降低了延迟
- 流量管理以确保服务质量 (QoS)
  - 跨 HDX/ICA 流量流的 QoS（单端口多流 HDX 自动 QoS）
  - HDX 和其他流量之间的 QoS
  - HDX 用户之间的 QoS 公平性
  - 端到端服务质量
- 链路绑定提供更多带宽，实现更快的性能
- 高可用性，具有无缝链路故障切换和 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 云的多租户管理平台，用于 Citrix SD-WAN.

部署体系结构



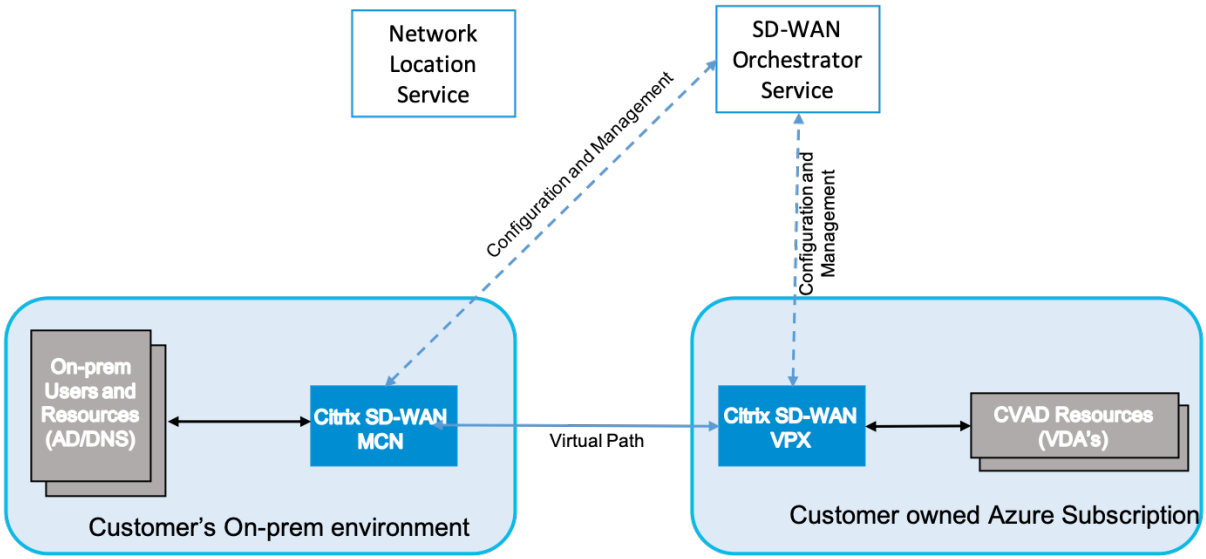
部署需要以下实体：

- 托管 SD-WAN 设备的本地位置，可以在分支模式下部署，也可以作为 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，你也可以选择使用 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。

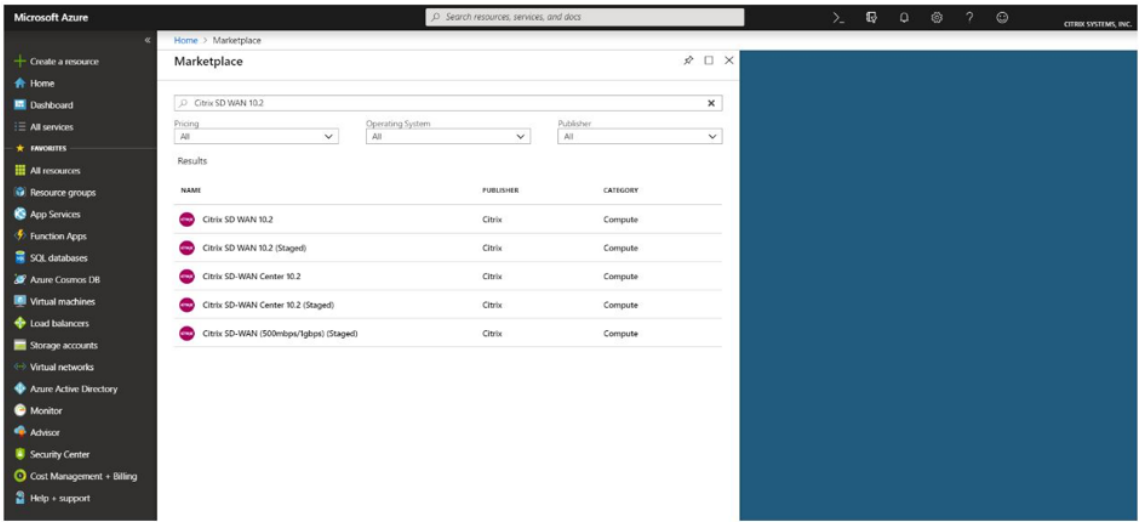
在客户管理的 Azure 订阅中，客户需要部署 Citrix SD-WAN 虚拟设备和 VDA。SD-WAN 设备通过 SD-WAN Orchestrator 理。配置 SD-WAN 设备后，它将连接到现有的 Citrix SD-WAN 网络，并通过 SD-WAN Orchestrator 处理配置、可见性和管理等其他任务。

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。有关详细信息，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，用于互联网连接。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。

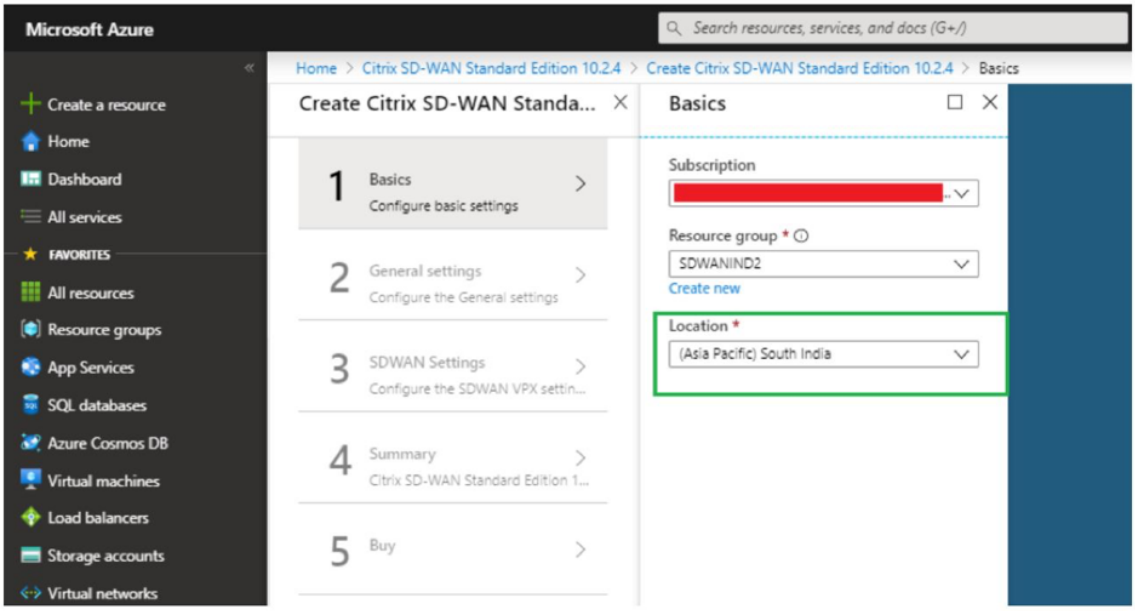


单击 创建后，将显示向导，提示创建虚拟机的必要详细信息。

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。

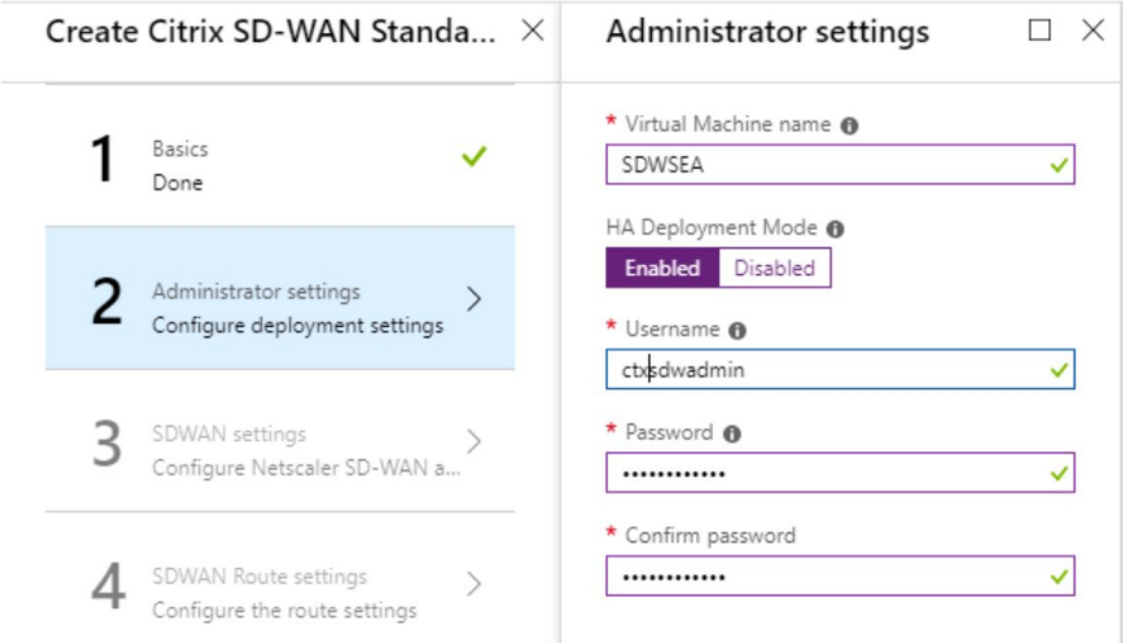
   对于 Citrix SD-WAN，建议您选择的资源组必须为空。同样，选择要在其中部署 SD-WAN 实例的 Azure 区域。该区域必须与部署 Citrix Virtual Apps and Desktops 资源的区域相同。



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 **OK**（确定）。

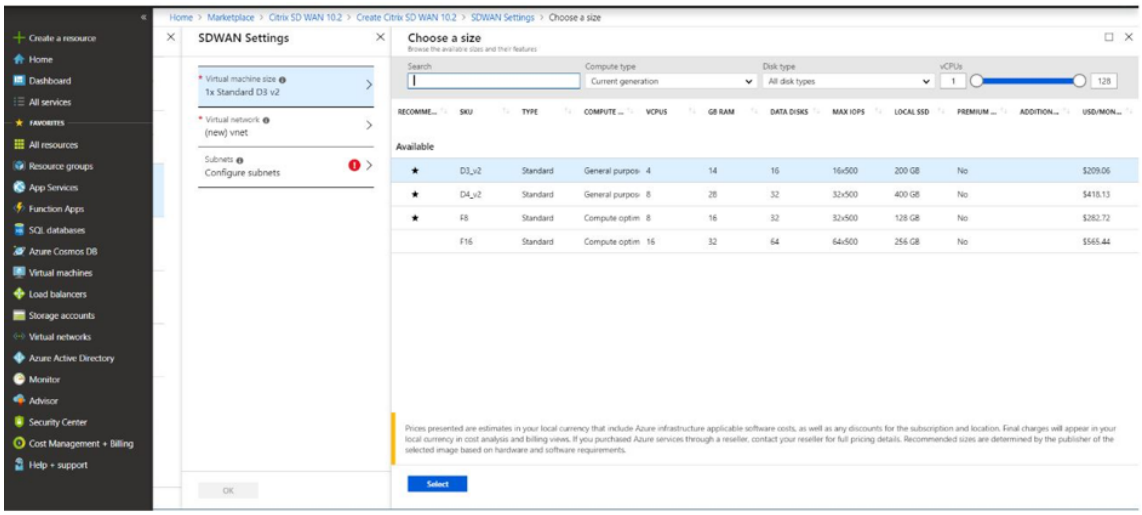
   以来宾用户身份登录到实例的管理界面需要此密码。要获得对实例的管理员访问权限，请使用 admin 作为用户名，并使用在 Provisioning 实例时创建的密码。如果您使用在 Provisioning 实例时创建的用户名，则可获得只读访问权限。此外，请在此处选择部署类型。

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。

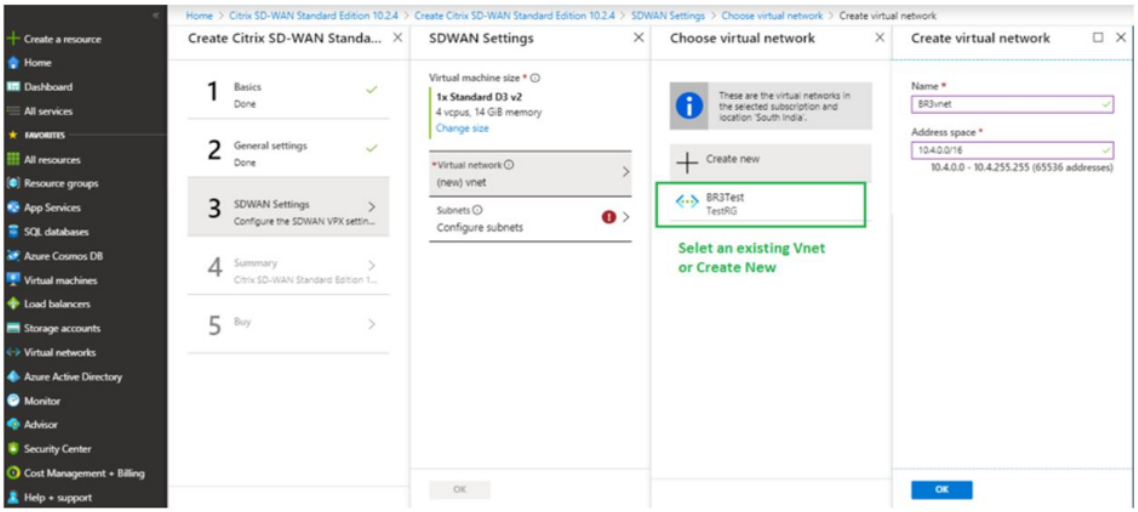


5. 在 **SD-WAN** 设置 页面下，选择要在其中运行映像的实例。根据您的要求选择以下实例类型：

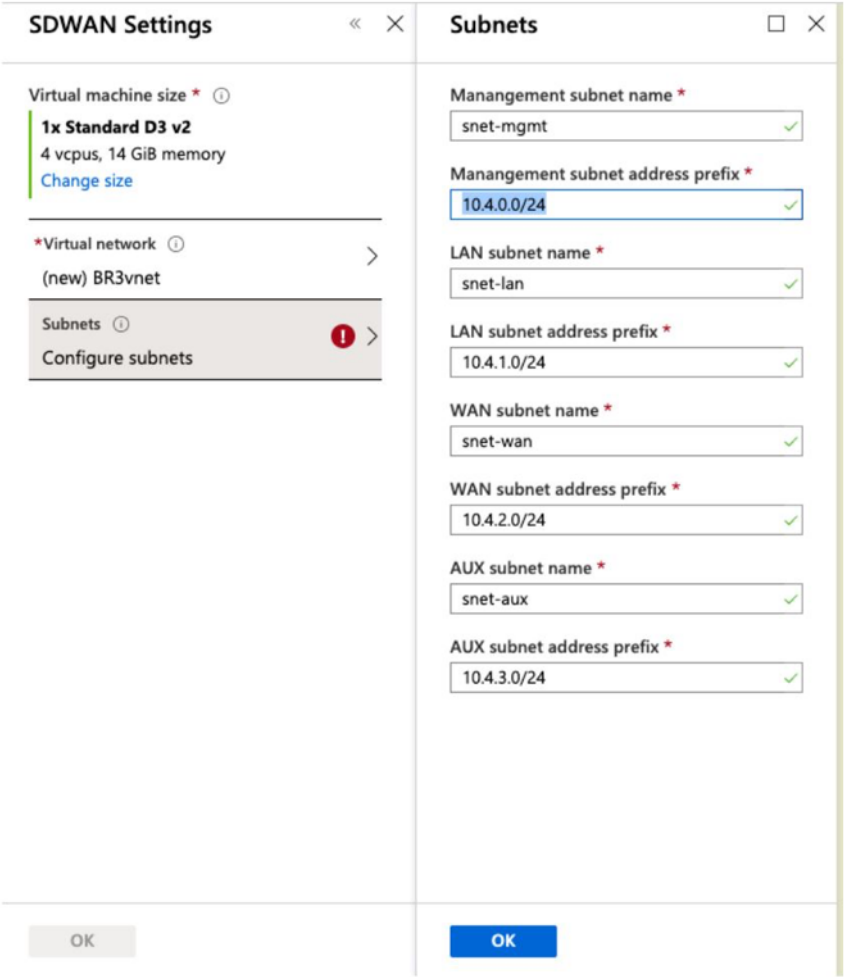
   - 实例类型 D3_V2，最大单向吞吐量为 200 Mbps，最多可直接连接 16 个分支。
   - 实例类型 D4_V2，最大单向吞吐量为 500 Mbps，最多可直接连接 16 个分支。
   - 实例类型 F8 标准，最大单向吞吐量为 1 Gbps，最多可直接连接 64 个分支。
   - 实例类型 F16 标准，最大单向吞吐量为 1 Gbps，最多可直接连接 128 个分支。



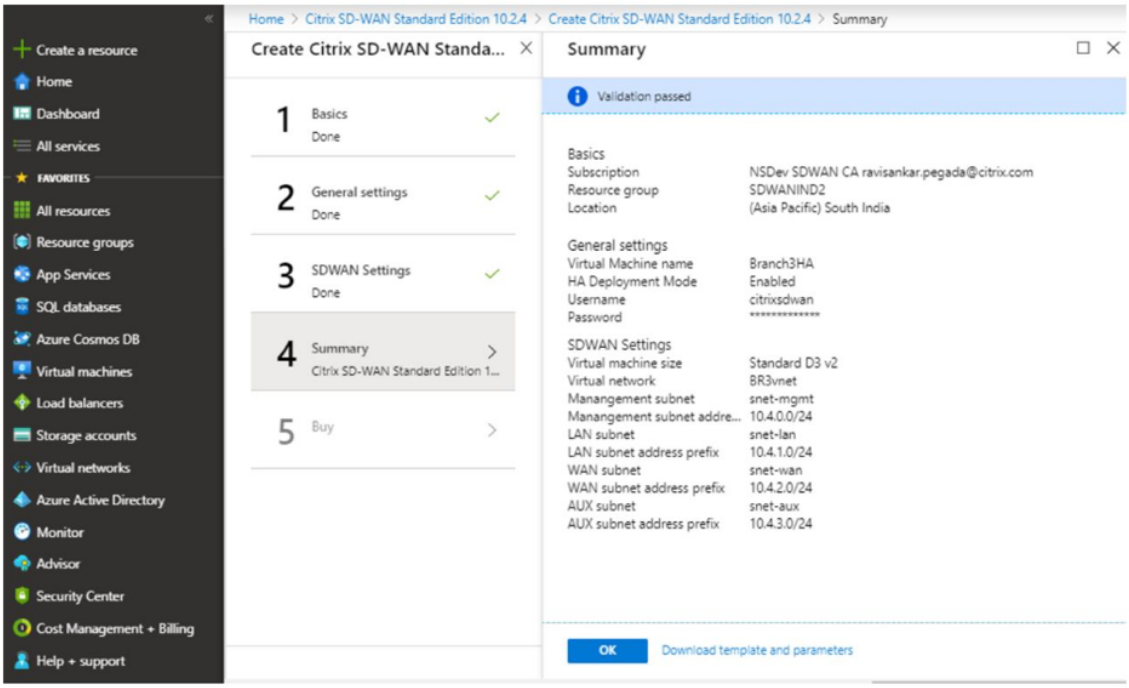
6. 创建新的虚拟网络 (VNet) 或使用现有虚拟网络。这是部署的最关键步骤，因为此步骤选择要分配给 SD-WAN VPX 虚拟机接口的子网。



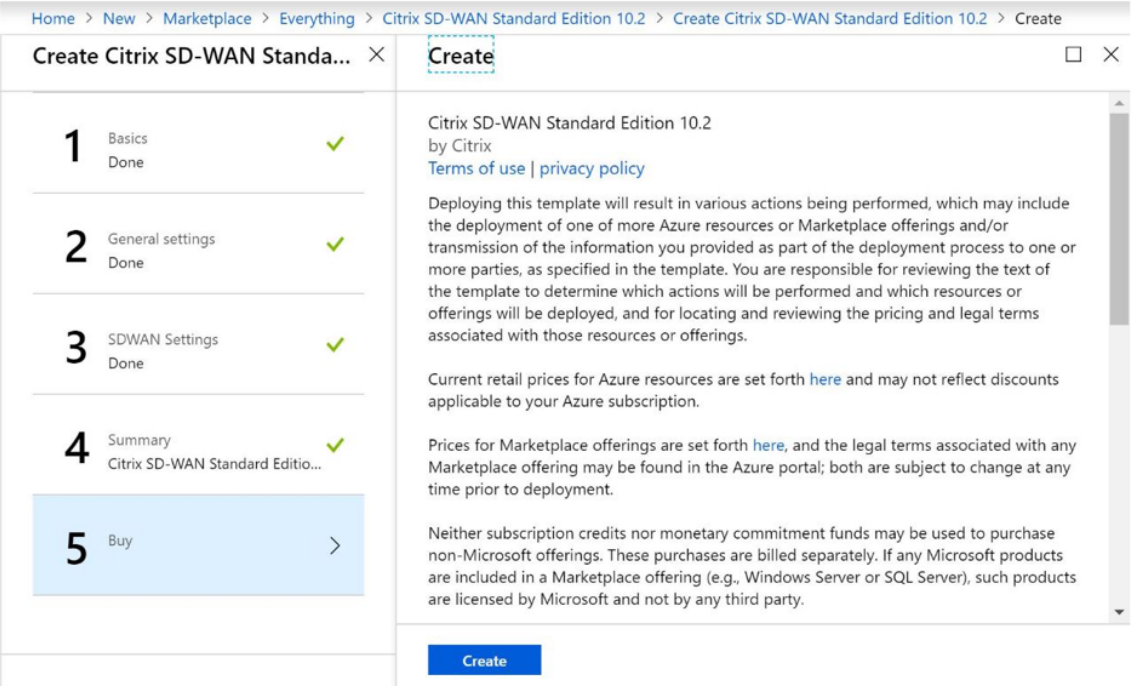
仅当您以 HA 模式部署实例时，才需要辅助子网。确保 SD-WAN 实例部署在与 Citrix Virtual Apps and Desktops 资源相同的 VNet 中，并且与 SD-WAN VPX 设备的 LAN 接口位于同一子网中。



7. 在“摘要”页面中验证配置，然后单击“确定”。



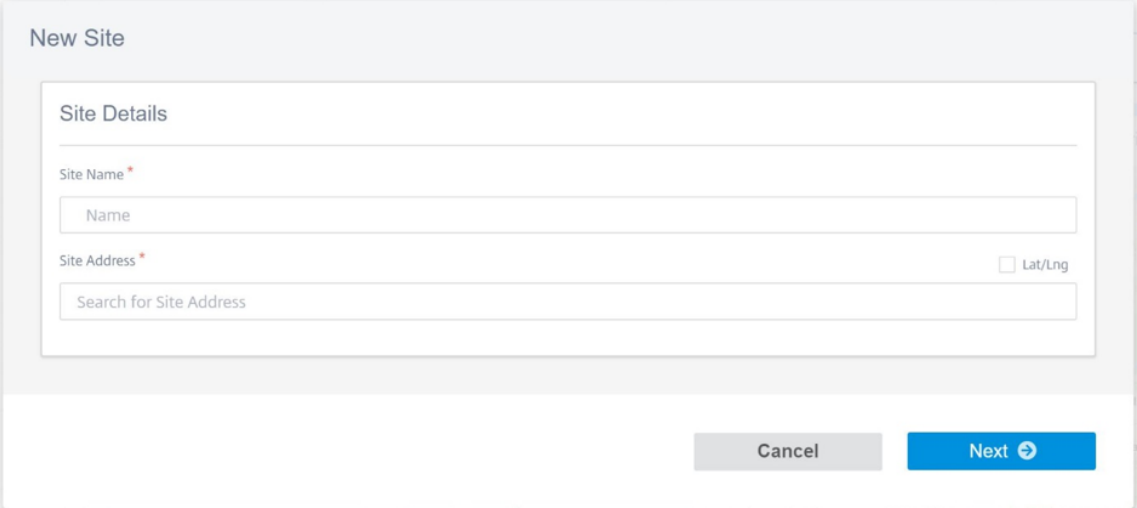
8. 在 购买 页面上，单击 创建 以启动实例的预配过程。预配置实例可能需要大约 10 分钟。你会在 Azure 管理门户中收到一条通知，建议实例创建成功/失败。



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。

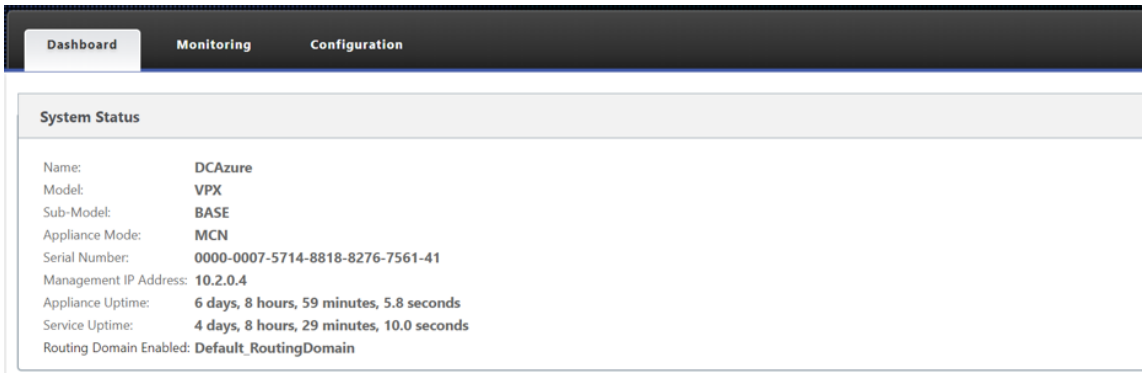
9. 置备站点后，登录 SD-WAN Orchestrator 以对其进行配置。如前提条件中所述，您必须拥有 SD-WAN Orchestrator 才能配置站点。如果你还没有它，请参阅 Citrix SD-WAN Orchestrator 加入。
10. 如果你已经有 SD-WAN 网络，则继续为在 Azure 中置备的站点创建配置。否则，您必须创建一个 MCN。有关详细信息，请参阅网络配置。
11. 一旦你有权访问 SD-WAN Orchestrator 并且已经设置了 MCN，请登录 SD-WAN Orchestrator，然后单击 **+** 新站 点开始配置 SD-WAN VPX 设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



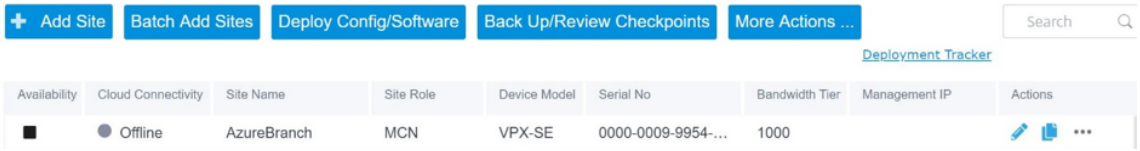
12. 提供唯一的站点名称，并根据要 Provisioning 映像的区域输入地址。要在 Azure 中设置实例，请参阅 基本设置。

> 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。

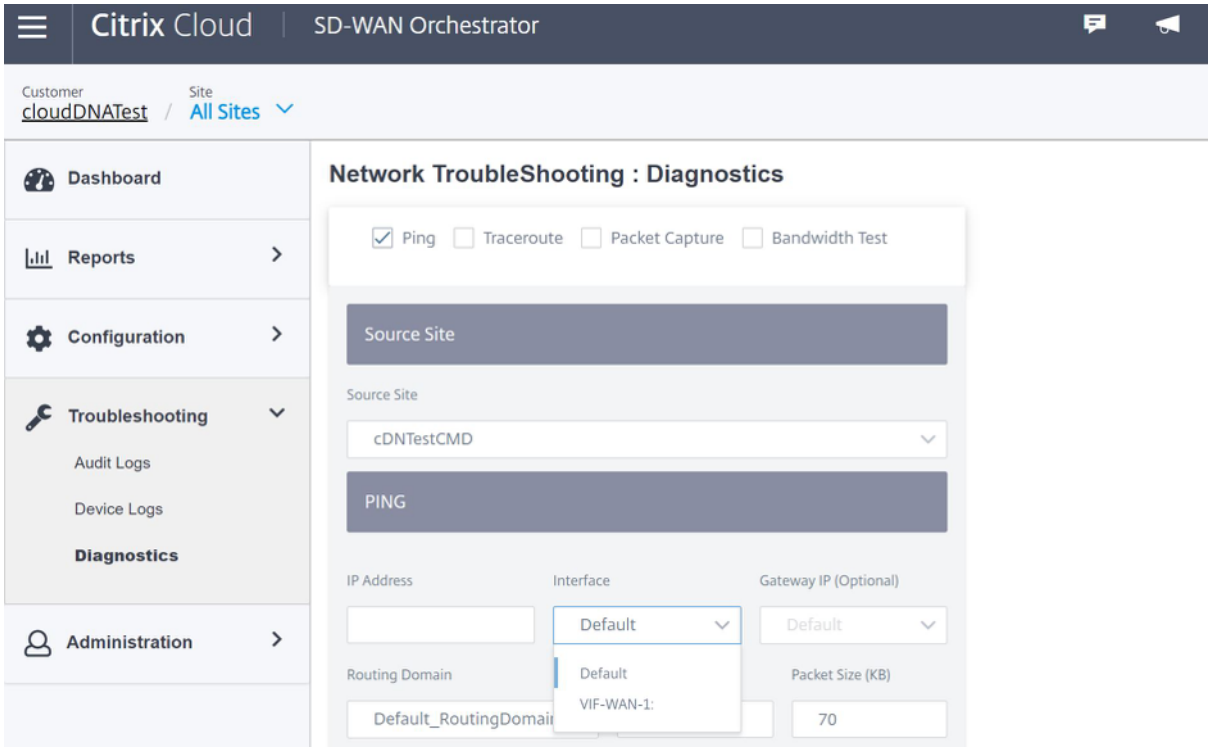


15. 如果没有问题且配置准确无误，则在运行配置部署后，必须在 Azure 中的实例和 MCN 之间建立虚拟路径。

Citrix Virtual Apps and Desktops 配置

正如 部署和配置 部分中所强调的那样，AD/DNS 存在于作为 DC 的本地位置，而在局域网上 SD-WAN 背后的部署中，AD/DNS 存在于 SD-WAN 的部署中。这是您需要在此处配置的 AD/DNS 的 IP。如果你正在使用 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。网络位置 服务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。

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

November 1, 2021

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。

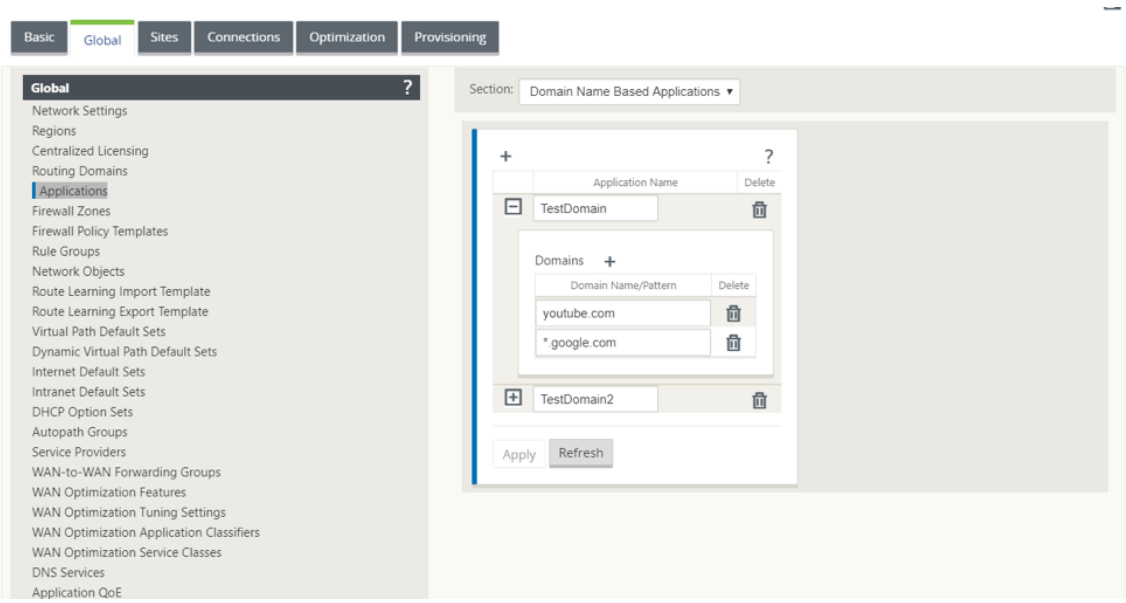
DNS 代理

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。

要将 SD-WAN 配置为 DNS 代理，请执行以下操作：

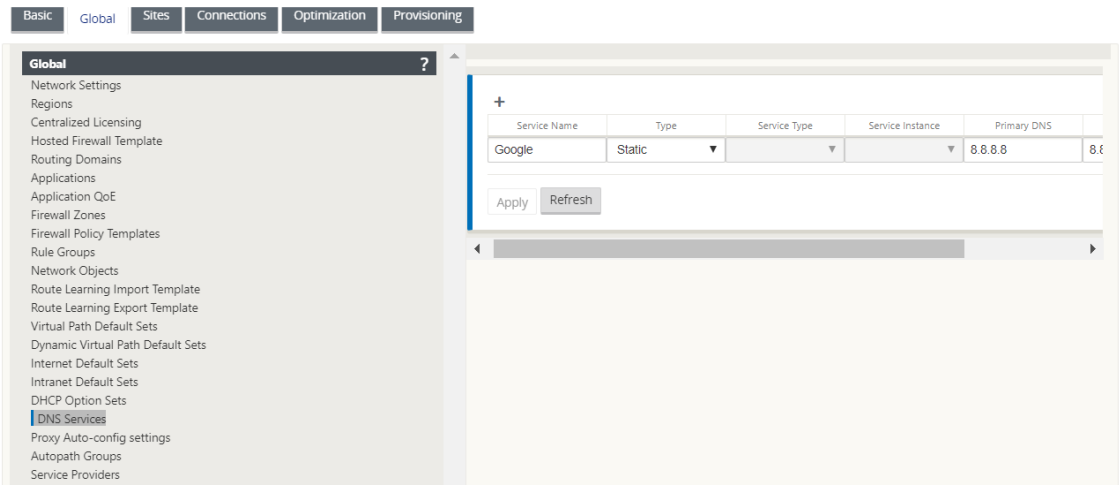
1. 定义基于域名的应用程序。在配置编辑器中，导航到 全局 **>** 应用程序 **>** 基于域名的应用程序。

   输入应用程序名称和所需的域名或模式。您可以将多个域名分组为应用程序。您可以在开头输入完整域名或使用通配符。例如 - *.google.com



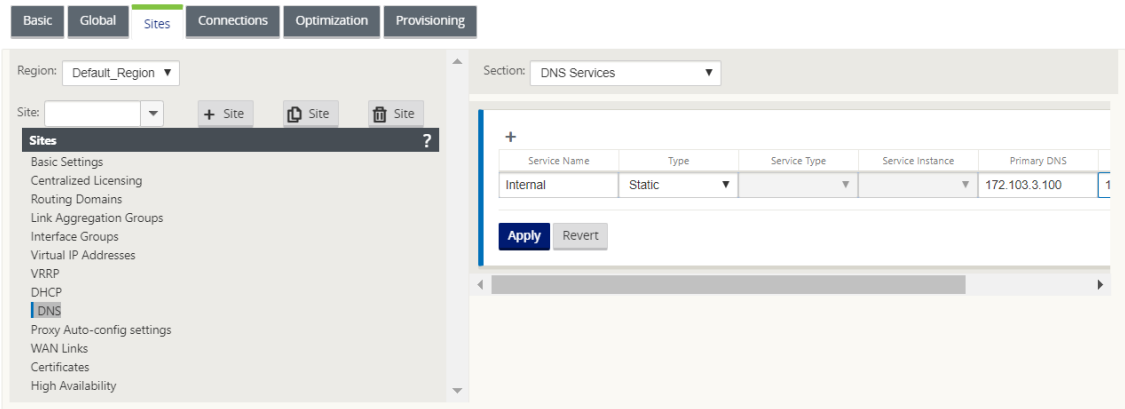
2. 定义所需的 DNS 服务。您可以定义静态或动态 DNS 服务。

   要配置静态 DNS 服务，请导航到 全局 > **DNS** 服务，选择 类型 为 静态（对于 IPv4 地址）或 **Staticv6** （对于 IPv6 地址）。输入 服务名称 以及一对主 DNS 服务器和辅助 DNS 服务器 IP 地址。



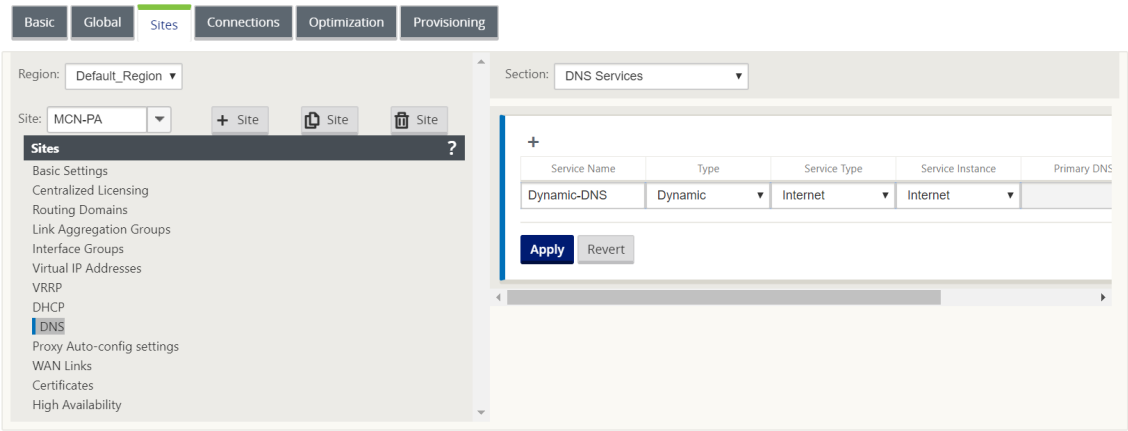
> 注意
>
> 如果您已配置 Office 365 分组策略，则会自动创建 Quad9 DNS 服务。有关详细信息，请参阅 Office 365 优化。

或者，您也可以在单个站点级别定义静态 DNS 服务。站点级别的 DNS 服务配置覆盖全局配置。要配置特定于站点的静态 DNS 服务，请导航到 站 点 > **DNS> DNS** 服务，然后选择类型为静态（对于 IPv4 地址）或 **Staticv6**（对于 IPv6 地址）。



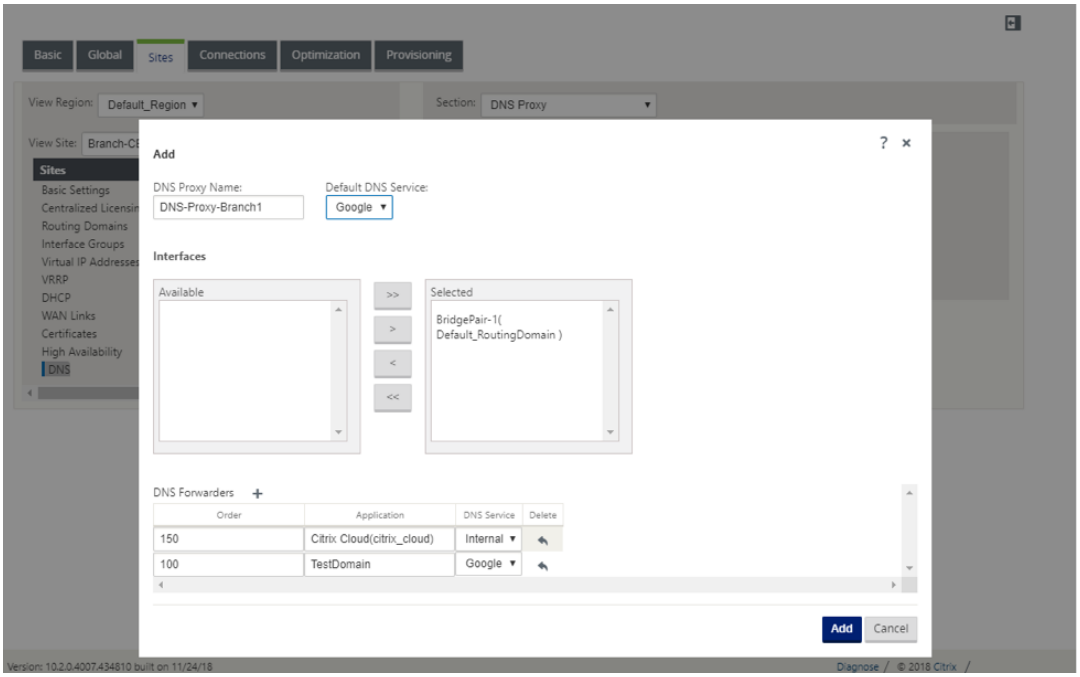
要配置动态 DNS 服务，请导航到 站点 > **DNS** > **DNS** 服务，然后选择 类型 为 动态（对于 IPv4 地址）或 **Dynamicv6** （对于 IPv6 地址）。输入 服务名称，然后为 服务类型和服务实例选择 **Internet**。

> 注意
>
> 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。



3. 为站点配置 DNS 代理。导航到 站点 **> DNS > DNS** 代理。单击 **+**。输入以下参数的值：

   - **DNS** 代理名称：DNS 代理的名称。
   - **IPv4** 默认 **DNS** 服务：如果 DNS 转发器查找中的应用程序都不匹配，则 DNS 请求将转发到的 IPv4 默认 DNS 服务。
   - **IPv6** 默认 **DNS** 服务：如果 DNS 转发器查找中的应用程序都不匹配，则 DNS 请求将转发到的 IPv6 默认 DNS 服务。
   - 接口：截获 DNS 请求的接口。仅允许受信任的接口。
   - **DNS** 转发器：DNS 转发器列表。
     - 顺序：货运代理的优先级。
     - 应用程序：必须将 DNS 请求转发到所选 DNS 服务的应用程序。
     - **IPv4 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv4 DNS 服务。
     - **IPv6 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv6 DNS 服务。



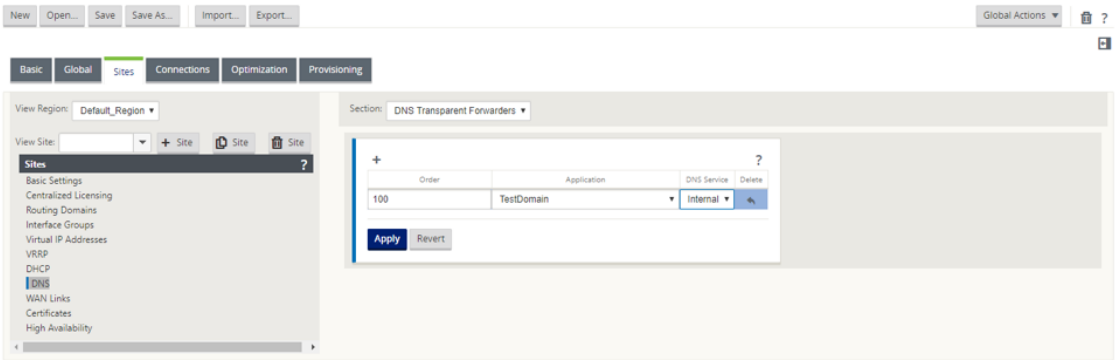
> 注意
>
> 在以下 SD-WAN 设备上无法配置 DNS 代理：
>
> - Citrix SD-WAN 1000 SE /PE
> - Citrix SD-WAN 2000 SE /PE
> - Citrix SD-WAN 4000 SE

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。

要将 SD-WAN 配置为 DNS 透明转发器，请执行以下操作：

1. 导航到 站点 **> DNS > DNS** 透明转发器。单击 **+**。
2. 输入以下参数的值：
   - 顺序：货运代理的优先级。
   - 应用程序：必须将 DNS 请求转发到所选 DNS 服务的应用程序。
   - **IPv4 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv4 DNS 服务。
   - **IPv6 DNS** 服务：为指定应用程序将 DNS 请求转发到的 IPv6 DNS 服务。



同样，继续根据需要添加其他 DNS 透明转发器。

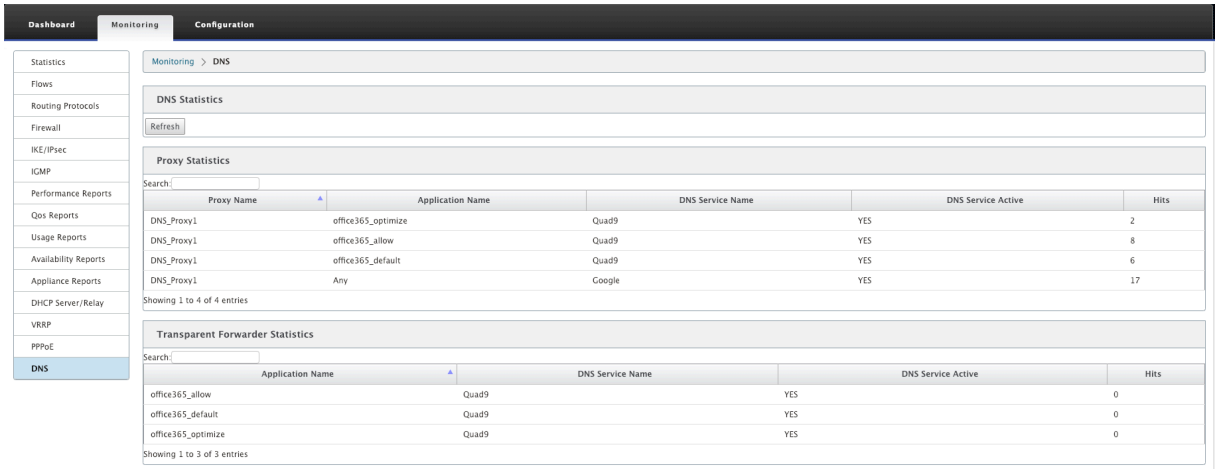
3. 单击应用。

监视

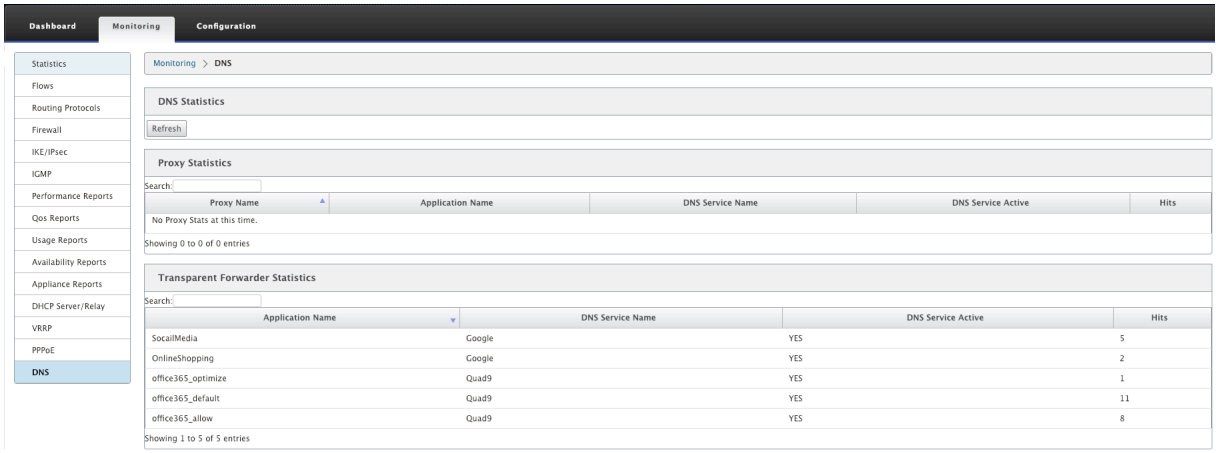
要查看代理统计信息和透明转发器统计信息，请导航到 监控 **> DNS**。

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



透明的货运代理统计



DHCP 服务器和 DHCP 中继

November 16, 2022

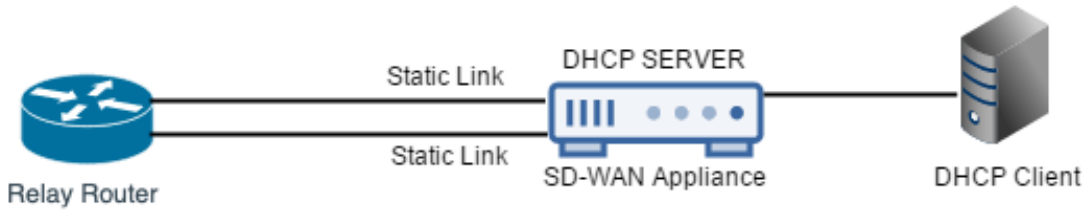
Citrix SD-WAN 引入了将 Standard 或 Premium Edition 设备用作 DHCP 服务器或 DHCP 中继代理的功能。通过 DHCP 服务器功能，与 SD-WAN 设备的 LAN/WAN 接口位于同一网络中的设备可以从 SD-WAN 设备获取其 IP 配置。通过 DHCP 中继功能，您的 SD-WAN 设备可以在 DHCP 客户端与服务器之间转发 DHCP 数据包。

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。

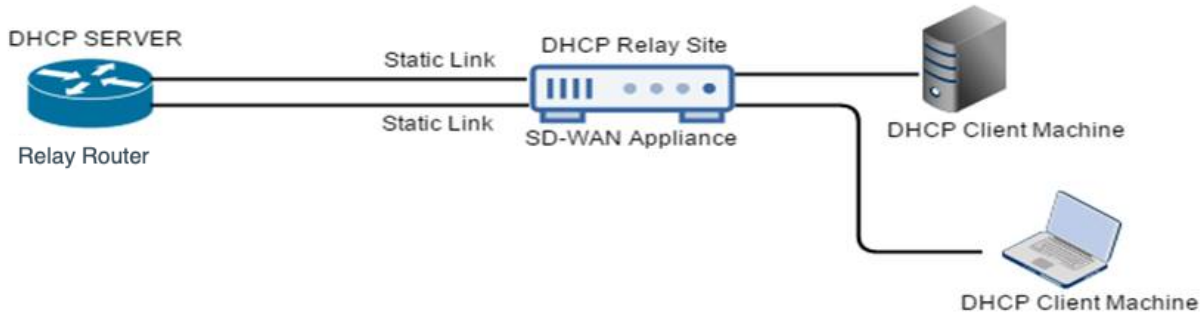
DHCP 服务器

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。



配置 **DHCP** 服务器和 **DHCP** 中继

November 1, 2021

使用配置编辑器配置 **DHCP** 服务器和 **DHCP** 中继

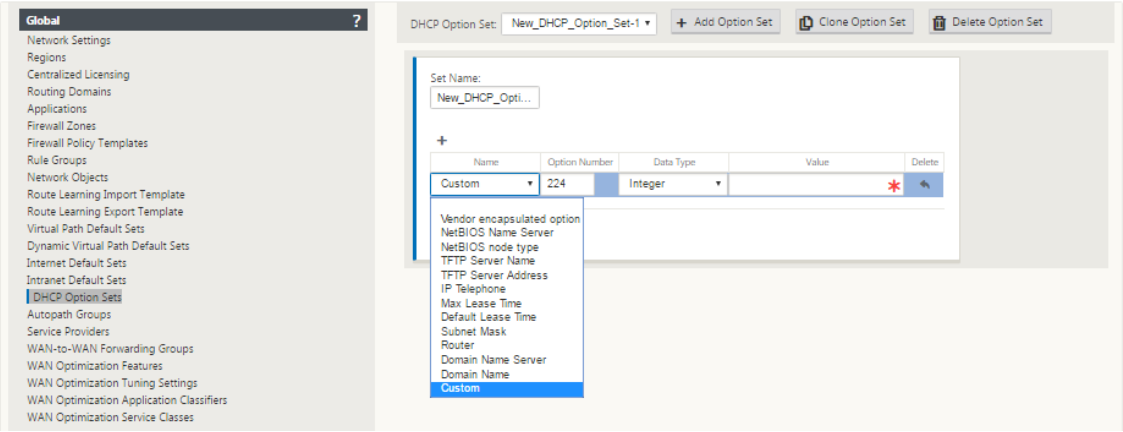
您可以使用配置编辑器为网络上的设备配置 DHCP 服务器和 DHCP 中继设置。通过更改管理过程，将配置推送到 SD-WAN 网络中的设备。

要使用配置编辑器将站点配置为 DHCP 服务器，请执行以下操作：

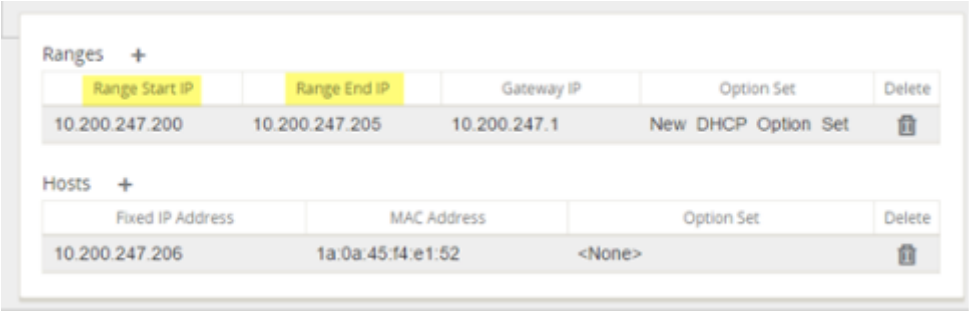
1. 导航到 配置编辑 器 > 站点 **>** 站 [点名称] > DHCP > 服务器子网。单击 **+**。
2. 如果存在多个域，请选择已配置的路由域。
3. 选择用于 接收 **DHCP** 请求的虚拟接口。DHCP 服务器用于提供地址的 IP 子网将自动填充。

4. 输入 域名、主 **DNS** 和 辅助 **DNS**。DHCP 服务器将此信息转发给客户端。
5. 单击 启用 以启用子网。
6. 配置将用于为客户端分配 IP 地址的动态 IP 地址池。指定起始和结束 IP 地址的范围，然后选择 选项集。

> 注意
>
> DHCP 选项集是可应用于各个 IP 地址范围的 DHCP 设置组。要创建 DHCP 选项集，请导航到 全局 > **DHCP** 选项集。选择所需的 DHCP 选项并为其指定值。



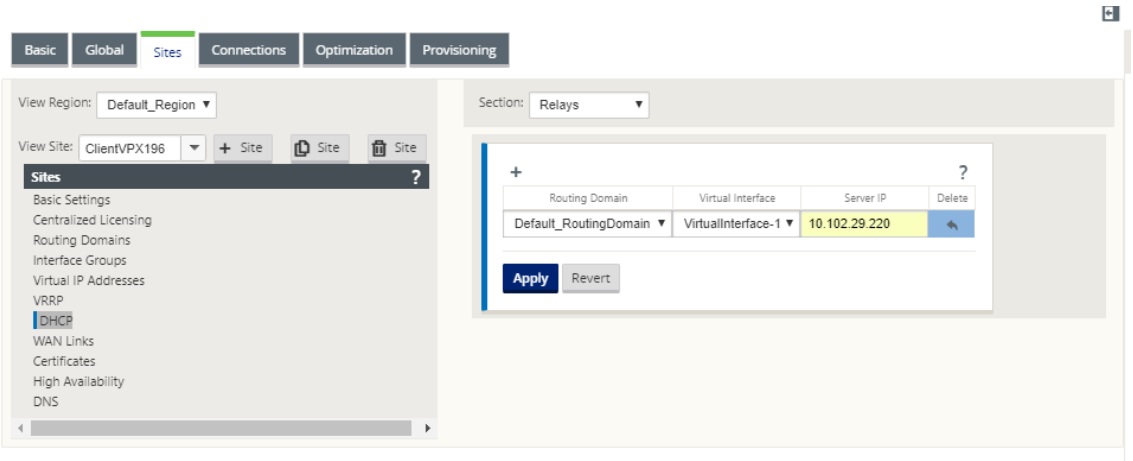
7. 根据 MAC 地址配置需要固定 IP 地址的各个主机。也称为 Reserver IP 地址。选择 固定 **IP** 地址、**MAC** 地址和选项集。



> 注意
>
> 对于固定 IP 地址，网关 **IP** 是通过在 **DHCP** 选项集中配置路由器选项来设置的。

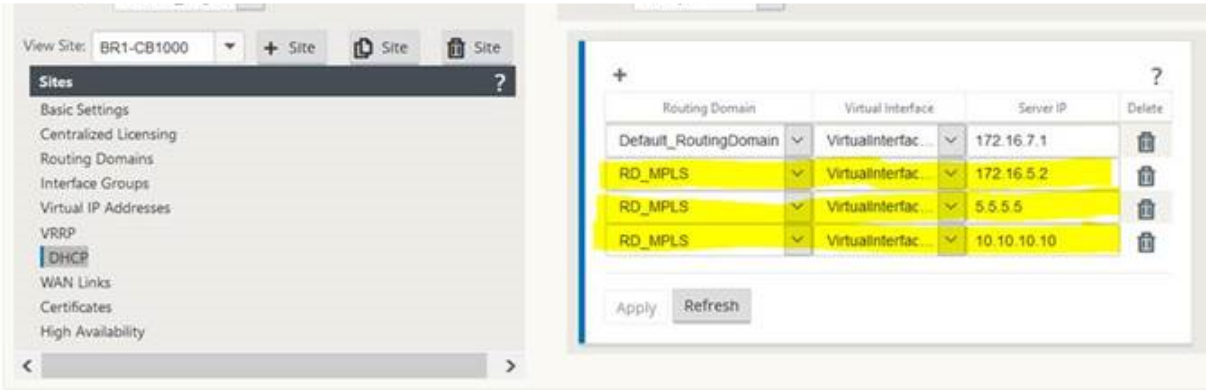
要使用配置编辑器将站点配置为 DHCP 中继，请执行以下操作：

1. 导航到 配置编辑器 > 站点 [点名称] > > **DHCP** > 中 继。单击 **+**。
2. 如果存在多个域，请选择已配置的路由域。
3. 选择与远程 DHCP 服务器通信的虚拟接口。
4. 输入中继将用于转发来自客户端的请求和响应的 DHCP 服务器 IP。

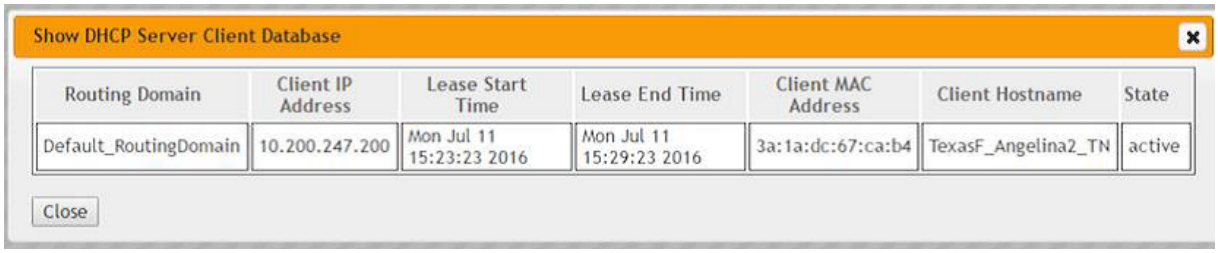


您可以使用公用虚拟网络接口配置单个 DHCP 中继，并将其指向多个 DHCP 服务器。

> 注意：
>
> 每个虚拟接口生成一个中继代理，每个中继代理总共可配置 16 台 DHCP 服务器。一个站点上最多可以配置 16 个中继代理。



要查看 DHCP 服务器数据库中的客户端列表，请在 Web 管理界面中导航到 监视 器 > **DHCP** 服务器/中继。



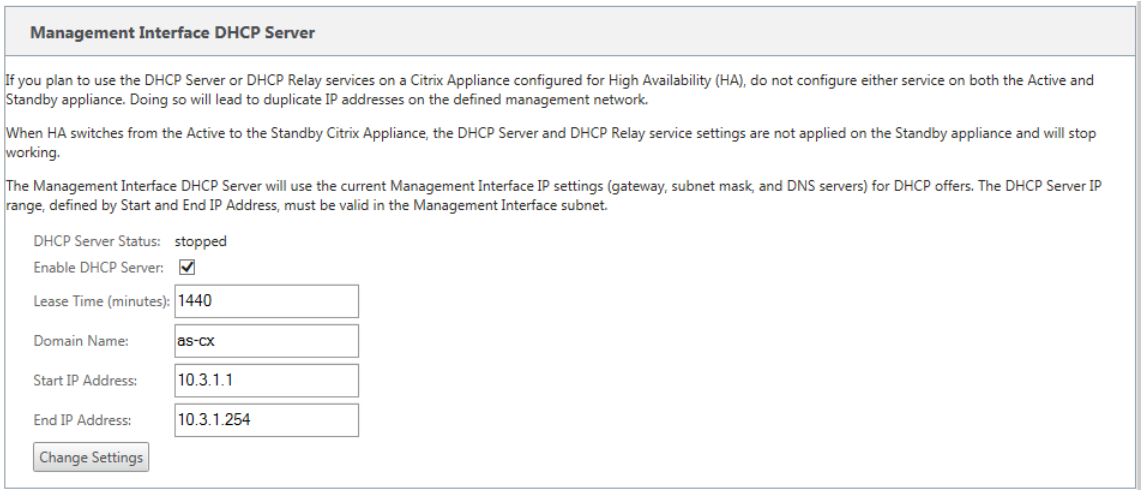
使用设备设置将 **SD-WAN** 设备配置为 **DHCP** 服务器或 **DHCP** 中继

您可以从设备设置页面手动将单个 SD-WAN 设备配置为 DHCP 服务器或 DHCP 重放。

要在 SD-WAN 设备上启用 DHCP 服务器，请执行以下操作：

1. 导航到 配置 > 装置设置 > 网络适配器。在“网络适配器”页面中，查找“管理接口 **DHCP** 服务器”窗格。
2. 单击 启用 **DHCP** 服务器 启动服务器，然后输入 租约时间（以分钟为单位）、域名，然后通过输入 开始 **IP** 地址和结束 **IP** 地址 ** 来定义 **IP** 地址 范围 **。

   > 注意：
   >
   > 服务器 IP 地址池应位于管理网络内。



3. 单击 更改设置 以完成 DHCP 服务器的配置。

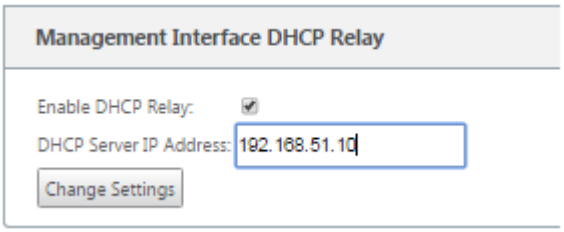
   > 注意
   >
   > 如果计划在配置为高可用性 (HA) 的 SD-WAN 设备上使用 DHCP 服务器，请勿在活动和备用设备上同时配置服务。这样做会导致定义的管理网络上的 IP 地址重复。

4. 单击 显示客户端 以查看当前的 DHCP 客户端，然后单击 清除客户 端以释放 DHCP 客户机租用

要在 SD-WAN 设备上启用 DHCP 中继服务，请执行以下操作：

1. 导航到 配置 > 装置设置 > 网络适配器。在“网络适配器”页面中，查找“管理接口 **DHCP** 中继”窗格。
2. 单击 启用 **DHCP** 中继 复选框以启用该服务。输入 **DHCP** 服务器 **IP** 地址，然后单击 更改设置以开始将设 备用作 DHCP 中继代理。

   > 注意
   >
   > 如果计划在配置为高可用性 (HA) 的设备上使用 DHCP 中继服务，请勿在活动和备用设备上配置该服务。这样做会导致定义的管理网络上的 IP 地址重复。



通过 DHCP 客户端进行 WAN 链接 IP 地址学习

June 8, 2022

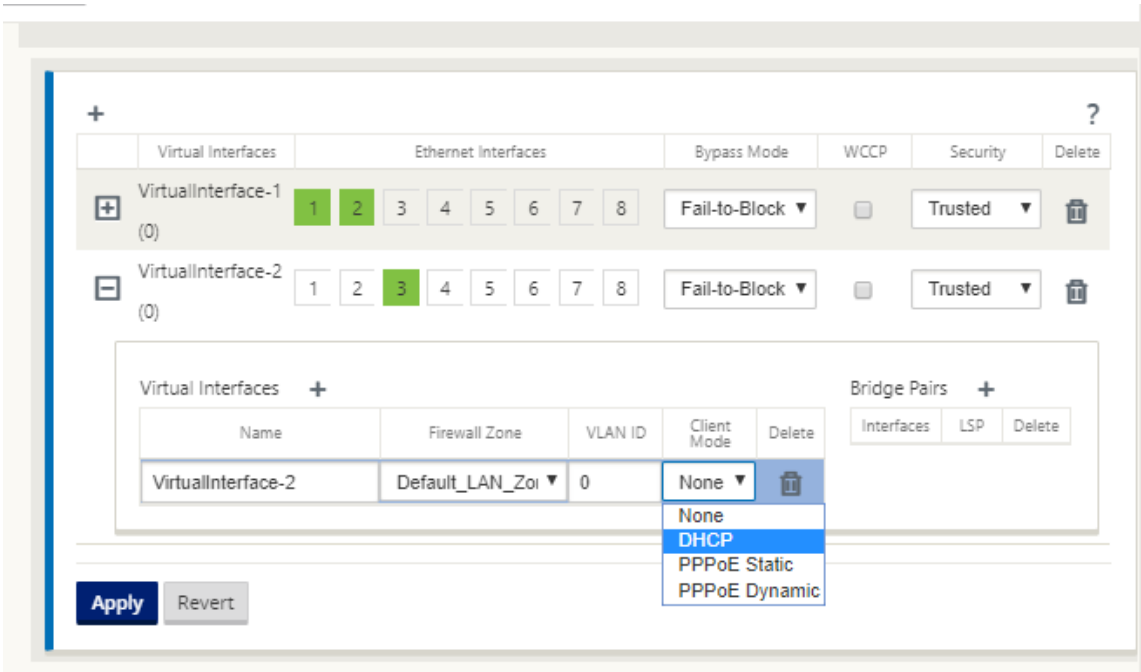
Citrix SD-WAN 设备支持通过 DHCP 客户端进行 WAN 链接 IP 地址学习。此功能减少了部署 SD-WAN 设备所需的手动配置量，并通过无需购买静态 IP 地址来降低 ISP 成本。SD-WAN 装置可以获取不受信任接口上 WAN 链路的动态 IP 地址。这样就不需要中间 WAN 路由器来执行此功能。

> 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。

要在故障到块模式下为不受信任的虚拟接口配置 DHCP，请执行以下操作：

1. 在配置编辑器中，转到站点 > [站点名称] > 接口组 > 虚拟接口。

   > 注意
   >
   > 接口组中的物理接口必须是单个接口上的非桥接对。



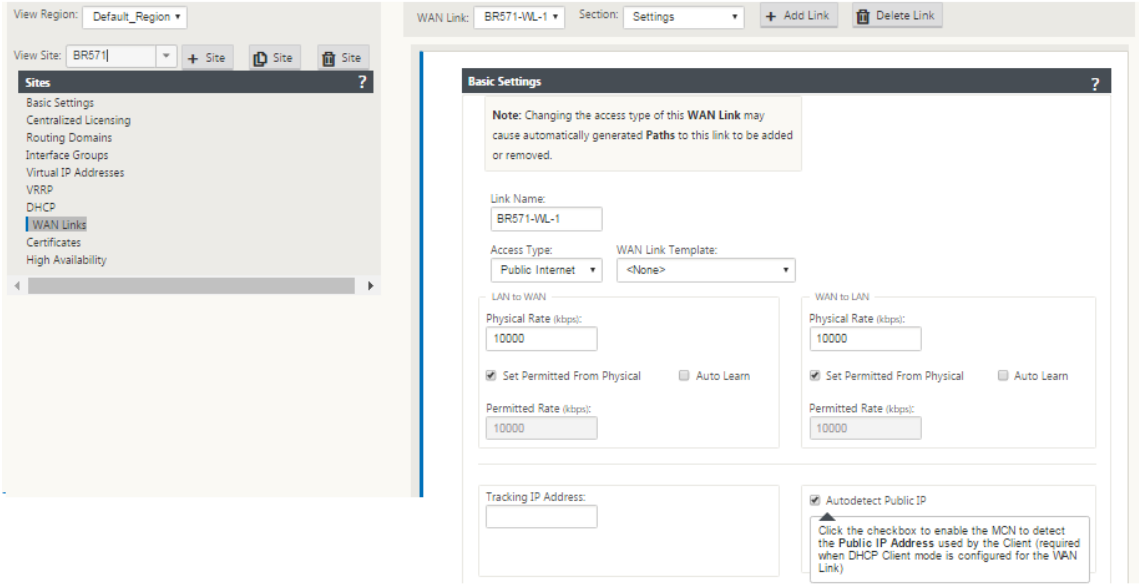
2. 选择以下选项之一作为 客户端模式：

   - 仅限 DHCP IPv4
   - 仅限 DHCP IPv6

- DHCP IPv4 IPv6

如果 SLAAC 和 DHCP IPv6 或 DHCP IPv4 IPv6 都启用，则 DHCPv6 将在无状态模式下运行。

1. 导航到 **Internet** 链接 > **[WAN** 链接名称**]** > 设置 > 基本设置。
2. 单击 自动检测公有 **IP** 复选框以使 MCN 能够检测客户端使用的公有 IP 地址。当为 WAN 链接配置 DHCP 客户端模式时，这是必需的。

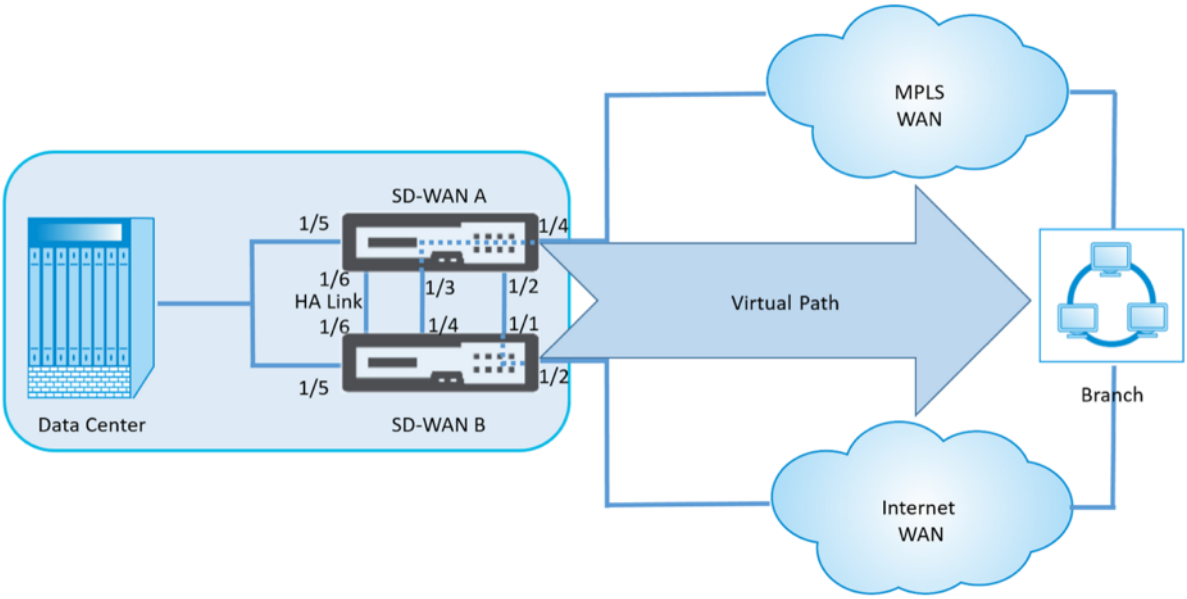


故障到线端口上的 **DHCP** 支持

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：

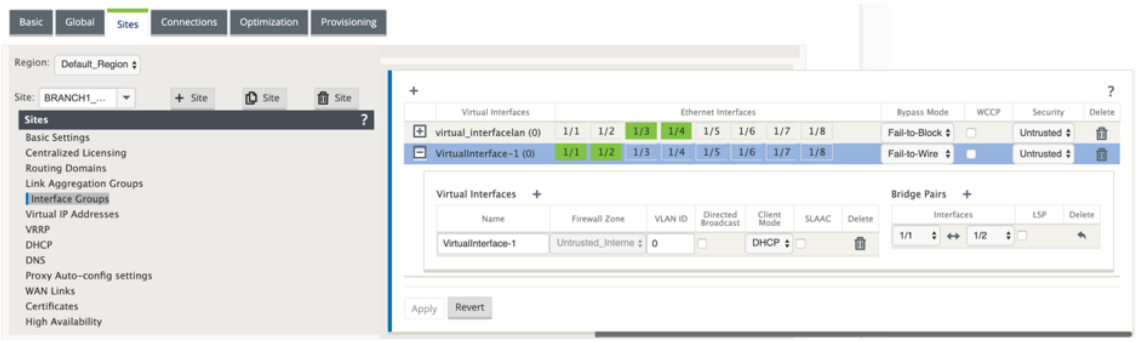
- 允许在具有故障到线网桥对和串行 HA 部署的不受信任接口组上进行 DHCP 客户端配置。
- 允许选择 DHCP 接口作为 专用内联网 **WAN** 链接的一部分。

专用内部网链接现在支持 DHCP 客户端。



要在故障到线模式下为不受信任的虚拟接口配置 DHCP，请执行以下操作：

1. 在配置编辑器中，转到站点 **>** [站点名称] **>** 接口组 **>** 虚拟接口。

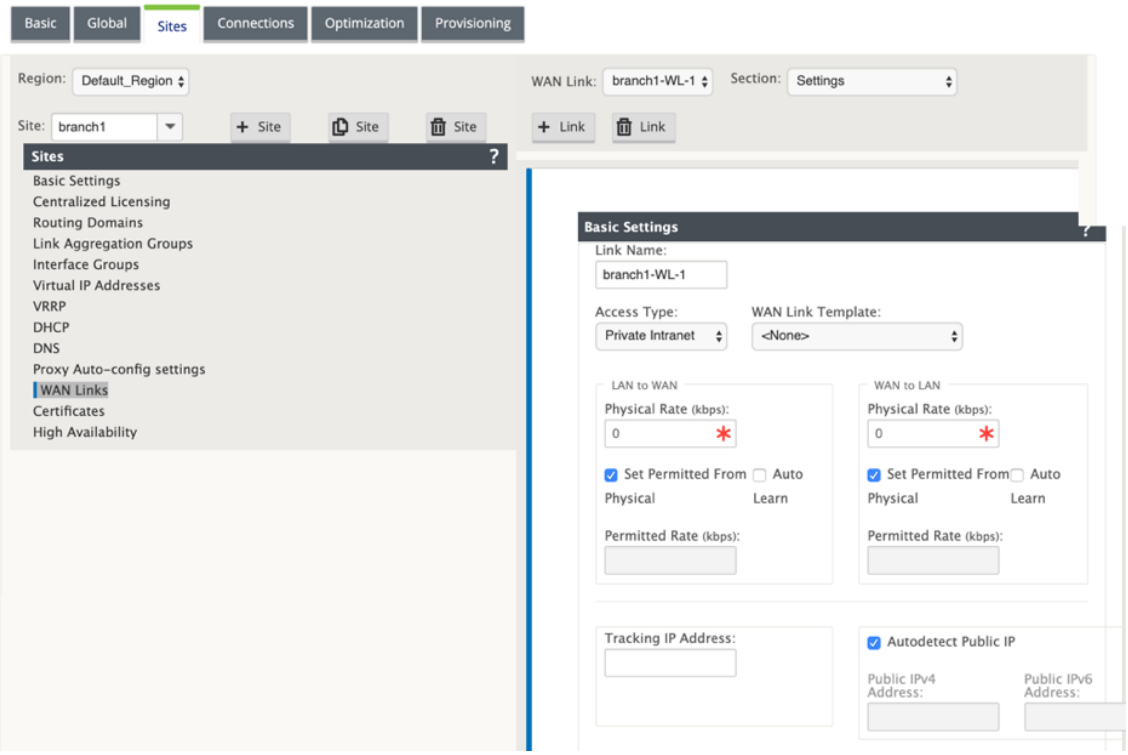


2. 选择以下选项之一作为 客户端模式，然后添加 网桥对：

   - 仅限 DHCP IPv4
   - 仅限 DHCP IPv6
   - DHCP IPv4 IPv6

3. 转到 **WAN** 链接 **>** 单击 **+ >** 从下拉列表中选择 **WAN** 链接名称 > 在区域字 段 中选择 设置 **>** 基本设置。

4. 单击 自动检测公有 **IP** 复选框以使 MCN 能够检测客户端使用的公有 IP 地址。当为 WAN 链接配置 DHCP 客户端模式时，这是必需的。



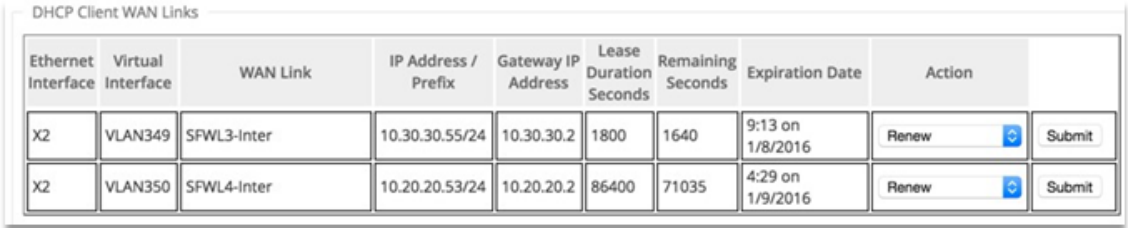
> 注意：
>
> 局域网接口不得连接到故障到线对，因为数据包可能会在接口之间桥接。

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。

```
Feb  4 11:58:30 BR1-Primary dhcpd: Internet Systems Consortium DHCP Server 4.3.2
Feb  4 11:58:30 BR1-Primary dhcpd: Copyright 2004-2015 Internet Systems Consortium.
Feb  4 11:58:30 BR1-Primary dhcpd: All rights reserved.
Feb  4 11:58:30 BR1-Primary dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Feb  4 11:58:30 BR1-Primary dhcpd: Wrote 0 deleted host decls to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: Wrote 0 new dynamic host decls to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: Wrote 1 leases to leases file.
Feb  4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-1/36:d0:d6:52:9f:cc/172.58.3.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Sending on   LPF/vni-1/36:d0:d6:52:9f:cc/172.58.3.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb  4 11:58:30 BR1-Primary dhcpd: Listening on LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Sending on   LPF/vni-0/de:82:2f:9e:4c:3d/172.58.30.0/24
Feb  4 11:58:30 BR1-Primary dhcpd: Server starting service.
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPDISCOVER from 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPOFFER on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPREQUEST for                 from 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: DHCPACK on 172.58.30.151 to 02:63:f0:de:19:3f via vni-0
Feb  4 11:58:31 BR1-Primary dhcpd: Lease time Start : 4 1970/01/01 00:00:00; Lease time end : 4 1970/01/01 00:00:00; for IP :              MAC-Address : 02:63:f0:de:19:3f; Client-id : <none>
```

> 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

June 22, 2021

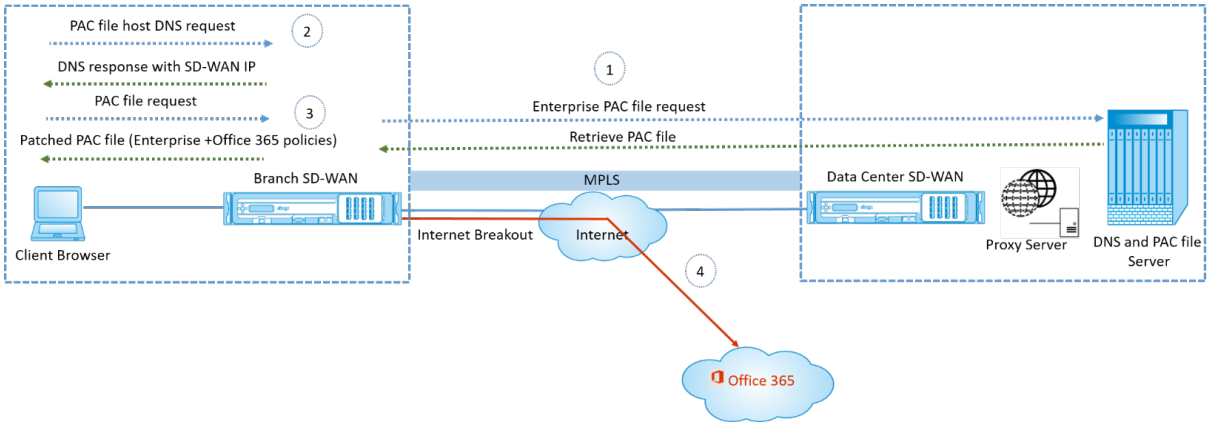
随着企业对任务关键型 SaaS 应用程序和分布式员工的采用率的增加，减少延迟和拥堵变得非常重要。延迟和拥堵是通过数据中心追加流量的传统方法所固有的。Citrix SD-WAN 允许直接互联网突破的 SaaS 应用程序，如 Office 365. 有关详细信息，请参阅Office 365 优化。

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互联网突破。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 设备将执行直接的互联网分组。

必备条件

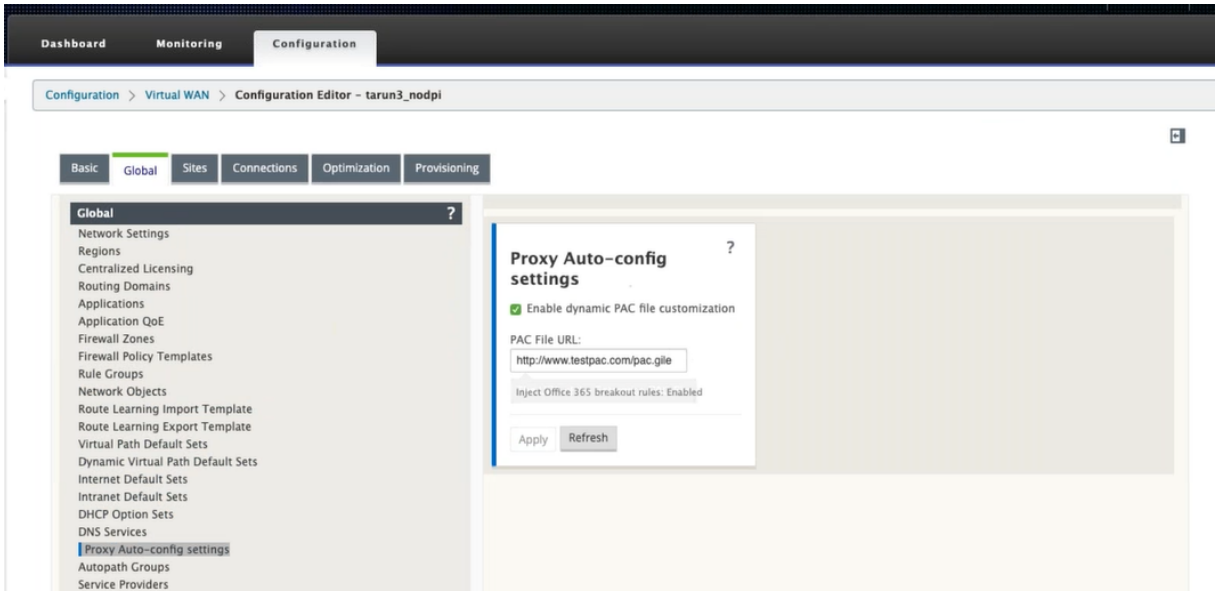
1. 企业应该有一个 PAC 文件托管。
2. PAC 文件应该有一个占位符 *SDWAN_TAG* 或一个出现的 *findproxyforurl* 函数修补 Office 365 网址。
3. PAC 文件 URL 应基于域，而不是基于 IP。
4. PAC 文件仅通过受信任的身份 VIP 提供。
5. Citrix SD-WAN 设备应能够通过其管理界面下载企业 PAC 文件。

配置 **PAC** 文件自定义

您可以在全局或站点级别启用 PAC 文件自定义。

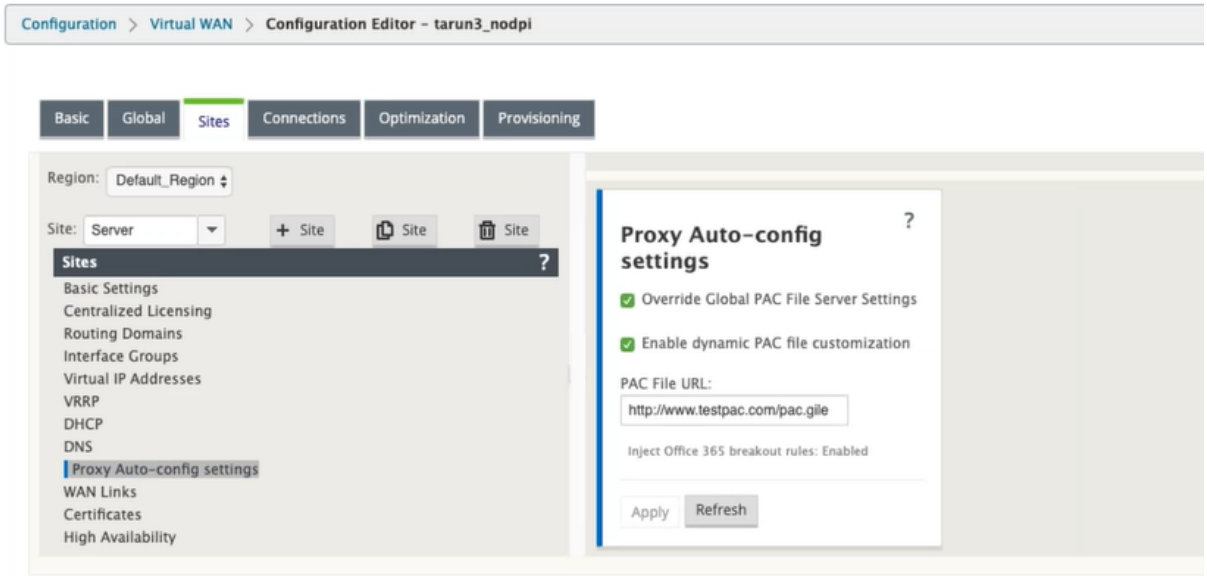
> 注意
>
> 必须为动态 PAC 文件自定义启用 Office 365 分组选项。有关如何启用 Office 365 分组的信息，请参阅Office 365 优化。

要为所有站点全局配置动态 PAC 文件自定义，请在配置编辑器中导航到 全 局 > 代理自动配置 设置。



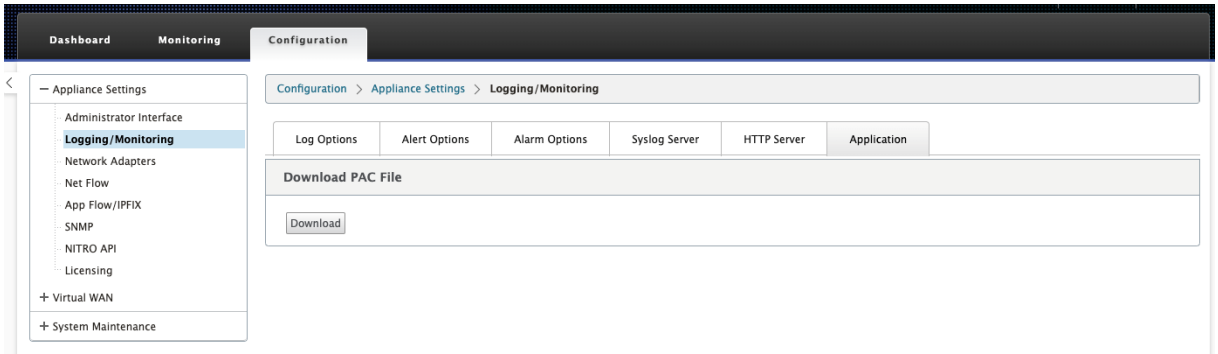
选择 启用动态 **PAC** 文件自定义。在 **PAC** 文件 **URL** 字段中，输入企业 PAC 文件服务器的 URL。Office 365 突破规则动态修补到企业 PAC 文件。

要为站点配置动态 PAC 文件自定义，请导航到 站点 >[站点] > 代理自动配置设置。您还可以选择覆盖全局 PAC 文件服务器设置，并指定不同的 PAC 文件服务器 URL。

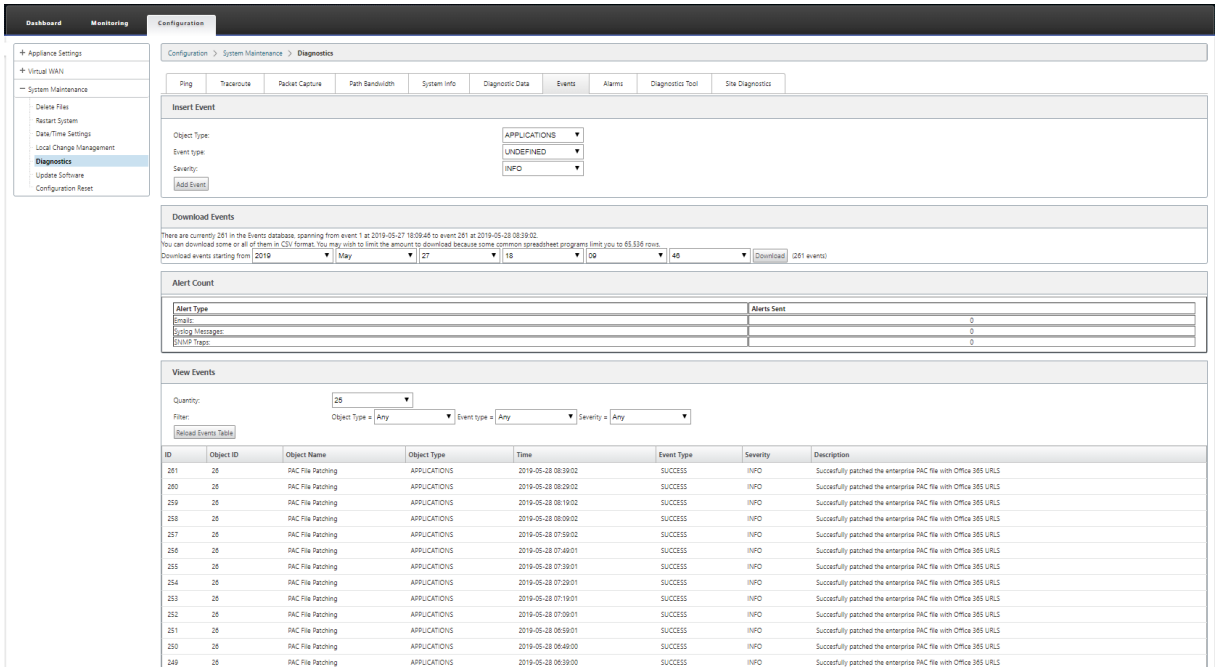


故障排除

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 > 设备设置 > 记录/监视 > 应用程序，然后单击 下载。



您还可以在 事 件 部分查看 PAC 文件修补状态，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 隧道

June 22, 2021

GRE 通道功能允许您配置 Citrix SD-WAN 设备，以终止 LAN 或内部网上的 GRE 通道。如果您不想将站点配置为 GRE 隧道终止节点，您可以跳过此步骤，并继续部分为 MCN 站点配置 WAN 链接。

要配置 GRE 隧道：

继续在新 MCN 站 点 的“站点”视图中，单击 **GRE** 隧道 标签左侧的 **+** 。新站点的 **GRE** 隧道 表打开. 有关详细信息，请参阅 GRE 主题。

配置 GRE 隧道 MCN 站点.

为分支站点配置 GRE 隧道。

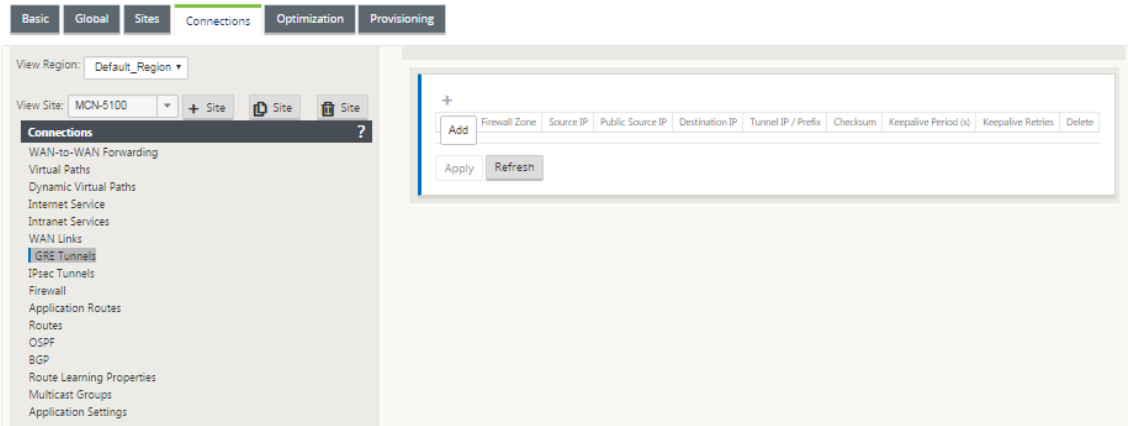
为 **MCN** 站点配置 **GRE** 隧道（可选）

November 1, 2021

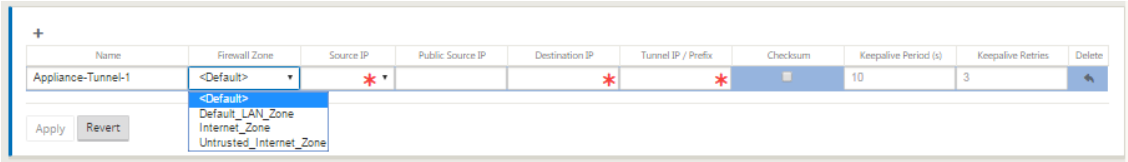
GRE 通道功能允许您将 Citrix SD-WAN 设备配置为终止 LAN 或内部网上的 GRE 通道。如果不想将此站点配置为 GRE 通道终止节点，则可以跳过此步骤，然后转到 为 MCN 站点配置 WAN 链接部分。

要配置 GRE 隧道，请执行以下操作：

1. 继续在新 MCN 站点的连接选项卡中，单击 **GRE** 隧道。这将打开新站点的 **GRE** 隧道 表.



2. 单击 **GRE** 通道右侧的 **+** 。这将向表中添加一个新的空白 GRE 隧道条目，并打开它进行编辑。



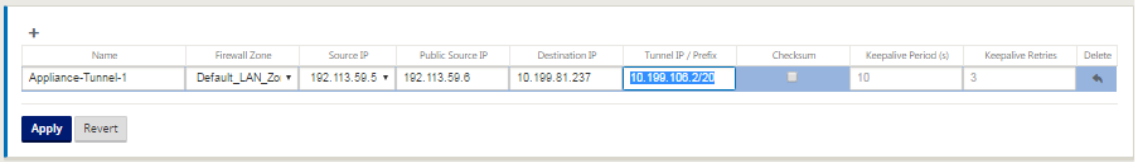
3. 配置 GRE 隧道设置。

   输入以下命令：

   - 服务类型 -从下拉列表中选择内联网或局域网的服务类型。

- 名称：
  - 如果服务类型为 Intranet，请从下拉菜单中的已配置 Intranet 服务列表中进行选择。
  - 如果服务类型为 LAN，请输入新 GRE 通道的名称或接受默认值。
  - 默认使用命名格式 设备隧道- <number> 其中 < numBE r> 是为此站点配置的 GRE 隧道数量，增加 1。
- **Intranet** 服务类型 -对于 Intranet 服务类型，请从下拉列表中选择 默认 或 **zScaler** 。
- 防火墙区域 -为 GRE 隧道选择文件区域。
- 来源 **IP** —从此字段的下拉菜单中选择通道的源 IP 地址。菜单选项是为此站点配置的虚拟接口列表。在配置 GRE 隧道之前，请至少配置一个虚拟接口。有关说明，请参阅为 MCN 站点配置虚拟接口组和为 MCN 站点配置虚拟 IP 地址。
  - 公共源 **IP**：输入要用作 GRE 通道中数据包的源地址的 IP 地址。源 IP 地址是 GRE 通道的起点。
  - 目标 **IP** —输入要用作主机目标的 IP 地址。目标 IP 地址是 GRE 通道的终点。
  - 通道 **IP** /前缀—输入用于 GRE 通道接口的 IP 地址和前缀。
  - 校验和—选中 校验 和框可为隧道 GRE 报头启用校验和。
  - 保持活动时间—输入保持活动消息之间的等待时间间隔（以秒为单位）。如果配置为 0，则不会发送 keepalive 数据包，但隧道保持启动 状态。默认值为 10。
  - **Keepalive** 重试—输入 Virtual WAN 设备在关闭隧道之前必须尝试的 keepalive 重试次数。默认值为 3。

4. 单击应用。这将提交您的设置，并将新 GRE 隧道添加到表中。



5. 要配置更多 GRE 通道，请单击 **GRE** 通道 右侧的 **+**，然后按照上述步骤进行操作。

下一步是为 MCN 站点配置 WAN 链接。

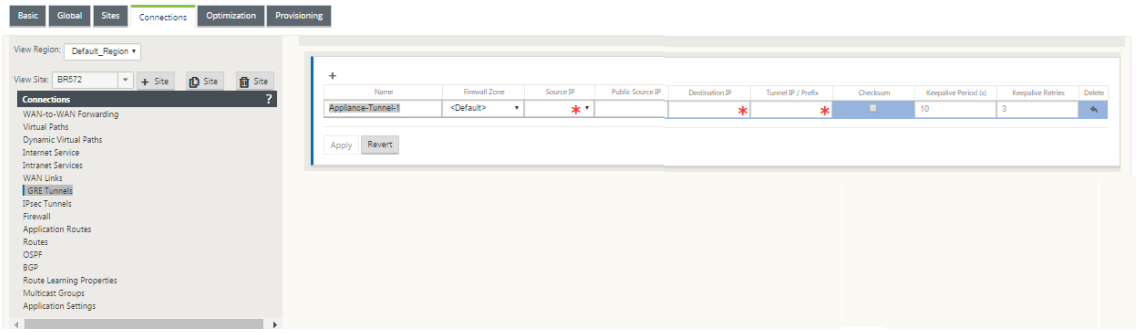
为分支站点配置 GRE 隧道

November 1, 2021

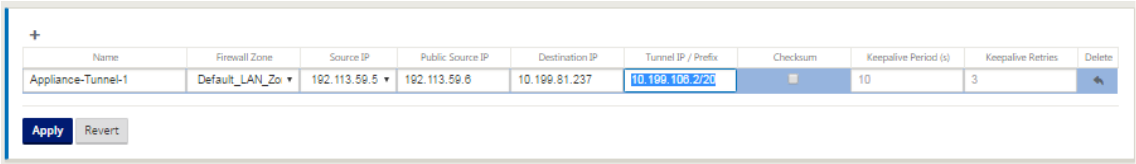
GRE 通道功能允许您配置 Citrix SD-WAN 设备，以终止 LAN 或内部网上的 GRE 通道。如果不想将此分支站点配置为 LAN GRE 通道终止节点，则可以跳过此步骤，然后转到 为分支站点配置 WAN 链接一节。

要为分支站点配置 LAN GRE 隧道：

1. 继续在新分支站点的连接视图中，单击 **GRE** 隧道。将打开新站点的 **GRE** 隧道 视图。
2. 单击 **GRE** 通道右侧的 **+**。这将向表中添加一个新的空白 GRE 隧道条目，并打开它进行编辑。



3. 配置 GRE 隧道设置。输入以下命令：
   - 服务类型 -从下拉列表中选择内联网或局域网的服务类型。
   - 名称：
     - 如果服务类型为 Intranet，请从下拉菜单中的已配置 Intranet 服务列表中进行选择。
     - 如果服务类型为 LAN，请输入新 GRE 通道的名称或接受默认值。
     - 默认使用命名格式 设备隧道**-** <number> 其中 < numBE r> 是为此站点配置的 GRE 隧道数量，增加 1。
   - **Intranet** 服务类型 -对于 Intranet 服务类型，请从下拉列表中选择 默认 或 **zScaler** 。
   - 防火墙区域 -为 GRE 隧道选择防火墙区域。
   - 来源 **IP** —从此字段的下拉菜单中选择通道的源 IP 地址。菜单选项是您为此站点配置的虚拟 IP 地址列表。配置至少一个虚拟接口和一个虚拟 IP 地址，然后才能配置 LAN GRE 隧道。有关说明，请参阅为分支站点配置虚拟接口组和配置分支站点的虚拟 IP 地址部分。
   - 公共源 **IP** -输入要用作 GRE 通道中数据包的源地址的 IP 地址。源 IP 地址是 GRE 通道的起点。
   - 目标 **IP** —输入要用作主机目标的 IP 地址。目标 IP 地址是 GRE 通道的终点。
   - 通道 **IP /**前缀—输入用于 GRE 通道接口的 IP 地址和前缀。
   - 校验和—选中 校验 和框可为隧道 GRE 报头启用校验和。
   - 保持活动时间—输入保持活动消息之间的等待时间间隔（以秒为单位）。如果配置为 0，则不会发送 keepalive 数据包，但隧道保持启动 状态。默认值为 10。
   - **Keepalive** 重试—输入 Virtual WAN 设备在关闭隧道之前必须尝试的 keepalive 重试次数。默认值为 3。
4. 单击应用。这将提交您的设置，并将新 GRE 隧道条目添加到表中。



5. 要配置更多 GRE 通道，请单击 **GRE** 通道 标签右侧的 **+**，然后按照上述步骤进行操作。

下一步是为 分支站点配置 WAN 链接。

带内和备份管理

February 10, 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。

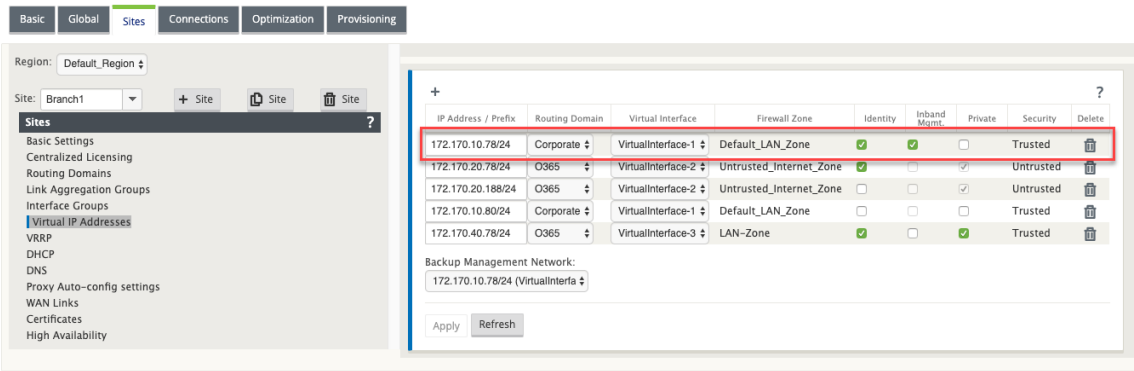
从 Citrix SD-WAN 11.4.2 版本起，必须在 SD-WAN 设备上配置带内管理，才能通过带内管理端口建立与 Citrix SD-WAN Orchestrator 服务的连接。否则，当管理端口未连接且未配置带内 IP 地址时，设备将失去与 Citrix SD-WAN Orchestrator 服务的连接。

> 注意
>
> - Citrix SD-WAN Center 不支持通过带内管理连接到高可用性设备。
> - 只能使用 MCN 配置编辑器将 服务类型 配置为 任意。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。

要在虚拟 IP 上启用带内管理，请执行以下操作：

1. 在配置编辑器中，导航到 站点 > 虚拟 **IP** 地址。
2. 为要启 用带内管 理的虚拟 IP 选择带内管理。

> 注意：
>
> 确保接口安全类型为 受信任 且 身份 已启用。



3. 单击 应用

有关配置虚拟 IP 地址的详细过程，请参阅 如何配置虚拟 IP。

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：

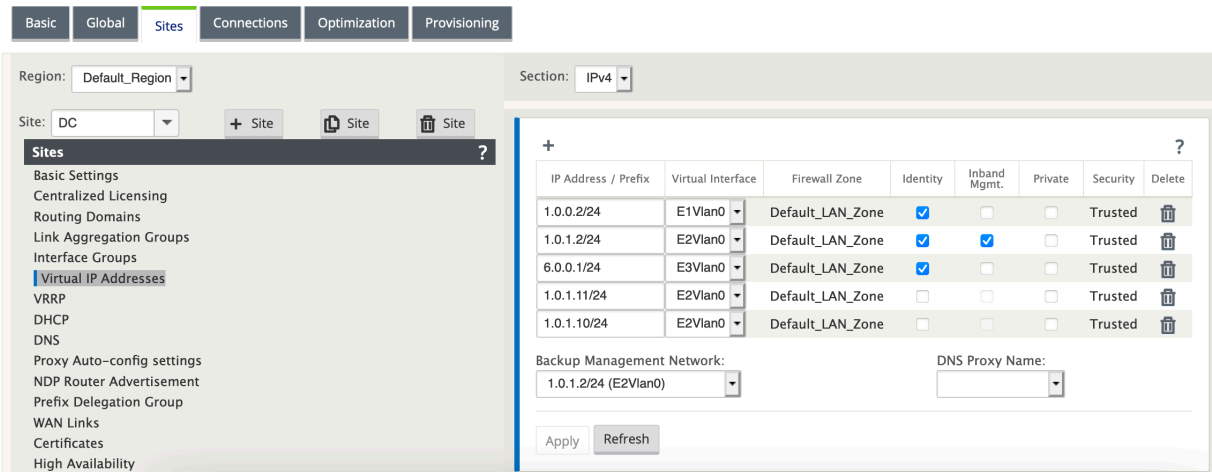
- HTTPS
  - 443-连接到活跃的 HA
  - 444-重定向到 HA 主
  - 445-重定向到医管局中学
- SSH
  - 22-连接到 HA 活动
  - 23-重定向到医管局主
  - 24-重定向到医管局二级
- SNMP
  - 161-连接到活动的 HA
  - 162-重定向到医管局主
  - 163-重定向到医管局辅助

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。

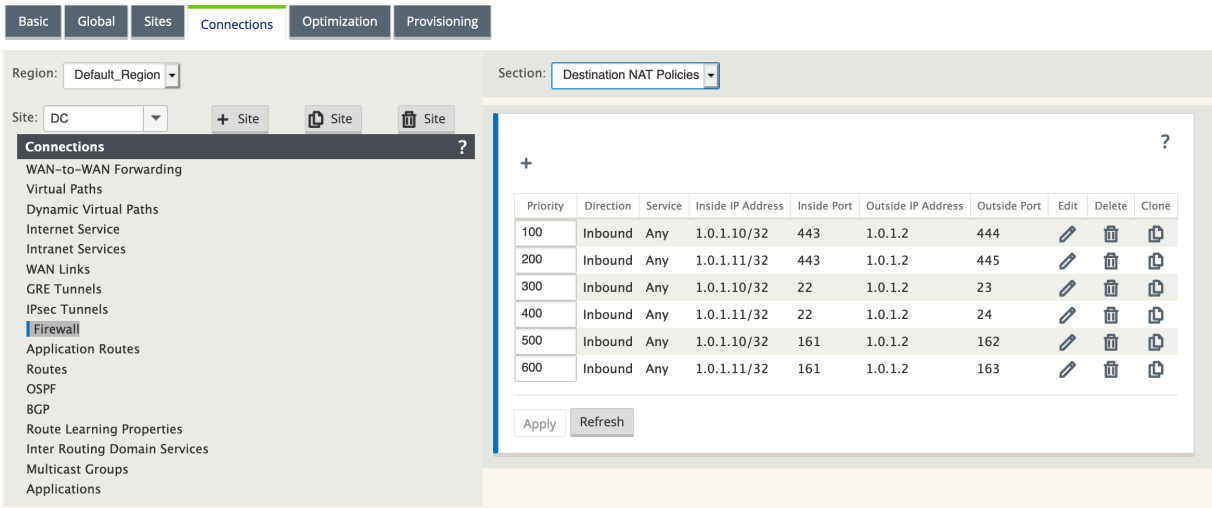
例如，以下带内 IP 地址用于访问设备：

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

创建两个与带内管理虚拟 IP 地址位于同一网络中的新虚拟 IP 地址的虚拟 IP 地址。在此示例中，1.0.1.2/24 是带内管理虚拟 IP 地址，1.0.1.2/24 选择作为备份网络。1.0.1.10 和 1.0.1.11 是创建的新虚拟 IP 地址。1.0.1.10 用于访问主设备，1.0.1.11 用于访问辅助设备。



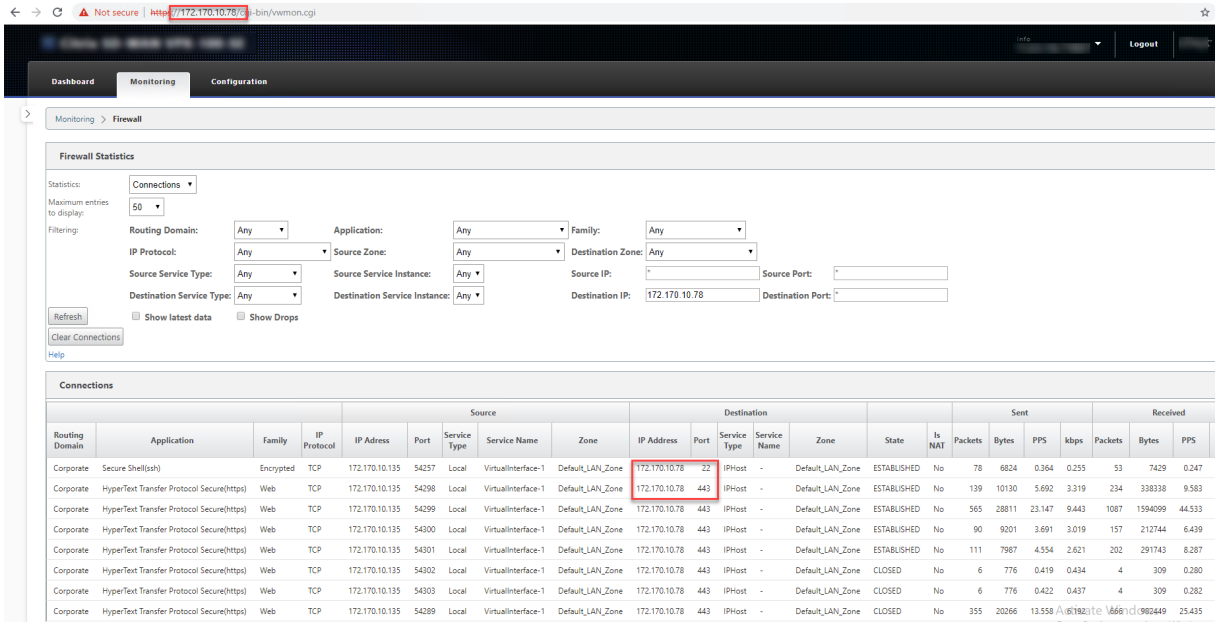
创建目标 NAT 策略。六个 DNAT 策略将服务的基本端口重定向到适当的带内 HA 端口。应用配置后，您可以使用内部 IP 地址直接访问主设备和辅助设备。



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。



> 注意
>
> 以下 SD-WAN 设备不支持带内管理：
>
> - Citrix SD-WAN 1000 SE /PE
> - Citrix SD-WAN 2000 SE /PE
> - Citrix SD-WAN 4000 SE

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互联网进行 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。有关通过 SD-WAN Center 进行零接触部署的信息，请参阅 零接触部署。有关通过 SD-WAN Orchestrator 进行零接触部署的信息，请参阅 零接触部署。

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。

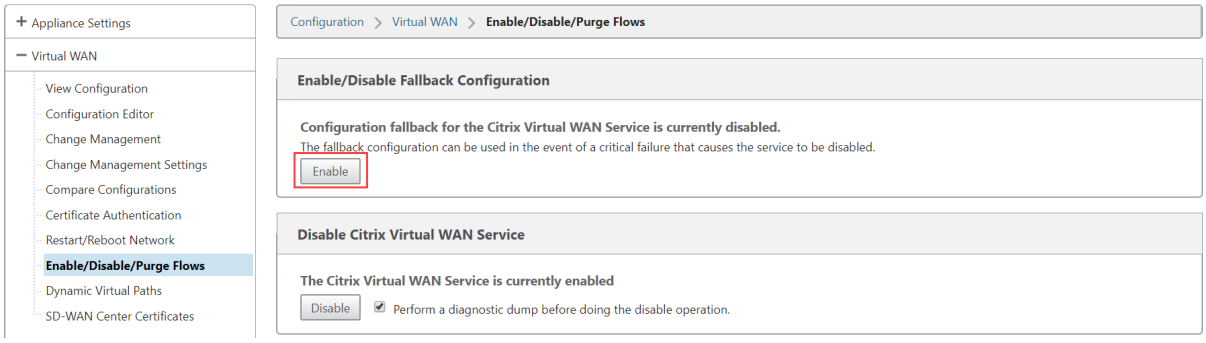
置备设备后，默认配置将被禁用，并由零接触部署服务接收的配置覆盖。如果设备许可证或宽限许可证过期，则会激活默认配置，以确保设备保持连接到零接触部署服务并接收通过零接触部署管理的许可证。

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。

如果已禁用回退配置，则可以通过导航到“配置”> “装置 设置”> “默认/备用配置”> 单击“启用”来启用它。



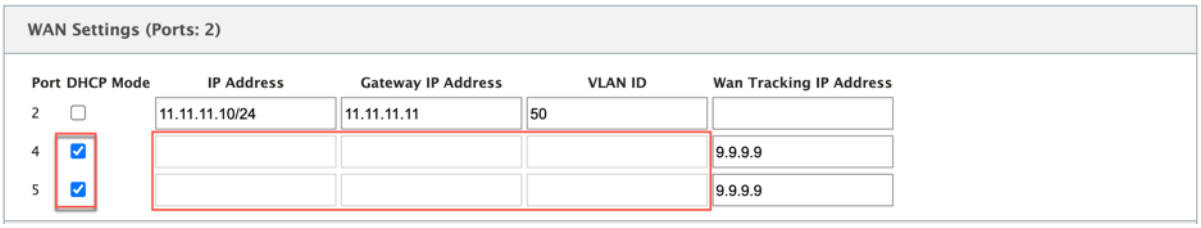
下表提供了在不同平台上用于备用配置的预先指定 WAN 和 LAN 端口的详细信息：

平台	WAN 端口	LAN 端口
110	1/2	1/1
110-LTE	1/2，LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4、1/5、LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
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。

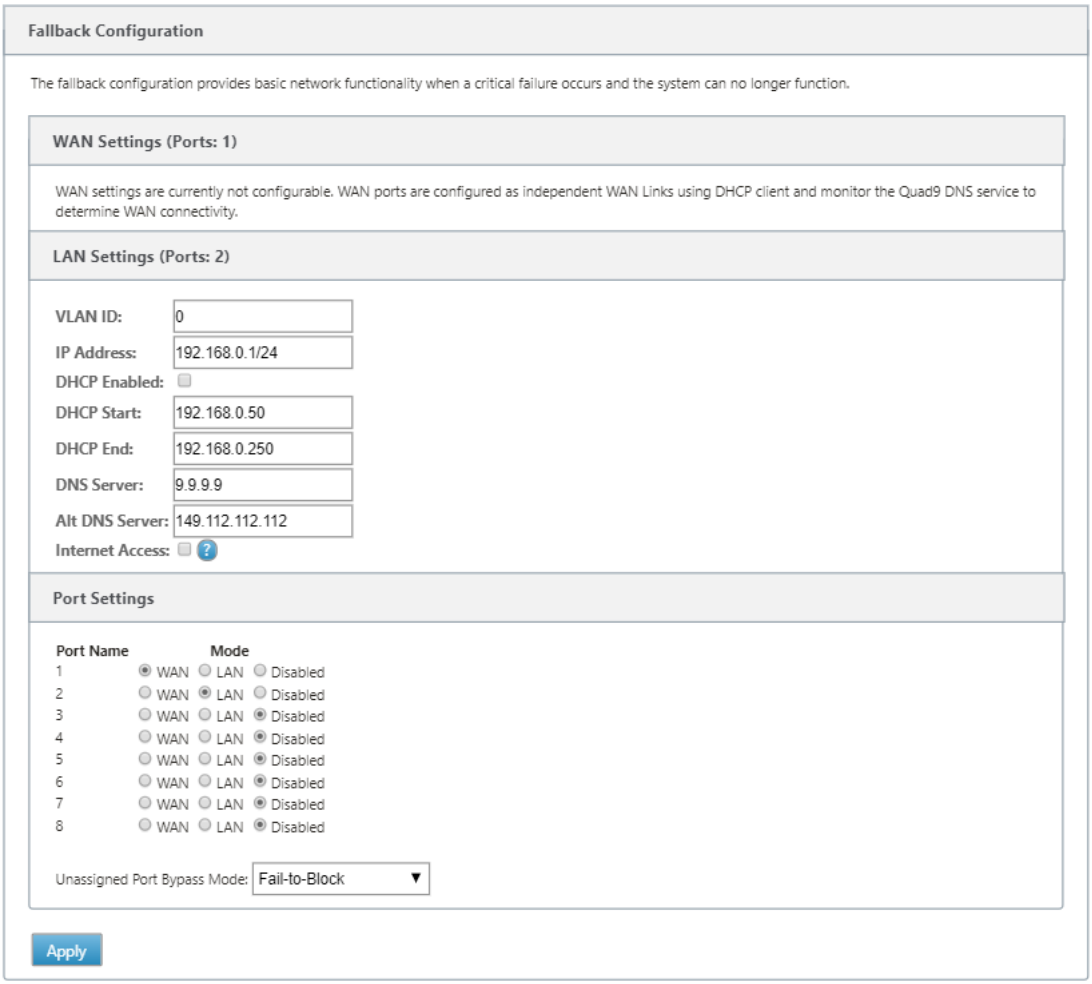


默认情况下，**WAN** 跟踪 **IP** 地址字段将自动填充 9.9.9.9。您可以根据需要更改地址。

> 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。

要根据 LAN 网络自定义备用配置，请执行以下操作：

1. 导航到 配置 > 装置设 置 > 默认/备用配置。
2. 根据您的网络要求编辑以下 LAN 设置的值。这是与零接触部署服务建立连接所需的最低配置。
    - **VLAN ID**：局域网端口必须分组到的 VLAN ID。
    - **IP** 地址：分配给 LAN 端口的虚拟 IP 地址。
    - **DHCP** 启用：将局域网端口启用为 DHCP 服务器。DHCP 服务器为 LAN 端口上的客户端分配动态 IP 地址。
    - **DHCP** 开始和 **DHCP End**：DHCP 用来向 LAN 端口上的客户端动态分配 IP 的 IP 地址范围。
    - **DNS** 服务器：主 DNS 服务器的 IP 地址。
    - **Alt DNS** 服务器：辅助 DNS 服务器的 IP 地址。
    - 互联网访问：允许所有 LAN 客户端访问互联网，无需其他过滤。



3. 为每个端口配置模式。端口可以是 LAN 端口或 WAN 端口，也可以禁用。显示的端口取决于设备型号。此外，将端口旁路模式设置为“故障到阻止”或“故障到线”。

要随时将回退配置重置为默认配置，请单击 重置。

> 注意
>
> 以下 SD-WAN 设备不支持回退配置：
>
> - Citrix SD-WAN 1000 SE /PE
> - Citrix SD-WAN 2000 SE /PE
> - Citrix SD-WAN 4000 SE

可配置的管理或数据端口

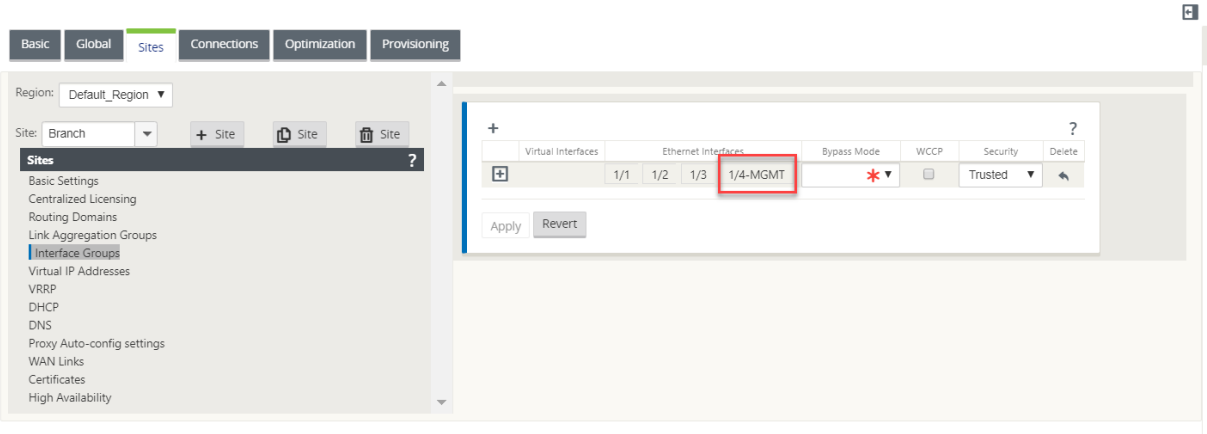
带内管理允许数据端口同时传输数据和管理流量，无需使用专用管理端口。这使得管理端口在已经具有较低端口密度的低端设备上未使用。Citrix SD-WAN 允许您将管理端口配置为作为数据端口或管理端口运行。

> 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

在配置编辑器上，使用配置中的管理端口。激活配置后，管理端口将转换为数据端口。

> 注意
>
> 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。

要配置管理界面，请在配置编辑器中导航到 站点，选择一个站点，然后单击 界面组。MGMT 接口可供配置。有关配置接口组的详细信息，请参阅 如何配置接口组。



要重新配置管理端口以执行管理功能，请删除配置。在不使用管理端口的情况下创建配置并将其激活。

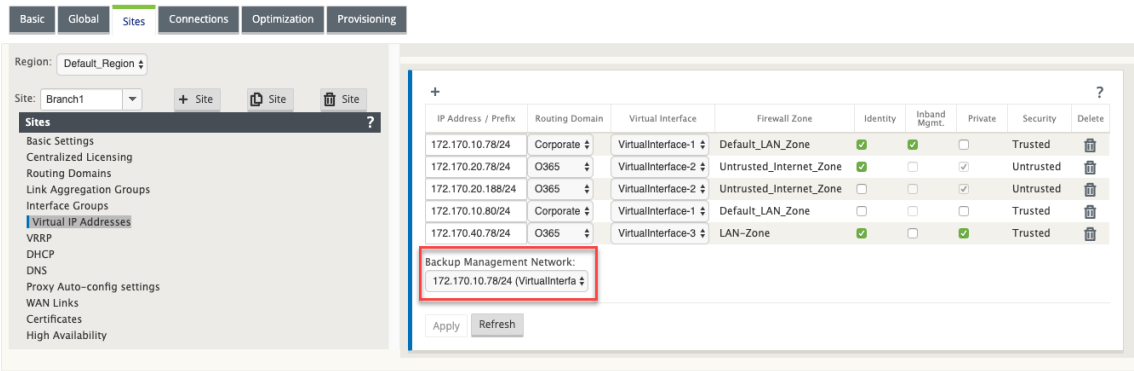
备份管理网络

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。

要选择虚拟 IP 作为备份管理网络，请执行以下操作：

1. 在配置编辑器中，导航到 站点 > 虚拟 **IP** 地址。
2. 选择虚拟 IP 地址作为备份管理网络。



3. 选择带内和备份管理平面 上的所有 DNS 请求都将转发到的 DNS 代理。

> 注意
>
> 只有在为虚拟 IP 启用带内管理和备份管理网络时，才能选择 DNS 代理。

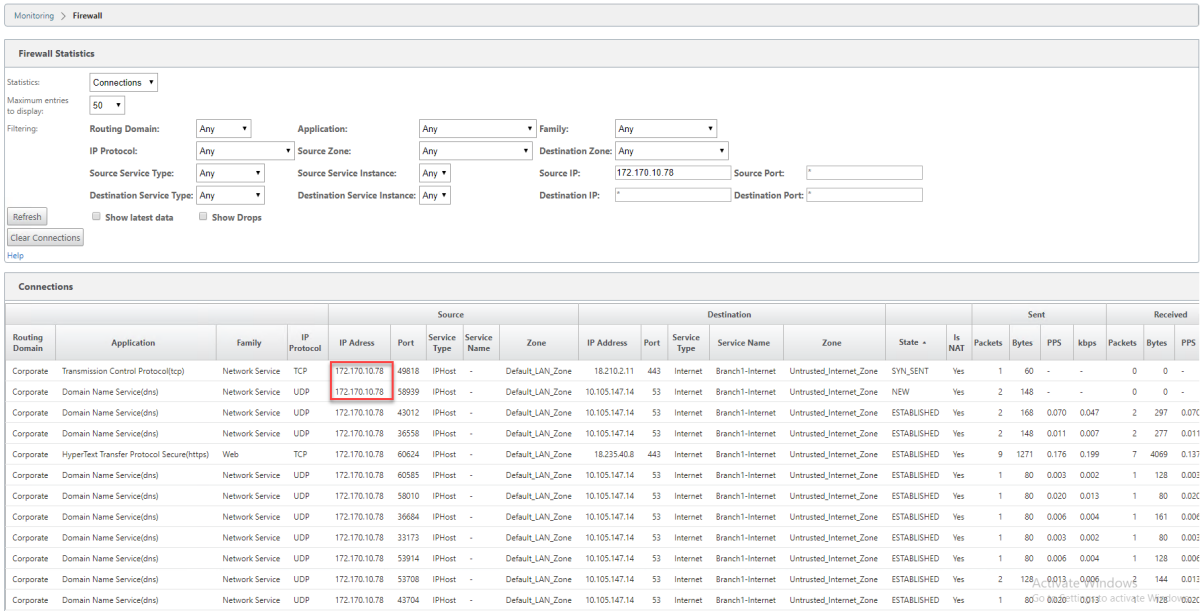
4. 单击应用。

有关配置虚拟 IP 地址的详细过程，请参阅 如何配置虚拟 IP 地址

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。



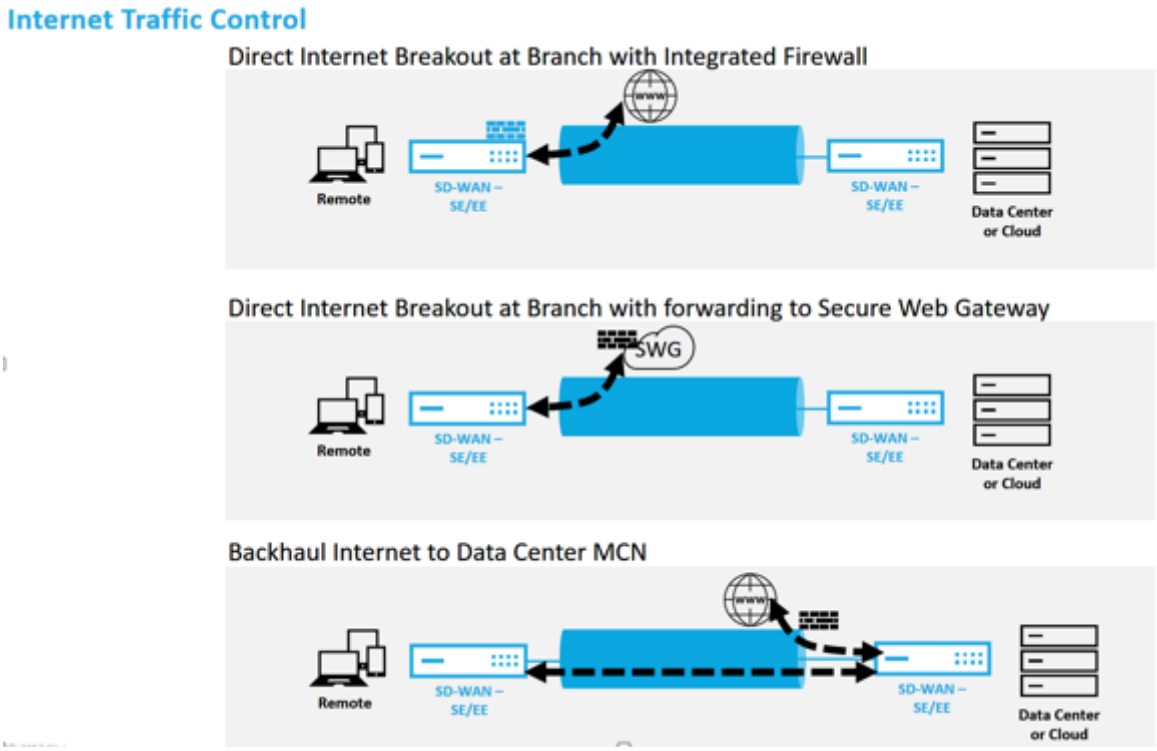
Internet 访问权限

June 22, 2021

互联网服务用于最终用户网站与公共互联网上的网站之间的通信。Internet 服务流量不被 SD-WAN 封装，并且不具有与通过虚拟路径服务传输的流量相同的功能。但是，在 SD-WAN 上对此流量进行分类和考虑是非常重要的。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互联网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 Provisioning 功能外，SD-WAN 还具有使用多个 Internet WAN 链接或可选择使用主配置或辅助配置中的 Internet WAN 链接通过 Internet 服务传输的流量负载平衡功能。

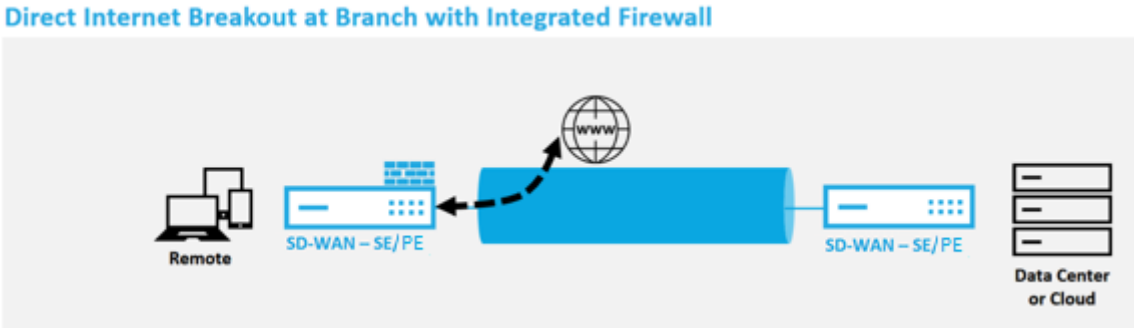
可以在以下部署模式下配置使用 SD-WAN 设备上 Internet 服务的 Internet 流量控制：

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



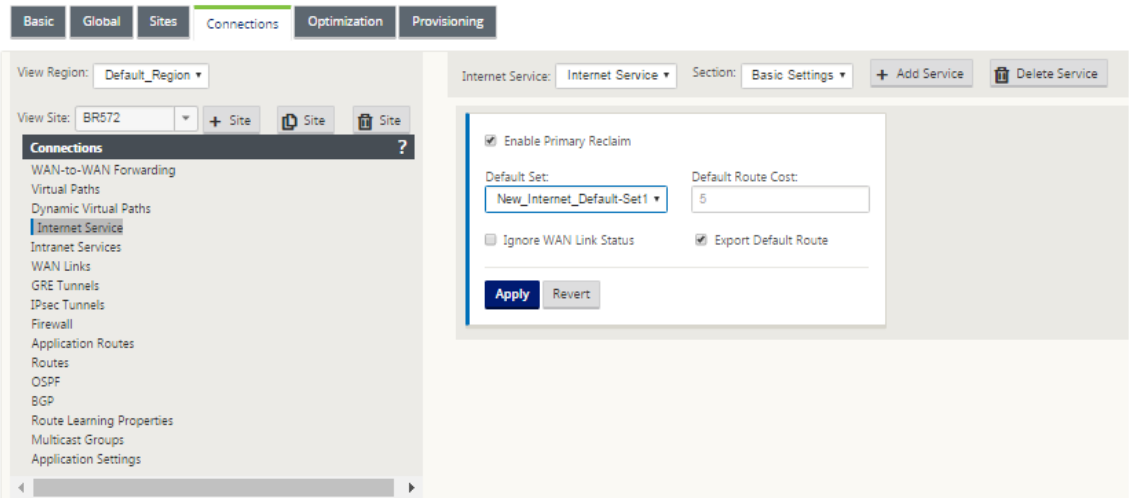
带集成防火墙的分支机构直接互联网突破

June 22, 2021

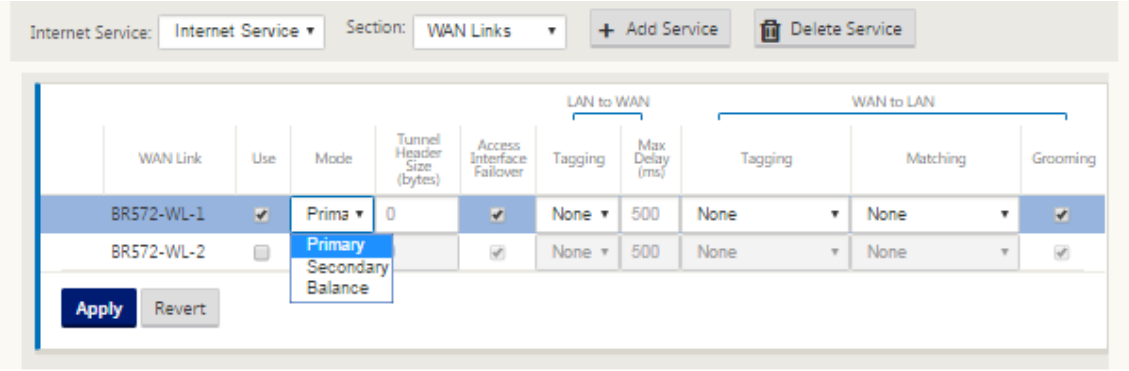


执行以下步骤，为任何站点（客户端节点或 MCN）启用 Internet 服务：

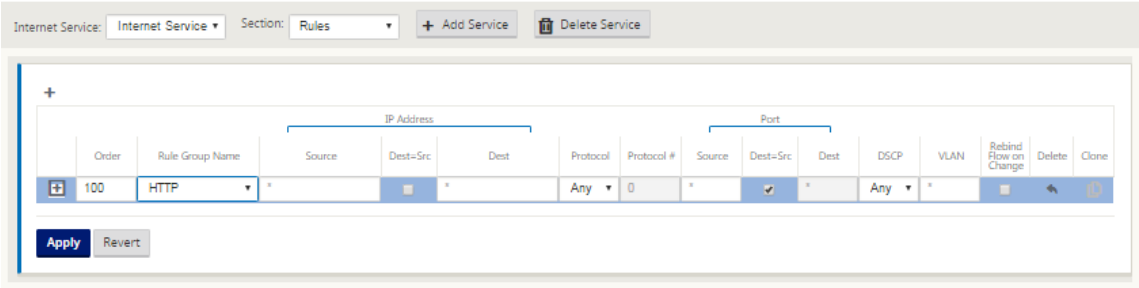
1. 在 配置编辑器中，导航到 连接磁贴。单击添加 (+) 图标以为该网站添加 Internet 服务。每个站点只能创建一个互联网服务。
2. 在 Internet 服务的 基本设置 中，有关于您希望 Internet 服务在 WAN 链接不可用期间的行为方式的几个选项。可以在全局磁贴中定义 Internet 默认集，其中包含一组规则，这些规则可应用于配置中启用了 Internet Service 的 任何节点，从而可以集中控制 Internet Service 管理，而无需单独配置每个节点。



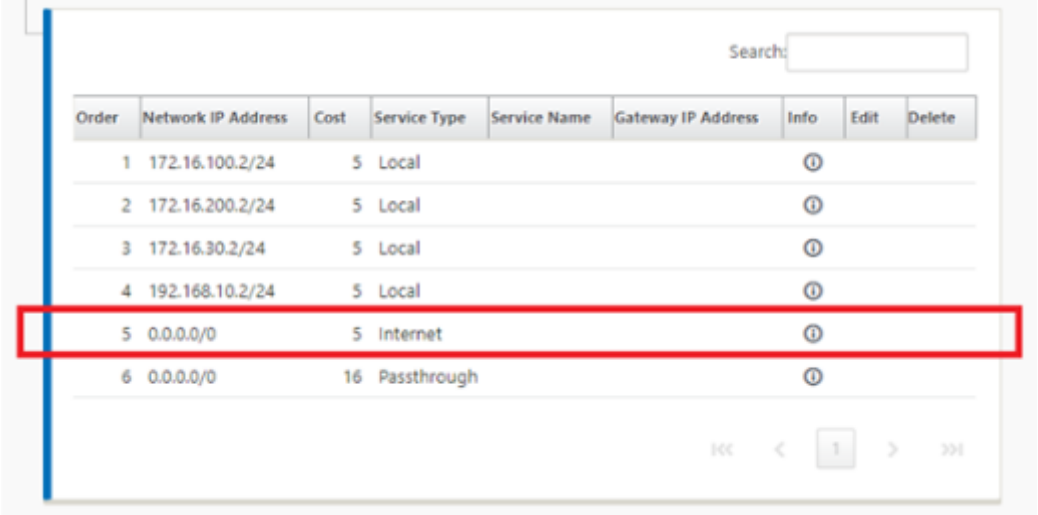
3. 在 Internet 服务 WAN 链接节点中，网站磁贴中构建的 WAN 链接可用于选择要用于 Internet 流量的 WAN 链接。除了其他选项之外，可用模式还包括主模式、辅助模式和平衡模式，允许管理员同时或以主动/被动角色使用可用的 WAN 链接。



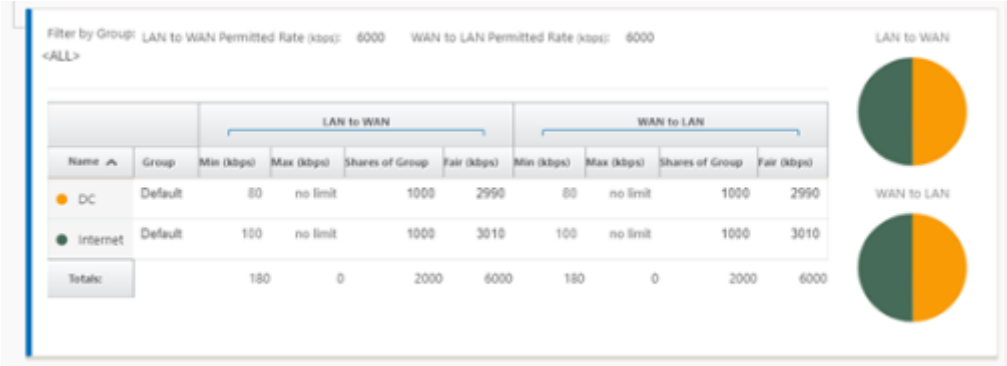
4. 提供了特定于站点节点的规则，使每个站点能够独特地覆盖在全局默认集中配置的任何常规设置。模式包括通过特定 WAN 链接进行所需的传输，或作为覆盖服务，允许直通或丢弃过滤的流量。



为节点创建 Internet 服务时，该特定节点的路由表将自动更新为 0.0.0.0/0 路由（对于等于 Internet 的服务类型和路由成本为 5），否则将颁布以直通作为服务类型的成本为 16 的默认路由，并且 Internet 流量将被交给底层网络进行路由。



在为站点节点启用 Internet 服务后，Provisioning 磁贴可用于允许在使用 WAN 链接的各种服务之间为 WAN 链接进行双向（LAN 到 WAN/WAN 到 LAN）分配带宽。服务 部分允许用户进一步微调带宽分配。此外，可以启用公平分享，允许所有服务在实施公平分配之前获得其最低保留带宽。



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 保护网络免受直接互联网连接。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。

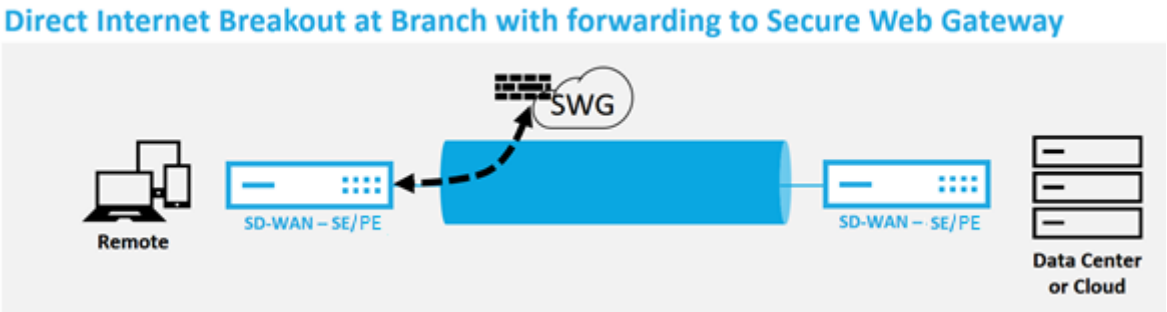
通过 **Secure Web Gateway** 直接访问互联网

November 1, 2021

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。



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

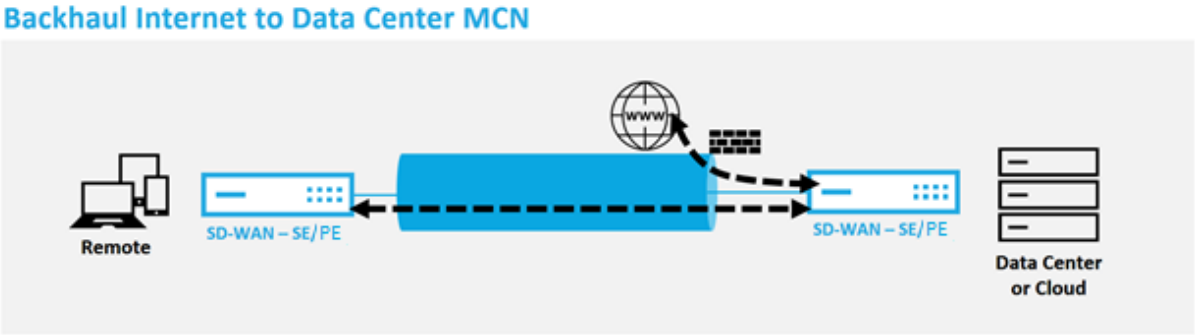
- Zscaler
- Forcepoint
- Palo Alto
- Citrix Secure Internet Access

回程互联网

June 22, 2021

Citrix SD-WAN 解决方案可以将互联网流量回传到 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 回传所有远程站点互联网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。

- 互联网流量的回传增加了互联网连接的延迟，并且根据数据中心分支站点的距离而变化。
- 互联网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。
- 互联网流量的回程可能会超额订阅数据中心的 Internet WAN 链接。



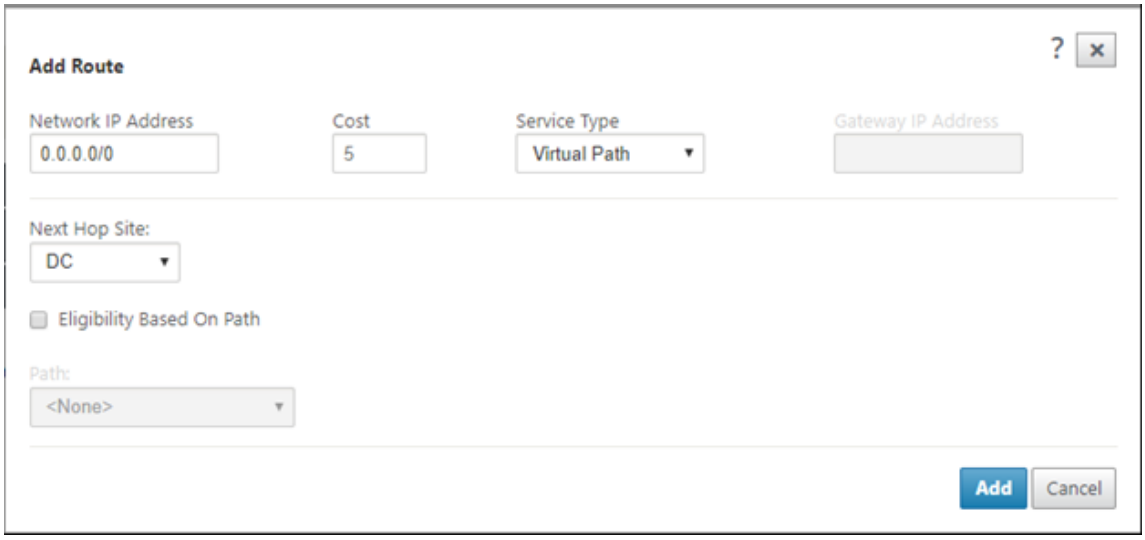
所有 Citrix SD-WAN 设备最多可以将八个不同的 Internet WAN 链接终止到单个设备中。聚合 WAN 链路的许可吞吐能力在 Citrix SD-WAN 数据手册中按相应设备列出。

Citrix SD-WAN 解决方案通过以下配置支持互联网流量的回传。

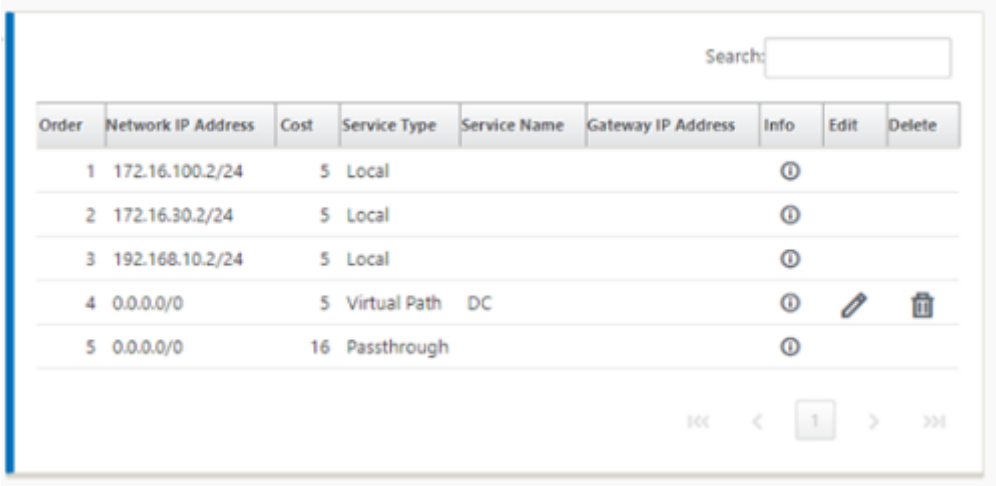
1. 在 MCN 站点节点或任何需要 Internet 服务的其他站点备注中启用 Internet 服务。

   > 注意
   >
   > 如果所有其他站点都位于 WAN 到 WAN 转发组中，则启用 Internet 服务和导出路由。

2. 在回传 Internet 流量的分支节点上，手动添加 0.0.0.0/0 路由，以将所有默认流量定向到虚拟路径服务。下一跳表示为 MCN 或中间站点。



3. 验证分支站点的路由表是否没有任何其他成本较低的路由，这些路由除了所需的回传路由之外，可以引导流量。

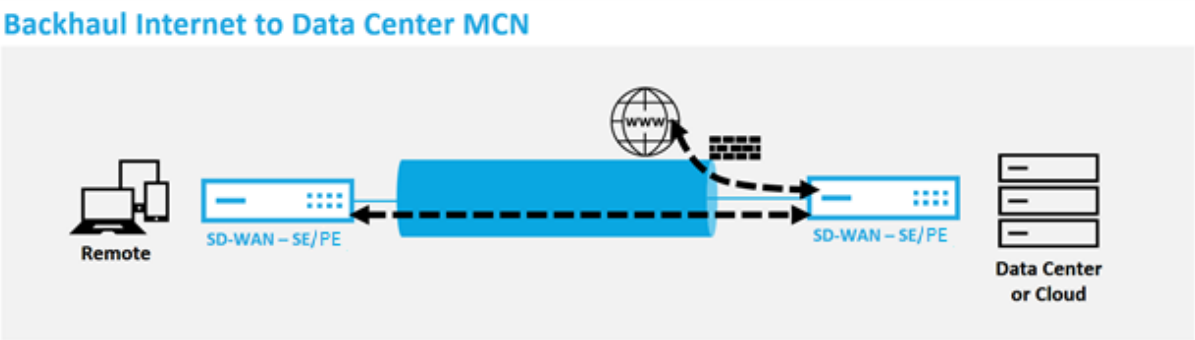


发夹模式

June 22, 2021

借助发夹部署，当本地互联网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互联网访问。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互联网访问，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 具有可用的互联网服务，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。

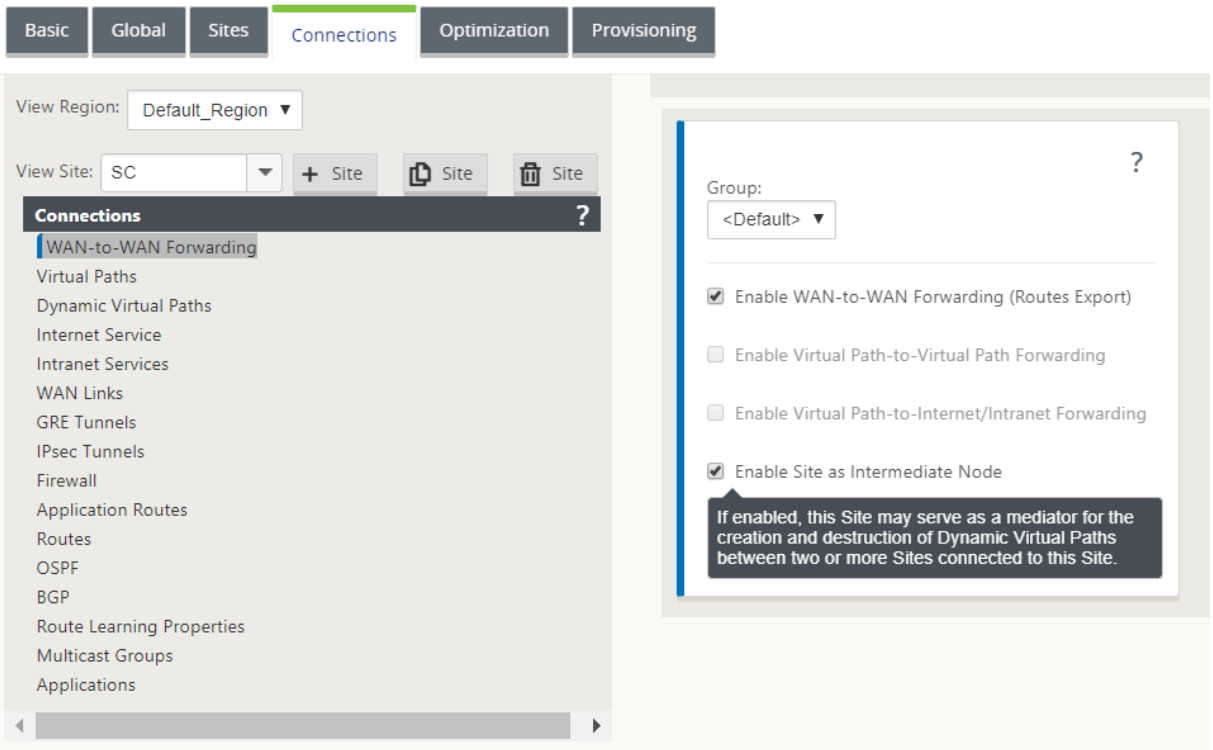
Wa 到 WAN 转发和发夹部署有一定的区别，即：

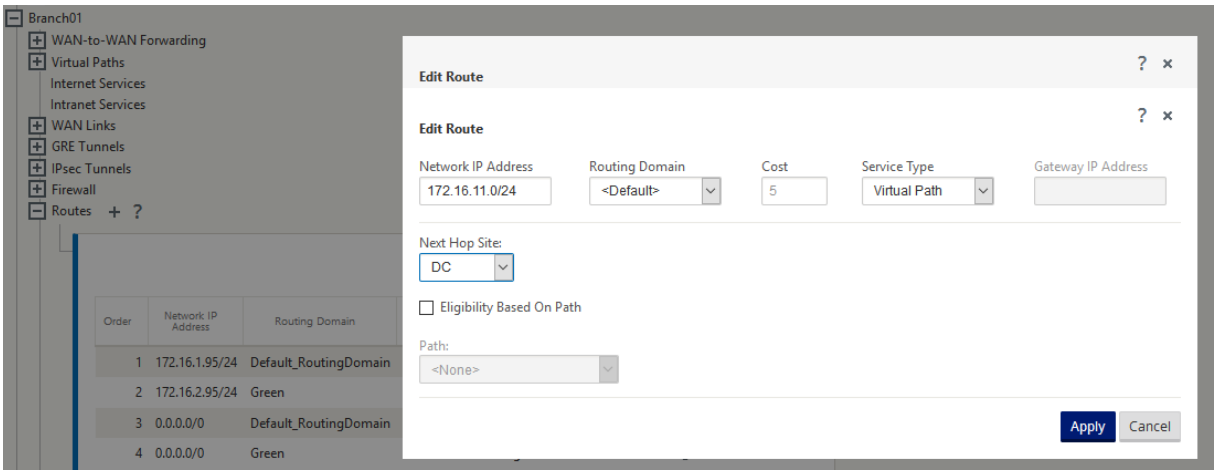
1. 未配置动态虚拟路径。中间站点始终会看到两个站点之间的所有流量。
2. 尚未加入 WAN 到 WAN 转发组。

   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/PE 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。

您可以通过配置编辑器中的 Citrix SD-WAN Web 管理界面配置发夹部署。





托管防火墙

June 22, 2021

目前，Citrix SD-WAN 支持以下托管的防火墙：

- 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

June 22, 2021

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** 模式中，并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。

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
- 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、局域网到互联网和互联网到局域网的流量

配置步骤

在 SD-WAN 上集成帕洛阿尔托网络虚拟机需要以下配置：

- 置备防火墙虚拟机
- 启用流量重定向到安全虚拟机

> 注意：
>
> 必须先配置防火墙虚拟机，然后才能启用流量重定向。

配置帕洛阿尔托网络虚拟机

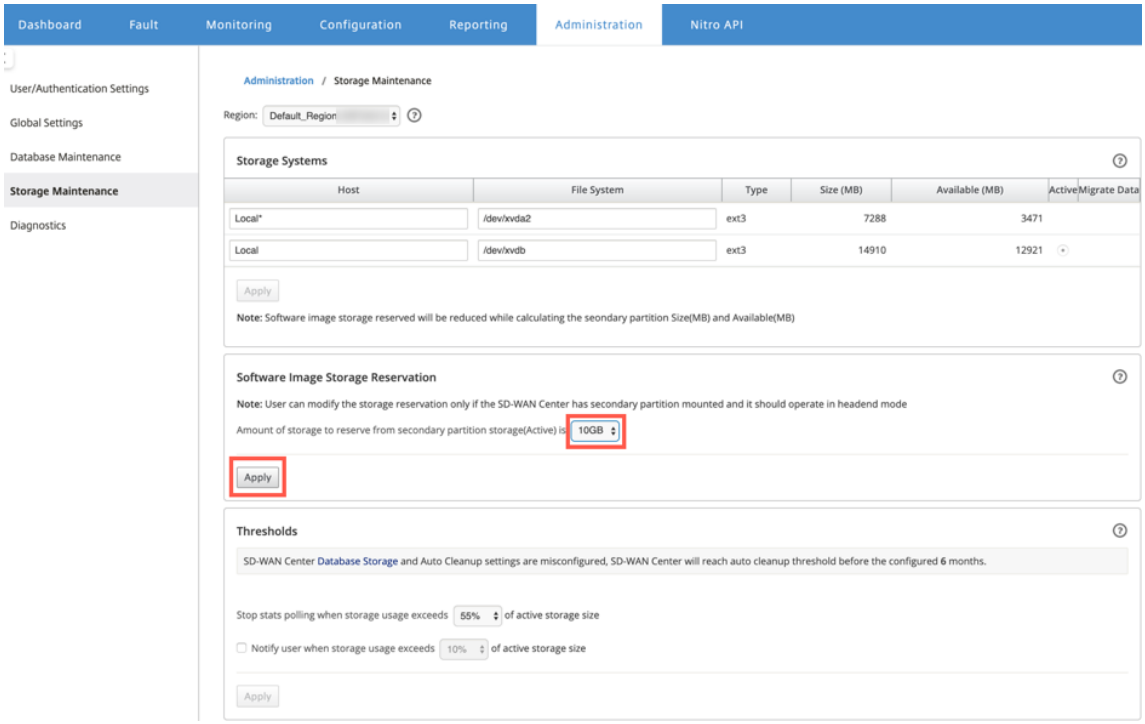
预配防火墙虚拟机有两种方法：

- 通过 SD-WAN 中心进行资源调配
- 通过 SD-WAN 设备 GUI 进行配置

通过 **SD-WAN** 中心 **Provisioning** 防火墙虚拟机

必备条件

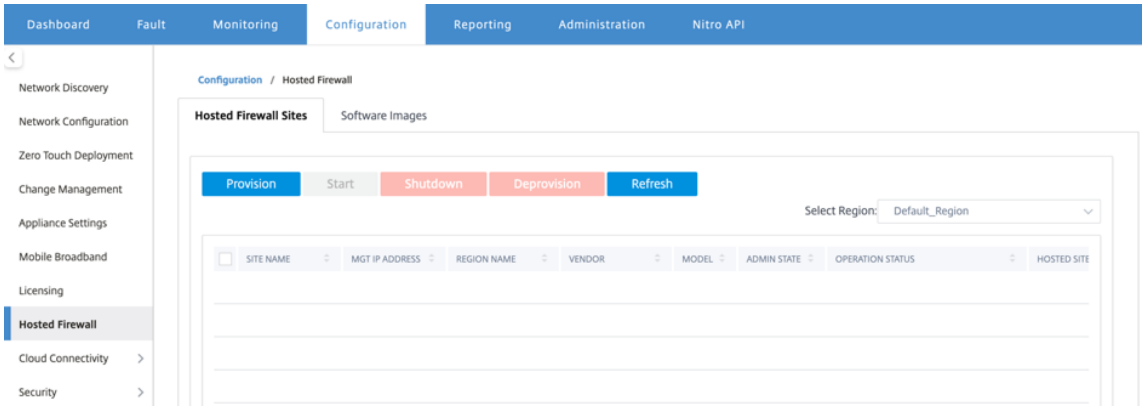
- 将辅助存储添加到 SD-WAN 中心以存储防火墙虚拟机映像文件。有关详细信息，请参阅系统要求和安装。
- 为防火墙 VM 映像文件保留辅助分区中的存储空间。要配置存储限制，请导航至 管理 **>** 存储维护。
  - 从列表中选择所需的存储量。
  - 单击应用。



> 注意：
>
> 如果满足条件，将从处于活动状态的辅助分区中保留存储空间。

通过 SD-WAN 中心平台 Provisioning 防火墙虚拟机，请执行以下步骤：

1. 从 Citrix SD-WAN Center GUI 中，导航到配置 **>** 选择托管防火墙。



您可以从下拉列表中选择 区域 以查看该选定区域的预配置站点详细信息。

2. 上传软件映像。

> 注意：
>
> 确保您有足够的磁盘空间来上传软件映像。

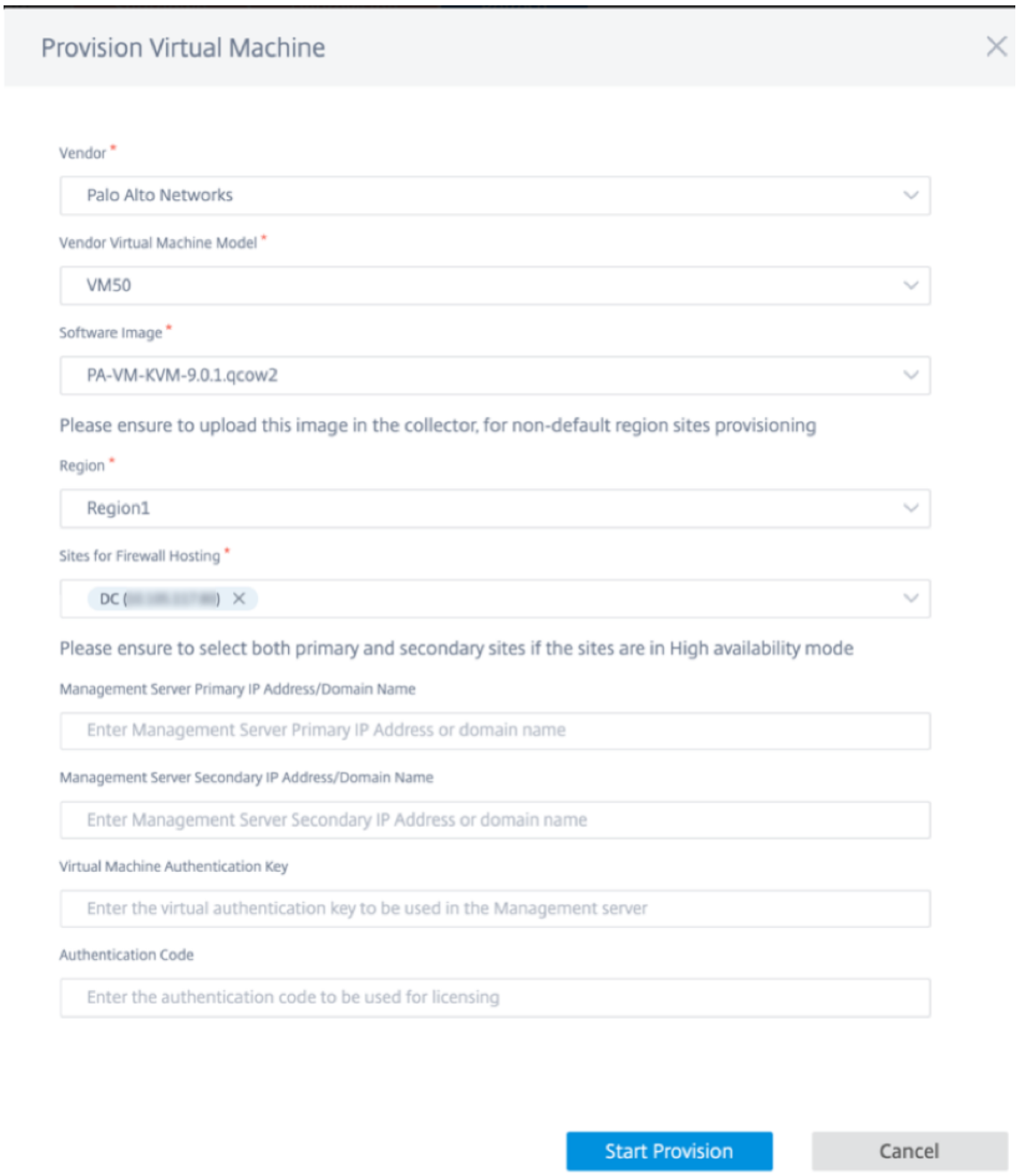
导航到 配置 **>** 托管防火墙 **>** 软件映像，然后从下拉列表中选择供应商名称作为 Palo Alto Networks。单击或拖放要上传的框中的软件映像文件。

将显示一个状态栏，其中包含正在进行的上载过程。在图像文件显示 100% 上载之前，请勿单击 刷新 或执行任何其他操作。

- 刷新：单击 刷新 选项可获取最新的映像文件详细信息。
- 删除：单击 删 除选项可删除任何现有图像文件。

> 注意
>
> - 要在非默认区域的站点部分置备防火墙虚拟机，请在每个收集器节点上上传映像文件。
> - 从 SDWAN 中心删除帕洛阿尔托虚拟机映像，将从 SDWAN 中心存储中删除该映像，而不是从设备中删除该映像。

3. 对于预配，请返回 托管防火墙站点 选项卡，然后单击 置备。

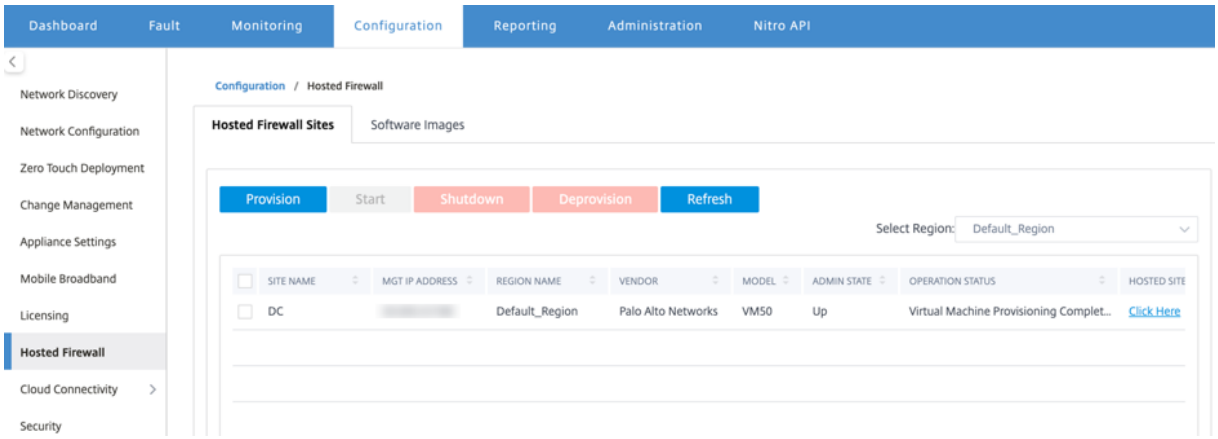


- 供应商：从下拉列表中选择 供应商 名称作为 **Palo Alto Networks** 。

- 供应商虚拟机型号：从列表中选择虚拟机型号。
- 软件映像：选择要预配的映像文件。
- 区域：从列表中选择区域。
- 防火墙托管站点：为防火墙托管列表选择站点。如果站点处于高可用性模式，则必须同时选择主站点和辅助站点。
- 管理服务器主 **IP** 地址/域名：输入管理主 IP 地址或完全限定域名（可选）。
- 管理服务器辅助 **IP** 地址/域名：输入管理服务器辅助 IP 地址或完全限定域名（可选）。
- 虚拟机身份验证密钥：输入要在管理服务器中使用的虚拟身份验证密钥。
- 身份验证代码：输入要用于许可的虚拟身份验证代码。

4. 单击 开始设置。
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 Center UI 上。

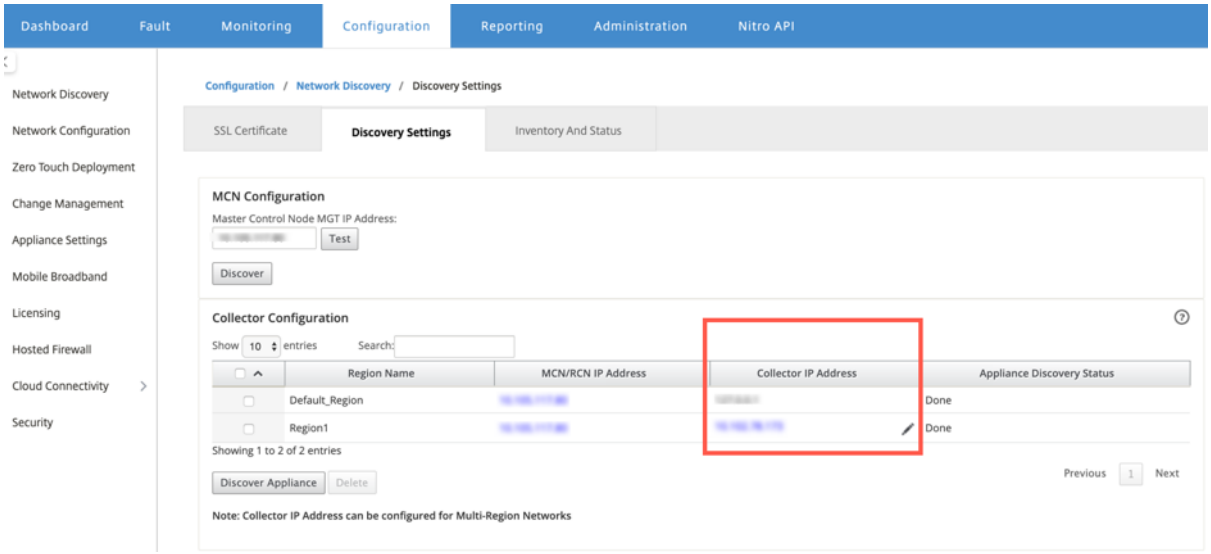
您可以根据需要 启动、关闭 和 取消 置备虚拟机。



- 站点名称：显示站点名称。
- 管理 **IP**：显示站点的管理 IP 地址。
- 区域名称：显示区域名称。
- 供应商：显示供应商名称（Palo Alto 网络）。
- 型号：显示型号 (VM50/VM100)。
- 管理状态：供应商虚拟机的状态（向上/向下）。
- 操作状态：显示操作状态消息。
- 托管站点：使用 单击此处 链接访问 Palo Alto Networks 虚拟机 GUI。

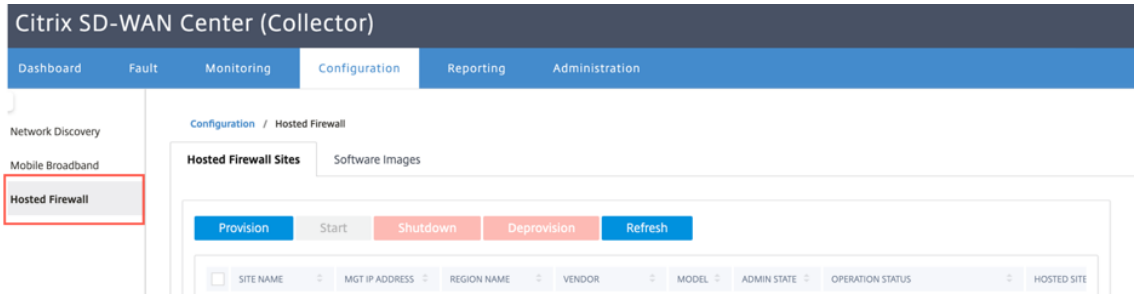
要预配非默认区域站点，您需要在 SD-WAN Center Collector 上上载软件映像。您可以从 SD-WAN Center 头端 GUI 或 SD-WAN Center Collector 配置 Palo Alto 网络。

要获取 SD-WAN Center Collector 的 IP 地址，请导航到配置 **>** 网络发现 **>** 选择发现设置选项卡。

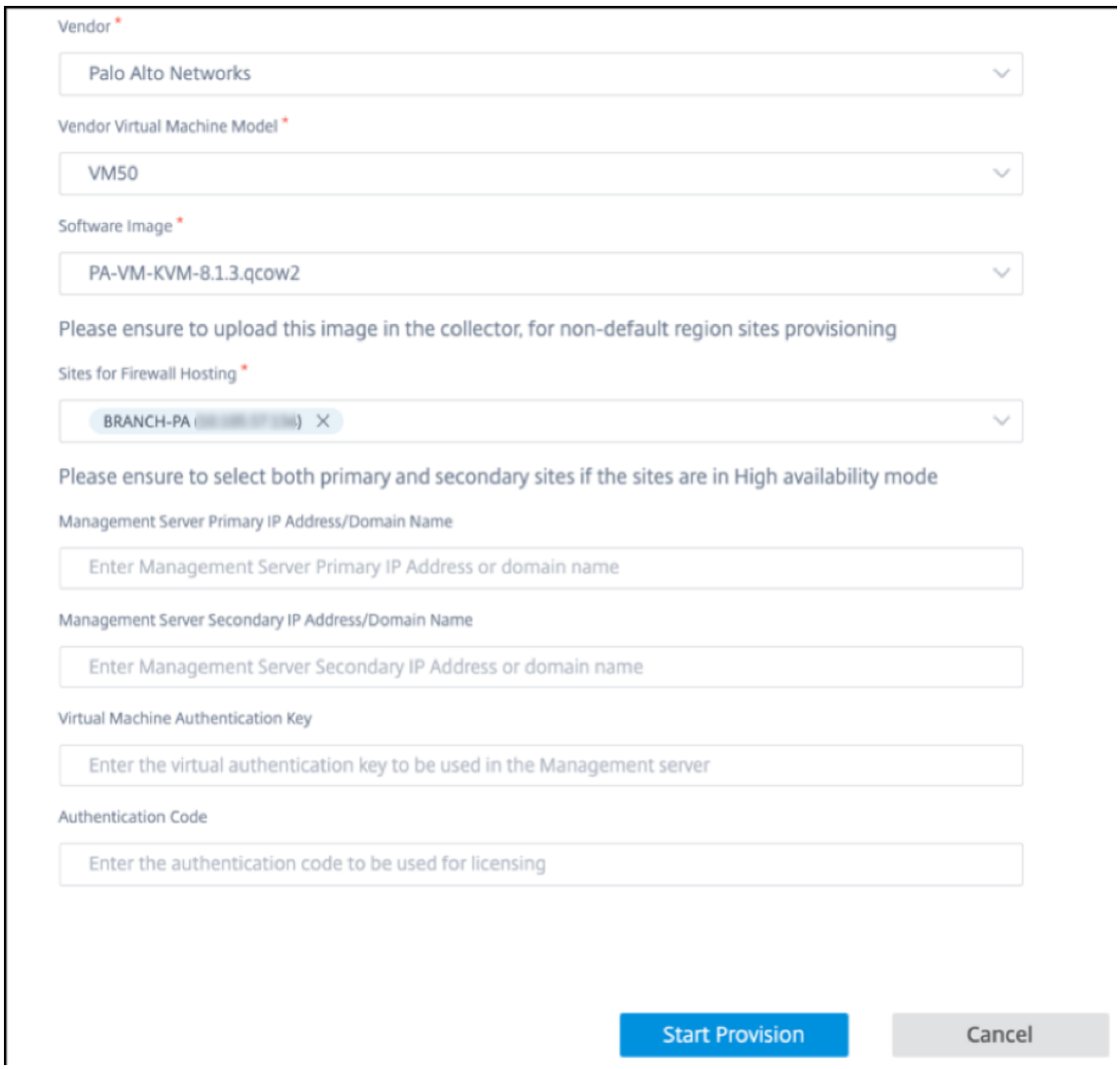


要从 SD-WAN Collector 配置 Palo Alto 网络，请执行以下操作：

1. 从 SD-WAN Collector GUI 中，导航到配置 **>** 选择托管防火墙。



2. 转到 软件映像 选项卡上传软件映像。
3. 单击 托管防火墙站点 选项卡下的 置 备
4. 提供以下详细信息，然后单击 开始置备。



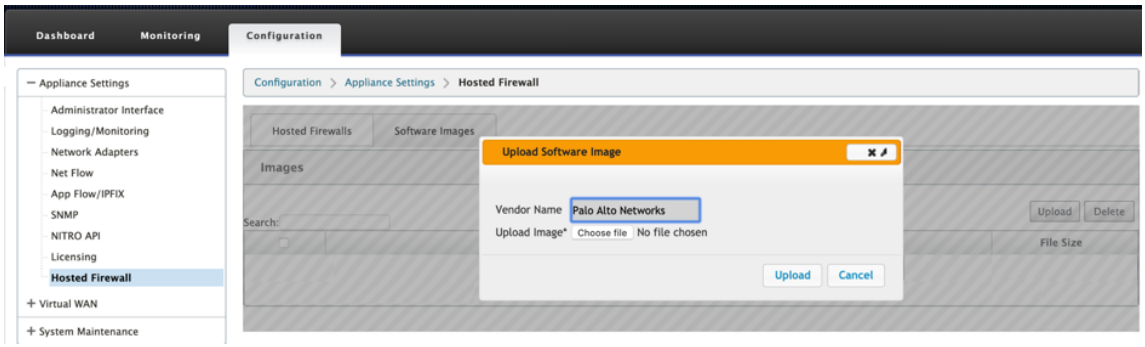
- 供应商：从下拉列表中选择 供应商 名称作为 **Palo Alto Networks** 。
- 供应商虚拟机型号：从列表中选择虚拟机型号。
- 软件映像：选择要预配的映像文件。
- 区域：从列表中选择区域。
- 防火墙托管站点：为防火墙托管列表选择站点。如果站点处于高可用性模式，则必须同时选择主站点和辅助站点。
- 管理服务器主 **IP** 地址/域名：输入管理主 IP 地址或完全限定域名（可选）。
- 管理服务器辅助 **IP** 地址/域名：输入管理服务器辅助 IP 地址或完全限定域名（可选）。
- 虚拟机身份验证密钥：输入要在管理服务器中使用的虚拟身份验证密钥。
- 身份验证代码：输入要用于许可的虚拟身份验证代码。

5. 单击 开始设置。

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：

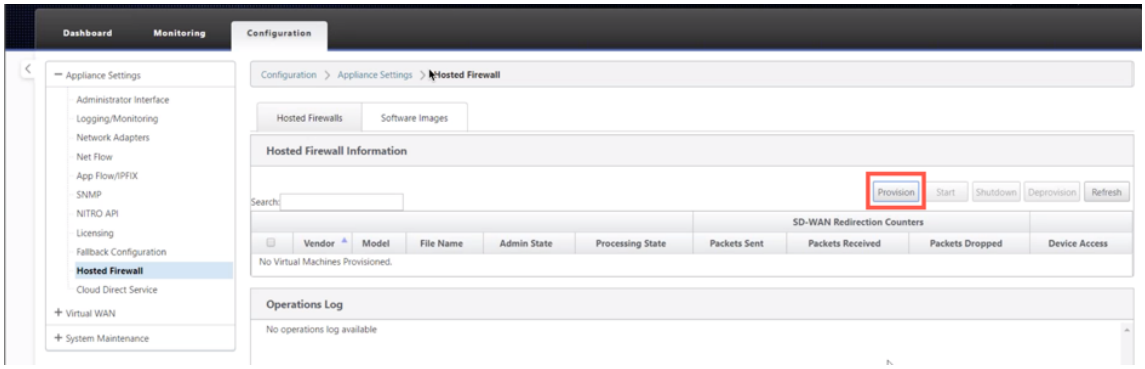
1. 从 Citrix SD-WAN GUI 中，导航到 配置 **>** 展开 设备设置 **>** 选择 托管防火墙。
2. 上传软件映像：
   - 选择 软件映像 选项卡。选择供应商名称作为 **Palo Alto** 网络。
   - 选择软件映像文件。
   - 单击上载。



> 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。

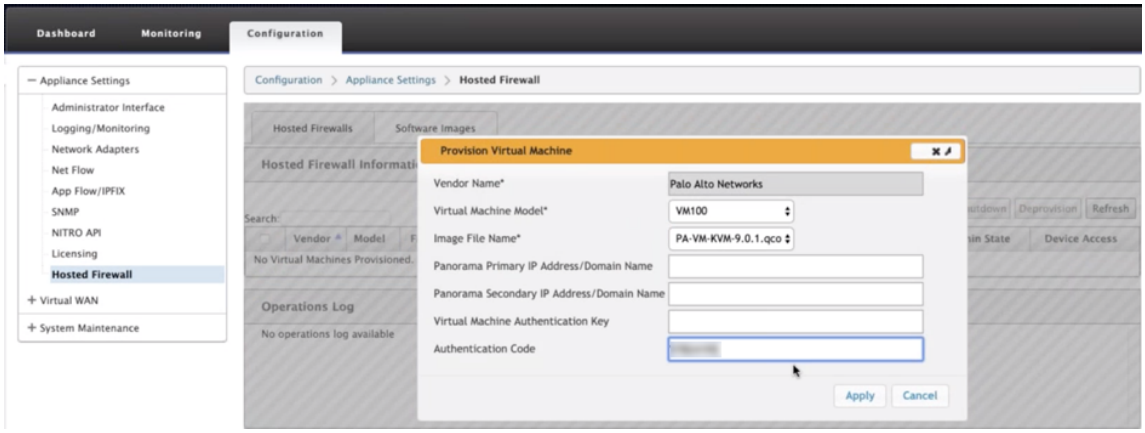
3. 对于预配，请选择 托管防火墙 选项卡，然后单击 置 备按钮



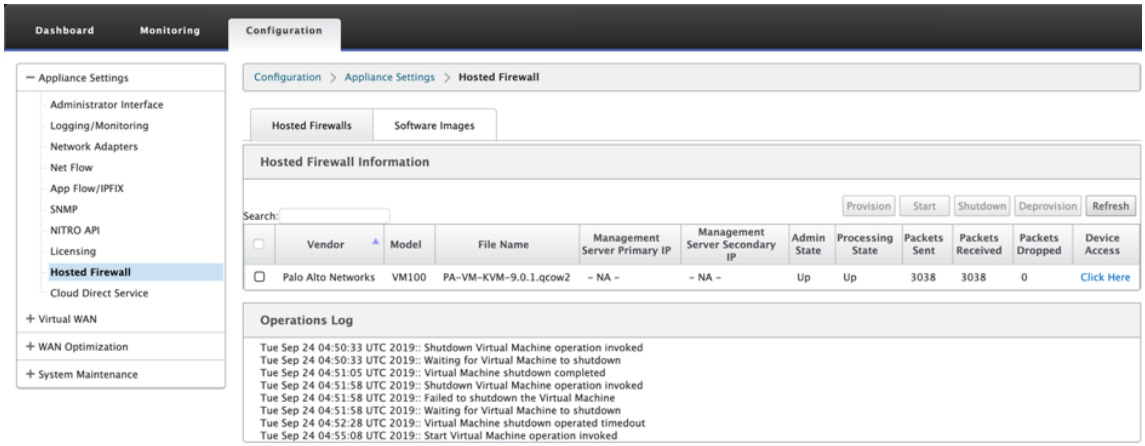
4. 请提供以下详细信息以供 Provisioning。
   - 供应商名称：选择供应商作为 **Palo Alto** 网络。
   - 虚拟机型号：从列表中选择虚拟机型号。
   - 图像文件名：选择图像文件。

- 全景主 **IP** 地址/域名：提供全景主 IP 地址或完全限定域名（可选）。
- 全景辅助 **IP** 地址/域名：提供全景辅助 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。
- 发送的数据包：从 SD-WAN 发送到安全虚拟机的数据包。
- 接收的数据包：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，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 网络虚拟机 GUI 或使用您的管理 IP 以及 4100 端口（管理 IP：4100）。

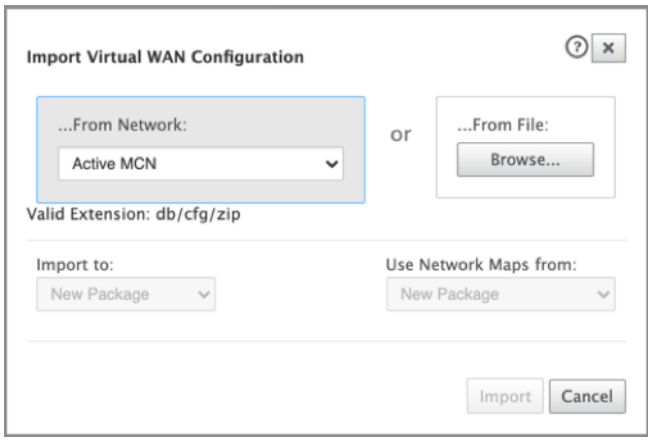
> 注意
> 始终使用隐身模式访问 Palo Alto 网络 GUI。

流量重定向

流量重定向配置可以通过 MCN 上的配置编辑器或 SD-WAN 中心上的配置编辑器完成。

要浏览 SD-WAN 中心的配置编辑器，请执行以下操作：

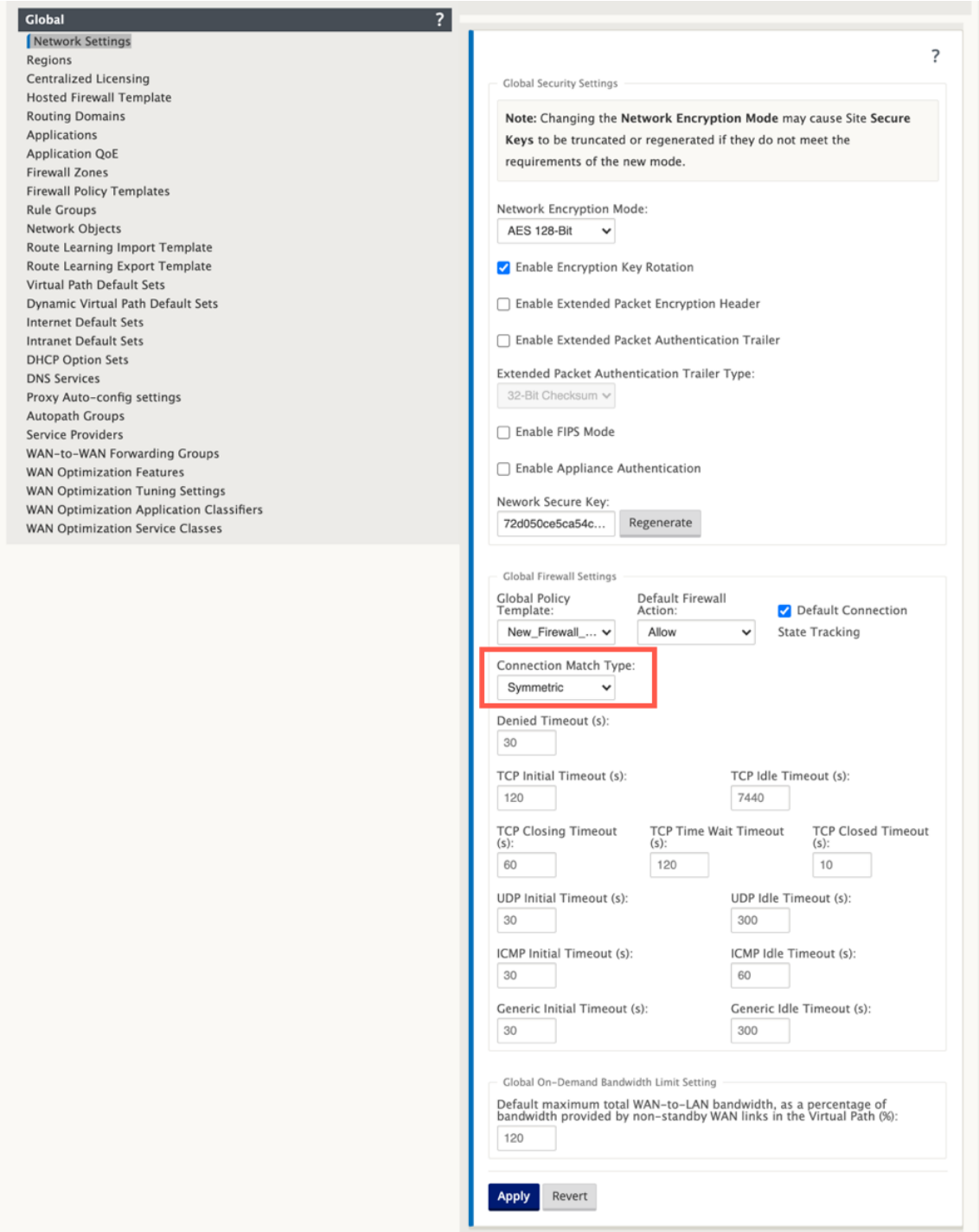
1. 打开 Citrix SD-WAN Center UI，导航到 配置 **>** 网络配置导入。从活动 MCN 导入虚拟 WAN 配置，然后单击导入。



其余步骤类似于以下步骤-通过 MCN 进行流量重定向配置。

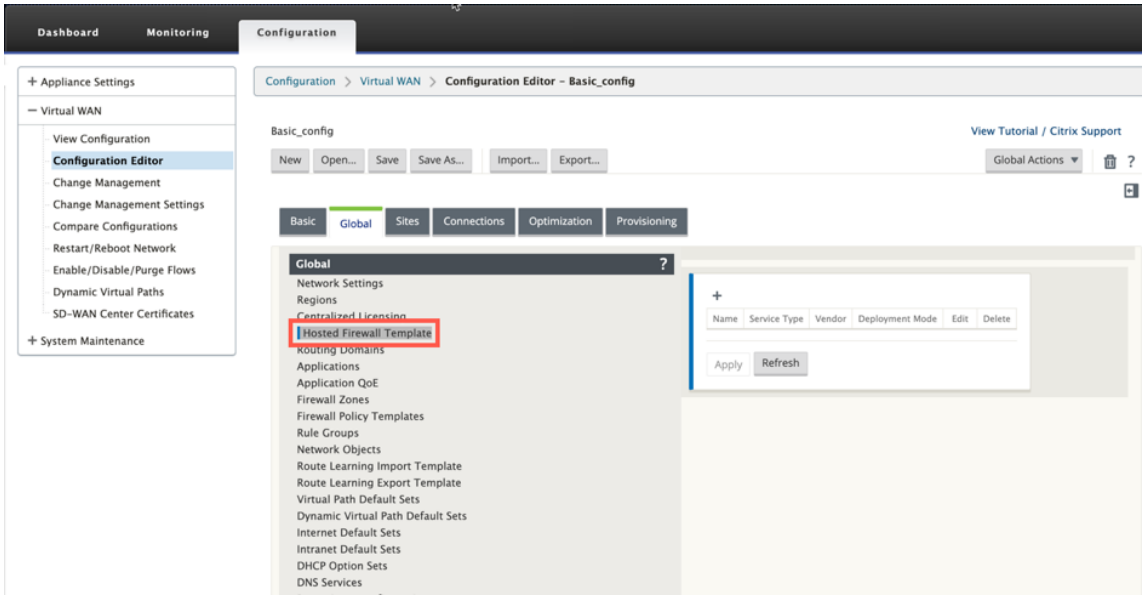
要在 MCN 上浏览配置编辑器：

1. 在 全局 **>** 网络设置下将连接匹配类型设置 为 对称。

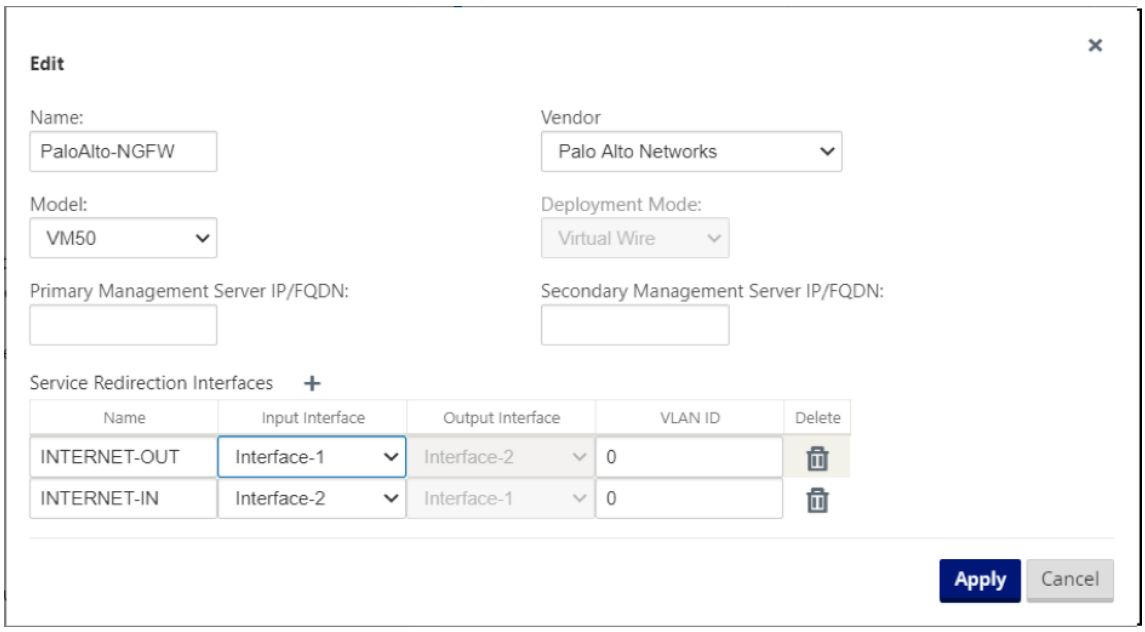


默认情况下，SD-WAN 防火墙策略是特定于方向的。对称匹配类型使用指定的匹配条件匹配连接，并在两个方向上应用策略操作。

2. 打开 **Citrix SD-WAN UI**，导航到 配置 **>** 展开虚拟广域网 ** 选择 ** 配置编辑器 > 选择 全局 部分下的 托管防火墙模板。



3. 单击 **+** 并在以下屏幕截图中提供所需信息以添加 托管防火墙 模板，然后单击 添加。



托管防火墙模板 允许您配置流量重定向到 SD-WAN 设备上托管的 防火墙虚拟机。以下是配置模板所需的输入：

- 名称：托管防火墙模板的名称。
- 供应商：防火墙供应商的名称。
- 部署模式：“部 署模式”字段自动填充并显示为灰色。对于 **Palo Alto Networks** 供应商，部署模式是 虚拟电线。
- 模型：托管防火墙的虚拟机模型。您可以选择虚拟机型号作为 Palo Alto 网络供应商的 VM 50/VM 100。
- 主管理服务器 **IP/FQDN**：Panorama 的主管理服务器 IP/FQDN。
- 辅助管理服务器 **IP/FQDN**：Panorama 的辅助管理服务器 IP/FQDN。
- 服务重定向接口：这些是用于 SD-WAN 和托管防火墙之间的流量重定向的逻辑接口。

接口 1、接口 2 是指托管防火墙上的前两个接口。如果 VLAN 用于流量重定向，则必须在托管防火墙上配置相同的 VLAN。配置为流量重定向的 VLAN 是 SD-WAN 和托管防火墙的内部。

> 注意
>
> 必须从连接启动程序方向选择重定向输入接口，重定向接口会自动选择响应流量。例如，如果出站 Internet 流量被重定向到接口 1 上的托管防火墙，则响应流量将自动重定向到接口 2 上的托管防火墙。如果没有互联网入站流量，则在上面的示例中不需要接口-2。

只有两个物理接口被分配到托管 Palo Alto 网络防火墙。如果需要将来自多个区域的流量重定向到托管防火墙，则可以使用内部 VLAN 创建多个子接口，并将其关联到托管防火墙上的不同防火墙区域。

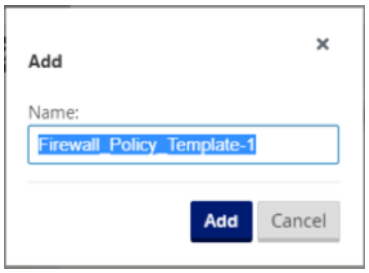
通过 SD-WAN 防火墙策略或站点级别策略，您可以将所有流量重定向到帕洛阿尔托网络虚拟机。

> 注意
>
> SD-WAN 防火墙策略是自动创建的，以 允许 流量进出托管防火墙管理服务器。这样可避免重定向来自（或）托管防火墙的管理流量。

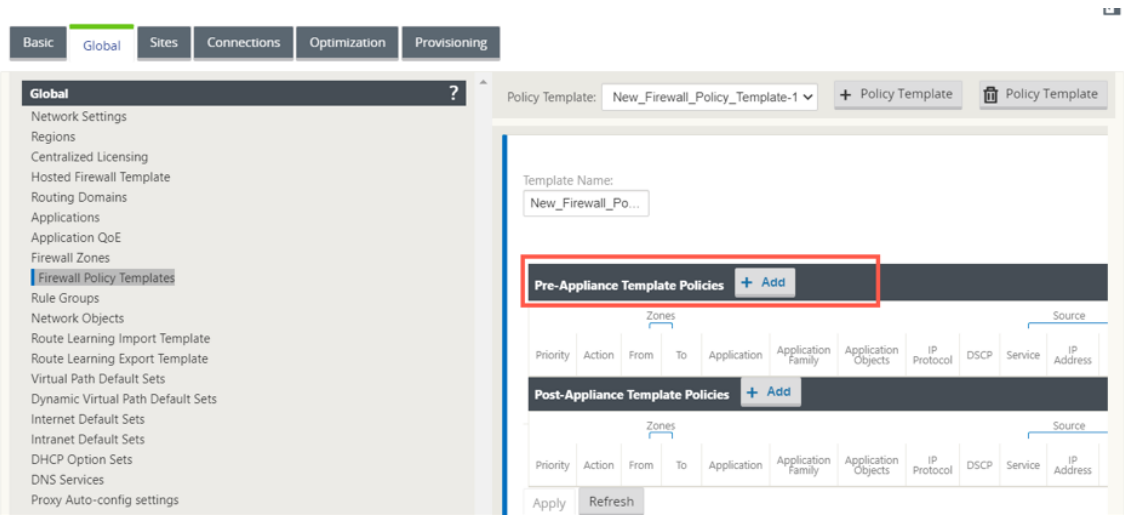
可以使用 SD-WAN 防火墙策略完成到防火墙虚拟机的流量重定向。有两种方法可以创建 SD-WAN 防火墙策略-通过 全局 部分中的防火墙策略模板或站点级别。

方法**-1**

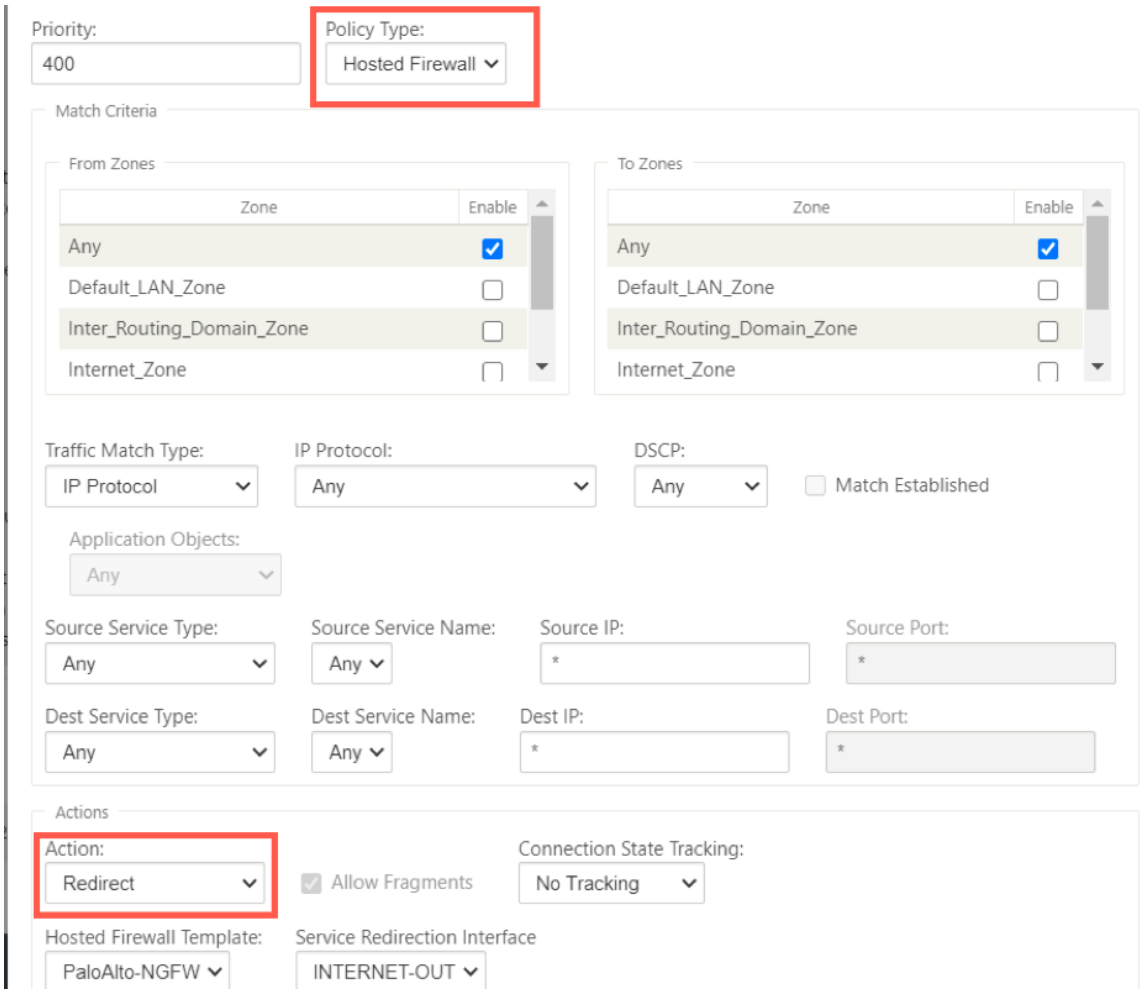
1. 在 Citrix SD-WAN GUI 中，导航到 配置 **>** 展开 虚拟 **WAN >** 配置编辑器。导航到 全 局选项卡，然后选择 防火墙策略模板。单击 **+** 策略模板。为策略模板提供名称，然后单击 添加。



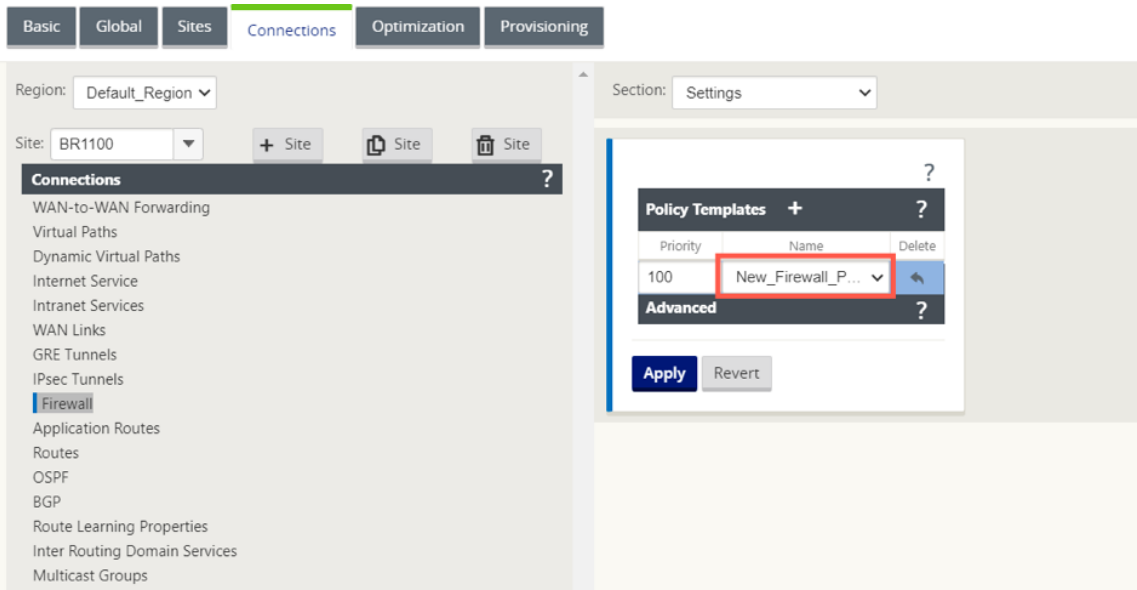
2. 单击“装置前模板策略”旁边的 **+** 添加。



3. 将 策略类型 更改为 托管防火墙。“操作”字段将自动填充以 重定向。从下拉列表中选择 托管防火墙模板 和 服务重定向接口。根据需要填写其他匹配条件。

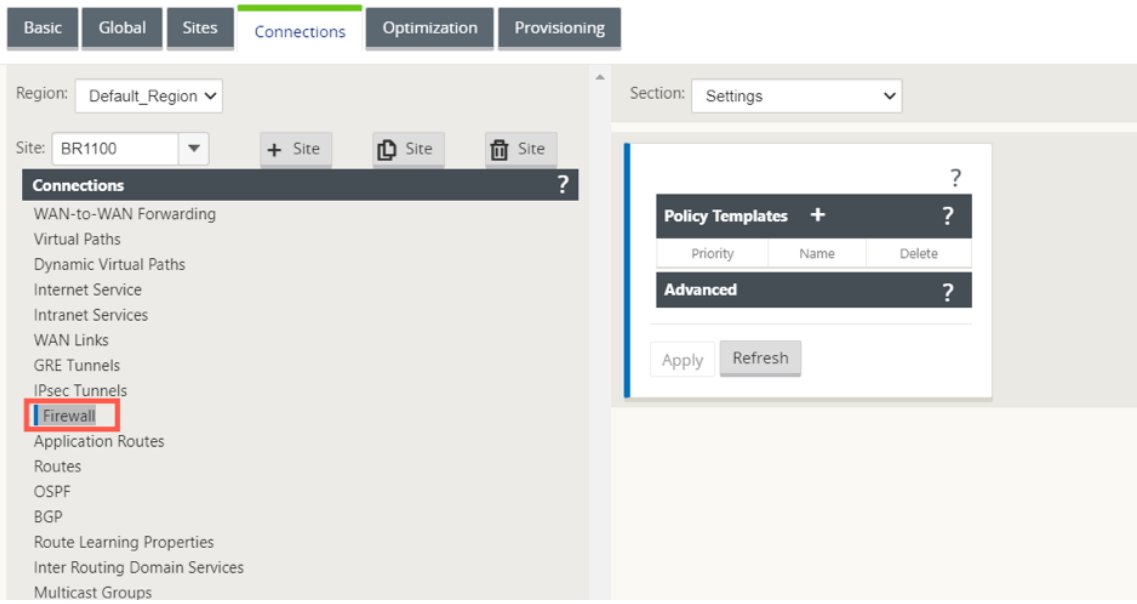


4. 导航到“连接” > “防火墙”，然后在“名称”字段下选择防火墙策略（您创建的）。单击应用。

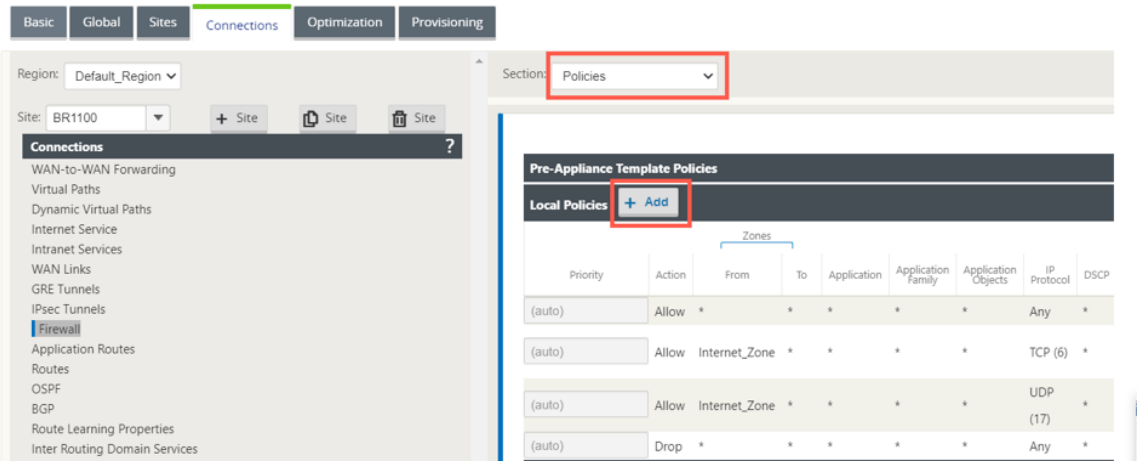


方法**-2**

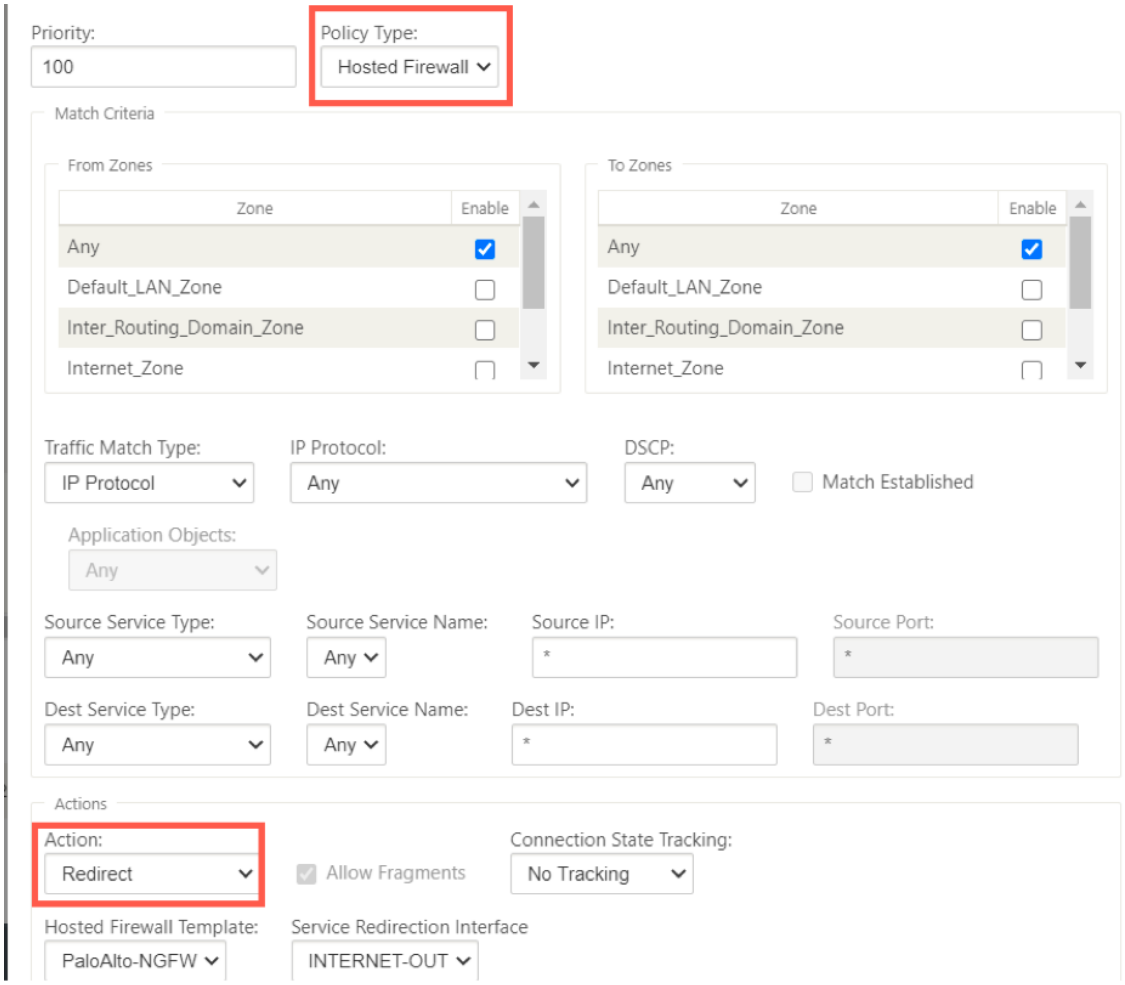
1. 要重定向所有流量，请在 配置编辑器 **>** 虚拟 **WAN** 下，导航到 连 接选项卡，然后选择 防火墙。



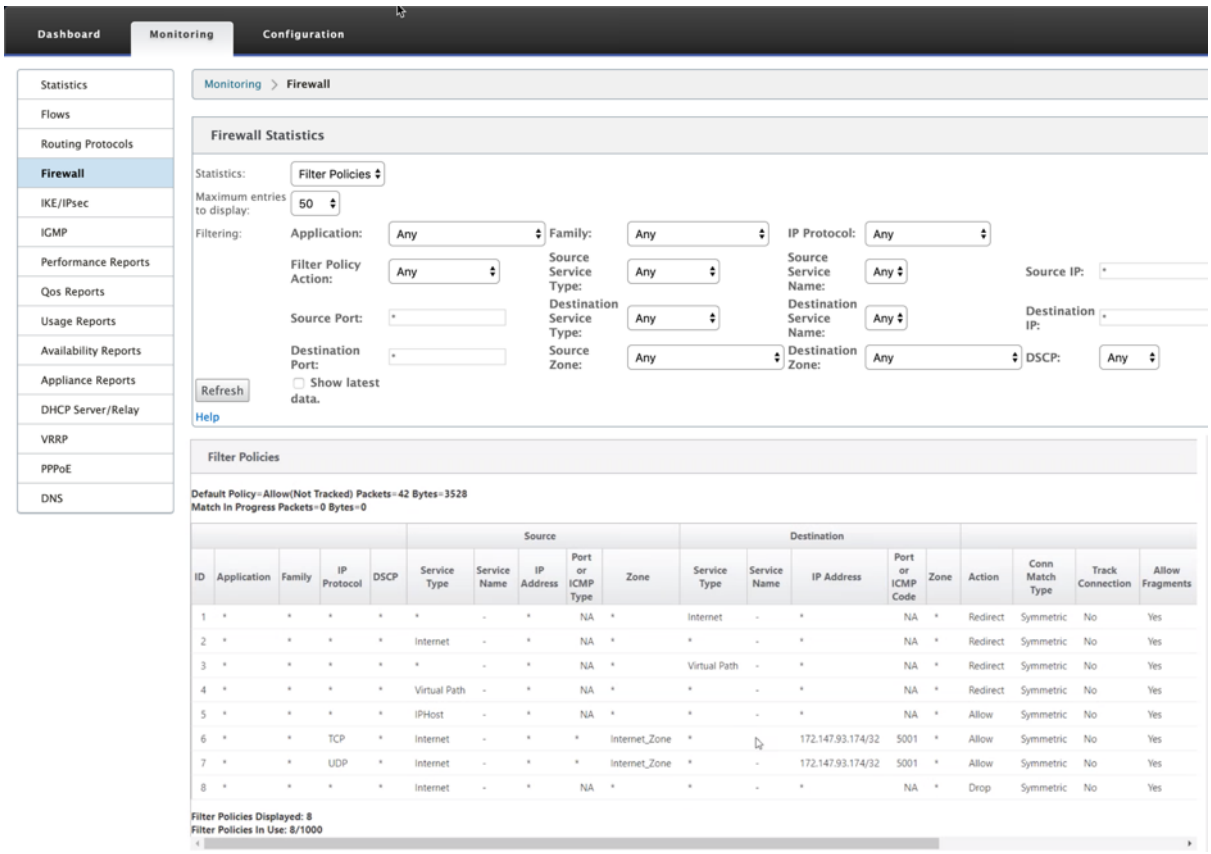
2. 从 区域 下拉列表中选择 策 略，然后单击 **+** 添加 以创建新的防火墙策略。



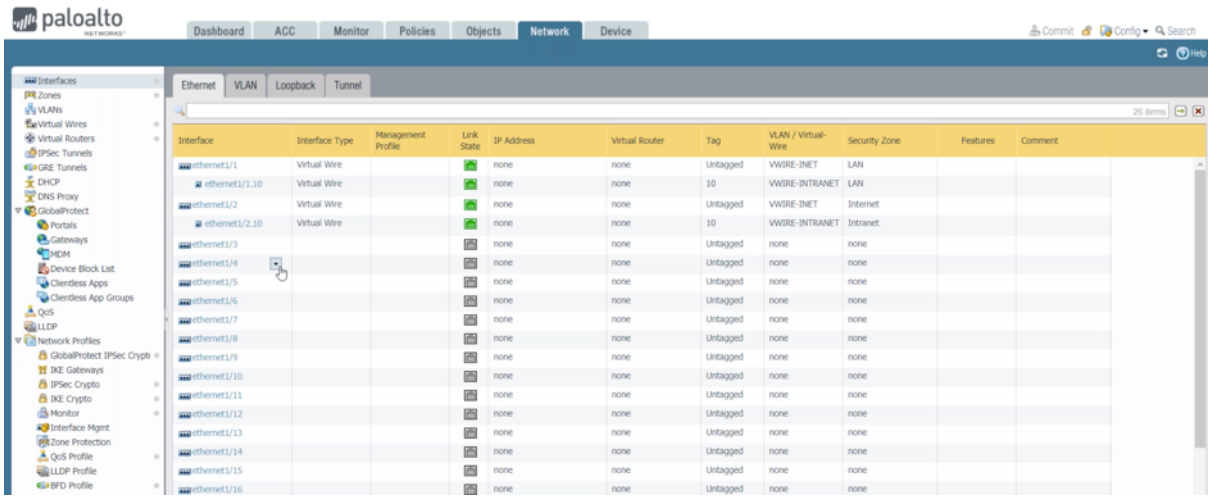
3. 将 策略类型 更改为 托管防火墙。操作字段自动填充为“重定向”。从下拉列表中选择 托管防火墙模板 和 服务重定向接口。单击添加。



当所有网络配置处于启动状态并运行模式时，您可以在监视 > 防火墙 > 统计列表下监控连接，选择筛选策略。



可以使用 Palo Alto 网络 UI 验证您在 SD-WAN 服务链模板上执行的配置与 Palo Alto 网络配置之间的映射。



> 注意
>
> 如果已在 1100 设备上配置了 **Cloud Direct** 或 **SD-WAN WANOP (PE)**，则无法配置帕洛阿尔托网络虚拟机。

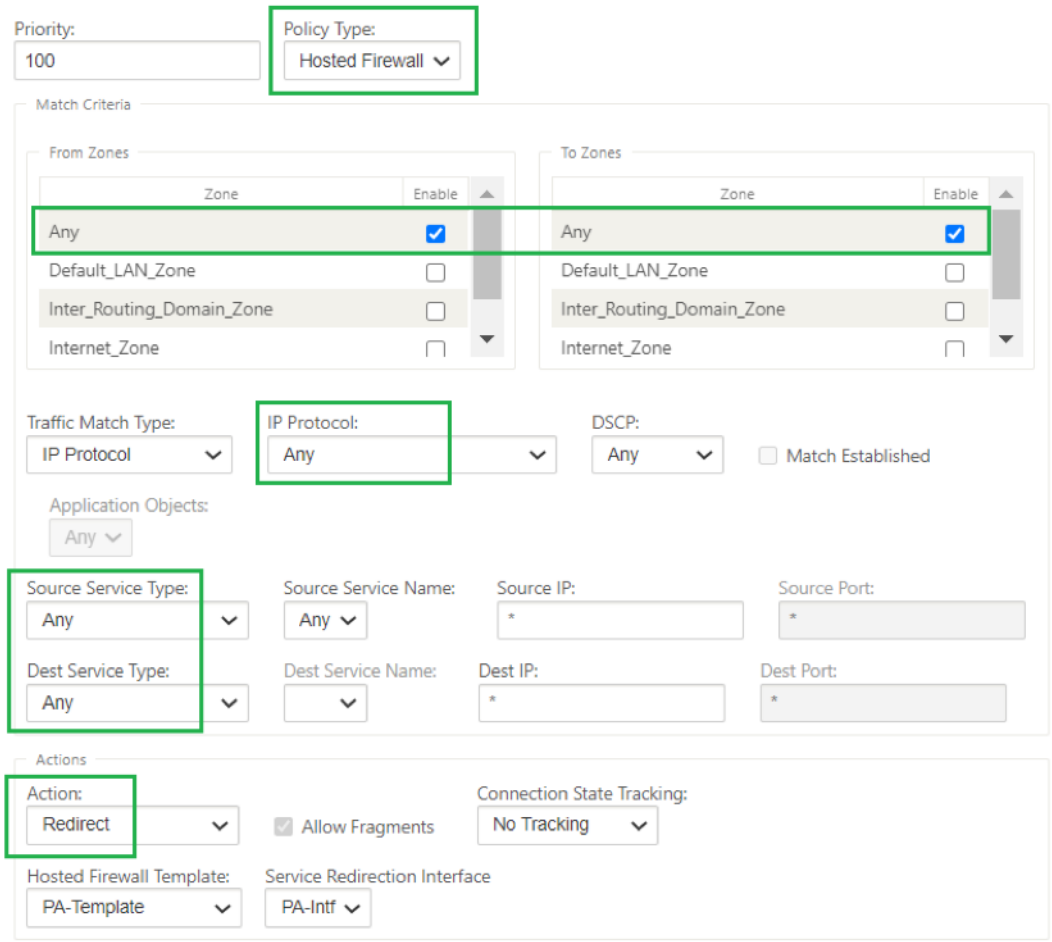
使用案例—**SD-WAN 1100** 上的托管防火墙

以下是使用 Citrix SD-WAN 1100 设备实现的一些使用案例方案：

使用案例 **1**：将所有流量重定向到托管防火墙

此使用案例适用于所有流量都由托管的下一代防火墙处理的小型分支使用情形。必须考虑带宽要求，因为重定向的流量吞吐量限制为 100 Mbps。

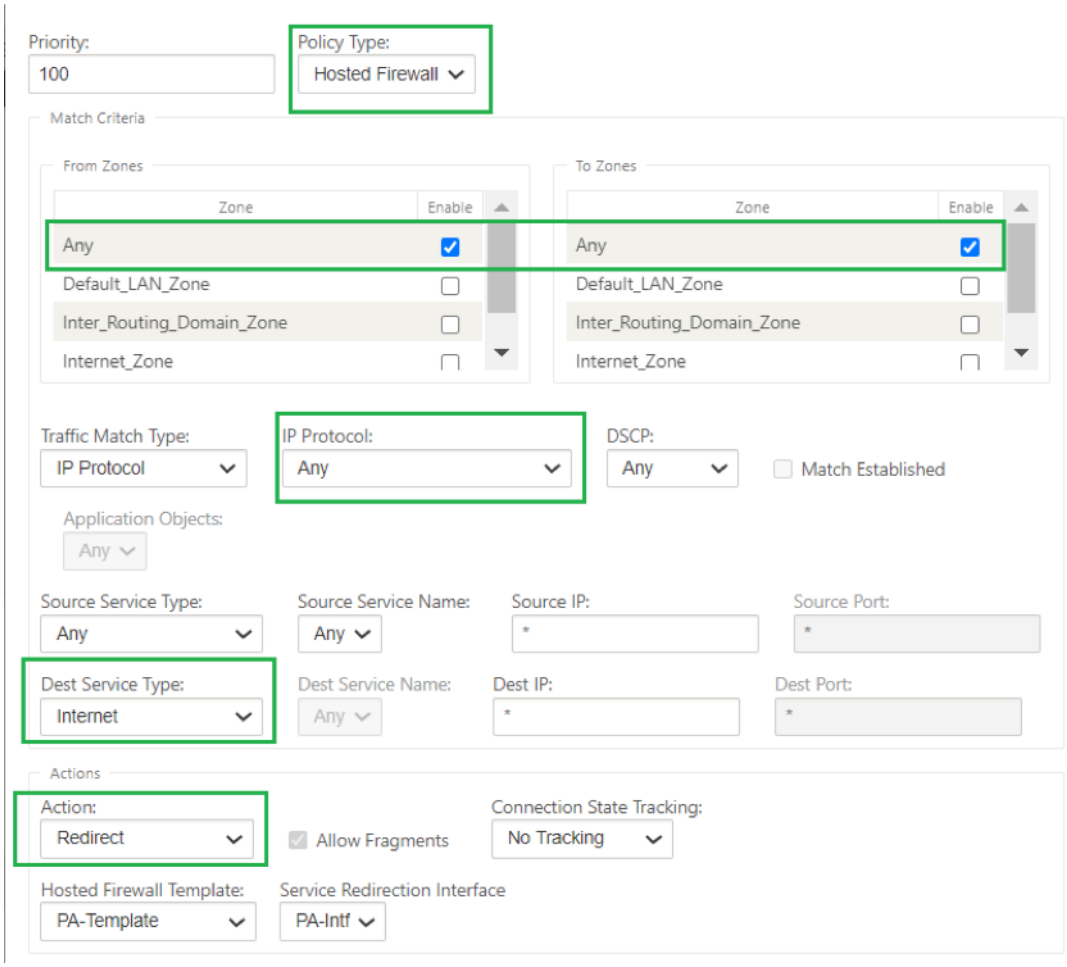
为此，请创建一个防火墙规则以匹配任何流量，并将 操 作作为 重定向创建防火墙规则，如以下屏幕截图所示：



使用案例 **2**：仅将 **Internet** 流量重定向到托管防火墙

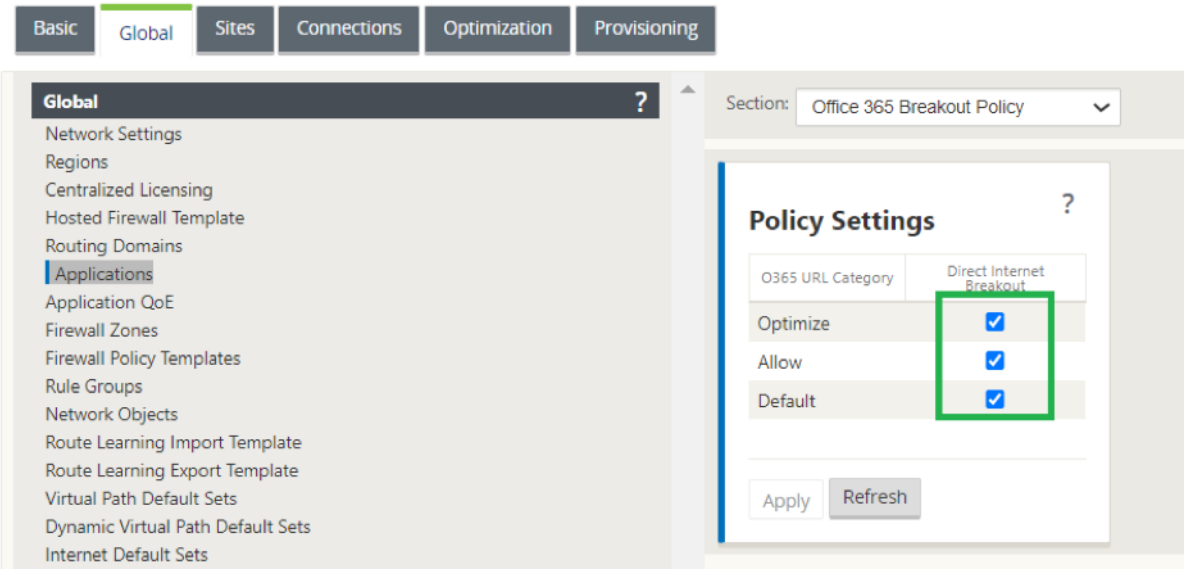
此使用案例适用于 Internet 绑定流量不超过支持的重定向流量吞吐量的任何分支站点。在这种情况下，分支到数据中心的流量由部署在数据中心的安全设备/服务处理。

要实现此目的，请创建一个防火墙规则以匹配任何流量，并使用 A **ction** 作为 重定向，如以下屏幕截图所示：

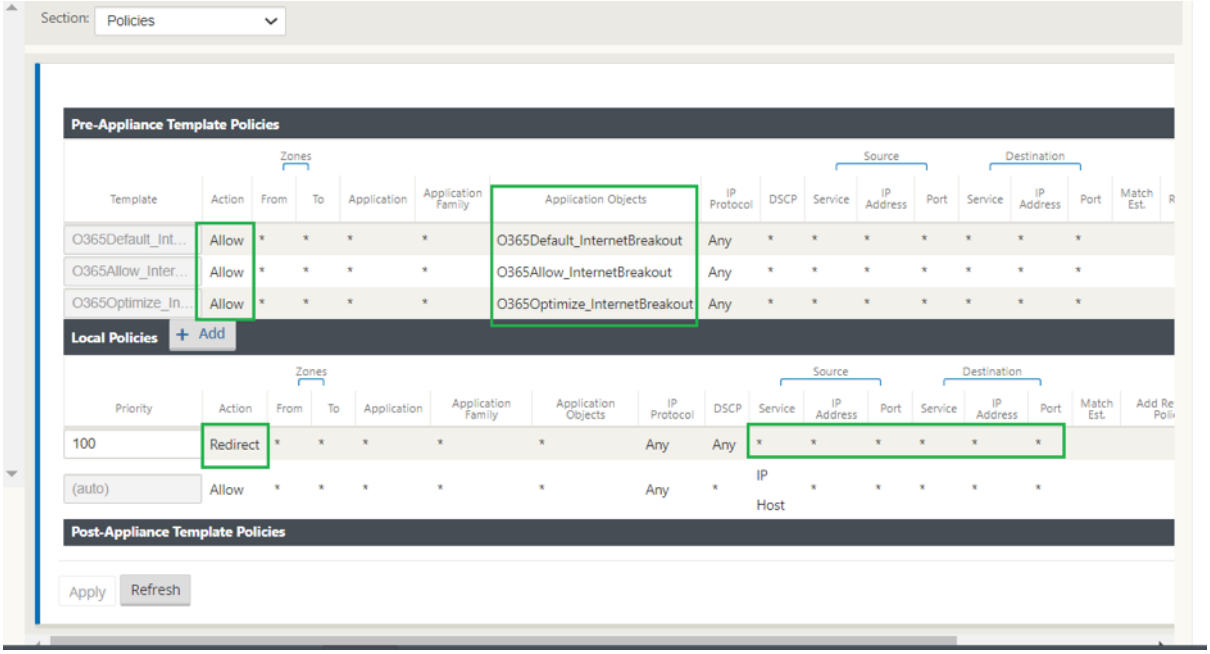


使用案例 **3**：针对受信任的 **Internet SaaS** 应用程序直接进行互联网突破，并将剩余的所有流量重定向到托管虚拟机

在此使用案例中，添加了防火墙规则，以便为可信 SaaS 应用程序（如 Office 365）执行直接互联网分解。首先启用 Office 365 分解策略，如以下屏幕截图所示：



这会自动添加 装置前模板策略 以允许 Office 365 流量，如以下屏幕截图所示。现在添加防火墙规则，以便将剩余的所有流量重定向到托管防火墙，如下所述。



> 注意
>
> 托管防火墙配置独立于 Citrix SD-WAN 配置。因此，可以根据企业安全要求配置托管防火墙。

SD-WAN 1100 平台上的 Check Point 防火墙集成

November 1, 2021

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

检查点量子边缘 在 SD-WAN 1100 平台上作为虚拟机运行。防火墙虚拟机以 Bridge 模式集成，并连接到它的两个数据虚拟接口。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。

> 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、局域网到互联网和互联网到局域网的流量

配置步骤

在 SD-WAN 上集成 Check Point 防火墙虚拟机需要以下配置：

- 置备防火墙虚拟机
- 启用流量重定向到安全虚拟机

> 注意：
>
> 必须先配置防火墙虚拟机，然后才能启用流量重定向。

置备检查点防火墙虚拟机

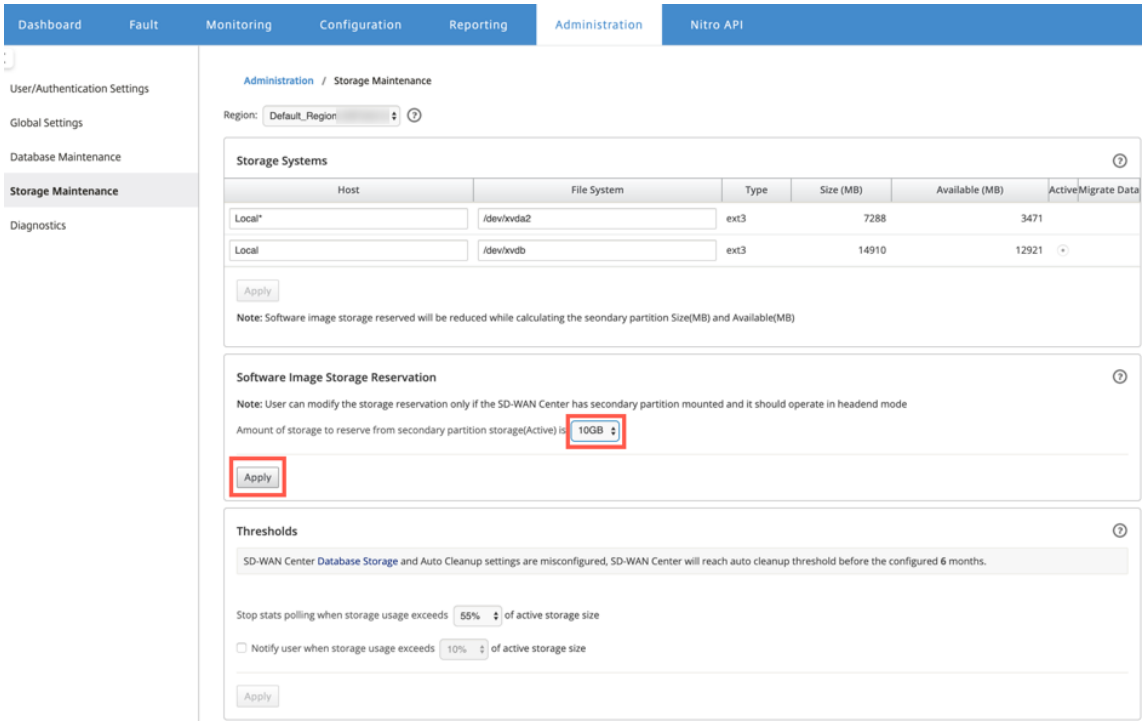
预配防火墙虚拟机有两种方法：

- 通过 SD-WAN 中心进行资源调配
- 通过 SD-WAN 设备 GUI 进行配置

通过 **SD-WAN** 中心 **Provisioning** 防火墙虚拟机

必备条件

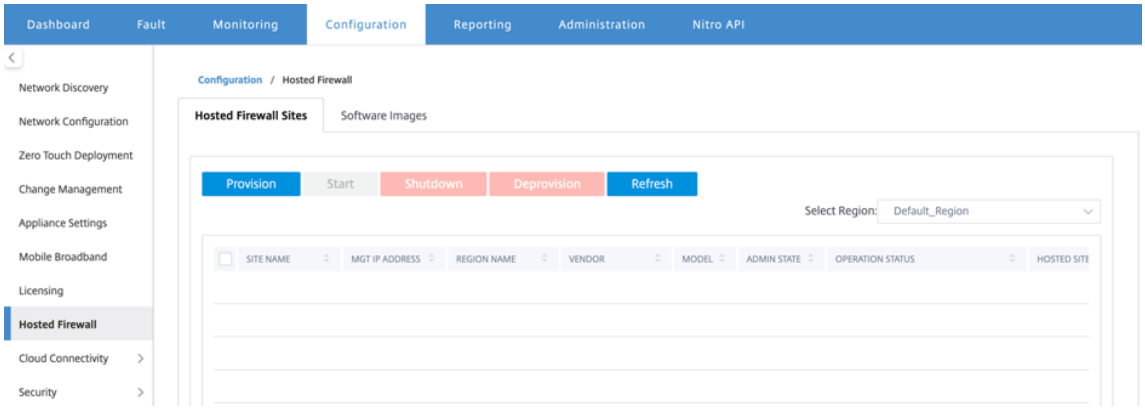
- 将辅助存储添加到 SD-WAN 中心以存储防火墙虚拟机映像文件。有关详细信息，请参阅 系统要求和安装。
- 为防火墙 VM 映像文件保留辅助分区中的存储空间。要配置存储限制，请导航至 管理 **>** 存储维护。
  - 从列表中选择所需的存储量。
  - 单击应用。



> 注意：
>
> 如果满足条件，将从处于活动状态的辅助分区中保留存储空间。

通过 SD-WAN 中心平台 Provisioning 防火墙虚拟机，请执行以下步骤：

1. 从 Citrix SD-WAN Center GUI 中，导航到配置 **>** 选择托管防火墙。

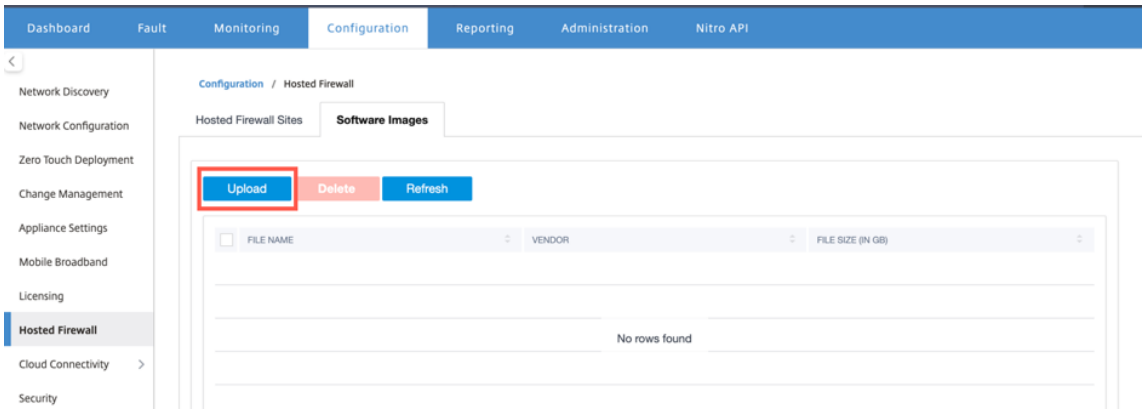


您可以从下拉列表中选择 区域 以查看该选定区域的预配置站点详细信息。

2. 上传软件映像。

> 注意：
>
> 确保您有足够的磁盘空间来上传软件映像。

导航到 配置 **>** 托管防火墙 **>** 软件映像，然后单击 上传。



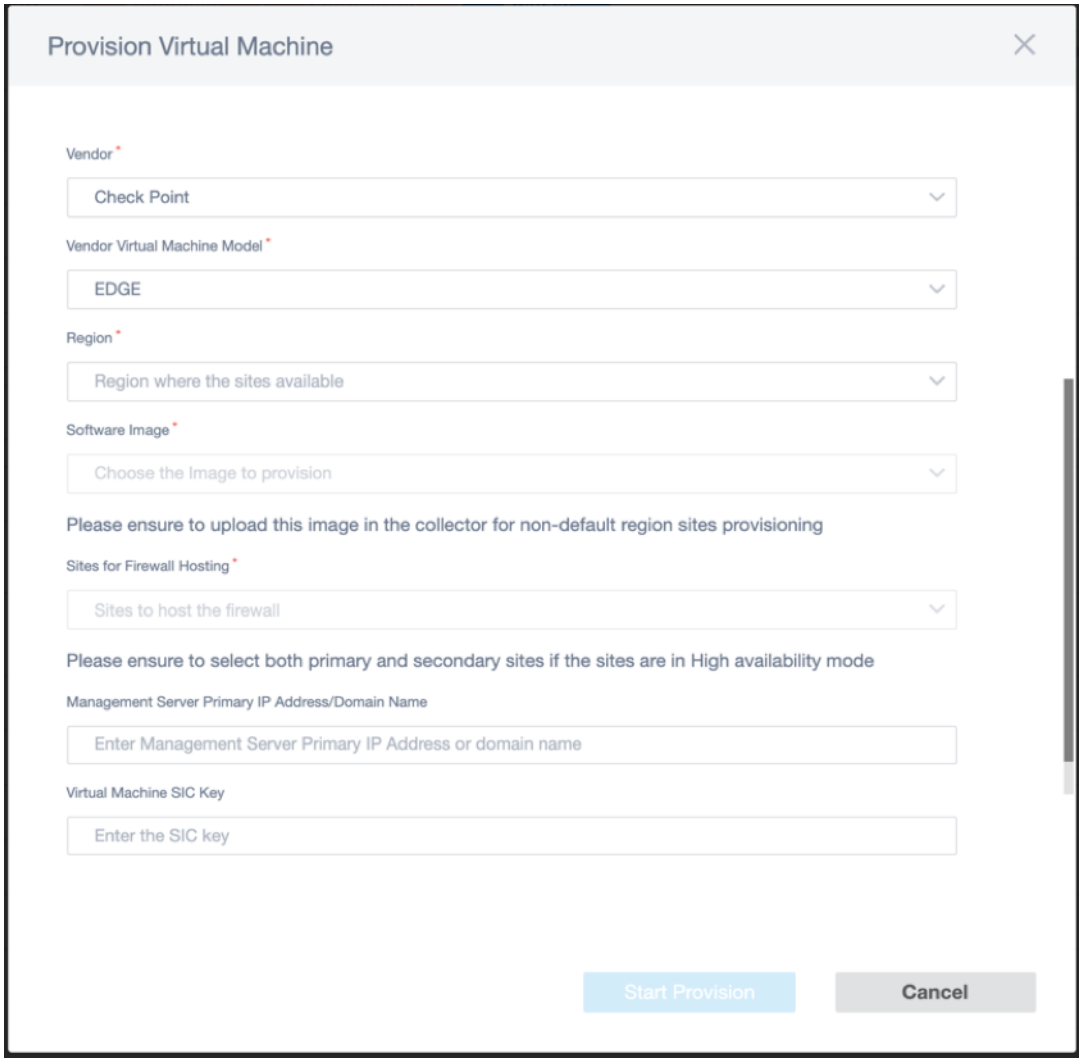
3. 从下拉列表中选择供应商名称作为 检查点。单击或拖放要上传的框中的软件映像文件。

将显示一个状态栏，其中包含正在进行的上载过程。在图像文件显示 100% 上载之前，请勿单击 刷新 或执行任何其他操作。

- 刷新：单击 刷新 选项可获取最新的映像文件详细信息。
- 删除：单击 删 除选项可删除任何现有图像文件。

> 注意：
>
> 要在非默认区域的站点部分上置备防火墙虚拟机，请在每个收集器节点上传映像文件。

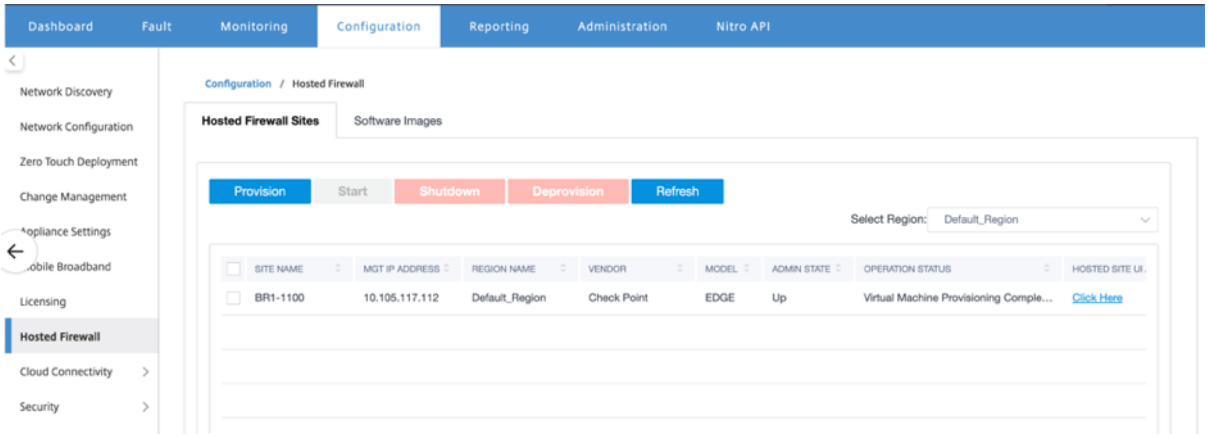
4. 要进行置备，请返回 托管防火墙站 点选项卡，然后单击 置备。



- 供应商：从下拉列表中选择供应商名称作为 检查点。
- 供应商虚拟机模型：虚拟机模型字段将自动填充为 Edge。
- 区域：从列表中选择区域。
- 软件映像：选择要预配的映像文件。
- 防火墙托管站点：为防火墙托管列表选择站点。如果站点处于高可用性模式，则必须同时选择主站点和辅助站点。
- 管理服务器主 **IP** 地址/域名：输入管理主 IP 地址或完全限定域名（可选）。
- 虚拟机 **SIC** 密钥：输入虚拟机安全内部通信 (SIC) 密钥。SIC 在 检查点 组件之间创建可信连接。

5. 单击 开始设置。
6. 单击 刷新 以获取最新状态。检查点虚拟机完全启动后，它将反映在 SD-WAN 中心用户界面上。

您可以根据需要 启动、关闭 和 取消 置备虚拟机。

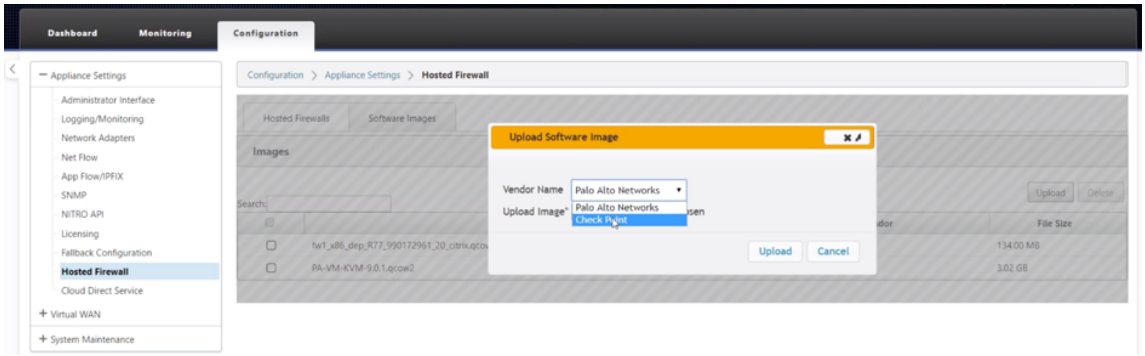


- 站点名称：显示站点名称。
- 管理 **IP**：显示站点的管理 IP 地址。
- 区域名称：显示区域名称。
- 供应商：显示供应商名称（检查点）。
- 型号：显示模型- **Edge**。
- 管理状态：供应商虚拟机的状态（向上/向下）。
- 操作状态：显示上次操作状态消息。
- 托管站点 **UI** 访问：使用 单击此处 链接访问检查点虚拟机 GUI。

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：

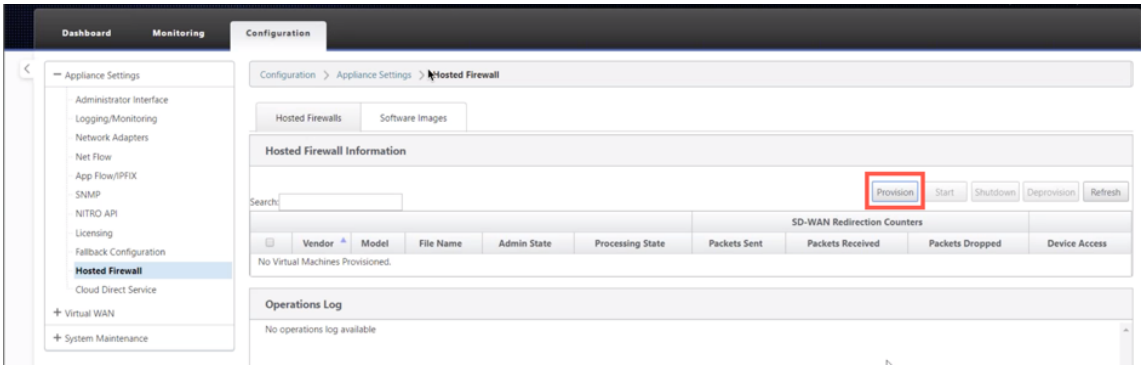
1. 从 Citrix SD-WAN GUI 中，导航到 配置 **>** 设 备设置 选择 托管防火墙。
2. 上传软件映像：
   - 选择 软件映像 选项卡。选择 供应商名称 作为检查点。
   - 选择软件映像文件。
   - 单击上载。



> 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。

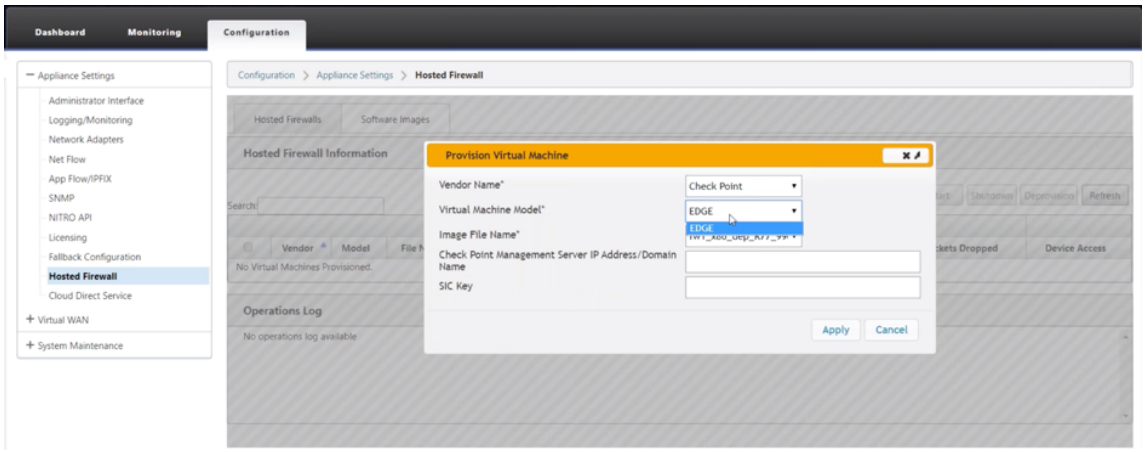
您可以看到一个状态栏来跟踪上载过程。图像成功上载后，文件详细信息会反映。无法删除用于预配的映像。不要执行任何操作或返回到任何其他页面，直到图像文件显示 100% 上载。

3. 对于预配，请选择 托管防火墙 选项卡 > 单击 置 备按钮

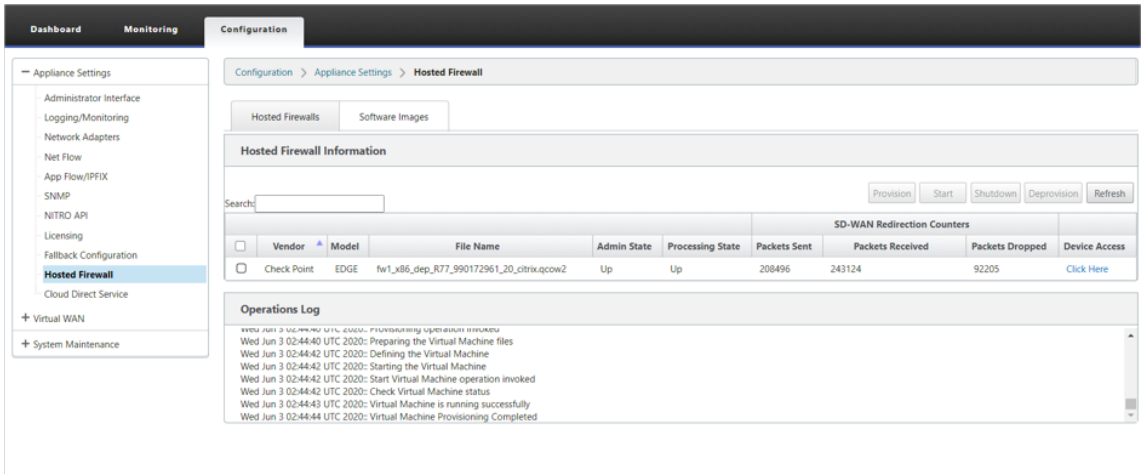


4. 请提供以下详细信息以供 Provisioning。

   - 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。

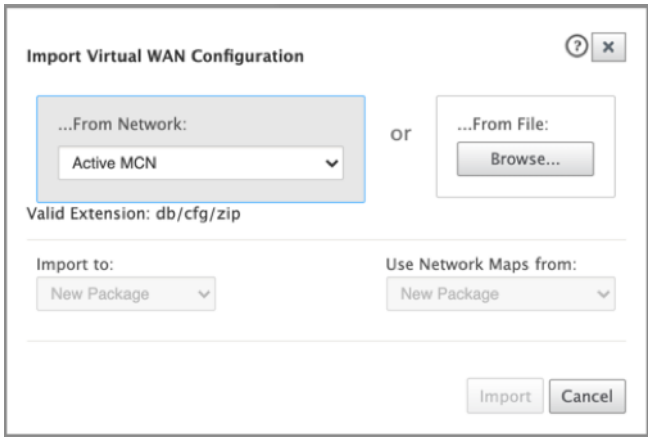
> 注意
>
> 始终使用隐身模式访问检查点 GUI。

将流量重定向到边缘

流量重定向配置可以通过 MCN 上的配置编辑器或 SD-WAN 中心上的配置编辑器完成。

要浏览 SD-WAN 中心的配置编辑器，请执行以下操作：

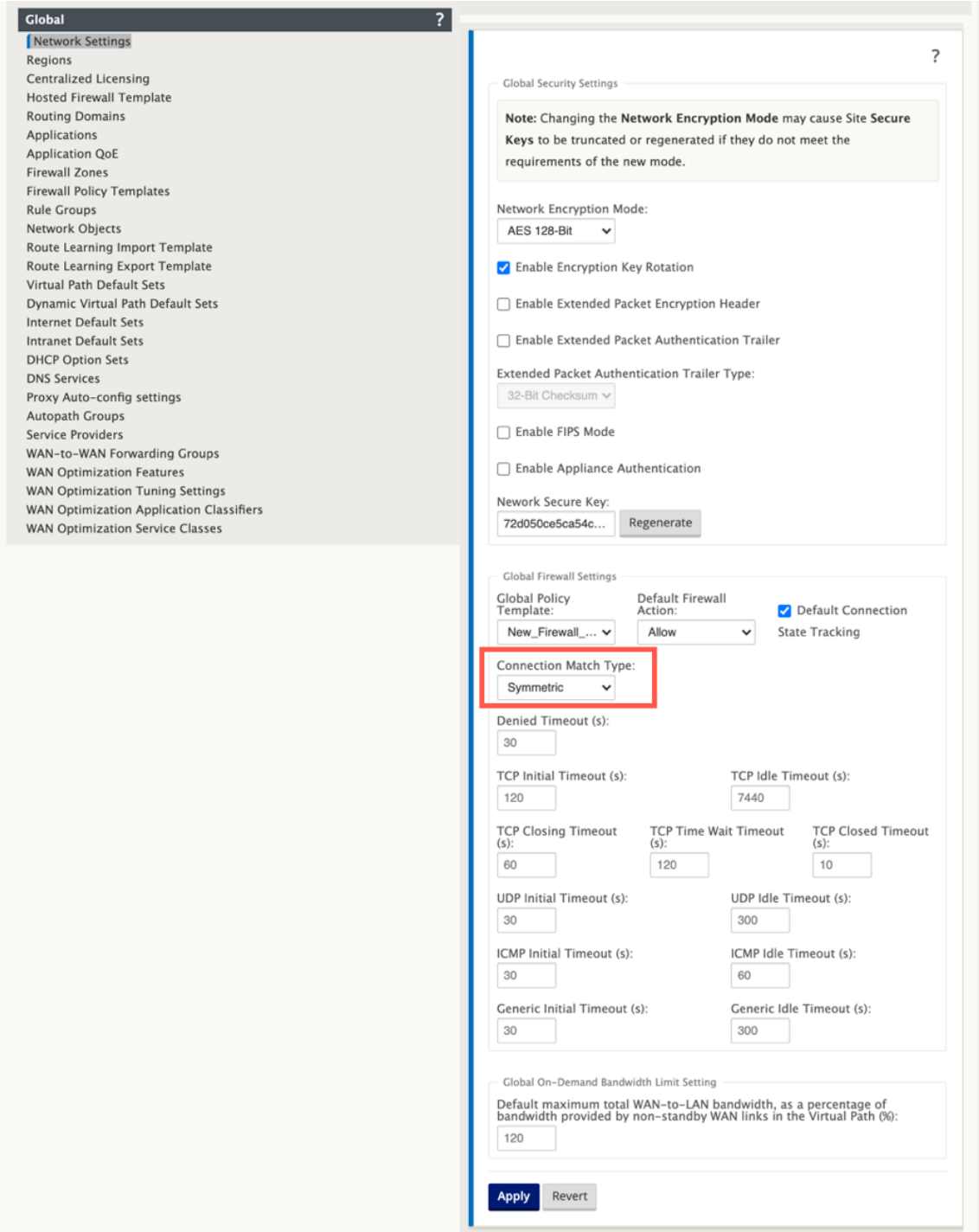
1. 打开 Citrix SD-WAN Center UI，导航到 配置 **>** 网络配置导入。从活动 MCN 导入虚拟 WAN 配置，然后单击导入。



其余步骤类似于以下步骤-通过 MCN 进行流量重定向配置。

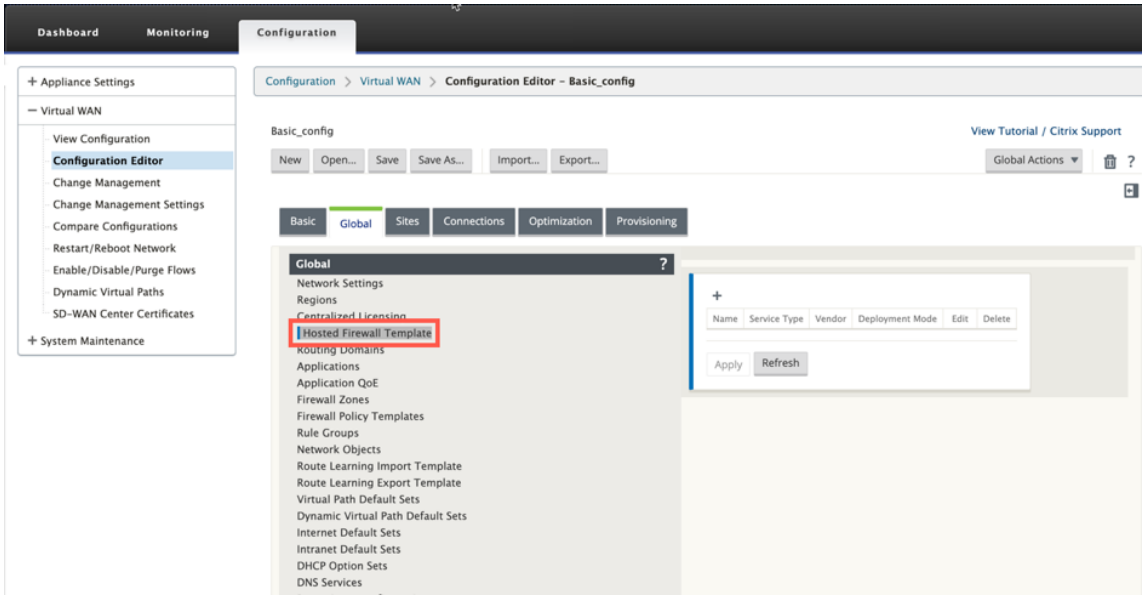
要在 MCN 上浏览配置编辑器：

1. 在 全局 **>** 网络设置下将连接匹配类型设置 为 对称。

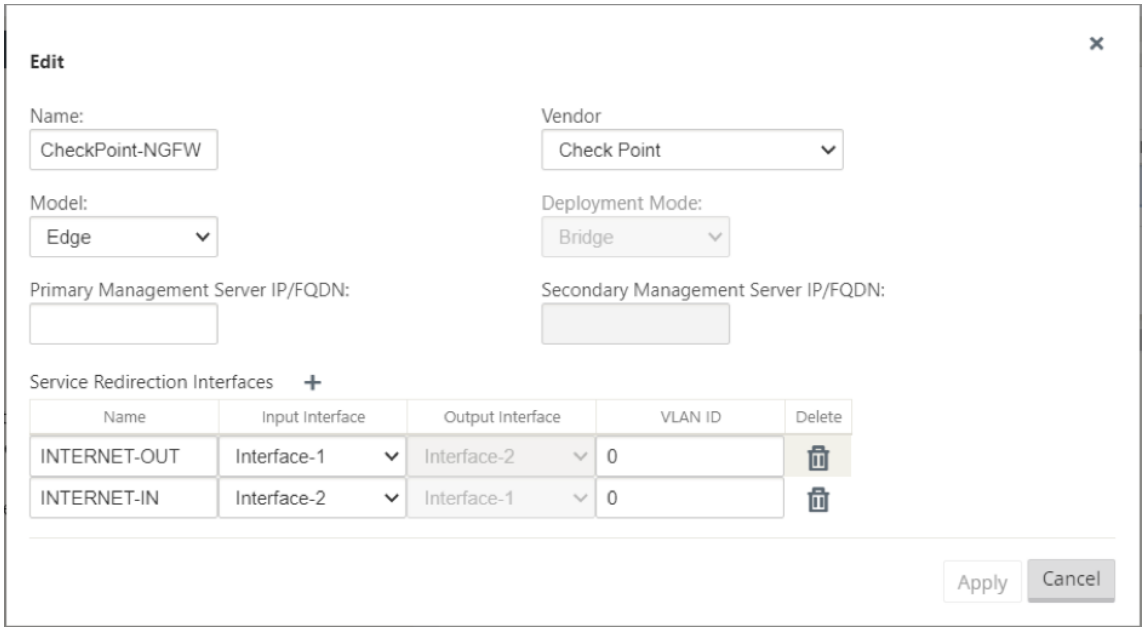


默认情况下，SD-WAN 防火墙策略是特定于方向的。对称匹配类型使用指定的匹配条件来匹配连接，并在两个方向上应用策略操作。

2. 打开 Citrix SD-WAN UI，导航到 配置 **>** 展开虚拟 WAN** 选择 ** 配置编辑器 ** 选择 ** 全局 部分下的 托管防火墙模板。



3. 单击 **+** 并在以下屏幕截图中提供所需信息以添加 托管防火墙模板。单击添加。



托管防火墙模板 允许您配置流量重定向到 SD-WAN 平台上托管的 防火墙虚拟机。以下是配置模板所需的输入：

- 名称：托管防火墙模板的名称。
- 供应商：防火墙供应商的名称—检查点。
- 部署模式：“部 署模式”字段自动填充并显示为灰色。对于 检查点 供应商，部署模式是 **Bridge**。
- 模型：托管防火墙的虚拟机模型。选择供应商作为 检查点后，模型字段将自动填充 E **dge**。
- 主管理服务器 **IP/FQDN**：主管理服务器 IP/FQDN。
- 辅助管理服务器 **IP/FQDN**：辅助管理服务器 IP/FQDN。
- 服务重定向接口：这些是用于 SD-WAN 和托管防火墙之间的流量重定向的逻辑接口。

> 注意：
>
> 必须从连接启动器方向选择重定向输入接口，为响应流量自动选择输出接口。例如，如果出站 Internet 流量被重定向到接口 1 上的托管防火墙，则响应流量将自动重定向到接口 2 上的托管防火墙。此外，如果没有互联网入站流量，则不需要接口-2。

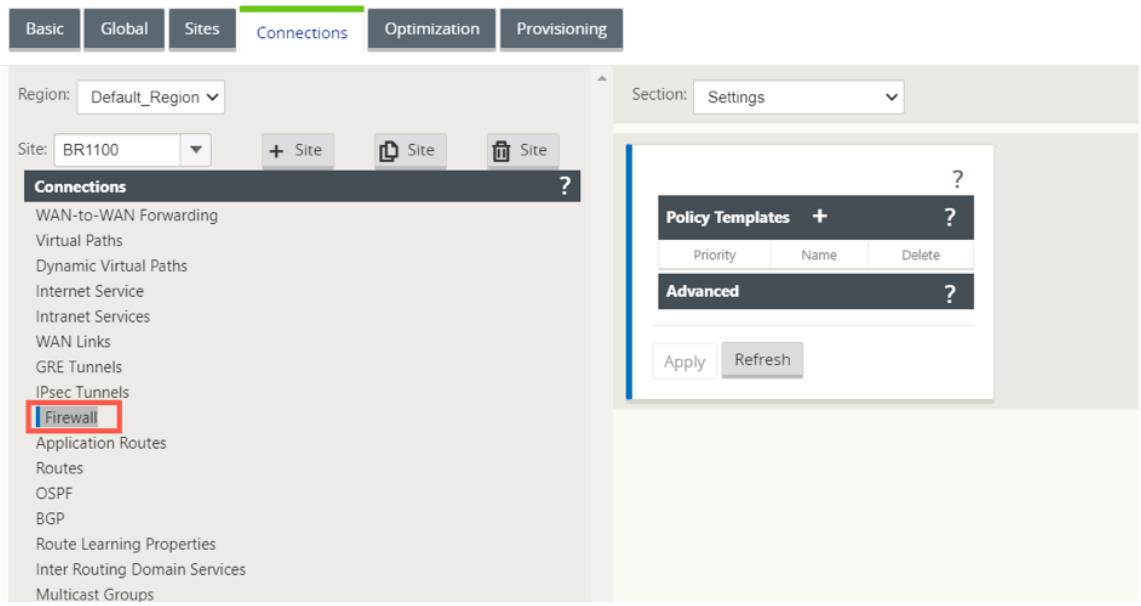
只有两个数据接口分配给 Check Point 虚拟机。

> 注意：
>
> SD-WAN 防火墙策略是自动创建的，以 允许 来自托管的防火墙管理服务器的流量。这样可避免发自（或）发往托管防火墙的管理流量的重定向。

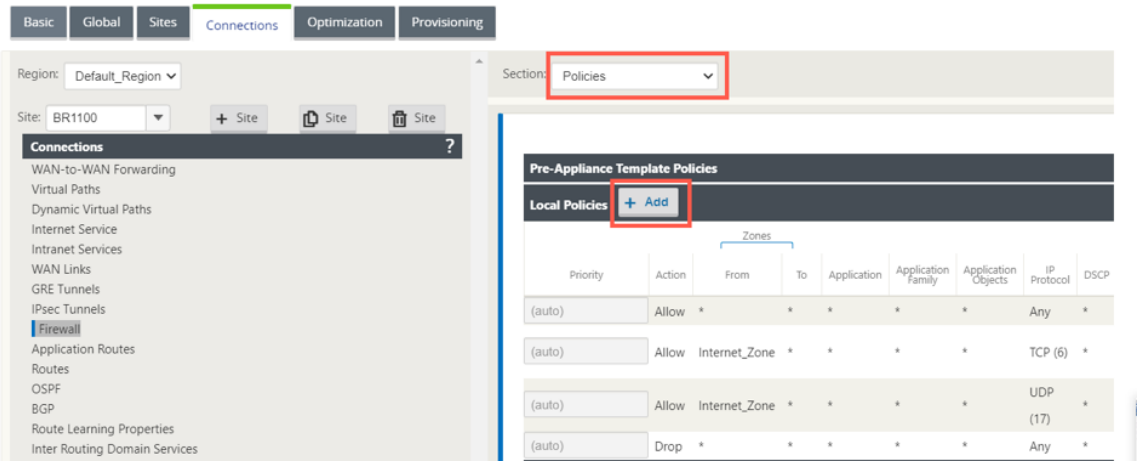
可以使用 SD-WAN 防火墙策略将流量重定向到防火墙虚拟机。有两种方法可以创建 SD-WAN 防火墙策略-通过“全局”部分中的防火墙策略模板或在站点级别创建。

方法**-1**

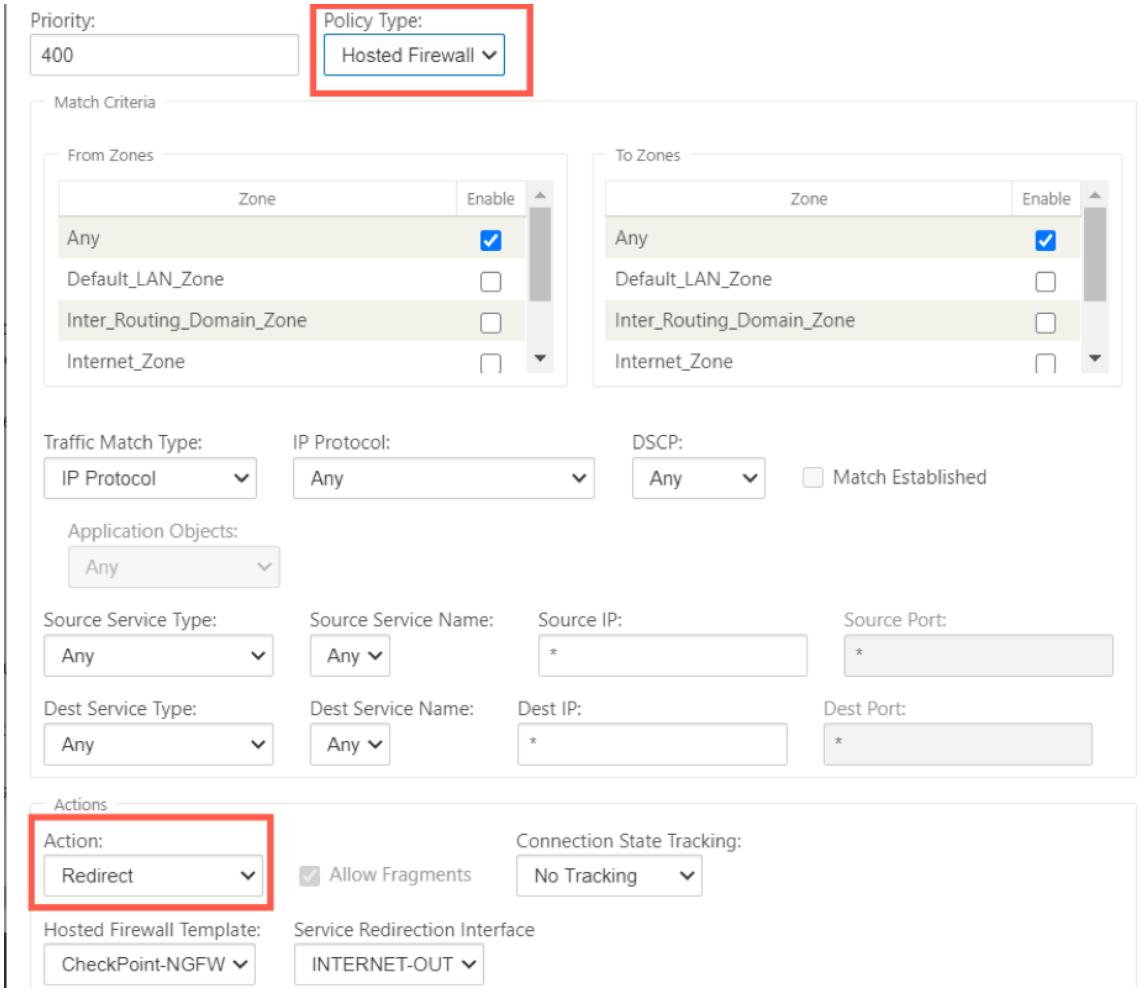
1. 在 Citrix SD-WAN GUI 中，导航到 配置 **>** 展开 虚拟 **WAN >** 配置编辑器。在 连接 下选择 防火墙。



2. 从 部分 下拉列表中选择 策 略，然后单击 **+** 添加 以创建防火墙策略。

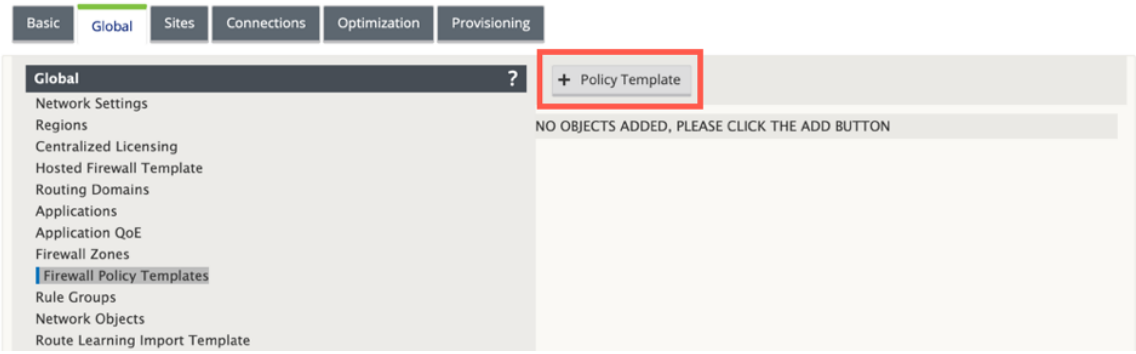


3. 将 策略类型 更改为 托管防火墙。操作字段自动填充为“重定向”。从下拉列表中选择 托管防火墙模板 和 服务重定向接口。单击添加。

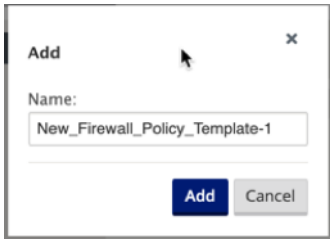


方法-**2**

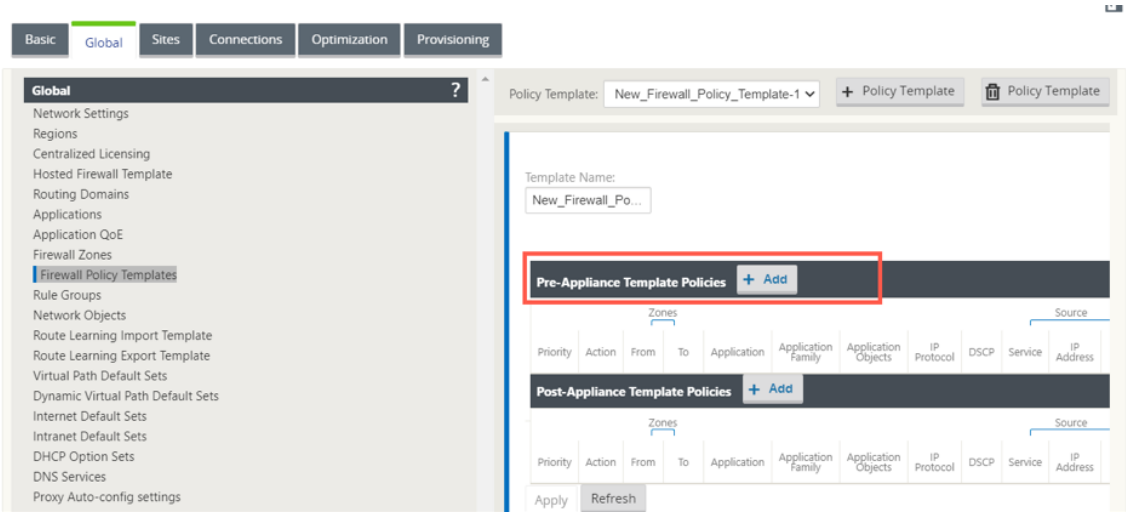
1. 导航到 全 局选项卡，然后选择 防火墙策略模板。单击 **+** 策略模板。



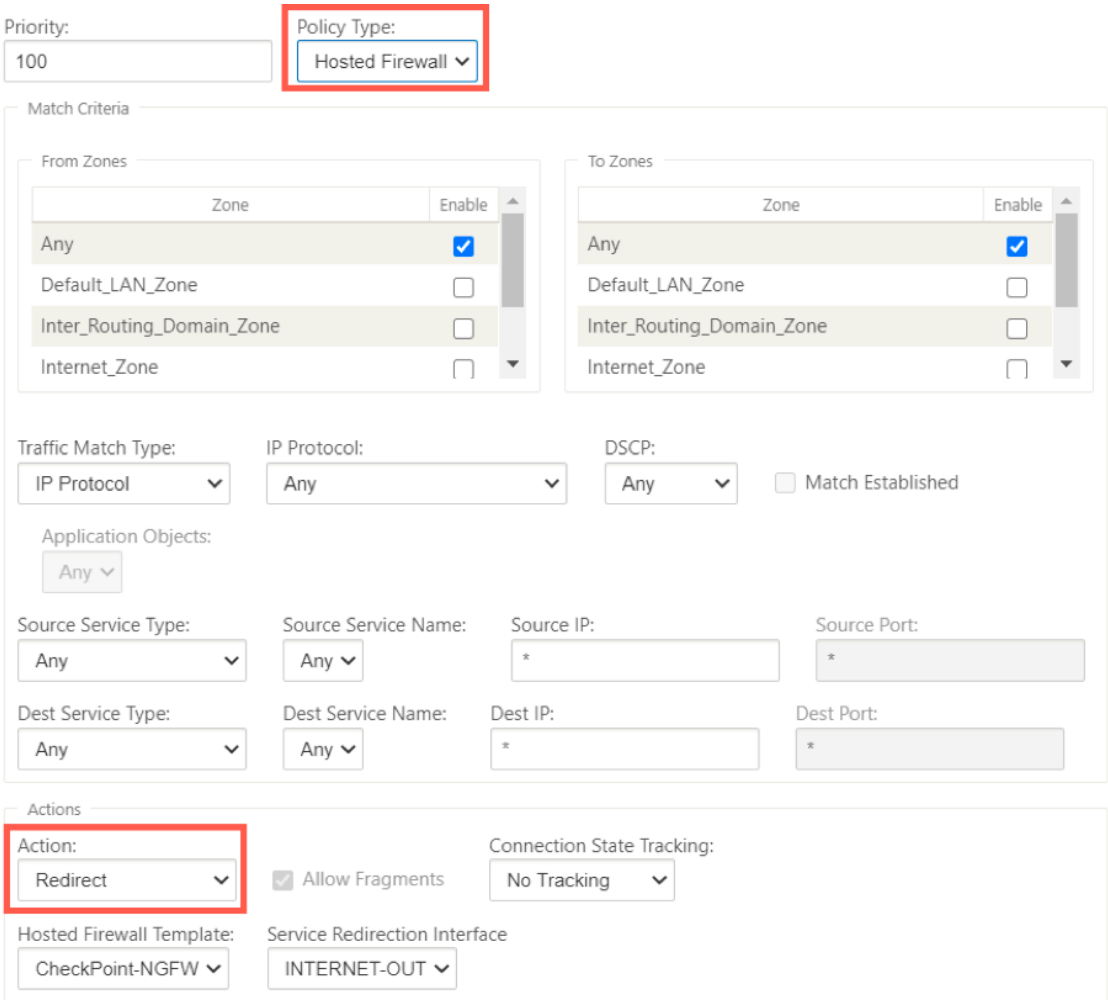
2. 为策略模板提供名称，然后单击 添加。



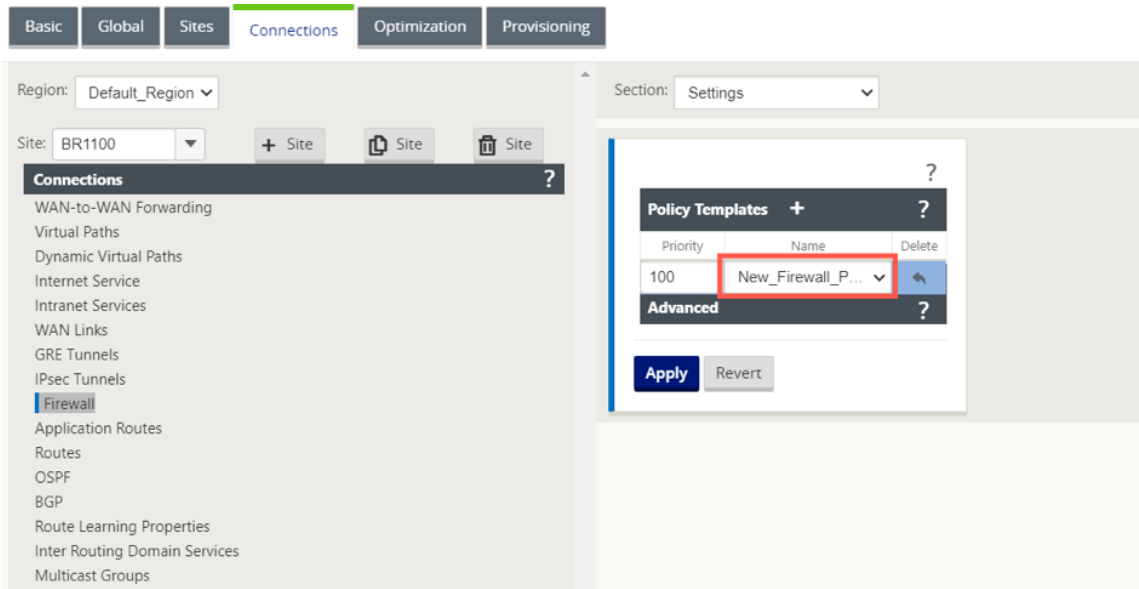
3. 单击“装置前模板策略”旁边的 **+** 添加。



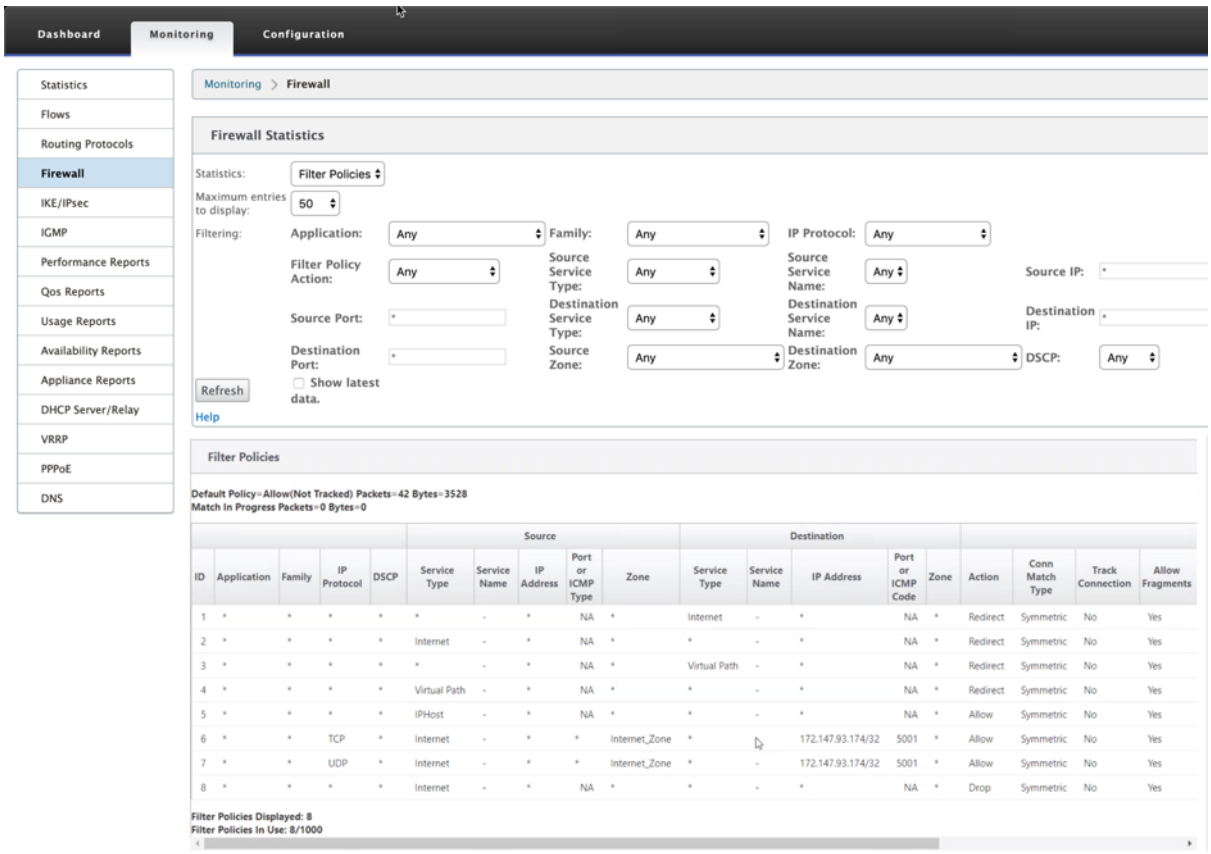
4. 将 策略类型 更改为 托管防火墙。“操作”字段将自动填充为 “重定向”。从下拉列表中选择 托管防火墙模板 和 服务重定向接口。单击添加。



5. 导航到“连接” > “防火墙”，然后在“名称”字段下选择防火墙策略（您创建的）。单击应用。



当所有网络配置处于启动状态并运行模式时，您可以在监视 > 防火墙 > 统计列表下监控连接，选择筛选策略。



链路聚合组

November 1, 2021

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 410 SE

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

LACP LAG 功能在以下平台上不可用：

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

> 注意
>
> VPX/VPXL 平台上不支持 LAG 功能。

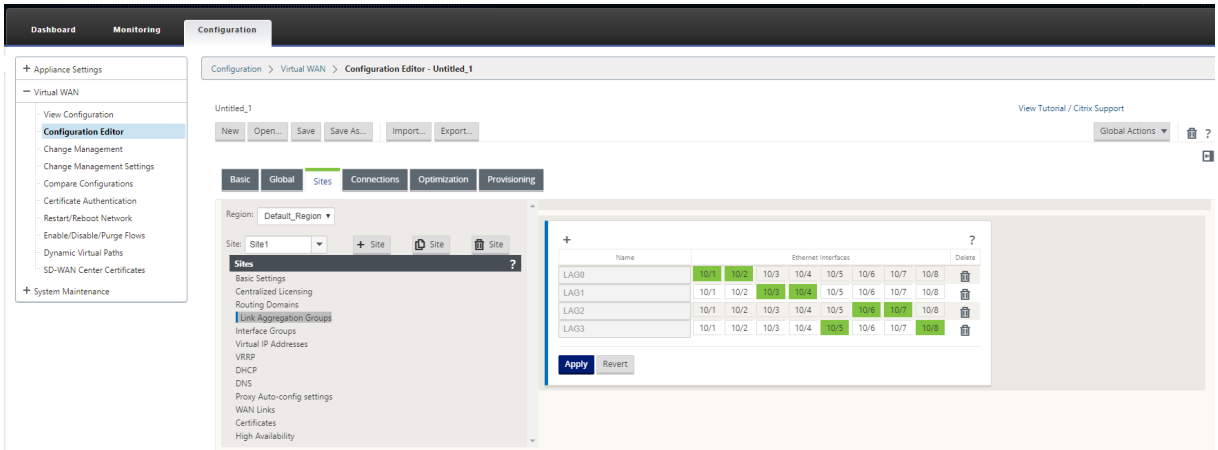
限制

- 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。

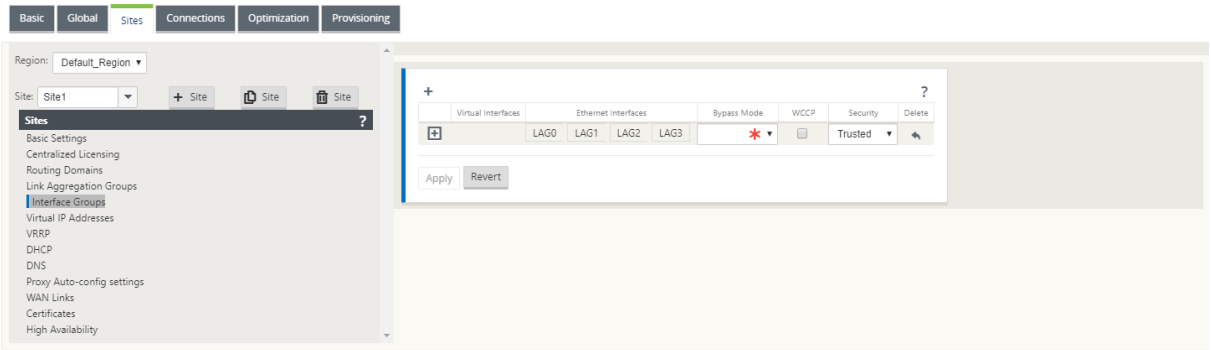
随着 11.3 版本的开始，在使用 LACP 实施的 SD-WAN 中，端口始终处于活动模式。这意味着 SD-WAN 始终可以开始谈判。

> 注意
>
> 对于 Citrix SD-WAN 210 和 410 设备，您只能创建一个 LAG，其中最多可分组三个端口。

要配置链接聚合组，请在 配置编辑器中导航到 站点 > 链接聚合组。您可以查看所有可用的物理端口和以太网接口。单击 **+** 创建 LAG。



选择成员端口，然后单击 应用。将端口添加到 LAG 后，您只能看到 接口组 中的 LAG，而不能看到成员端口。

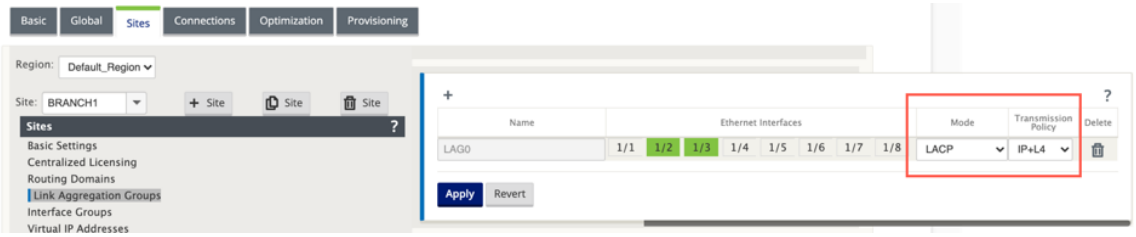


同样，如果要使用 LACP 模式配置 LAG：

1. 单击 **+** 创建 LAG 并选择以太网接口端口。
2. 从下拉列表中选择配置模式作为 **LACP** 。
3. 从下拉列表中选择 传输策略。

   > 注意：
   >
   > 如果该模式被选为“主动备份”，则“传输策略”字段将被禁用。

4. 单击应用。



由于 LAG 组有许多端口，因此 传输策略 有助于选择可用于发送流量的端口。只有聚合模式为“主动-主动”时，才能启用传输策略字段。定义了两个传输策略——MAC +IP 和 IP+L4。

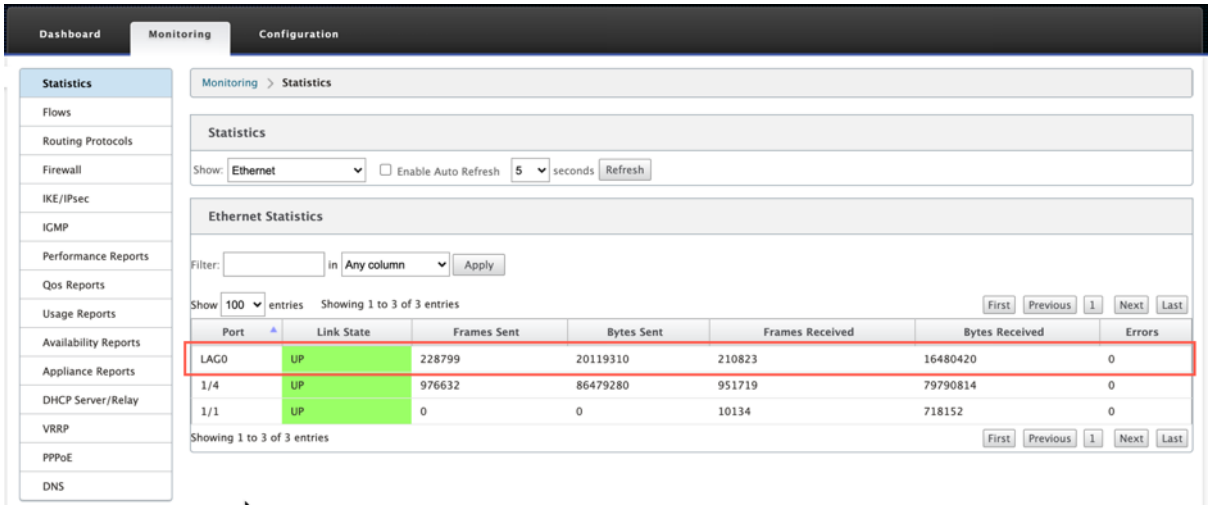
- **MAC+IP**：给定数据包的链路选择基于第 2 层和第 3 层参数。因此，源和目标 MAC 和 IP 地址采用这些参数并哈希它们。根据哈希，它选择端口。
- **IP+L4**：IP+L4 策略基于源 IP 和目标 IP 以及第 4 层端口和协议。IP+L4 策略通知哪个数据包正在通过哪个端口。
  具有相同参数的数据包将始终在其中一个链路上发送。这意味着，相同或单个流（相同的源和目标 Mac 和 IP）始终通过相同的端口，而不会在其他端口上分布。作为一项好处，无序数据包无法到达目的设备

您可以使用 LAG 创建虚拟接口，这些接口将进一步用于配置 LAN/WAN 链接和 HA。

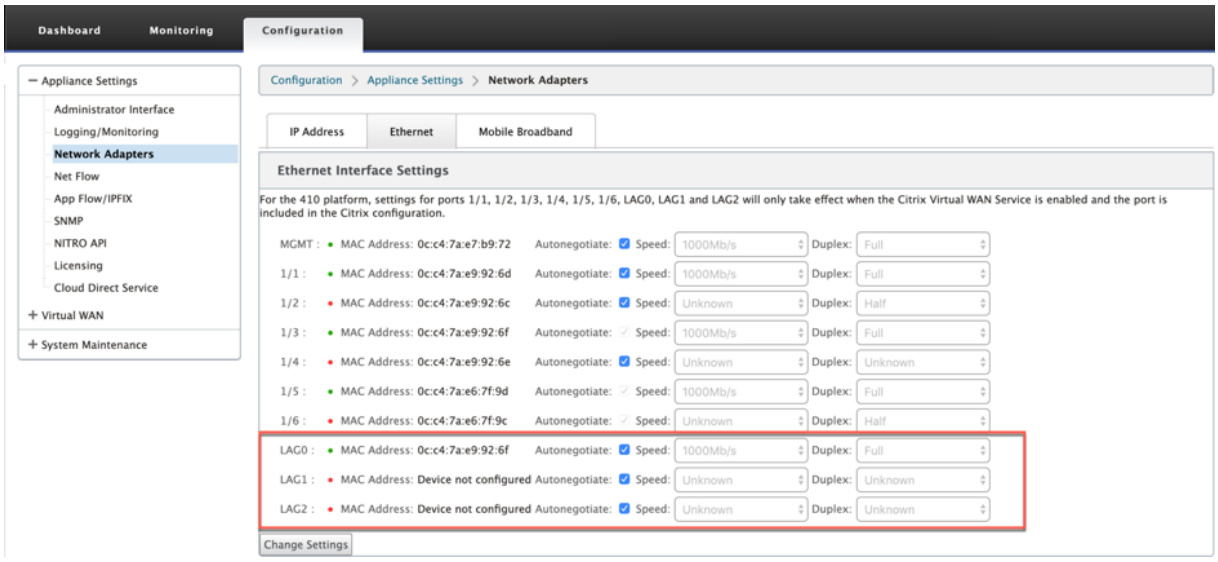
> 注意
>
> 如果在 接口组中将 LAG 用作以太网接口，则不支持链路状态传播 (LSP) 功能。

监视和故障排除

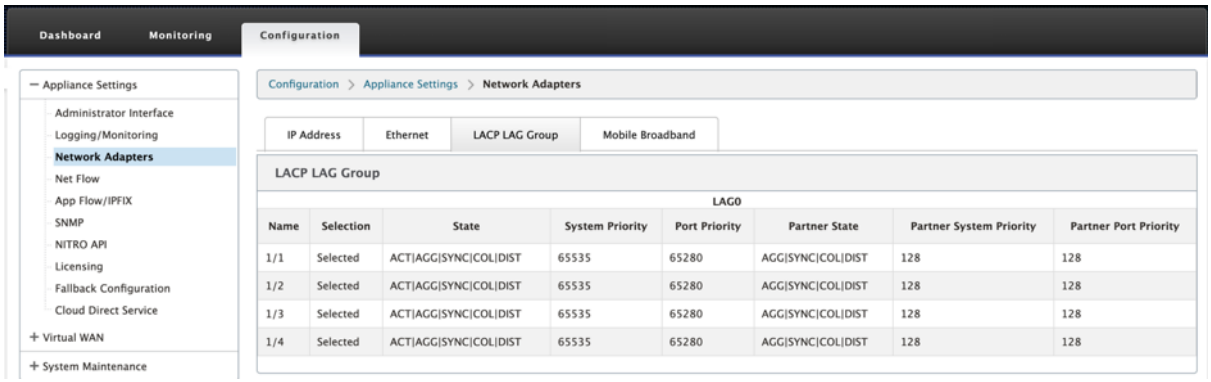
要查看统计信息或链接状态，请导航到 监视 **>** 统计信息。从 显 示下拉列表中选择 以太网。



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。

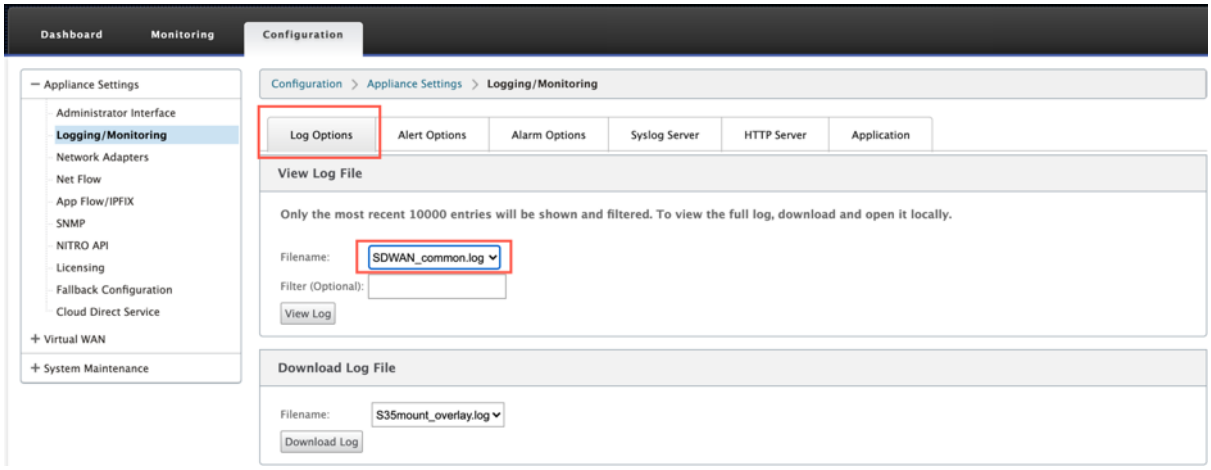


选择 L **ACP LAG Grou** p 选项卡以查看与 LACP LAG 组相关的各种详细信息。



> 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

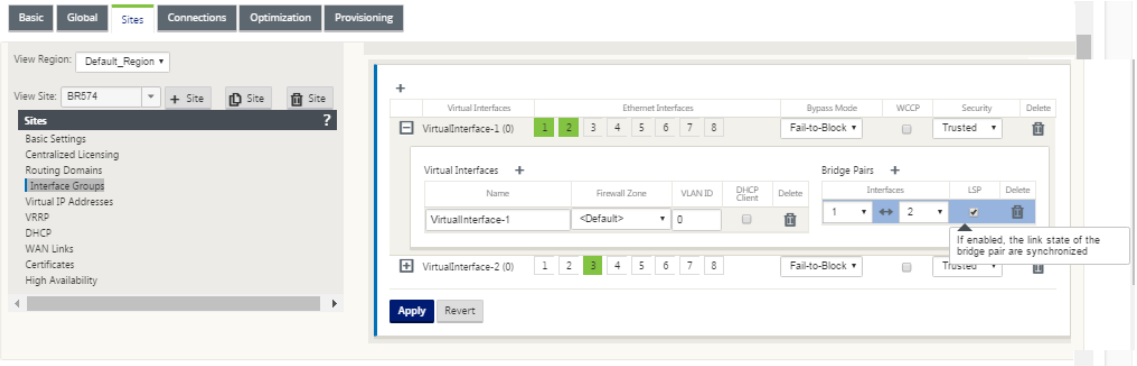
June 22, 2021

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，允许链路另一侧连接的设备在链路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，耦合链接将以管理方式取消激活。如果您的网络架构包含并行故障转移网络，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。

如何配置链路状态传播

要配置链路状态传播，请执行以下操作：

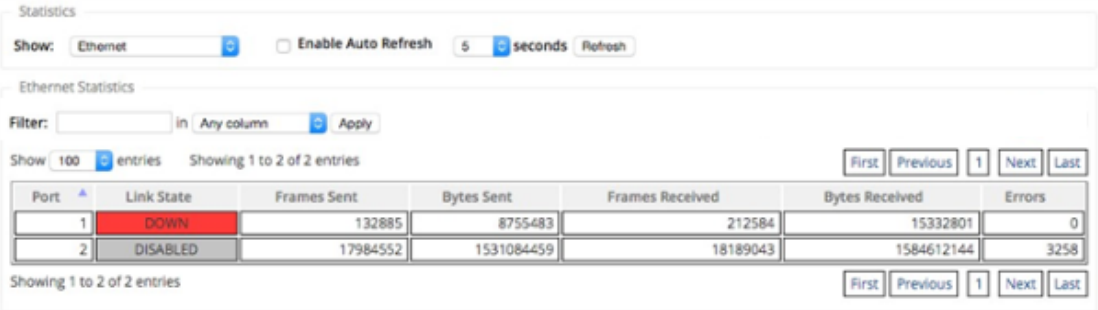
1. 导航到 配置编辑器 > 站点 > **[**站点名称**]** > 接口组。
2. 展开虚拟接口，然后在网桥对下单击 **LSP** 复选框以启用网桥对的链路状态传播。单击应用以保存设置。



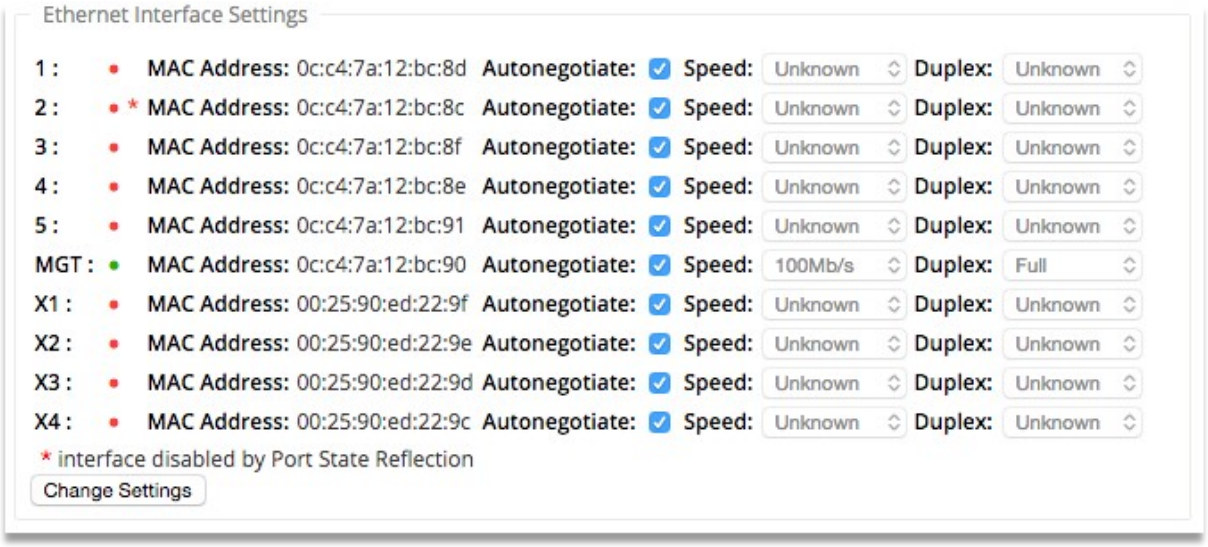
监测链接统计

要监视链接统计信息，请执行以下操作：

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，以查看已启用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 > 设备设置 > 网络适配器 > 以太网选项卡。以太网接口设置列表中的红色星号 (*) 表示以管理方式下降的端口。



计量和备用 **WAN** 链接

June 22, 2021

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、宽带互联网、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（公共互联网/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。此使用警告事件也可以在 SD-WAN 中心查看。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 -待机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 -待机路径处于非活动状态时使用的心跳间隔（默认值 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-按 需备用路径在以下之间形成：
  - 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 非待机、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）。

具有禁用检测信号的备用路径的路径状态假定为 好，并且在 监视 下的 路径统计 表中显示为 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）。

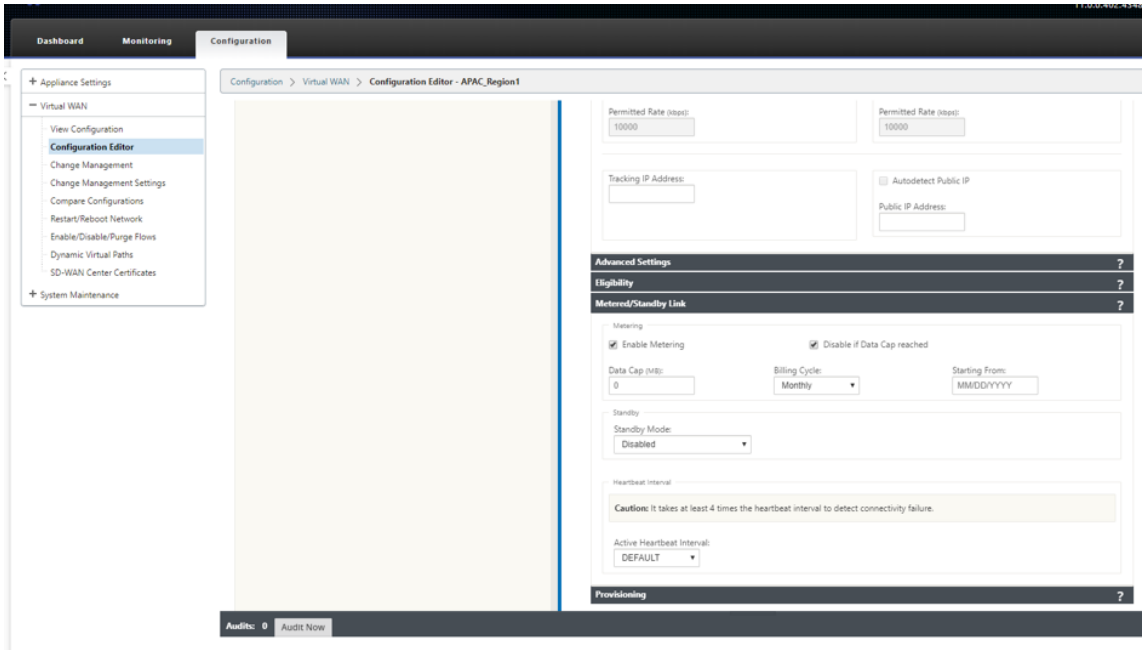
当备用路径在备用路径和活动之间转换时，会生成事件和日志消息。

配置先决条件：

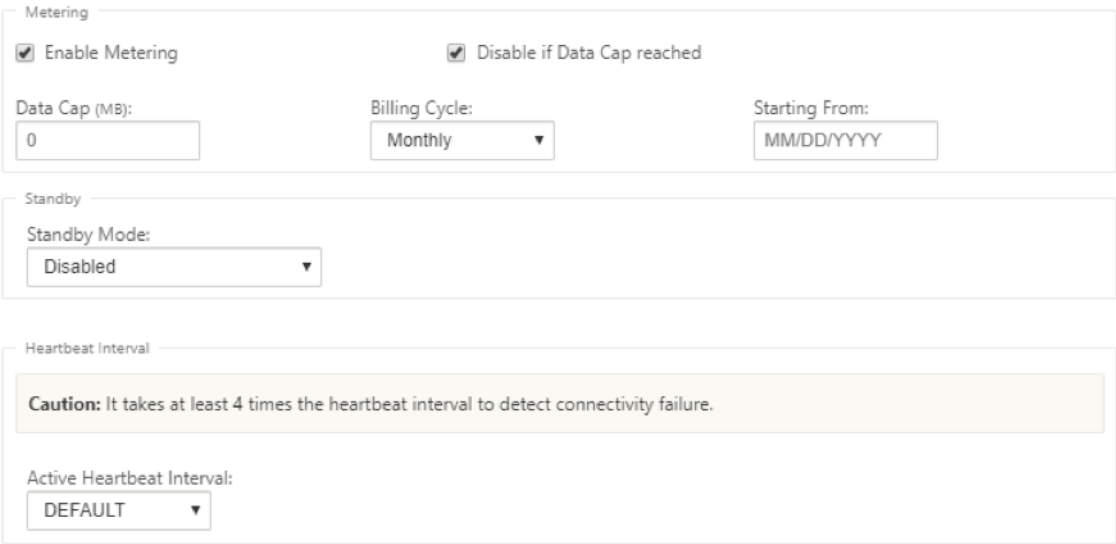
- 仪表链接可能是任何访问类型。
- 站点上的所有链接都可以在启用计量的情况下进行配置。
- 备用链接可能是公共 Internet 或专用 Intranet 访问类型。私有 MPLS 访问类型的 WAN 链接无法配置为备用链接。
- 每个站点必须至少配置一个非备用链接。每个站点最多支持 3 个备用链路。
- 可能不会在按需备用链接上配置 Internet/内联网服务。按需备用链接仅支持虚拟路径服务。
- Internet 服务可能在最后的备用链接上配置，但仅支持负载平衡模式。
- Intranet 服务可能在最后的备用链接上配置，但仅支持辅助模式，并且必须启用主回收。

要配置按计费链接，请执行以下操作：

1. 在 SD-WAN Web 管理界面中，导航到 配置 **>** 虚拟 **WAN >** 选择 配置编辑器 **>** 添加或从下拉列表中选择 站点 > 选择 **WAN** 链接 **>** 单击 流星**/**备用链接 选项卡以展开它。



2. 选中 启用计量 复选框。您可以为“数据上限”、“开单周期开始日期”、“已使用的近似用量”和“活动检测信号间隔提供值。



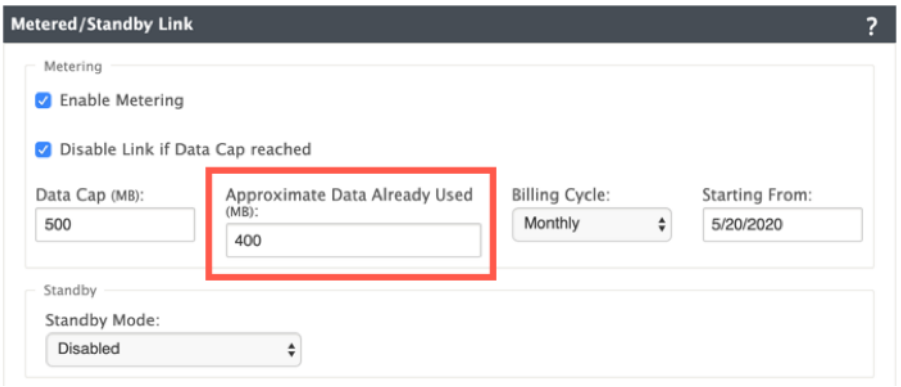
3. 如果达到数据上限，则禁用链接：

   - 如果选中了“在 达到数据上限时禁用链接”复选框，则 在数据使用量达到数据上限时，计费链接及其所有相关路径将被禁用，直到下一个计费周期。
   - 默认情况下，如果达到数据上限，则禁用链接 复选框将处于未选中状态，该复选框将保留当前模式或状态，以便在达到数据上限后继续进行计费链接，直到下一个计费周期。

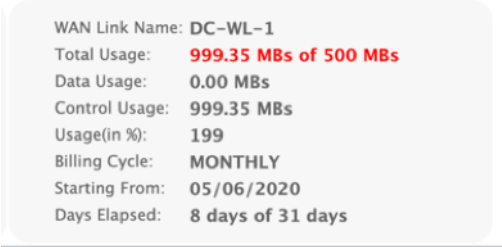
4. 如果配置了按流量计费的链路，则可以为按流量计费的链路提供已使用的近似数据（以 MB 为单位）。

   要跟踪正确的计费链接使用情况，如果该链接已在当前计费周期中使用了某些天，则必须在按计费链接上输入大

致使用情况。这种近似用法仅适用于第一个周期。计算开始日期至当前日期的总使用量，并显示在仪表板中。

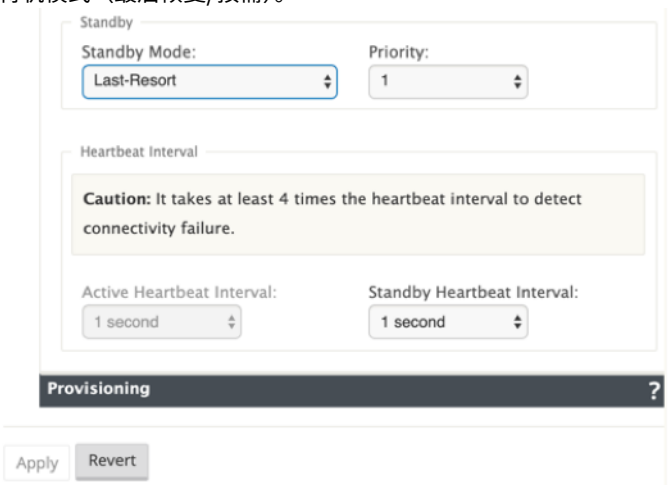


执行配置更新后，您可以在仪表板上查看使用详细信息。

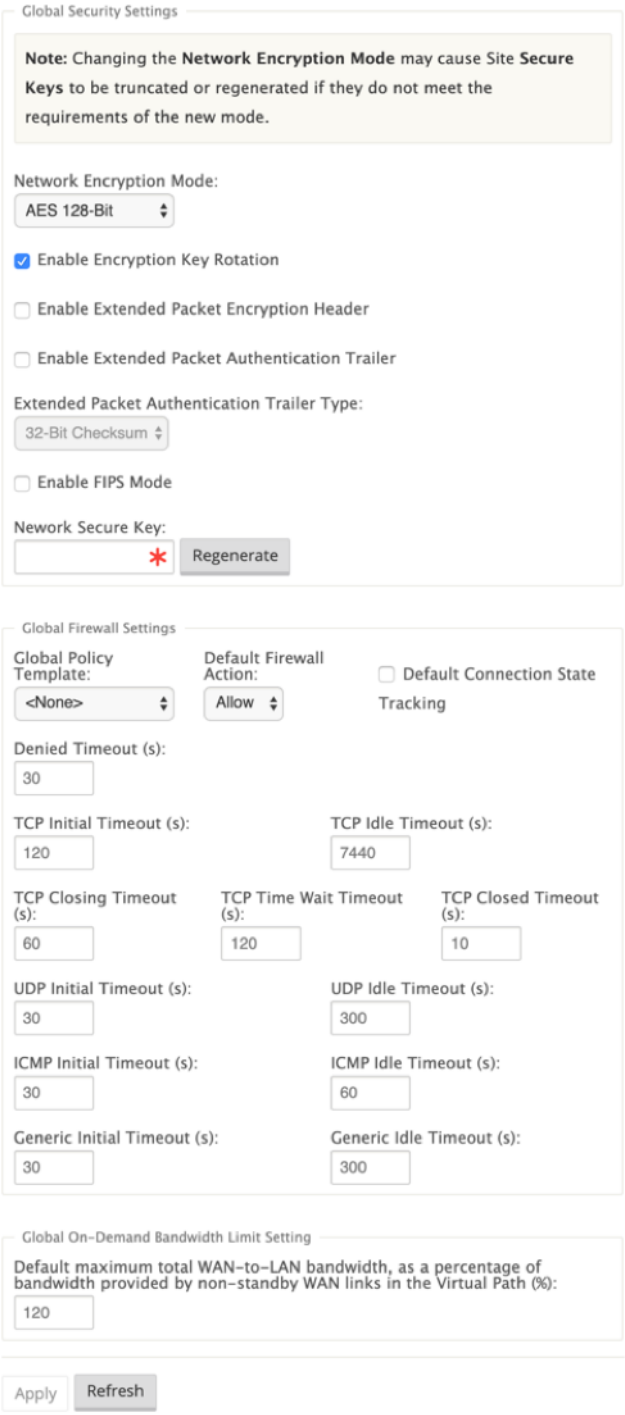


要配预配用链接，请执行以下操作：

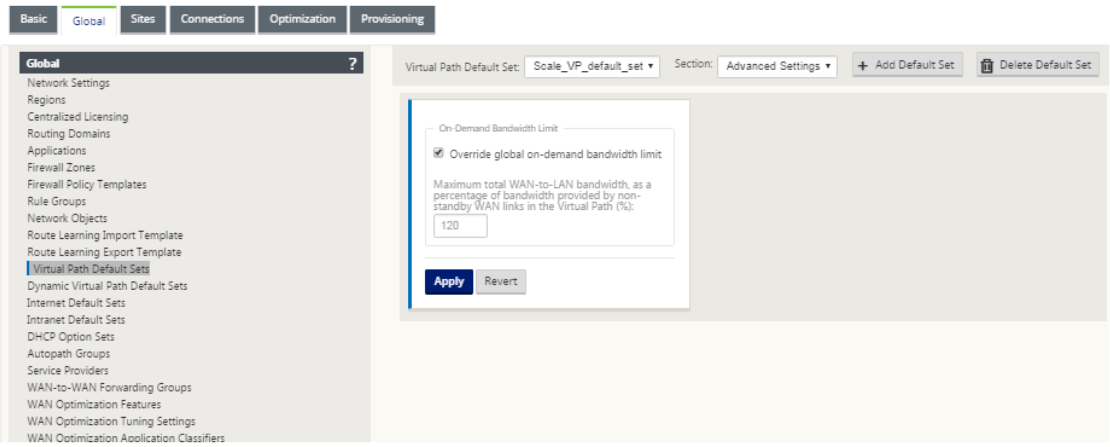
1. 默认情况下，WAN 链路的待机模式处于禁用状态。要将 WAN 链接配置为待机状态，请从下拉列表中选择一种待机模式（最后恢复/按需）。



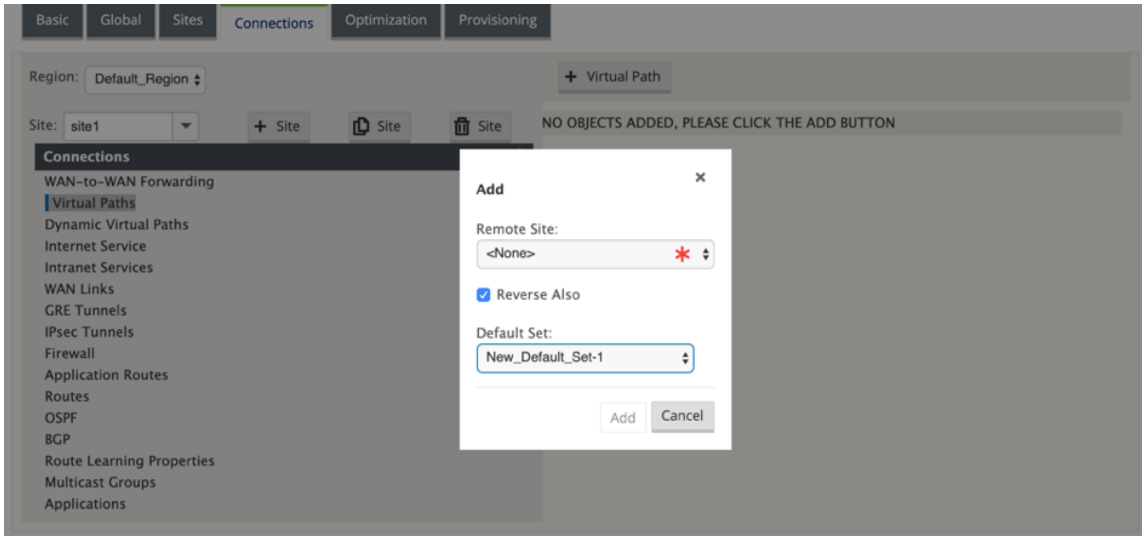
2. 选择待机模式后，根据需要选择待机优先级、活动心跳间隔和待机心跳间隔。单击 应用 以验证配置。
3. 如果配置了按需备用链路，则将对虚拟路径应用全局默认按需带宽限制 (120%)。这指定了虚拟路径允许的最大 WLAN 带宽。它以虚拟路径中所有非备用链路提供的总带宽的百分比表示。只要虚拟路径中的可用带宽低于限制，并且有足够的使用率，设备就会尝试激活按需路径以补充带宽。
4. 要查看或更改全局默认按需带宽限制，请打开 全局 > 虚拟 **WAN** 网络 设置 部分。



5. 如果要应用特定于虚拟路径的按需带宽限制并保持全局默认设置不变，则必须创建虚拟路径默认设置，并且可以更改高级设置中的按需带宽限制。

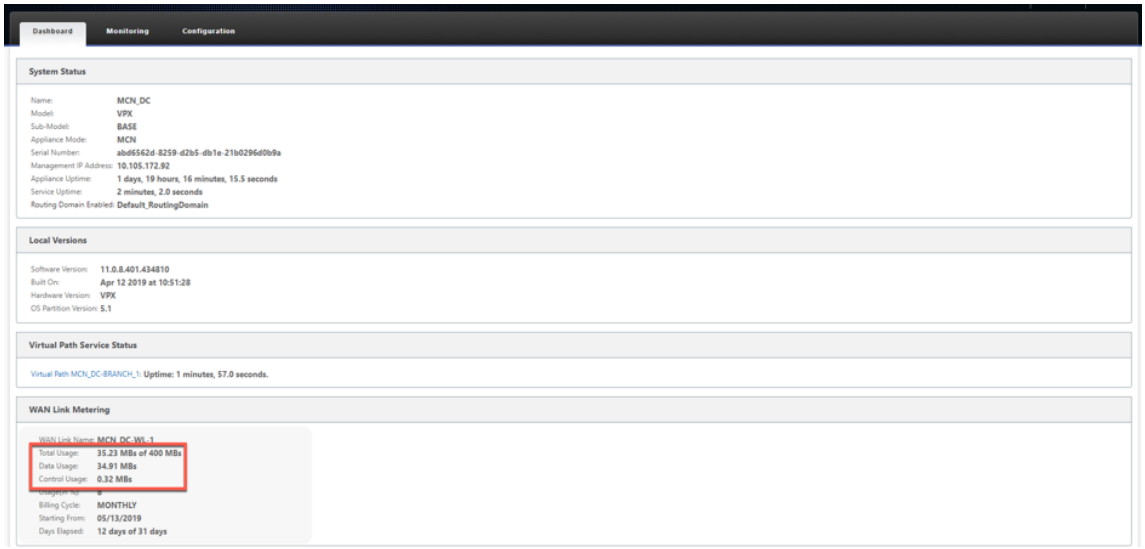


6. 要应用特定虚拟路径的设置，请导航到 连接 **>** 虚拟路径 部分，然后单击 **+** 虚拟路径。

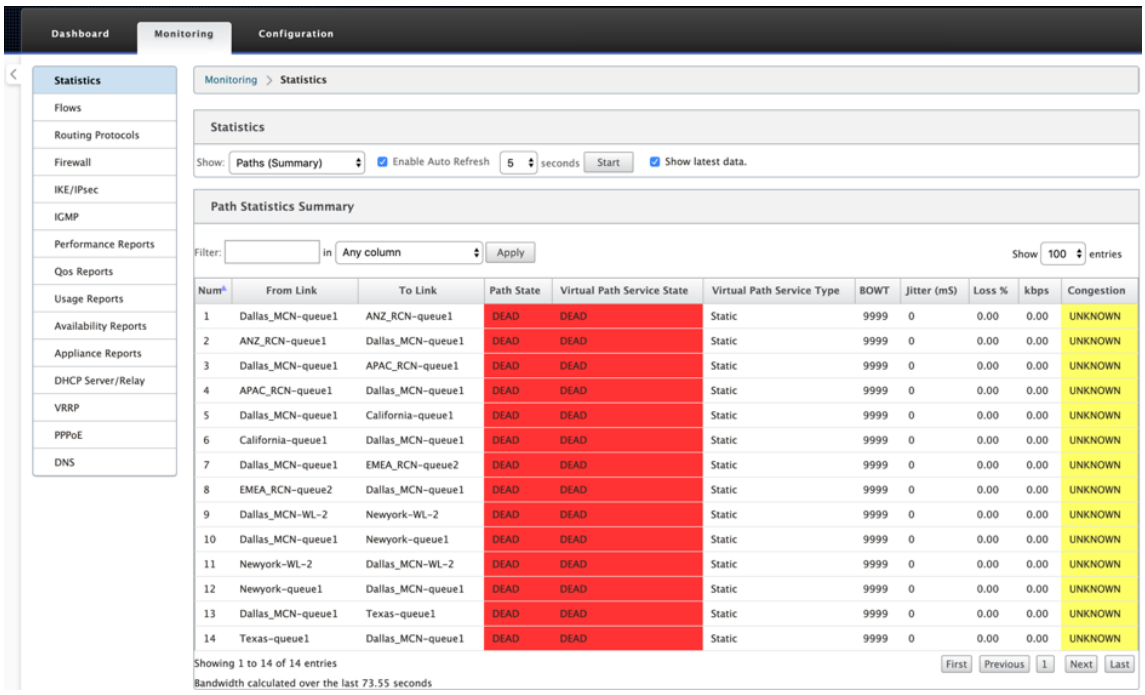


监视计量和备用 **WAN** 链接

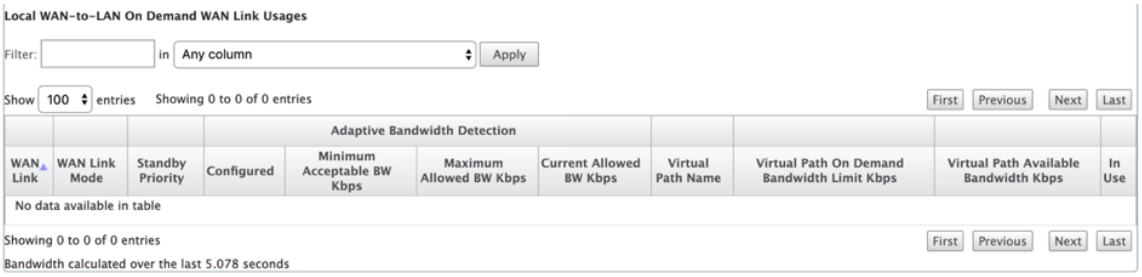
- 控制面板 页面提供以下 **WAN** 链接计量 信息和使用值：
  - **WAN** 链接名称：显示 WAN 链接名称。
  - 总使用量：显示总流量使用量（数据使用量 + 控制使用量）。
  - 数据使用情况：按用户流量显示使用情况。
  - 控制使用情况：通过控制流量显示使用情况。
  - 使用率（以**%** 为单位）：以百分比（总使用量/数据上限）x 100 显示已使用的数据上限值。
  - 计费周期：计费频率（每周/每月）
  - 开始：计费周期的开始日期
  - 已用天数：已用时间（以天、小时、分钟和秒为单位）



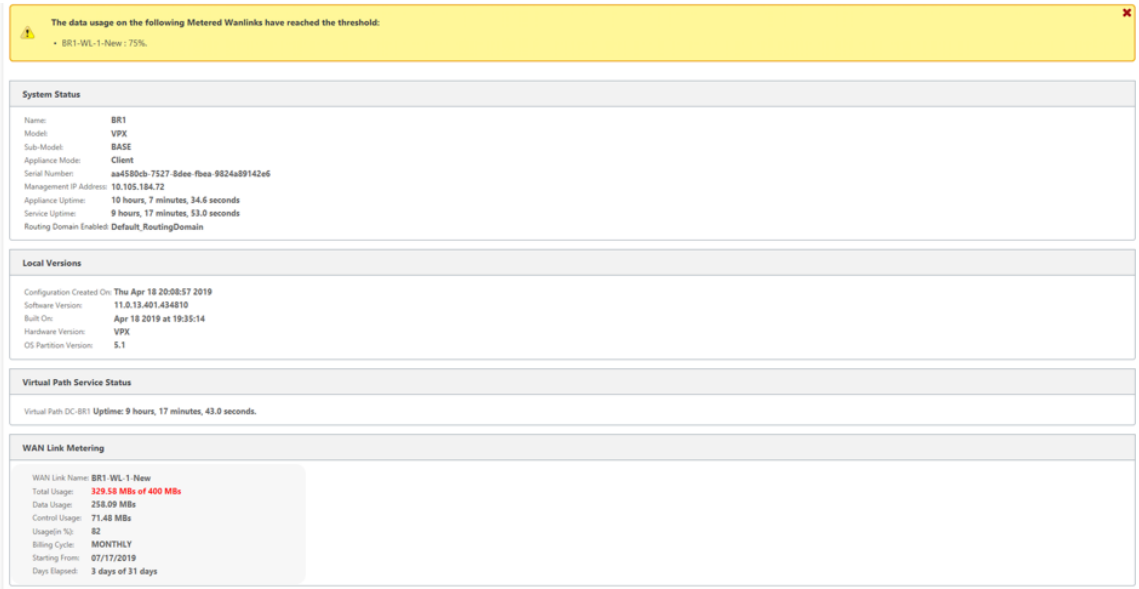
- 显示路径统计信息（监视 **>** 统计信息 **>** 路径）时，按照屏幕截图中所示标记按流量计量的链接和备用链接。



- 如果设备具有本地或远程按需备用链接的虚拟路径，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显示按需带宽的额外表（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，如果使用率超过配置的数据上限的 75%，则会高亮显示朝向控制板底部的数字计量信息。



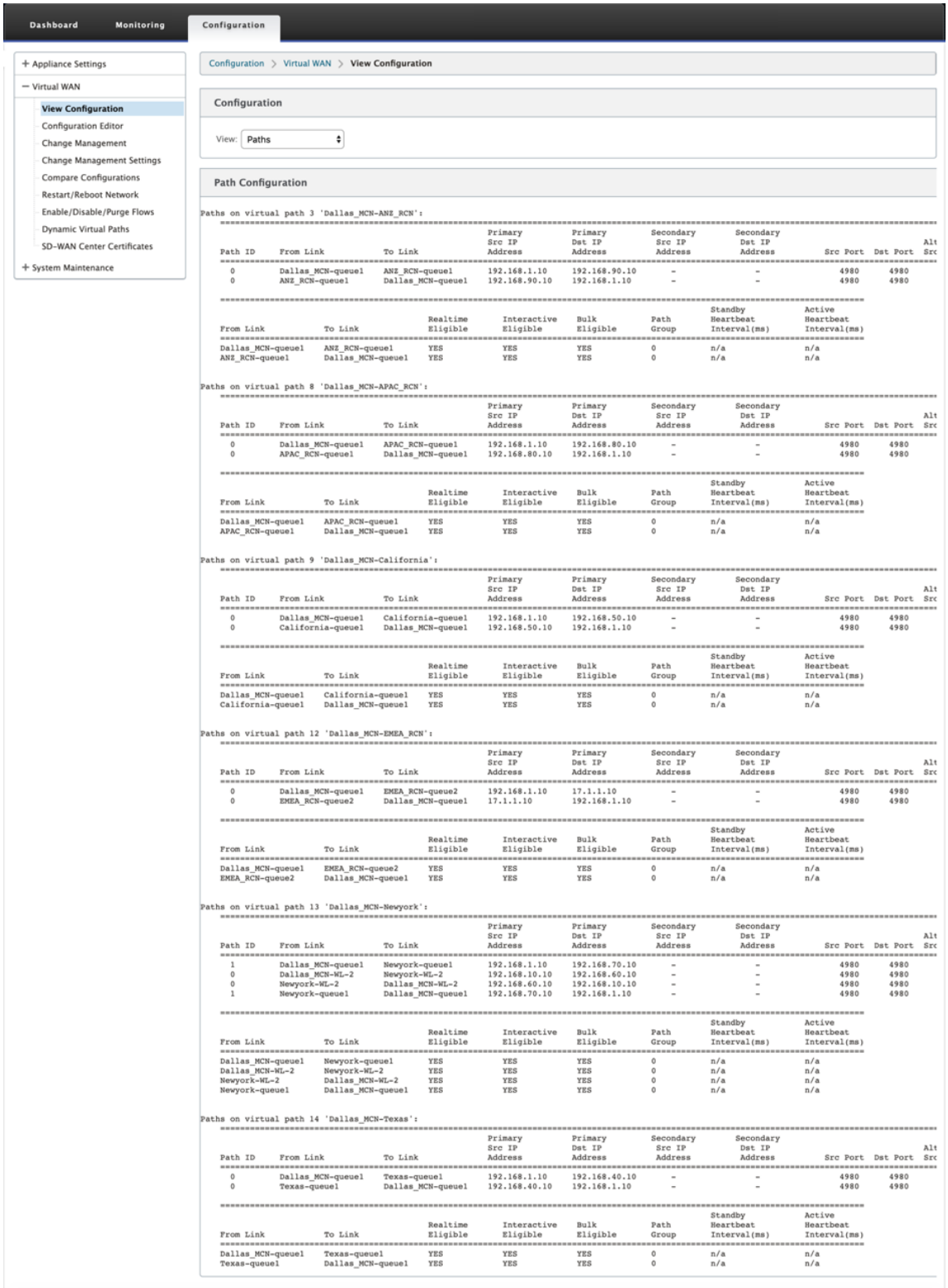
当使用量超过配置数据上限的 50%、75% 和 90% 时，也会在设备上生成 WAN 链路使用情况事件。

17654	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:22:58	USAGE_3	WARNING	Total usage 1.84 GBytes used (91% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17653	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:17:58	USAGE_2	WARNING	Total usage 1.52 GBytes used (75% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017
17652	1	RL-TB-CL1-WL-2	WAN LINK	2017-05-24 10:09:58	USAGE_1	WARNING	Total usage 1.00 GBytes used (50% of limit 2.00 GBytes) in 1 of 31 days in this billing cycle since 00:00:00 05/24/2017

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。

24640	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become standby
24639	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:32	STANDBY	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become standby
24638	1	RL-TB-CL2-WL-1->RL-TB-MCN-WL-2	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-2 state has changed from BAD to GOOD because notified by peer.
24637	2	RL-TB-MCN-WL-2->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24636	2	RL-TB-MCN:RL-TB-CL2	VIRTUAL PATH	2017-05-26 10:18:27	GOOD	NOTICE	The state of Virtual Path RL-TB-MCN-RL-TB-CL2 has changed from BAD to GOOD
24635	0	RL-TB-CL2-WL-1->RL-TB-MCN-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-CL2-WL-1->RL-TB-MCN-WL-1 state has changed from BAD to GOOD because notified by peer.
24634	0	RL-TB-MCN-WL-1->RL-TB-CL2-WL-1	PATH	2017-05-26 10:18:27	GOOD	NOTICE	Virtual Path RL-TB-MCN-RL-TB-CL2 Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-1 state has changed from BAD to GOOD .
24633	3	RL-TB-MCN-WL-2->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-2->RL-TB-CL2-WL-2 has become active
24632	1	RL-TB-MCN-WL-1->RL-TB-CL2-WL-2	PATH	2017-05-26 10:18:27	ACTIVE	ERROR	Virtual Path RL-TB-MCN-RL-TB-CL2 Backup Path RL-TB-MCN-WL-1->RL-TB-CL2-WL-2 has become active

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 1, 2021

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互联网。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互联网连接的 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
- 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。

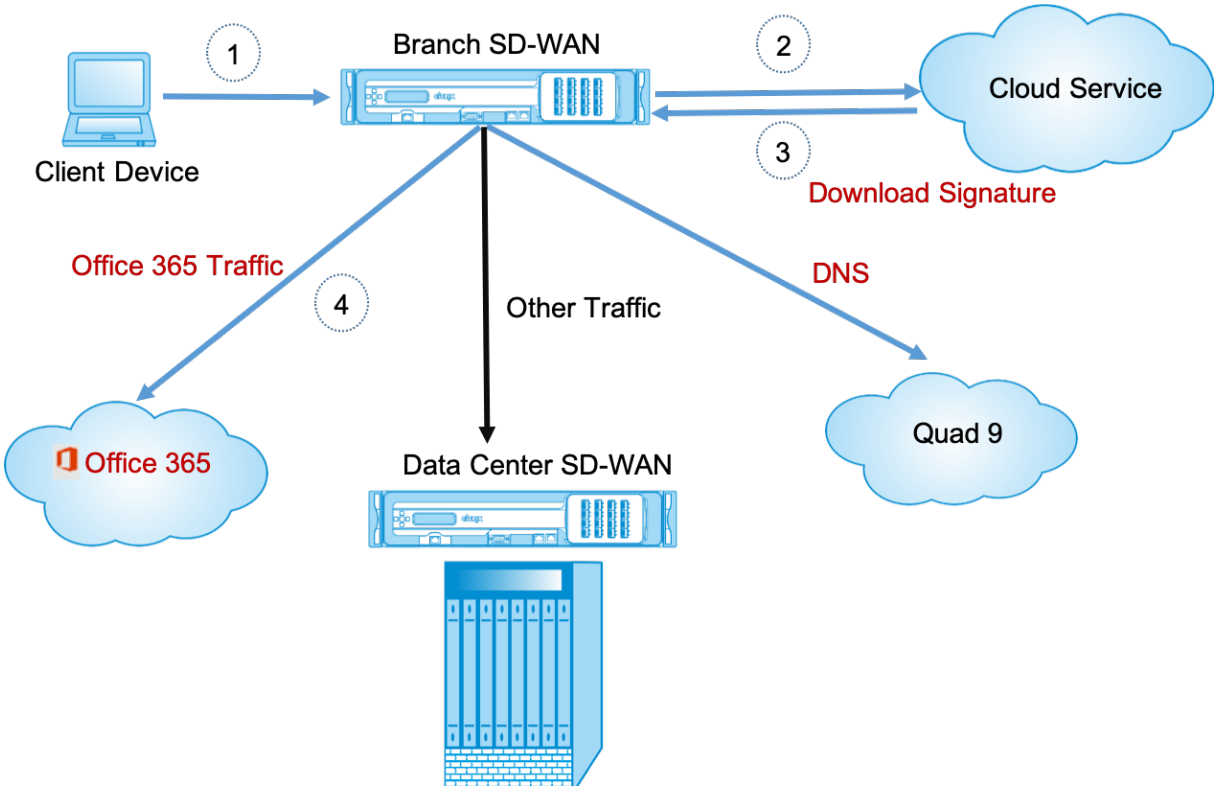
- 默认值 -这些终端节点提供不需要任何优化的 Office 365 服务，并且可以被视为正常的 Internet 流量。其中一些终端节点可能不会托管在 Microsoft 数据中心中。此类别中的流量不容易受到延迟变化的影响。因此，与 Internet 突破相比，直接脱离这种类型的流量不会导致任何性能改进。此外，此类别中的流量可能并不总是 Office 365 流量。因此，建议在网络中启用 Office 365 突破时禁用此选项。

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。

配置 **Office 365** 分组

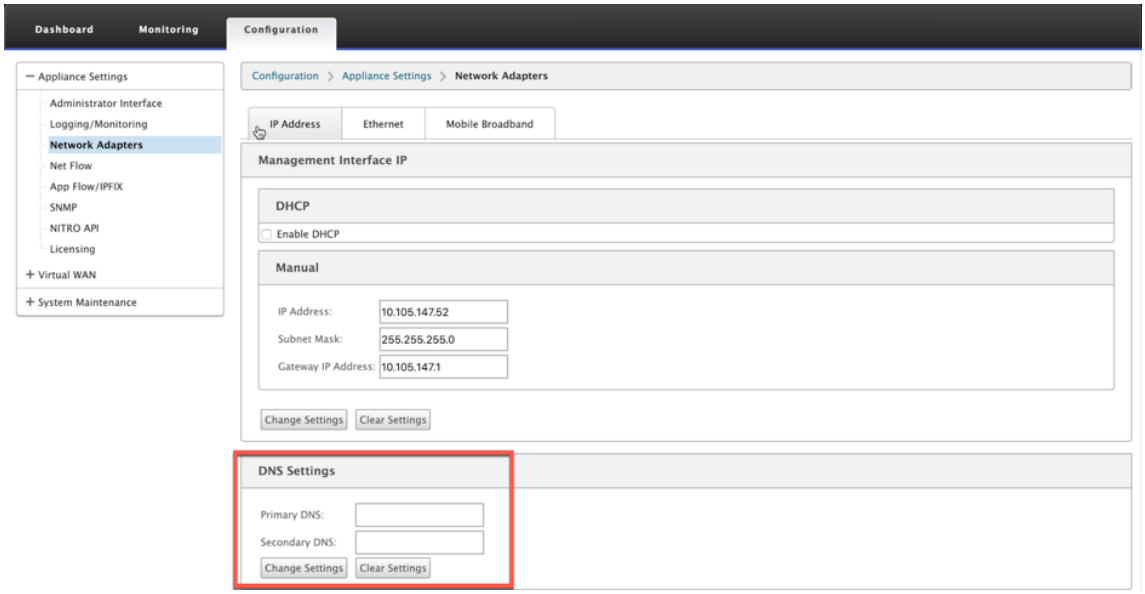
Office 365 分组策略允许您指定可以直接从分支中分出的 Office 365 流量的类别。启用 Office 365 分组并编译配置后，将自动创建 DNS 对象、应用程序对象、应用程序路由和防火墙策略模板，并将其应用于具有 Internet 服务的分支站点。

必备条件

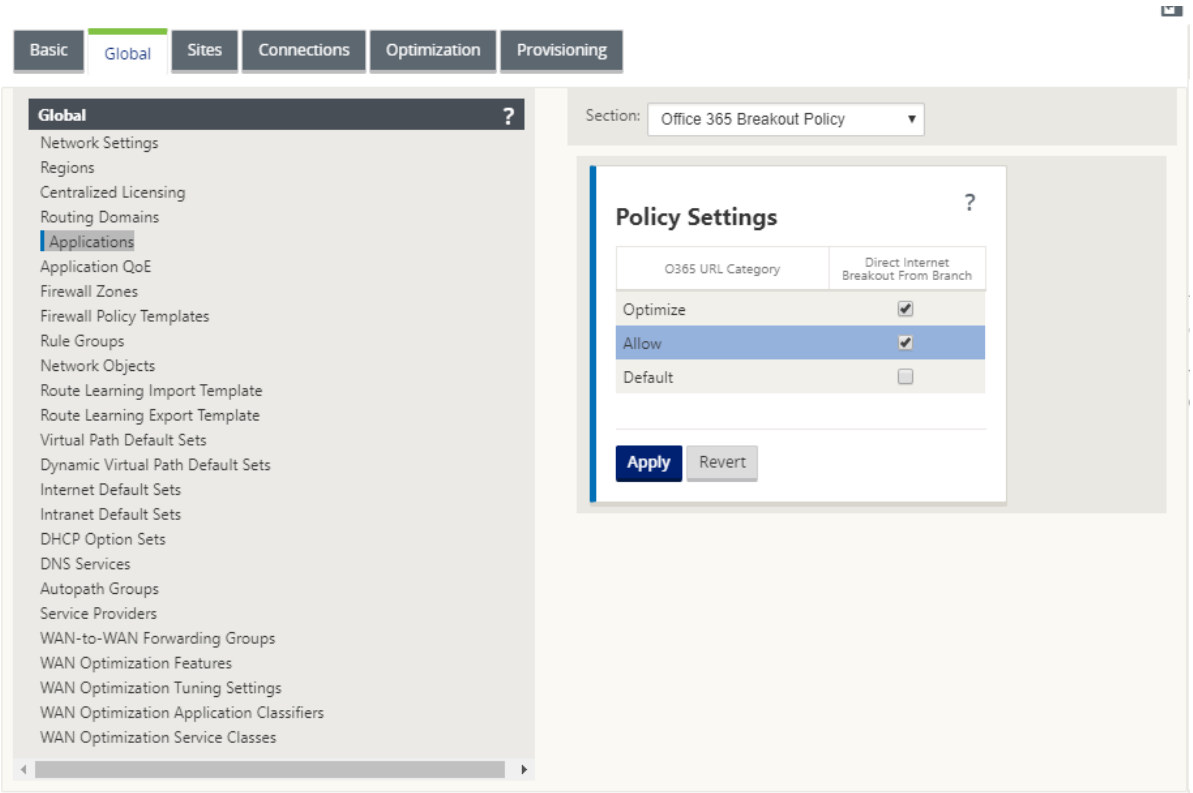
请确保您具有以下对象：

1. 要执行 Office 365 分组讨论，必须在设备上配置互联网服务。有关配置互联网服务的详细信息，请参阅 互联网访问。
2. 确保管理界面具有互联网连接。

   可以使用 Citrix SD-WAN Web 界面配置管理界面设置。
3. 确保已配置管理 DNS。要配置管理界面 DNS，请导航到 配置 **>** 设备设置 **>** 网络适配器。在 **DNS** 设置 部分下，提供主 DNS 和辅助 DNS 服务器详细信息，然后单击 更改设置。



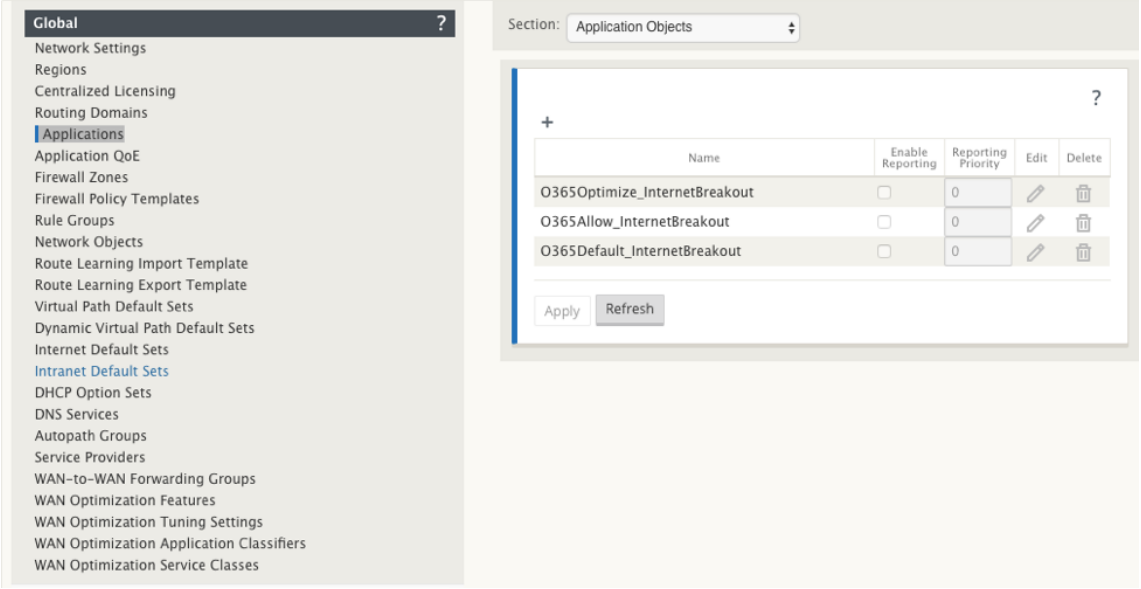
Office 365 分组策略设置在 全局设置下可用，为 Internet 分组选择所需的 Office 365 类别，然后单击 应用。



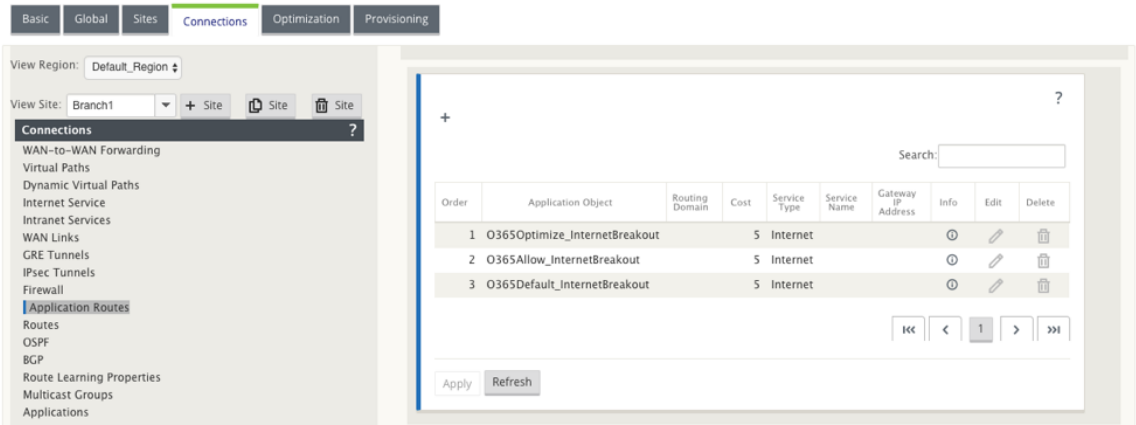
配置 Office 365 打破策略设置并编译配置后。以下设置将自动填充。

- **DNS** 对象 -DNS 对象指定要转发到用户配置的 DNS 服务的流量类型。在所有受信任的接口上都会听到 DNS 请求，并且 DNS 转发器将 Office 365 DNS 请求引导到 Quad9 服务。此转发器规则采用最高优先级。有关详细信息，请参阅 域名服务 部分。

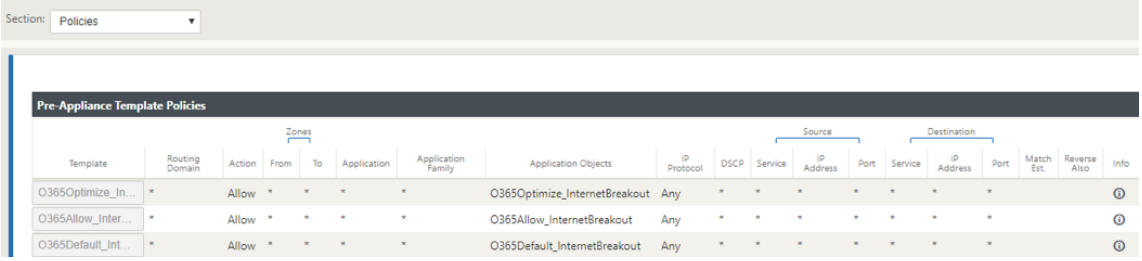
- 应用程序对象 -将创建具有由用户选择的 Office 365 类别或子类别的应用程序对象。如果您选择了“默认”类别以及“优化”和“允许”的子类别，则会创建相应的应用程序对象，如以下屏幕截图所示：



- 应用程序路由：为具有 Internet 服务类型的 Office 365 应用程序对象创建应用程序路由。有关升级注意事项的信息，请参阅 升级重要注意事项。



- 防火墙预设备策略模板：为每个配置的 Office 365 类别创建全局预设策略模板。此模板应用于具有 Internet 服务的所有分支站点。设备前策略优先于本地策略和后置设备策略模板。有关升级注意事项的信息，请参阅 升级重要注意事项。

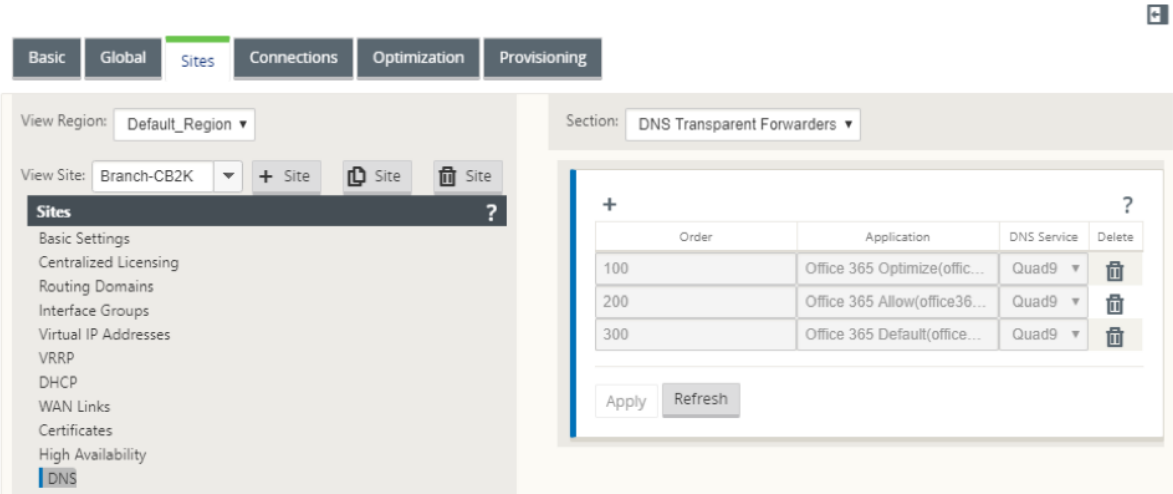


适用于 **Office 365** 的透明转发器

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。

每个启用了互联网服务和 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

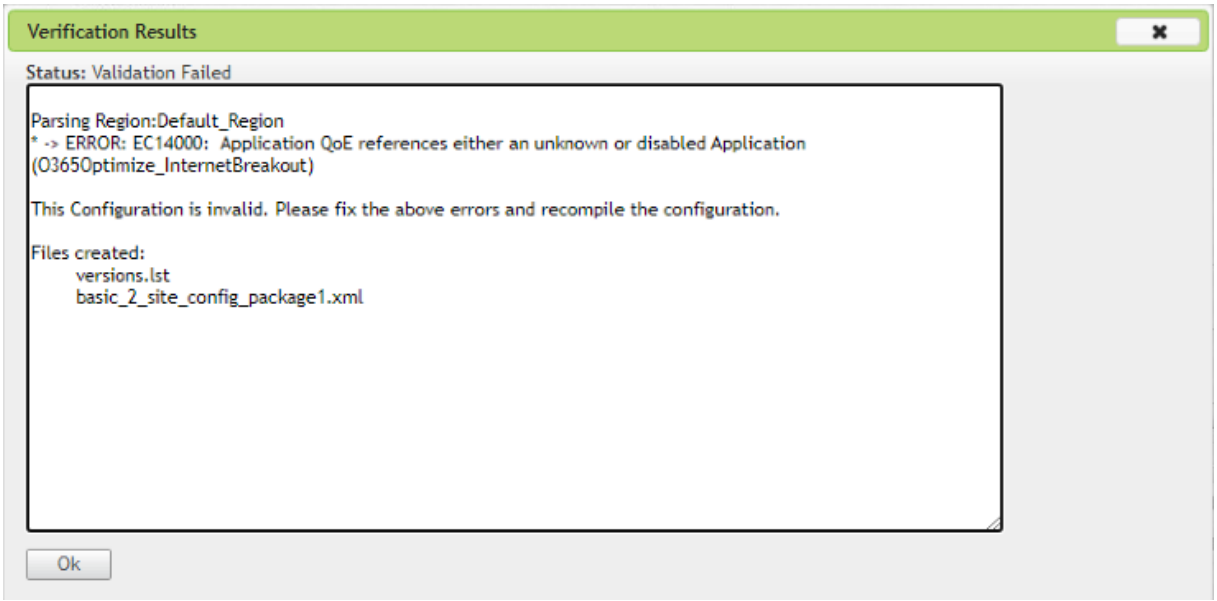
如果您已为 优化 和 允许 Office 365 类别启用了互联网分组策略，Citrix SD-WAN 会在 升级到 Citrix SD-WAN 11.4.0 时自动为相应子类别启用 Internet 突破策略。

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 O365 **Optimize_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/路线不需要此升级。它仅适用于您创建的规则/路线。

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。

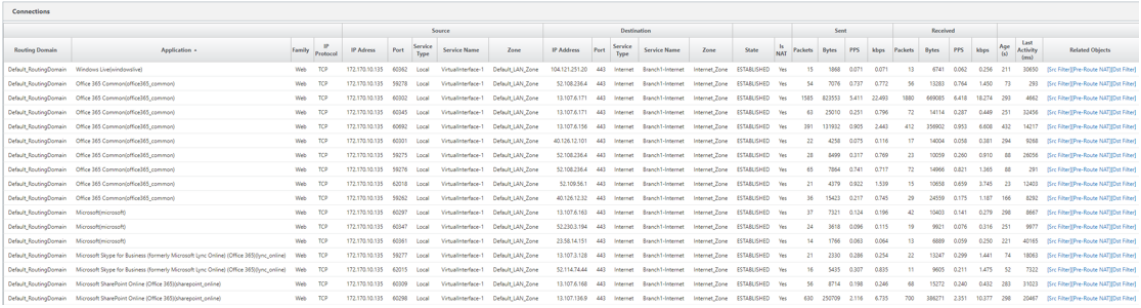
如果在不删除旧的 DNS 代理或透明转发器规则的情况下继续 Citrix SD-WAN 11.4.0 升级，则不会看到任何错误，升级也会成功。但是，DNS 代理规则和透明转发规则在 Citrix SD-WAN 11.4.0 中不生效。

> 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



Connections																															
				Source					Destination							Sent				Received							
Routing Domain	Application	Family	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (s)	Last Activity (ms)	Related Objects
Default_RoutingDomain	Windows Live(windowslive)	Web	TCP	172.170.10.135	60362	Local	VirtualInterface-1	Default_LAN_Zone	104.121.251.20	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	15	1868	0.071	0.071	13	6741	0.062	0.256	211	30850	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59278	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	54	7076	0.737	0.772	56	13283	0.764	1.450	73	293	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60302	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	1585	823553	5.411	22.493	1880	669085	6.418	18.274	293	4662	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60345	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.171	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	63	25010	0.251	0.796	72	14114	0.287	0.449	251	32456	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60692	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.156	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	391	131932	0.905	2.443	412	356902	0.953	6.608	432	14217	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	60301	Local	VirtualInterface-1	Default_LAN_Zone	40.126.12.101	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	22	4258	0.075	0.116	17	14004	0.058	0.381	294	9268	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59275	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	28	8499	0.317	0.769	23	10059	0.260	0.910	68	28256	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59276	Local	VirtualInterface-1	Default_LAN_Zone	52.108.236.4	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	65	7864	0.741	0.717	72	14066	0.821	1.365	68	291	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	62018	Local	VirtualInterface-1	Default_LAN_Zone	52.109.56.1	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	21	4379	0.822	1.539	15	10850	0.659	3.745	23	12403	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Office 365 Common(office365_common)	Web	TCP	172.170.10.135	59262	Local	VirtualInterface-1	Default_LAN_Zone	40.126.12.32	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	36	15423	0.217	0.745	29	24559	0.175	1.187	166	8292	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60297	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.163	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	37	7321	0.124	0.196	42	10403	0.141	0.279	298	8867	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60347	Local	VirtualInterface-1	Default_LAN_Zone	52.230.3.194	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	24	3618	0.096	0.115	19	9921	0.076	0.316	251	9877	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft(microsoft)	Web	TCP	172.170.10.135	60361	Local	VirtualInterface-1	Default_LAN_Zone	23.58.14.151	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	14	1766	0.063	0.064	13	6889	0.059	0.250	221	40165	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)(lync_online)	Web	TCP	172.170.10.135	59277	Local	VirtualInterface-1	Default_LAN_Zone	13.107.3.128	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	21	2330	0.288	0.254	22	13247	0.299	1.441	74	18063	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)(lync_online)	Web	TCP	172.170.10.135	62015	Local	VirtualInterface-1	Default_LAN_Zone	52.114.74.44	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	16	5435	0.307	0.835	11	9605	0.211	1.475	52	7322	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60309	Local	VirtualInterface-1	Default_LAN_Zone	13.107.6.168	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	56	8714	0.198	0.246	68	15272	0.240	0.432	283	31023	[Src Filter][Pre-Route NAT][Dst Filter]
Default_RoutingDomain	Microsoft SharePoint Online (Office 365)(sharepoint_online)	Web	TCP	172.170.10.135	60298	Local	VirtualInterface-1	Default_LAN_Zone	13.107.136.9	443	Internet	Branch1-Internet	Internet_Zone	ESTABLISHED	Yes	630	250709	2.116	6.735	700	386271	2.351	10.377	298	20487	[Src Filter][Pre-Route NAT][Dst Filter]

- 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

Dashboard | Monitoring | Configuration

Statistics
Flows
Routing Protocols
Firewall
IKE/IPsec
IGMP
Performance Reports
Qos Reports
Usage Reports
Availability Reports
Appliance Reports
DHCP Server/Relay
VRRP
PPPoE
DNS

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
DNS_Proxy1	office365_optimize	Quad9	YES	2
DNS_Proxy1	office365_allow	Quad9	YES	8
DNS_Proxy1	office365_default	Quad9	YES	6
DNS_Proxy1	Any	Google	YES	17

Showing 1 to 4 of 4 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
office365_allow	Quad9	YES	0
office365_default	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 3 of 3 entries

- 应用程序路径统计

Monitoring > Statistics

Statistics

Show: Application Routes | Enable Auto Refresh | 5 seconds | Stop | Clear Counters on Refresh | Processing...

Application Route Statistics

Maximum allowed routes: 64000

Application Routes for routing domain : Default_RoutingDomain

Filter: in Any column Apply

Show 100 entries Showing 1 to 3 of 3 entries

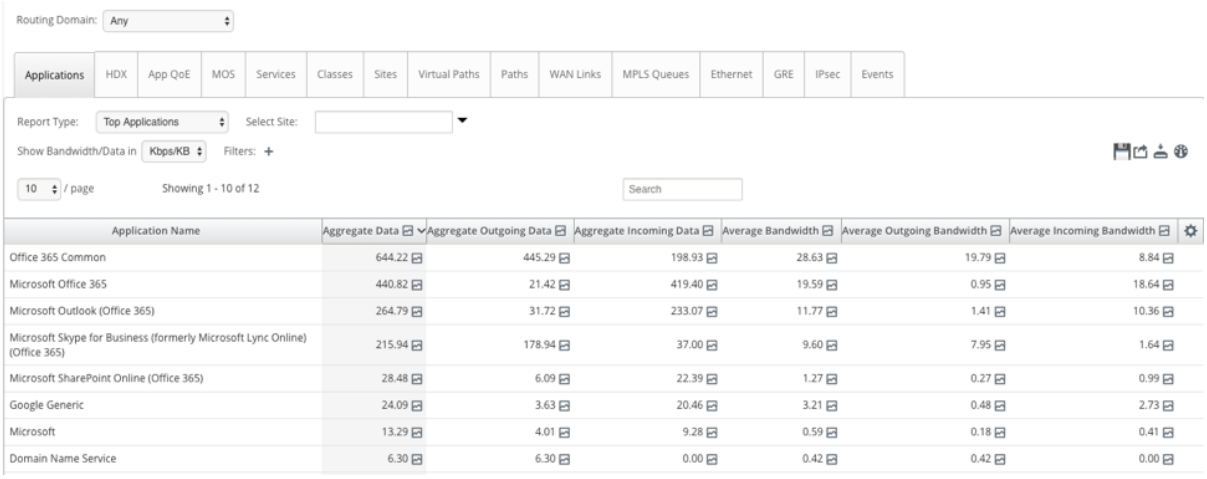
First Previous 1 Next Last

Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	O365Optimize_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1792	YES	N/A	N/A
2	O365Allow_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	1395	YES	N/A	N/A
1	O365Default_InternetBreakout	*	Internet	Internet_Zone	YES	Branch1	Static	5	0	YES	N/A	N/A

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

您还可以在 SD-WAN 中心应用程序报告中查看 Office 365 应用程序统计信息。

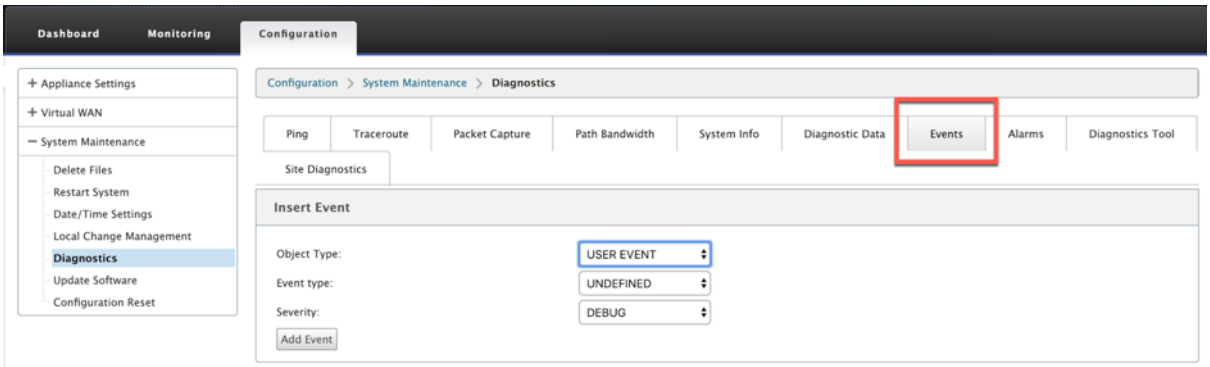


Application Name	Aggregate Data	Aggregate Outgoing Data	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth	Average Incoming Bandwidth
Office 365 Common	644.22	445.29	198.93	28.63	19.79	8.84
Microsoft Office 365	440.82	21.42	419.40	19.59	0.95	18.64
Microsoft Outlook (Office 365)	264.79	31.72	233.07	11.77	1.41	10.36
Microsoft Skype for Business (formerly Microsoft Lync Online) (Office 365)	215.94	178.94	37.00	9.60	7.95	1.64
Microsoft SharePoint Online (Office 365)	28.48	6.09	22.39	1.27	0.27	0.99
Google Generic	24.09	3.63	20.46	3.21	0.48	2.73
Microsoft	13.29	4.01	9.28	0.59	0.18	0.41
Domain Name Service	6.30	6.30	0.00	0.42	0.42	0.00

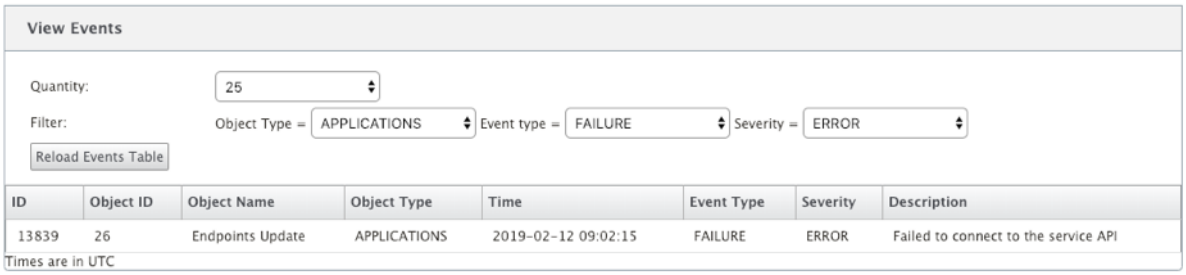
故障排除

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。

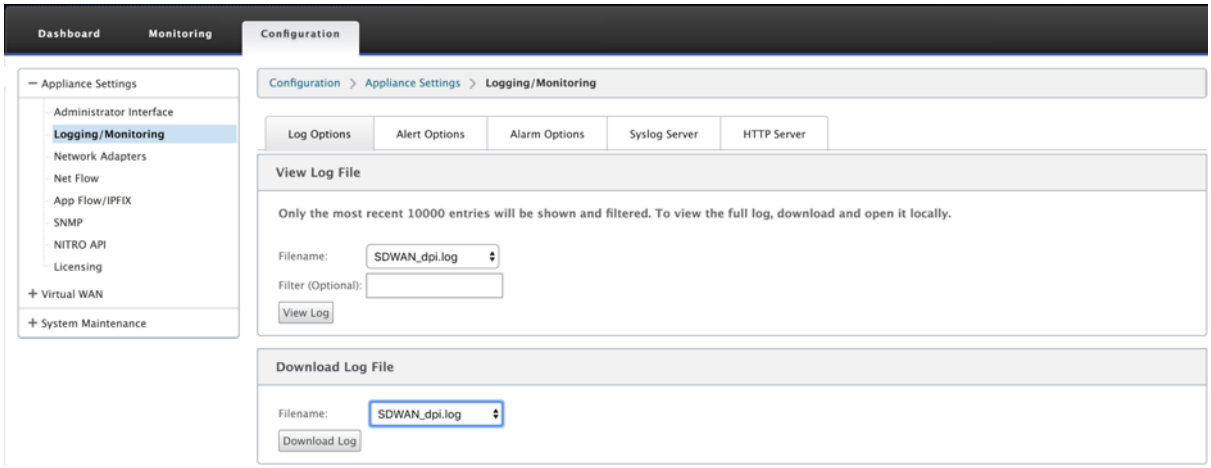


ID	Object ID	Object Name	Object Type	Time	Event Type	Severity	Description
13839	26	Endpoints Update	APPLICATIONS	2019-02-12 09:02:15	FAILURE	ERROR	Failed to connect to the service API

Times are in UTC

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

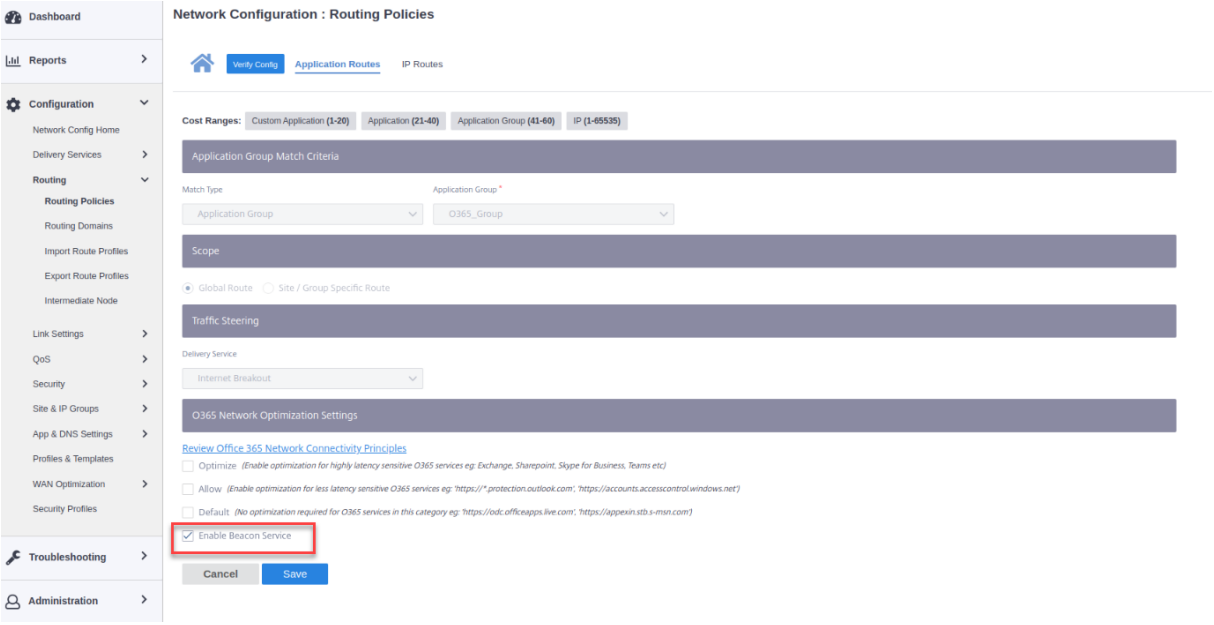
微软提供 Office 365 信标服务来衡量 Office 365 通过 WAN 链接的可达性。信标服务基本上是一个 URL-SDWAN. 测量. 办公室/apC/转接.png，它会定期进行探测。每台设备都会对每个启用互联网的 WAN 链路进行探测。对于每个探测器，HTTP 请求都会发送到信标服务，并且需要 HTTP 响应。HTTP 响应确认了 Office 365 服务的可用性和可访问性。

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 分组讨论的互联网链接。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。

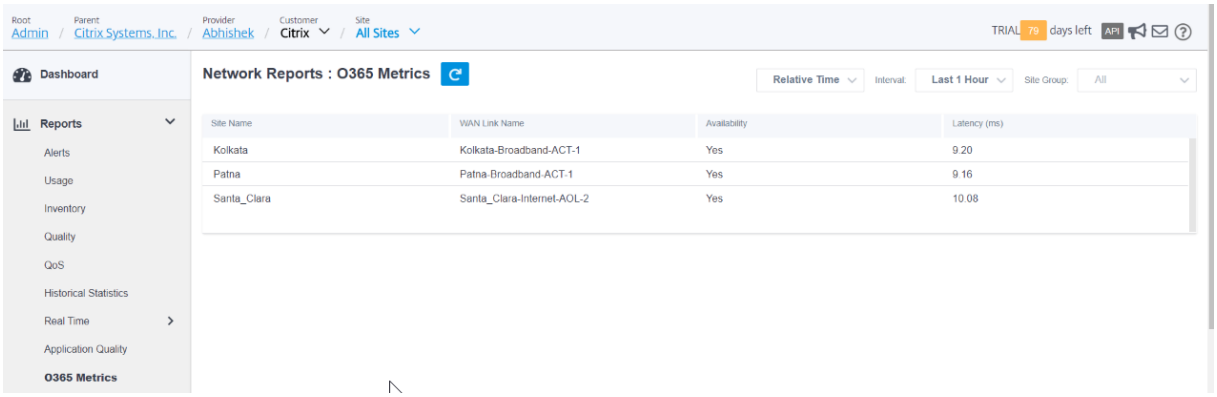
> 注意
>
> 在按流量计量的链接上未启用 Office 365 信标探测。

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。

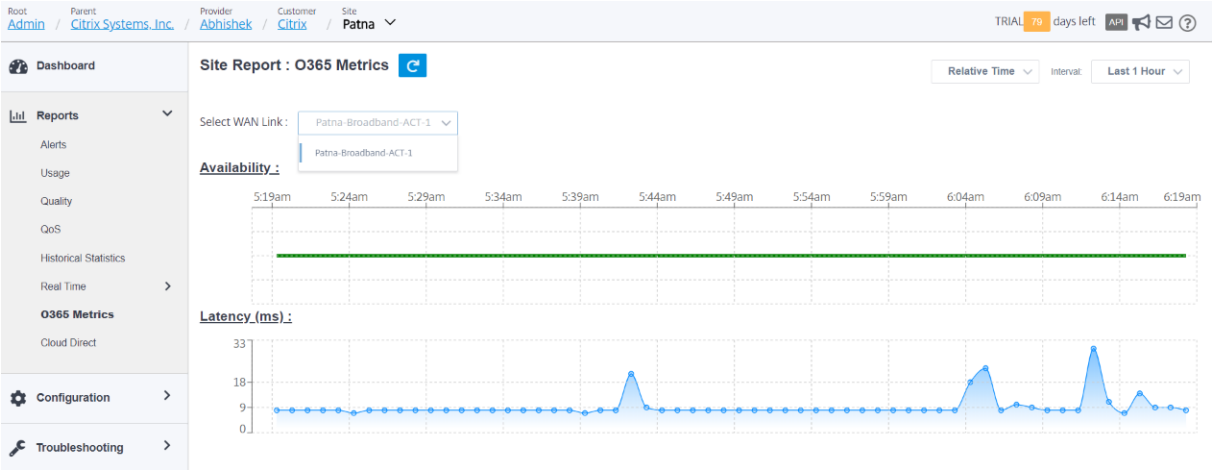
要禁用 Office 365 信标服务，请在 SD-WAN Orchestrator 中，在网络级别导航到 配置 > 路由 **>** 路由策略 >**O365** 网络优化设置，然后清除启用信标服务。



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。
> - 从 Citrix SD-WAN 11.4.3 开始，Citrix SD-WAN Orchestrator 服务流量签名与设备软件版本一起打包，并在 Citrix SD-WAN Orchestrator 服务的变更管理暂存过程中加载到设备上。此步骤有助于克服可能阻止设备在初始安装或软件升级后从 Citrix SD-WAN Orchestrator 服务下载签名的任何限制。

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：

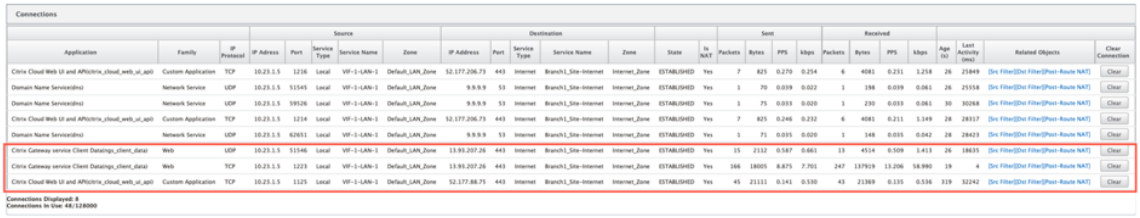
- **Citrix Cloud**：启用此功能可检测和路由发往 Citrix Cloud Web UI 和 API 的流量。
  - Citrix SD-WAN Orchestrator 和依赖的关键服务：
    - **Citrix SD-WAN Orchestrator**：支持在 Citrix SD-WAN 设备与 Citrix SD-WAN Orchestrator 之间建立和维护连接所需的心跳和其他流量的直接 Internet 突破。
    - **Citrix Cloud** 下载服务：启用直接 Internet 突围，以便将设备软件、配置、脚本等下载到 Citrix SD-WAN 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）。

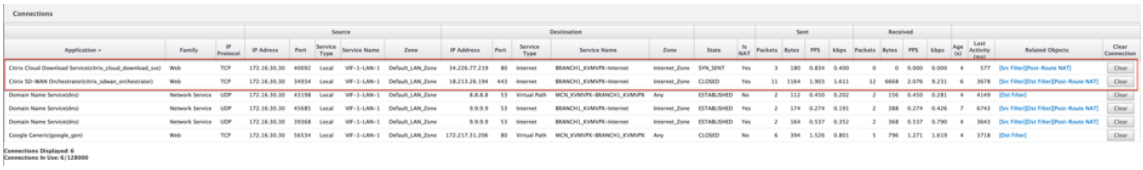
- 网关服务客户端数据：在客户端和 Citrix Gateway 服务之间启用 ICA 数据通道的直接 Internet 突破。它需要高带宽和低延迟。
- 网关服务服务器数据：在虚拟交付代理 (VDA) 和 Citrix Gateway 服务之间启用 ICA 数据通道的直接 Internet 突破。它需要高带宽和低延迟，并且仅适用于 VDA 资源位置（VDA 到 Citrix Gateway 关服务连接）。
- 网关服务控制流量：支持控制流量的直接 Internet 突破。没有特定的 QoS 注意事项。
- 网关服务 **Web** 代理流量：启用 Web 代理流量的直接 Internet 突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

监视

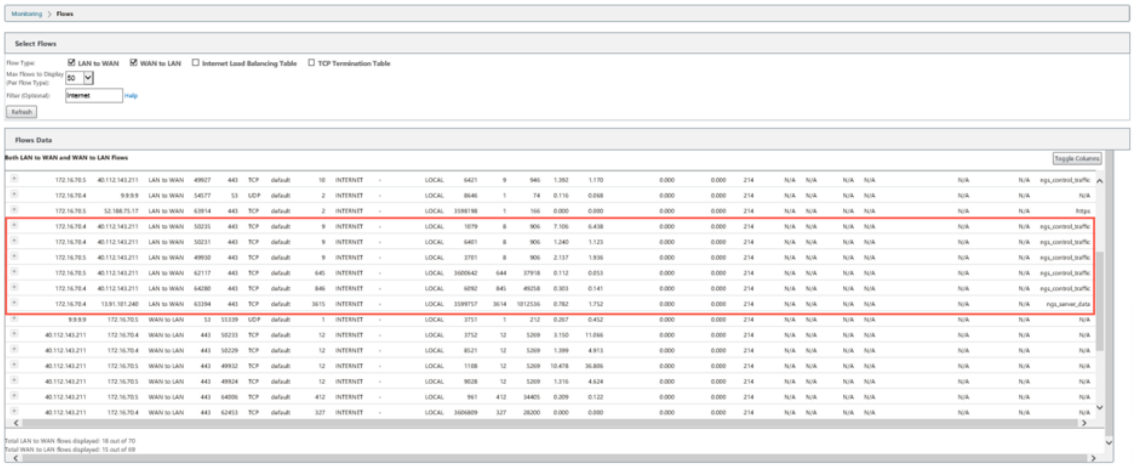
您可以在以下 SD-WAN 统计报告中监视网关服务统计信息：

- 防火墙统计信息





- 流



Flows Data

Both LAN to WAN and WAN to LAN Flows

Toggle Columns

IP DSCP	Hit Count	Service Type	Service Name	LAN GW 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
default	3	INTERNET	-	LOCAL	8034	2	174	0.249	0.173	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	N/A
default	4	INTERNET	-	LOCAL	2875	3	180	0.507	0.244	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_cloud_download_svc
default	16	INTERNET	-	LOCAL	4059	15	1372	1.927	1.410	0.000	0.000	147	N/A	N/A	N/A	N/A	N/A	N/A	citrix_sdwan_orchestrator
default	3	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	6447	2	112	0.310	0.139	0.141	0.000	57	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	N/A
default	7	Virtual Path	MCN_KVMVPX-BRANCH1_KVMVPX	LOCAL	5967	6	394	0.969	0.509	0.442	0.000	1	N/A	13	INTERACTIVE	BRANCH1_KVMVPX-Internet-ACT-1->MCN_KVMVPX-Internet-ACT-1	N/A	Load Balanced, Reliable	google_gen

- DNS 统计信息

Monitoring > DNS

DNS Statistics

Refresh

Proxy Statistics

Search:

Proxy Name	Application Name	DNS Service Name	DNS Service Active	Hits
Default	office365_optimize	Quad9	YES	0
Default	citrix_cloud_web_ui_api	Quad9	YES	4
Default	ngs_client_data	Quad9	YES	14
Default	ngs_server_data	Quad9	YES	0
Default	ngs_control_traffic	Quad9	YES	2286
Default	ngs_web_proxy	Quad9	YES	0
Default	Any	azureDNS	YES	51490

Showing 1 to 7 of 7 entries

Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_web_ui_api	Quad9	YES	0
ngs_client_data	Quad9	YES	0
ngs_control_traffic	Quad9	YES	0
ngs_server_data	Quad9	YES	0
ngs_web_proxy	Quad9	YES	0
office365_optimize	Quad9	YES	0

Showing 1 to 6 of 6 entries

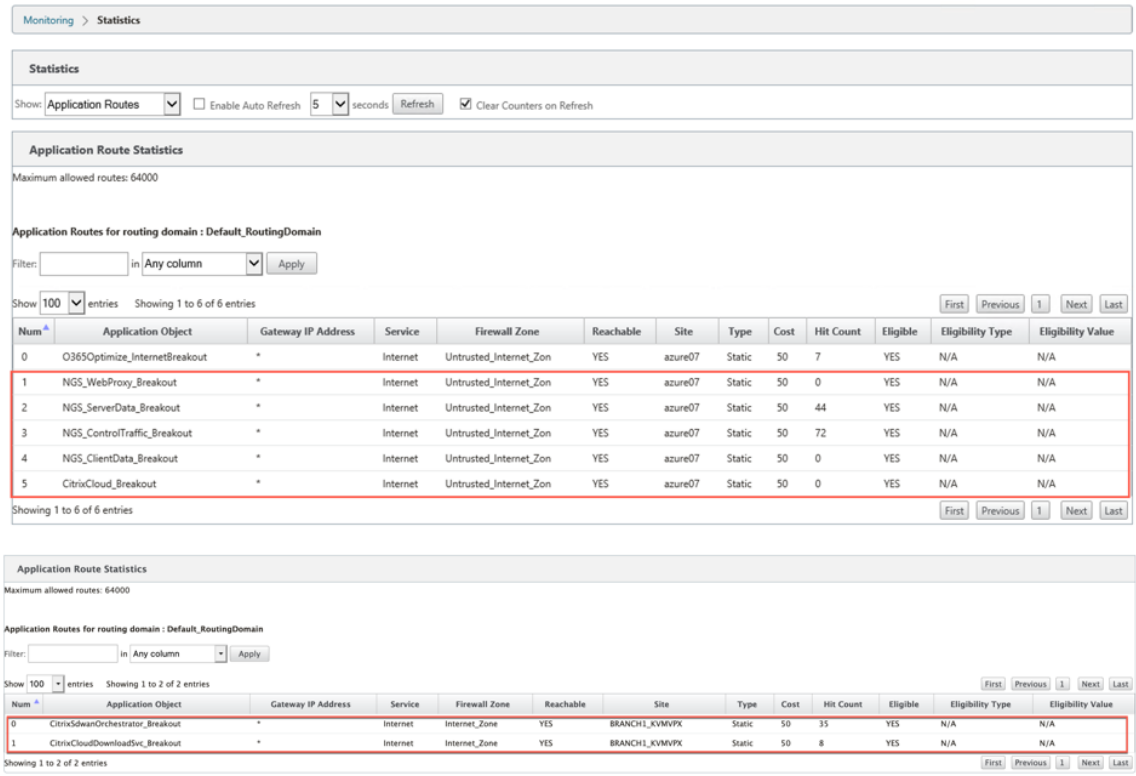
Transparent Forwarder Statistics

Search:

Application Name	DNS Service Name	DNS Service Active	Hits
citrix_cloud_download_svc	Quad9	YES	1
citrix_sdwan_orchestrator	Quad9	YES	1

Showing 1 to 2 of 2 entries

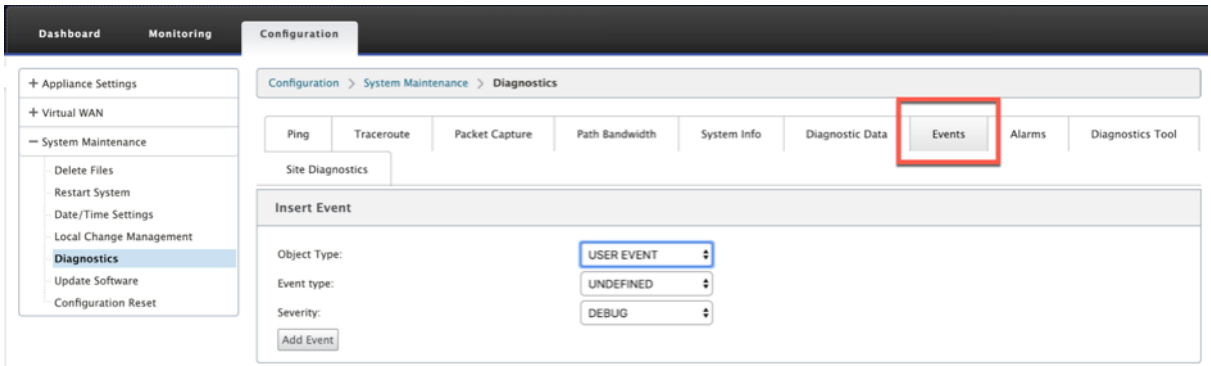
- 应用程序路由统计信息



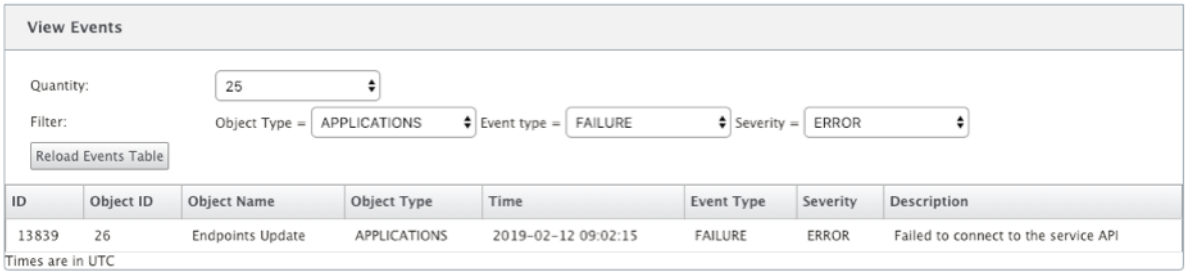
故障排除

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。

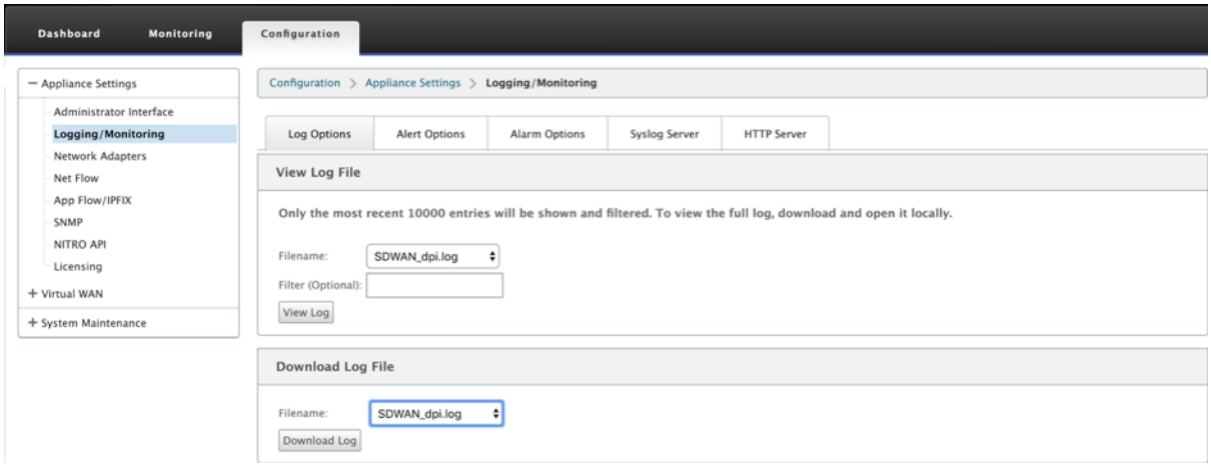


如果连接到 Citrix 服务（sdwan-app-路由.citrixnetworkapi.net）时出现问题，则错误消息将反映在“查看事件”表中。



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。



适用于 **Citrix SD-WAN** 设备上的内部部署配置的 **Citrix SD-WAN** 管弦乐器

November 16, 2022

适用于本地的 Citrix SD-WAN Orchestrator 是 Citrix SD-WAN Orchestrator 服务的本地软件版本。适用于内部部署的 Citrix SD-WAN Orchestrator 为 Citrix 合作伙伴提供了一个单一窗格管理平台，可以通过适当的基于角色的访问控制来集中管理多个客户。

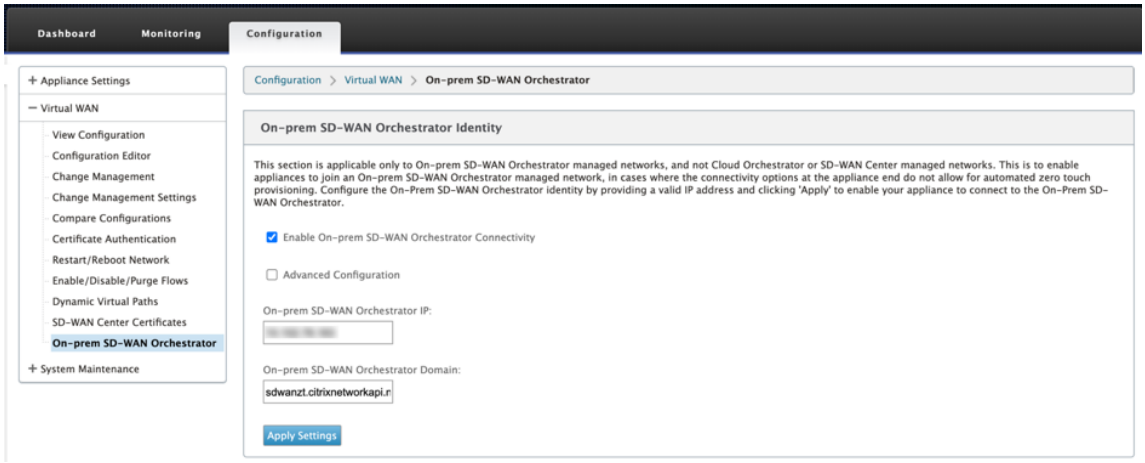
通过启用 Orchestrator 连接并为本地身份指定 Citrix SD-WAN 管弦乐队，您可以在 Citrix SD-WAN 设备和适用于内部部署的 Citrix SD-WAN Orchestrator 之间建立连接。

> 注意
>
> - 如果在 SD-WAN 设备上配置了 **SD-WAN** 设备上的本地 **SD-WAN Orchestrator** 配置 功能，则 Cloud Orchestrator 零接触部署将不起作用。
> - 如果在 Citrix SD-WAN Orchestrator 版本 11.3.0 中配置的 SD-WAN 设备上的 Citrix SD-WAN 本地

> 管弦乐器配置降级至 10.2.7 版，则 SD-WAN 设备上本地的 Citrix SD-WAN 管弦乐器将丢失。不支持从 11.3.0 版降级到 10.2.7 版。解决方法是在降级后为本地身份重新配置 Citrix SD-WAN Orchestrator。
> - 将 SD-WAN 设备从 11.3.0 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 UI 上再次应用身份设置。如果有与用于本地配置或 SD-WAN 设备连接的 Citrix SD-WAN Orchestrator 相关的任何问题，请禁用 Citrix SD-WAN Orchestrator 进行本地连接，然后再次启用 Citrix SD-WAN Orchestrator 进行本地连接。

要为内部部署连接启用 Citrix SD-WAN Orchestrator：

1. 在 SD-WAN 设备 UI 中，导航到 配置 > 虚拟广域网 > 本地 **SD-WAN Orchestrator**。
2. 选中 启用本地 **SD-WAN Orchestrator** 连接 复选框。



3. 输入适用于本地 IP 地址或域的 Citrix SD-WAN Orchestrator 或两者（IP 地址和域）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。

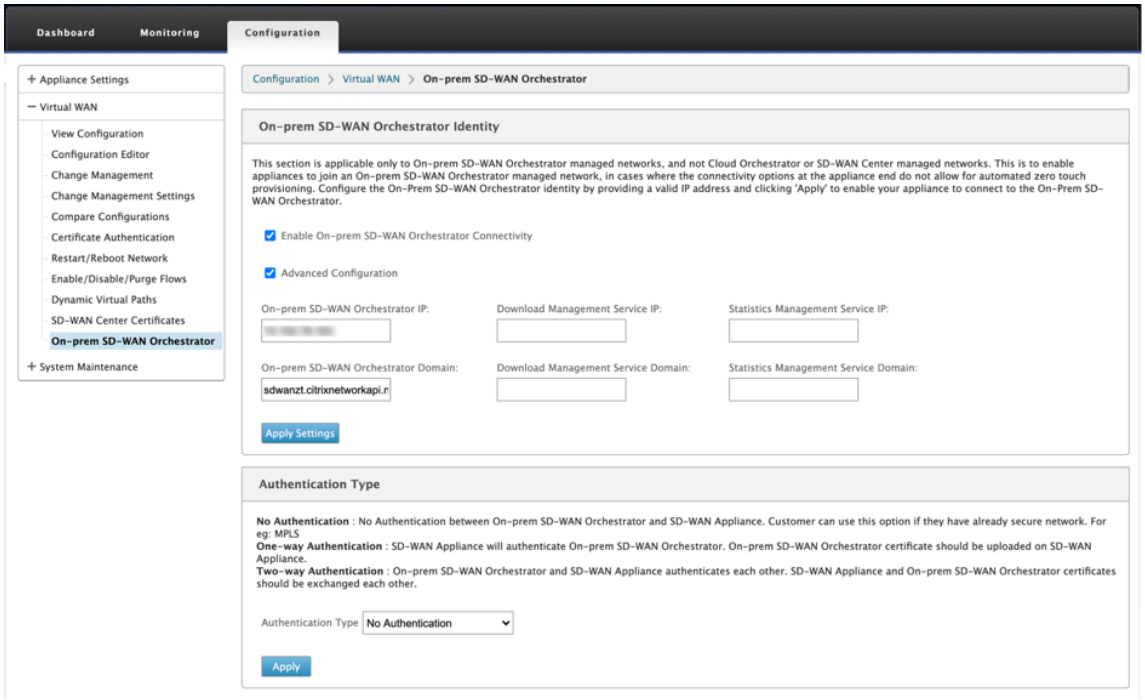
   例如，如果适用于内部部署域的 Citrix SD-WAN Orchestrator 配置为 **citrix.com**，则必须在 DNS 服务器中为以下 FQDN 和 Citrix SD-WAN Orchestrator 为本地 IP 地址创建 DNS 记录：

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

   在高级配置中：

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

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



Orchestrator 本地可能支持运行下载、独立服务器实例的统计数据等服务，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. 选择 身份验证类型。以下是 SD-WAN 设备和 Citrix SD-WAN Orchestrator 之间支持的用于本地连接的身份验证类型：

   - 无身份验证—SD-WAN Orchestrator 本地和 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—选择 单向身份验证 类型时，必须上传 Orchestrator 本地证书。从 Orchestrator 本地下载 Orchestrator 本地证书，然后单击 上传。SD-WAN 设备使用上传的证书在本地信任 Orchestrator。
   - 双向身份验 证—Orchestrator 本地证书和设备证书必须彼此交换。对于 双向身份验证，您必须在 Orchestrator 内部重新生成、下载和上传 SD-WAN 设备证书。SD-WAN 设备和 Orchestrator 本地使用交换的证书相互信任。

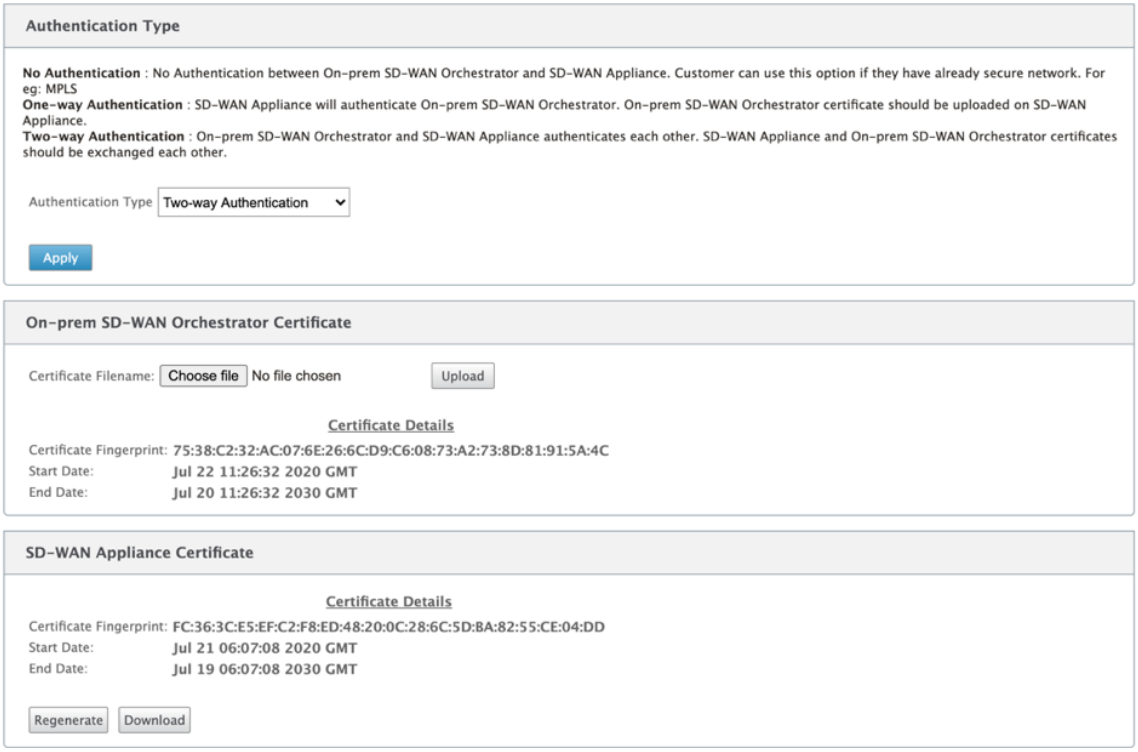
> 注意
>
> 建议仅使用单向身份验证或双向身份验证。在无身份验证的情况下，请确保 DNS 是安全的，免受 DNS 攻击。

如果禁用了 Orchestrator 本地 身份验证类型，则设备可以通过 无身份验证或单向身份验证或 ** 双向身份验证 ** 模式连接到 Orchestrator 本地。

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

在将 Orchestrator 本地的 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 Orchestrator 本地才能连接。

> 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 Orchestrator 本地和 SD-WAN 设备之间重新生成和交换证书，以避免设备与本地 Orchestrator 的连接中断。



5. 单击 应用设置。

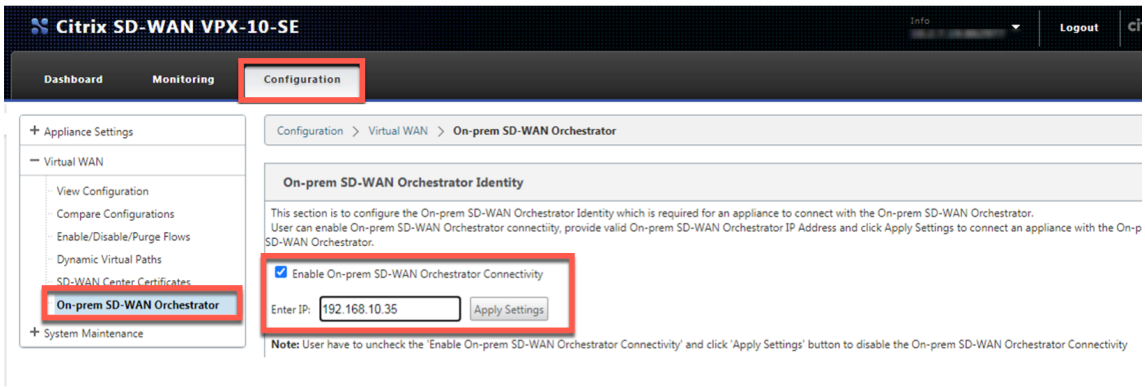
要为本地连接禁用 Citrix SD-WAN Orchestrator，请清除 启用 **Citrix SD-WAN Orchestrator** 本地连接 选项，然后单击 应用设置。要将 Orchestrator 本地托管网络转换为云管弦乐队或 MCN 托管网络，您需要为本地连接禁用 Citrix SD-WAN Orchestrator，并且必须执行配置重置。要重置配置，请导航到 配置 **>** 系统维护 **>** 配置重置。

使用适用于内部部署的 **Citrix SD-WAN** 管弦乐器部署在软件版本 **10.2.7**、**11.1.1** 或 **11.2.0** 上运行的 **Citrix SD-WAN** 设备

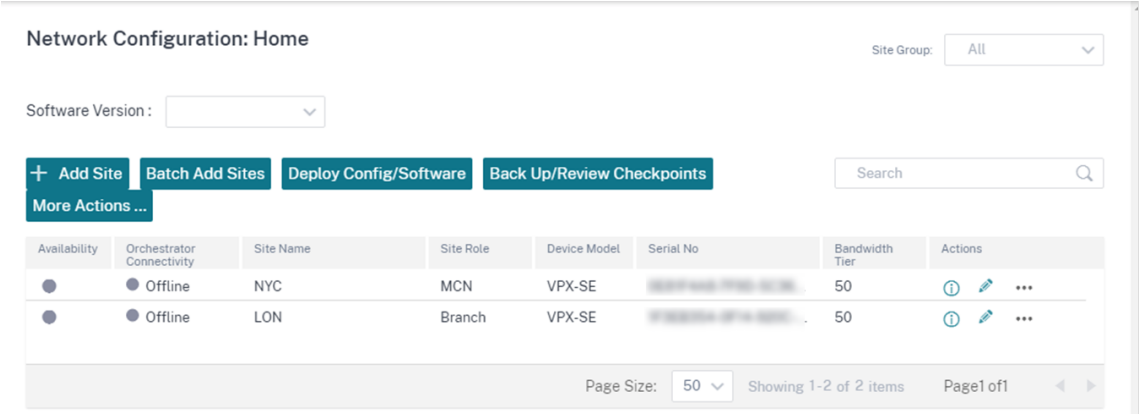
> 注意
>
> 要使用软件版本 10.2.7、11.1.1 或 11.2.0 部署 Citrix SD-WAN 设备，您需要使用适用于本地版本 11.1 或更高版本的 Citrix SD-WAN Orchestrator。

1. 对于软件版本为 10.2.7、11.1.1 或 11.2.0 的每台 Citrix SD-WAN 设备，请登录设备 Web 界面并执行以下操作：

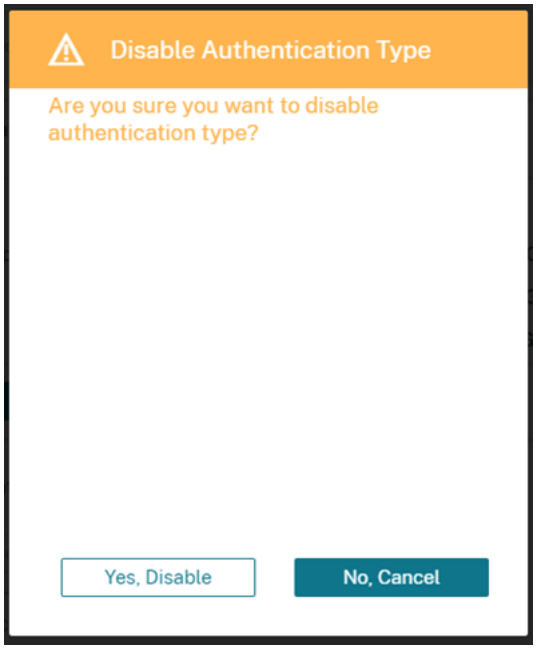
   a) 导航到 配置 **>** 虚拟广域网 **>** 本地 **SD-WAN Orchestrator** ，然后选中 启用本地 **SD-WAN Orchestrator** 连接 复选框。
   b) 输入适用于本地的 Citrix SD-WAN Orchestrator 的 IP 地址。
   c) 单击 应用设置。

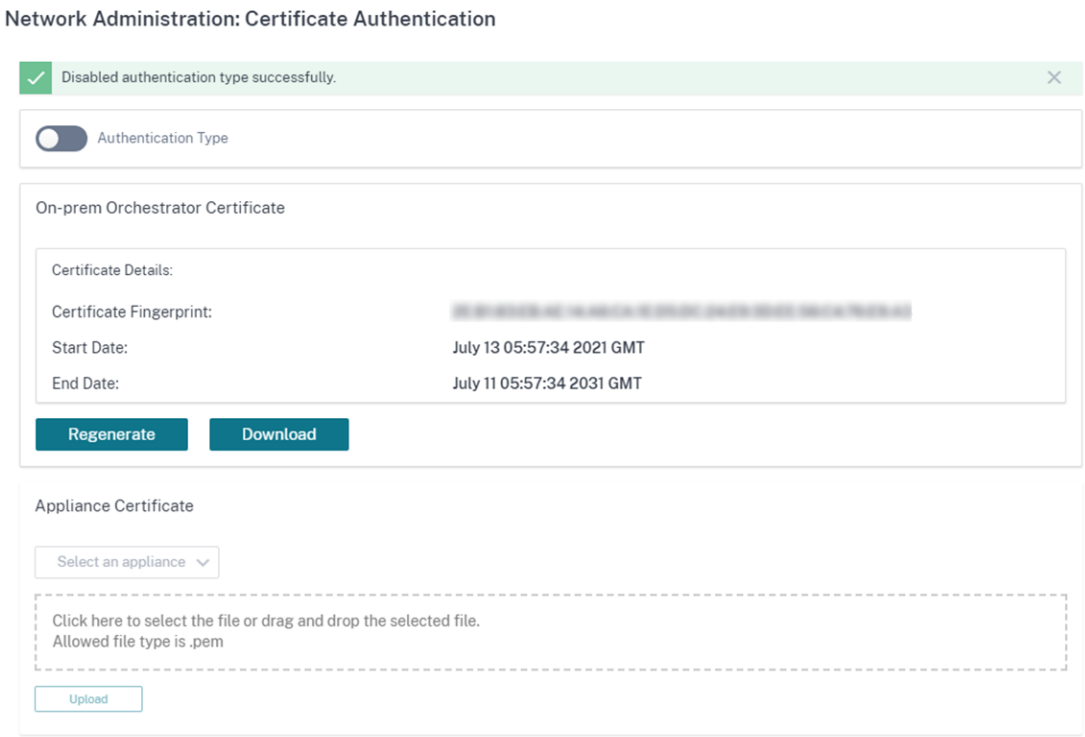


2. 登录适用于本地用户界面的 Citrix SD-WAN Orchestrator。创建站点并构建配置。在各自的站点配置中输入每台 Citrix SD-WAN 设备的序列号。保存配置。

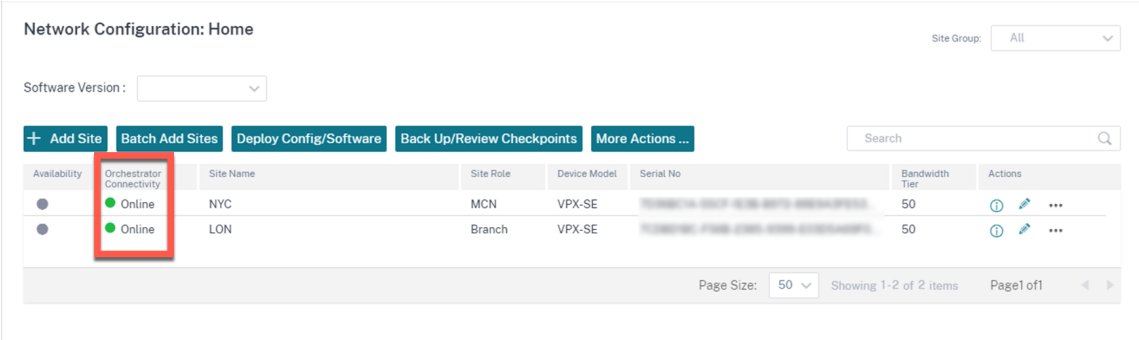


3. 导航到 管理 > 证书身份验证，然后将 身份验证类型 切换开关设为 关。单击 是，禁用以批准禁用 的 身份验证类型 弹出窗口。

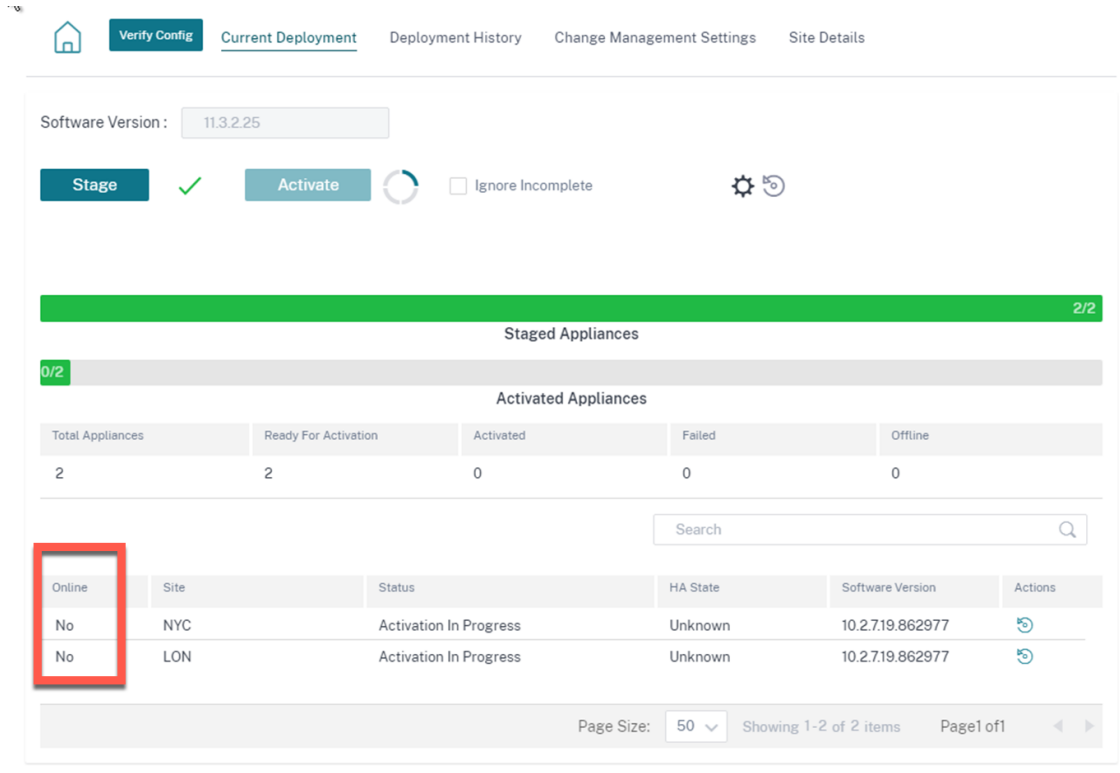




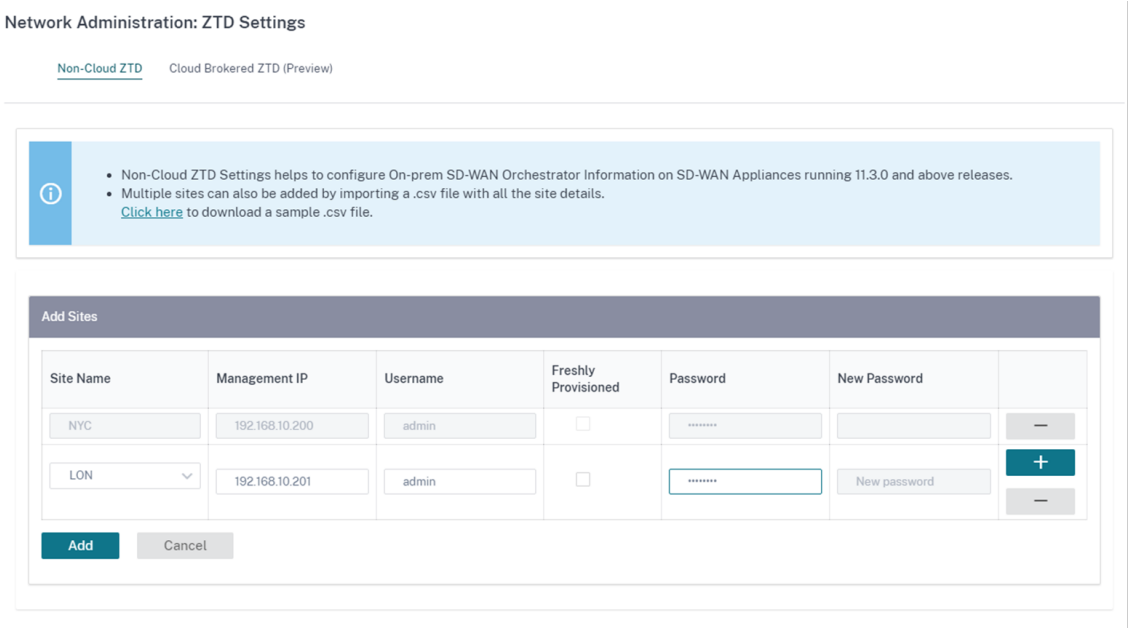
4. 在 配置 **>** 网络配置主 页中，SD-WAN 设备 在云连接 列下显示为联机。这是由于在适用于本地的 Citrix SD-WAN Orchestrator 上禁用了证书身份验证，并且为 Citrix SD-WAN Orchestrator 启用了 SD-WAN Orchestrator 使用适当的 IP 地址进行本地连接的 SD-WAN 设备。等待几分钟，让设备报告为在线状态。



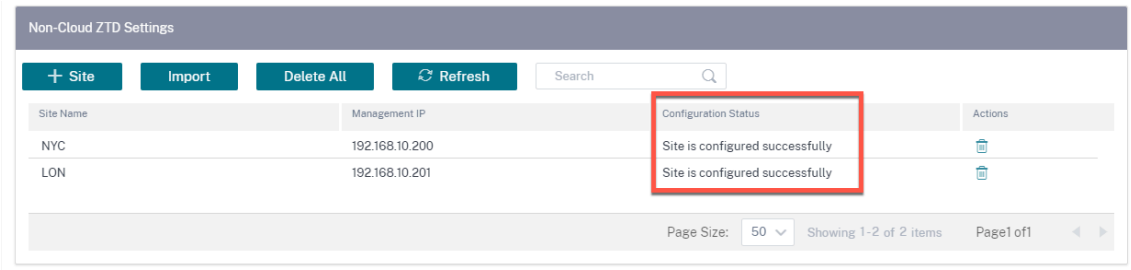
5. 选择已发布的软件版本（11.3.0 或更高版本），然后单击 部署配置/软件。有关选择已发布软件版本的更多详细信息，请参阅 软件。暂停并激活站点。激活后，设备将在联机列中显示 “** 否”。**



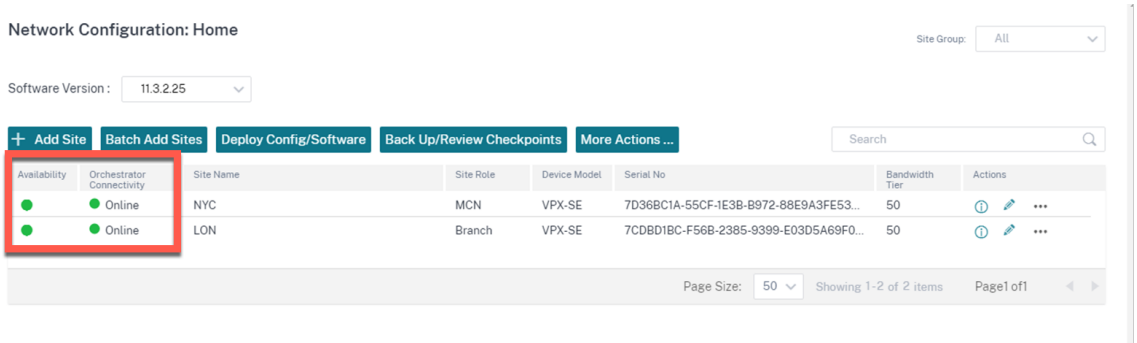
6. 导航到 管理 **> ZTD** 设置 **>** 非云 **ZTD**。单击 **+** 站 点并添加站点。输入每台设备的管理 IP 和登录凭据。单击 **+** 添加更多站点。单击添加。



7. 单击 刷新 以监视配置状态。成功配置站点后，“配置状态”列将显示“站点已成功配置”。



8. 导航到 配置 > 网络配置主 页。成功配置的站点 在 **Orchestrator** 连接 列下显示为联机。



9. 按照相同的过程添加任何其他站点。执行上述步骤不会影响任何现有的站点部署。

PPPoE 会话

June 22, 2021

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互联网。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 线路使用共享互联网接入。

Citrix SD-WAN 用作 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。

要建立成功的 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。

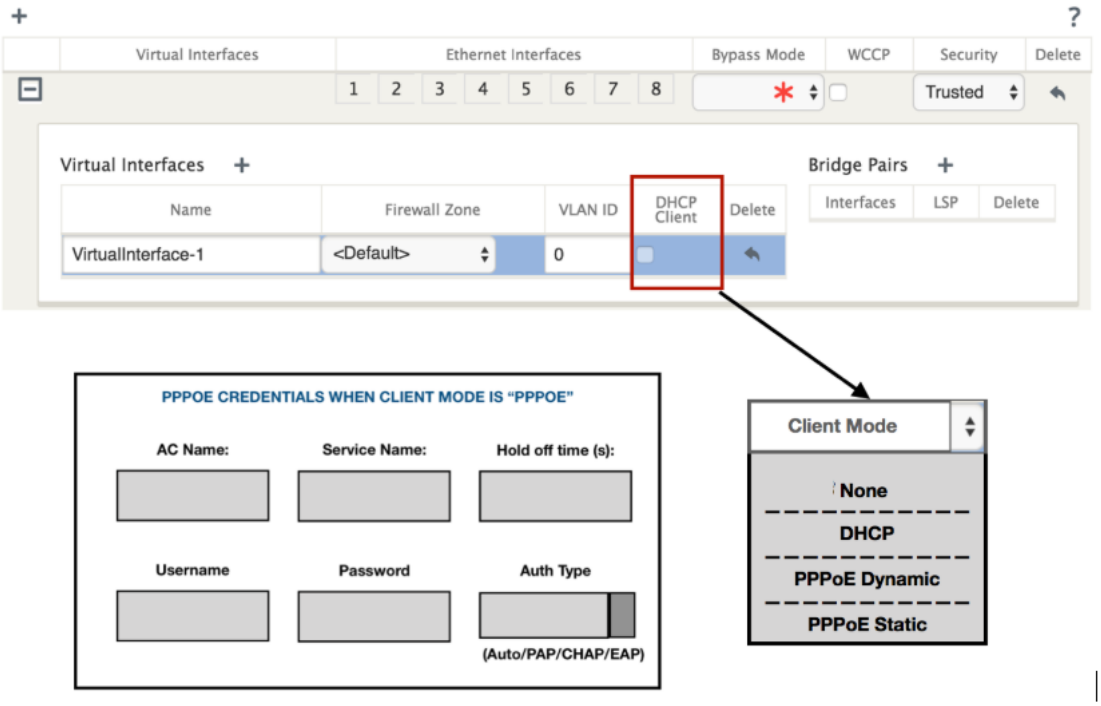
  > 注意：
  >
  > 允许使用相同的 802.1Q VLAN 标记创建多个 VNI。

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。
- IPv6 和 IPX 协议。
- 购买力平价多链接。
- 范雅各布森风格 TCP/IP 头压缩.
- 范雅各布森风格 TCP/IP 头压缩连接 ID 压缩选项.
- 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。

为了方便配置 PPPoE，**DHCP** 客户端选项被替换为站点配置下的 SD-WAN Web 管理界面中名为客户端模式的新选项。



下表分别介绍了 MCN 和分支 SD-WAN 设备上可用的客户端模式 PPPoE 配置选项。

MCN

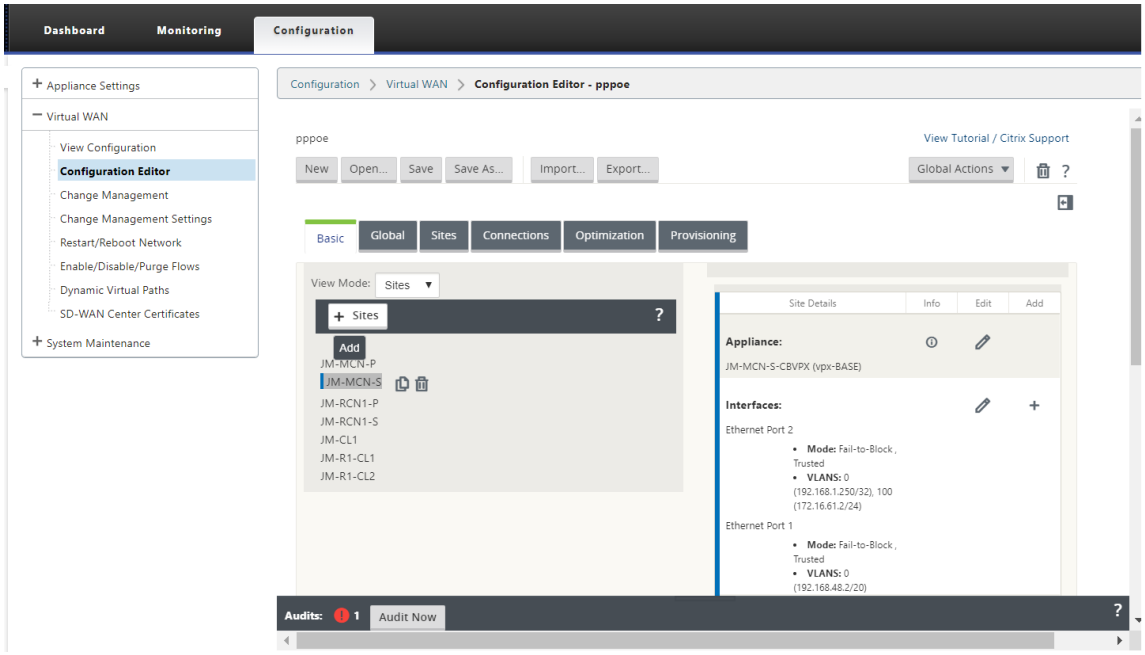
- 无
- PPPoE 静态

Branch

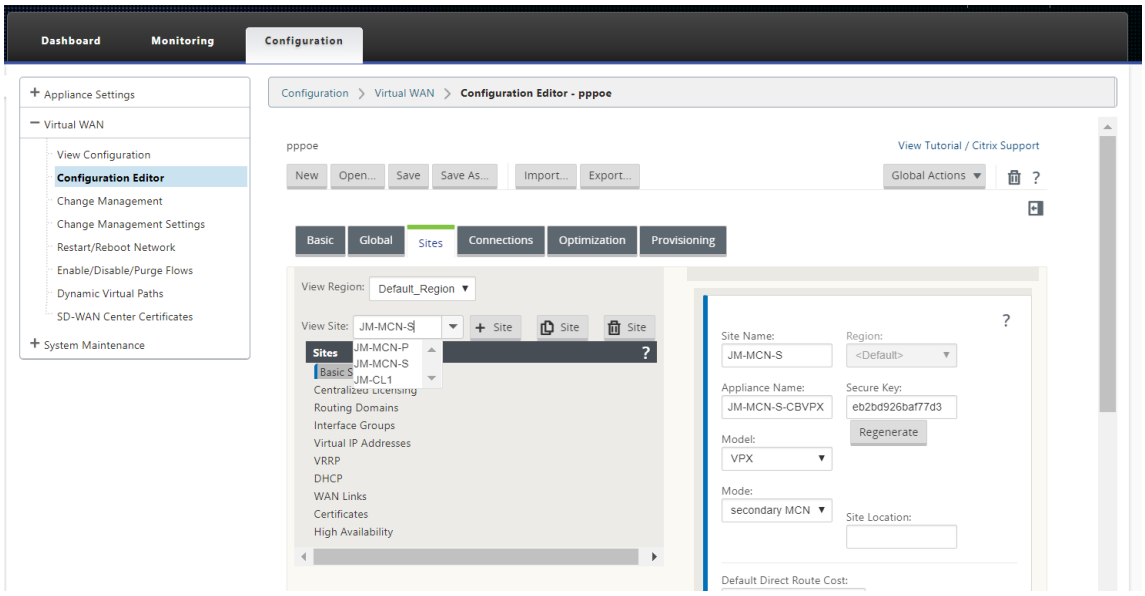
- 无
- PPPoE 静态
- PPPoE 动态
- DHCP

配置 **MCN** 设备

1. 在 SD-WAN MCN 设备 GUI 中，导航到 配置 > 虚拟 **WAN** > 配置编辑器。在 基本 选项卡下添加站点。有关详细信息，请参阅中的分支节点配置 配置 MCN。



2. 创建新站点后，打开 站点 选项卡。从 查看站点 下拉列表中选择新创建的站点。

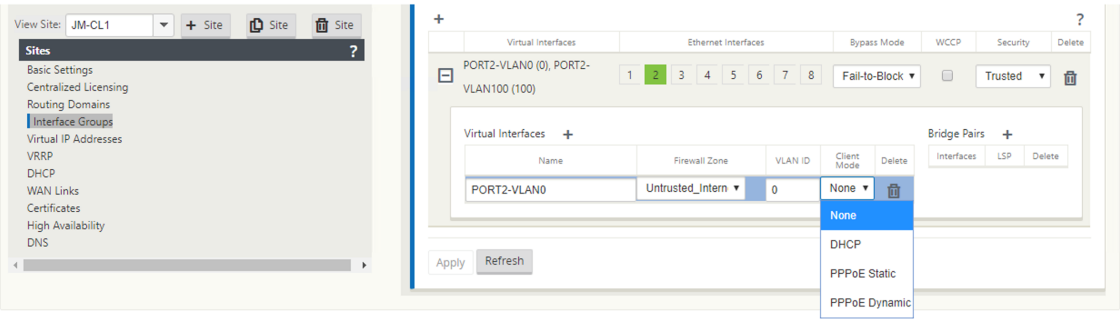


3. 选择 **MCN** 站点的接口组。请执行以下操作：

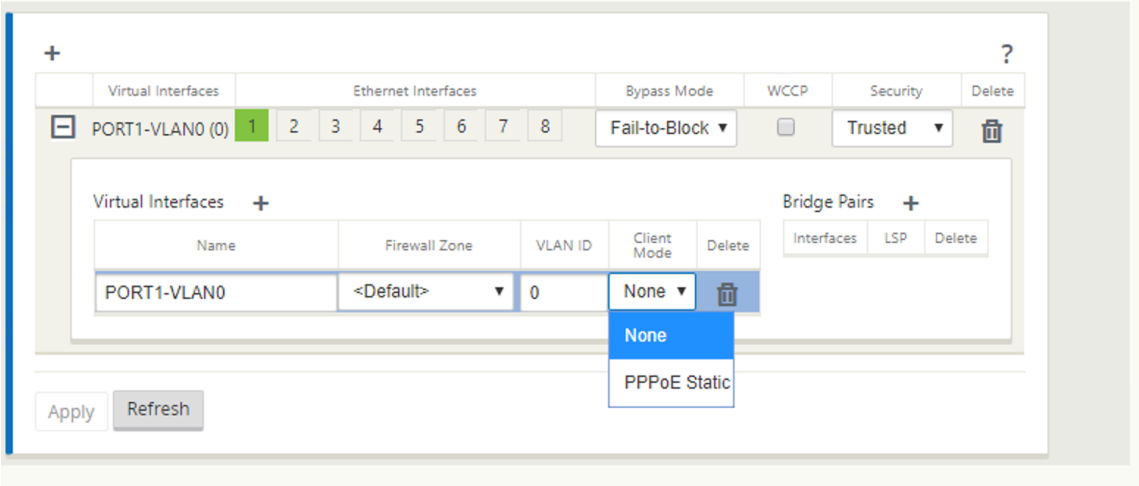
   - 添加虚拟接口。
   - 配置以太网接口。
   - 配置旁路模式。
   - 如有必要，请选择 **WCCP**。
   - 选择安全性—可信/不可信。

   对于虚拟接口：

- 配置名称、防火墙区域、VALN ID 和客户端模式。
- 配置了多个接口的 VNI 只能有一个接口用于 PPPoE 连接。
- 如果配置了多个接口和 PPPoE 连接的 VNI 更改为不同的接口，则可以使用监视器页面停止现有会话并启动新会话，然后可以在新接口上建立新会话。



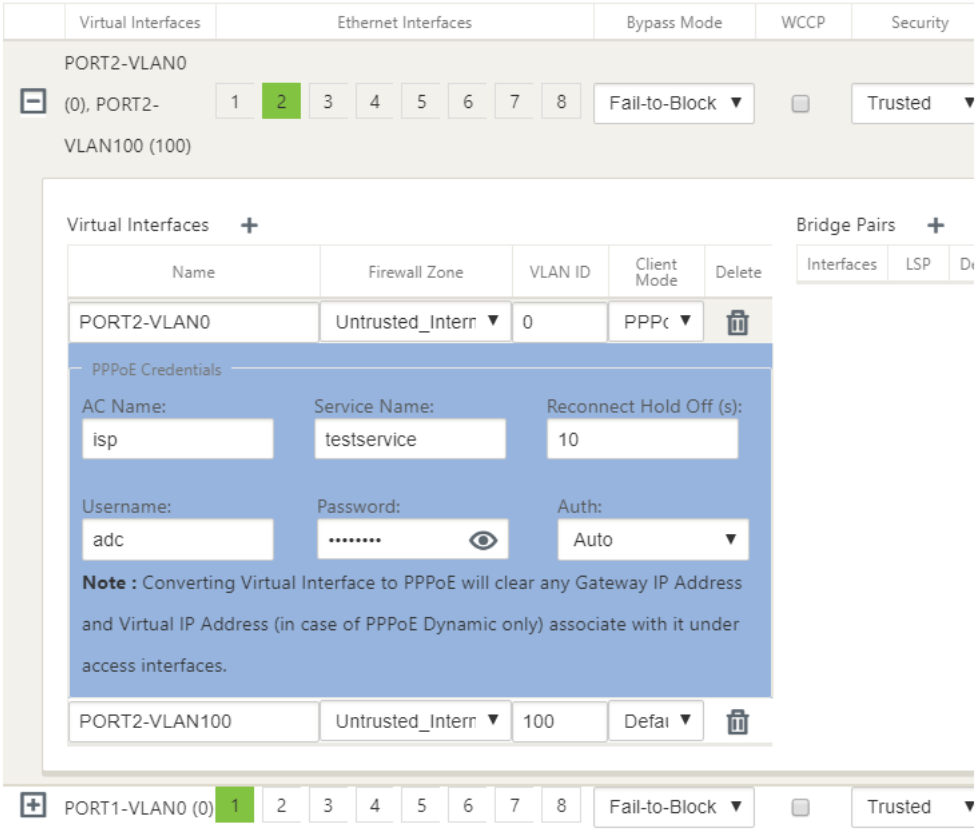
4. 根据您对 MCN 设备上的客户端模式选项的网络配置要求，选择 **PPPoE** 静态或无。将显示以下更多选项。



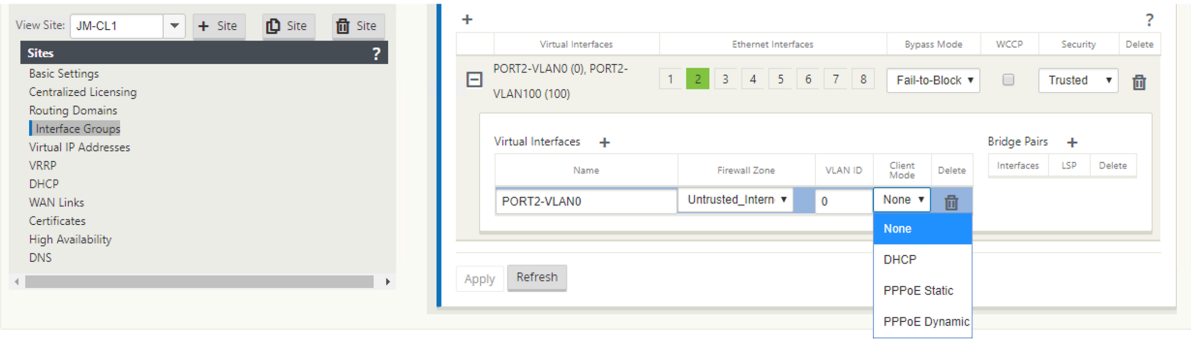
配置以下 PPPoE 参数，然后单击应用。

- 访问集中器 (AC) 名称字段。
- Service Name（服务名称）。
- 保留重新连接时间（默认为立即重新连接，’0’）
- 身份验证类型-（自动/PAP/CHAP/EAP）。
  - 当身份验证选项设置为自动时，SD-WAN 设备将接受从服务器接收的受支持的身份验证协议请求。
  - 将 Auth 选项设置为 PAP/CHAP/EAP 时，将仅接受特定的身份验证协议。如果 PAP 在配置中并且服务器使用 CHAP 发送身份验证请求，连接请求将被拒绝。如果服务器不与 PAP 协商，则会出现身份验证失败。
- CHAP 包括–CHAP、Microsoft CHAP 和 Microsoft CHAPv2。
- EAP 支持 EAP-MD5。

- 用户名和密码。



下图显示了分支 SD-WAN 设备的 PPPoE 客户端模式选项。如果选择 PPPoE 动态，则 VNI 必须为“不受信任”。

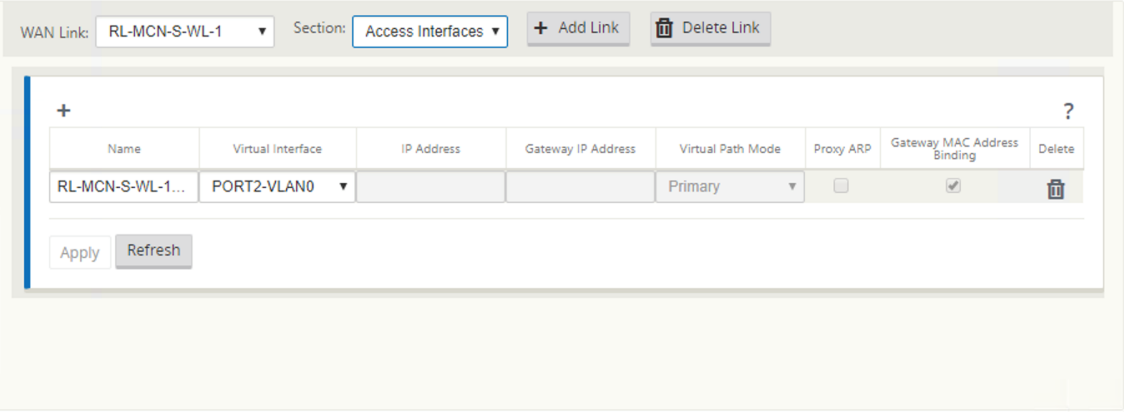


配置 **WAN** 链接

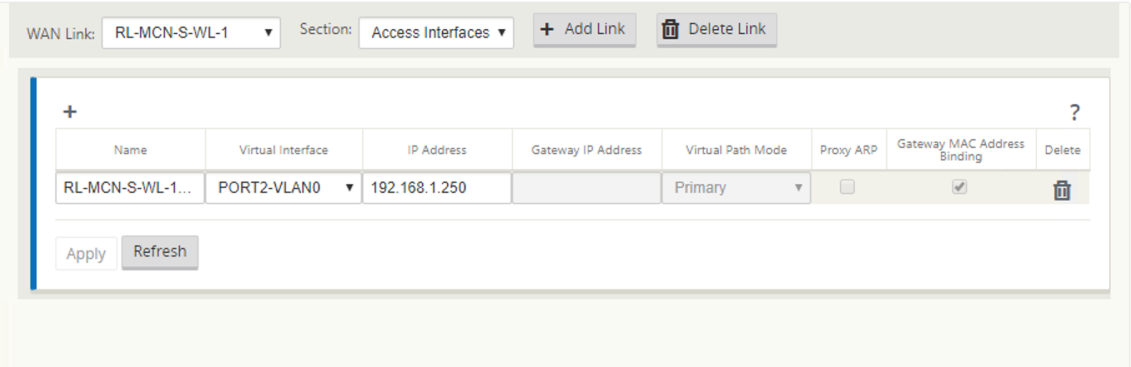
1. 在 SD-WAN GUI 中，导航到 站点 **> WAN** 链接。每个 PPPoE 静态或动态 VNI 只允许创建一个 WAN 链接。WAN 链接配置因客户端模式的 VNI 选择而异。
2. 如果 VNI 配置为 PPPoE 动态客户端模式：
   - IP 地址和网关 IP 地址字段变为非活动状态。

- 虚拟路径模式设置为“主”。
- 无法配置代理 ARP。

默认情况下，选择网关 MAC 地址绑定。



3. 如果 VNI 配置了 PPPoE 静态客户端模式，请配置 IP 地址。



> 注意：
>
> 如果服务器不遵守配置的静态 IP 地址并提供不同的 IP 地址，则会发生错误。PPPoE 会话尝试定期重新建立连接，直到服务器接受配置的 IP 地址。

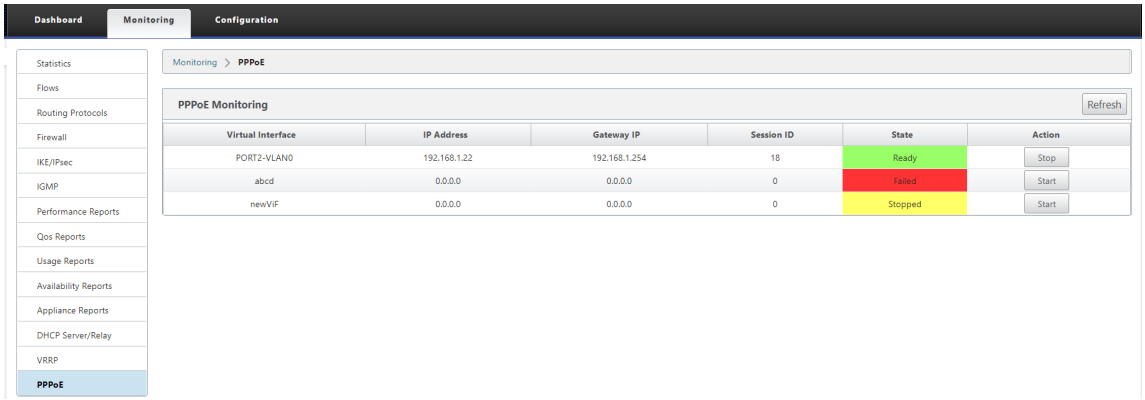
监测 **PPPoE** 会议

您可以通过导航到 SD-WAN GUI 中的 监视 **> 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。它允许您手动启动或停止会话以进行故障排除。

- 如果 VNI 已启动并准备就绪，则 **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。
- 将鼠标悬停在网关 IP 列上显示从接收会话和 IP 的 PPPoE 访问集中器的 MAC 地址。

- 将鼠标悬停在“状态”值上会显示一条消息，这对于“失败”状态更有用。



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。

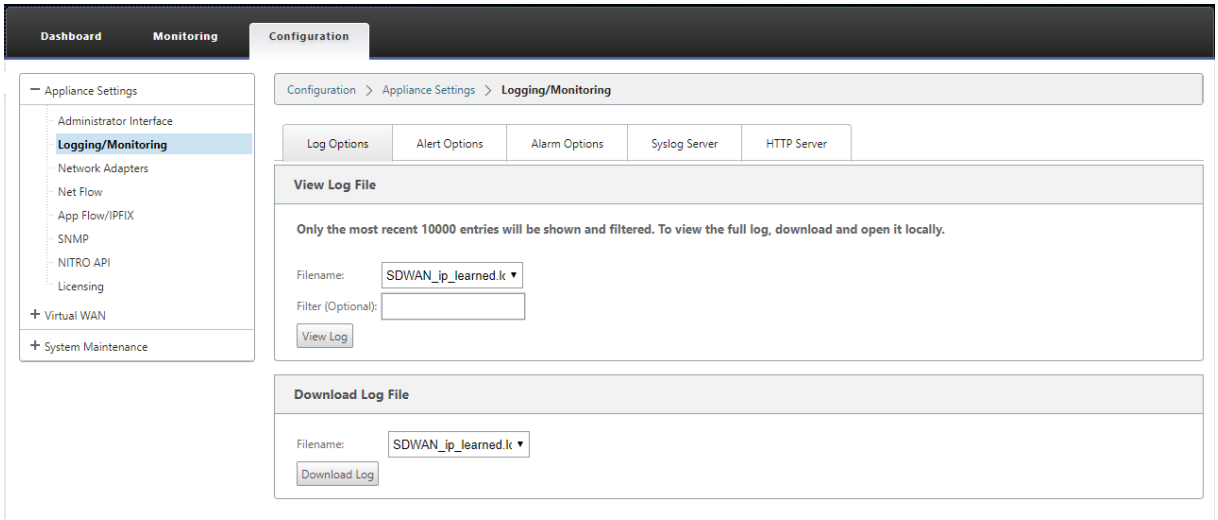
- 如果故障正常，它将立即重新启动。
- 如果失败是错误，则重新启动将恢复 10 秒。
- 如果失败是致命的，则重新启动将恢复 30 秒，然后重新启动。

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

日 志 文件包含与 PPPoE 相关的日志。

要从 SD-WAN GUI 查看或下载 *SDWAN_IP_learne.log* 文件，请导航到 设备设置 > 日 志/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。

班级

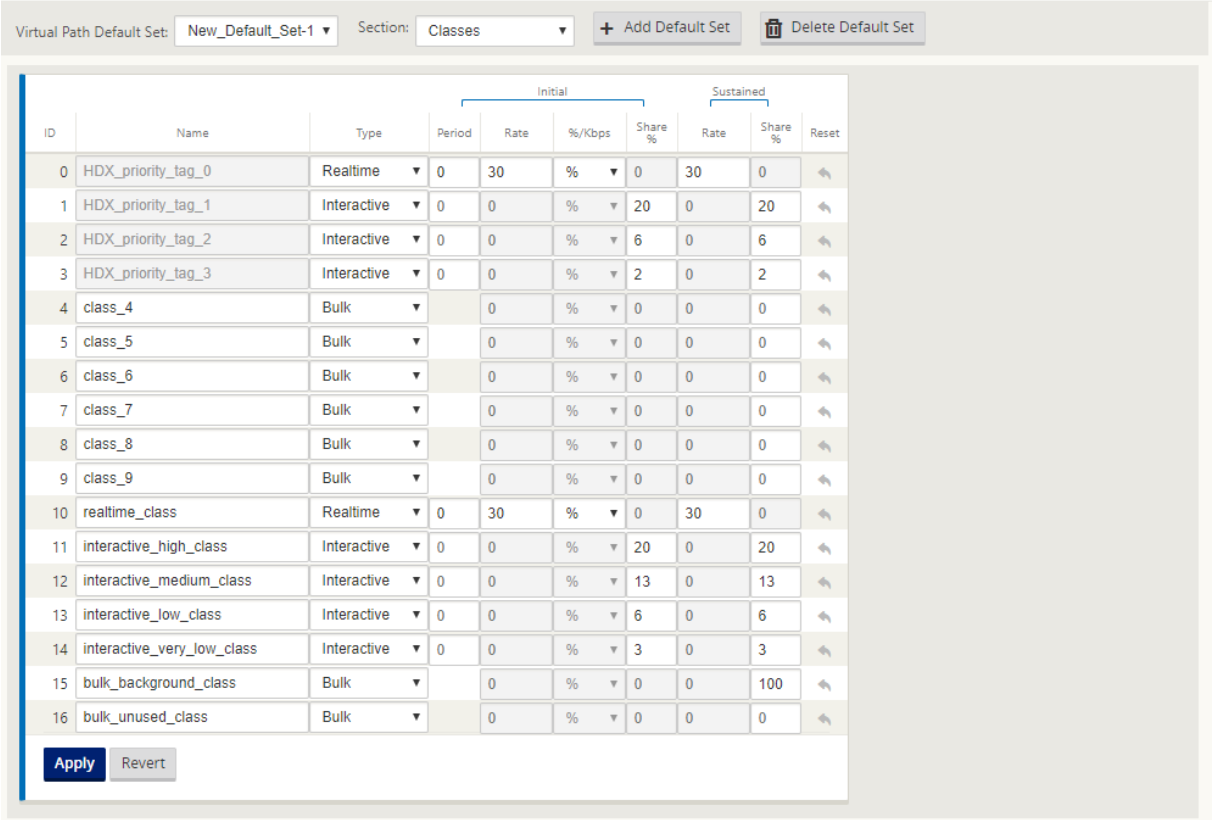
November 1, 2021

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。

有关应用程序 QoS 和基于 IP 地址/端口的 QoS 的更多信息，请参阅 按应用程序名称规则和按 IP 地址和端口号 分别规则。

SD-WAN 提供 17 个类（ID：0—16）。以下是所有 17 个类的默认配置。



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：用于具有中低延迟要求和中低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%

带宽分配结果为

- 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。

要自定义类：

1. 如果正在使用虚拟路径默认集，则可以在“全局”**>** “虚拟路径默认集”下修改类。

   > 注意
   >
   > 您还可以在虚拟路径级别修改类（连接**->** 虚拟路径**->** 类）

2. 单击 添加默认集，输入默认集的名称，然后单击 添加。在“节”字段中，选择“类”。
3. 在 名称 字段中，保留默认名称或输入您选择的名称。
4. 在类型字段中，选择班级类型（实时、交互或批量）。
5. 对于实时类，您可以指定以下属性：
   - 初始周期：在切换到持续速率之前应用初始速率的时间周期（以毫秒为单位）。
   - 初始速率：最初期间数据包离开队列的最大速率或百分比。
   - 持续速率：初始周期后数据包离开队列的最大速率或百分比。
6. 对于交互式类，您可以指定以下属性：
   - 初始周期：在切换到持续百分比之前应用初始可用带宽百分比的时间段（以毫秒为单位）。通常情况下，20 毫秒。
   - 初始共享百分比：在初始时段实时服务后，虚拟路径带宽的最大份额。

- 持续共享百分比：在初始时段后为实时流量提供服务后，虚拟路径带宽的最大份额。

7. 对于批量类，您只能指定持续份额 **(%)**，该百分比确定在提供实时和交互式流量后用于批量类的剩余虚拟路径带宽。
8. 单击应用。

> 注意：
>
> 保存配置，将其导出到变更管理收件箱，然后启动变更管理进程。

按 **IP** 地址和端口号进行规则

June 22, 2021

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)”。

使用配置编辑器，您可以为流量创建规则，并将规则与应用程序和类关联。您可以指定筛选流量的条件，并可以应用常规行为、LAN 到 WAN 行为、WAN 到 LAN 行为和数据包检查规则。

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。

按 **IP** 地址和端口号创建规则

1. 在 SD-WAN 配置编辑器中，导航到“全局”> “虚拟路径默认集”。

   > 注意
   >
   > ：您可以通过导航到站点 **>** 连接 **>** 虚拟路径 **>** 规则在站点级别创建规则。

2. 单击 添加默认集，输入默认集的名称，然后单击 添加。在部分字段中，选择 规则，然后单击 **+**。
3. 在“订单”字段中，输入定单值以定义在相对于其他规则应用规则的时间。
4. 在 规 则组名称 字段中，选择一个规则组。具有相同规则组的规则的统计数据将被分组，并可一起查看。

   要查看规则组，请导航到 监控 **>** 统计信息，然后在 显示 字段中选择 规则组。

   您还可以添加自定义应用程序。有关详细信息，请参阅添加 规则组并启用 MOS。

5. 在 路由域 字段中，选择一个已配置的路由域。

6. 您可以定义规则匹配条件，以根据以下列出的参数过滤服务。过滤后，规则设置将应用于符合这些条件的服务。

   - 源 **IP** 地址：与流量匹配的源 IP 地址和子网掩码。
   - 目标 **IP** 地址：目标 IP 地址和与流量匹配的子网掩码。

     > 注意
     >
     > 如果选中了 **Dest=Src** 复选框，则源 IP 地址也将用于目标 IP 地址。

   - 协议：与流量匹配的协议。
   - 源端口：要与流量匹配的源端口号或端口范围。
   - 目标端口：要与流量匹配的目标端口号或端口范围。

     > 注意
     >
     > 如果选中了 **Dest=Src** 复选框，则源端口也将用于目标端口。

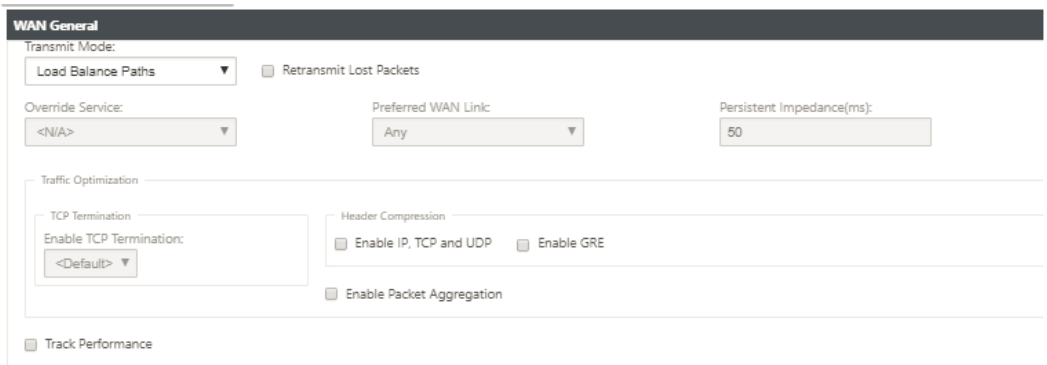
   - **DSCP**：IP 标头中要与流量匹配的 **DSCP** 标记。
   - **VLAN**：要与流量匹配的 **VLAN ID**。

7. 单击新规则旁边的添加 (+) 图标。
8. 单击 使用协议初始化属 性 可通过应用规则默认值和协议的推荐设置来初始化规则属性。这将填充默认规则设置。您还可以手动自定义设置，如以下步骤所示。
9. 单击 **WAN** 常规 磁贴以配置以下属性。

   - 发射模式：选择以下发射模式之一。
     - 负载平衡路径：流的流量将在服务的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。剩余的数据包通过下一个最佳路径发送。
     - 持久路径：流的流量保持在同一路径上，直到路径不再可用。
     - 重复路径：流量在多个路径上复制，从而提高可靠性。
     - 覆盖服务：流的流量覆盖到不同服务。在 覆盖服务 字段中，选择服务覆盖的服务类型。例如，虚拟路径服务可以覆盖到内部网、Internet 或直通服务。
   - 重新传输丢失的数据包：通过可靠服务将与此规则匹配的流量发送到远程设备，然后重新传输丢失的数据包。
   - 启用 **TCP** 终止：为此流启用 TCP 终止流量。缩短了数据包确认的往返时间，从而提高了吞吐量。
   - 首选 **WAN** 链接：流应首先使用的 WAN 链接。
   - 持久阻抗：在路径超过配置值的等待时间之前，流量将保持在同一路径中的最短时间（以毫秒为单位）。
   - 启用 **IP**、**TCP** 和 **UDP**：压缩 IP、TCP 和 UDP 数据包中的标头。

> 注意
>
> IPv6 数据包不支持报头压缩。

- 启用 **GRE**：压缩 GRE 数据包中的标头。
- 启用数据包聚合：将小数据包聚合到较大的数据包中。
- 跟踪性能：将此规则的性能属性记录在会话数据库中（例如，丢失、抖动、延迟和带宽）。

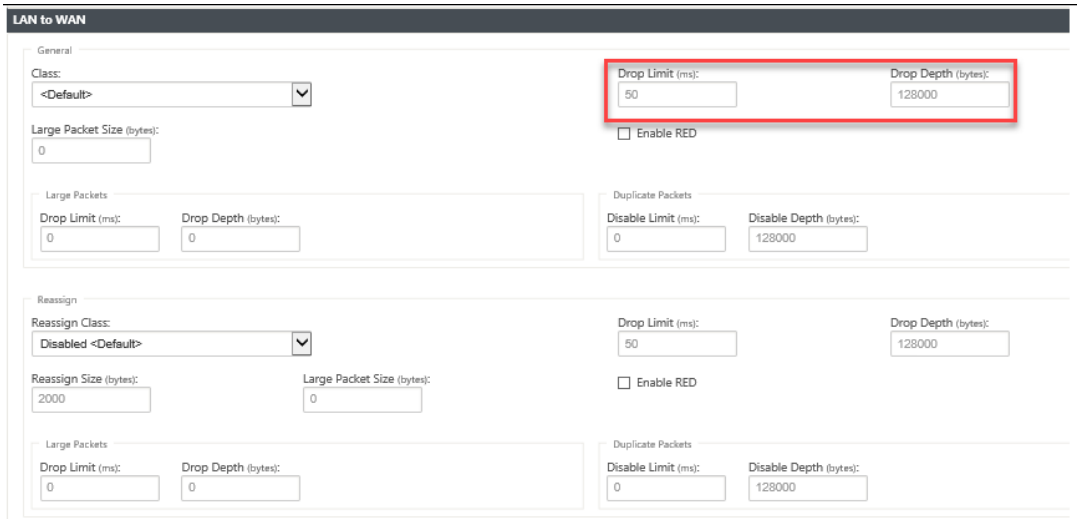


10. 单击 **LAN** 到 **WAN** 磁贴，以便为此规则配置 LAN 到 WAN 行为。

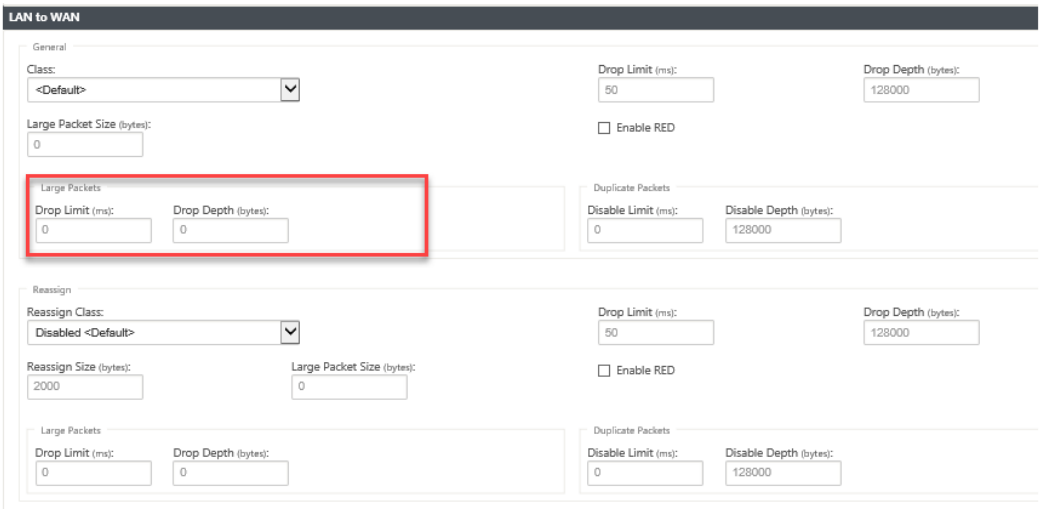
- 类：选择要将此规则关联的类。

> 注意
>
> 您还可以在应用规则之前自定义类，有关更多信息，请参阅如何自定义类。

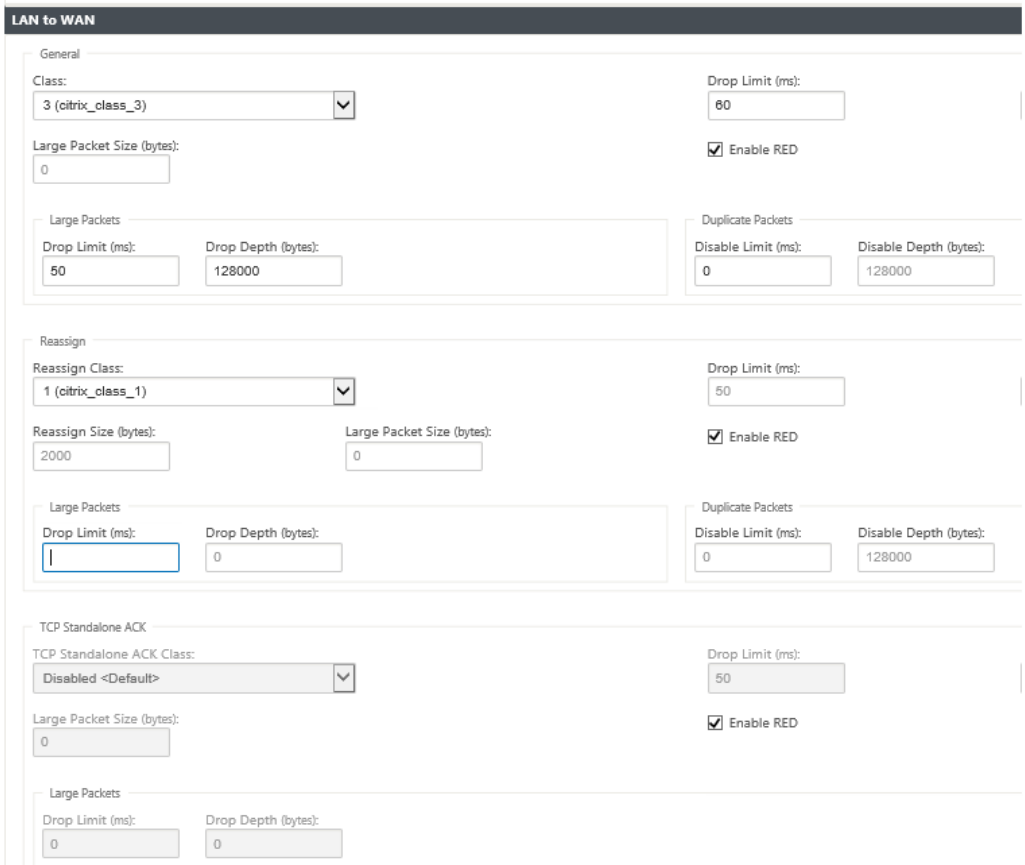
- 大数据包大小：小于或等于此大小的数据包将被分配在 类字段右侧的字段中指定的 放置限制和 放置深度值。



大于此大小的数据包将按屏幕的“大数据包”部分的默认“丢弃限制”和“丢弃深度”字段中指定的值分配。

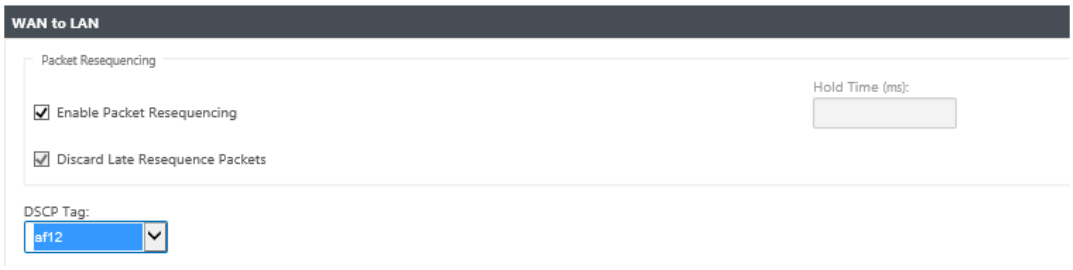


- 删除限制：删除类调度程序中等待的数据包之后的时间长度。不适用于批量类。
- 丢弃深度：队列深度阈值之后丢弃数据包。
- 启用 **RED**：随机早期检测 (RED) 通过在发生拥塞时丢弃数据包，确保公平共享类资源。
- 重新分配大小：超过数据包长度时会导致数据包重新分配到 重新分配类 字段中指定的类。
- 重新分配类：当数据包长度超过 重新分配大小 字段中指定的数据包长度时使用的类。
- 禁用限制：可禁用重复以防止重复数据包消耗带宽的时间。
- 禁用深度：类调度程序的队列深度，此时不会生成重复的数据包。
- **TCP** 独立 **ACK** 类：在大型文件传输过程中 TCP 独立确认映射到的高优先级类。



11. 单击 **WAN** 转 **LAN** 磁贴以配置此规则的 WAN 到 LAN 行为。

    - 启用数据包重新同步：将数据包排序到目标处的正确顺序。
    - 保留时间：保留数据包以重新同步的时间间隔，之后数据包将发送到 LAN。
    - 丢弃延迟重新分配数据包：丢弃在重新分配所需的数据包发送到 LAN 之后到达的不顺序的数据包。
    - **DSCP** 标记：DSCP 标记应用于与此规则匹配的数据包，然后将其发送到 LAN。



12. 单击 深度数据包检查 磁贴，然后选择 启用被动 **FTP** 检测，以允许规则检测用于 FTP 数据传输的端口，并自动将规则设置应用于检测到的端口。

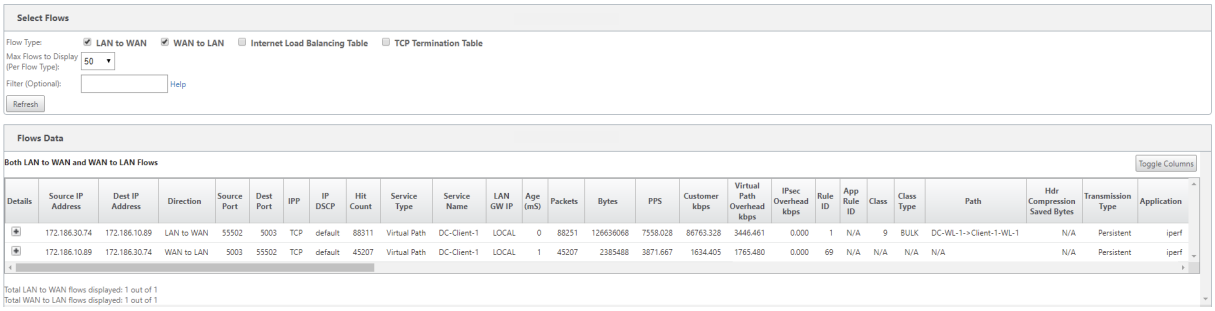
13. 单击应用。

> 注意
>
> 保存配置，将其导出到更改管理收件箱，然后启动更改管理过程。

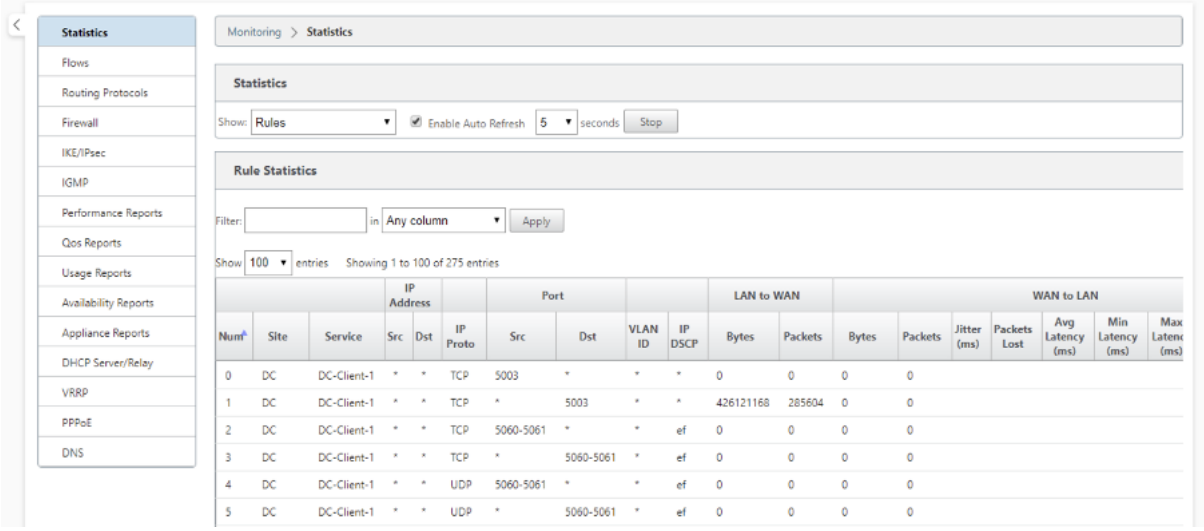
验证规则

在配置编辑器中，导航到监视 **>** 流程。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。



在配置编辑器中，导航到 监控 **>** 统计信息，然后验证配置的规则。



按应用程序名称进行的规则

June 22, 2021

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筛选流量，并将应用程序规则应用于这些流量。应用程序规则与互联网协议 (IP) 规则类似。有关知识产权规则的信息，请参阅 规则按 IP 地址和端口号。

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：应用程序流量保持在同一路径上，直到路径不再可用。
- 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)	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_1	(HDX_priority_tag_1)	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_2	(HDX_priority_tag_2)	负载平衡路径	真	假	真	250	真	350	30000	真	0	128000
HDX_Priority_3	(HDX_priority_tag_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。

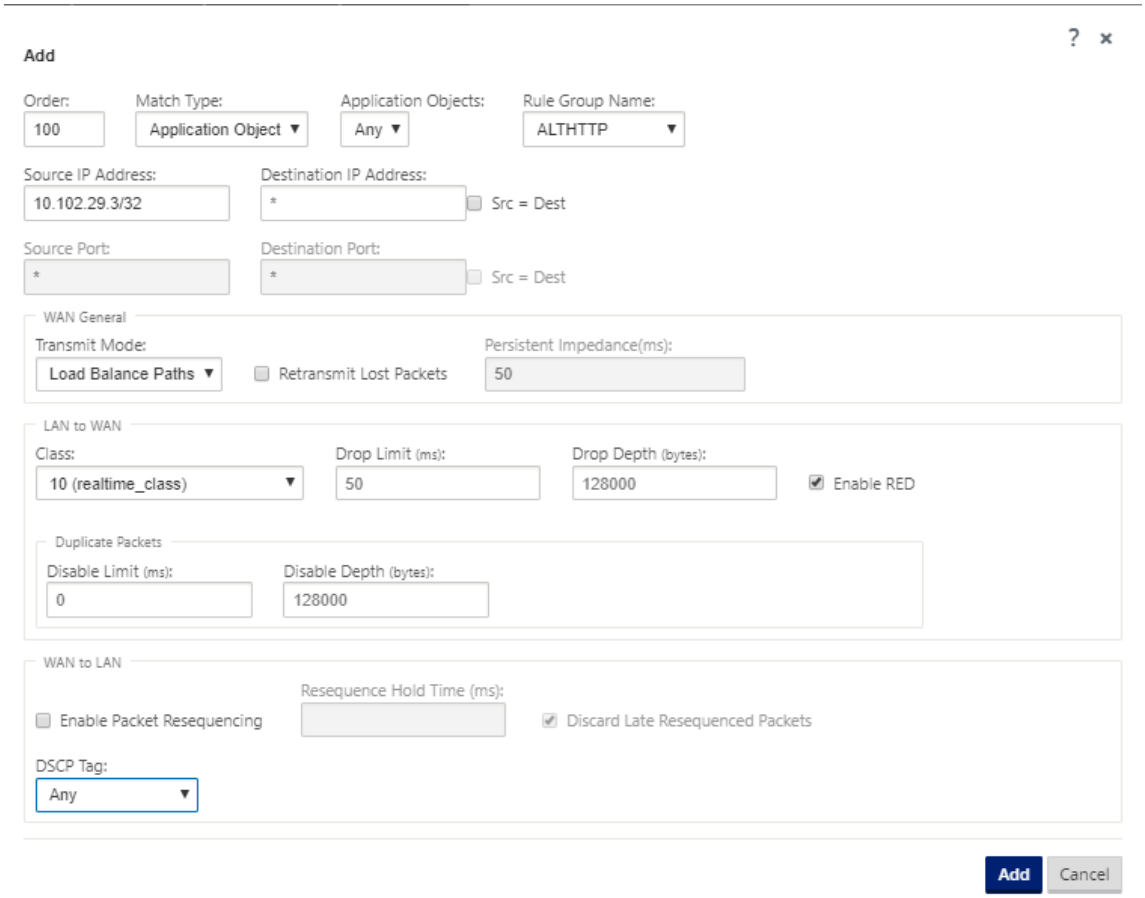
例如，假设您已为使用 SMTP 协议的 Web 邮件应用程序（例如 Google Mail）指定了应用程序规则。SMTP 协议的 IP 规则集最初应用于 DPI 分类之前。解析数据包并将其分类为属于 Google Mail 应用程序后，应用为 Google Mail 应用程序指定的应用程序规则。

创建应用程序规则

要创建应用程序规则，请执行以下操作：

1. 在 SD-WAN 配置编辑器中，导航到“全局”> “虚拟路径默认集”。
2. 单击 添加默认集，输入默认集的名称，然后单击 添加。在 部分 字 段 中，选择 应用程序 **QoS**，然后单击 **+**。

> 注意
>
> 您还可以通过导航到“连接”> “虚拟路径”> “应用程序 **QoS** ”或“全局”> “动态虚拟路径默认集”> “应用程序 **QoS**”来创建应用程序规则。



3. 在定 单 字段中，键入定单值以定义规则何时应用与其他规则相关。
4. 在 匹配类型 字段中，选择以下匹配类型之一：
   - 应用程序—如果选择了此匹配类型，则指定用作此筛选器匹配条件的应用程序。
   - 应用程序系 列—如果选择了此匹配类型，请选择用作此筛选器匹配条件的应用程序系列。
   - 应用程序对象—如果选择了此匹配类型，请选择用作此筛选器的匹配条件的应用程序对象。

   有关应用程序、应用程序系列和应用程序对象的更多信息，请参阅应用程序分类。
5. 在 规 则组名称 字段中，选择一个规则组。具有相同规则组的规则的统计数据将被分组，并可一起查看。

   要查看规则组，请导航到“监视” > “统计”，然后在“显示”字段中选择“规则组”。

   您还可以添加自定义规则组。有关详细信息，请参阅添加自定义应用并启用 MOS。
6. 指定以下应用程序规则匹配条件以筛选应用程序流量。过滤后，规则设置将应用于符合这些条件的服务。
   - 源 **IP** 地址：与流量匹配的源 IP 地址和子网掩码。
   - 目标 **IP** 地址：目标 IP 地址和与流量匹配的子网掩码。
   - 源端口：要与流量匹配的源端口号或端口范围。
   - 目标端口：要与流量匹配的目标端口号或端口范围。

> 注意
>
> 如果源和目标互联网协议地址相同，请选择 **Src = Destt**。

7. 配置以下常规 WAN 设置：

   - 在 发 射模式 字段中，选择以下发射模式之一：

     – 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，直到完全使用该路径为止。剩余的数据包将通过下一个最佳路径发送。

     – 持久路径：应用程序流量保持在同一路径上，直到路径不再可用。

       在 持 久阻抗 字段中，指定流量将保持在同一路径中的最短时间（以毫秒为单位），直到路径上的等待时间长于配置的值。

     – 重复路径：应用程序流量跨多个路径复制，从而提高可靠性。

   - 选中 重新传输丢失 的数据包 以通过可靠服务将与此规则匹配的流量发送到远程设备，并重新传输丢失的数据包。

8. 将 LAN 配置为 WAN 设置：

   - 类：选择要将此规则关联的类。

     您还可以在应用规则之前自定义类，有关详细信息，请参阅 自定义类。

   - 删除限制：删除类调度程序中等待的数据包之后的时间长度。不适用于批量类。
   - 丢弃深度：队列深度阈值，超过该阈值将丢弃数据包
   - 启用 **RED**：随机早期检测 (RED) 通过在发生拥塞时丢弃数据包，确保公平共享类资源。
   - 禁用限制：可以禁用复制以防止重复数据包消耗带宽的时间。
   - 禁用深度：类调度程序的队列深度，此时不会生成重复的数据包。

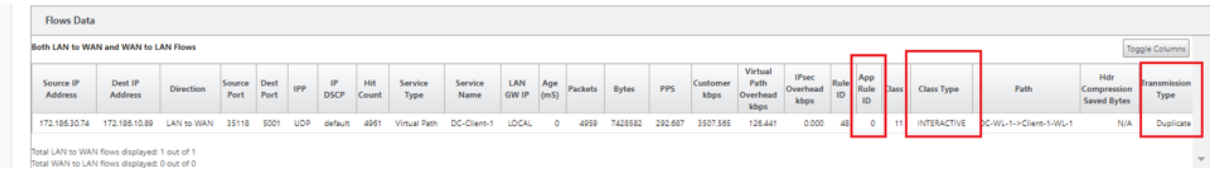
9. 为此规则配置以下 WAN 到 LAN 行为：

   - 启用数据包重新同步：在目标处按正确顺序排列数据包。
   - 重新平衡保留时间：保留数据包以进行重新平衡的时间间隔，之后数据包将发送到 LAN。
   - 丢弃延迟重新分配数据包：丢弃在重新分配所需的数据包发送到 LAN 之后到达的不顺序的数据包。

10. 单击应用。

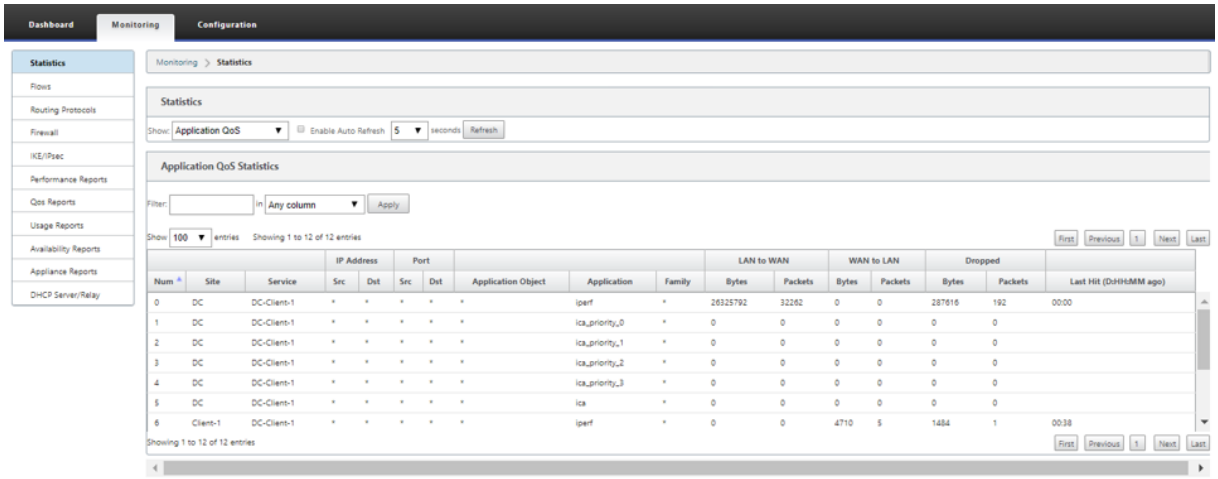
要确认应用程序规则是否应用于流量流，请导航到 监视 > 流 量。

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

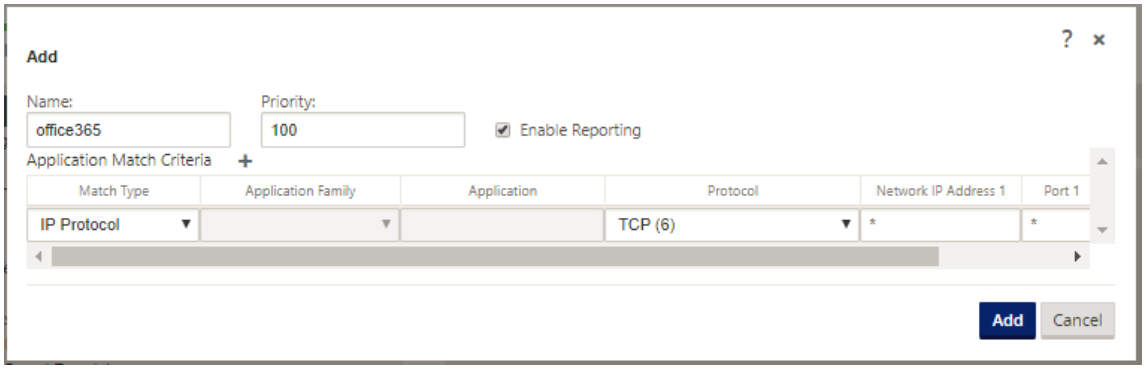
DPI 分类器分析传入的数据包，并根据指定的匹配条件将其分类为应用程序。您可以在 QoS、防火墙和应用程序路由中使用这些分类的自定义应用程序。

> 提示
>
> 您可以指定一个或多个匹配类型。

您可以在 SD-WAN Center 查看分类自定义应用程序的报告。有关详细信息，请参阅应用程序报告。

要创建自定义应用程序，请执行以下操作：

1. 在配置编辑器中，导航到 全局 > 应用程序 > 自定义应用程序，然后单击 **+**。



2. 设置以下参数：

   - 名称：自定义应用程序的名称
   - 启用报告：允许在 SD-WAN Center 查看自定义应用程序报告。有关详细信息，请参阅应用程序报告。
   - 优先级：自定义应用程序的优先级。当传入的数据包匹配两个或多个自定义应用程序定义时，将应用具有最高优先级的自定义应用程序定义。

3. 在 应用程序匹配条件 部分单击 +。

4. 选择以下匹配类型之一：

   - **IP** 协议：指定协议、网络 IP 地址、端口号和 DSCP 标签。
   - 应用程序：指定应用程序名称、网络 IP 地址、端口号和 DSCP 标签。
   - 应用程序系列：选择应用程序系列并指定网络 IP 地址、端口号和 DSCP 标记。

5. 单击 **+** 添加更多应用程序匹配条件。

6. 单击应用。

添加 规则组并启用 **MOS**

June 22, 2021

网络中的特定应用程序可以由应用于该应用程序的一组规则来定义。SD-WAN 配置编辑器提供了规则组的默认列表。您还可以创建自定义规 则组，并将单个 IP 规则或应用程序 QoS 规则标记到应用程序。

有关规则的更多信息，请参阅按 IP 地址和端口号进行规则和按应用程序名称规则。

具有相同规则组的规则的统计数据将分组在一起，并可以一起查看。

要查看基于规则组的统计信息，请导航到 “监视” **>** “统计信息”，然后在“显示”字段中选择“规则组”。

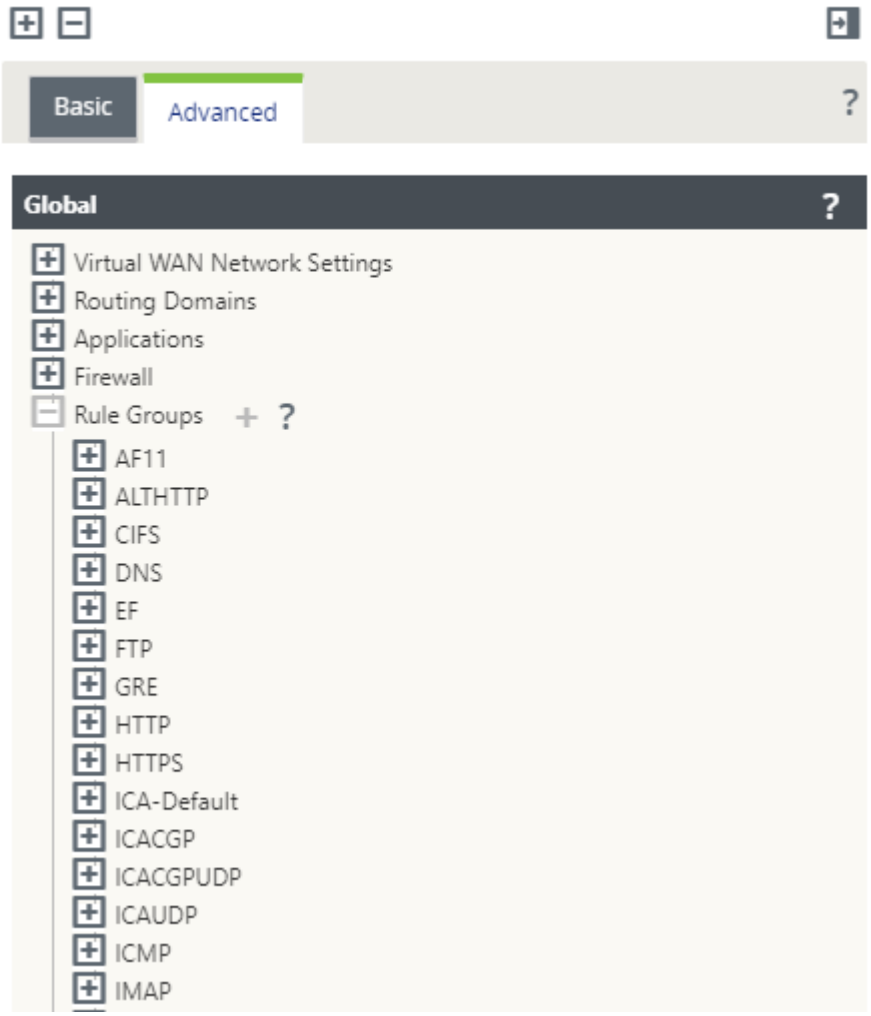
平均意见评分 (MOS) 是衡量应用程序向最终用户提供的体验质量的数值测量。它主要用于 VoIP 应用程序。在 SD-WAN 中，MOS 也用于评估非 VoIP 应用程序的质量，方法是判断流量，就像是 VoIP 通话一样。

平均 MOS 分数按 1 分钟的采样间隔计算。由其他第三方工具计算的 MOS 分数可能会有所不同，具体取决于所使用的采样间隔。

SD-WAN Center 显示通过虚拟路径的现有流量的 MOS。有关在 SD-WAN Center 查看 MOS 的更多信息，请参阅MOS 应用。

要添加自定义规则组，请执行以下操作：

1. 在配置编辑器中，导航到“全局”> “规则组”。。此时将显示 规则组的默认列表。
2. 单击添加 (+) 图标。
3. 输入应用程序名称。
4. 单击编辑图标，然后选择 启用 **MOS** 。



5. 单击应用。

> 注意
>
> - 您还可以通过选择启用 MOS 来 启用默认应用程序的 **MOS** 估计。
> - 启用“规则”下的“轨道性能”选项可以估算应用的 MOS，并将其显示在 SD-WAN Center。欲了解更多信息。请参阅MOS 应用。

应用程序分类

November 16, 2022

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。

要启用 DPI 库分类，请在配置编辑器中导航到全局 **>** 应用程序 **> DPI** 设置，然后选中启用深度数据包检查复选框。

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 Standard Edition 不支持通过 SSL/TLS 或 DTLS 传送的 ICA 流量分类，但 SD-WAN Premium Edition 和 SD-WAN WANOP Edition 支持。
>
> 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 功能正常工作，您必须具有 SD-WAN Standard Edition 10.1 或更高版本或 SD-WAN Premium Edition。
> - 要在 SDWAN 中心显示基于 HDX 用户的报告，您必须具有 SD-WAN Standard Edition 或 Premium Edition 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。

要启用基于 ICA 的分类，请在配置编辑器中导航到全局 **>** 应用程序 **> DPI** 设置，然后选中为 **Citrix ICA** 应用程序启用深度数据包检查复选框。

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。

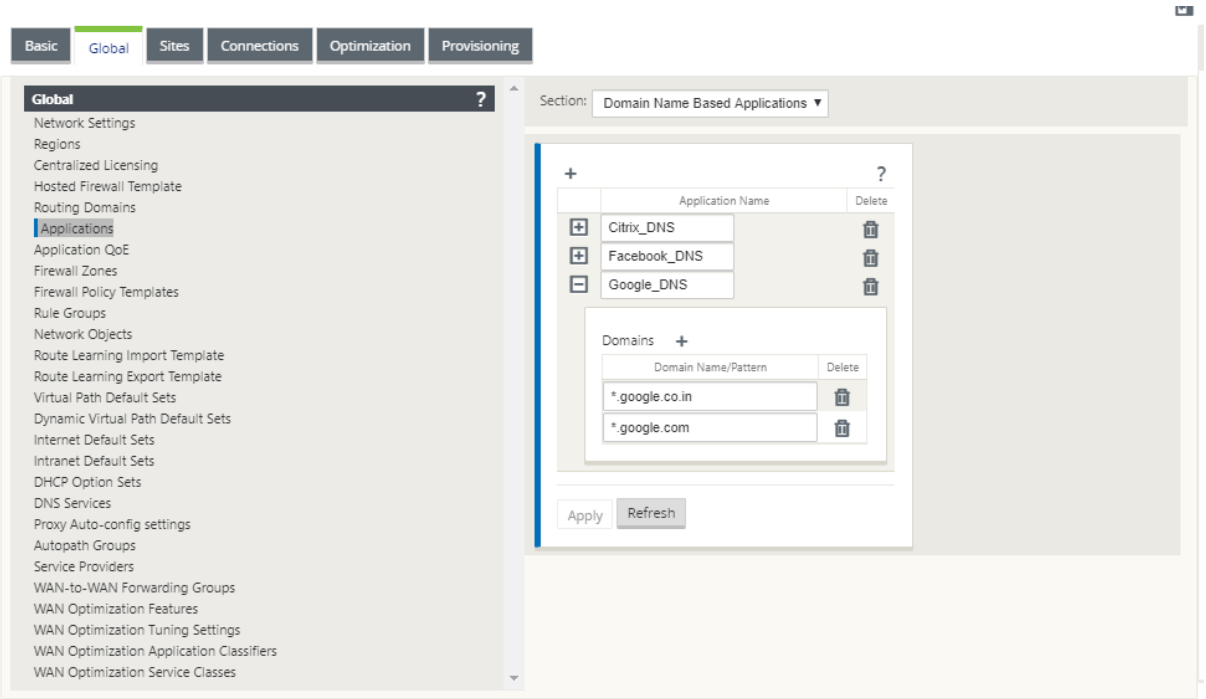
基于域名的应用程序分类

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。

要定义基于域名的应用程序，请在配置编辑器中导航到 全局 > 应用程序 > 基于域名的应用程序。输入应用程序名称并添加所需的域名或模式。您可以在开头输入完整域名或使用通配符。允许使用以下域名格式：

- example.com
- *.example.com



基于分类域名的应用程序用于配置以下内容：

- DNS 代理
- DNS 透明转发器
- 应用程序对象
- 应用程序路由
- 防火墙策略
- 应用 QoS 规则
- 应用程序 QoE

> 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。

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。
- 不支持 AAA 记录或 IPv6 记录。
- 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。

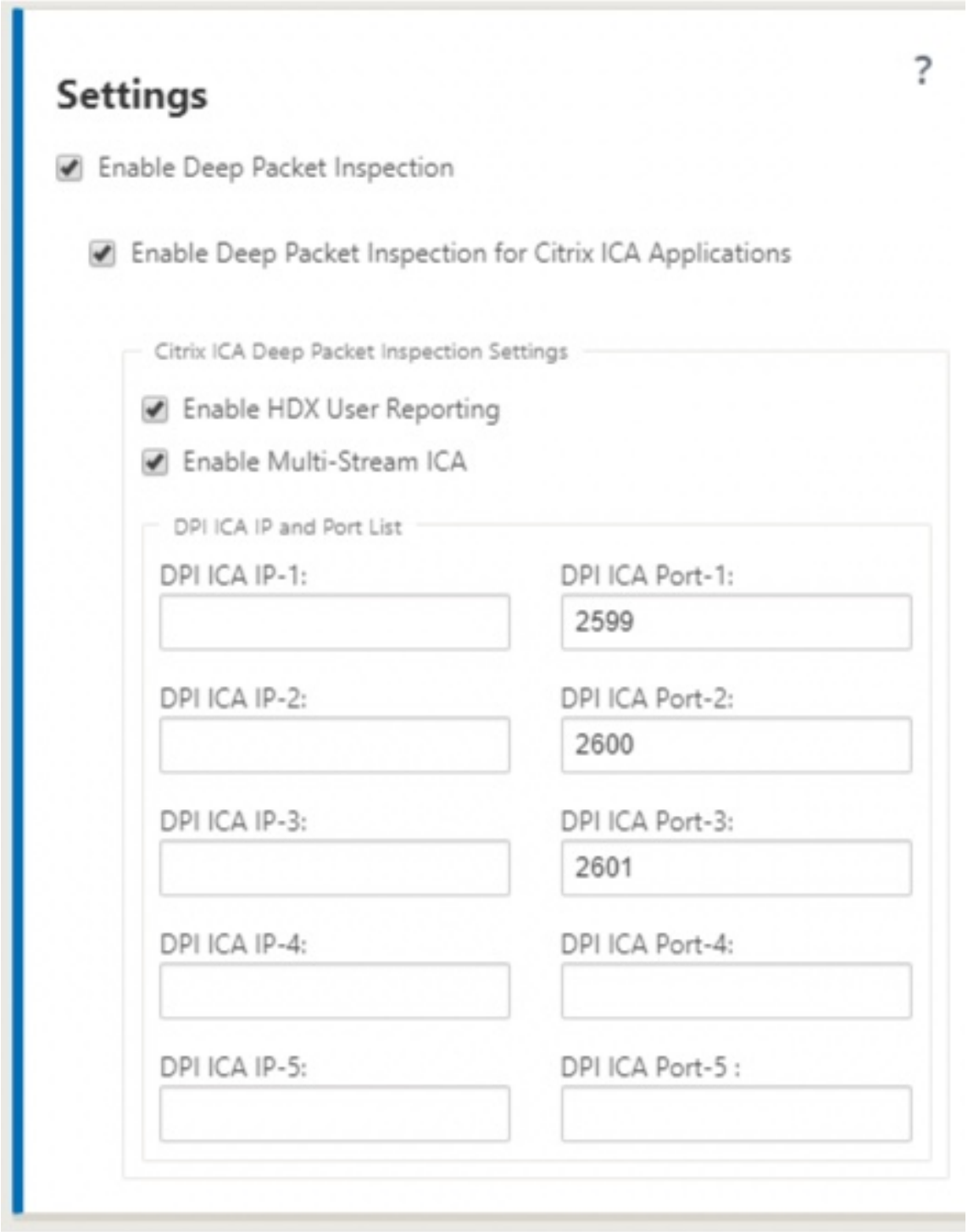
对加密流量进行分类

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。

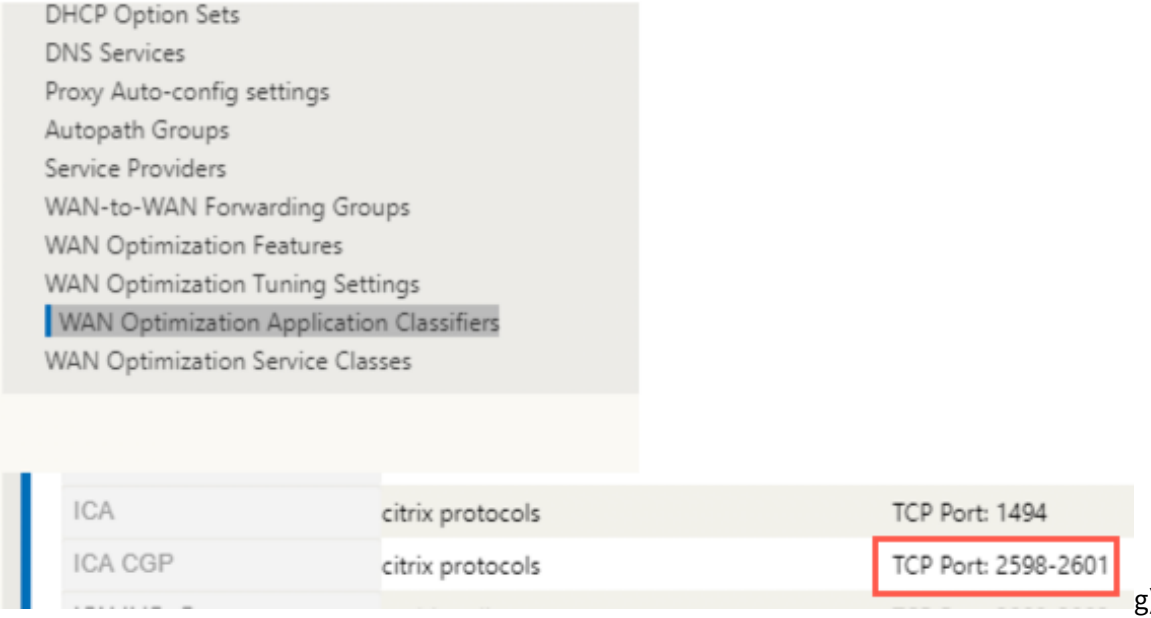
要配置应用程序分类设置，请执行以下操作：

1. 在 配置编辑器中，单击 全局 > 应用程序 > 设置。



注意

如果为多端口部署添加额外的 ICA 端口，则必须将这些端口添加到 WAN 优化应用程序分类器中。否则，三个额外端口上的流量将不会转发到 WANOP。如果将 ICA 配置为优化，则只转发默认的 2598 端口。



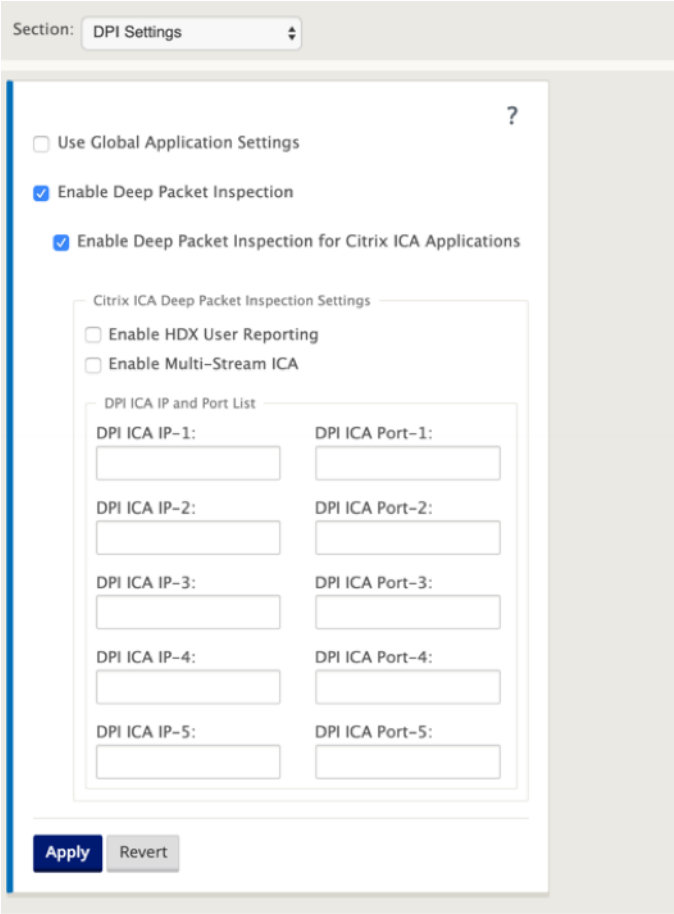
g)

2. 选择 启用深度数据包检查。这将启用设备上的应用程序分类。您可以在 SD-WAN Center 查看和监视应用程序统计信息。有关详细信息，请参阅 应用报告。

   > 注意
   >
   > 默认情况下，启用深度数据包检测 收集分类数据的统计信息

3. 选择 为 **Citrix ICA** 应用程序启用深度数据包检测。这样可以对 Citrix ICA 应用程序进行分类，并收集用户、会话和流量计数的统计信息。如果不启用此选项，可能仍会对 HDX 流量的某些风格进行分类并计算 QoE，但 SD-WAN Center 的统计数据不可用。您可以在 SD-WAN Center 查看和监视 ICA 应用程序统计信息。默认情况下启用此选项。有关更多信息，请参阅 HDX 报告。

4. 选择启用 **HDX** 用户报告以生成新添加的基于用户的报告（HDX 摘要、HDX 用户会话和 **HDX** 应用程序），这些报告在 SD-WAN Center 中提供。这不适用于 **HDX** 站点统计 报告。此选项在全局和站点级别可用，类似于启用 DPI 选项。要在站点级别 启用 **HDX** 用户报告，请在 配置编辑器中单击 连接 **>** 应用程序。



5. 在 **DPI ICA** 端口中，指定用于处理 HDX 分类的 XA/XD 策略中的非标准端口。请勿在此列表中包含标准端口号 2598 或 1494，因为这些端口号已包含在内部。
6. 在 **DPI ICA IP** 中，指定用于进一步将端口限制为特定目标的 IP 地址。

   > 注意
   >
   > 使用“*”表示发往任何 IP 地址的端口。

7. 单击 应用

您可以在每个站点分别配置应用程序分类设置。单击 连接，选择站点，然后单击 应用程序设置。您还可以选择使用全局应用程序设置。

搜索应用程序

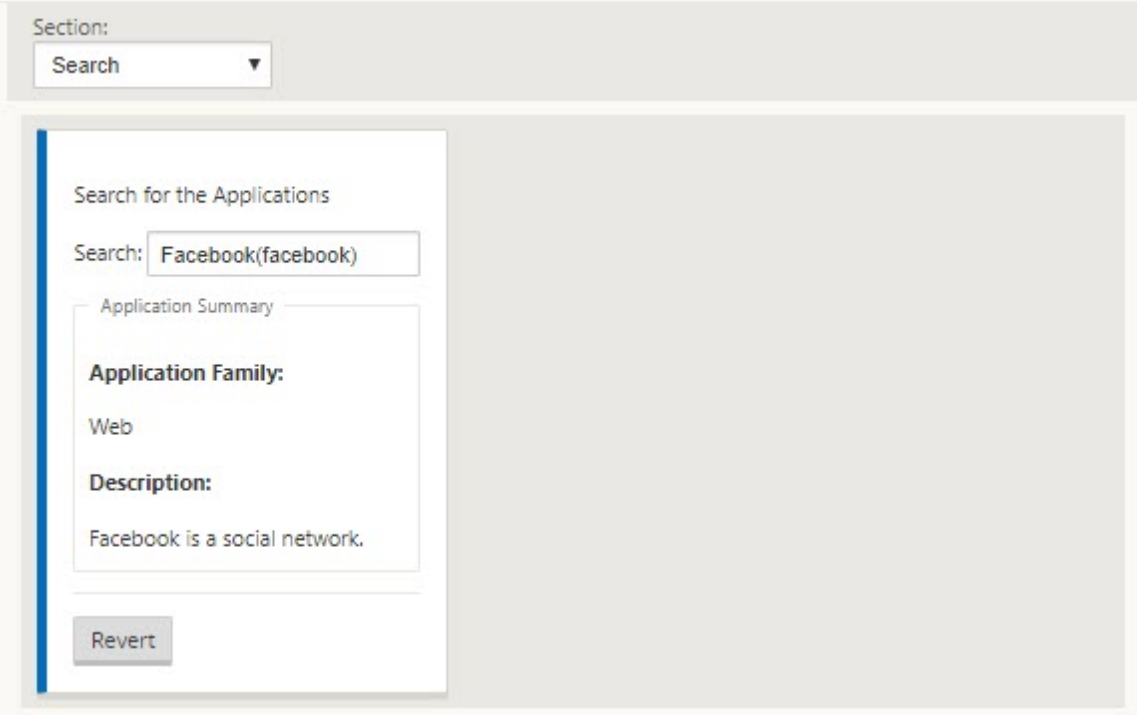
您可以搜索应用程序以确定应用程序的家族名称。此外，还提供了应用程序的简要说明。

要搜索应用程序，请执行以下操作：

1. 在配置编辑器中，单击 全局 > 应用程序 > 搜索。

2. 在 搜索 字段中，应用程序的名称，然后单击 回车。

   此时将显示应用程序和应用程序系列名称的简要描述。



以下功能使用应用程序作为匹配类型：

- 防火墙策略
- 应用 QoS 规则
- 应用程序 QoE

> 注意
>
> 有关 SD-WAN 设备可以使用深度数据包检测识别的应用程序的信息，请参阅应用 程序签名库。

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。

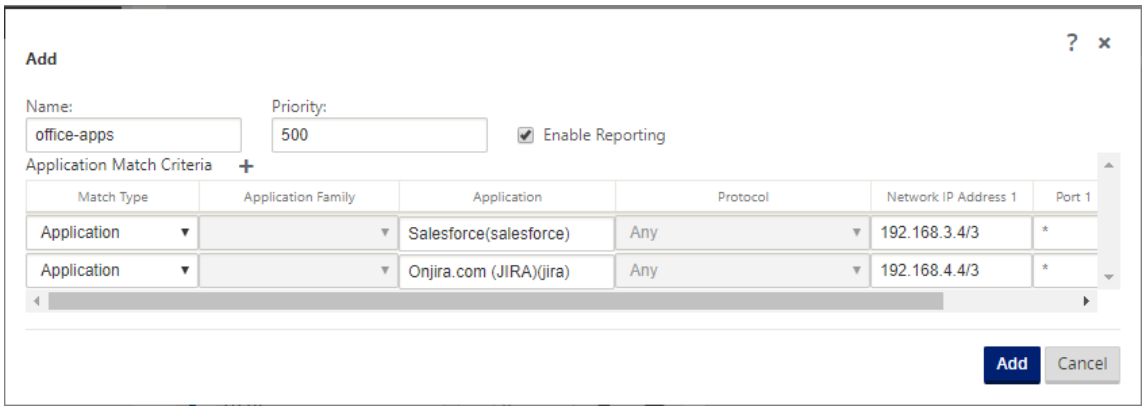
以下功能使用应用程序对象作为匹配类型：

- 应用程序路由
- 防火墙策略
- 应用 QoS 规则

- 应用程序 QoE

要创建应用程序对象，请执行以下操作：

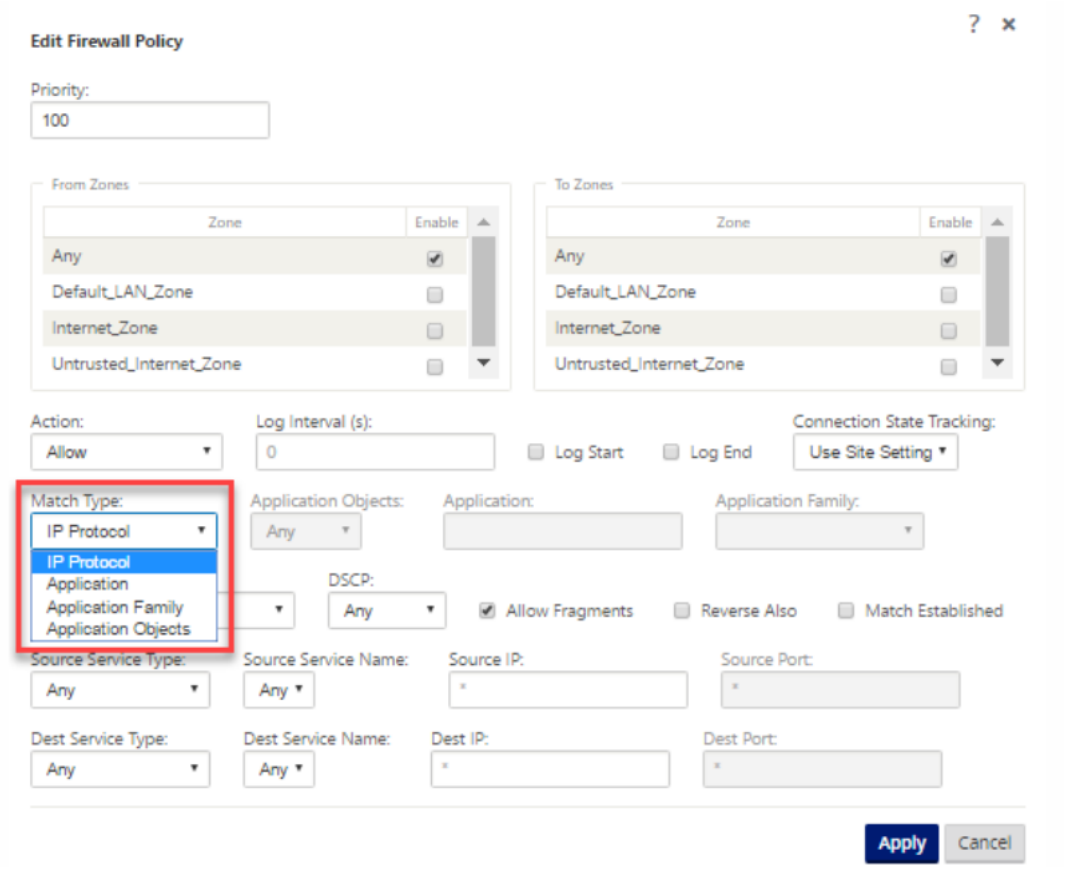
1. 在配置编辑器中，单击 全局 > 应用程序 **>** 应用程序对象。
2. 单击 添加，然后在 名称 字段中输入对象的名称。



3. 选择 启用报 告以允许在 Citrix SD-WAN Center 中查看自定义应用程序报告。有关更多信息，请参阅 应用报告。
4. 在 优先级 字段中，输入应用程序对象的优先级。当传入的数据包匹配两个或多个应用程序对象定义时，将应用具有最高优先级的应用程序对象。
5. 单击“应用程序匹配条件”部分中的 **+** 。
6. 选择以下匹配类型之一：
   - **IP** 协议：指定协议、网络 IP 地址、端口号和 DSCP 标记。
   - 应用程序：指定应用程序名称、网络 IP 地址、端口号和 DSCP 标记。
   - 应用程序系列：选择一个应用程序系列，然后指定网络 IP 地址、端口号和 DSCP 标记。
7. 单击 **+** 添加更多应用程序匹配条件。
8. 单击添加。

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。



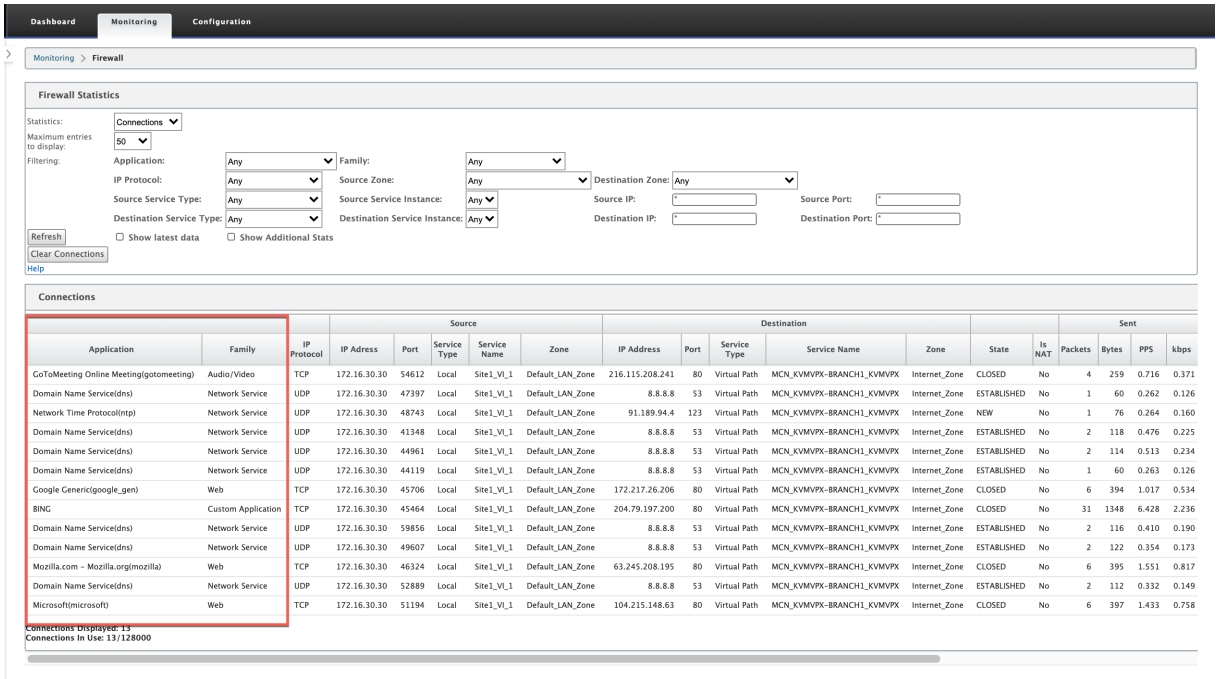
查看应用程序分类

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：

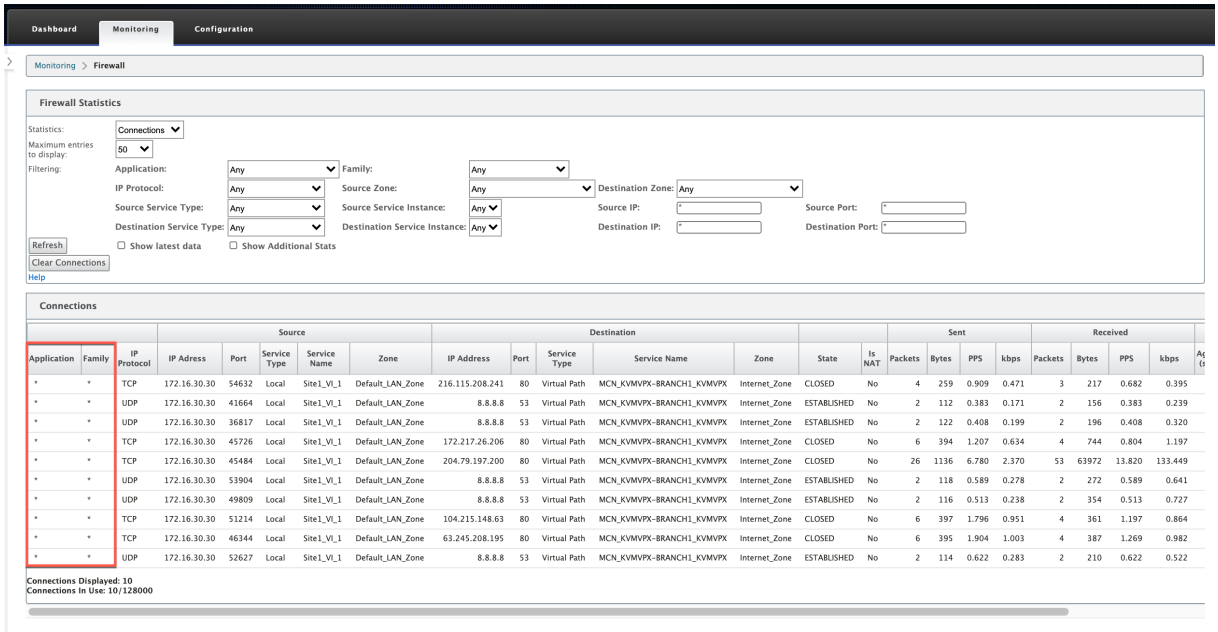
- 防火墙连接统计
- 流信息
- 应用程序统计

防火墙连接统计

在 配置编辑器中，导航到 监视 > 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。

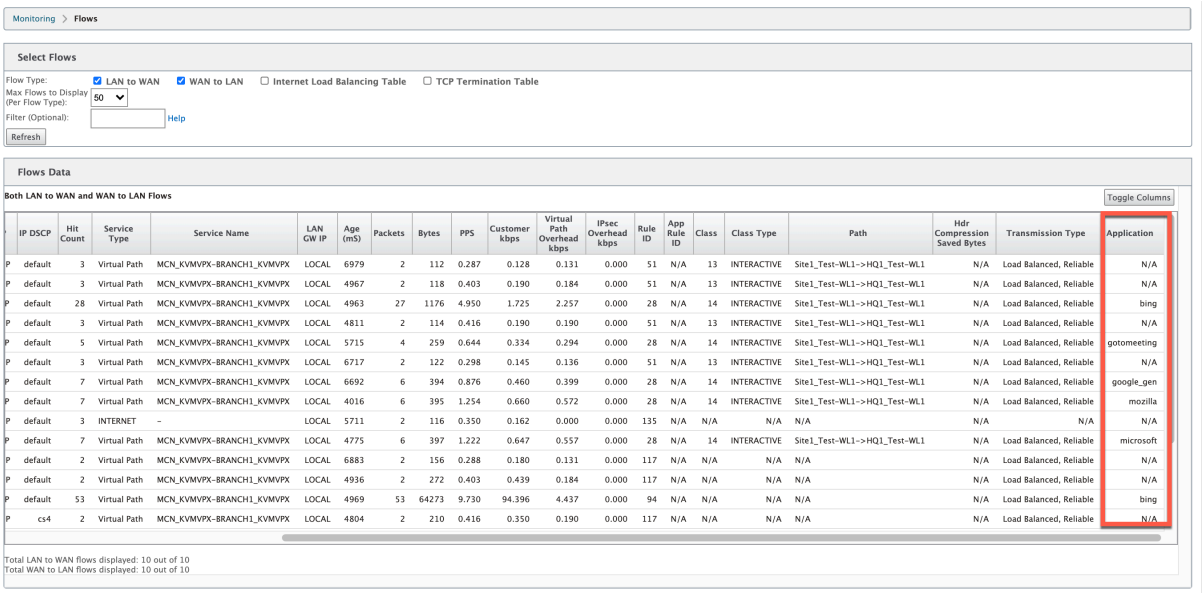


如果未启用应用程序分类，则应用程序和系列列不显示任何数据。



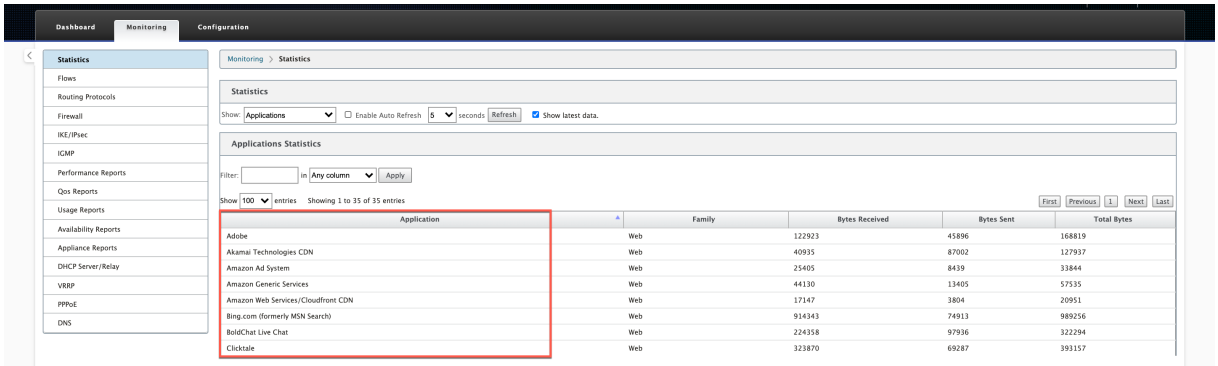
流信息

在 配置编辑器中，导航到 监控 > 流程。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

在 配置编辑器中，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)

June 22, 2021

QoS 公平性功能通过使用 QoS 类和随机早期检测 (RED) 来提高多个虚拟路径流的公平性。虚拟路径可以分配给 16 个不同类之一。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部放置行为，以避免持有大量流量。TCP 连接的性质是少量流量来填充虚拟路径，这使得新的 TCP 连接难以实现公平的带宽份额。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

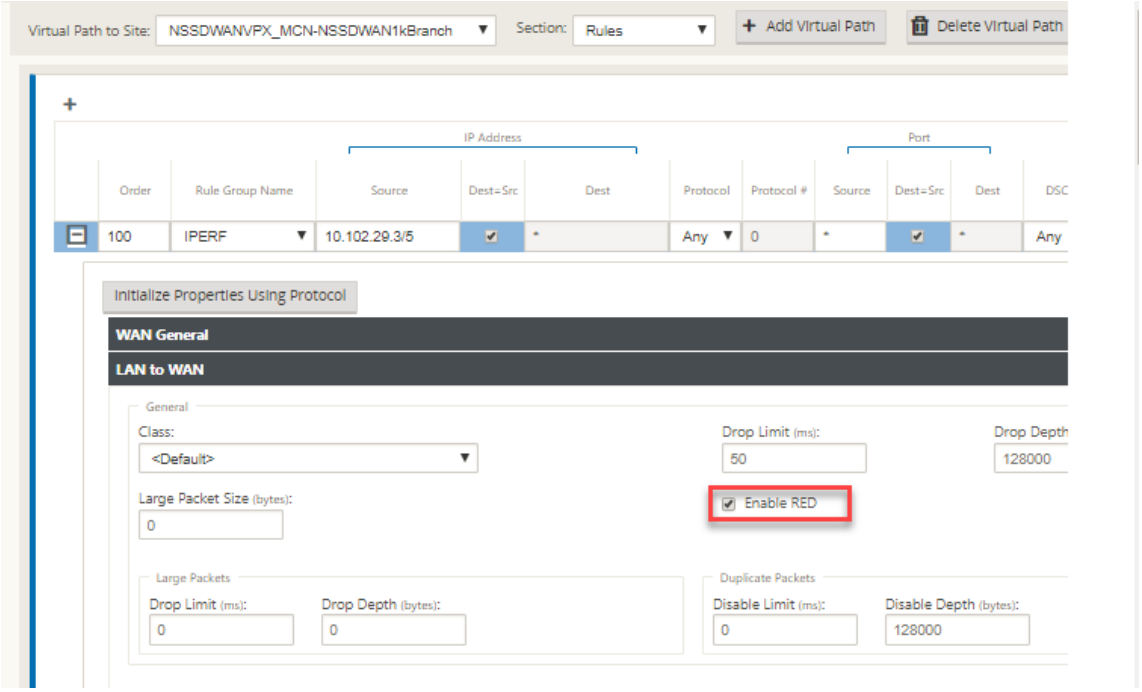
随机早期检测 (RED) 可防止流量队列填满并导致尾部掉落操作。它可以防止虚拟路径调度程序不必要地排队，而不会影响 TCP 连接可以实现的吞吐量。

如何使用红色

1. 启动 TCP 会话以创建虚拟路径。验证启用 RED 时，该类的等待时间在稳定状态下保持在 50 ms 左右。
2. 启动第二个 TCP 会话并验证这两个 TCP 会话是否均匀共享虚拟路径带宽。验证班级上的等待时间保持稳定状态。
3. 验证配置编辑器是否可用于启用和禁用 RED，并且它显示了参数的正确值。
4. 验证 SD-WAN GUI 页面中的 视图配置 显示是否为规则启用了 RED。

如何启用 **RED**

1. 导航到 配置编辑器 > 连接 > 虚拟路径 >[选择虚拟路径]> 规则 > 选择规则，例如; **(VOIP)**。
2. 展开 **LAN** 到 **WAN** 窗格。在 **LAN** 到 **WAN** 部分下，单击 启用 **RED** 复选框，以便为基于 TCP 的规则启用它。



MPLS 队列

June 22, 2021

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。

允许 MPLS 提供程序基于 DSCP 标记识别流量，以便提供程序可以应用该服务类别。

> 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。

配置私有 **MPLS WAN** 链接

1. 将 WAN 链接访问类型定义为私有 MPLS。
2. 定义与服务提供商 MPLS 队列对应的 MPLS 队列。
3. 为虚拟路径服务启用 WAN 链接（默认情况下为私有 MPLS WAN 链接启用）。
4. 从 WAN 链接上的虚拟路径中，分配一个自动分配组。

   > 注意
   >
   > 如果从 WAN 链接级别分配了自动分配组，SD-WAN 会根据匹配的 DSCP 标签在 MCN 和客户端 MPLS 队列之间自动创建路径。如果自动路径组是从 MPLS 队列级别分配的，则无论 DSCP 标记是否匹配，SD-WAN 都会自动创建路径。

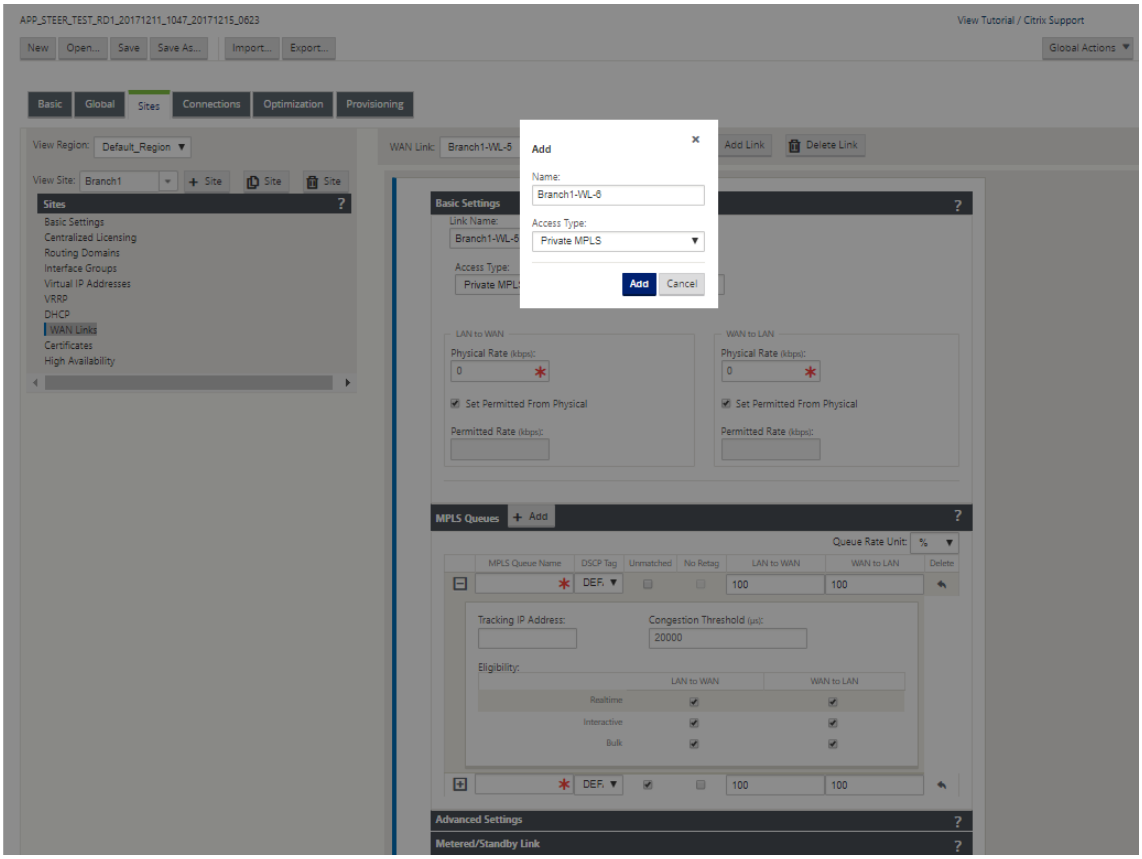
5. 确保在 MCN 和客户端配置了相同的自动传输组。
6. 验证 WAN 链接的路径是否自动构建。
7. 如果需要，将 Intranet 服务分配给特定队列。

> 注意
>
> SD-WAN 配置可能没有针对基于提供程序的队列的一对一映射。这基于特定的部署方案。不能在不同的私有访问类型之间创建自动分析组。例如，您不能在专用 Internet 访问类型和私有 MPLS 访问类型之间创建自动传输组。

如何添加私人 **MPLS WAN** 链接

要为专用 MPLS 配置新的 WAN 链路访问类型，请执行以下操作：

1. 在配置编辑器中，导航到 站点 > **[**站点名称**]** > **WAN** 链接。单击 添加链接。输入 WAN 链接名称，然后选择 私有 **MPLS** 作为访问类型。



2. 在 基本设置 下，现在有一个新的 **MPLS** 队列选项卡。单击 + 添加以添加特定 MPLS 队列。这些应与服务提供程序定义的队列相对应。

字段	说明
MPLS 队列名称	MPLS 队列名称
DSCP 标签	服务提供商的队列 DSCP 标签设置。
无与伦比的	启用后，到达的任何与配置文件中定义的标签不匹配的帧都将映射到此队列以及为此队列定义的带宽。
局域网至广域网允许速率 (kbps)	允许 SD-WAN 设备用于上载的带宽量，不能超过 WAN 链接的定义物理上载速率。
广域网到广域网允许费率 (kbps)	SD-WAN 设备允许用于下载的带宽量，不能超过 WAN 链接的定义物理下载速率。

展开 MPLS 队列定义（通过单击 +），将显示更多选项。这些选项包括：

字段	说明
跟踪 IP 地址	WAN 链接跟踪地址

字段	说明
拥塞阈值	定义的拥塞时间量（以微秒为单位），之后 MPLS 队列会限制数据包传输以避免更多拥塞。当拥塞超过设定的阈值时，SD-WAN 会退出发送速率。
资格	MPLS 队列处理特定类流量的资格。如果禁用特定类流量的资格，则该类流量不太可能通过 MPLS 队列进行路由，除非网络条件需要。

配置与现有服务提供商 WAN 链接队列定义对应的 MPLS 队列。

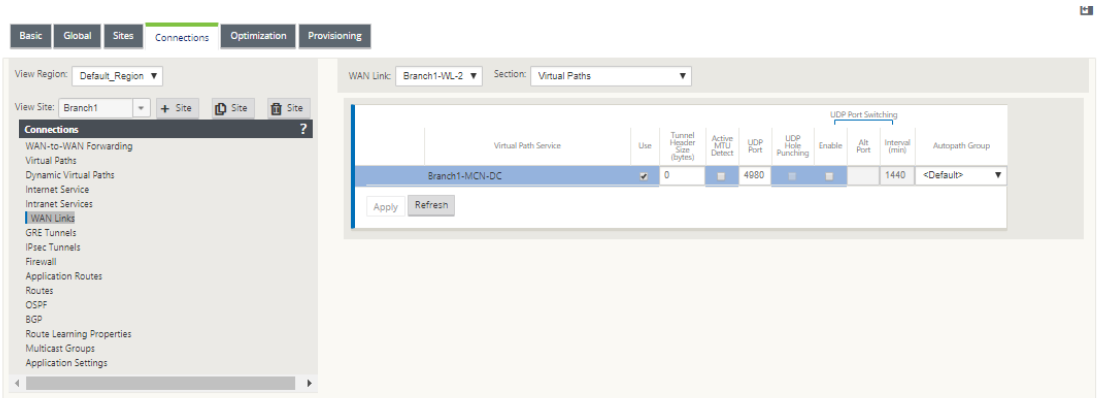
> 注意
>
> 在 SD-WAN 9.1 之前配置的任何现有 MPLS WAN 链接都不会受到影响。

定义私有 **MPLS** 的 **WAN** 链接属性

定义了私有 MPLS WAN 链接及其 MPLS 队列后，您应该在特定的虚拟路径定义下为 WAN 链接分配一个自动分配组。

要分配自动解析组：

1. 转到连接 > **[**站点名称**] >WAN** 链接 > [**MPLS WAN** 链接名称] > 虚拟路径 > [虚拟路径名称] > [本地网站] > **WAN** 链接，然后单击编辑 ()。
2. 单击 自动分配组 下拉菜单，然后从可用的组中进行选择。默认情况下，MPLS 队列继承分配给 MPLS WAN 链接的自动分配组。您可以选择将各个 MPLS 队列设置为继承选定的自动路径组，也可以从“自动路径组”下拉菜单中为每个 MPLS 队列选择一个替代队列。



> 注意

> 如果在本地站点和远程站点的队列之间没有基于 DSCP 标记的一对一映射，则必须将 MPLS 队列映射到特定的自动路径组。从 MPLS WAN 链接继承自动解决组会 自动生成具有匹配 DSCP 标记的队列之间的路径。

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

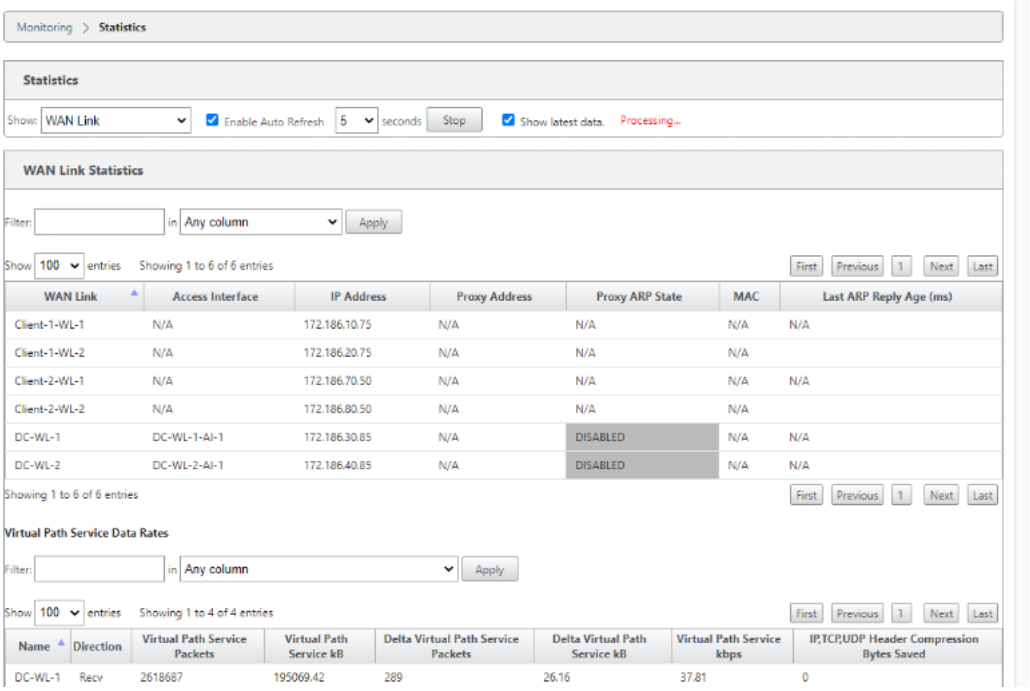
SD-WAN Web 界面现在允许您查看 WAN 链路和 WAN 链路使用的允许速率，以及 WAN 链路、路径或虚拟路径是否处于拥塞状态。在以前的版本中，此信息仅在 SD-WAN 日志文件中以及通过 CLI 提供。这些选项现在可在 Web 界面中使用，以帮助进行故障排除。

查看允许的费率

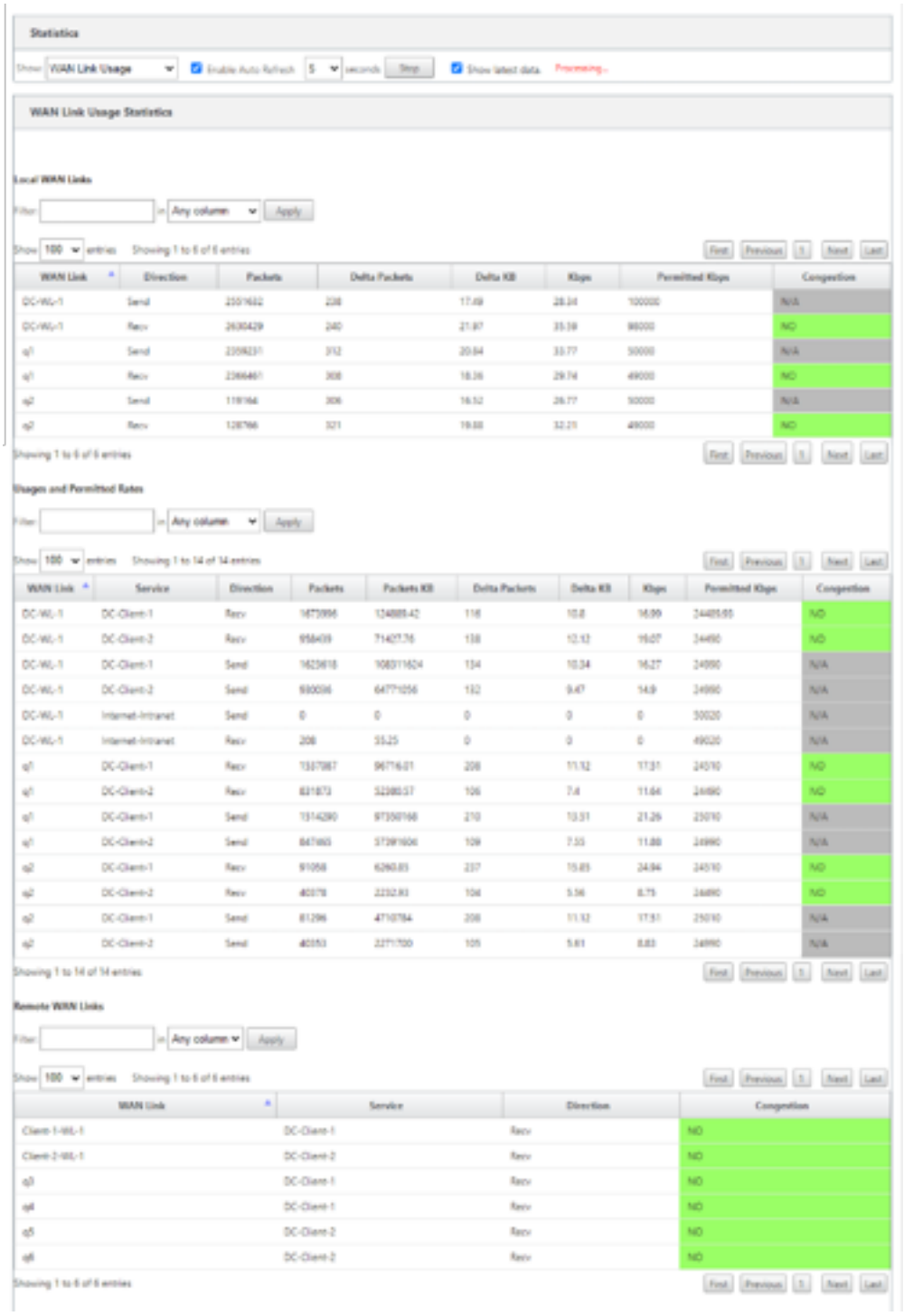
允许速率是指特定 WAN 链接、虚拟路径服务、Intranet 服务或 Internet 服务在给定时间点允许使用的带宽量。WAN 链接的允许速率是静态的，并且在 SD-WAN 配置中明确定义。虚拟路径服务、Intranet 服务或 Internet 服务的允许费率将随着时间的推移而波动，以响应拥堵、用户需求和公平分享，但始终大于或等于该服务的最低预留带宽。

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。

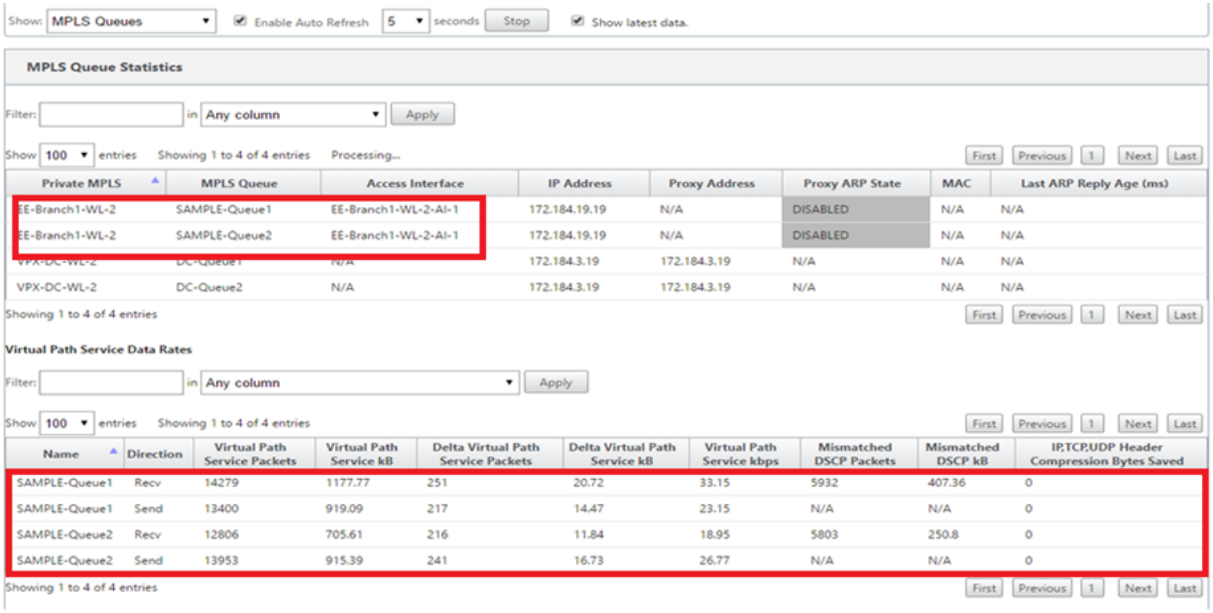


转到 监控 **>** 统计信息，然后从 显示 下拉列表中选择 **WAN** 链接使用情况。



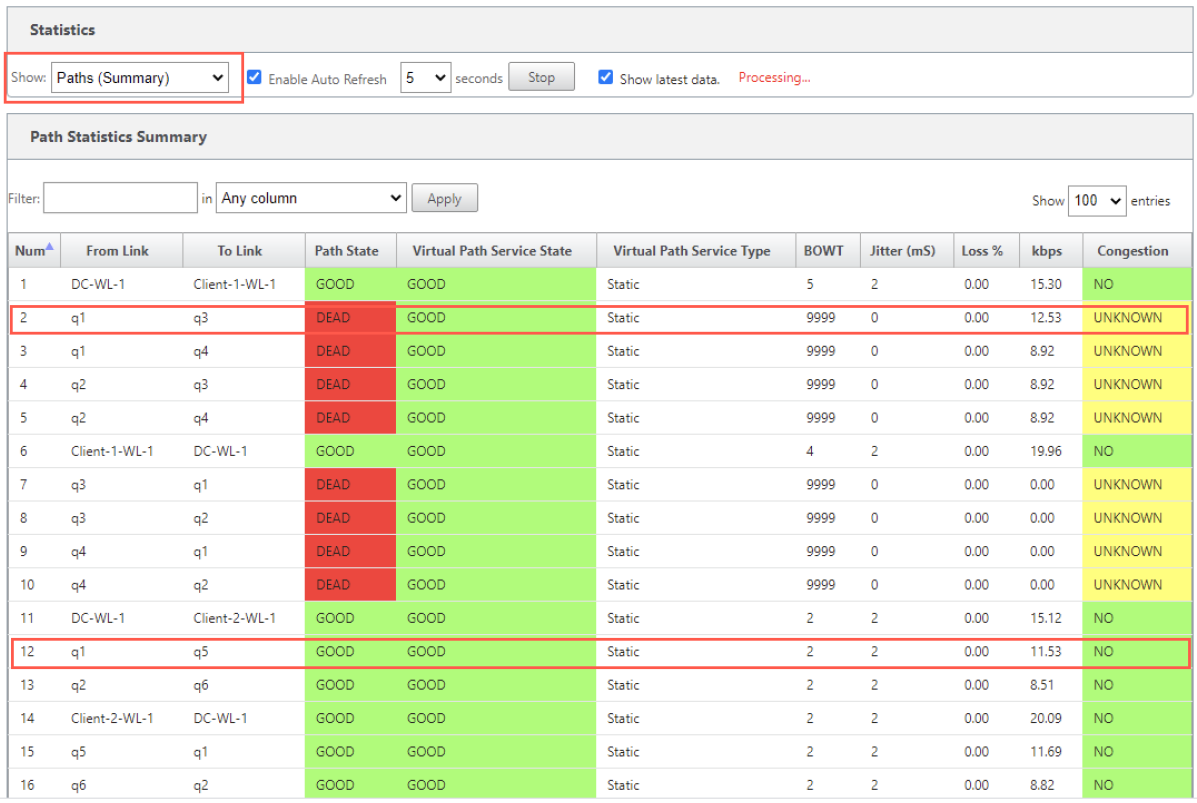
监视 **MPLS** 队列

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

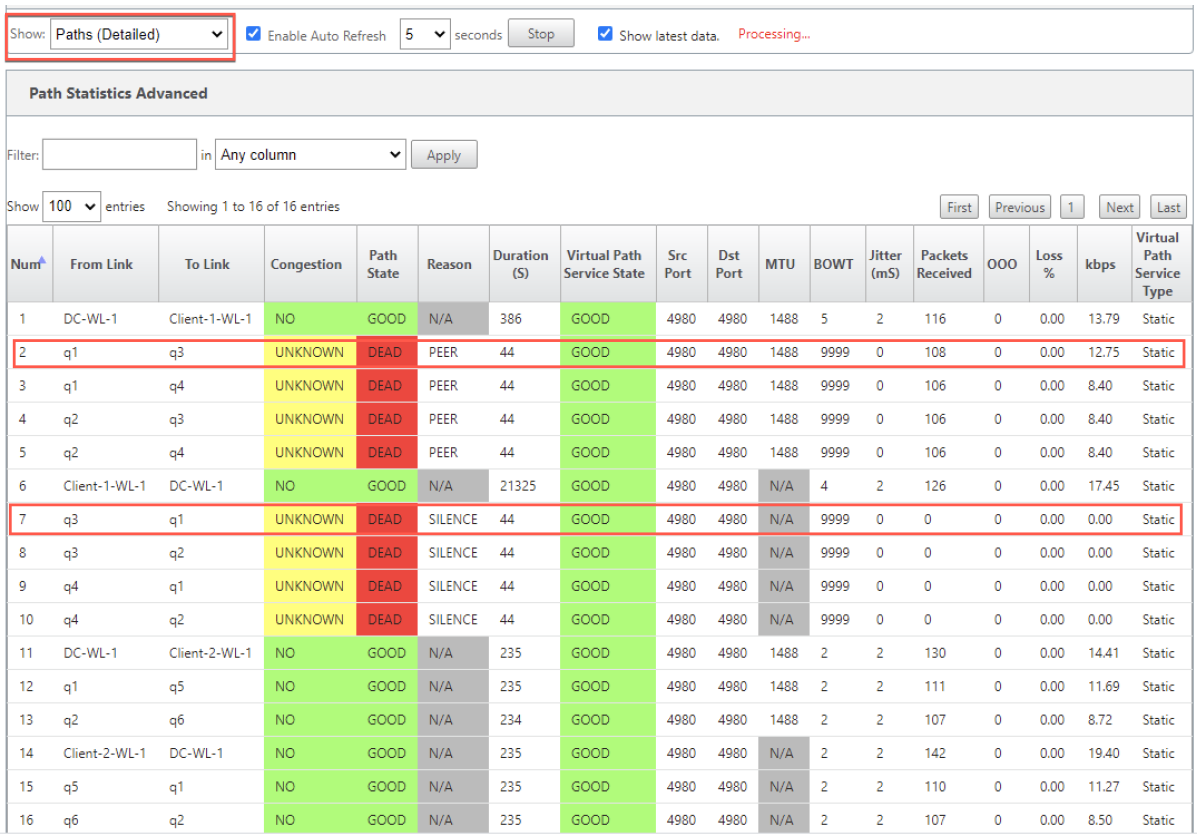
要检查 MPLS 队列的状态，请导航到 监控 **>** 统计信息，然后从 显示 下拉列表中选择 路径（摘要）。在以下示例中，从 MPLS 队列“q1”到“q3”的路径处于“死亡”状态，并以红色显示。从 MPLS 队列“q1”到“q5”的路径处于“良好”状态并显示为绿色。



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

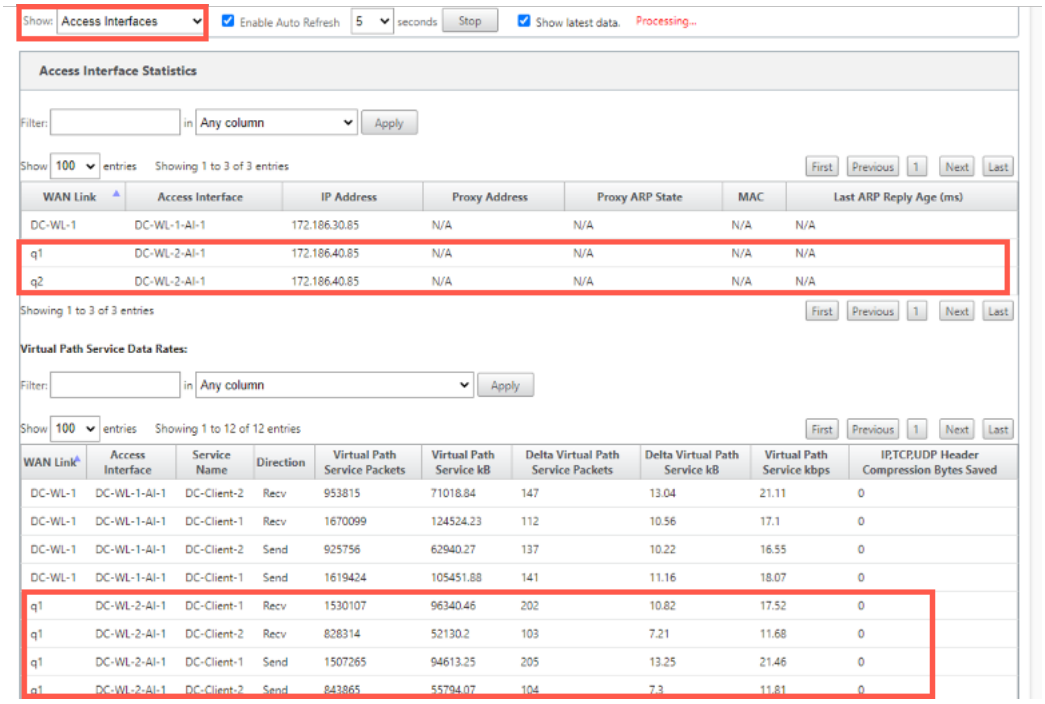
在下面的示例中，从 MPLS 队列“q1”到“q3”的路径处于死亡状态，原因是 PEER。从 MPLS 队列“q3”到“q1”的路径已死，原因是沉默。下表提供了列表（如果可用的原因）及其说明。

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

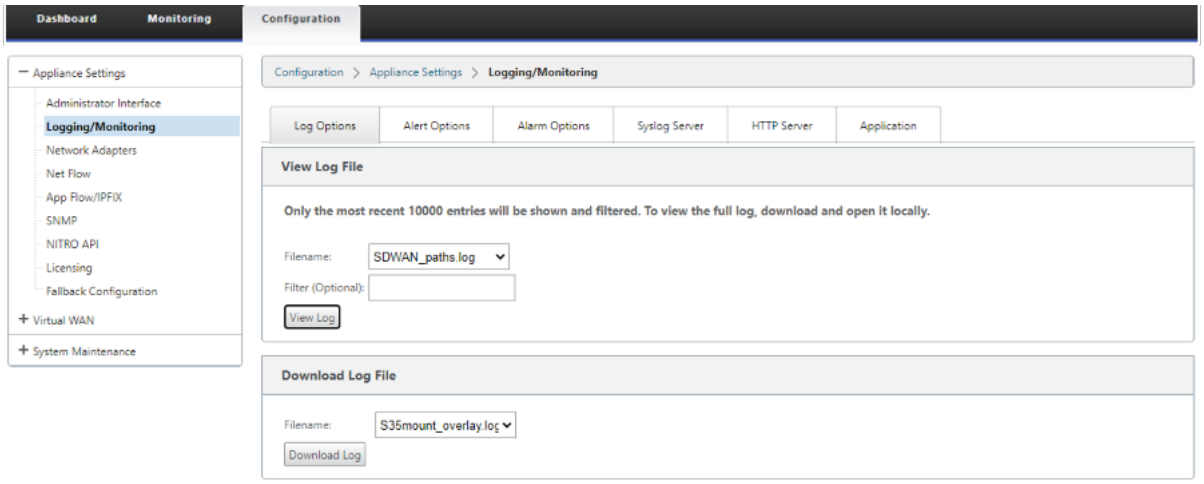


Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Src Port	Dst Port	MTU	BOWT	Jitter (mS)	Packets Received	OOO	Loss %	kbps	Virtual Path Service Type
1	DC-WL-1	Client-1-WL-1	NO	GOOD	N/A	386	GOOD	4980	4980	1488	5	2	116	0	0.00	13.79	Static
2	q1	q3	UNKNOWN	DEAD	PEER	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

June 22, 2021

应用程序 QoE

多个净流集热器

应用程序 **QoE**

June 22, 2021

应用程序 **QoE** 是 SD-WAN 网络中应用程序体验质量的衡量标准。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。有关详细信息，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。

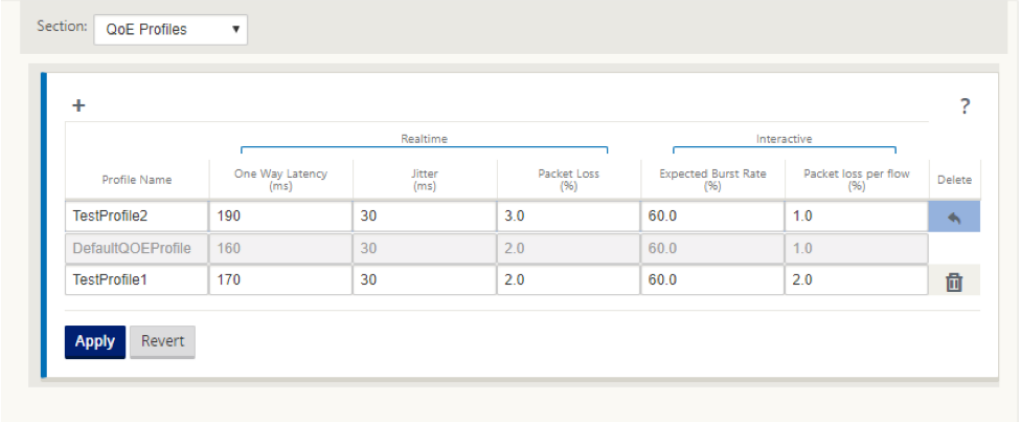
配置应用程序 **QoE**

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。

要创建自定义 QoE 配置文件：

1. 在配置编辑器中，导航到 全局 **>** 应用程序 **QoE > QoE** 配置文 件，然后单击 **+**。
2. 输入以下参数的值：
    - 配置文件名称：用于标识设置实时和交互式流量阈值的配置文件的名称。
    - 实时：为触及实时 QoS 策略的流量配置阈值。满足低于延迟、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。
        - 单向延迟：以毫秒为单位的延迟阈值。默认的 QoE 配置文件值为 160 毫秒。
        - 抖动：抖动阈值（以毫秒为单位）。默认的 QoE 配置文件值为 30 毫秒。
        - 数据包丢失：数据包丢失的百分比。默认的 QoE 配置文件值为 2%。
    - 交互式：为触及交互式 QoS 策略的流量配置阈值。交互式应用程序如果满足突发比率和数据包丢失阈值低于阈值，则被认为具有良好的质量。
        - 预期突发率：预期突发率的百分比。出口突发率至少应为入口突发率的配置百分比。默认的 QoE 配置文件值为 60%。

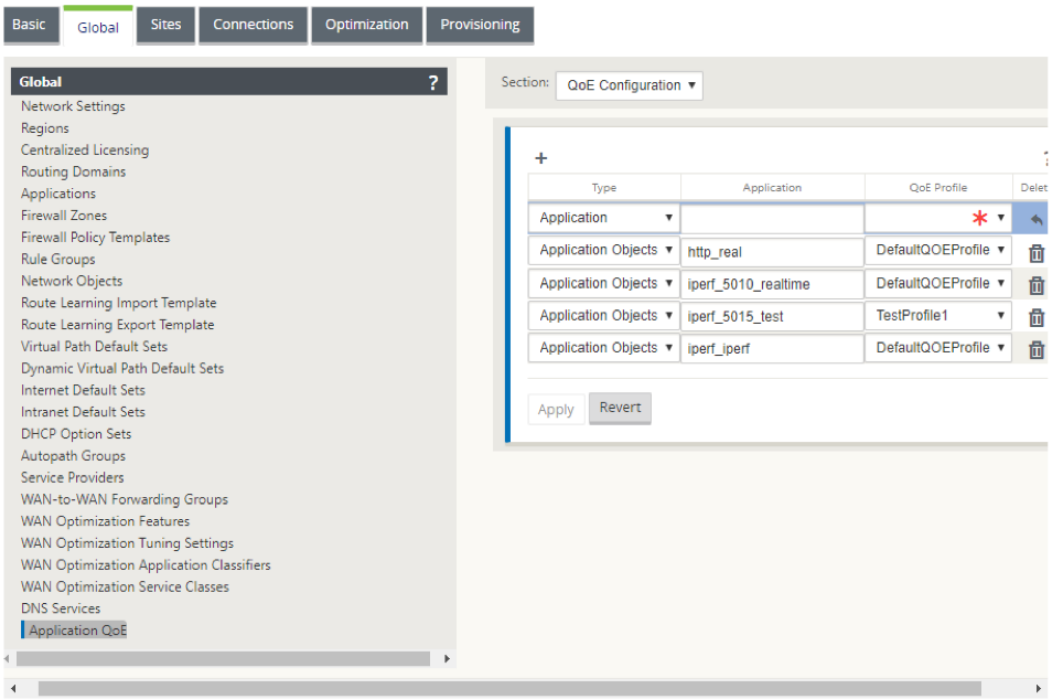
– 每个流量的数据包丢失：数据包丢失的百分比。默认的 QoE 配置文件值为 1%。



3. 单击应用。

要使用 QoE 配置文件映射应用程序或应用程序对象，请执行以下操作：

1. 在配置编辑器中，导航到 全局 **>** 应用程序 **QoE > QoE** 配置，然后单击 **+**。
2. 为以下参数选择值：
   - 类型：DPI 应用程序或应用程序对象。
   - 应用程序：根据所选类型搜索并选择应用程序或应用程序对象。
   - **QoE** 配置文件：选择要映射到应用程序或应用程序对象的 QoE 配置文件。



3. 单击应用。

您最多可以使用 QoE 配置文件映射 10 个应用程序或应用程序对象。您可以在 SD-WAN Center 查看应用程序 QoE 报告。欲了解更多信息，请参阅应用程序质量评价报告报告。

HDX QoE

June 22, 2021

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。

有关详细信息，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。

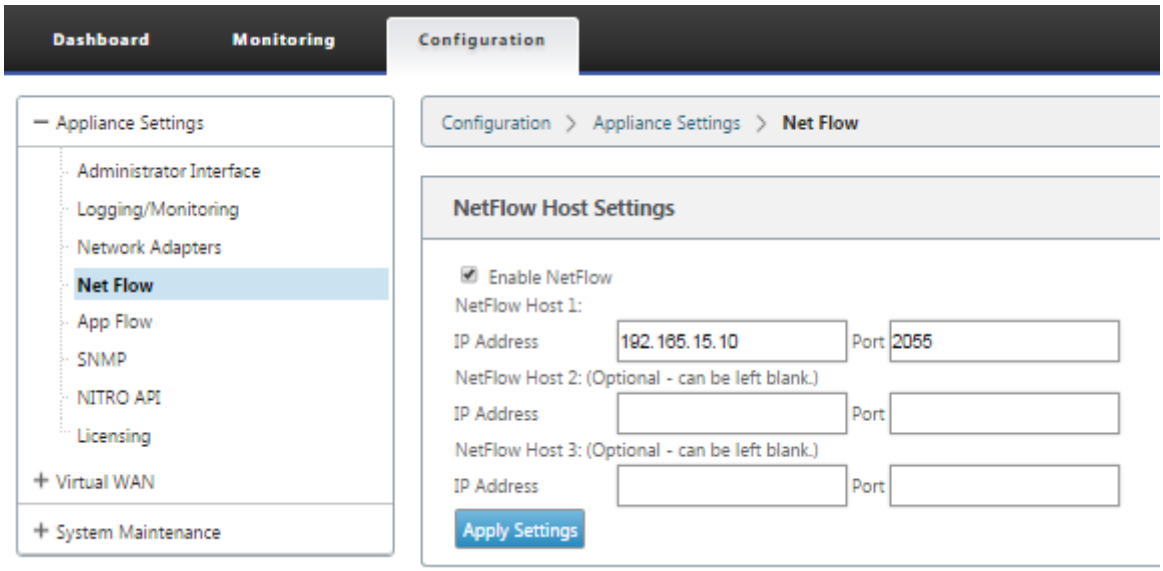
多个净流集热器

February 10, 2022

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 标准版和 高级（企业）版设备支持 Net Flow 。

要配置网络流主机，请执行以下操作：

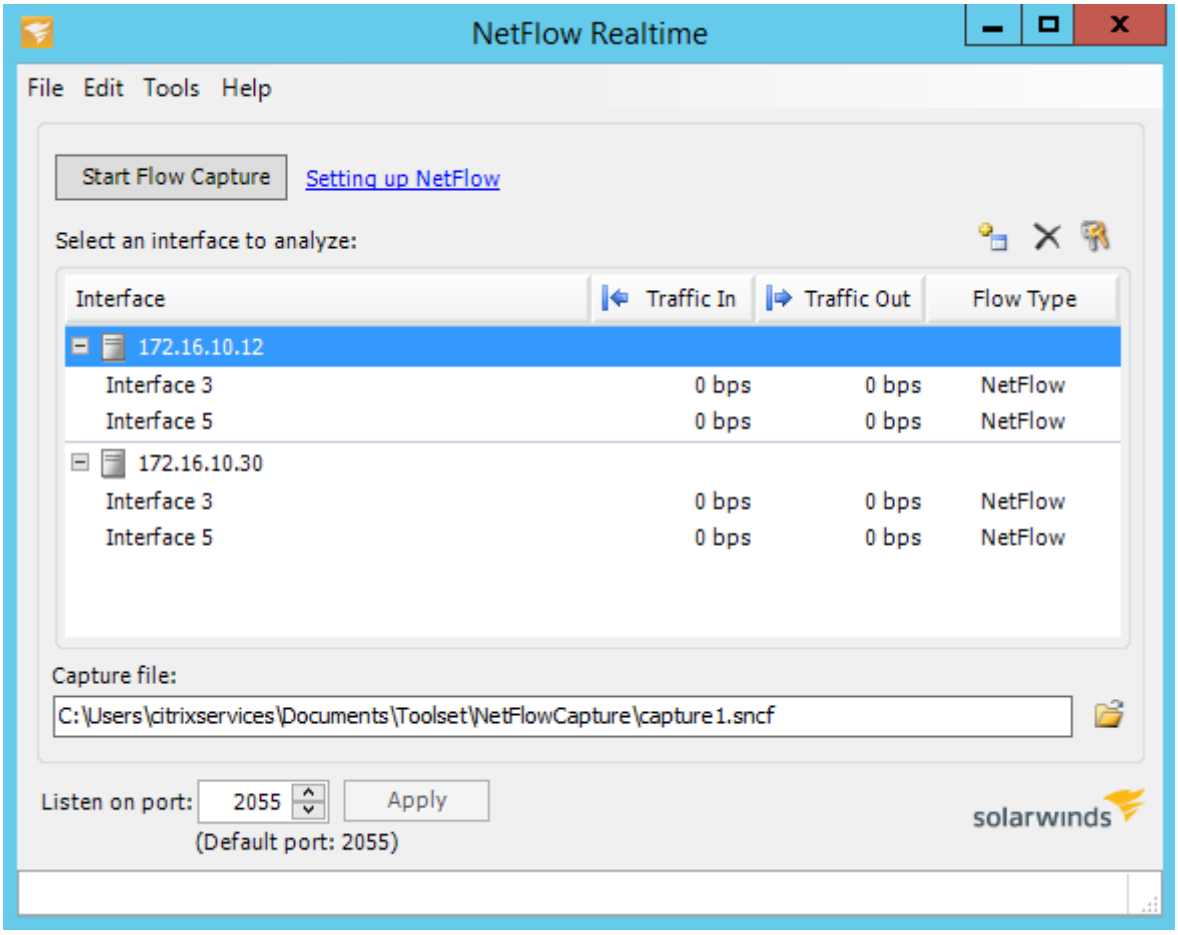
导航到 配置 **>** 装置设置 **>** 网络流量 **> Netflow** 主机设置 页面。单击“启用 **NetFlow** ”复选框，输入最多三台网络流主机的 **IP** 地址和 端口 号，然后单击 应用设置 保存更改。

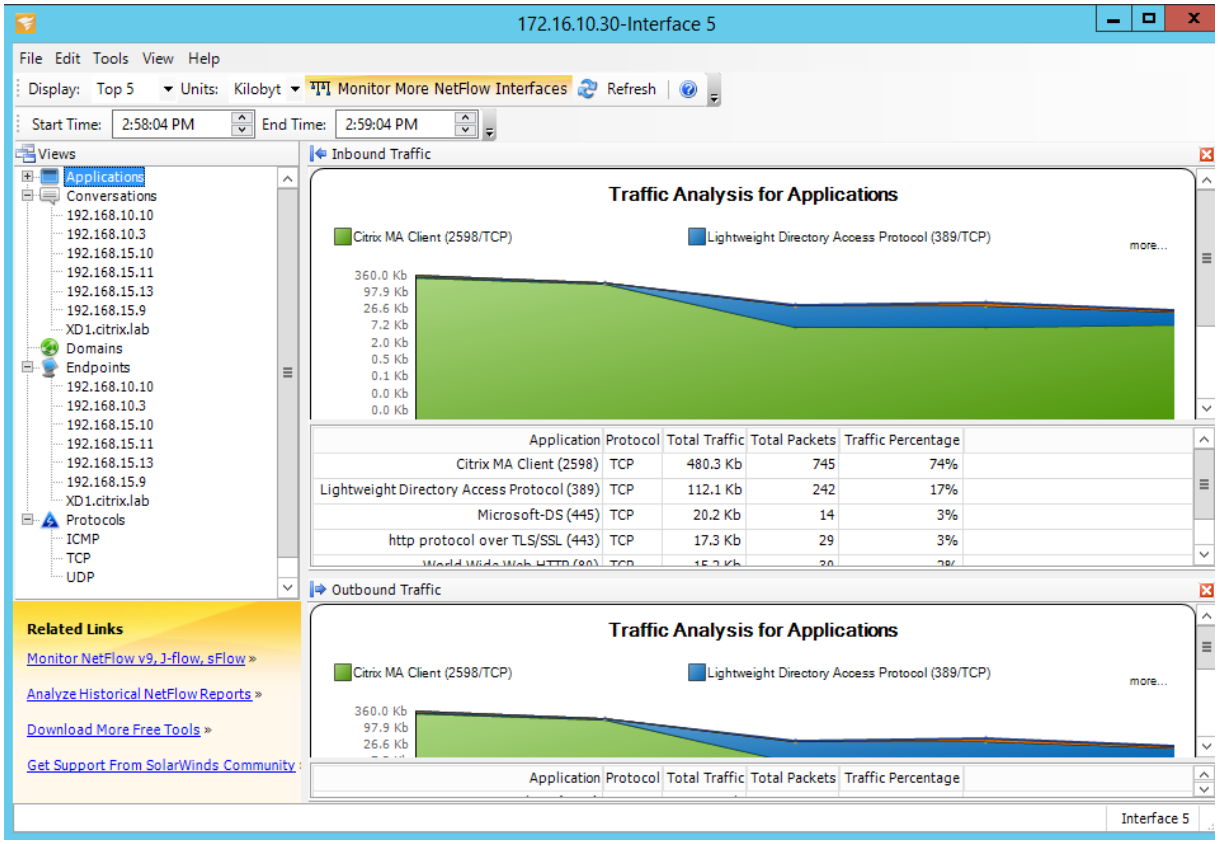


NetFlow 导出

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）。有关详细信息，请参阅

SNMP





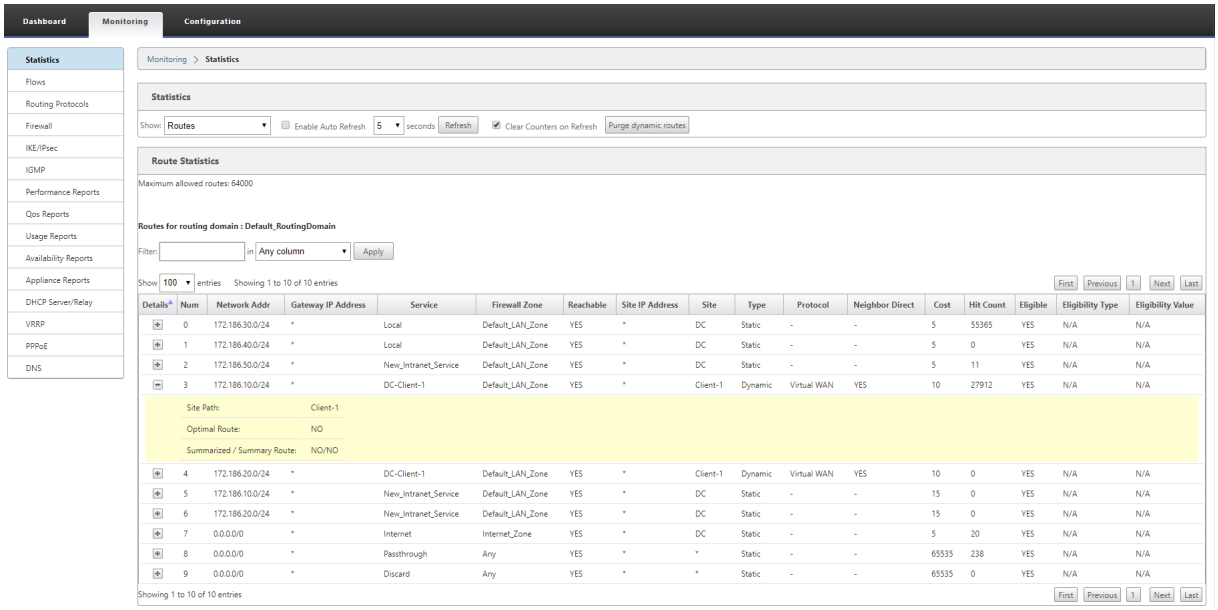
NetFlow 限制

- 如果在 SD-WAN 标准和高级版设备上启用了 Netflow，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 的网络流导出的互联网标准，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。

路线统计

June 22, 2021

要查看 SD-WAN 设备的路线统计信息，请在 SD-WAN GUI 中导航到 监视 > 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 + 以显示以下信息。
  - 站点路径：站点路径是接收前缀的真值指标源。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，路由是否是到达该子网的最佳路由。此最佳路径将导出到其他站点。
  - 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。汇总路线有 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：路径使用的防火墙区域。

- 可达：路线是否可到达。
- 站点 **IP** 地址：站点的 IP 地址。
- 站点：站点的名称。
- 类型：路径类型取决于路径学习的来源。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。
  - 虚拟广域网：从对等 SD-WAN 设备学到的前缀。
  - **OSPF**：从 OSPF 动态路由对等学习的前缀。
  - **BGP**：从 BGP 动态路由对等体学习的前缀。
- 邻居直接：指示子网是否连接到路由到设备的分支。
- 成本：用于确定目标网络的最佳路径的成本。
- 单击计数：单击路由将数据包转发到该子网的次数。
- 合格：表示路由符合条件，并用于在流量处理过程中将数据包转发或路由到前缀单击。
- 资格类型：以下两种资格类型可用。
  - **Gateway** 资格：确定网关是否可访问。
  - 路径资格：确定路径是已死还是未死。
- 资格值：在系统中创建路由时为 Gateway 或配置中的路径选择的值。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

June 22, 2021

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。

路线汇总

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

June 22, 2021

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 设备之间建立隧道来实现这一目标，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 配置允许特定站点的静态路由条目，并允许通过支持的路由协议（如 OSPF、eBGP 和 iBGP）从底层网络学习路由条目。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** —这与 Intranet 类似，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。

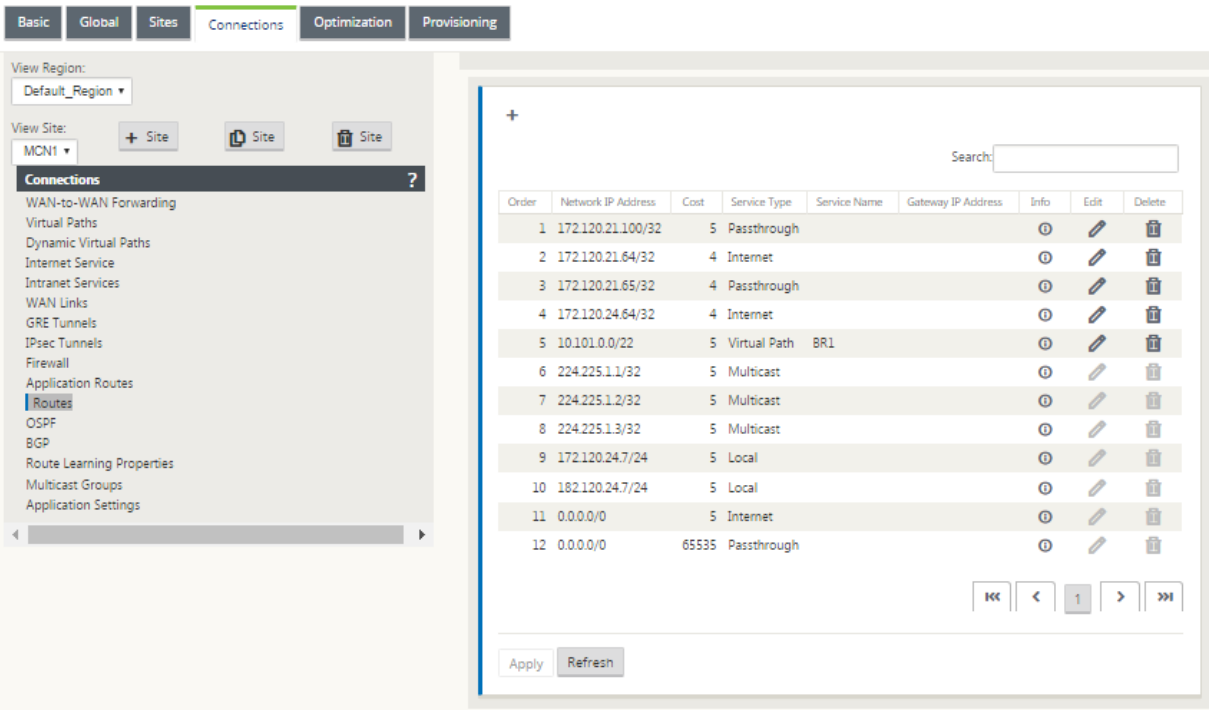
> 注意
>
> Internet 服务路由可以播发到其他 SD-WAN 设备或阻止导出，具体取决于您是否通过虚拟路径进行互联网访问。

- 直通—当设备处于内联模式时，此服务充当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）。

  SD-WAN 配置编辑器为每个可用站点启用路由表自定义：

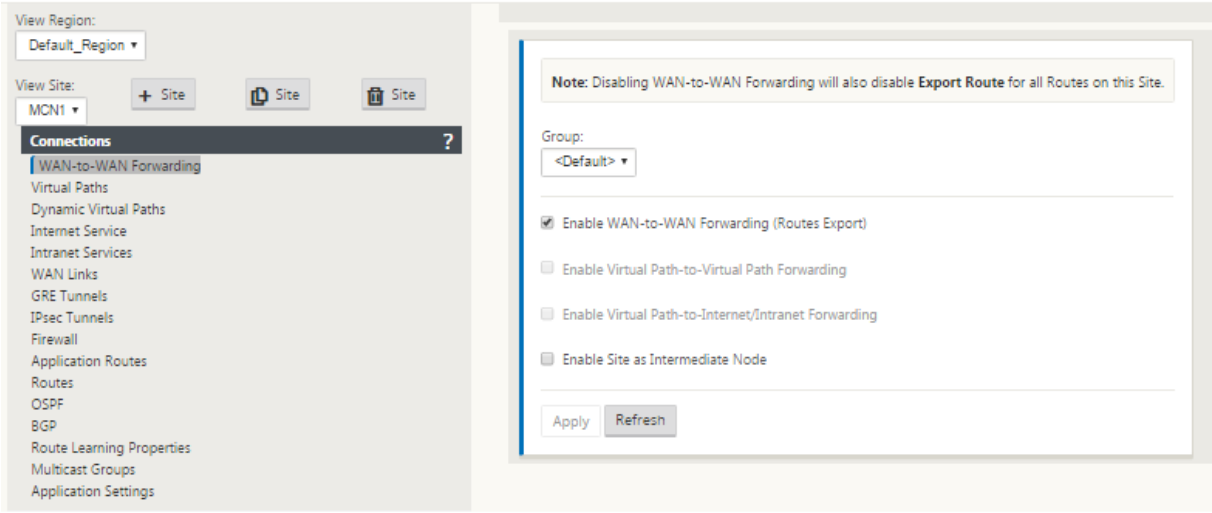


路由表条目从不同的输入填充：

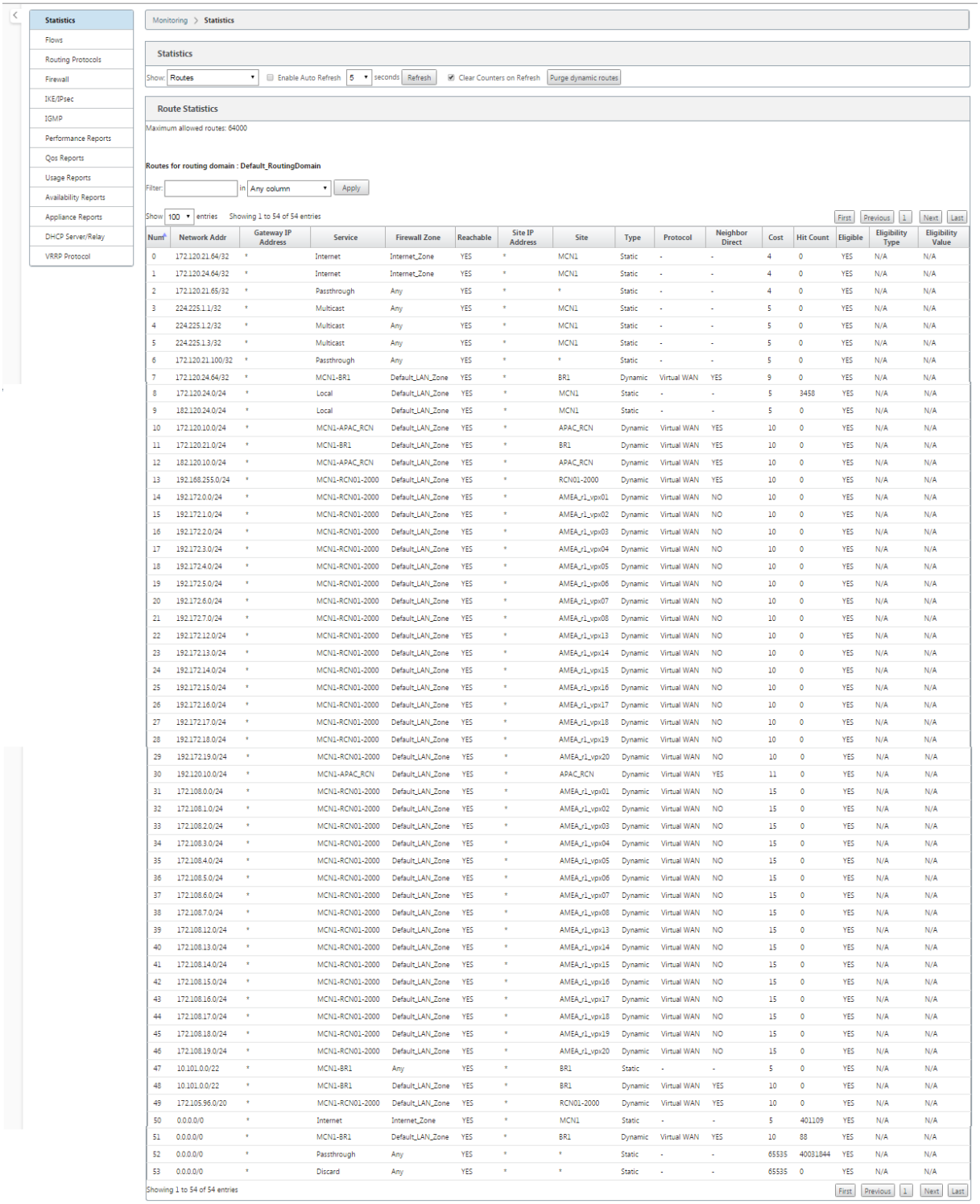
- 配置的虚拟 IP 地址 (VIP) 自动填充为服务类型本地路由。配置编辑器阻止将相同的 VIP 分配给不同的站点节点。
- 在本地站点启用的 Internet 服务在本地自动填充默认路由 (0.0.0.0/0) 以便实现直接 Internet 突破。
- 管理员在每个站点的基础上定义静态路由，这也将被定义为服务类型本地路由。
- 默认值 (0.0.0.0/0) 捕获定义为直通的成本为 16 的所有路由

管理员可以配置上述路由之一，但除了路由开销外，还可以根据服务类型配置服务类型、下一跳或 Gateway。默认路由开销将自动添加到每个路由类型中（有关默认路由开销，请参阅下表）。此外，只有受信任的路由才会通告到其他 SD-WAN 设备。不受信任的路由仅由本地设备使用。

默认情况下，客户端节点路由仅播发到 MCN 节点，而不会播发其他客户端节点。要使客户端节点路由对另一个客户端节点可见，必须在 MCN 节点启用 WAN 到 WAN 转发。



在 全局 设置下启用 WAN 到 WAN 转发（路由导出模板）后，MCN 站点将播发的路由共享给参与 SD-WAN 叠加的所有客户端。启用此功能可在不同客户端节点站点上的主机之间实现 IP 连接，并且通过 MCN 进行通信。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。



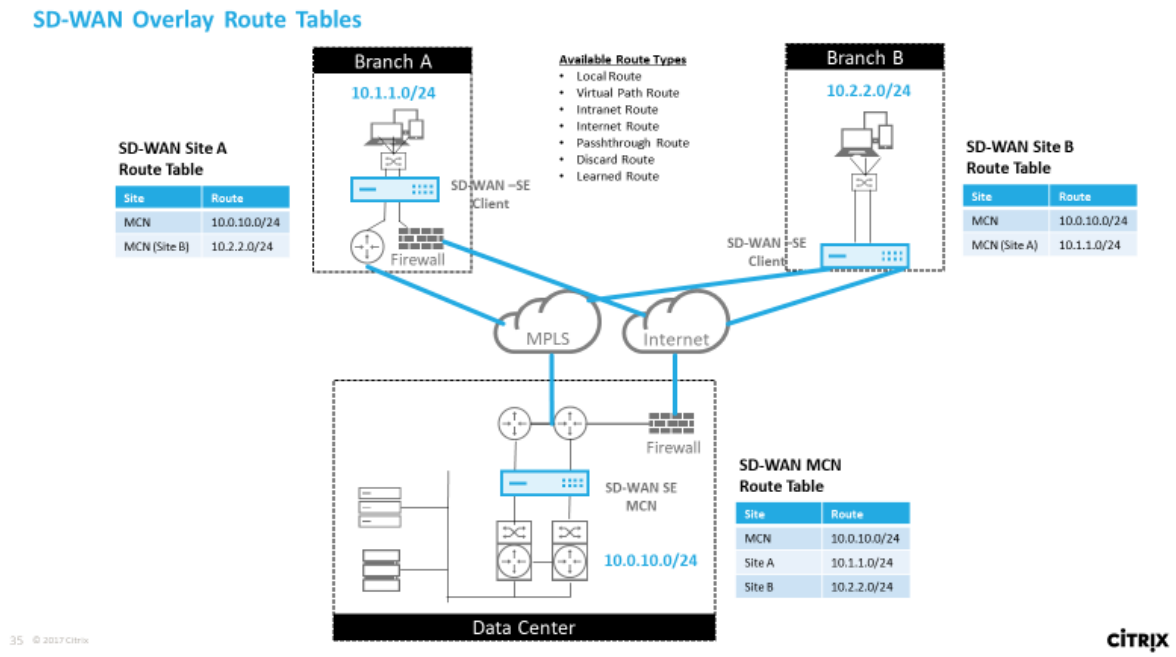
Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
0	172.120.21.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
1	172.120.24.64/32	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	4	0	YES	N/A	N/A
2	172.120.21.65/32	*	Passthrough	Any	YES	*	*	Static	-	-	4	0	YES	N/A	N/A
3	224.225.1.1/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
4	224.225.1.2/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
5	224.225.1.3/32	*	Multicast	Any	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
6	172.120.21.100/32	*	Passthrough	Any	YES	*	*	Static	-	-	5	0	YES	N/A	N/A
7	172.120.24.64/32	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	9	0	YES	N/A	N/A
8	172.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	3458	YES	N/A	N/A
9	182.120.24.0/24	*	Local	Default_LAN_Zone	YES	*	MCN1	Static	-	-	5	0	YES	N/A	N/A
10	172.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
11	172.120.21.0/24	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
12	182.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
13	192.168.255.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
14	192.172.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
15	192.172.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
16	192.172.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
17	192.172.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
18	192.172.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
19	192.172.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
20	192.172.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
21	192.172.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
22	192.172.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
23	192.172.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
24	192.172.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
25	192.172.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
26	192.172.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
27	192.172.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
28	192.172.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
29	192.172.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	10	0	YES	N/A	N/A
30	192.120.10.0/24	*	MCN1-APAC_RCN	Default_LAN_Zone	YES	*	APAC_RCN	Dynamic	Virtual WAN	YES	11	0	YES	N/A	N/A
31	172.108.0.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx01	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
32	172.108.1.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx02	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
33	172.108.2.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx03	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
34	172.108.3.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx04	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
35	172.108.4.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx05	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
36	172.108.5.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx06	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
37	172.108.6.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx07	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
38	172.108.7.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx08	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
39	172.108.12.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx13	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
40	172.108.13.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx14	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
41	172.108.14.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx15	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
42	172.108.15.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx16	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
43	172.108.16.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx17	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
44	172.108.17.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx18	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
45	172.108.18.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx19	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
46	172.108.19.0/24	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	AMEA_r1_vpx20	Dynamic	Virtual WAN	NO	15	0	YES	N/A	N/A
47	10.101.0.0/22	*	MCN1-BR1	Any	YES	*	BR1	Static	-	-	5	0	YES	N/A	N/A
48	10.101.0.0/22	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
49	172.105.96.0/20	*	MCN1-RCN01-2000	Default_LAN_Zone	YES	*	RCN01-2000	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
50	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	MCN1	Static	-	-	5	401109	YES	N/A	N/A
51	0.0.0.0/0	*	MCN1-BR1	Default_LAN_Zone	YES	*	BR1	Dynamic	Virtual WAN	YES	10	88	YES	N/A	N/A
52	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	40031844	YES	N/A	N/A
53	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 54 of 54 entries

First Previous 1 Next Last

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、互联网、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 从隧道接收并进行处理。
  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。在 SD-WAN 上启用了相同的路由协议，使用 SD-WAN 覆盖的子网的配置变得更加简单。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。

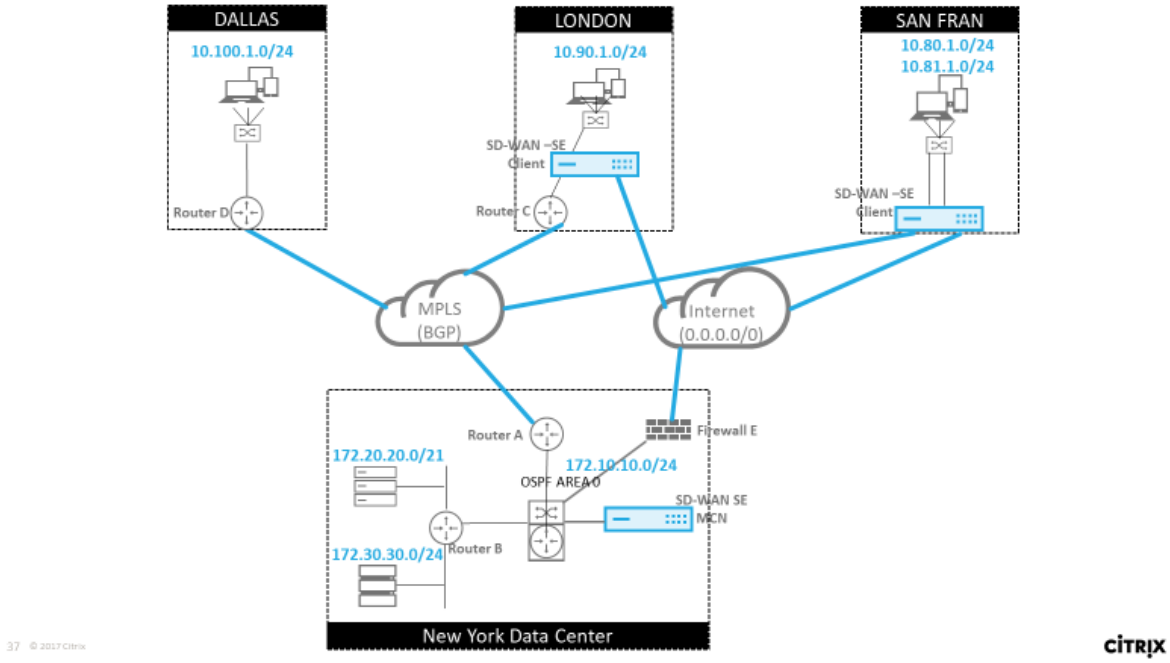
> 重要
>
> 如果你不小心，很容易泄漏不需要的路线。

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，所有互联网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互联网的路径。

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。路线成本表明它们是从 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。请注意路线成本。与 OSPF 110/10 相比，BGP 默认情况下是低于 20/1 的管理域和成本。

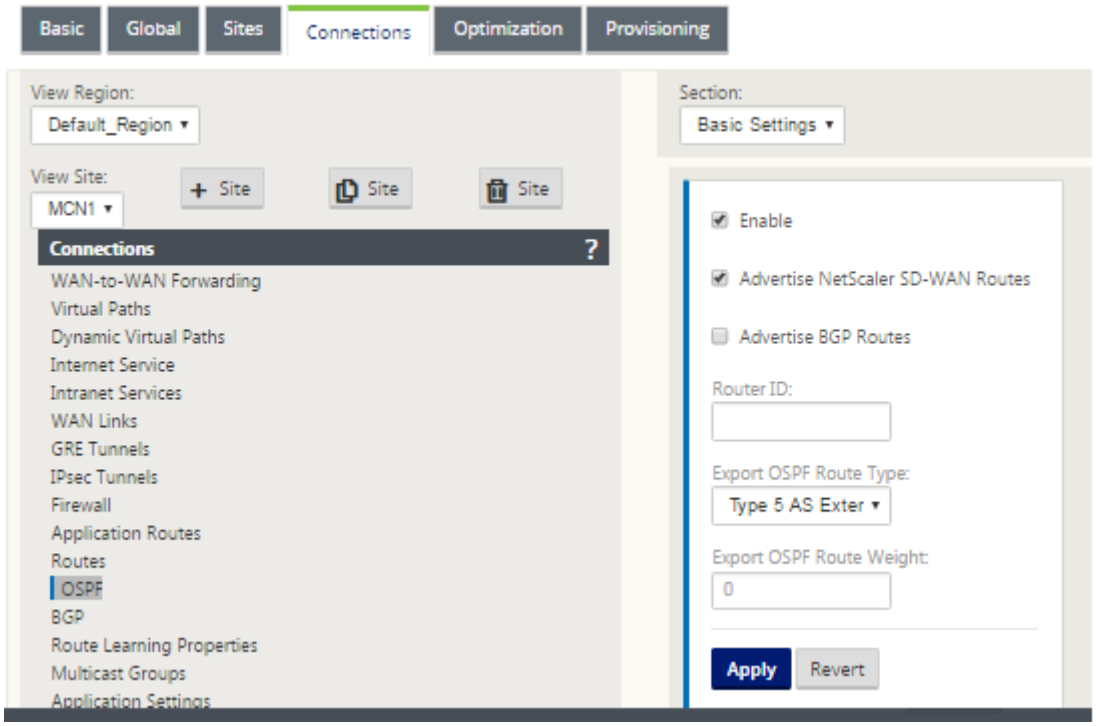
达拉斯路由器 **D**：

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
```

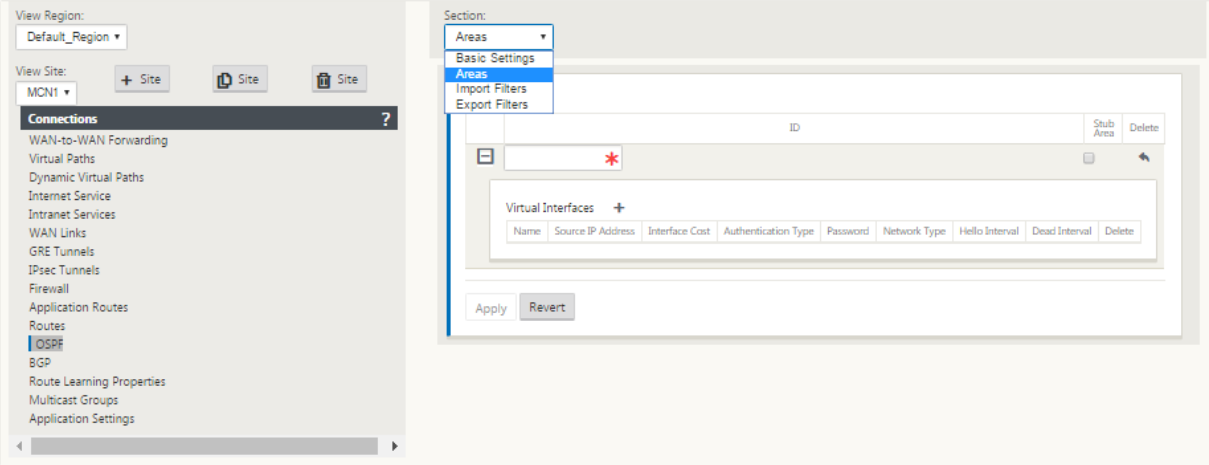
> 注意
>
> 在此示例中，您可以忽略 192.168.65.0/24 子网。这是一个管理网络，与示例无关。所有路由器都连接到管理子网，但没有在任何路由协议中通告。

在 Citrix SD-WAN 中，我们可以通过在位于纽约站点的 连接 > 查看站 点 > OSPF > 基本设置 下的 SD-WAN 上启用 **OSPF** 来添加 SD-WAN 覆盖：



> 注意
>
> 默认情况下，导出 **OSPF** 路由类型 为外部类型 5。这是因为 SD-WAN 路由表被认为是 OSPF 协议外部的，因此 OSPF 倾向于内部获取的路由（区域内），因此 SD-WAN 通告的路由可能不优先。

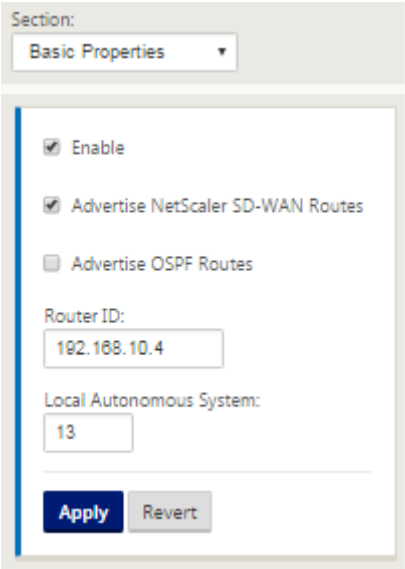
当 OSPF 在 WAN（即 MPLS 网络）中使用时，可以将其更改为类型一个区域内。OSPF 区域可以配置如下所示。

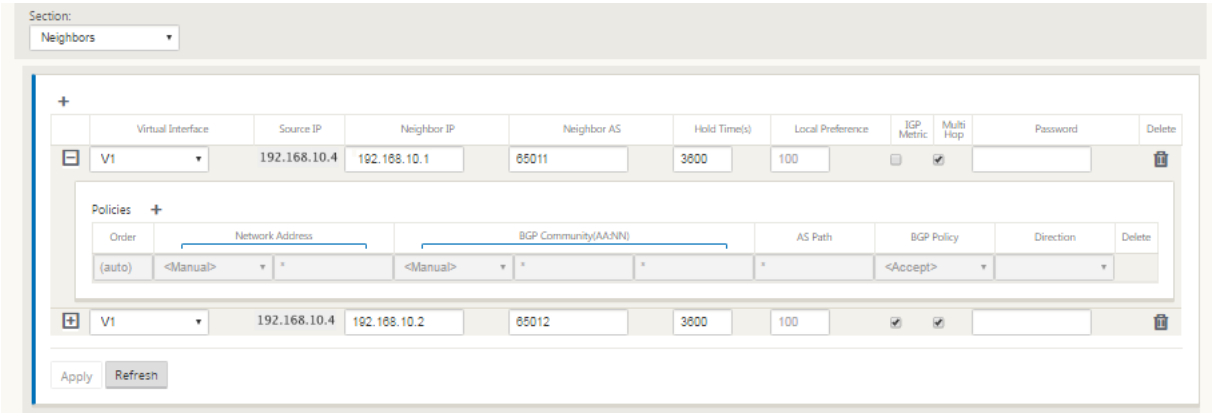


从虚拟接口 (172.10.10.0) 派生的本地网络添加了区域 0，所有其他设置都保持默认状态。

对于新旧金山站点，我们必须启用 eBGP，因为它将直接连接到 MPLS 网络并作为站点的客户端路由运行。可以在“连接”> “查看站点”> “**BGP**”> “基本设置”下启用 **BGP**。

注意自治系统编号为 13。

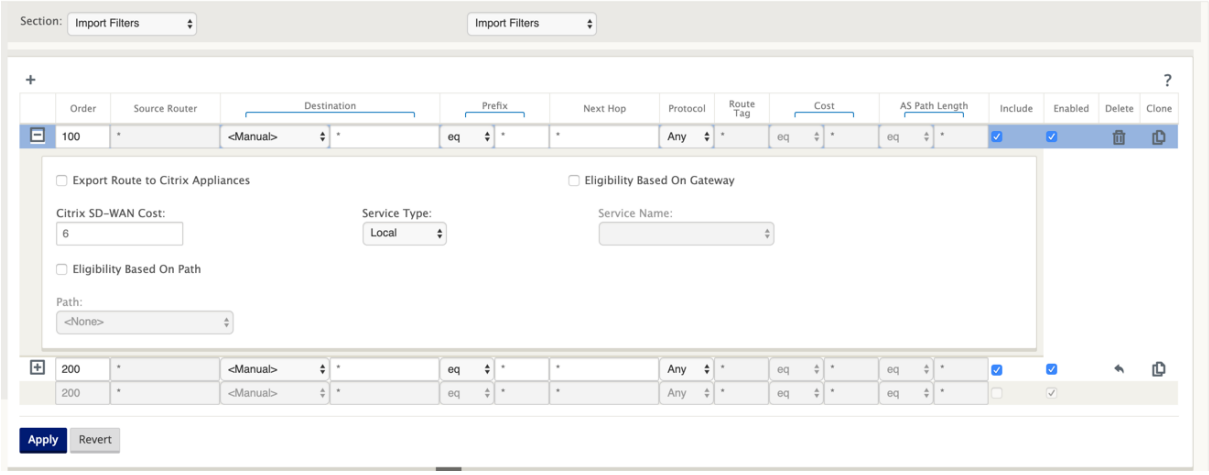




eBGP 彼此之间的对等位置。每个 ASN 是不同的。

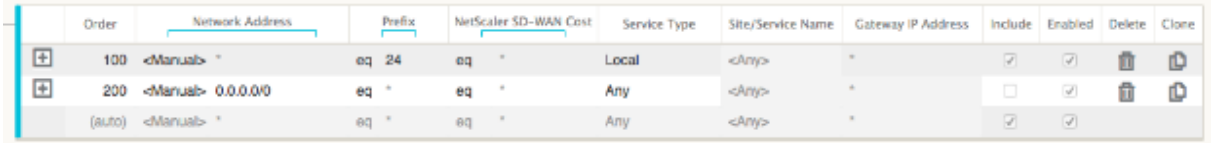
了解如何在虚拟路径路由表和正在使用的动态路由协议之间传递路由非常重要。以不利的方式创建路由循环或公告路由很容易。过滤器机制使我们能够控制进出路由表的内容。我们依次考虑每个位置。

- 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 导入所有路线。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。



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线：

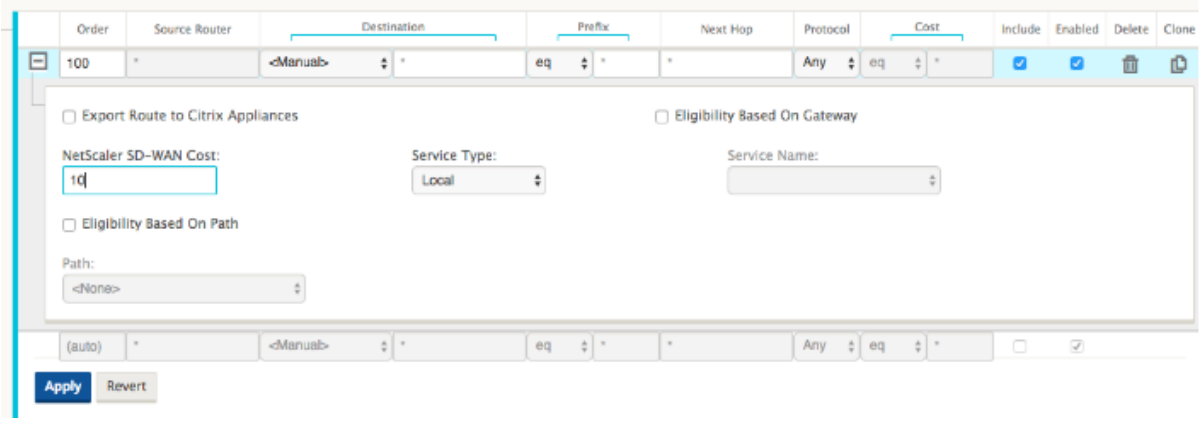
- 作为虚拟路径路由（数字 3），服务 = NYC-SFO，开销为 5 并键入静态。这是由 SD-WAN 设备在纽约宣传的本地子网。它是静态的，因为它直接连接到设备，或者它是在配置中输入的手动静态路由。它可以访问，因为站点之间的虚拟路径处于工作/启动状态。
- 作为通过 BGP（6 号）的广告路线，成本为 6。这现在被认为是一个后备路由。

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。

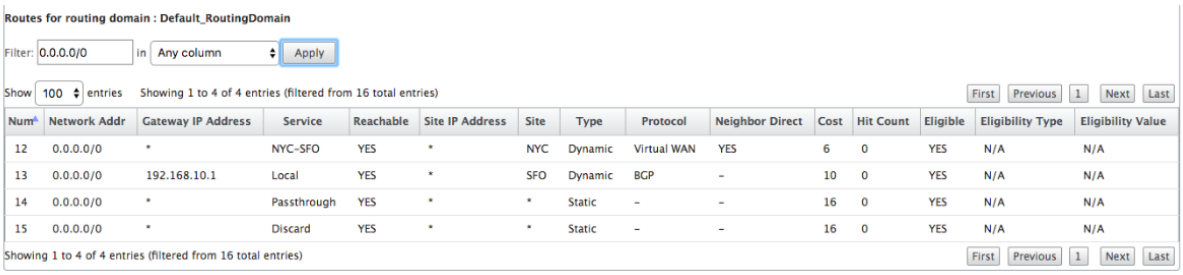
- 这是作为虚拟路径路由学习的（数字 9），但具有动态类型，开销为 6。这意味着远程 SD-WAN 设备通过路由协议（在本例中为 OSPF）了解此路由。默认情况下，路径成本较高。
- SD-WAN 还以相同的开销通过 BGP 获取此路由，因此在这种情况下，此路由可能优先于虚拟路径路由。

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互联网流量到纽约。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。



我们还看到一个直通和丢弃路线与成本 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。

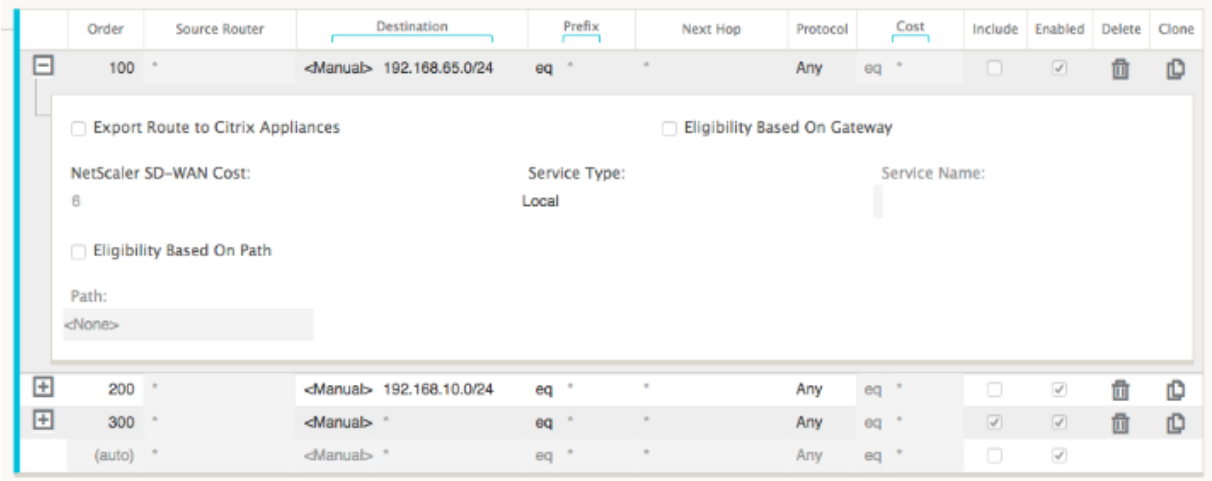
现在关注纽约站点，我们希望在虚拟路径处于活动状态时将发往远程站点（伦敦和旧金山）的流量定向到 SD-WAN 设备。

纽约站点中有多个子网可用：

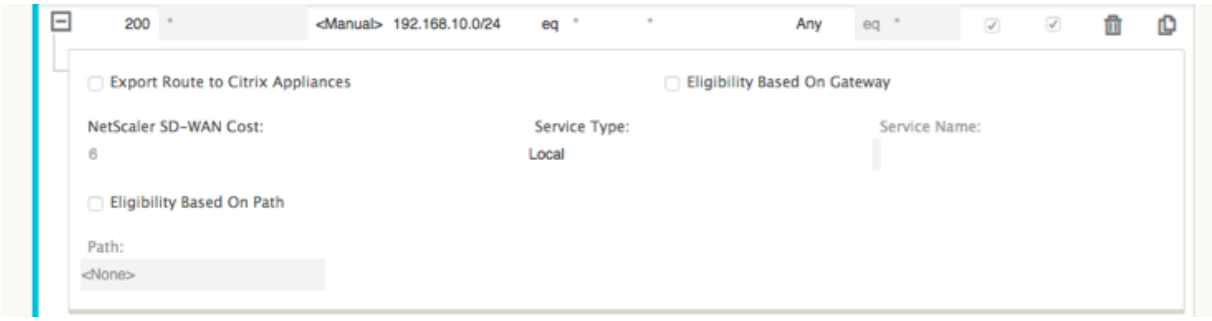
- 172.10.10.0/24（直接连接）
- 172.20.20.0/24（从核心路由器 B 通过 OSPF 公告）
- 172.30.30.0/24（从核心路由器 B 通过 OSPF 公告）

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 的所有互联网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线。

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。

Order	Network Address	Prefix	NetScaler SD-WAN Cost	Service Type	Site/Service Name	Gateway IP Address	Include	Enabled	Delete	Clone
100	<Manual> 192.168.10.0/24	eq *	eq *	Any	<Any>	*				
(auto)	<Manual> *	eq *	eq *	Any	<Any>	*				

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** 路线表：

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。

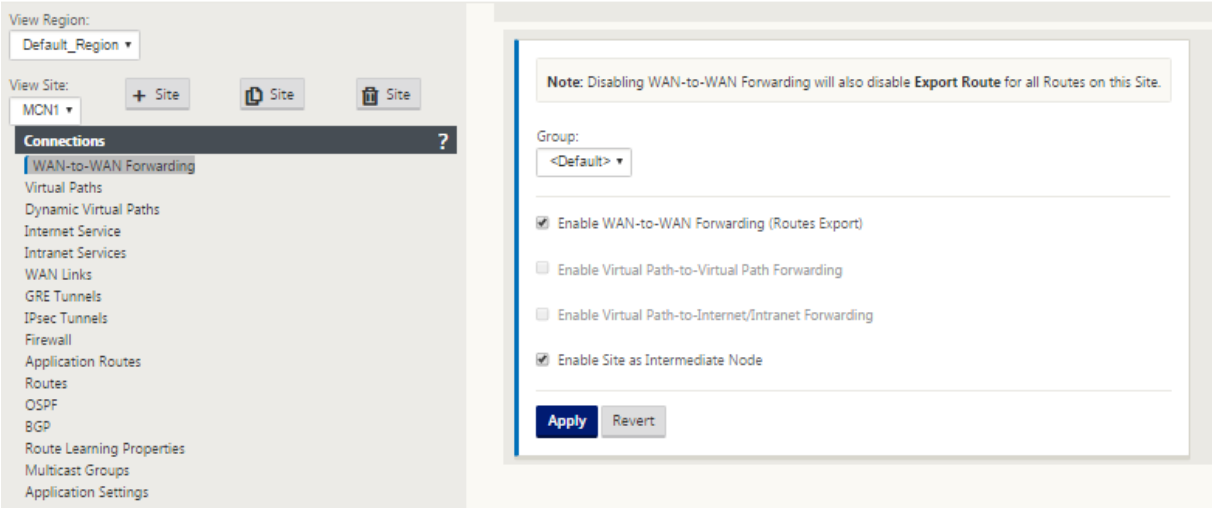
动态虚拟路径

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。

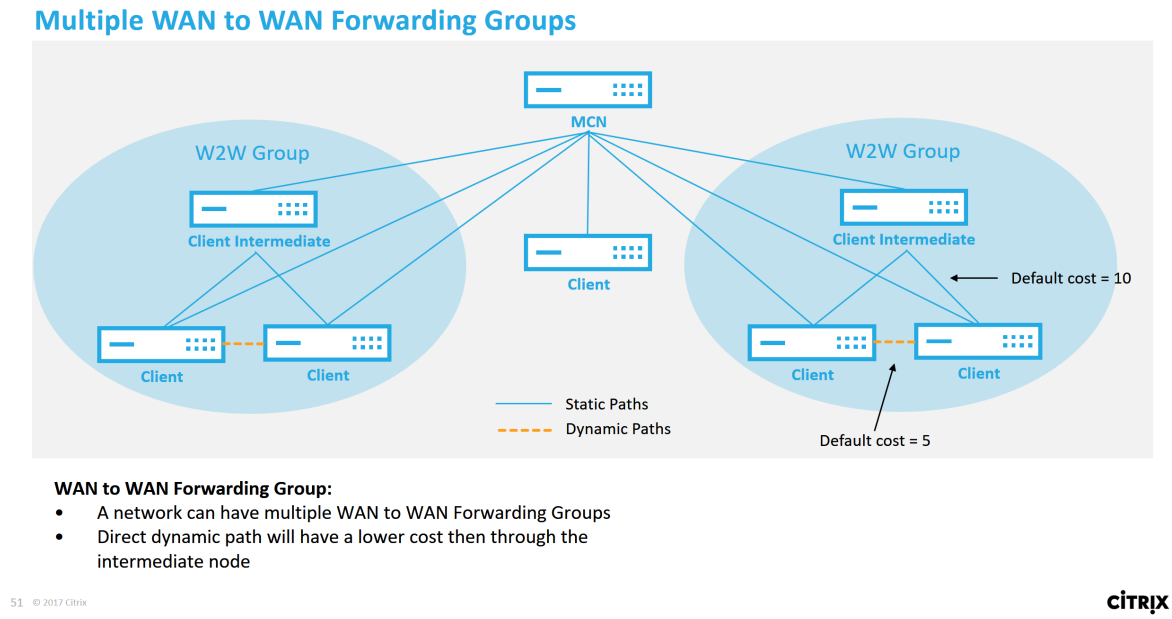
满足动态虚拟路径的阈值后，客户端节点会使用站点之间的所有可用 WAN 路径，动态地创建彼此的虚拟化路径，并按以下方式充分利用它：

- 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

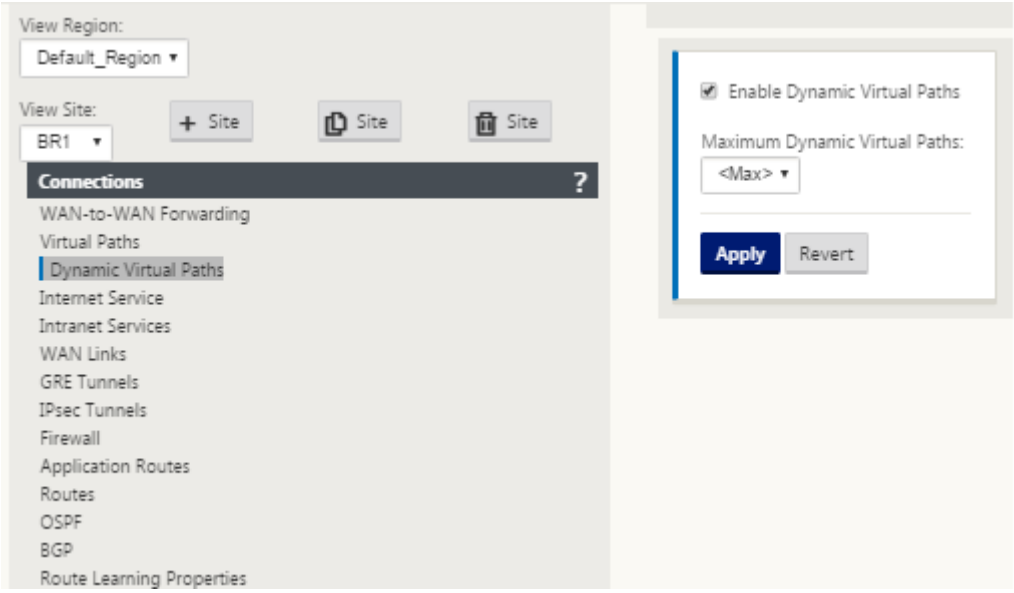
  动态虚拟路径具有中间站点的概念。中间站点可以是 MCN 站点或网络中配置了静态虚拟路径并连接到两个或多个其他客户端节点的任何其他站点。另一个设计考虑要求是启用 WAN 到 WAN 转发，允许将所有站点的所有路由播发到需要动态虚拟路径的客户端节点。除了为此中间站点 启用 **WAN** 到 **WAN** 转发 之外，还必须启用“将站点作为中间节点启用”，以监视客户端节点通信并指定何时必须建立和拆除动态路径。



SD-WAN 配置中可以允许多个 WAN 到 WAN 转发组，从而实现对某些客户端节点之间路径建立的完全控制，而不是其他节点之间的路径建立。



要使客户端节点作为中间站点运行，需要在静态虚拟路径与与 **WAN** 到 **WAN** 转发组关联的客户端之间配置静态虚拟路径。此外，客户端节点需要为每个客户端节点 启用 启用动态虚拟路径 选项。



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线顺序（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—应用于此路线的服务

- 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-特定路线的成本
- 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。
- 路线 10 —与 Internet 服务定义, 该系统添加了一个捕获所有路由直接互联网突破为本地站点.
- 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。

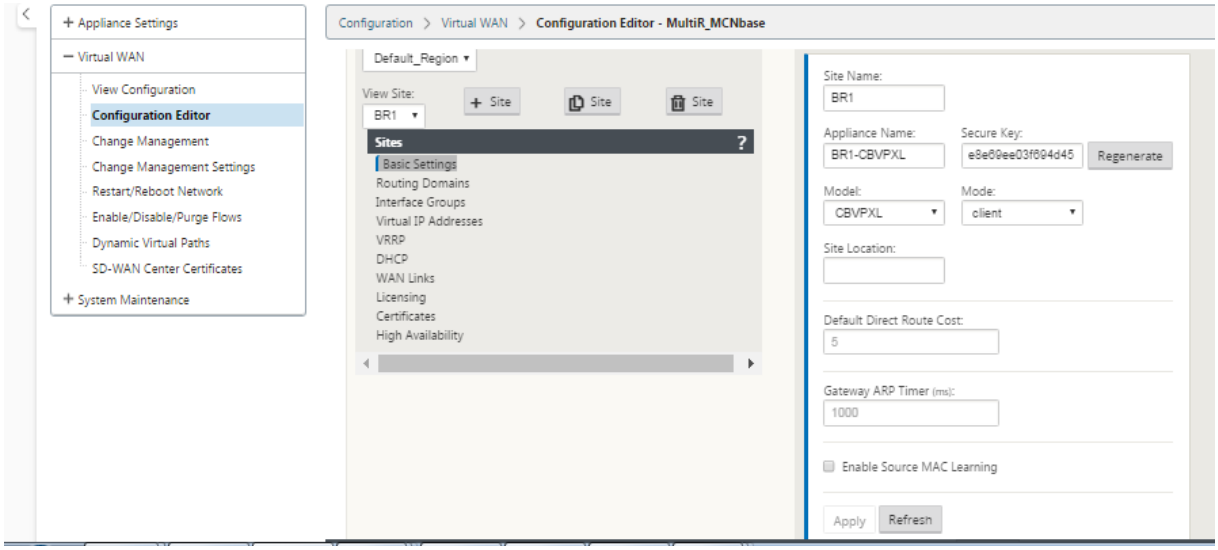
默认工艺路线成本值：

- 广域网到广域网转发—10
- 默认直接路线成本—5
- 自动生成的路线—5
- 虚拟路径—5
- 当地——5
- 内联网——5
- 互联网—5
- 直通-5
- 可选—路由为定义为服务级别的 0.0.0.0/0

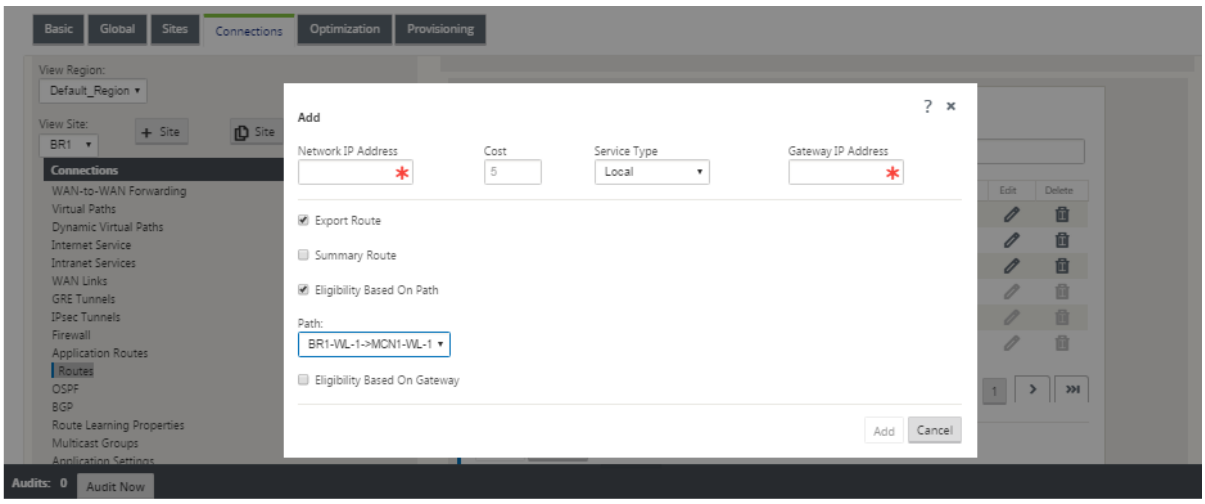
定义这些路径后，了解流量如何使用定义的路径流动非常重要。这些流量流分为以下流量：

- 局域网到 WAN（虚拟路径）—进入 SD-WAN 覆盖隧道的流量
- WAN 到局域网（虚拟路径）—存在 SD-WAN 覆盖隧道的流量
- 非虚拟路径流量—路由到底层网络的流量

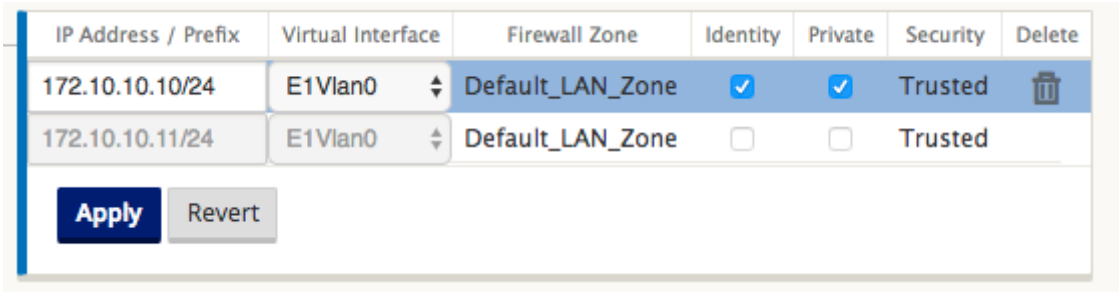
默认路径成本可以根据每个站点进行更改。配置可以在 查看站点 > 基本设置 下找到：



静态路由可以在 连接 > 站点 > 路 由 节点下为每个 站 点定义：



您注意到路由可以绑定到虚拟路径或网关 IP 可用性。Internet 路由可以导出到虚拟路径叠加或不取决于所需的行为。您也可以创建静态虚拟路径路由来强制流量到虚拟路径，即使我们没有获得通告到 SD-WAN 的前缀（即最后采用的成本较高的路由）。SD-WAN 还可以通过将虚拟 IP 地址 (VIP) 设置为私有，禁止本地子网进行播发。



> 注意
>
> 配置确实需要每个路由域中至少有一个非私有 VIP。

内联网和互联网路由

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/互联网-必需）
- 内网/互联网必须为 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
- 每个站点的最大路线学习导入过滤器：512
- 每个站点的最大路线学习导出过滤器：512
- 最大 BGP 路由策略：255
- 最大 BGP 社区字符串对象：255

路由域

June 22, 2021

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 隧道
  - 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。

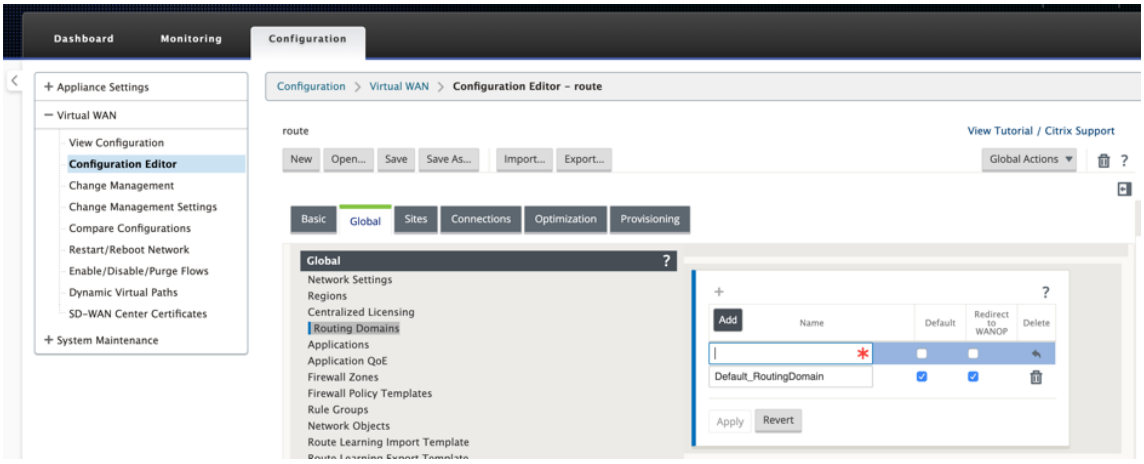
配置路由域

June 22, 2021

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。

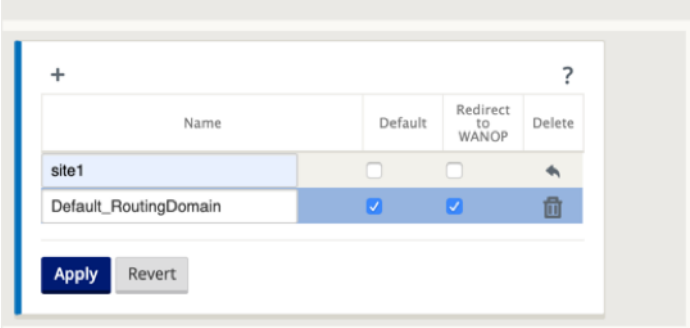
要配置路由域，请执行以下操作：

1. 在 SD-WAN Web 界面中，导航到 配置 > 虚拟 **WAN** > 配置编辑器。在 配置编辑器中，导航到 全局 > 路由域，单击 添加 **(+)**，然后输入新路由域的名称。



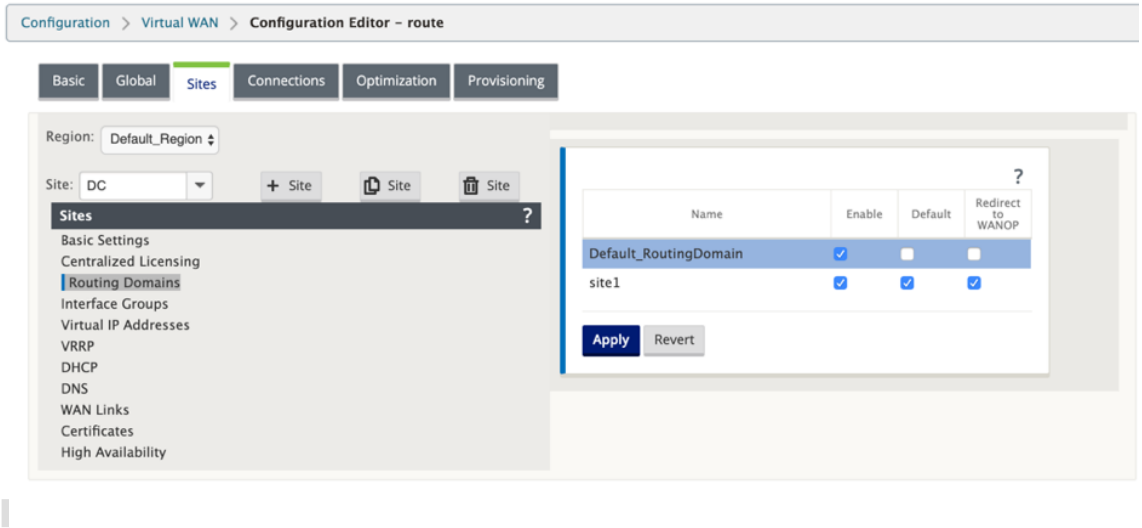
2. 如果要默认使用此路由域，请单击 默认 复选框。单击 应用 以保存更改。如果您计划实现单个路由域，则不需要显式配置。

   所有新配置都会自动填充默认路由域。



3. 导航到 站点 → [客户端站点名称] > 路由域。单击 启用 复选框以为站点启用已配置的路由域。

4. 单击 默认 复选框，使该路由域成为站点的默认设置。单击 应用 以保存更改。



> 注意
>
> 取消选中 为路由域 启 用 将使其无法在站点上使用。

在 11.0.2 版本中，允许 没有可路由虚拟 **IP (VIP)** 的路由域 具有以下功能：

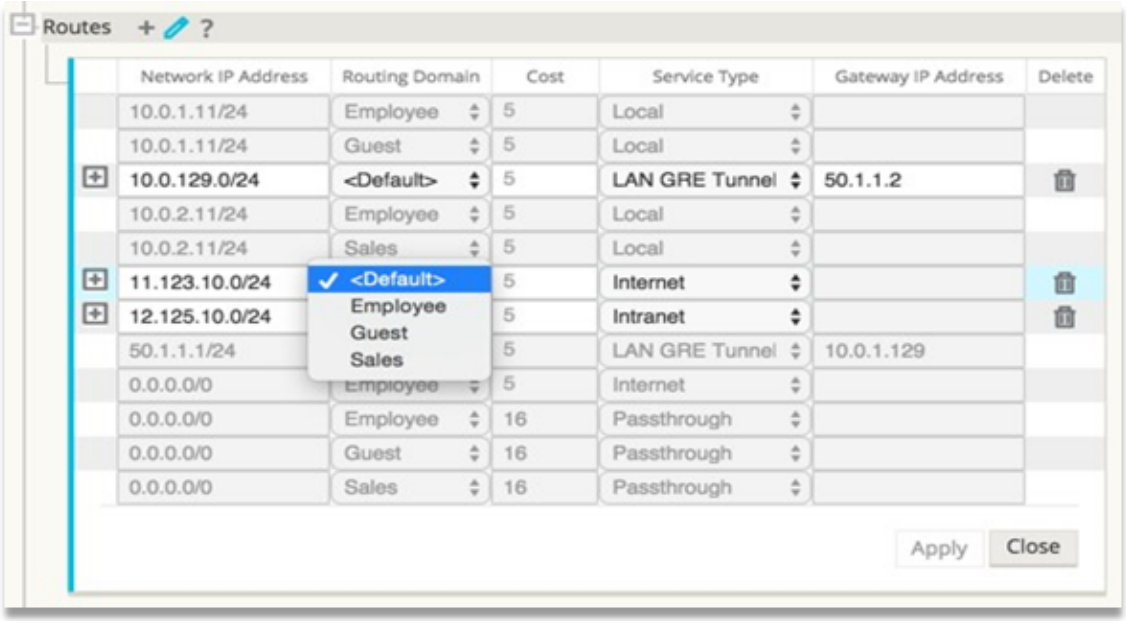
- 允许设备拥有不受信任或无接口的路由域。
- 允许分支机构通过在中间站点没有物理存在的路由域相互通信。

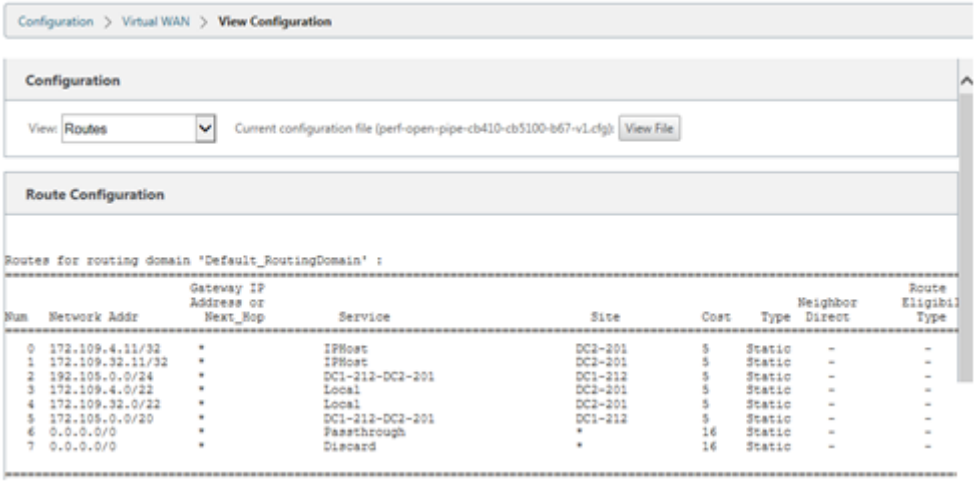
配置路由

June 22, 2021

要配置路由，请执行以下操作：

1. 在 配置编辑器中，导航到 连接 > [站点名称]> 路由。
2. 从下拉菜单中选择 路由域。新路由会自动与默认路由域关联。有关详细说明，请参阅 配置路由。





配置路由后，通过导航到“配置”> “虚拟 **WAN** ”> “查看”> “路由”来验证已 配置 路由域的 路由表。

使用 **CLI** 访问路由

June 22, 2021

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

November 1, 2021

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。

> 注意
>
> ：无法在以下 SD-WAN 设备上配置动态路由器 ID：
>
> - Citrix SD-WAN 1000 SE /PE
> - Citrix SD-WAN 2000 SE /PE
> - Citrix SD-WAN 4000 SE

OSPF

OSPF 是互联网工程任务组（IETF）的内部网关协议（IGP）小组为互联网协议（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。

现在，您可以配置 Citrix SD-WAN 设备 (Standard and Premium (Enterprise) Edition)，以便使用 OSPF 了解路由和宣传路由。

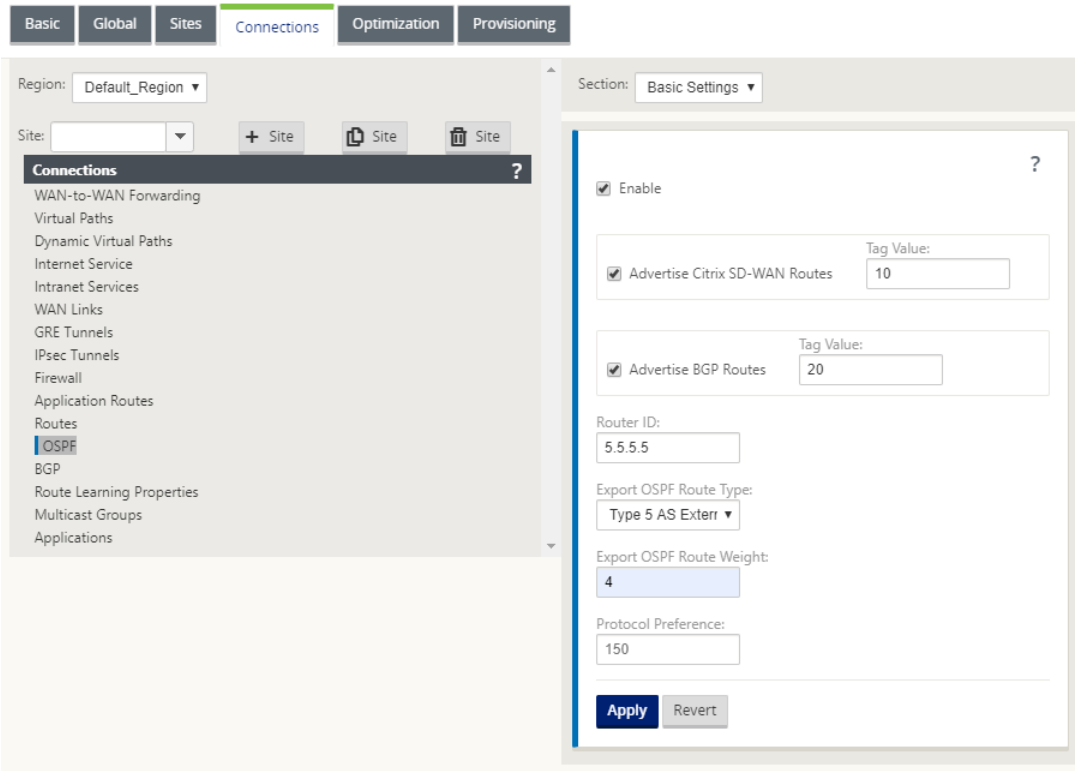
> 注意
>
> - Citrix SD-WAN 设备不作为指定路由器 (DR) 和 BDR (备份指定路由器) 参与每个多访问网络，因为默认 DR 优先级设置为“0”。
> - Citrix SD-WAN 设备不支持将总结作为区域边界路由器 (ABR)。

配置 **OSPF**

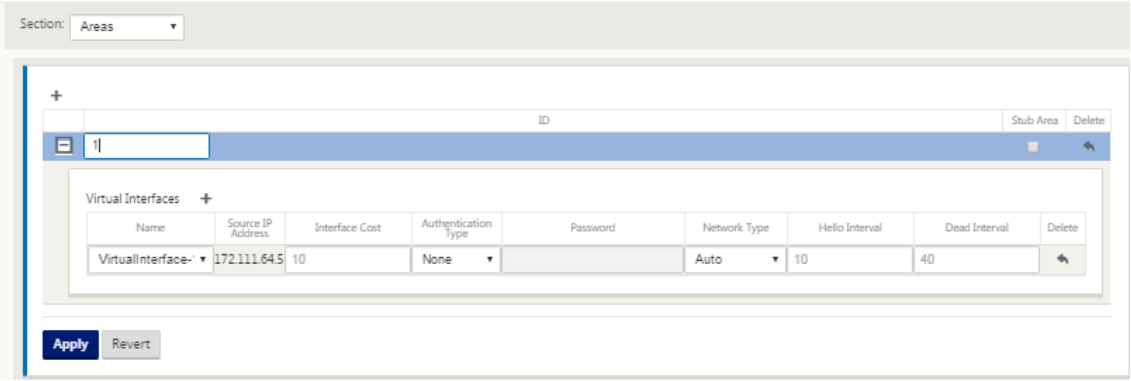
要配置 OSPF，请执行以下操作：

1. 在 配置编辑器中，导航到 连接 **>** 区域 **>** 站点 **> OSPF >** 基本设置。
2. 单击 启用，选择或输入以下参数的值，然后单击 应用。
   - 通告 **Citrix SD-WAN** 路由：允许通过 OSPF 通告 Citrix SD-WAN 路由。您还可以为 OSPF 重新分发指定一个标签。
   - 通告 **BGP** 路由：允许通过 OSPF 通告从 BGP 对等体获知的路由。您还可以为 OSPF 重新分发指定一个标签。
   - 路由器 **ID**：唯一的路由器标识符，路由器用于 OSPF 通告。如果未指定路由器 ID，则会自动选择它 作为 SD-WAN 网络中托管的最低虚拟 IP。

- 导出 **OSPF** 路由类型：将 Citrix SD-WAN 路由作为区域内路由或外部路由通告给 OSPF 对等体。
- 导出 **OSPF** 路由权重：将 Citrix SD-WAN 路由导出到 OSPF 时，请将此权重添加到每个路由的 Citrix SD-WAN 成本中。
- 协议首选项：如果通过多个路由协议获知前缀，则协议首选项值将决定路由协议的选择。有关详细信息，请参阅 协议首选项。



3. 展开 **OSPF** -> 区域，然后单击 编辑。



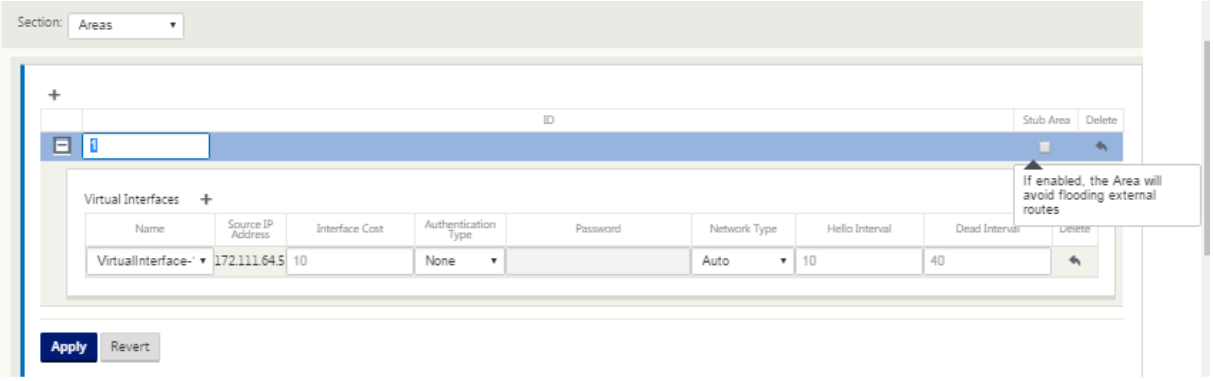
4. 输入一个 区域 **ID** 以了解路线和通告到的路线。
5. 如果没有为特定的虚拟 IP 地址检查身份，则关联的虚拟接口不可用于 IP 服务。
6. 从“名称”菜单中选择一个可用的虚拟接口。虚拟接口决定源 **IP** 地址。
7. 输入 接口成本（默认值为 10）。

8. 从菜单中选择 身份验证类型。
9. 如果您在步骤 8 中选择了 密码 或 **MD5** ，请输入密码关联的文本字段。
10. 在 **Hello** 间隔 字段中，输入向直接连接的邻居发送 Hello 协议数据包之间等待的时间（默认为 10 秒）。
11. 在 死间隔 字段中，输入在将路由器标记为死机之前要等待的时间间隔。默认死区间为 40 秒。
12. 单击应用以保存所做的更改。

存根面积

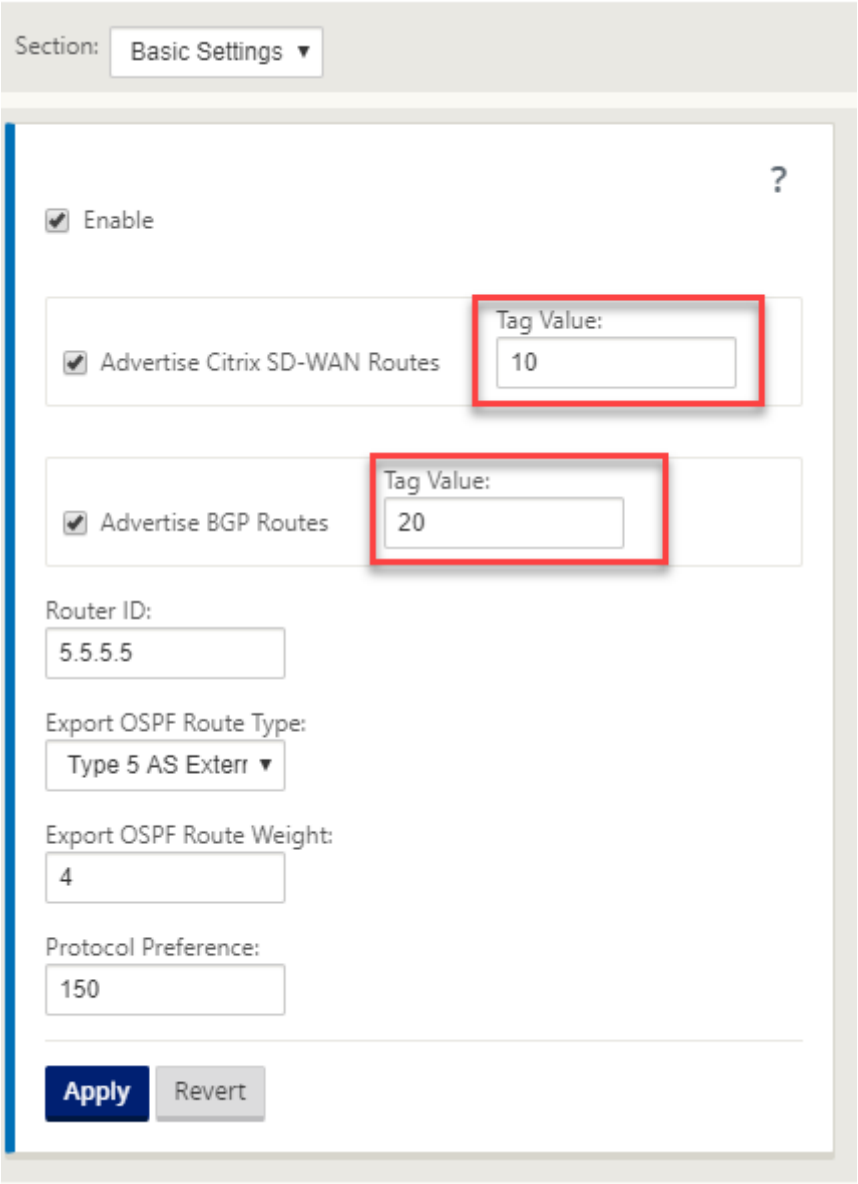
存根区域不受外部路由的影响，并接收有关属于同一 OSPF 域其他区域的网络的信息。

启用 存根区域 复选框。



OSPF 重新分配标签

您可以使用 OSPF 标签来防止在 OSPF 和其他协议之间相互重新分配过程中的路由循环。在 OSPF 域中，如果有 SD-WAN 和 BGP 学习到的路由到同一子网，则 OSPF 循环防护机制将其识别为循环并忽略路由。为 SD-WAN 和 BGP 学习路由指定不同的标签允许将这些路由安装在 OSPF 路由表中。
您可以在 OSPF 基 本设置 部分中为通过 SD-WAN 和 BGP 学习的路由配置 OSPF 重新分发标记。



BGP

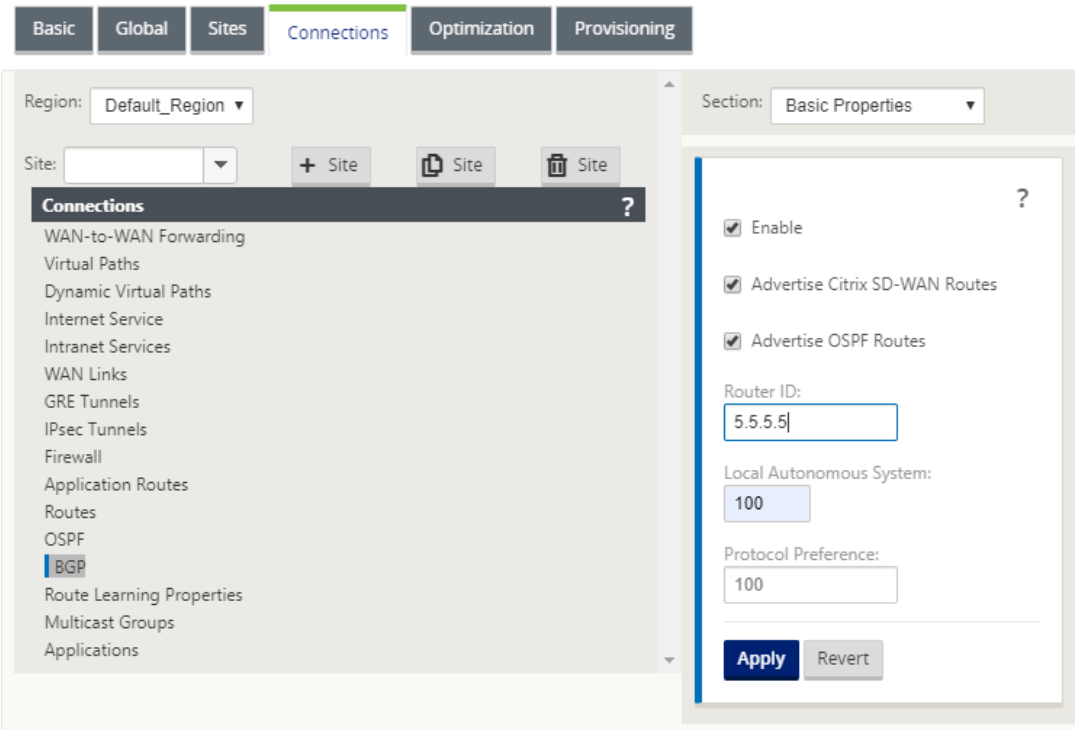
BGP 是一种自主的系统路由协议。自治网络或网络组在通用管理和通用路由策略下进行管理。BGP 用于交换互联网的路由信息，是 ISP 之间使用的协议。客户网络部署内部网 Gateway 协议，如 RIP 或 OSPF，用于在其网络中交换路由信息。客户连接到 ISP，ISP 使用 BGP 交换客户和 ISP 路线。在自治系统 (AS) 之间使用 BGP 时，协议称为外部 BGP (eBGP)。如果服务提供商使用 BGP 在 AS 内交换路由，则该协议称为内部 BGP (iBGP)。

BGP 是部署在互联网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。

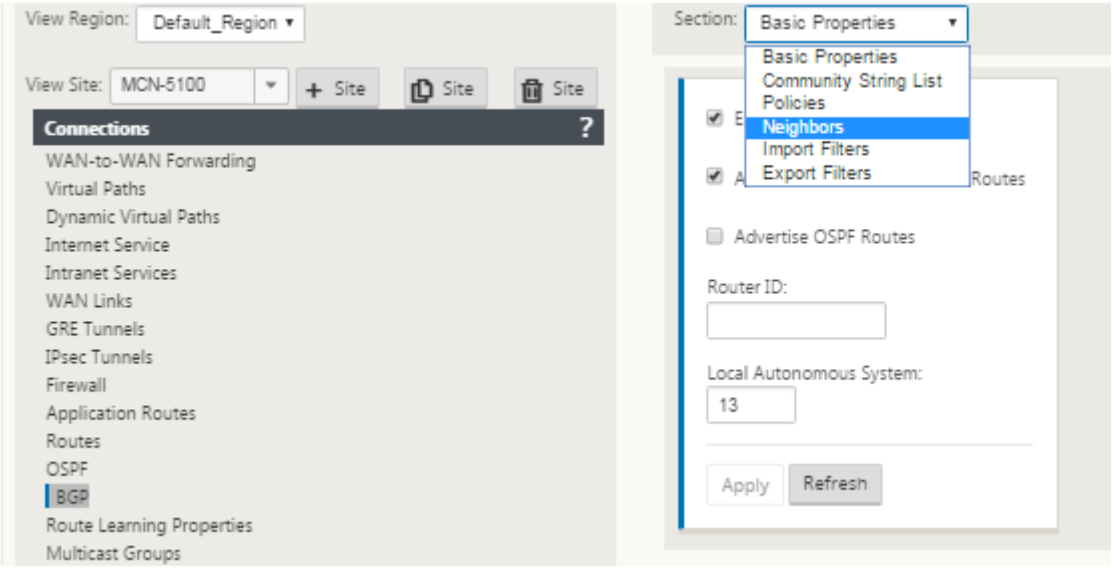
配置 **BGP**

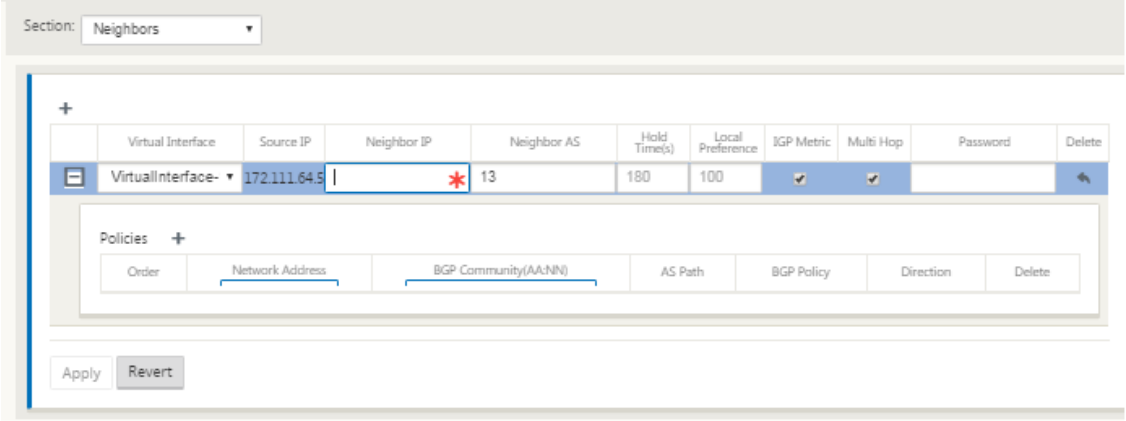
要配置 BGP，请执行以下操作：

1. 在 配置编辑器中，导航到 连接 **>** 区域 **>** 站点 **> BGP >** 基本设置。
2. 单击 启用，选择或输入以下参数的值，然后单击 应用。
   - 公布 **Citrix SD-WAN** 路由：允许通过 BGP 通告 Citrix SD-WAN 路由。
   - 通告 **OSPF** 路由：允许通过 BGP 通告从 OSPF 对等体获知的路由。
   - 路由器 **ID**：唯一的路由器标识符，路由器用于 OSPF 通告。如果未指定路由器 ID，则会自动选择它 作为 SD-WAN 网络中托管的最低虚拟 IP。
   - 本地自治系统：从中获取路由并通告路由的本地自治系统编号。自治系统号码必须与相邻路由器上的一个相匹配。
   - 协议首选项：如果通过多个路由协议获知前缀，则协议首选项值将决定路由协议的选择。有关详细信息，请参阅 协议首选项。



3. 展开 基本设置 **>** 邻居，然后单击 添加 **(+)** 图标。





对于具有多个路由域的站点，选择一个路由域。路由域决定哪些虚拟接口可用。

4. 从菜单中选择一个 虚拟接口。虚拟接口决定源 IP 地址。
5. 在邻居 **IP** 字段中输入 **IBGP** 邻居路由器的 **IP** 地址，在邻居 AS 字段中输入 本地自治系统 编号。
6. 在 保持时间字段 中，输入在宣布邻居关闭之前等待的保持时间（默认值为 180）。
7. 在 本 地首选项 字段中，输入 本地首选项 值（以秒为单位），该值用于从多个 BGP 路由中进行选择（默认值为 100）。
8. 单击 **IGP** 度量 复选框以启用内部距离的比较以计算最佳路径。
9. 单击 多跳 复选框可为路由启用多个跃点。
10. 在 密码 字段中，输入 BGP 会话 MD5 身份验证的密码（不需要进行身份验证）。

> 注意
>
> SD-WAN 网络中不支持为 iBGP 配置路由反射器和联合会。

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：

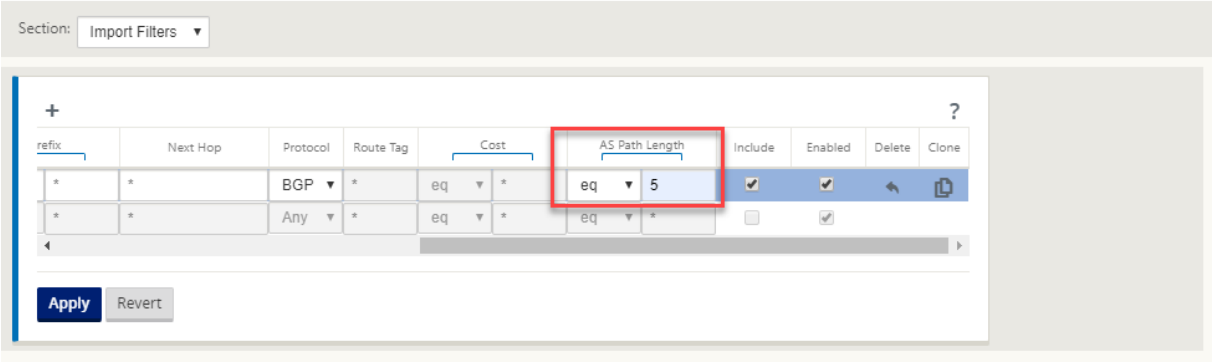
- SD-WAN 站点通过 eBGP 与非 SD-WAN 站点通信
- 基于虚拟路径和 eBGP 的 SD-WAN 站点之间的通信
- 在单臂拓扑中实现 OSPF
- MPLS 网络中 OSPF Type5 到 Type1 部署
- SD-WAN 和非 SD-WAN（第三方）设备 OSPF 部署
- 使用 SD-WAN 网络实现 OSPF，具有高可用性设置

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。

要在导入过滤器中配置 AS 路径长度，请选择 BGP 作为协议，选择谓词，然后输入 **AS** 路径长度。有关详细信息，请参阅 路由过滤



监视路线统计

导航到 监视器 > 统计信息。从 显示 下拉菜单中选择 路线。

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

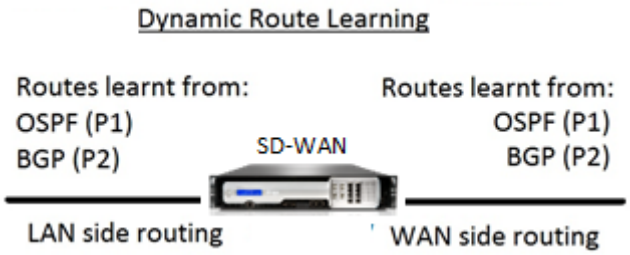
June 22, 2021

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：动态路线共享

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。

要配置 OSPF 类型 1：

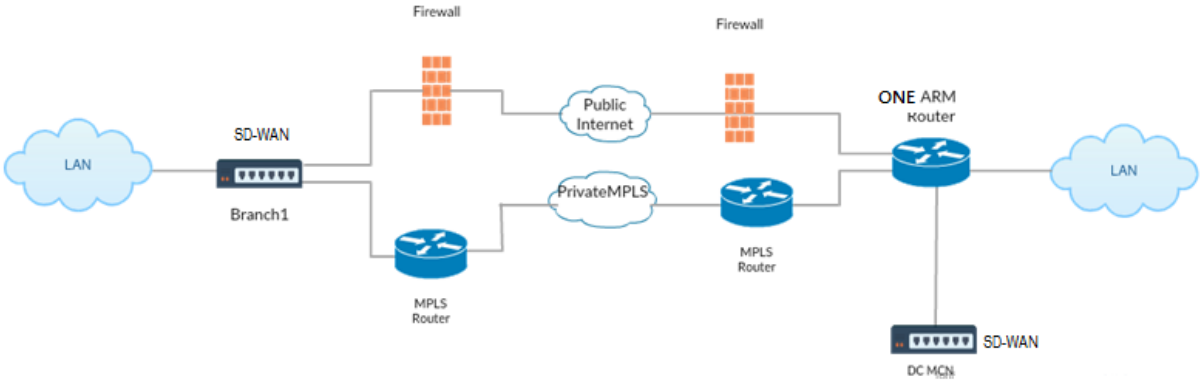
1. 在 DC 站点和分支站点上配置虚拟接口和 **WAN** 链路，以便在它们之间创建虚拟路径。
2. 在 连接 > [**MCN**] > 路线学习 > **OSPF** > 基本设置 下，选择 导出 **OSPF** 路线类型 为类型 **1** 内区域。
3. 保存配置、转储和激活配置。

您 必须能够在 “
导出 **OSPF** 路由类型” 下看到以下路由类型：

- 5 型 A 外部
- 1 型内部区域

您 必须能够配置 类型 **5 AS** 外部 路由。

激活更改后的配置后，您 必须在配置 > 虚拟广域网 > 查看配置 **** > **** 动态路由下看到路由类型更改。

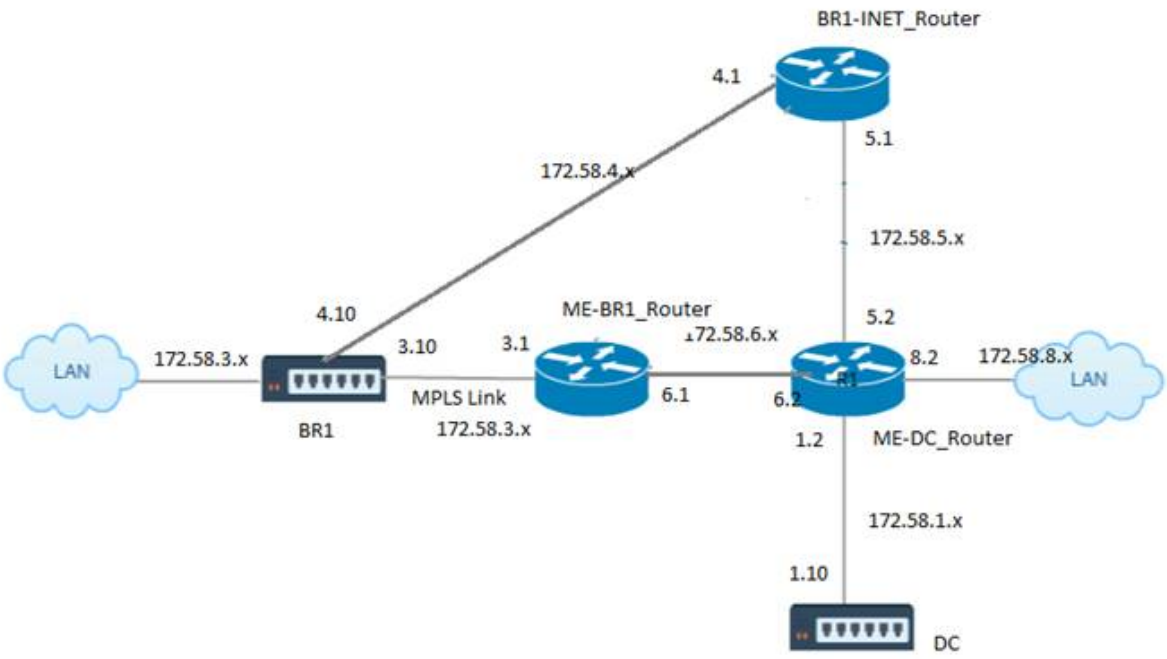


如上图所示，DC MCN 部署在单臂拓扑中。DC 站点启动时，单臂路由器会将所有流量从本地 LAN 转发到其他站点，例如目的 IP 地址位于同一子网内的分支本地 LAN，然后 SD-WAN 设备将所有数据包包装到路由器，并将其发送到所有数据包目标 IP 地址中的分支虚拟 IP 地址。然后，路由器将这些数据包转发到 WAN。

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 中的 我-*BR1_* 路由器 和 我-*DC_* 路由器 之间配置。
- OSPF 在区域 0 中的 *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。

要在基本 **OSPF** 设置下将 OSPF 导出的路由配置为 Type1：

1. 在 DC 站点和分支站点上配置虚拟接口和 **WAN** 链路，以在它们之间创建虚拟路径。
2. 在 连接->[**MCN**]> 路线学习->**OSPF**-> 基本设置下，选择 导出 **OSPF** 路线类型为类型 **1** 内区域。
3. 保存配置、转储并激活相同的配置。您 必须能够在“导出 **OSPF** 路由类型”下看到以下两种路由类型：
   - 5 型 A 外部
   - 1 型内部区域

激活已更改的配置后，您可以在 配置 **>** 虚拟 WAN**>** 查看配置 > 动态路由 下看到路由 类型更改。

路由必须由 SD-WAN 设备通告为 Type5 外部 AS。通过 SD-WAN 获取的路由必须在相邻路由器中显示为 Type5 AS 外部路由。

要在基本 **OSPF** 设置下配置 OSPF 导出的路由权重：

1. 在 DC 站点和分支站点上配置虚拟接口和 WAN 链路，以在它们之间创建虚拟路径。
2. 在 连接 [**MCN**] > 路由学习 > **OSPF** > 基本设置 下，配置 导出 **OSPF** 路由权重。
3. 保存配置、转储并激活相同的配置。

4. 现在，将导出 OSPF 路由权重配置为介于 **1** 到 **65529** 之间的任何数值。
5. 激活已更改的配置后，您可以在 配置 **>** 虚拟 WAN**>** 查看配置 > 动态路由 下看到 路由 权重。导出的默认路径权重必须为 0。路由的实际成本必须仅为 SD-WAN 的成本。

要在“导出过滤器”设置下将 OSPF 导出的路由配置为 Type1，请执行以下操作：

1. 在 DC 和 Branch 上配置虚拟接口 和 **WAN** 链路，以便我们可以在它们之间创建虚拟路径 1。在 连接 > **[MCN]** > 路由学习 > **OSPF** > 导出筛 选器 下，配置导出筛选器。
2. 展开筛选器。将 导出 **OSPF** 路线类型 配置为 类型 **1** 区域内 路线。
3. 保存配置、转储并激活相同的配置。您 必须能够在“导出 **OSPF** 路由类型”下看到以下两种路由类型
   - 5 型 A 外部
   - 1 型内部区域

激活更改后的配置后，用户 必须能够在 配置 **>** 虚拟广域网 **>** 查看配置下看到路由类型更改。路由类型必须显示为类型 5 AS 外部。

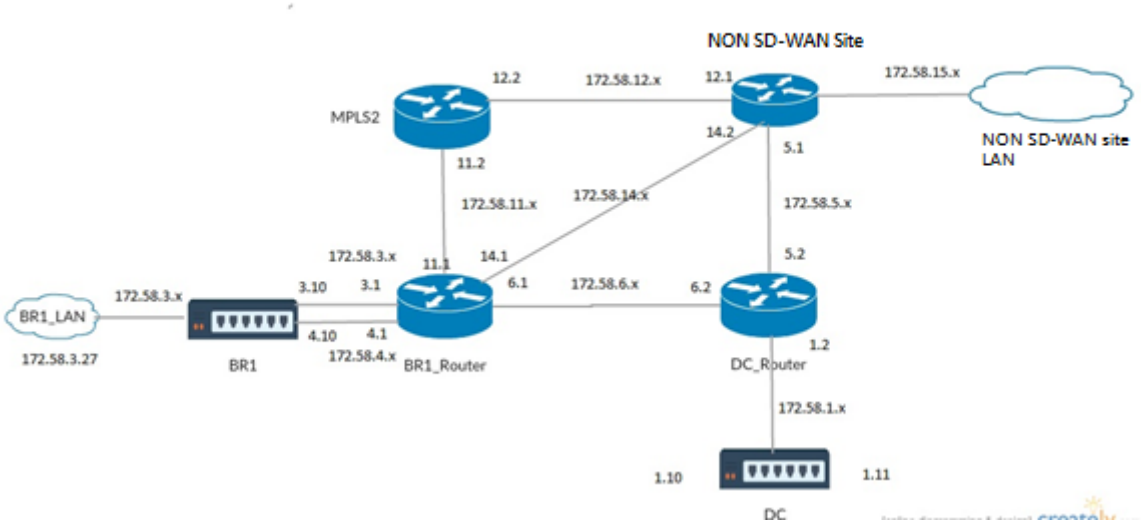
要在 导出筛选器 设置下配置 OSPF 导出的路由权重：

1. 在 DC 和分支上配置虚拟接口和 WAN 链路，以便我们可以创建它们之间的虚拟路径。
2. 在 连接 > [**MCN**] > 路由学习 > **OSPF** > 导出筛 选器 下配置导出筛选器。
3. 展开筛选器。将导出 OSPF 路由权重配置为介于 **1** 到 **65529** 之间的任何数值。
4. 保存配置、转储并激活相同的配置。

激活更改后的配置后，用户 必须能够在 配置 **>** 虚拟广域网 **>** 查看配置下看到路由类型更改。
在导出筛选器下配置的路由权重必须覆盖 基本 **OSPF** 设置下配置的权重。

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。



配置步骤：

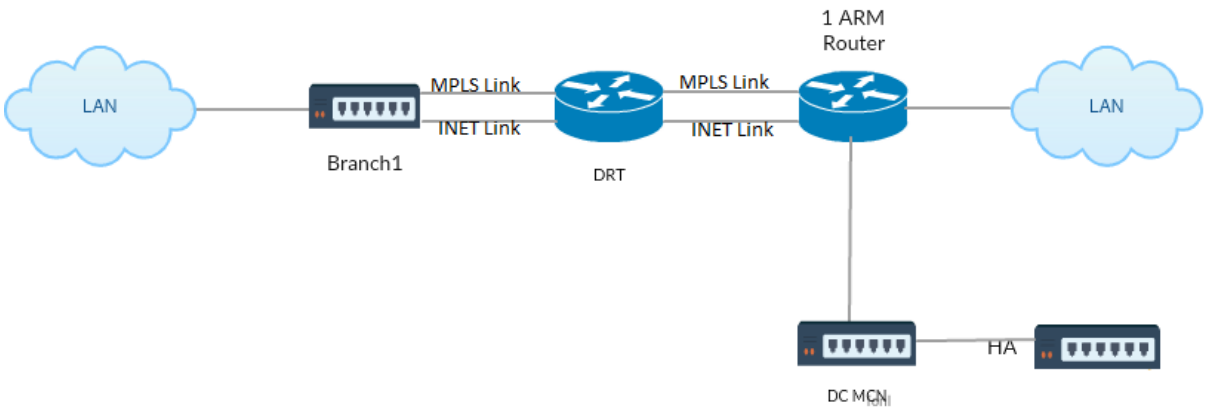
1. 在 DC 和分支上配置 虚拟接口 和 **WAN** 链 接，以便在站点之间创建虚拟路径。
2. 将导出路由类型配置为 **Type1**，并在 SD-WAN 设备上将成本分配为 **195**。
3. 保存、转储和激活配置。
4. 在 DC 站点和分支站点上的最终主机之间发送流量。
5. 关闭 R1 和 R2 之间的链路。
6. 在 DC 站点和分支站点上的最终主机之间发送流量。
7. 取消关闭 R1 与 R2 之间的链接。
8. 在 DC 站点和分支站点上的最终主机之间发送流量。
9. 禁用 DC 站点上的虚拟广域网服务，以便虚拟路径关闭。
10. 在 DC 站点和分支站点上的最终主机之间发送流量。

验证配置：

1. 最初，在步骤 4 中，所有流量都通过 SD-WAN 设备。
2. 在步骤 6 中，当 R1 和 R2 之间的链接断开时，通过 R3 将流量路由到 SD-WAN。
3. 在步骤 8 中，流量流经 SD-WAN 设备，R2 作为 LAN 路由器 R1 的下一跳。
4. 在步骤 10 中，虚拟 WAN 路径在 DC 和 BR1 设备之间断开，流量必须与配置 SD-WAN 网络之前一样正常流动。

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**



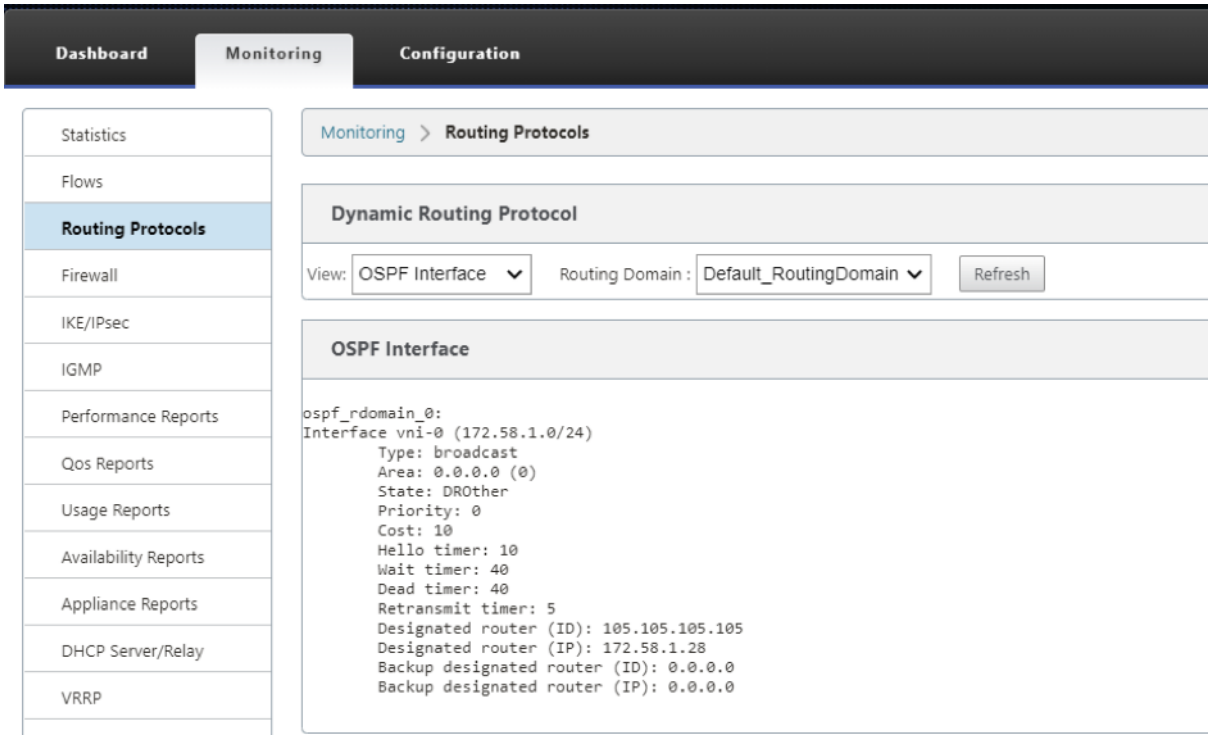
OSPF Type5 到 Type1 与高可用性站点在故障转移到备用设备并部署在高可用性设置中：

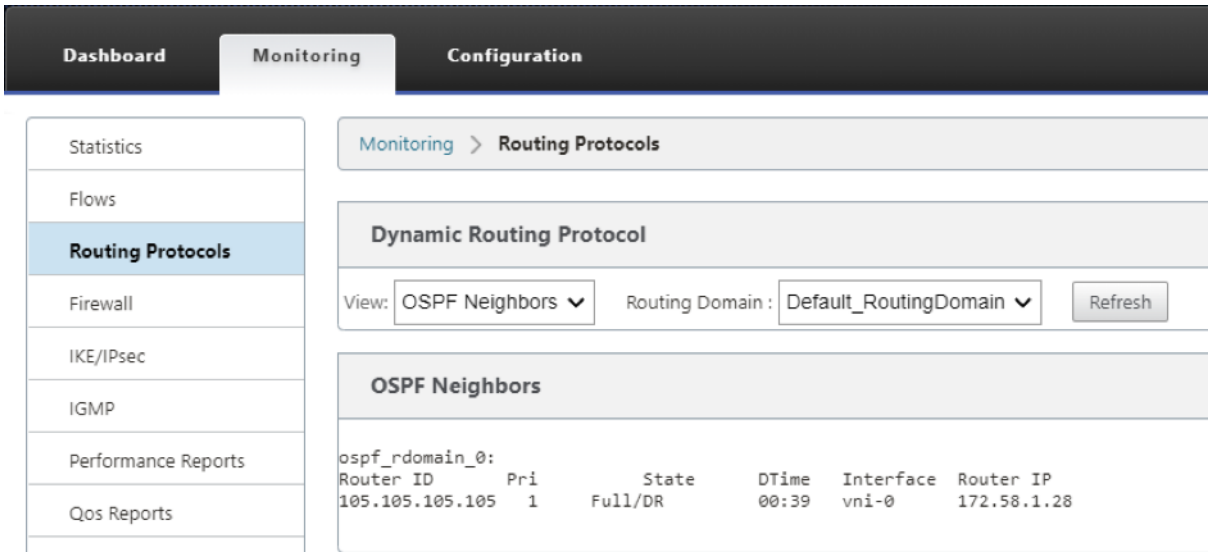
要在 HA 部署中配置 OSPF，请执行以下操作：

1. 在 DC 和 **Branch** 上配置虚拟接口和 **WAN** 链 路，以在它们之间创建虚拟路径。
2. 设置高可用性。
3. 导出配置为 类型 **1** 和路径重量为 ****50** 的路径 ** 类型。
4. 保存配置、转储并激活相同的配置。
5. 启动流量。
6. 请注意，在 监控 > 统计 > 路由下，OSPF 路由的命中计数会以最低的成本增加。
7. 将活动 MCN 放下并观察行为。
8. 恢复原来的活动 MCN。
9. 控制板 > 高可用性状态 显示适用于活动和备用的 HA 本地设备和对等设备。
10. 在 配 置 > 查 看 配 置 > 动 态 路 由 下，OSPF 已 启 用，**export_ospf_route_type** 显 示 **Type1** 和 **export_ospf_route_weight** 显示为 **50**。
11. 即使在故障转移后，高可用性状态也会显示本地和对等设备的正确 OSPF 配置。
12. 查看 监视器 > 统计信息 > 路径。以最低成本的 OSPF 路线的命中次数增加。
13. 故障恢复后，“高可用性状态” 会显示本地和对等设备的正确 OSPF 配置。
14. 在 “监视器” **>** “统计信息” **>** “路由” 视图下验证 **OSPF** 路由的命中计数是否以低成本增加。

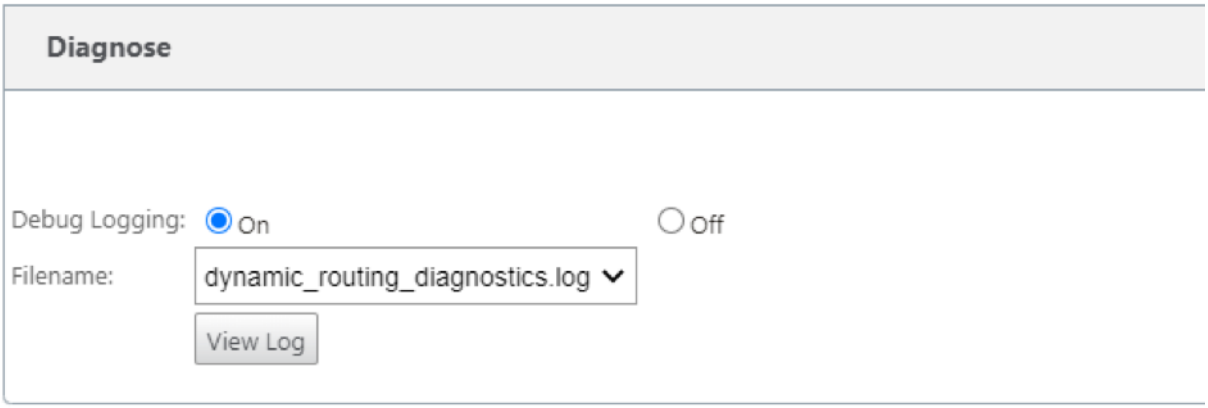
故障排除

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

June 22, 2021

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。

配置策略

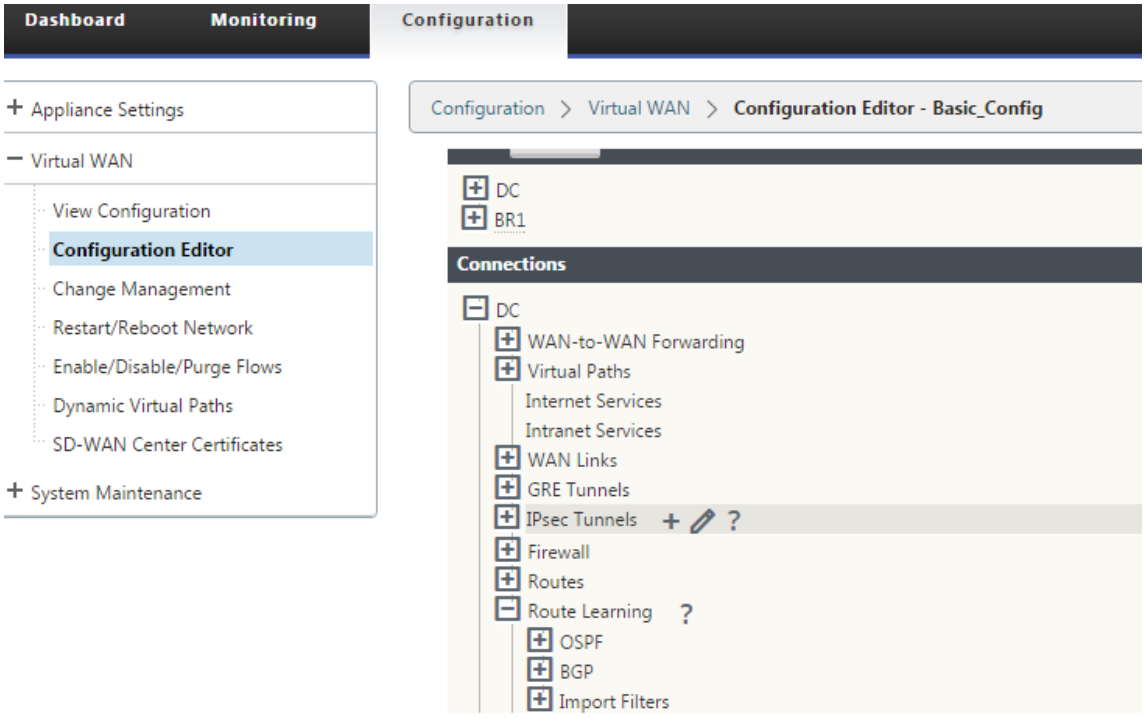
在 SD-WAN Web 管理界面中，配置编辑器在 路由学习 > BGP 下有一个新的部分，即 **BGP** 策略。在本节中，用户可以添加构成策略的 BGP 属性。支持添加团体字符串、预置 AS 路径以及配置 MED。

您可以手动配置每个社区字符串，也可以从下拉菜单中选择不播发或不导出社区字符串。对于手动配置，您可以输入一个系统号码和社区。您可以选择 插入/删除 以标记路线或从路线中移除社区。

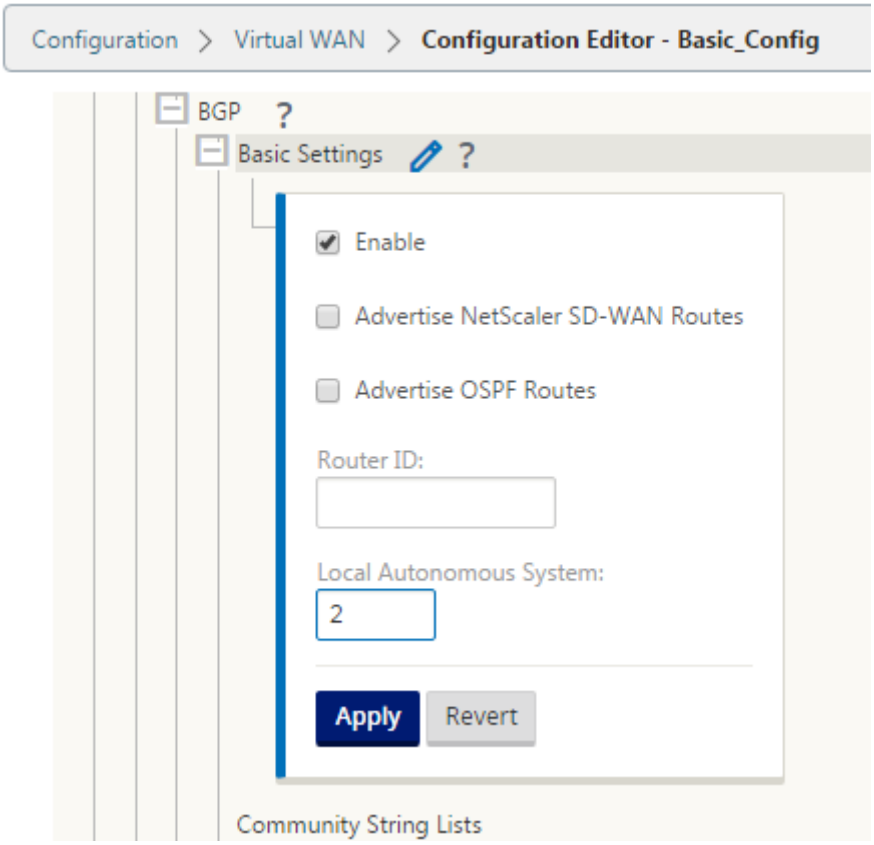
您可以配置要在本地网络之外进行公告之前将本地 as 预先添加到 CA 路径 的次数。您可以为匹配路由配置 MED。

要配置 BGP 策略，请执行以下操作：

1. 在 NetScaler SD-WAN Web 管理界面中，转到 配置 > 虚拟广域 网 > 配置编辑器。打开现有配置包。转到 站点 > **DC** 或 分支 设置。

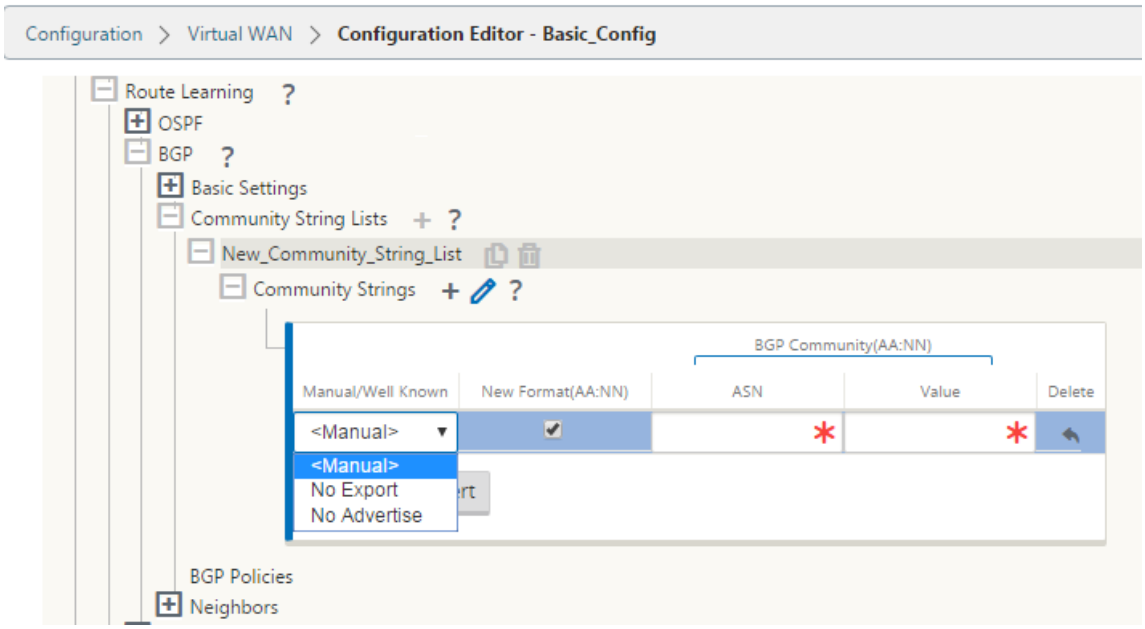


2. 展开 **BGP** ，然后单击 基本设置 下的 启用。输入 路由器 **ID** 和 本地自治系统 值，然后单击 应用。

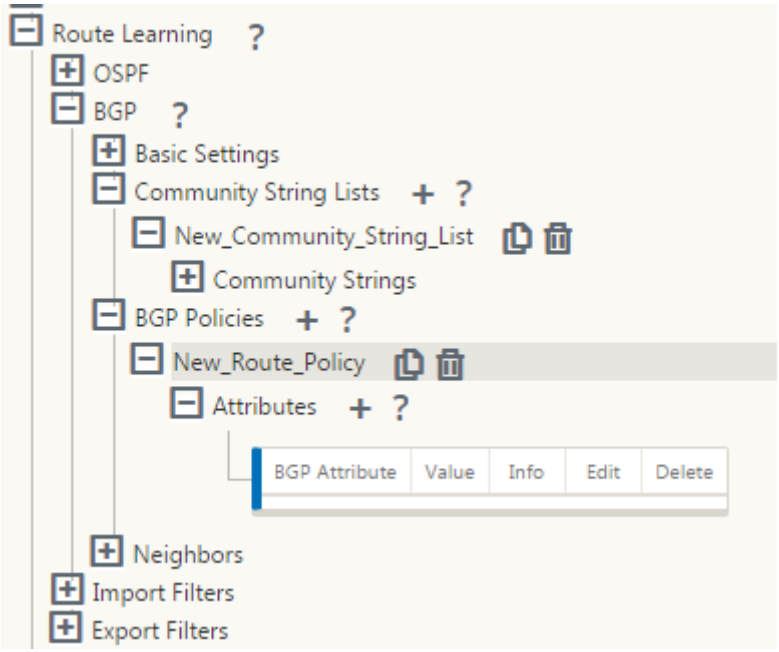


3. 单击 社区字符串列表旁边的 + 签名。手动配置每个社区字符串，或通过从下拉菜单中选择 无宣传 或 无导出社区

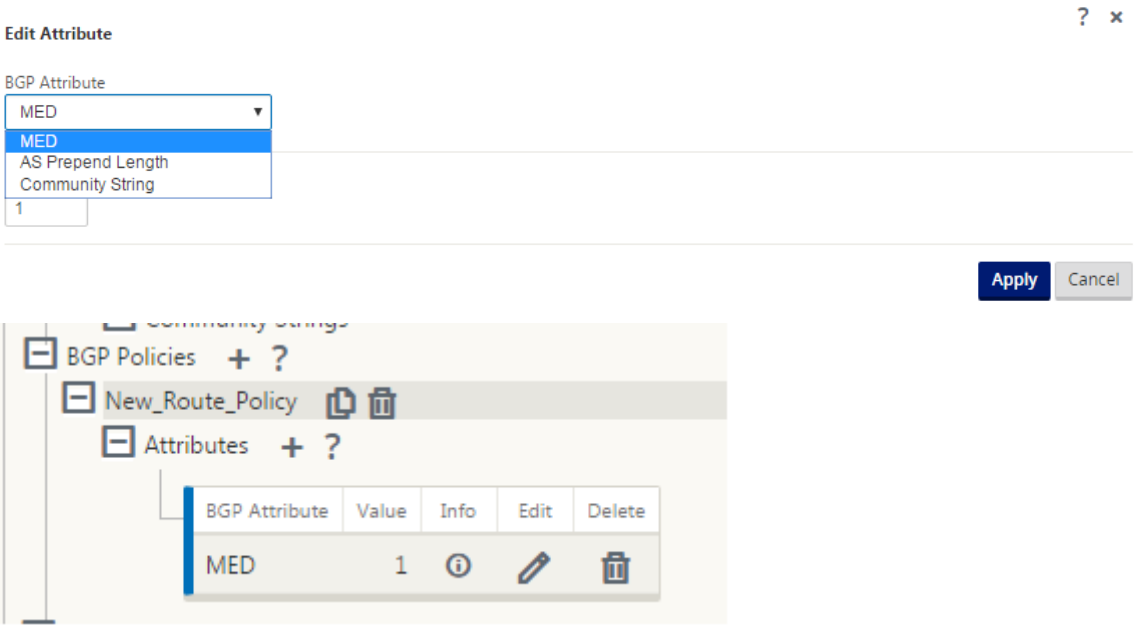
字符串 来配置每个社区字符串。对于手动配置，您可以输入一个系统号码和社区。您可以选择 插入/删除 标记与社区字符串的路由，或者从从对等方接收的路由中删除社区字符串。



4. 通过扩展 BGP 策略来配置 **BGP** 策略。将 BGP 属性添加到 新建路径策略。



5. 单击属 性 旁边的 **+** 符号以 编辑 BGP 属性。此时将显示 编辑属性 窗口。从下拉菜单中选择所需的 BGP 属性。根据您的选择，输入 **MED**、前缀长度或社区字符串的所需值。单击应用。



> 注意
>
> 任何策略只能有一个属性匹配项，并且不能多次出现同一属性。您不能有 2 MED 或 2 作为路径前缀。它可以有 MED/AS-PATH 前缀/社区字符串或组合。

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

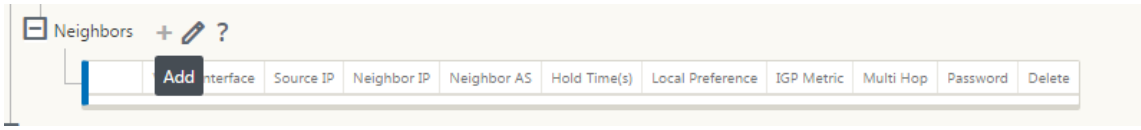
使用此选项，您可以添加网络对象并为该网络对象添加配置的 BGP 策略。这类似于创建路径映射和 ACL 以匹配特定路径以及为该邻居配置 BGP 属性。您可以指定方向以指示此策略是否适用于传入或传出的路由。

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。

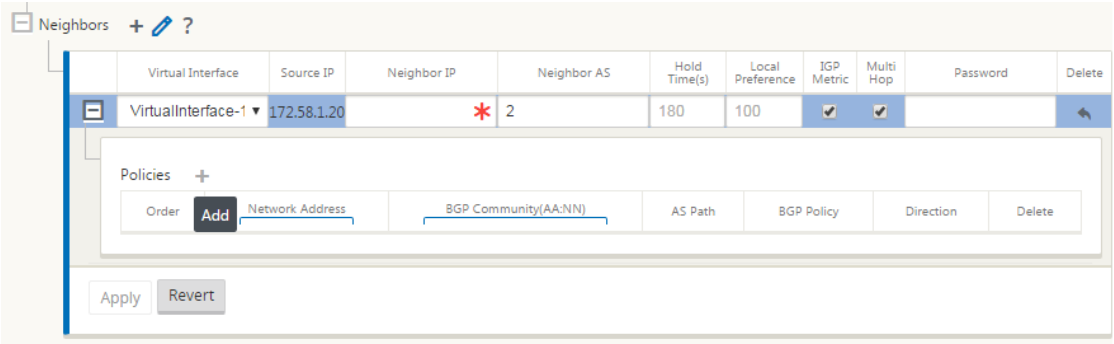
您可以根据网络地址（目标地址）、作为路径、社区字符串匹配路由，并分配策略并选择要应用的策略的方向。

要配置邻居，请执行以下操作：

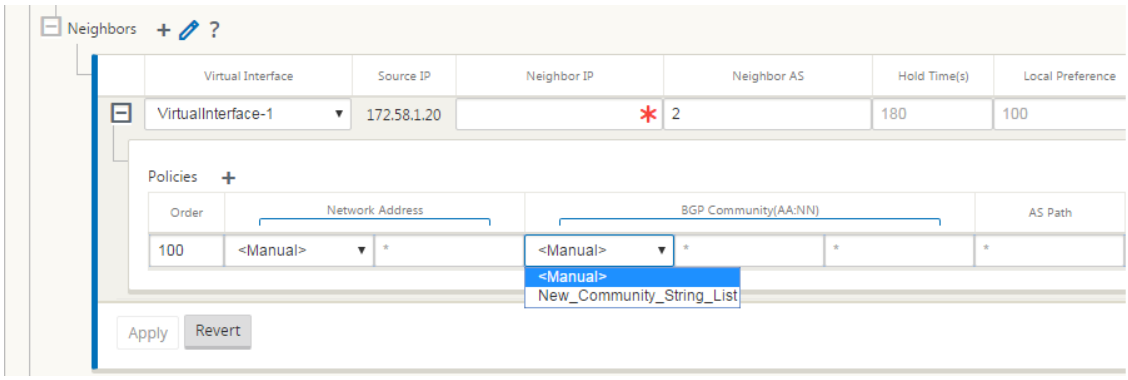
1. 通过单击 添加 来配置邻居，如下所示。

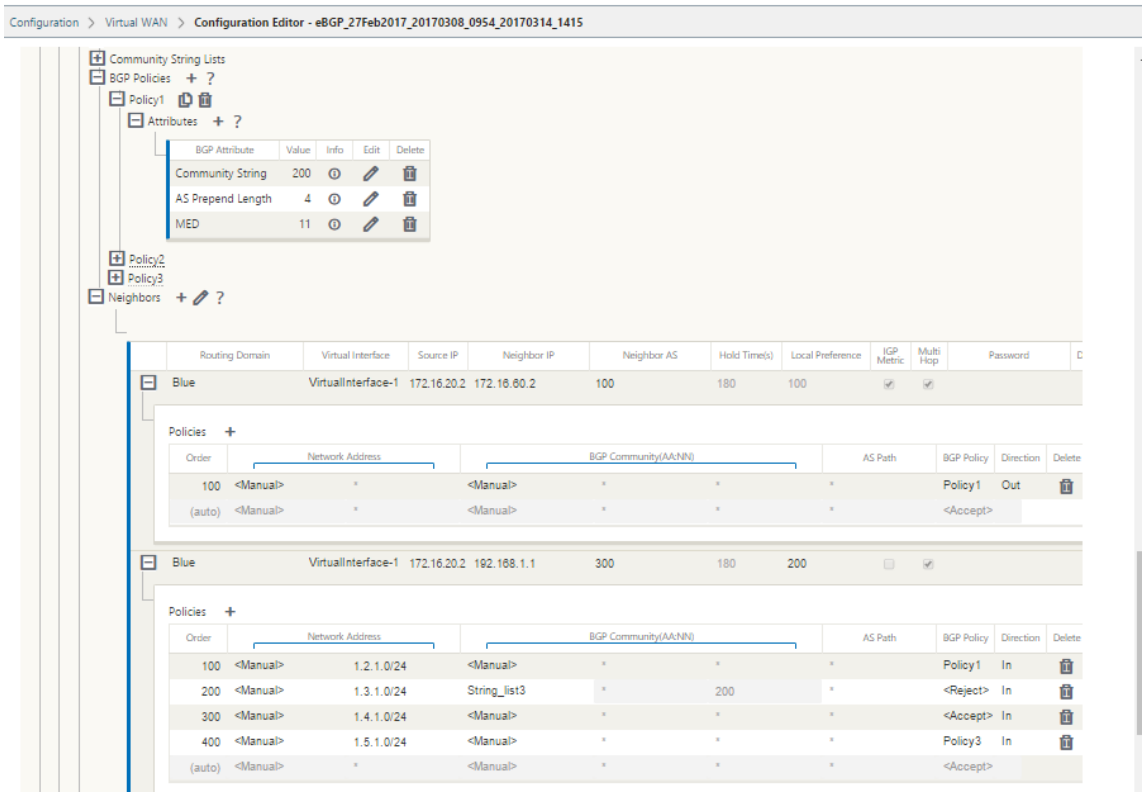


2. 单击 **+** 符号。选择一个 虚拟接口。输入 邻居 **IP** 地址。



3. 添加策略。根据需要选择 网络地址、**BGP** 社区和 **AS** 路径详细信息。单击应用。





4. 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。

您可以启用调试日志记录并从 监视器 > 路由 协议 页查看路由 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_ 诊 tics.log* 中捕获，可以从路由协议的监视中查看。

BGP 软重新配置

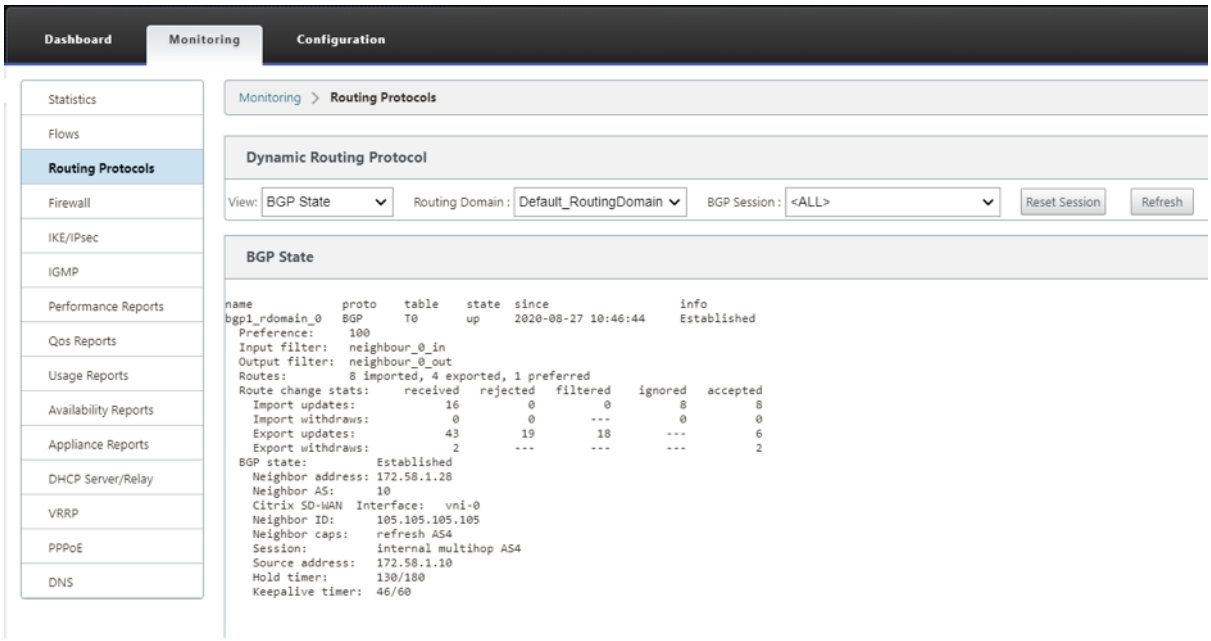
BGP 对等方的路由策略包括可能影响入站或出站路由表更新的路由映射、通讯组列表、前缀列表和筛选列表等配置。当路由策略发生更改时，必须清除或重置 BGP 会话，以使新策略生效。

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。

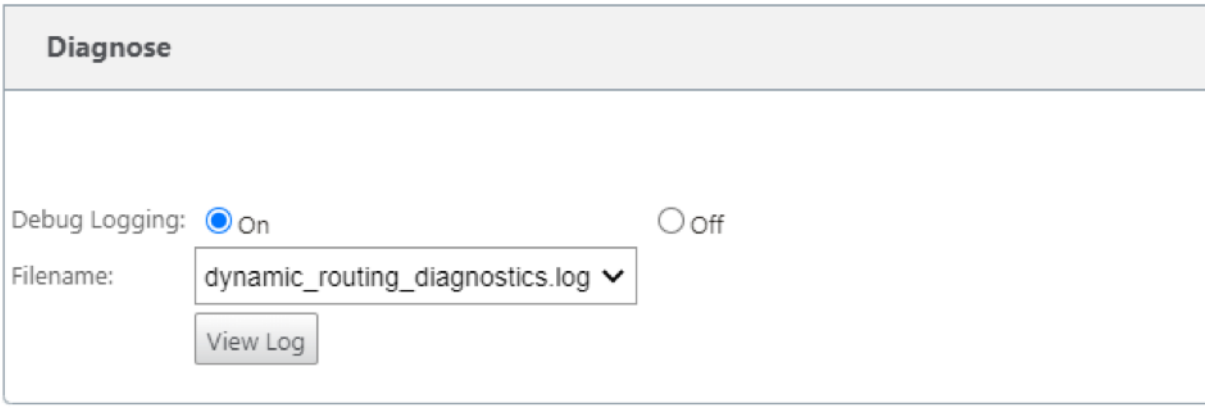
BGP 软重置增强功能为不依赖于存储的路由表更新信息的入站 BGP 路由表更新的动态软重置提供了自动支持。

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

June 22, 2021

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。

限制：

- 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

June 22, 2021

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（仅可用互联网）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。

申请路线

June 22, 2021

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。

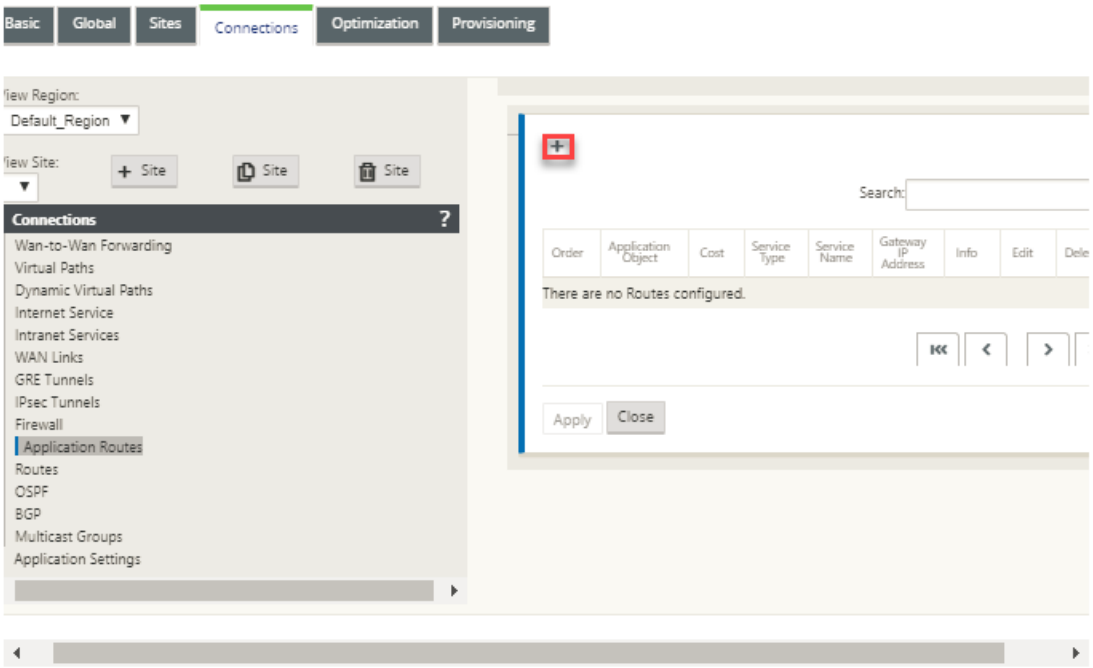
Citrix SD-WAN 允许您定义以下服务的应用程序路由：

- 虚拟路径：此服务管理跨虚拟路径的流量。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。互联网流量没有封装。当发生拥塞时，SD-WAN 通过相对于虚拟路径和 Intranet 流量的速率限制互联网流量来主动管理带宽。
- **Intranet**：此服务管理尚未定义为跨虚拟路径传输的企业 Intranet 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：此服务管理站点与其他服务不匹配的本地流量。SD-WAN 忽略来源和发往本地路由的流量。
- **GRE** 隧道：此服务管理发往 GRE 隧道的 IP 流量，并与站点配置的 LAN GRE 隧道匹配。GRE 隧道功能使您能够配置 SD-WAN 设备以终止局域网上的 GRE 隧道。对于具有服务类型 GRE 隧道的路由，Gateway 必须位于本地 GRE 隧道的隧道子网之一。
- **LAN IPSec** 隧道：此服务管理发往 LAN IPsec 隧道的 IP 流量，并与站点配置的 LAN IPsec 隧道匹配。通过 LAN IPsec 隧道功能，您可以将 SD-WAN 设备配置为终止局域网或 WAN 端的 IPsec 隧道。

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。

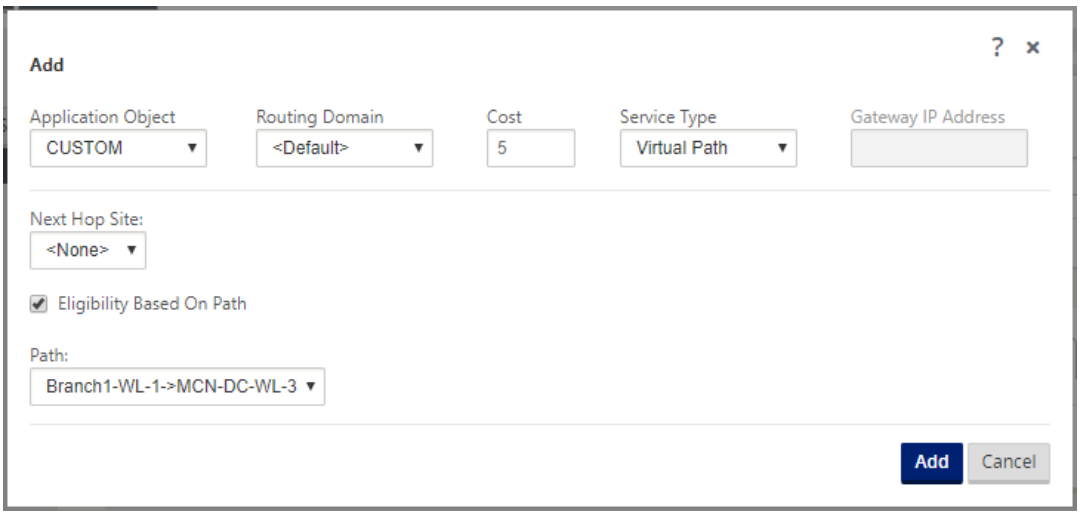
要配置应用程序路由，请执行以下操作：

1. 在配置编辑器中，导航到 连接 > 应用程序路由，然后单击 **+**。



2. 在 添 加 页面上，设置以下参数：

- 应用程序对象：要引导的应用程序对象。此处列出了您创建的应用程序对象。有关详细信息，请参阅应用分类 主题中的 应用程序对象 部分。



- 路由域：要由应用程序路由使用的路由域。选择一个已配置的路由域。
- 成本：用于确定此路径的路径优先级的权重。成本较低的路径优先于成本较高的路径。这个范围是 1-65534。默认值为 5。
- 服务类型：选择以下服务之一。这将应用程序映射到服务。
- 虚拟路径：将应用程序流量标识为虚拟路径流量，并根据虚拟路径规则匹配虚拟路径。在“下一跳站点”字段中，输入虚拟路径数据包定向到的下一跳远程站点。

> 注意
>
> 触及虚拟路径应用程序路由的任何流都不会超过动态虚拟路径。

- **Internet**：将应用程序流量标识为 Internet 流量，并与 Internet 服务匹配。
- **Intranet**：将应用程序流量识别为 Intranet 流量，并根据 Intranet 规则匹配 Intranet 服务。在 **Intranet** 服务 字段中，选择要用于路由的 Intranet 服务。
- 本地：将应用程序流量标识为站点的本地流量并且不匹配任何服务。来源和发往本地路径的流量将 被忽略。

  > 注意
  >
  > 对于本地服务类型，完成 DPI 分类后，配置的 IP 路由将作出路由决策。

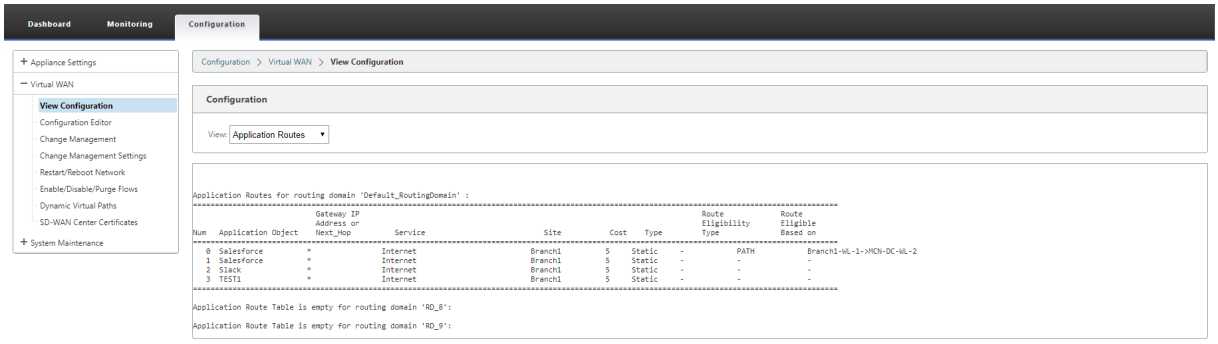
- **GRE** 隧道：确定应用程序流量为目的地 GRE 隧道，并匹配在现场配置的 LAN GRE 隧道. 在 网关 **IP** 地址字段中，输入必须位于 LAN GRE 隧道子网中的网关 IP 地址。选择 基于网关的资格 以允许路由在无法访问网关时不接收任何流量。
- 局域网 **IPsec** 隧道：将应用程序流量识别为目标到局域网 IPsec 隧道，并与站点中配置的 LAN IPsec 隧道匹配。在 **IPsec** 隧道 字段中，选择一个已配置的 IPsec 隧道。选择 基于隧道的资格，以便在隧道无法到达时使路径无法接收任何流量。

  > 注意
  >
  > 为自定义应用程序选择服务后，请勿对其进行更改。

- 基于路径的资格：选择该选项可在指定路径停止时启用路径不接收流量。在 路径 字段中，指定用于确定路径资格的路径。

3. 单击应用。

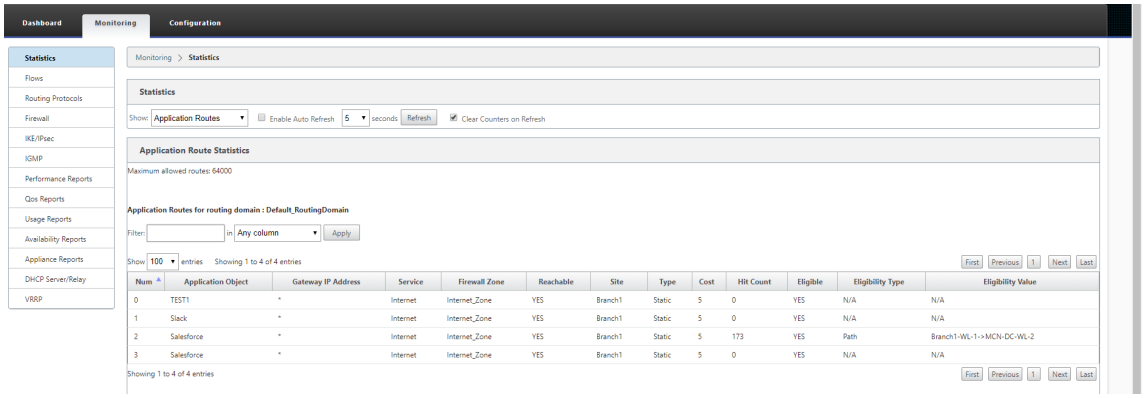
查看 SD-WAN 设备上配置的应用程序路由。在 SD-WAN GUI 中，导航到 配置 > 虚拟 **WAN** > 查看配置。从 查看 下拉菜单中选择 应用程序路由。



要查看应用程序路由的统计数据：

1. 在 SD-WAN GUI 中，导航到 监视 > 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：使用 GRE 隧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：路径的优先级。
- 单击计数：使用应用程序路由来引导流量的次数。
- 符合条件：申请路线是否符合发送流量的条件。
- 资格类型：应用于此路径的路径资格条件类型。资格类型可以是路径、网关或隧道。
- 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

June 22, 2021

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。

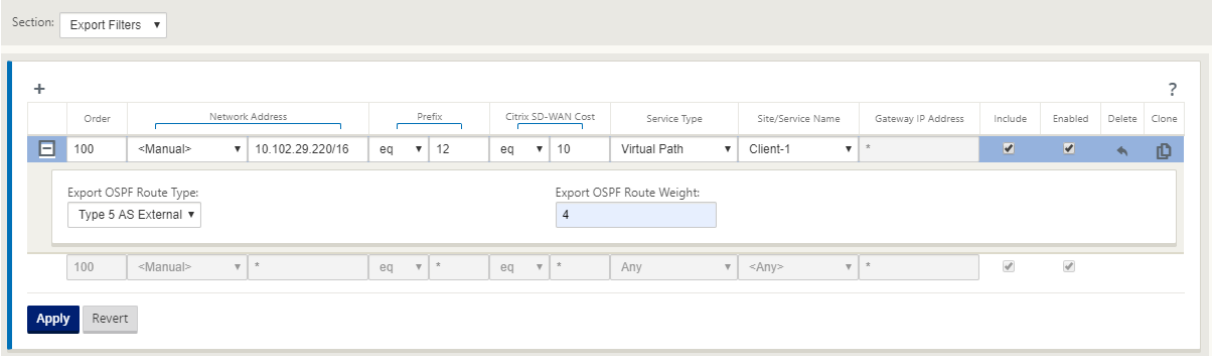
- 导出 筛选器 用于包含 或 排除 使用 OSPF 和 BGP 协议基于 特定 匹配的 播 发路由 标准。导出筛选器规则是在通过动态路由协议公告 SD-WAN 路由时必须满足的规则。默认情况下，所有路由都会公布给同级。
- 导入过滤器用于接受或不接受基于特定匹配条件使用 OSPF 和 BGP 邻居接收的路由。导入筛选器规则是在将动态路由导入 SD-WAN 路由数据库之前必须满足的规则。默认情况下不导入任何路由。

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。

配置导出筛选器

在 配置编辑器中，导航到 连接 **>** 片段 **>** 站点 **>** **OSPF** 或 **BGP** **>** 导出筛选器。



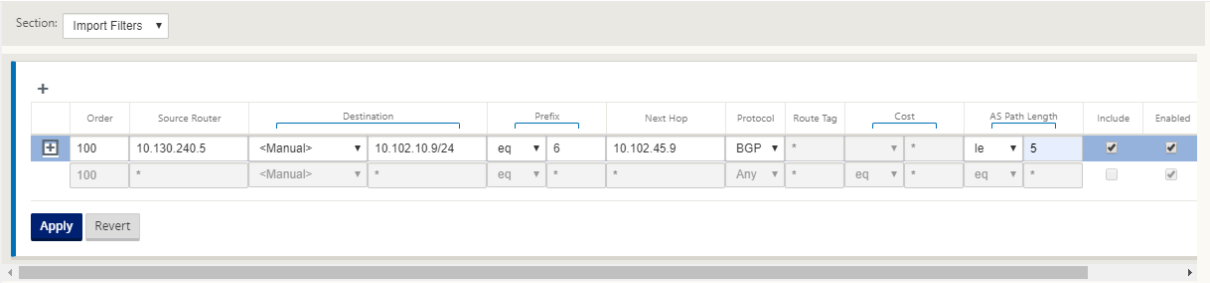
使用以下条件构建要创建的每个导出筛选器。

字段标准	说明	值
命令	筛选器的优先级顺序。路由匹配的第一个过滤器应用于该路由	100, 200, 300, 400, 500, 600
网络地址	输入描述路由网络的已配置网络对象的 **IP** 地址 和子网掩码	• IP 地址
前缀	要按前缀匹配路由，请从菜单中选择匹配谓词，然后在相邻字段中输入路由前缀	• eq: 等于,- LT: 小于,- LE: 小于或等于,- GT: 大于,- ge: 大于或等于

字段标准	说明	值
Citrix SD-WAN 成本	用于缩小导出路由选择范围的方法（谓词）和 SD-WAN 路由成本	数值
服务类型	从 Citrix SD-WAN 服务列表中选择分配给匹配路由的服务类型	任何、本地、虚拟路径、互联网、内联网、局域网 GRE 隧道、局域网 IPsec 隧道
站点/服务名称	对于 Intranet、LAN GRE 隧道和 LAN IPsec 隧道，请指定要使用的已配置的服务类型的名称	文本字符串
网关 IP 地址	如果您选择 LAN GRE 隧道作为服务类型，请输入隧道的 Gateway IP	IP 地址
包括	选中 包括与此筛选器匹配的路径 复选框。否则匹配的路由将被忽略	无
已启用	选中 启用此筛选器 复选框。否则，过滤器将被忽略	无
删除	选择删除图标以删除此过滤器。	无
克隆	单击克隆图标以复制现有筛选器	无

配置导入筛选器

在 配置编辑器中，导航到 连接 **>** 片段 **>** 站点 **> OSPF** 或 **BGP >** 导入筛选器。



使用以下条件构建要创建的每个导出筛选器。

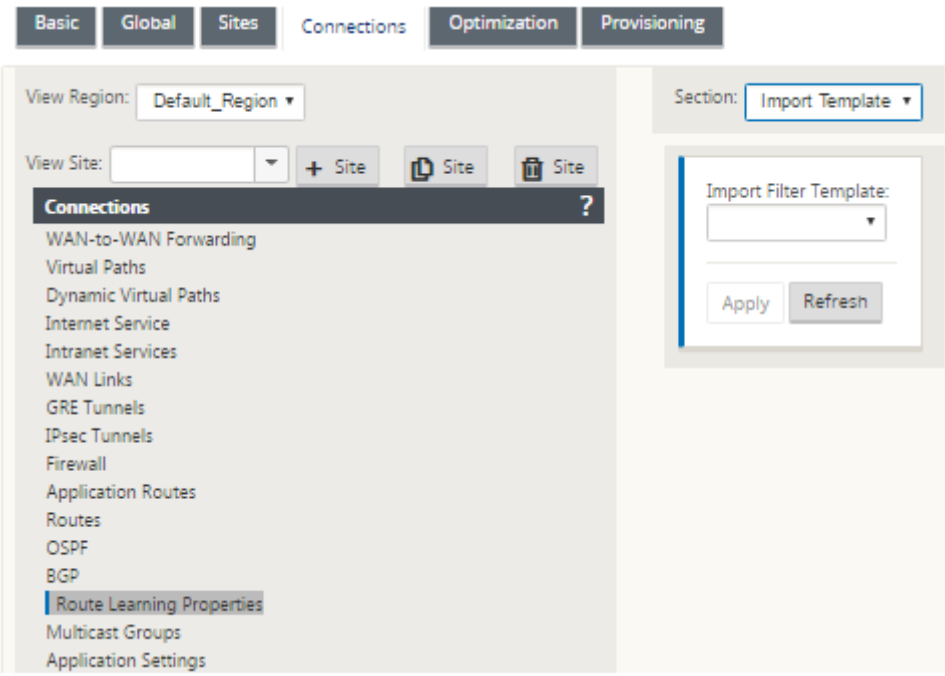
字段标准	说明	值
命令	筛选器的优先级顺序。路由匹配的第一个过滤器应用于该路由	100, 200, 300, 400, 500, 600
源路由器	源路由器的 IP 地址，只适用于 iBGP	• IP 地址
目标	路由目标的 IP 地址和子网掩码	• IP 地址

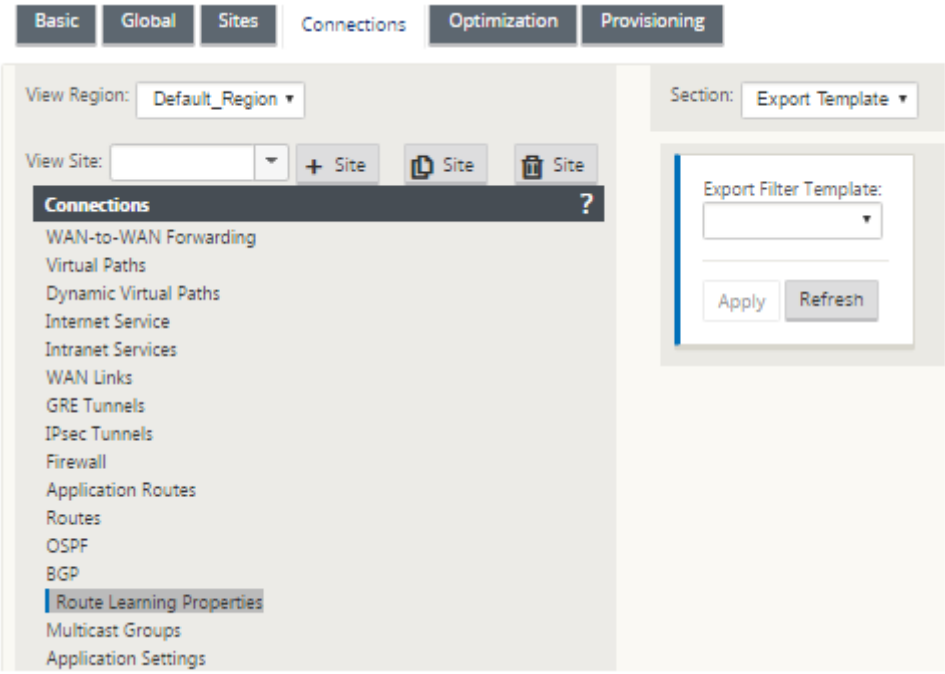
字段标准	说明	值
前缀	要按前缀匹配路由，请从菜单中选择匹配谓词，然后在相邻字段中输入路由前缀	• eq: 等于,- LT: 小于,- LE: 小于或等于,- GT: 大于,- ge: 大于或等于
下一个跳	下一个跃点的 IP 地址	• IP 地址
协议	用于学习路由的路由协议	OSPF 或 BGP
路由标签	筛选器匹配的 OSPF 路由标记。OSPF 路由标签在 OSPF 和其他协议之间相互重新分配过程中防止路由循环	数值
成本	用于匹配导入 OSPF 路由的路由成本	数值
作为路径长度	用于匹配导入 BGP 路由的 AS 路径长度	数值
包括	选中 包括与此筛选器匹配的路径 复选框。否则匹配的路由将被忽略	无
已启用	选中 启用此筛选器 复选框。否则，过滤器将被忽略	无
删除	单击删除图标以删除此过滤器。	无
克隆	单击克隆图标以复制现有筛选器	无

配置路由策略筛选器模板

您可以使用各种筛选规则创建多个导入或导出筛选器模板，并在每个站点关联模板。

用户创建的站点级导入/导出筛选器规则具有更高的优先级。模板规则与 连接 的 路径学习 部分中的站点关联时遵循用户创建的规则。





路线汇总

June 22, 2021

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。

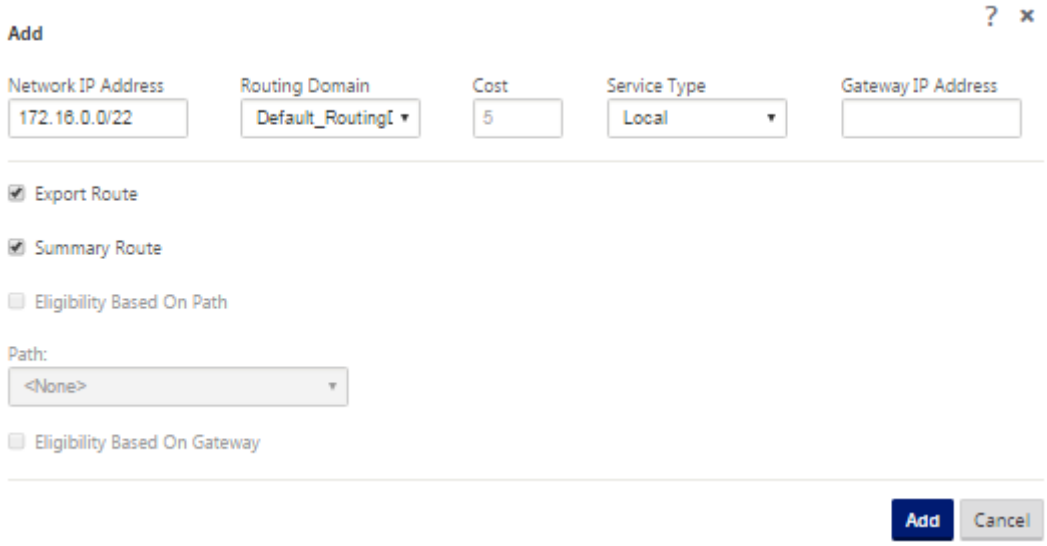
要为本地子网配置摘要路由，请执行以下操作：

1. 在配置编辑器中，导航到 连接 > 路由，然后单击 **+** 以 添加路由。
2. 在 添加工艺路线 页上，设置以下参数，然后单击 添加。

- 网络 **IP** 地址：计算出的摘要路由 IP 地址。
- 成本：用于确定此路径的路径优先级的权重。成本较低的路径优先于成本较高的路径。这个范围是 1-15。默认值为 5。
- 路由域：路由协议提供单点管理管理公司网络、分支办公室网络或数据中心网络。
- 服务类型：选择本地服务类型。

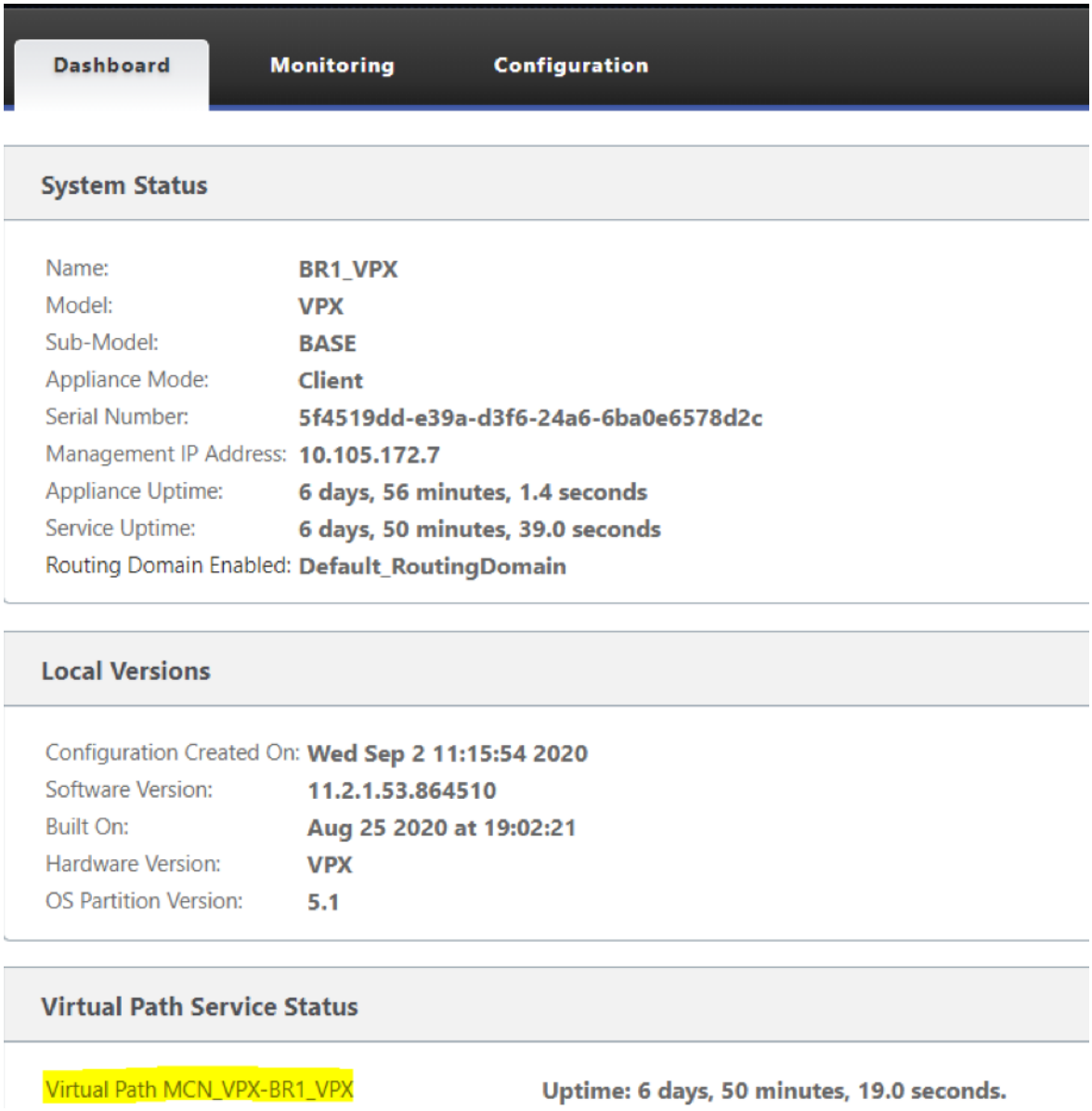
> 注意
>
> 您只能为汇总路径选择 本地 和 丢弃 服务类型。

- 网关 **IP** 地址：此路由的网关 IP 地址。
- 导出路径：将路径导出到其他连接站点。
- 摘要路由：将路由作为单个摘要路由通告到其他连接的设备，而不是所有其他匹配的子网。



故障排除

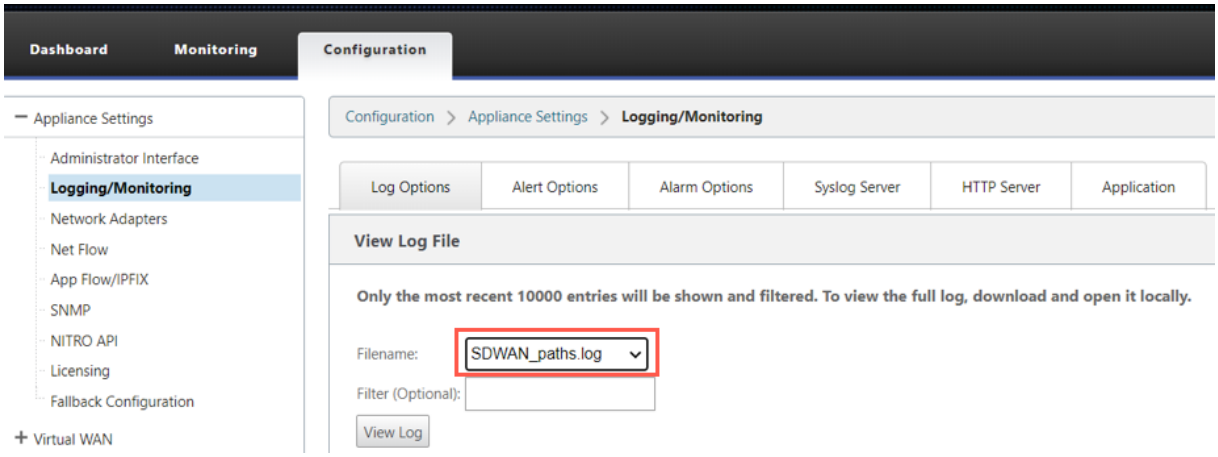
MCN 上配置的汇总路由通过虚拟路径发送到分支机构。如果您在分支的路由表中没有看到虚拟路径详细信息，请检查 Branch 控制面板。仪表板显示 MCN 和 Branch 之间的虚拟路径的状态。



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

June 22, 2021

协议首选项是 Citrix SD-WAN 特定功能，类似于路由器管理距离。

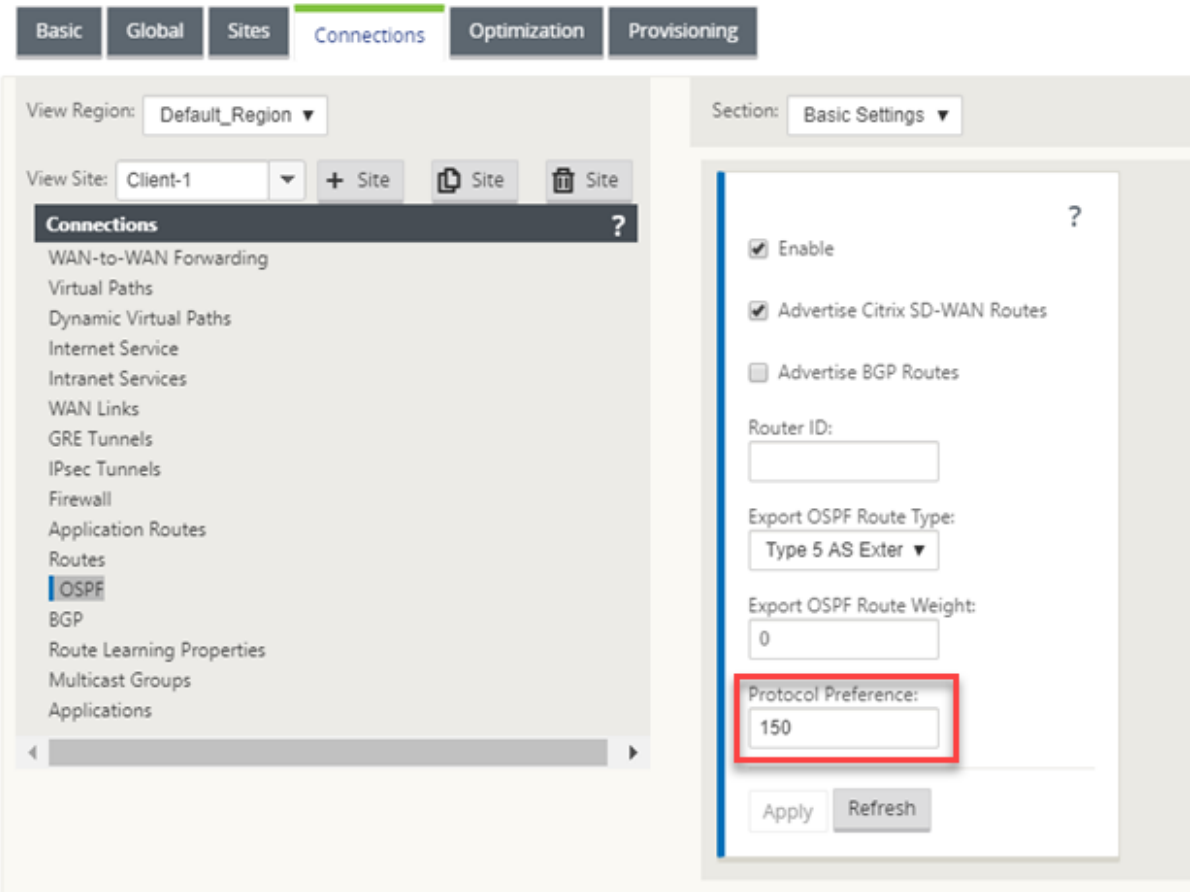
Citrix SD-WAN 同时通过虚拟路径、OSPF 协议或 BGP 协议学习路由前缀时，它将遵循以下默认首选项顺序。

- OSPF -150
- BGP - 100
- 南湾-250

首选顺序最高的协议是最优选的。使用具有最高协议首选项值的协议的路由

在配置 BGP 或 OSPF 协议时，您还可以通过设置协议首选项值来选择在 OSPF 协议上使用 BGP 协议。您可以在 100—200 范围内指定首选项。

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

June 22, 2021

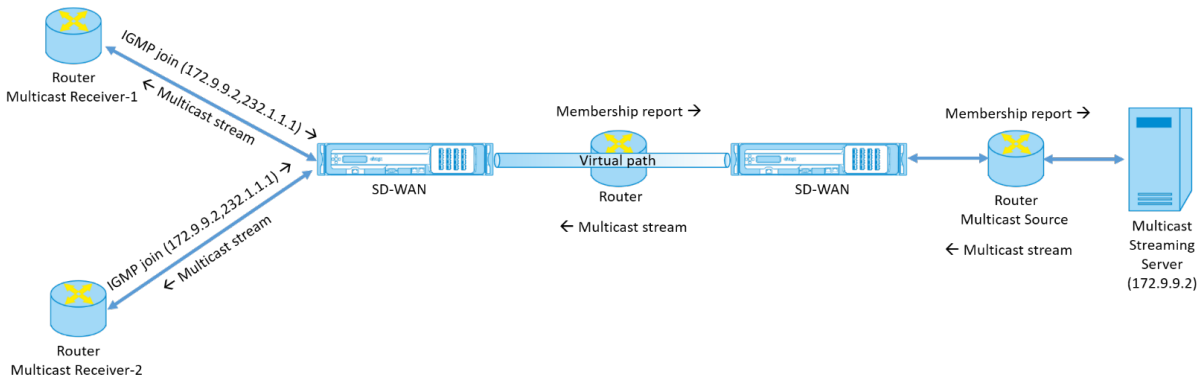
组播路由实现了一对多流量的高效分配。多播源，将单个流中的多播流量发送到多播组。多播组包含使用 IGMP 协议进行多播通信的主机和相邻路由器等接收器。IP 语音、视频点播、IP 电视和视频会议是使用多播路由的一些常见技术。在 Citrix SD-WAN 设备上启用多播路由时，该设备将充当多播路由器。

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。

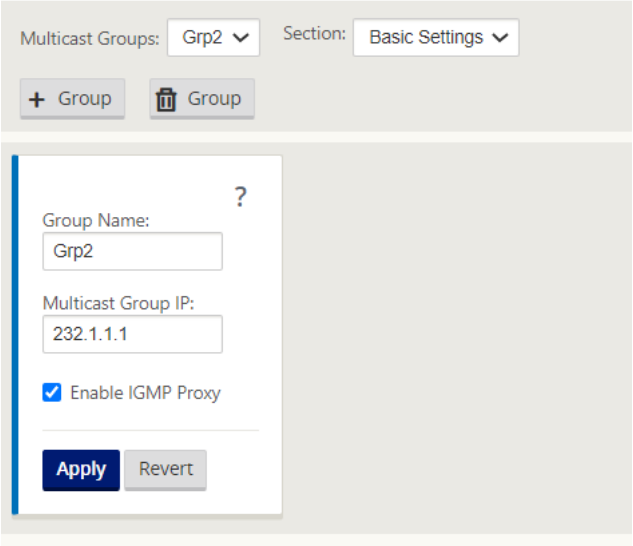
控制通道流量和多播流经过分支机构和数据中心之间已建立的虚拟路径。Citrix SD-WAN 叠加路径可确保和隔离多播流量免受 WAN 降级或链路变化的影响。

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。

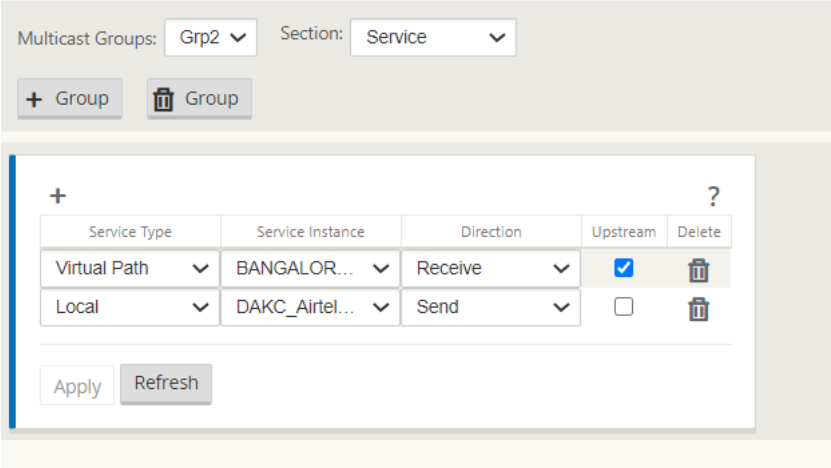
1. 创建多播组-为多播组提供名称和 IP 地址。对于源特定的多播，组播组 IP 必须在 232.0.0.0/8 范围内。
2. 启用 IGMP 代理—您可以将 Citrix SD-WAN 设备配置为 IGMP 代理，以便传输用于多播路由的 IGMP 控制通道信息。要进行单源多播，需要 IGMP V3。
3. 定义上游和下游服务-上游接口使 IGMP 代理能够连接到更接近实际多播源的 SD-WAN 设备，以流式传输流量。下游接口使 IGMP 代理能够连接到远离流通信量的实际多播源的主机。
   源设备和目标设备的上游和下游服务不同

要在 Citrix SD-WAN 设备上配置多播，请导航到 连接 > 多播组。通过为多播组提供名称和 IP 地址来创建多播组。单击启用 **IGMP** 代理。

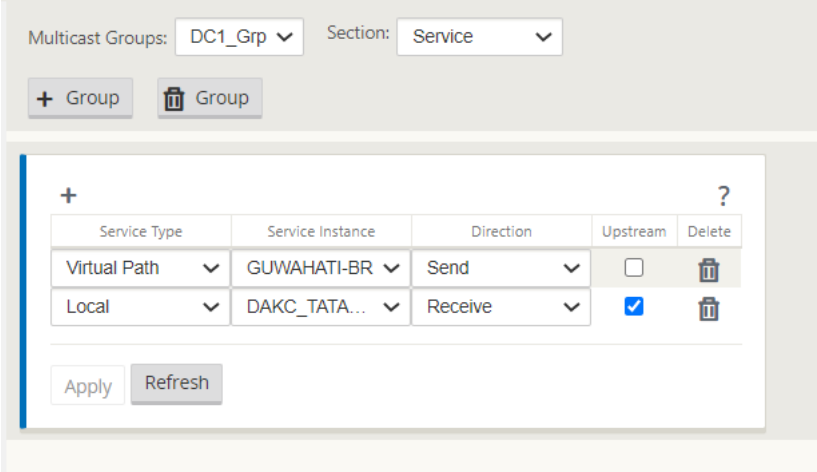


配置分支机构和数据中心设备的上游和下游路径。

对于靠近多播接收器（分支）的设备，设备会在虚拟路径接口上接收组播流量，并将本地接口上的流量发送到接收方。



对于靠近多播源（数据中心）的设备，设备将在本地接口上接收组播流量，然后在虚拟路径接口上发送流量。

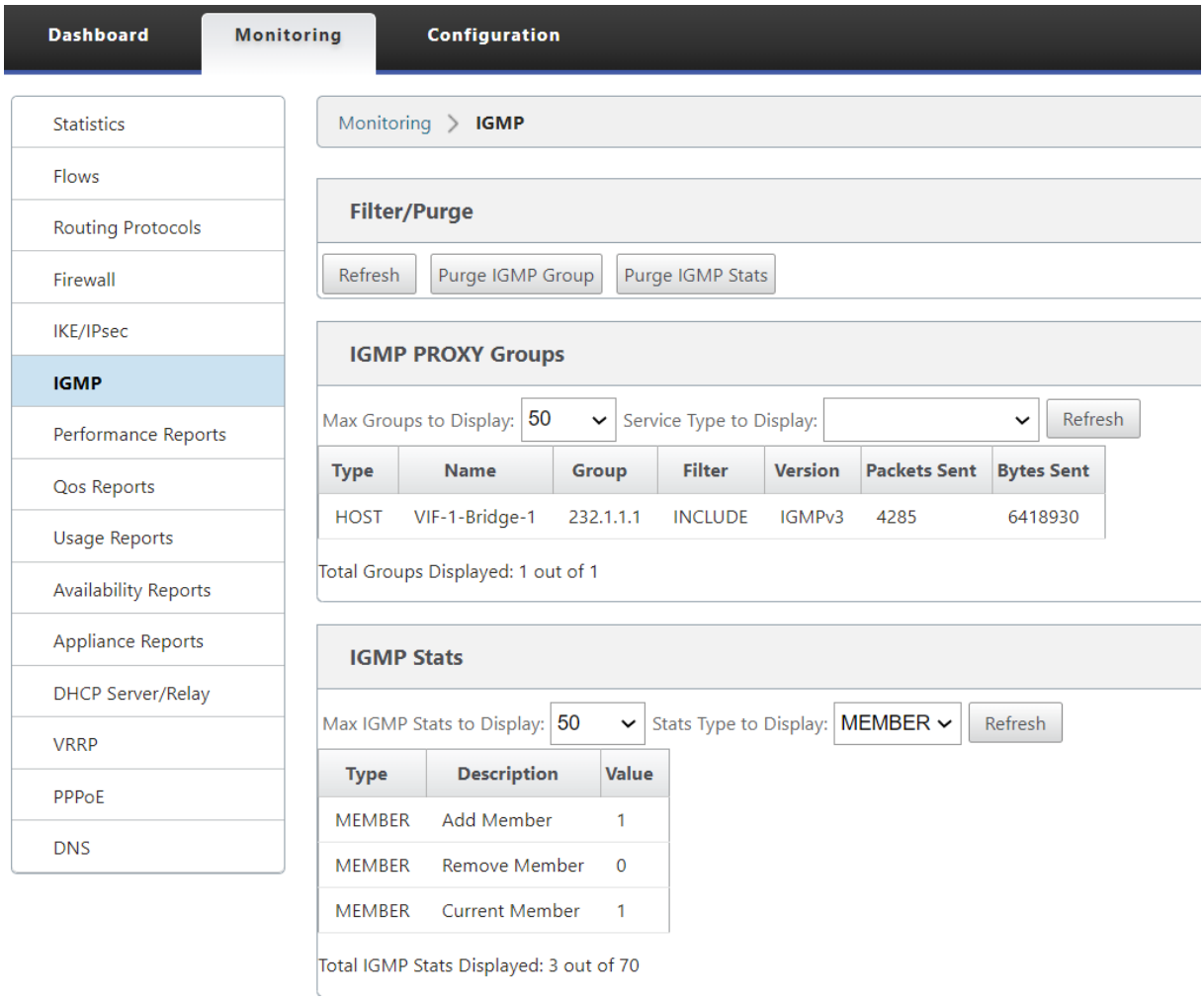


监视

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。

下图显示启动了 IGMP 版本 3 联接，并使用过滤器类型包括特定的源地址。您还可以查看 IGMP 成员统计信息。



配置虚拟路径路由成本

June 22, 2021

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。

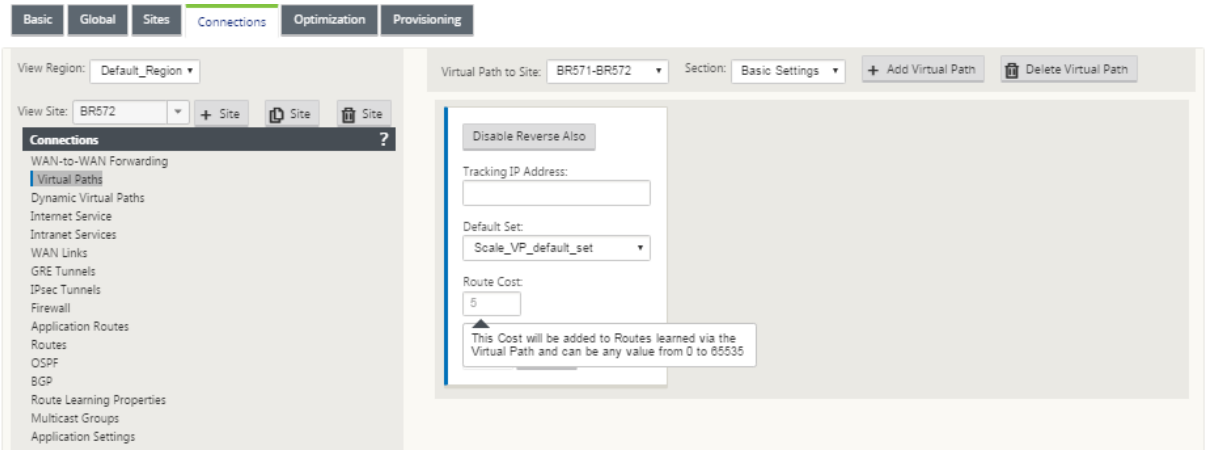
此功能会使 WAN 到 WAN 转发成本失效或删除。

- 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。

如何配置虚拟路径路由成本

您可以在 SD-WAN GUI 中在 连接 > 查看区域 **>** 查看站点 **>** 虚拟路径 **>** 基本设置下配置虚拟路径路由。所有路由都使用基本 Citrix SD-WAN 成本 + VP 路由成本安装，以影响跨多个虚拟路径的路由成本。



使用案例：

例如，存在子网 172.16.2.0/24 和 172.16.3.0/24。假定有两个数据中心 DC1 和 DC2 使用这两个子网将流量传输到 SD-WAN。如果使用默认的虚拟路径路由开销，则无法影响路由，因为它取决于首先安装的路由，可以是 DC2 第一个，也可以是下一个 DC1。

使用虚拟路径，您可以特别影响 DC2 虚拟路径，使其具有较高的虚拟路径路由开销（例如 10），而 DC1 的默认 VP 路由开销为 5。此操作有助于首先安装 DC1 和 DC2 的路由。

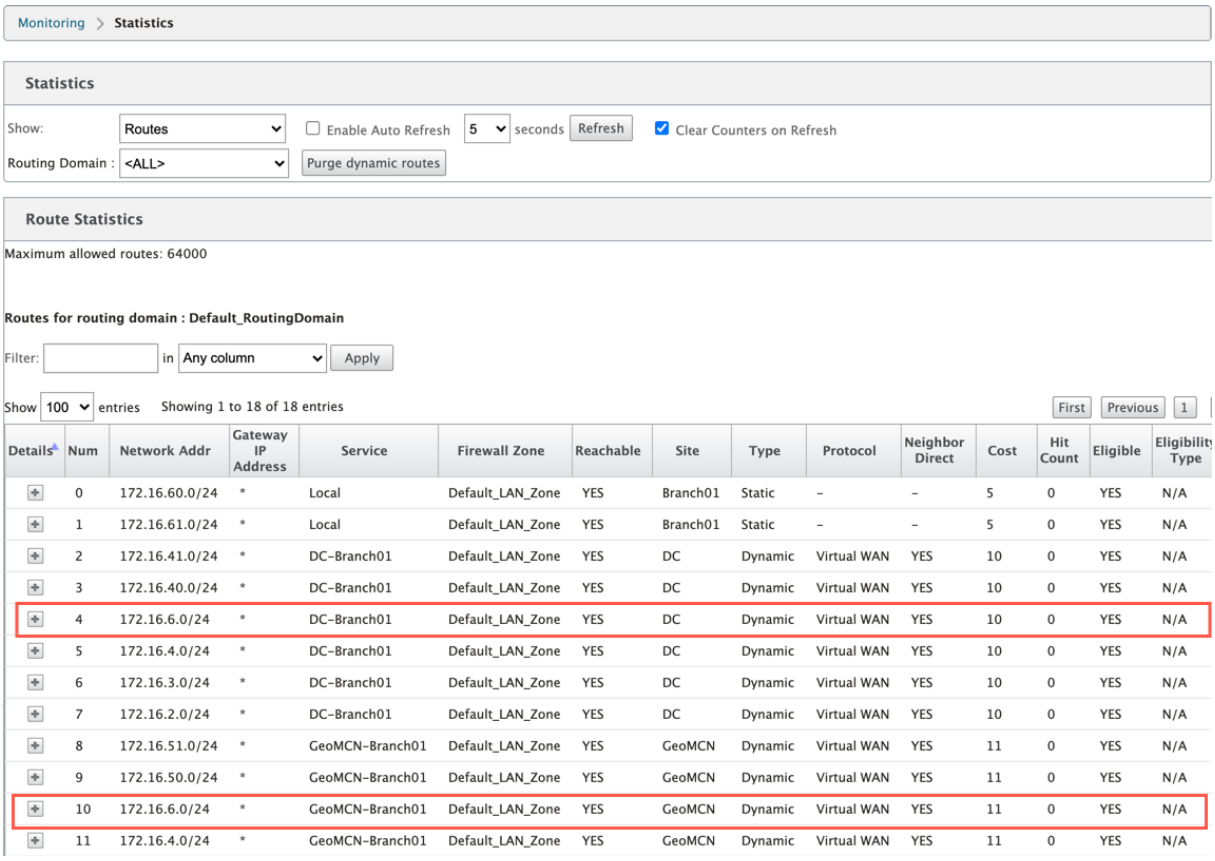
您可以有四条路由路线，两条路由到 172.16.2.0/24；一条通过 DC1 以较低的成本路由，然后通过 DC2 以较高的成本路由，另外两条针对 172.16.3.0/24 路由。

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

June 22, 2021

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。

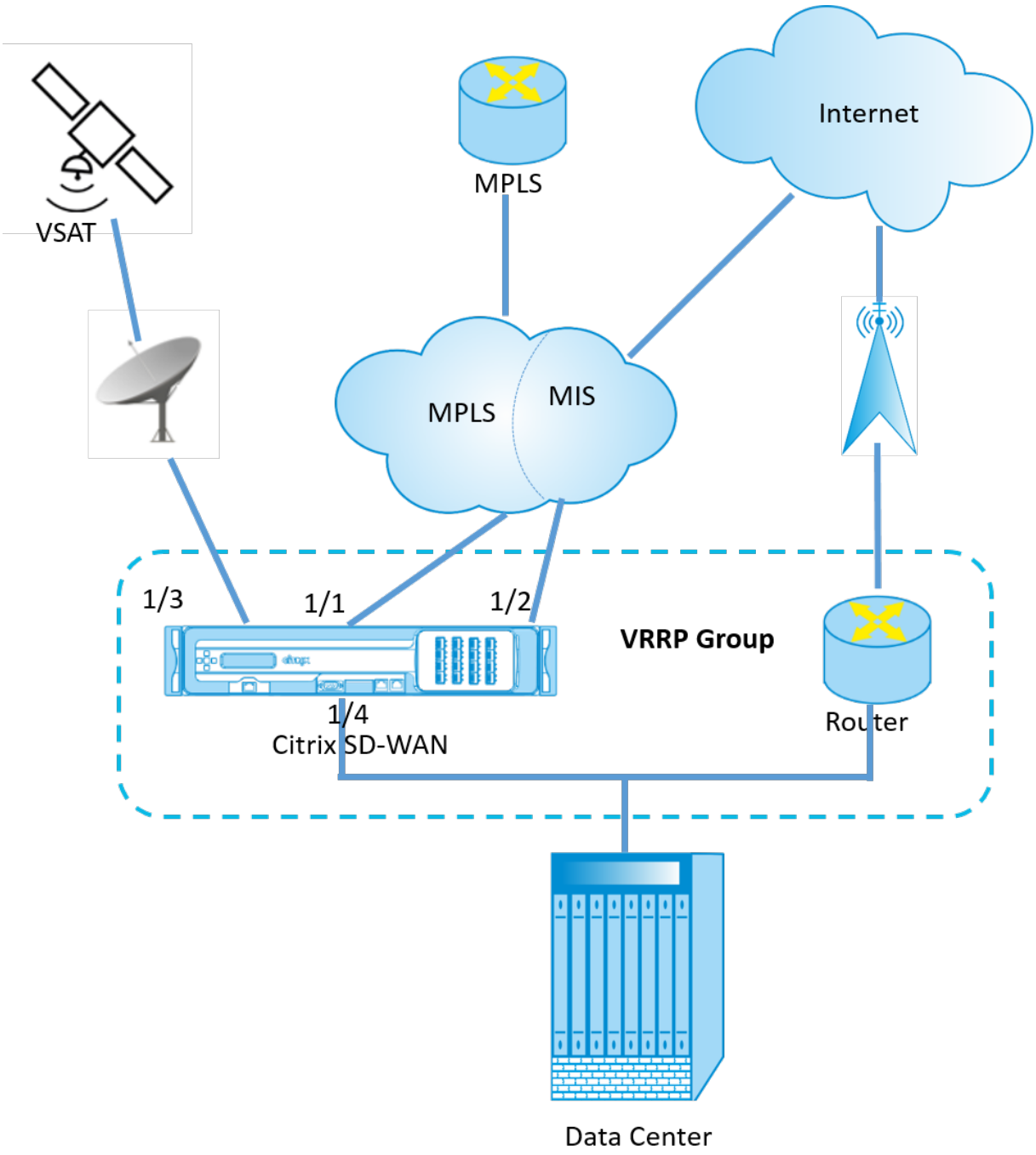
如果主路由器/主路由器出现故障，备份路由器会自动接管。在 VRRP 设置中，主路由器向备份路由器发送称为播发的 VRP 数据包。如果主路由器停止发送播发，备份路由器将设置间隔计时器。如果在此保留期内未收到播发，备份路由器将启动故障转移例程。

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。

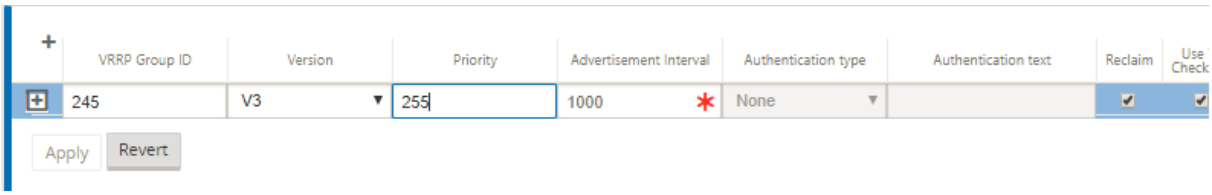
Citrix SD-WAN 版本 10.1 支持 VRP 版本 2 和版本 3 与任何第三方路由器互操作。SD-WAN 设备充当主路由器，并将流量引导到站点之间使用虚拟路径服务。可以将虚拟接口 IP 配置为 VRRP IP，并通过手动将优先级设置为高于对等路由器的值，来将 SD-WAN 设备配置为 VRRP 主服务器。您可以配置播发间隔和抢占选项。

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。



要配置 VRRP 实例，请执行以下操作：

1. 在配置编辑器中，导航到 站点 > 站点名称 > **VRRP** ，然后单击 **+**。



1. 配置 VRRP 实例。输入以下字段的值：

- **VRRP 组 ID**：VRRP 组 ID。组 ID 的值范围必须为 1—255。备份路由器上也必须配置相同的组 ID。

> 注意
>
> 目前，您最多只能配置四个组。

- 版本：VRRP 协议版本。可以在 VRRP 协议 V2 和 V3 之间进行选择。
- 优先级： Citrix SD-WAN 设备对于 VRRP 组的优先级。优先级范围为 1–254。将此值设置为最大值 (254)，使 SD-WAN 设备成为主设备。

> 注意
>
> 如果路由器是 VRRP IP 地址的所有者，则默认情况下，优先级设置为 255。

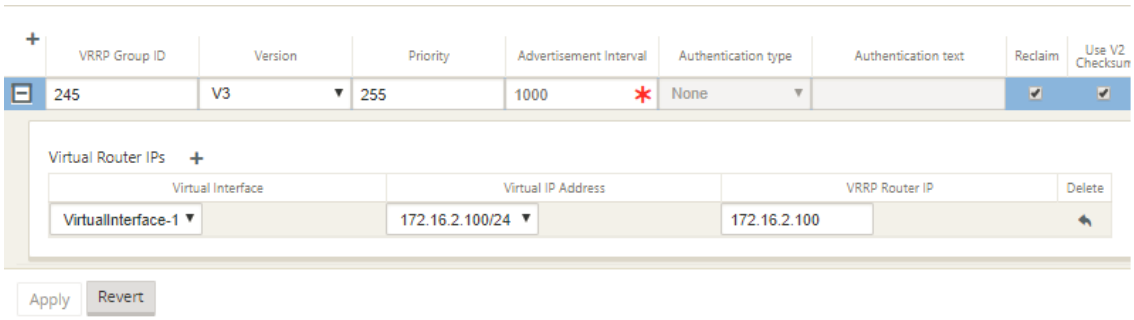
- 公告 **Interval**：以毫秒为单位的频率，当 SD-WAN 设备是主设备时发送 VRP 公告。默认公告时间间隔为 1 秒。
- 身份验证类型：您可以选择 纯文本 输入身份验证字符串。身份验证字符串以纯文本格式发送，在 VRRP 公告中不进行任何加密。如果不希望设置身份验证，请选择无。
- 身份验证文本：要在 VRRP 播发中发送的身份验证字符串。如果身份验证类型为纯文本，则启用此选项。

> 注意
>
> 仅在 VRRPv2 中支持身份验证。

- 回收：当 SD-WAN 设备的优先级在 VRRP 组中最高时启用抢占。这在 VRRP 选举过程中使用。
- 使用 **V2** 校验和：为 VRRPv3 启用与第三方网络设备的兼容性。默认情况下，VRRPv3 使用 v3 校验和计算方法。某些第三方设备可能只支持 VRRPv2 校验和计算。在这种情况下，请启用此选项。

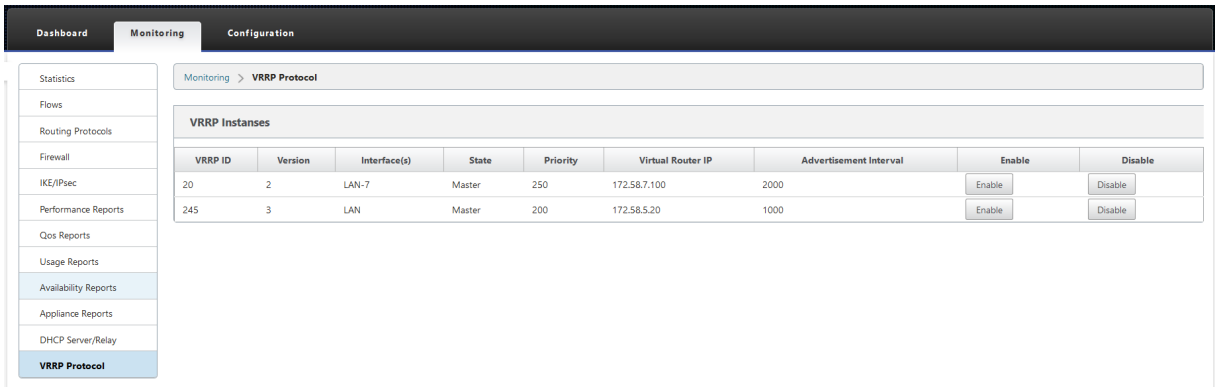
配置 VRRP IP 地址。输入以下字段的值，然后单击 应用。

- 虚拟接口: 用于 VRRP 的虚拟接口。选择一个已配置的虚拟接口。
- 虚拟 **IP** 地址：分配给虚拟接口的虚拟 IP 地址。为虚拟接口选择一个已配置的虚拟 IP 地址。
- **VRRP 路由器 IP**：VRRP 组的虚拟路由器 IP 地址。默认情况下，将 SD-WAN 设备的虚拟 IP 地址指定为虚拟路由器 IP 地址。



VRRP 统计数据

您可以在 监视 > VRRP 协议下查看 **VRP** 统计信息。



您可以查看以下统计数据：

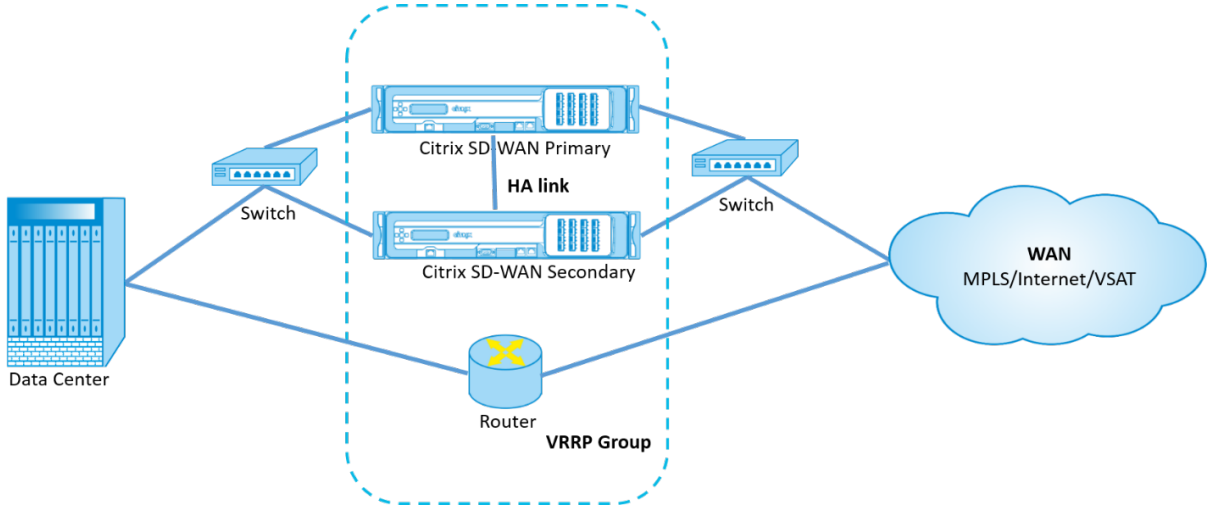
- **VRRP ID**： VRP 组 ID
- 版本： VRRP 协议版本。
- 接口：用于 VRRP 的虚拟接口。
- 状态： SD-WAN 设备的 VRP 状态。它指示设备是主设备还是备份。
- 优先级： VRRP 组的 SD-WAN 设备的优先级
- 虚拟路由器 **IP**： VRRP 组的虚拟路由器 IP 地址。
- 播发间隔： VRP 播发的频率。
- 启用：选择此选项可在 SD-WAN 设备上启用 VRRP 实例。
- 禁用：选择此选项可禁用 SD-WAN 设备上的 VRP 实例。

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更多信息，请参阅高可用性。

配置网络对象

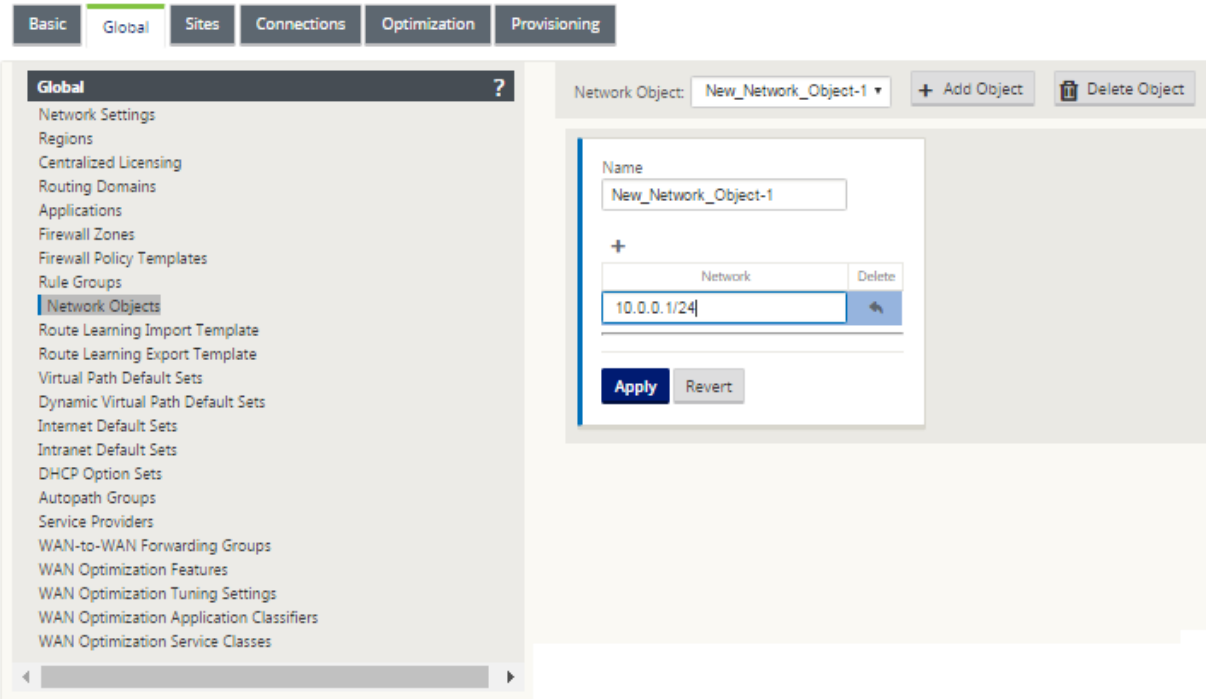
June 22, 2021

Citrix SD-WAN 引入了在配置编辑器的 全局 面板下添加网络对象的选项。您可以在定义路由筛选器时将多个子网组合在一起并引用单个网络对象，而不是为每个子网创建筛选器。

要配置网络对象，请执行以下操作：

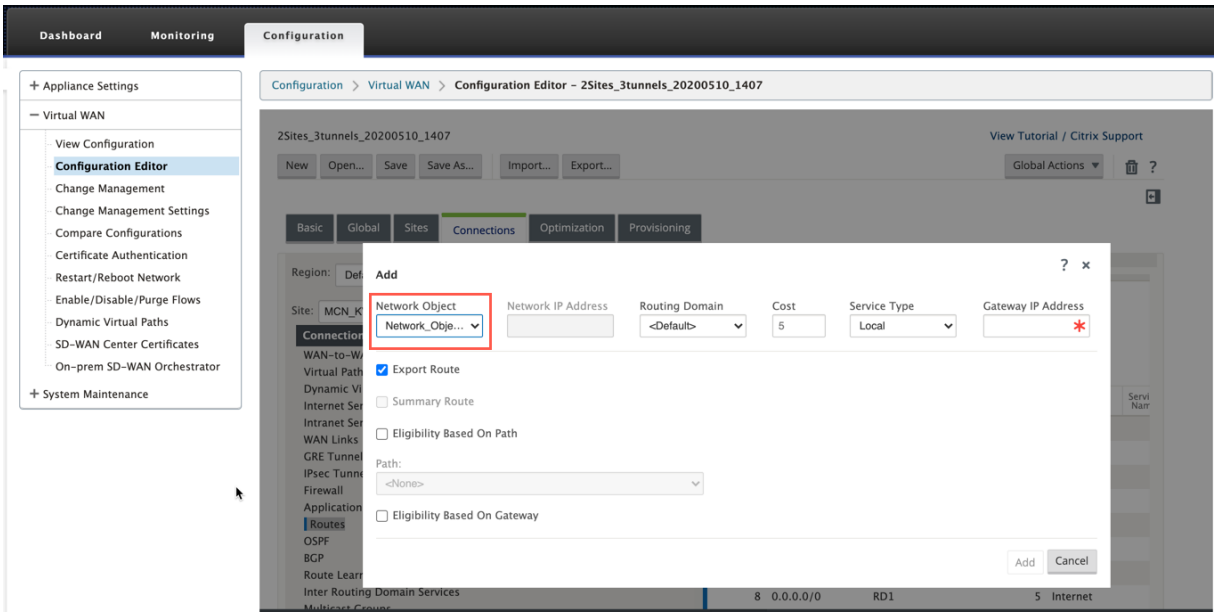
1. 在 配置编辑器中，导航到 全局 → 网络对象，单击 添加 **(+)**。
2. 单击网络下的 添加 **(+)**。
3. 输入新网络对象的 **IP** 地址和子 网。
4. 单击应用以保存设置。

要编辑网络对象的名称，请单击网络对象的名称，然后输入新名称。

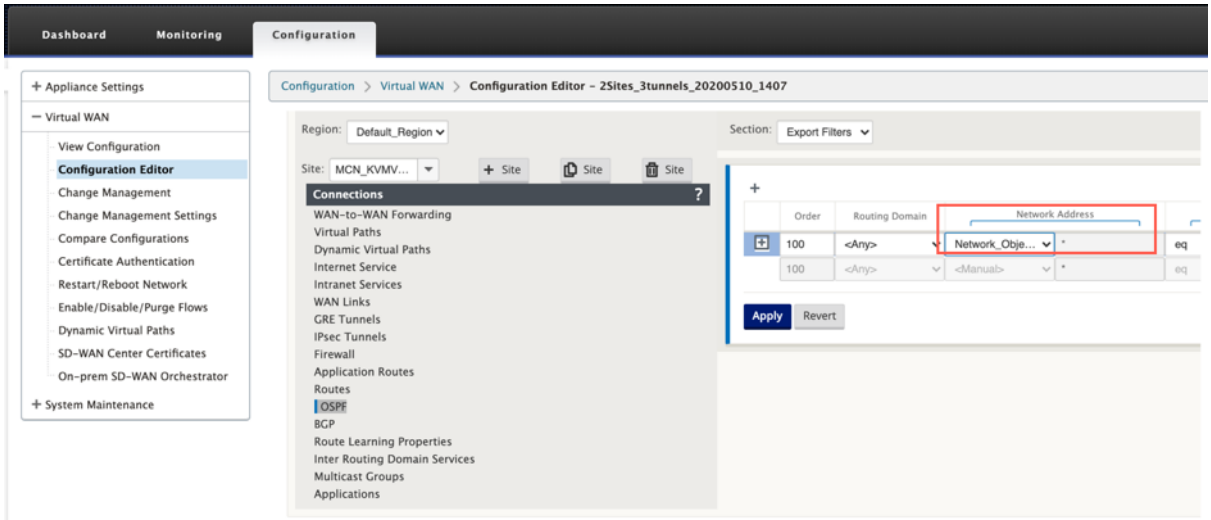


以下功能正在利用网络对象：

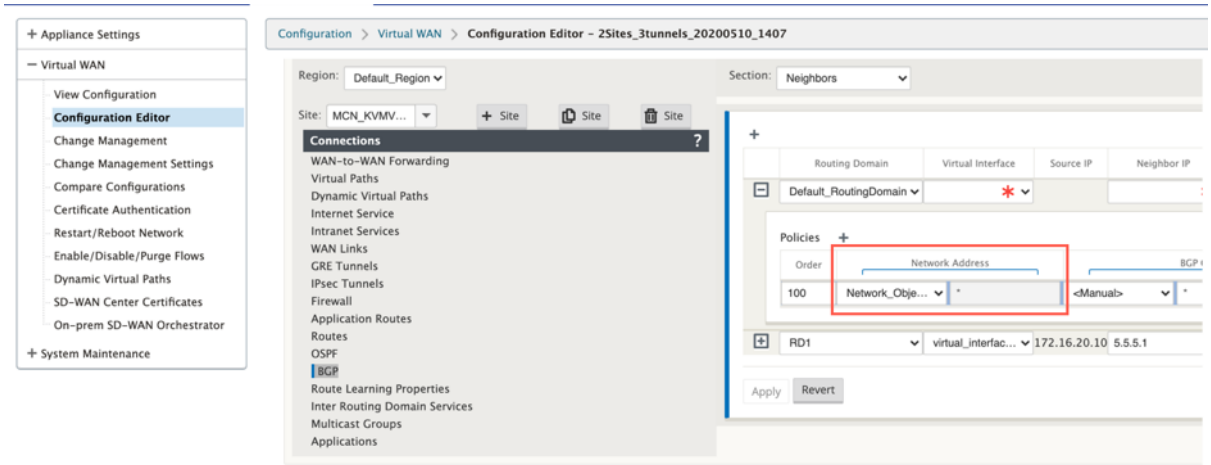
- 路由（配置编辑器 **>** 连接 **>** 路由 **>** 单击 **+** > 网络对象）



- BGP 和 OSPF 导入和导出过滤器（配置编辑器 **>** 连接 **> BGP/OSPF >** 导出/导入过滤器 **>** 单击 **+ >** 网络地址）



- BGP 邻居策略（配置编辑器 **>** 连接 **> BGP >** 邻居 **>** 策略 **>** 单击 **+ >** 网络地址）



LAN 分段路由支持

June 22, 2021

SD-WAN Standard 和 Premium (Enterprise) Edition 设备在部署任一设备的不同站点之间实施局域网分段。这些设备可识别并维护可用 LAN 端 VLAN 的记录，并针对其他 LAN 网段 (VLAN) 可以在远程位置使用其他 SD-WAN 标准或高级（企业）版设备连接的规则进行配置。

通过使用 SD-WAN 标准版或高级（企业）版设备中维护的虚拟路由和转发 (VRF) 表来实现上述功能，该表跟踪本地 LAN 区段可访问的远程 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。VLAN 与 VLAN 关联的配置是

通过 SD-WAN 管理 Web 界面中的 MCN 配置编辑器实现的。

路由间域服务

June 22, 2021

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。有关路由域的更多信息，请参阅 路由域。

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。

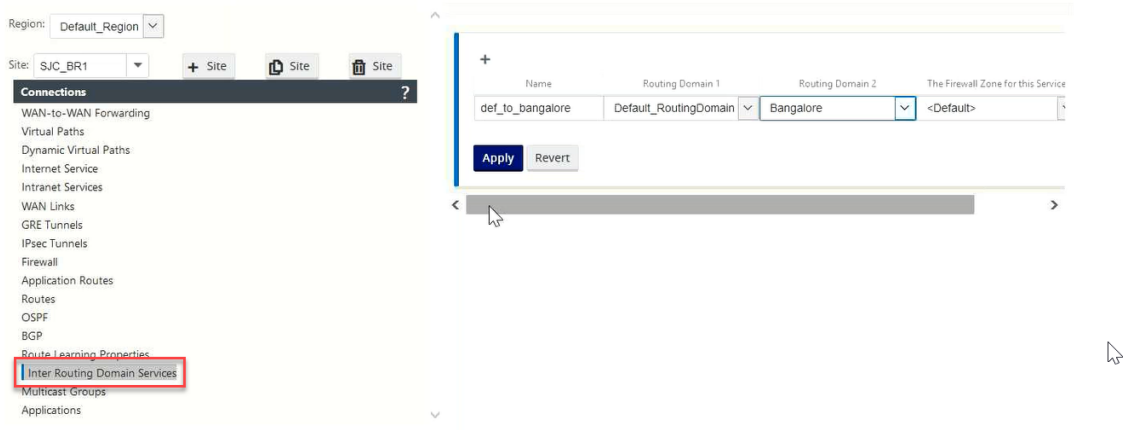
> 注意
>
> Citrix SD-WAN PE 设备不会对路由间域数据包执行 WAN 优化功能。

在两个路由域之间配置路由间域服务。

考虑一个 SD-WAN 网络，其中包含一个 MCN 和 2 个或更多分支机构，其中至少有两个全局配置的路由域。默认情况下，MCN 上的所有路由域都处于启用状态。在其他站点上有选择地启用所需的路由域。有关配置路由域的信息，请参阅 配置路由域。

1. 在 SD-WAN 配置编辑器中，导航到 连接 > 选择站点 > 路由间域服务。
2. 单击 **+** 并输入以下参数的值：

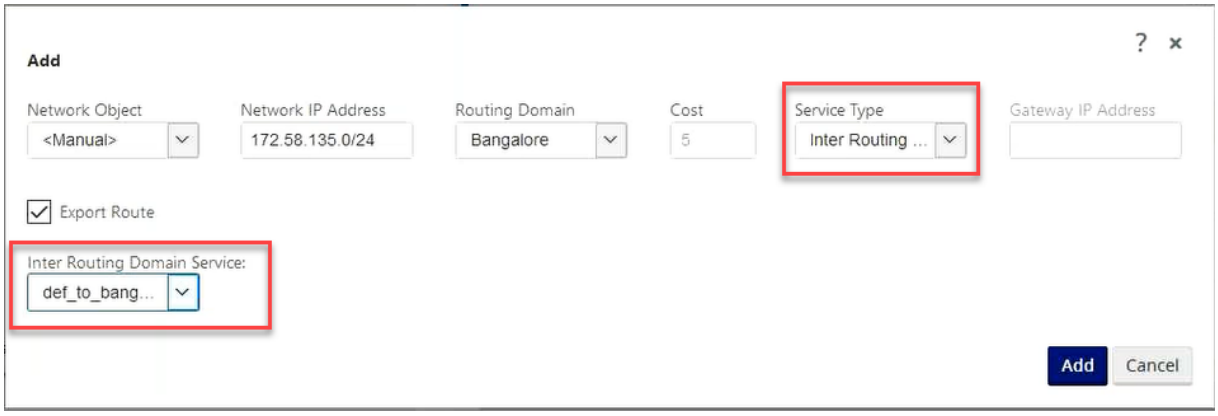
- 名称：路由间域服务的名称。
- 路由域 **1**：对的第一个路由域。
- 路由域 **2**：对的第二个路由域。
- 防火墙区域：服务的防火墙区域。
  - 默认值：分配了 Inter_Routing_Domain_Zone 防火墙区域。
  - 无：未选择任何区域，数据包的原始区域将被保留。
  - 可能会选择网络中配置的所有区域。



1. 单击 应用 以创建路由间域服务。创建的服务可用于创建路由、防火墙策略和 NAT 策略。

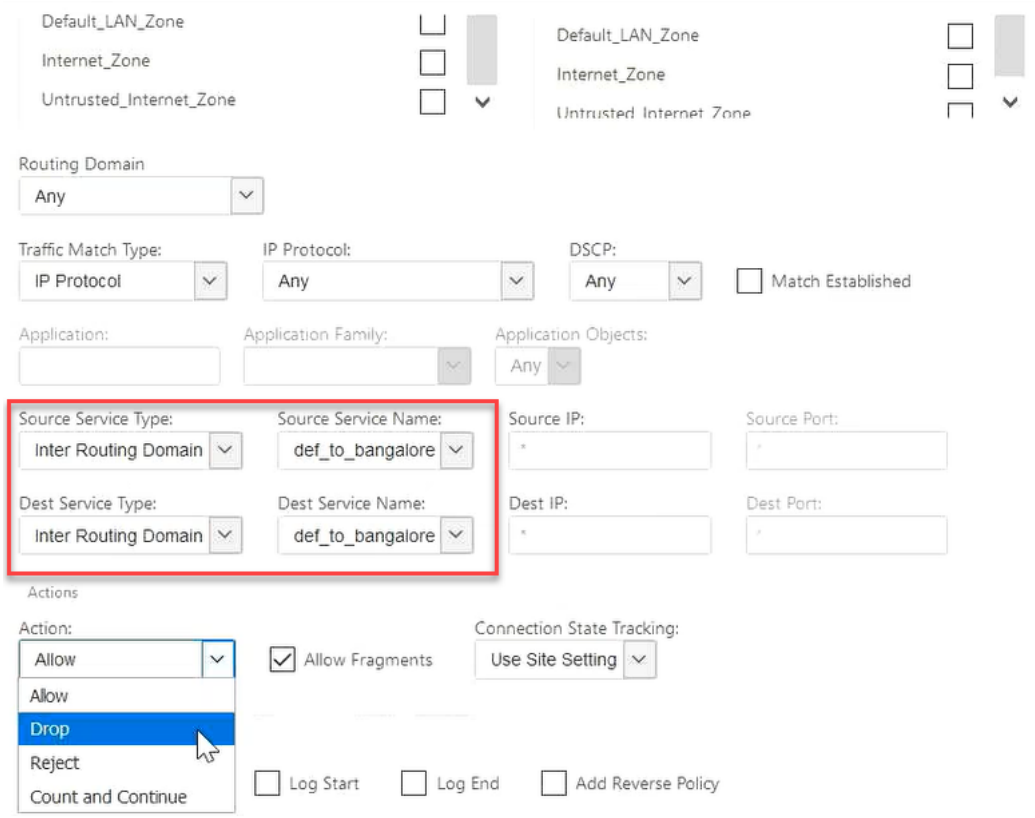
> 注意：
>
> 您无法使用站点上未启用的路由域来配置路由间域服务。

要使用路由间域服务创建路由，请创建一个 服务类型 为 路由间域服务的路由，然后选择路由间域服务。有关配置路由的更多信息，请参阅 如何配置路由。

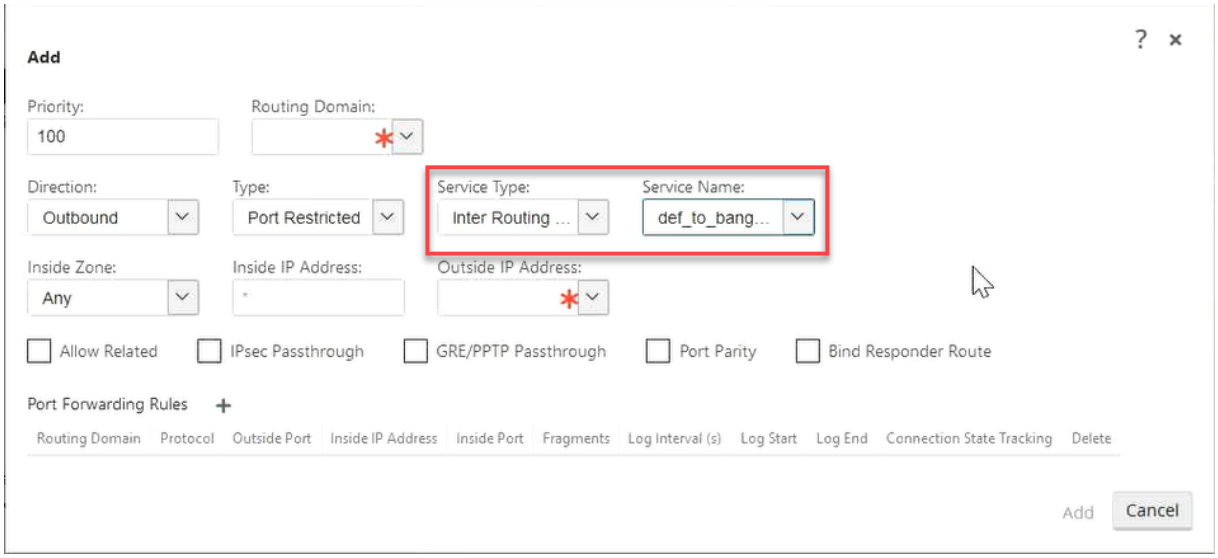


同时添加来自其他路由域对的路由，以建立与两个路由域之间的连接。

您还可以配置防火墙策略来控制路由域之间的流量。在防火墙策略中，为源服务和目标服务选择路由间域服务，然后选择所需的防火墙操作。有关配置防火墙策略的信息，请参阅 策略。

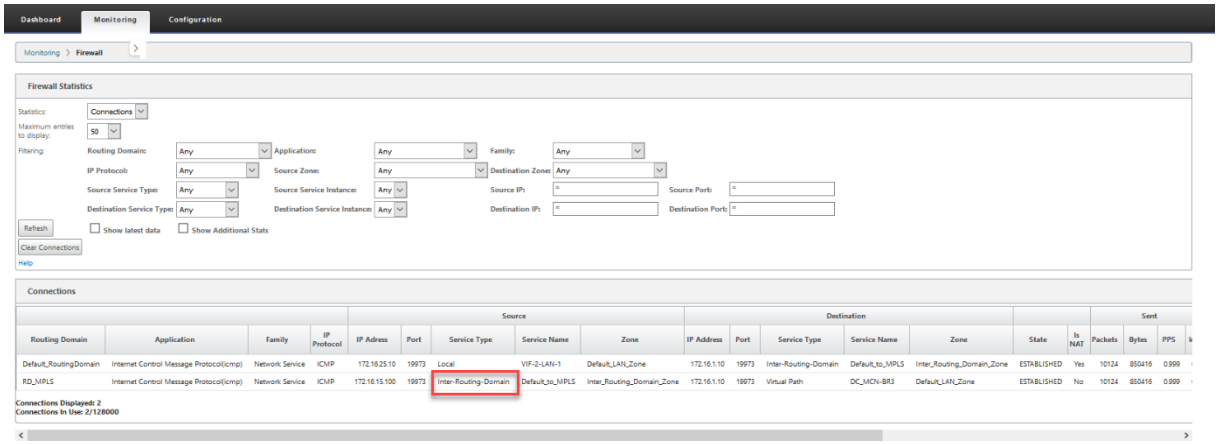


您还可以选择 Intranet 服务类型来配置静态和动态 NAT 策略。有关配置 NAT 策略的更多信息，请参阅 网络地址转换。



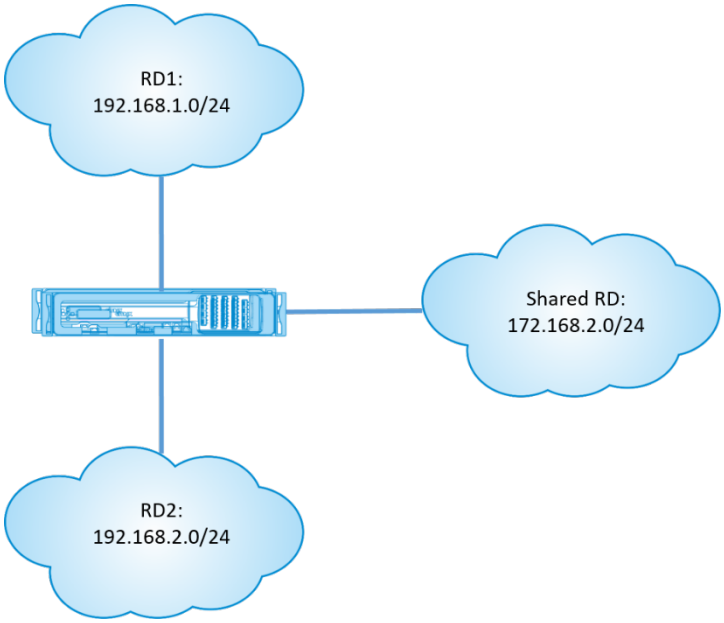
监视

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。



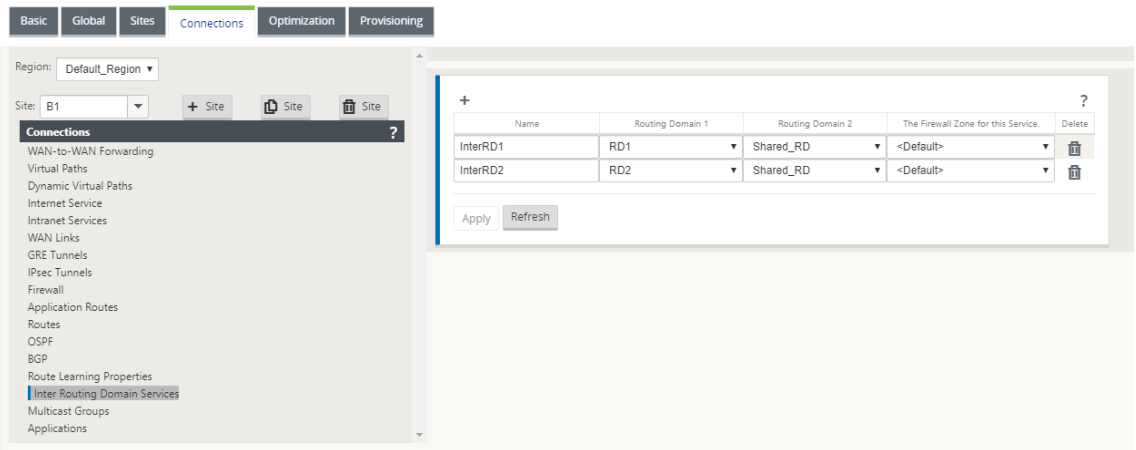
使用案例：跨路由域共享资源

让我们考虑一个场景，即不同路由域中的用户需要访问公共资产，例如打印机或网络存储。分支 RD1、RD2 和共享 RD 有 3 个路由域，如图所示。

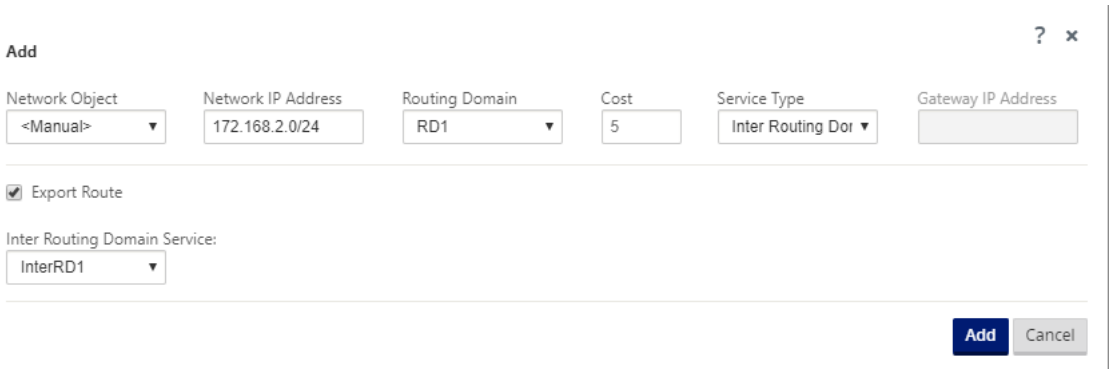


要使 RD1 和 RD2 中的用户能够访问共享 RD 中的资源，请执行以下操作：

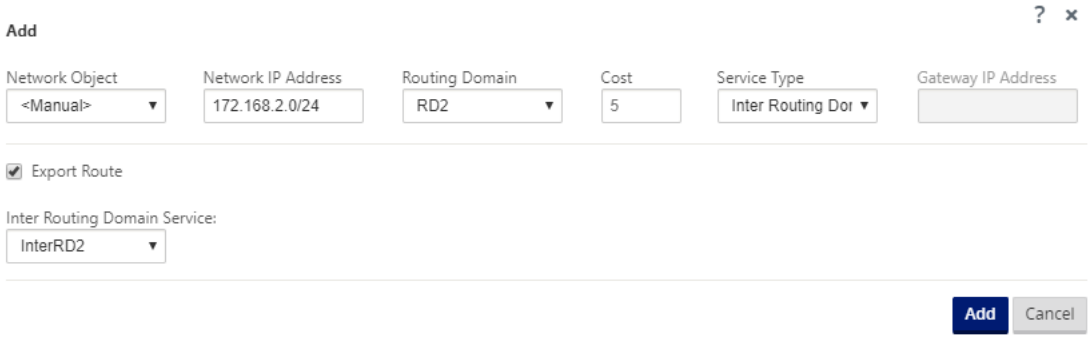
1. 在 RD1 和共享 RD 之间创建路由间域服务，例如 **Inter RD1**。
2. 在 RD2 和共享 RD 之间创建路由域间服务，例如 **Inter RD2**。



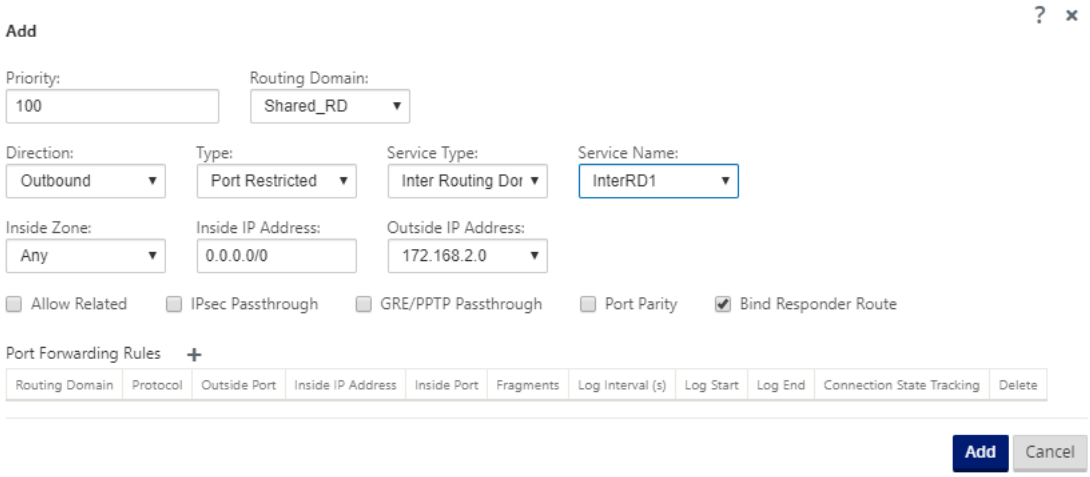
3. 从 RD1 和 RD2 配置到共享 RD 的静态路由。在 RD1 中，将一条路由 172.168.2.0/24 添加到国际线路 1。



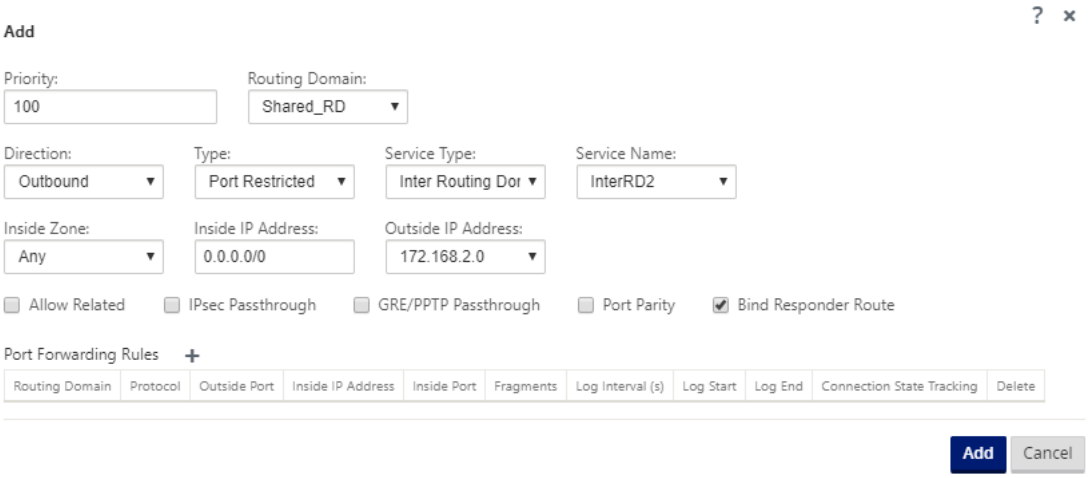
4. 在 RD2 中，将一条路由 172.168.2.0/24 添加到国际线路 2。



5. 使用共享 RD 中的 VIP 将动态 NAT 规则添加到 InterRD1。启用 绑定响应程序路由 以确保反向路由使用相同的服务类型。



6. 使用共享 RD 中的 VIP 将动态 NAT 规则添加到 InterRD2，例如 10.0.0.11。启用 绑定响应程序路由 以确保反向路由使用相同的服务类型。



7. 使用筛选器限制 RD1/RD2 中允许用户访问共享 RD 中的哪些资源。

ECMP 负载平衡

February 10, 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：

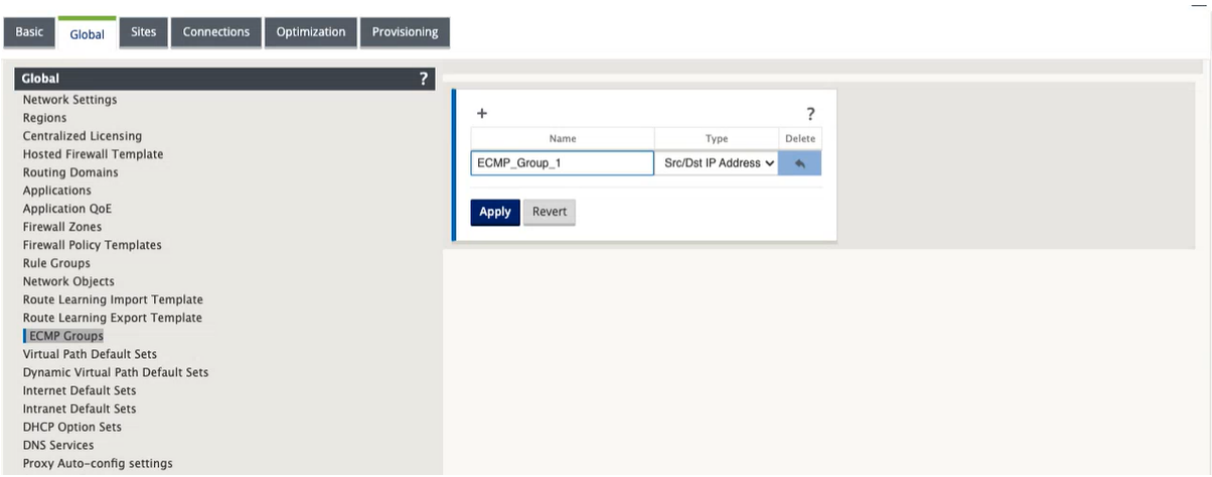
- 通过多条等价路径分布流量。

- 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 隧道上的静态路由。

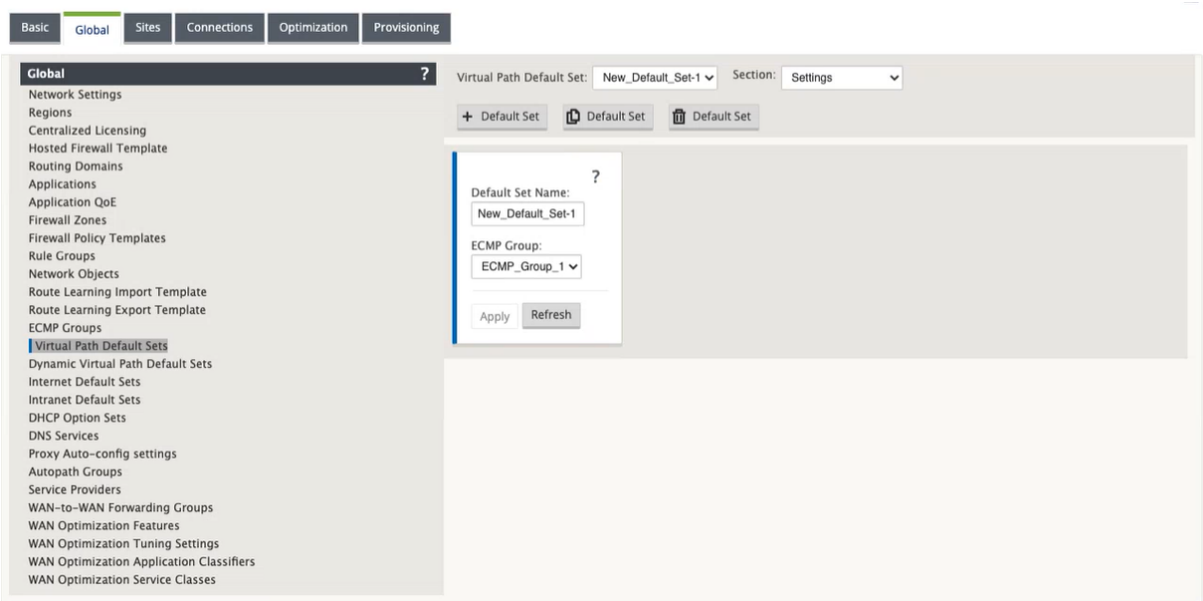
虚拟路径和内联网服务支持 ECMP 负载平衡。ECMP 组是在全球范围内定义的。您最多可以在网络中定义 254 个 ECMP 组。ECMP 组中符合 ECMP 条件的路由的最大数量取决于您的设备和许可证类型。Citrix SD-WAN 支持以下两种类型的 ECMP 组：

- 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。

要配置 ECMP 组，请在配置编辑器中导航到 全局 > **ECMP** 组。提供 ECMP 组的名称，然后根据需要选择类型为 **Src/Dest IP** 地址 或 会话。

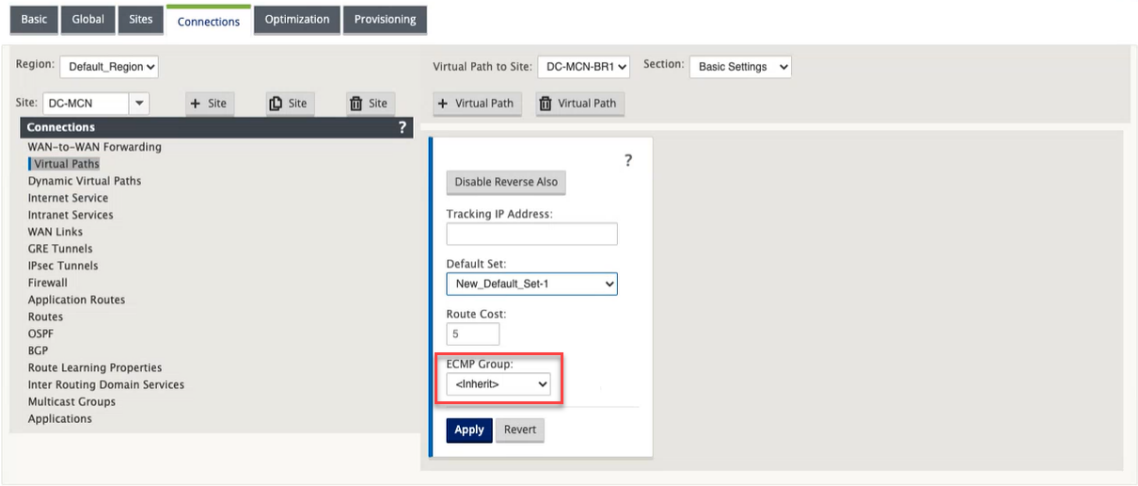


您可以将 ECMP 组与虚拟路径和 Intranet 默认集关联。

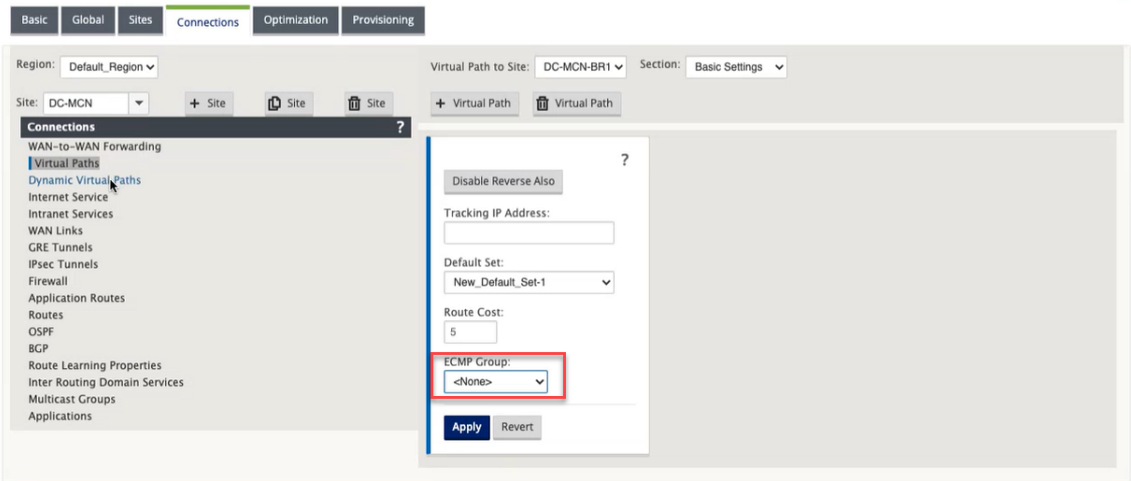


以下是将 ECMP 组与虚拟路径和 Intranet 服务关联的三种方法：

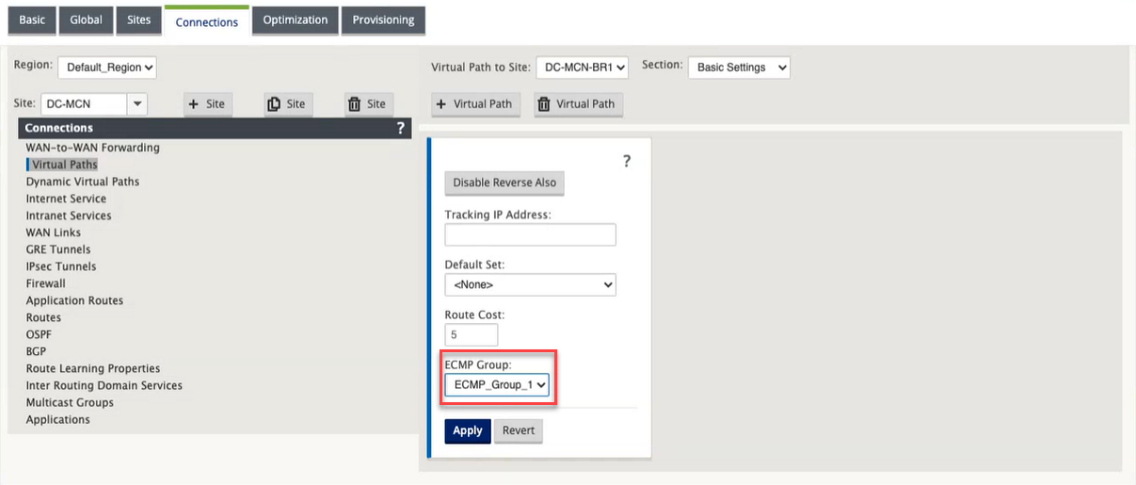
- 继承：服务继承与默认集关联的 ECMP 组。如果没有与默认集关联的 ECMP 组，则该服务不会与任何 ECMP 组关联。



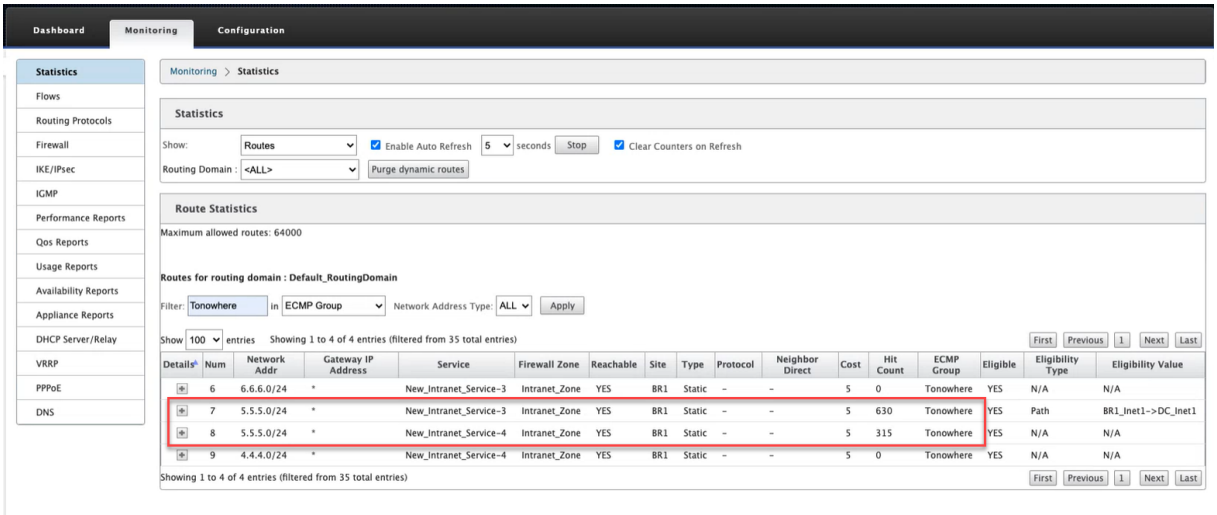
- 无：即使默认集与 ECMP 组关联，该服务也不会与任何 ECMP 组关联。



- **ECMP** 组：选择在全局级别定义的其中一个 ECMP 组以将 ECMP 组与服务关联。选定的 ECMP 组将覆盖与默认集关联的 ECMP 组。



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 隧道路径之间进行负载均衡。
>
> 以下 SD-WAN 设备不支持 ECMP 负载平衡功能：
>
> - Citrix SD-WAN 1000 SE /PE
> - Citrix SD-WAN 2000 SE /PE
> - Citrix SD-WAN 4000 SE

安全对等

June 22, 2021

高级（企业）版设备可以安装在数据中心，并可以启动自动或手动安全对等，创建 SSL 配置文件和关联服务类，并将设备加入 Windows 域控制器，以允许用户/管理员使用独立 WANOP 的扩展丰富功能设备。

以下是自动安全对等和手动安全对等支持的部署模式：

自动安全对等部署：

从直流站点上的独立 WANOP/SDWAN SE/WANOP 执行与 PE 设备的自动安全对等。

启动此部署的步骤：

- WANOP 直流设备处于听开模式（2312/ 任何非标准端口），分支 PE 处于连接至模式。
- WANOP DC 启动与 PE 设备的自动安全对等，该设备安装专用 CA 证书和证书密钥对，并在 PE 设备上使用 WANOP LISTEN-ON IP 配置 CONNECT-TO。

执行从直流站点和分行站点 PE 设备启动的自动安全对等。

启动此部署的步骤：

- PE 直流设备处于侦听开启模式（端口 443 上）。分支 PE 处于连接至模式。
- PE DC 设备启动与 PE 分支设备的自动安全对等，该设备将安装私有 CA 证书和 CERT 密钥对，并使用 DC PE 的 Listen-On IP 在 PE 分支设备上配置 Connect-to。
- PE 的 LISTEN-ON IP 位于与启用了“重定向到 WANOP”的路由域关联的接口 IP 中。

与 WANOP/ SDWAN SE 设备在直流站点和分支机构发起自动安全对等。

启动此部署的步骤：

- PE 直流设备处于侦听开启模式（端口 443 上）。分支 WANOP/SD-WAN SE 处于连接到模式。
- PE DC 设备启动与分支 WANOP/SD-WAN SE 设备的自动安全对等，该设备安装私有 CA 证书和证书密钥对，并使用 DC PE 的 Listen-On IP 在 PE 设备上配置连接至。

手动安全对等部署：

从直流站点的 PE 设备到分支 PE 设备的手动安全对等。

启动此部署的步骤：

- PE 直流设备处于侦听开启模式（端口 443 上）。分支 PE 处于连接至模式。
- PE 的 LISTEN-ON IP 位于与启用了“重定向到 WANOP”的路由域关联的接口 IP 中。
- 手动上载从证书颁发机构的真实来源获得的 CA 和证书密钥对证书。

从直流站点的 PE 设备发起手动安全对等，到分支 WANOP/SDWAN-SE 设备。

启动此部署的步骤：

- PE 直流设备处于侦听开启模式（端口 443 上）。分支 WANOP/SD-WAN SE 处于连接到模式。
- PE 的 LISTEN-ON IP 位于与启用了“重定向到 WANOP”的路由域关联的接口 IP
- 手动上载从证书颁发机构的真实来源获得的 CA 和证书密钥对证书。

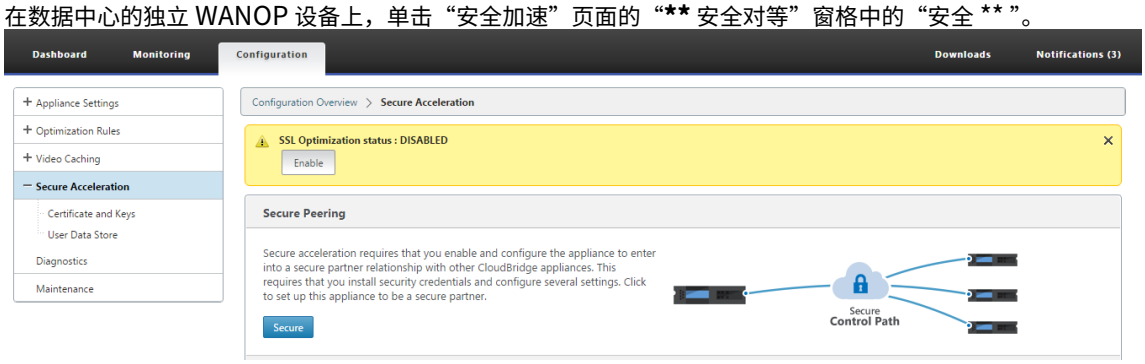
从直流站点上的独立 **SD-WAN SE** 和 **WANOP** 设备到 **PE** 设备的自动安全对等

June 22, 2021

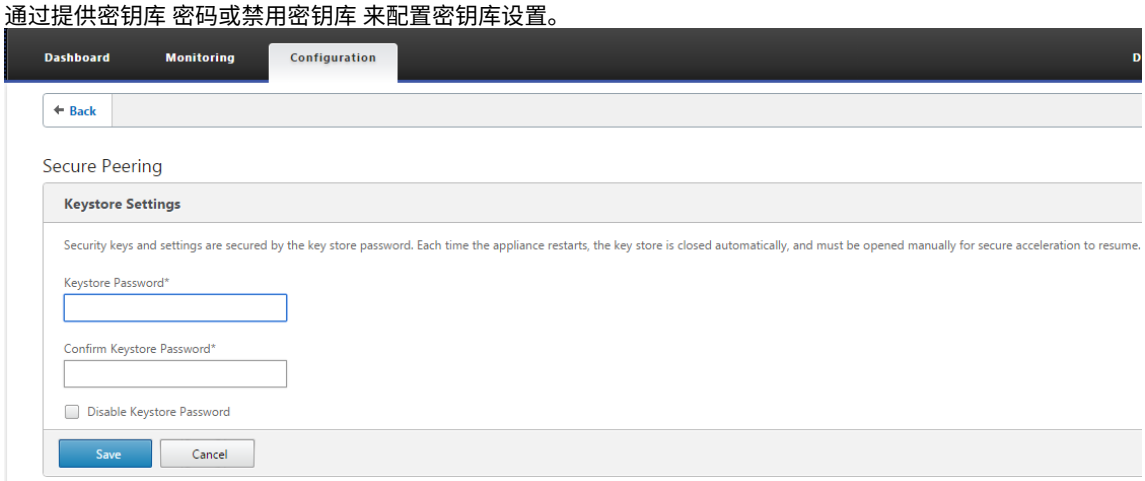
要从直流侧的独立 SD-WAN SE 和 WANOP 设备对 PE 设备执行自动安全对等，请执行以下操作：

- WANOP 直流设备处于听开模式（2312/ 任何非标准端口）。
- 分支 PE 设备处于连接至模式。
- WANOP DC 启动与 PE 设备的自动安全对等，该设备安装专用 CA 证书和证书密钥对，并在 PE 设备上使用 WANOP LISTEN-ON IP 配置 CONNECT-TO。

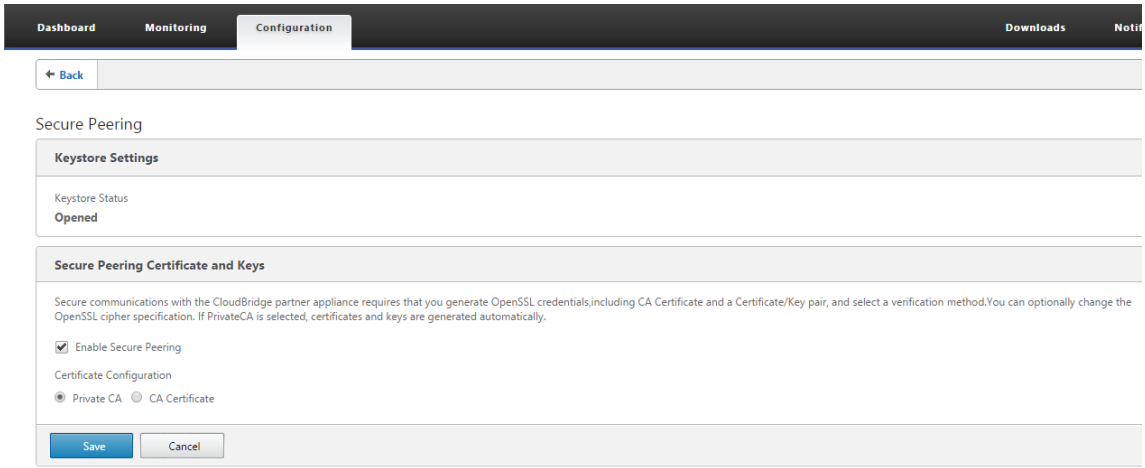
1. 在数据中心的独立 WANOP 设备上，单击“安全加速”页面的“**** 安全对等”窗格中的“安全 ** ”。



2. 通过提供密钥库 密码或禁用密钥库 来配置密钥库设置。



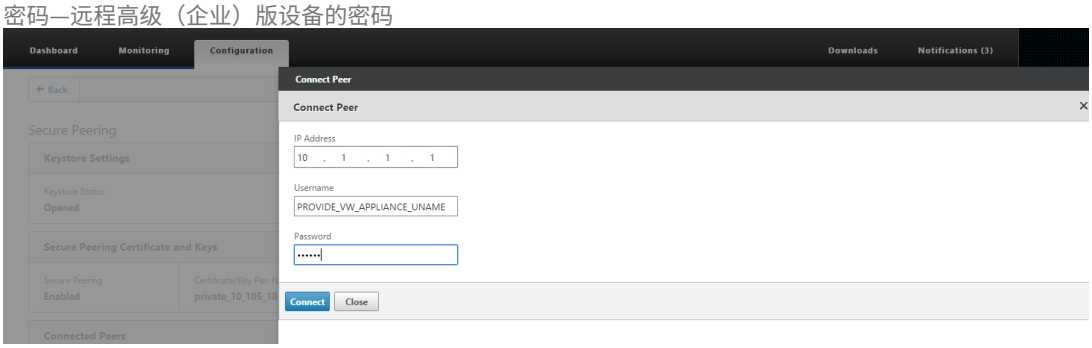
3. 通过选择 私有 **CA** 以执行自动安全对等来启 用安全对等互连。



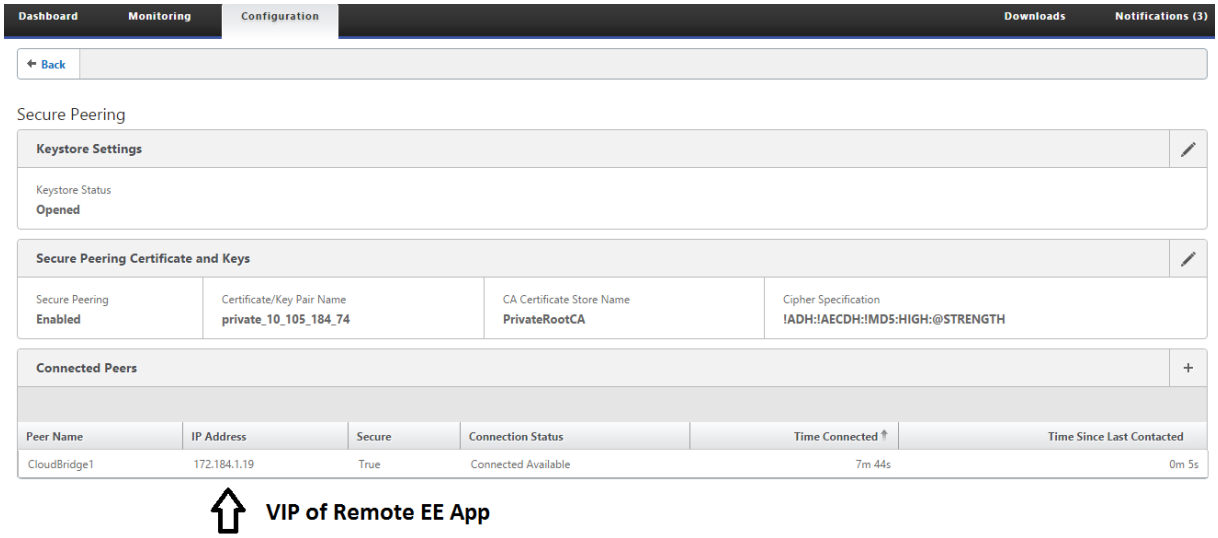
4. 在本地 WANOP 上生成设备级别 CA 证书以及私有证书和密钥，并显示一个用于添加远程对等执行自动安全对等的表。
5. 单击 **+** 图标，并显示一个弹出窗口以添加用户名和密码的 IP 地址。使用提供的凭据的远程 IP 成功进行身份验证后，将向远程计算机发送请求，该计算机将为本地（在远程计算机上）安装 CA 证书和私有证书和密钥。

注意

- IP 地址—远程高级（企业）版设备管理 IP 的 IP 地址
- 用户名—远程高级（企业）版设备的用户名
- 密码—远程高级（企业）版设备的密码



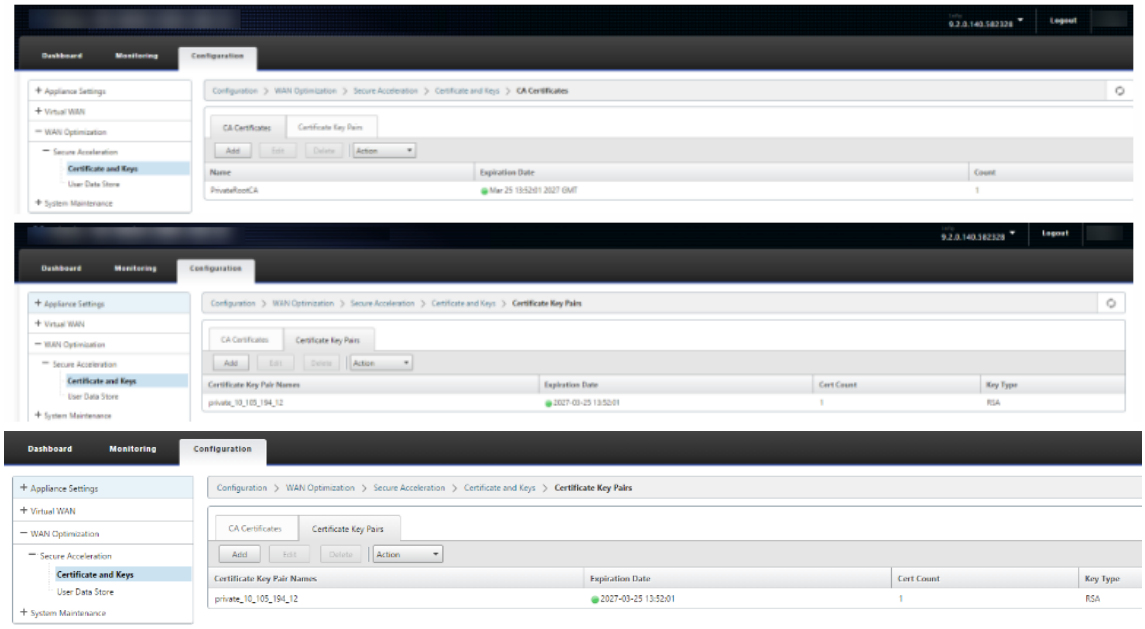
身份验证成功后，您将看到安全对等互连为 TRUE，合作伙伴 IP 地址是远程高级（企业）版设备的虚拟 IP 地址之一。



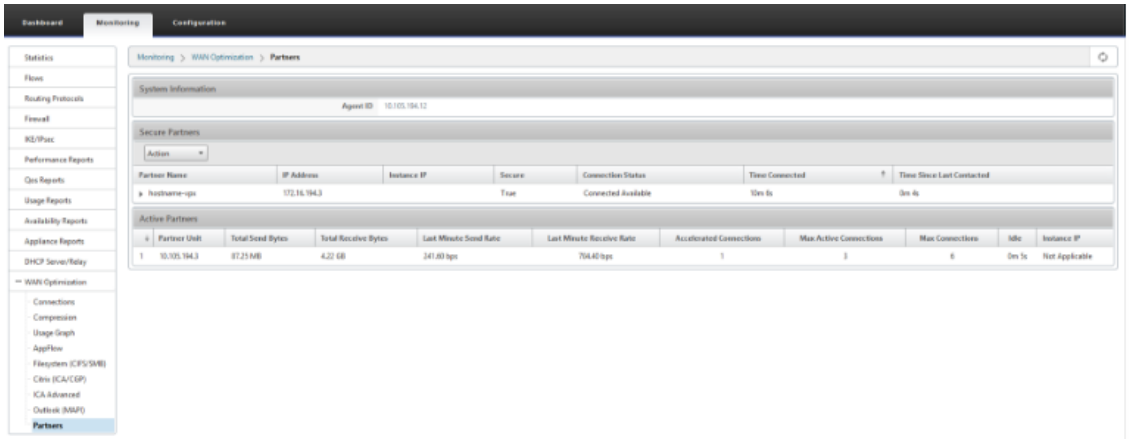
监视

在 监 控页面的 **WANOPT** ION > 合作伙伴下，查看高级（企业）版设备上的安全合作 伙伴 信息。

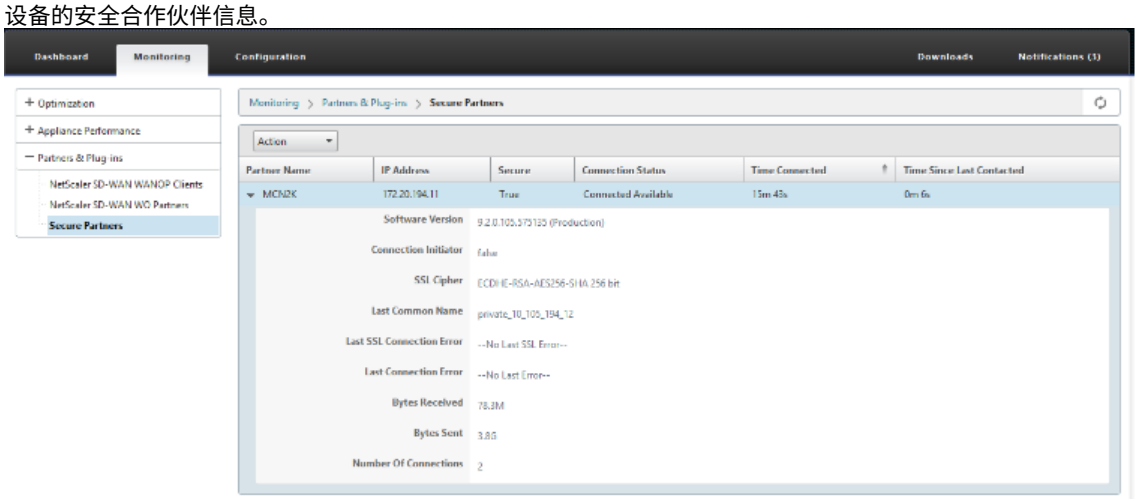
1. 通过从 高级（企业）版设备的 优化 节点下的 MCN 启用功能，可以在 高级（企业）版设备上执行数据存储加密。
2. 对于 高级（企业）版设备，始终 启用安全对等。
3. To validate if the **Private CA** and **Private Certificate Key** pair is generated successfully, review the information below:



4. 在 监视 > **WAN** 优化 > 合作伙伴页面下，查看高级（企业）版设备上的安全合作伙伴信 息。

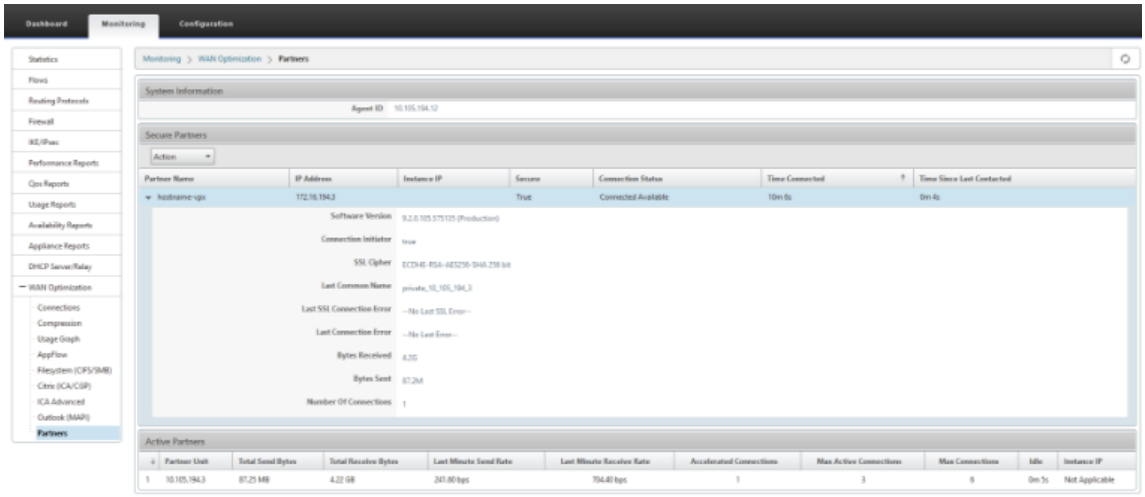


5. 在合作伙伴设备上，在监视 > 合作伙伴和插件 > 安全合作伙伴页面下查看 **Premium (Enterprise) Edition** 设备的安全合作伙伴信息。

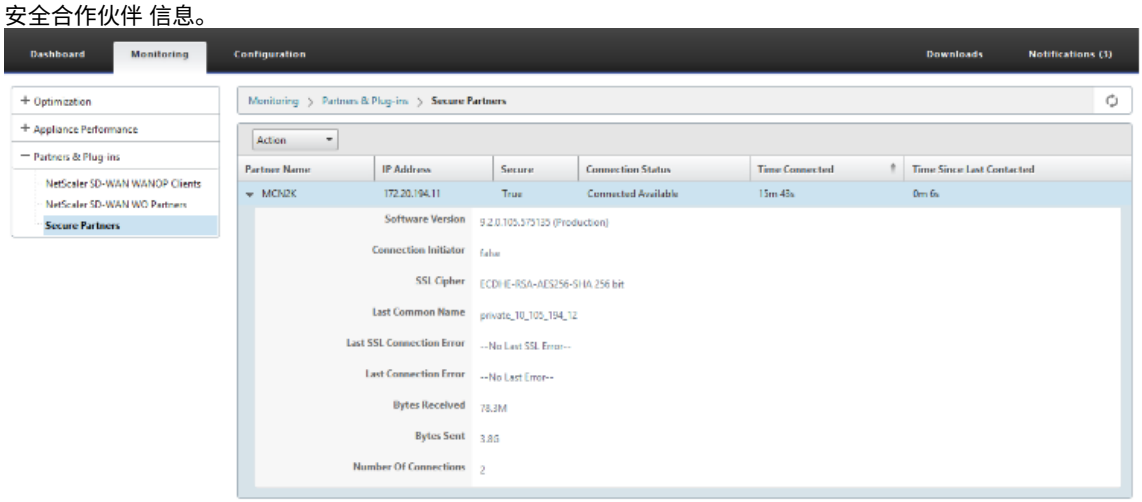


故障排除

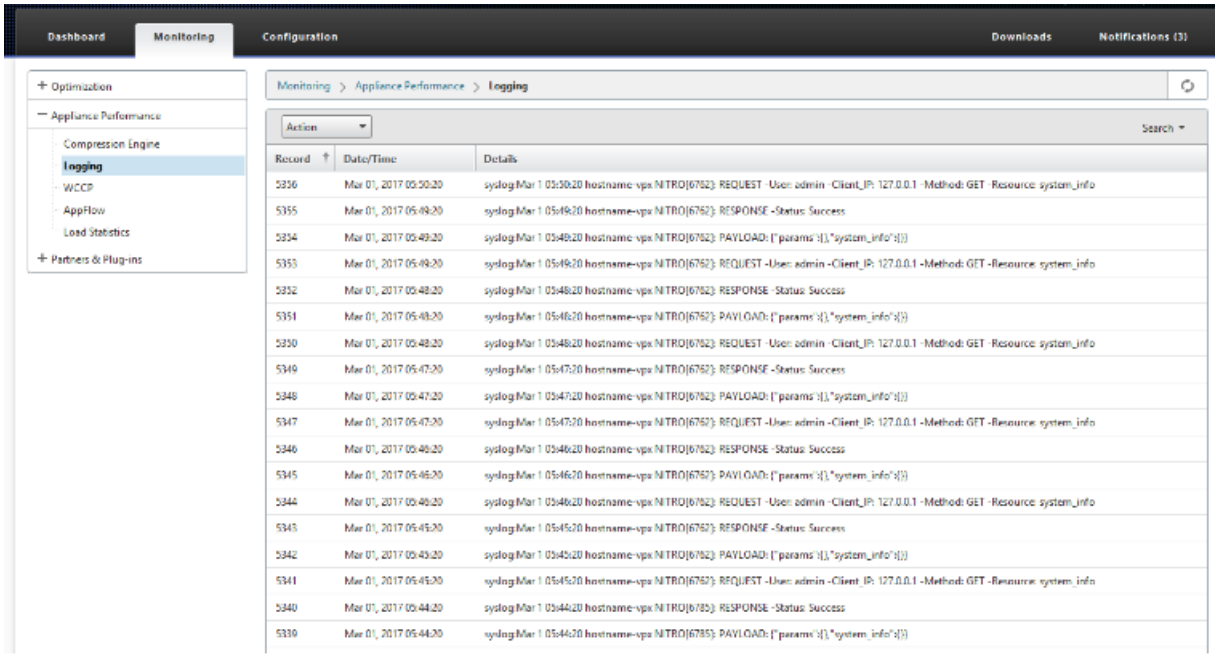
1. 在 监控 > **WAN** 优化 > 合作伙伴 > 安全合作伙伴页面下，查看高级（企业）版设备上的安全合作伙伴成 功/ 失败信 息。



2. 在合作伙伴设备上，在“监视”> “合作 伙伴和插件”**>** “安全合作伙伴”页面下，查看高级（企业）版设备上的安全合作伙伴 信息。



3. 在合作伙伴设备上，在 监控 > 设备 性能 **>** 日志记录页面下查看高级（企业）版设备 上的安全合作伙伴信息。



直流站点和分支站点 **PE** 设备启动自动安全对等

June 22, 2021

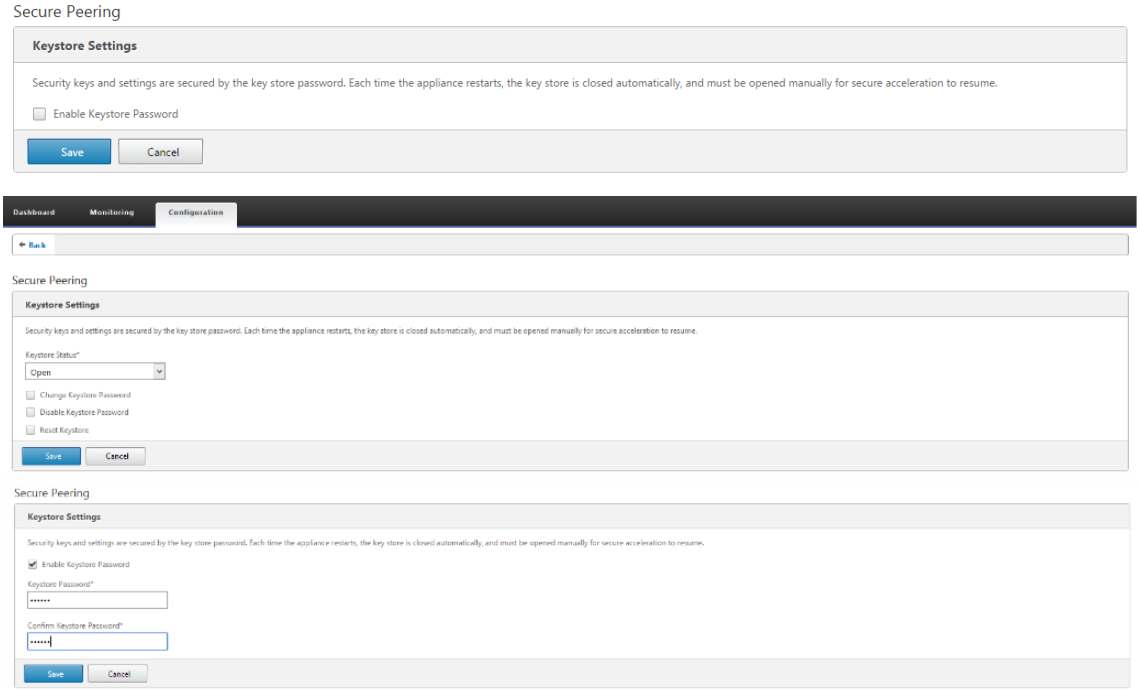
配置

要在 DC 新的高级（企业）版设备上配置自动安全对等，请执行以下操作：

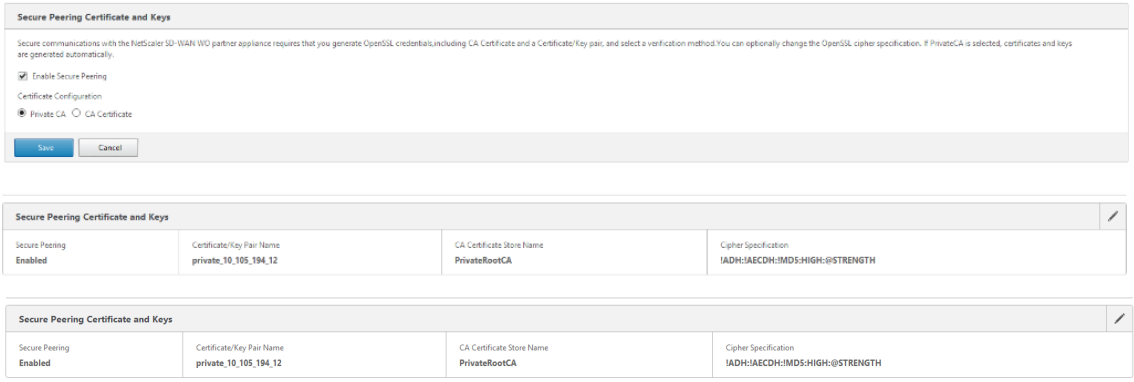
- PE 直流设备处于侦听开启模式（端口 443 上）。分支 PE 设备处于连接至模式。
- PE DC 设备启动与 PE 分支设备的自动安全对等，该设备将安装私有 CA 证书和 CERT 密钥对，并在 PE 分支设备上使用 DC EE 的 Listen-On IP 配置连接至。
- PE 设备的 LISTEN-ON IP 位于与已启用“重定向到 WANOP”的路由域关联的接口 IP 中。

1. 在 SD-WAN Web GUI 中，导航到 配置 > **WAN** 优化 > 安全加速 > 安全对等。

2. 通过提供密 钥库密码或禁用密钥库来配置密钥库。

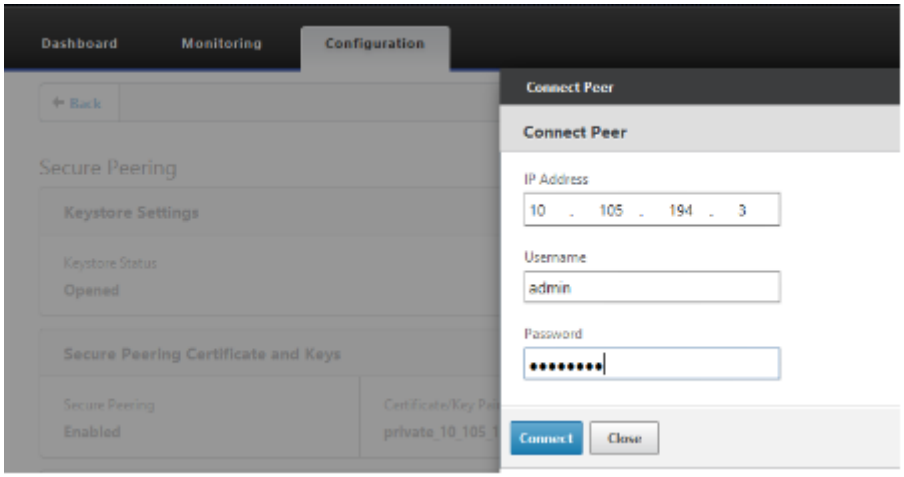


3. 通过选择私有 CA 来执行自动安全对等，启用安全对等。



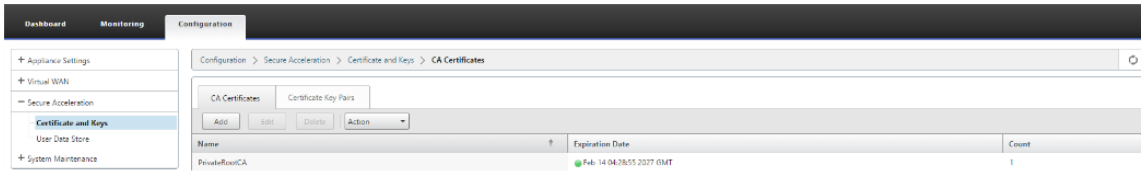
4. 单击 + 图标并添加带有用户名和密码的 IP。使用提供的远程 IP 和凭据成功进行身份验证后，将向远程计算机发送请求，该计算机将在远程计算机上本地安装 CA 证书和私有证书和密钥。

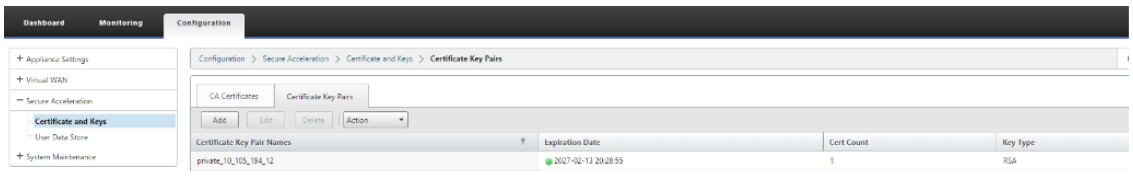
> 注意
>
> IP 地址—远程 EE 设备管理 IP 的 IP 地址
>
> 用户名—远程 EE 设备的用户名
>
> 密码—远程 EE 设备的密码



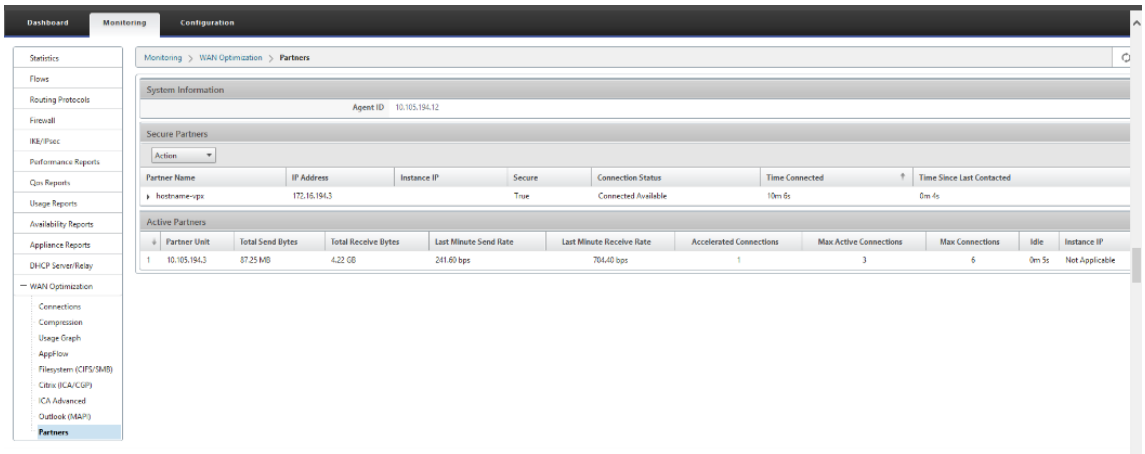
监视

1. 要验证是否成功生成私有 CA 和私有证书密钥对，请查看下面显示的信息。

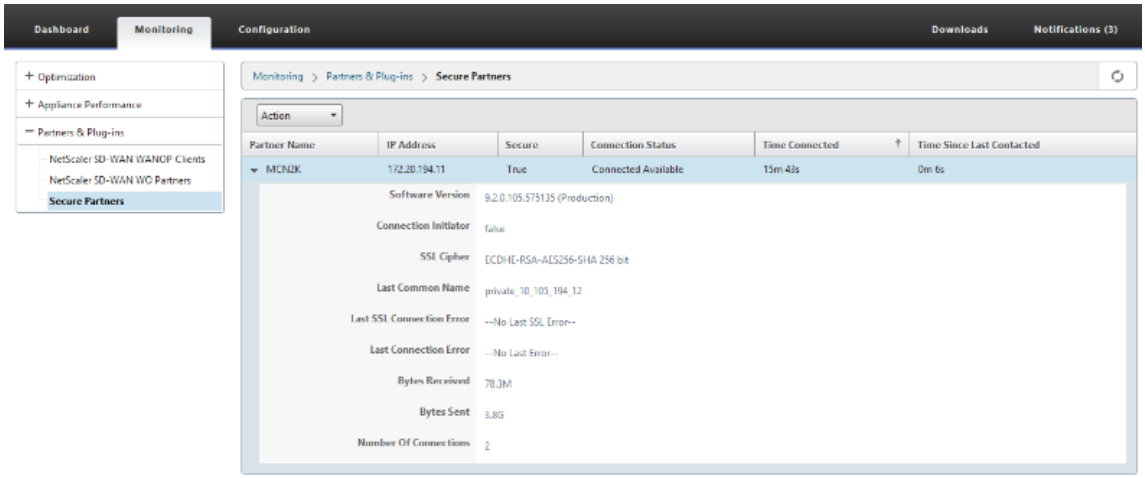




2. 在 监视 > **WAN** 优化 > 合作伙伴页面下，查看高级（企业）版设备上的安全合作伙伴信 息。

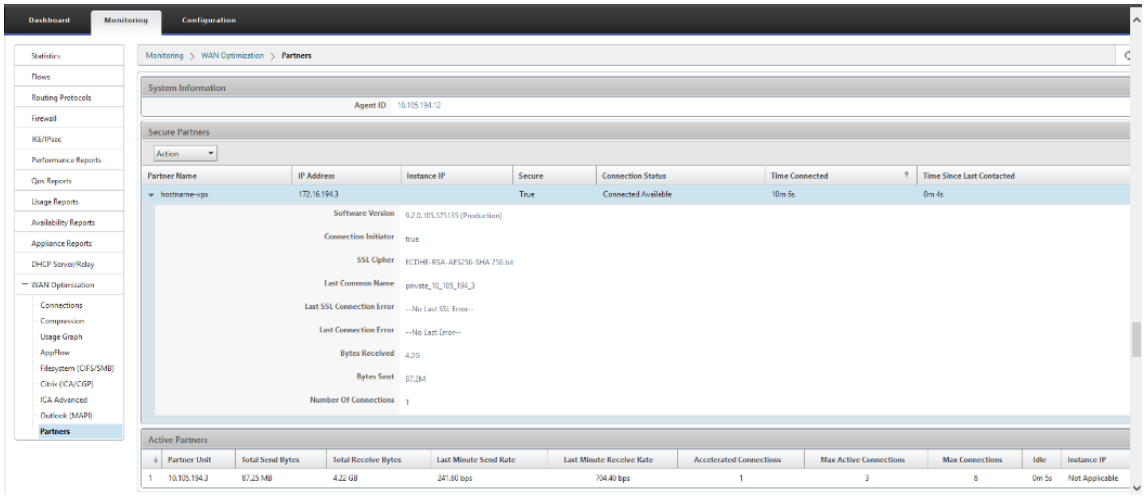


3. 在合作伙伴设备上，查看 监视 > 合作 伙伴和插件 **>** 安全合作伙伴 页面下的 高级（企业）版设备 上的 安全合作伙伴 信息。

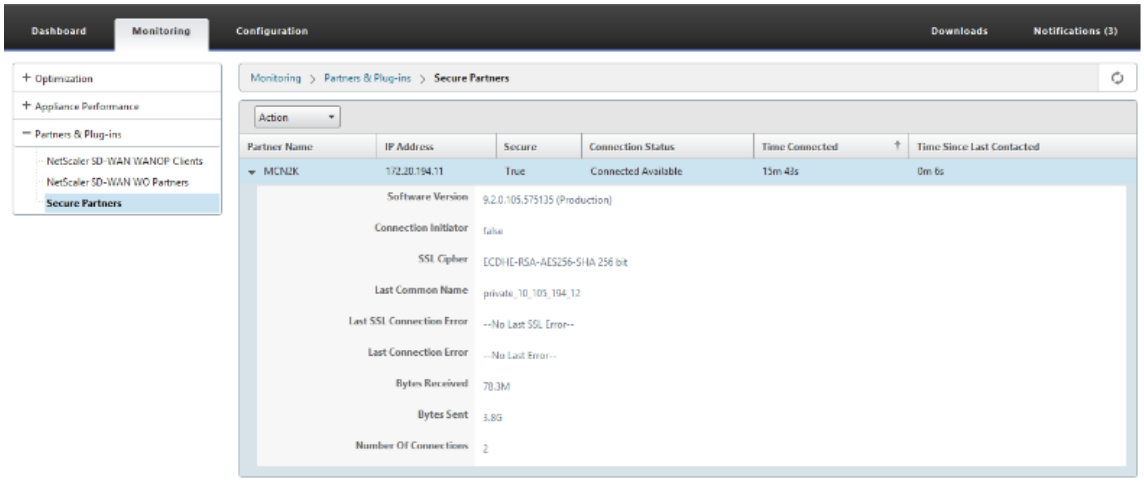


故障排除

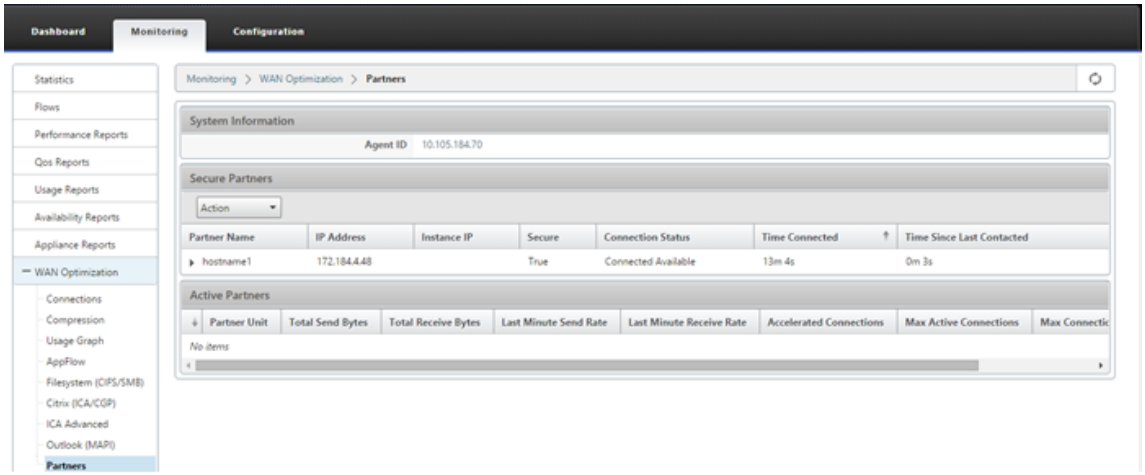
1. 在 监视 > **WAN** 优化 > 合作伙伴 > 安全合作伙伴页面下，查看高级（企业）版设备上的 安全 合作 伙伴 成功/失败信息。

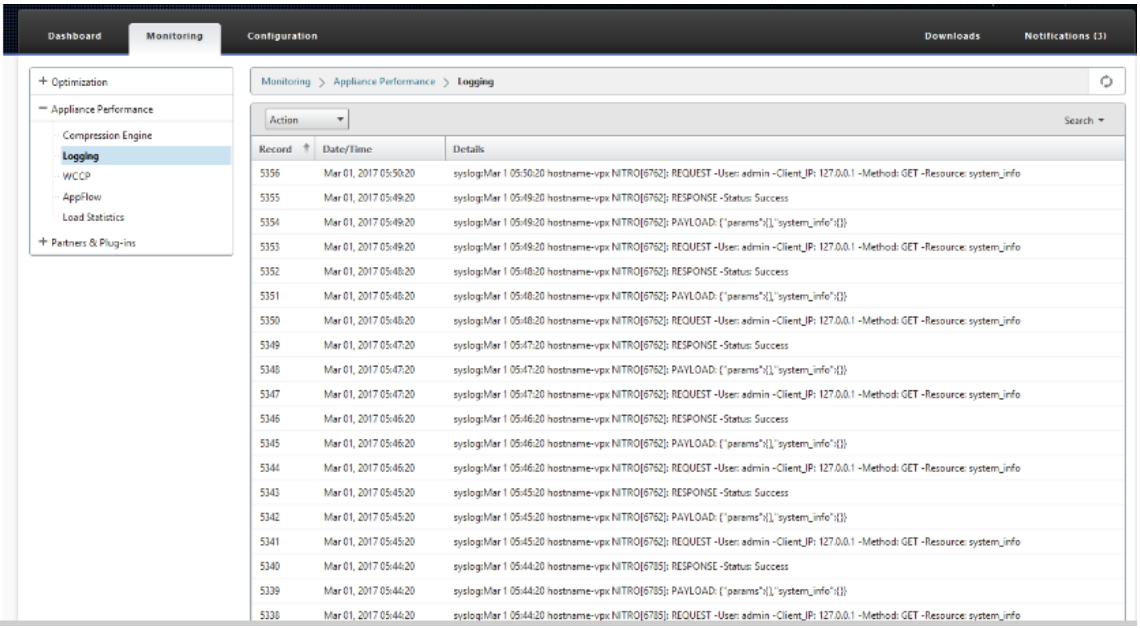


2. 在合作伙伴设备上，查看 监视 > 合作 伙伴和插件 **>** 安全合作伙伴 页面下的 高级（企业）版设备 上的 安全合作伙伴 信息。



3. 在合作伙伴设备上，查看 监视 > 设备 性能 **>** 日志记录页面下的 高级（企业）版设备 上的 安全合作伙伴信息。





通过独立 **SD-WAN SE** 和 **WANOP** 设备在直流站点和分支机启动自动安全对等

June 22, 2021

配置

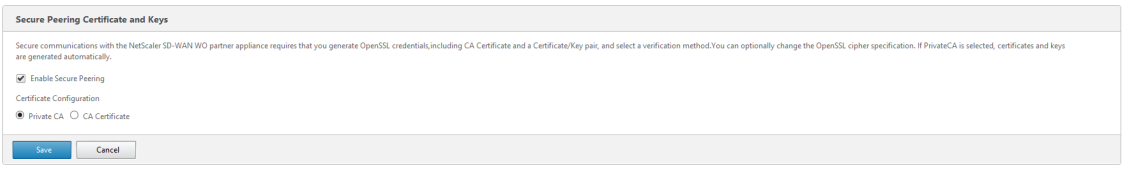
使用独立 SD-WAN 和 WANOP 设备在 DC 站点和分支机构配置具有自动安全对等功能的新高级（企业）版设备：

- PE 直流设备处于侦听开启模式（端口 443 上）。
- 分支独立 SD-WAN SE 和 WANOP 处 于连接到模式。
- PE DC 设备启动与分支独立 SD-WAN SE 和 WANOP 设备的自动安全对等，后者安装私有 CA 证书和 CERT 密钥对，并在 PE 设备上使用 DC EE 的 Listen-On IP 配置连接至。

1. 在 SD-WAN Web GUI 中，导航到 配置 > **WAN** 优化 > 安全加速 > 安全对等。

2. 通过提供密钥库密码或禁用密 钥库来配置密钥库。

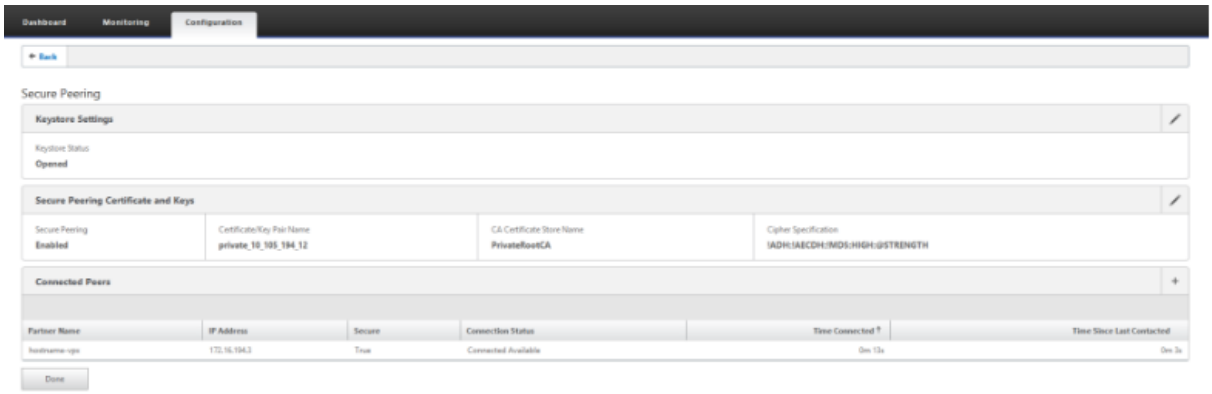
3. 通过选择私有 CA 来执行自动安全对等，启用安全对等。



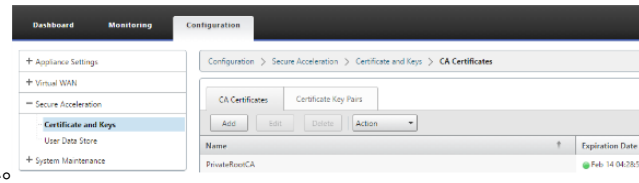
4. 单击“+”图标并添加带有用户名和密码的 IP。使用提供的远程 IP 和凭据成功进行身份验证后，将向远程计算机发送请求，该计算机将在远程计算机上本地安装 CA 证书和私有证书和密钥。

   - IP 地址—远程 WANOP 独立或标准版设备管理 IP 的 IP 地址。
   - 用户名—远程 WANOP 独立或标准版设备的用户名。
   - 密码—远程 WANOP 独立或标准版设备的密码。

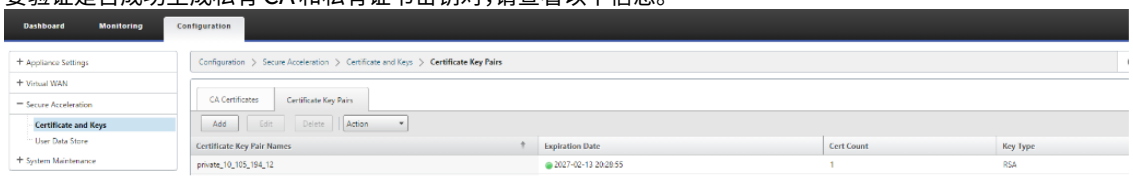
身份验证成功后，您可以将安全对等视为 TRUE，将伙伴 IP 视为远程 WANOP 独立设备的虚拟 IP 之一。



监视

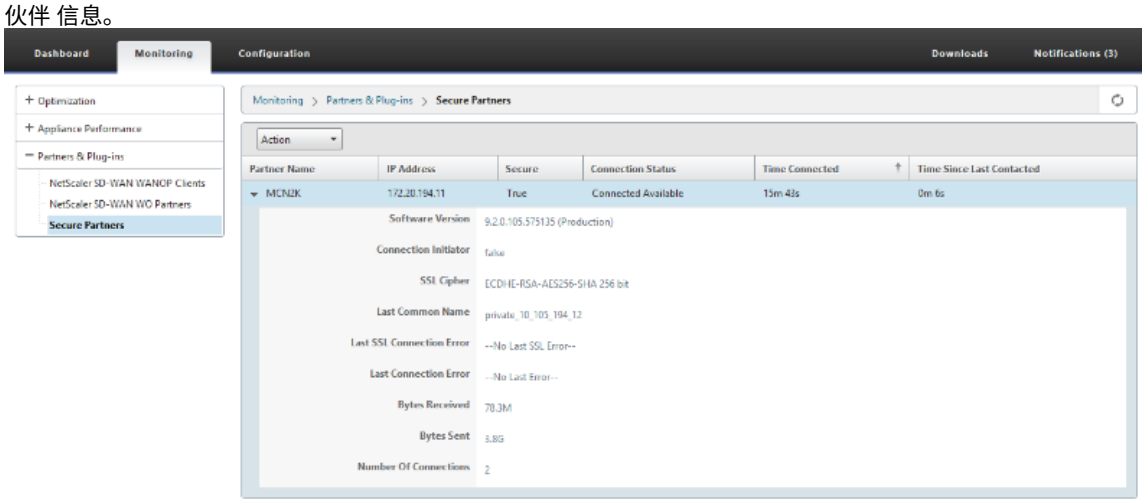


1. 要验证是否成功生成私有 CA 和私有证书密钥对，请查看以下信息。



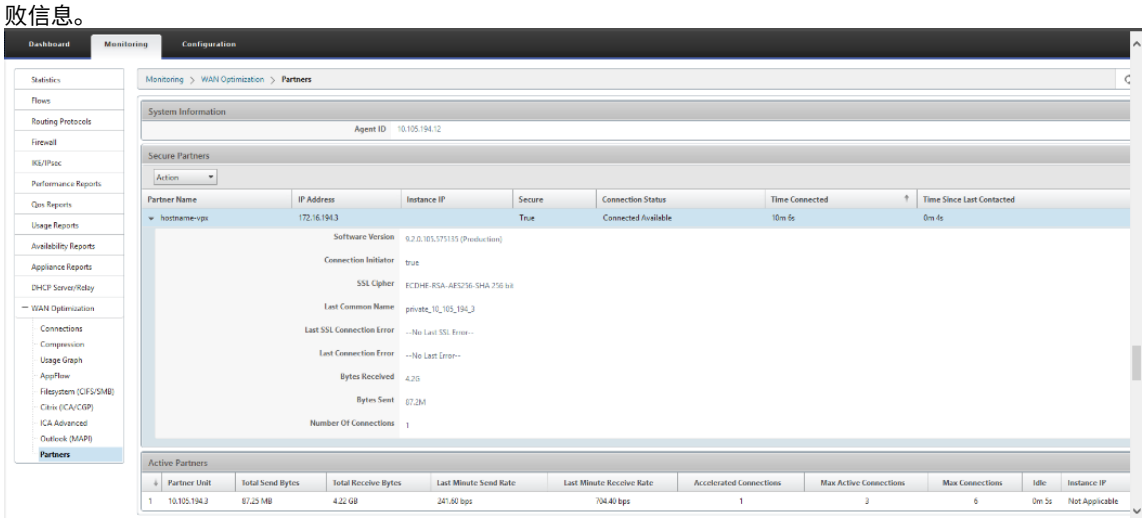
2. 在 监控 > **WAN** 优化 > 合作伙伴页面下查看高级（企业）版设备上的安全合作 伙伴 信息。

3. 在合作伙伴设备上，在 监视 > 合作 伙伴和插件 **>** 安全合作伙伴 页面下，查看高级（企业）版设备上的 安全合作伙伴 信息。

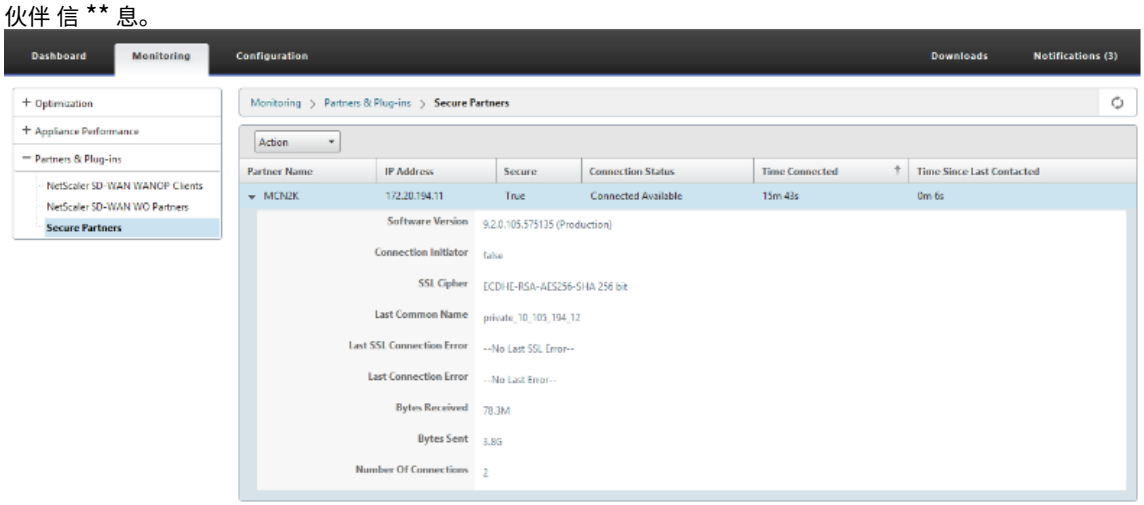


故障排除

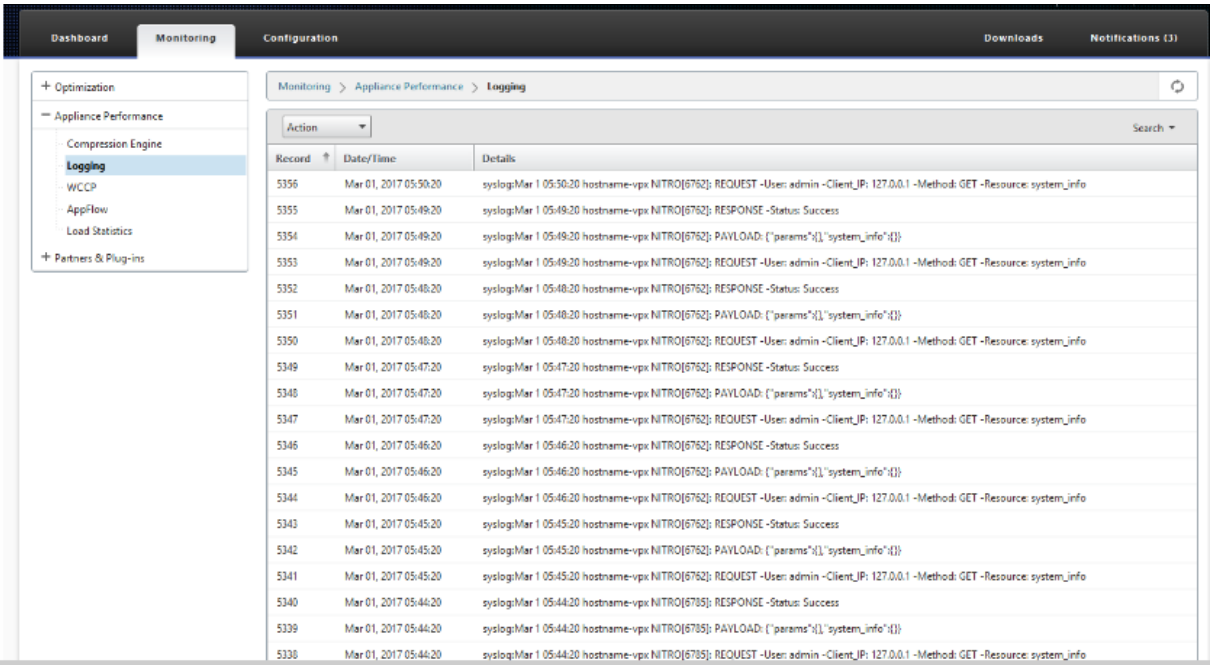
1. 在 监视 > 广域网优化 > 合作伙伴 > 安全合作伙伴 页面下，查看高级（企业）版设备上的 安全 合作 伙伴 成功/失败信息。



2. 在合作伙伴设备上，在 监控 > 合作 伙伴和插件 **>** 安全合作伙伴页面下查看高级（企业）版设备上的 ****** 安全合作伙伴 信 ** 息。



3. 在合作伙伴设备上，查看高级（企业）版设备上的 监视 > 设 备性能 > 日志记录 页面下的 安全合作伙伴信 息。



从直流站点的 **PE** 设备和分支 **PE** 设备启动手动安全对等

June 22, 2021

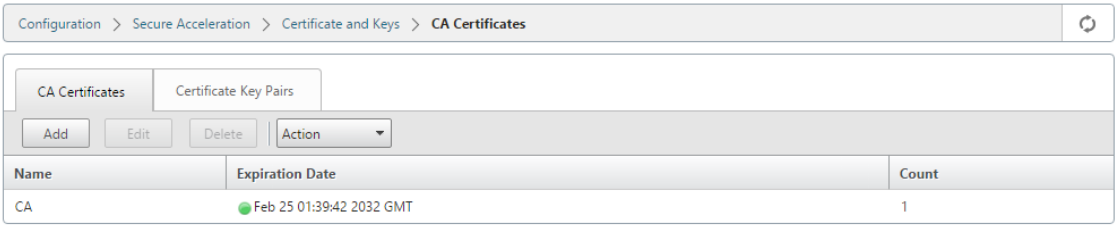
此部署将在聆听开启模式下配置 DC 站点 PE 设备，并在连接到模式下配置分支站点 PE 设备。

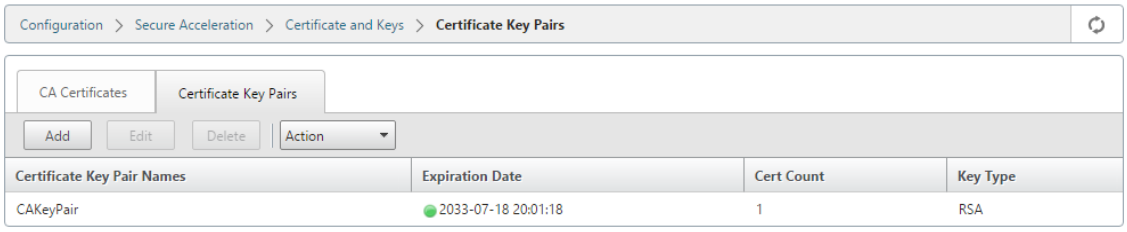
- PE 直流设备处于侦听开启模式（端口 443 上）。
- 分支 PE 设备处于连接至模式。
- PE 的 LISTEN-ON IP 位于与启用了“重定向到 WANOP”的路由域关联的接口 IP 中。
- 手动上载从证书颁发机构的真实来源获得的 CA 和证书密钥对证书。

配置

要配置从 DC 站点的 PE 设备和分支站点的 PE 设备启动的自动安全对等，请执行以下操作：

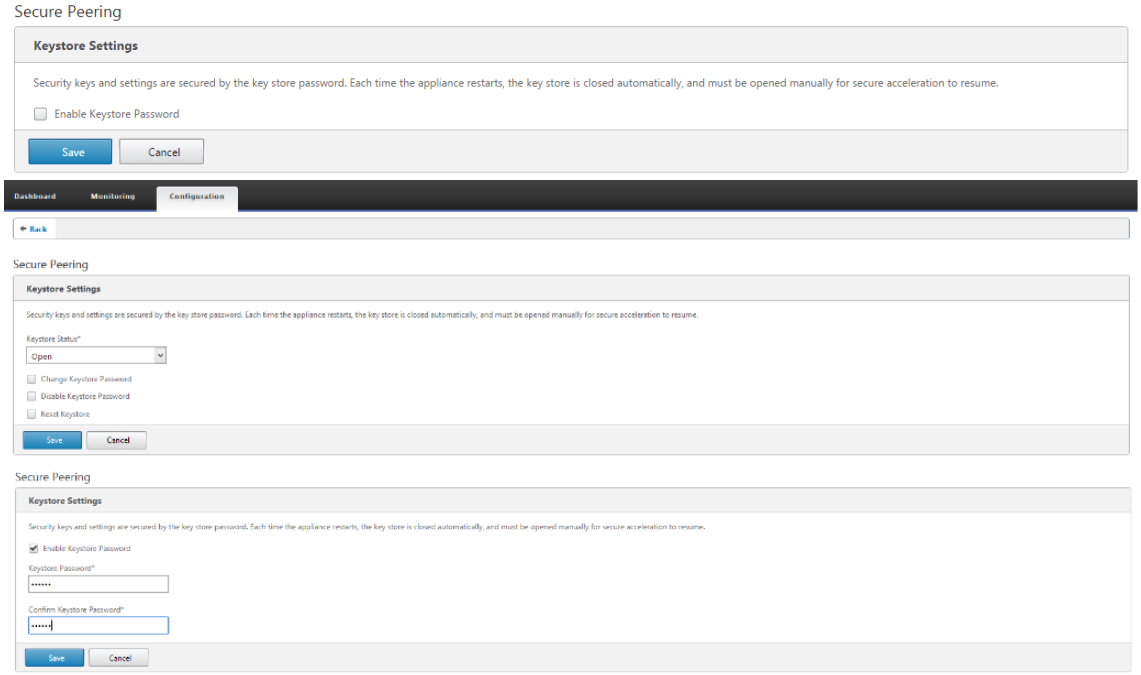
1. 上载从真实 证书 获得的 **CA** 证书和 **CA** 密钥 证书，并提供给 SD-WAN，如下所示。



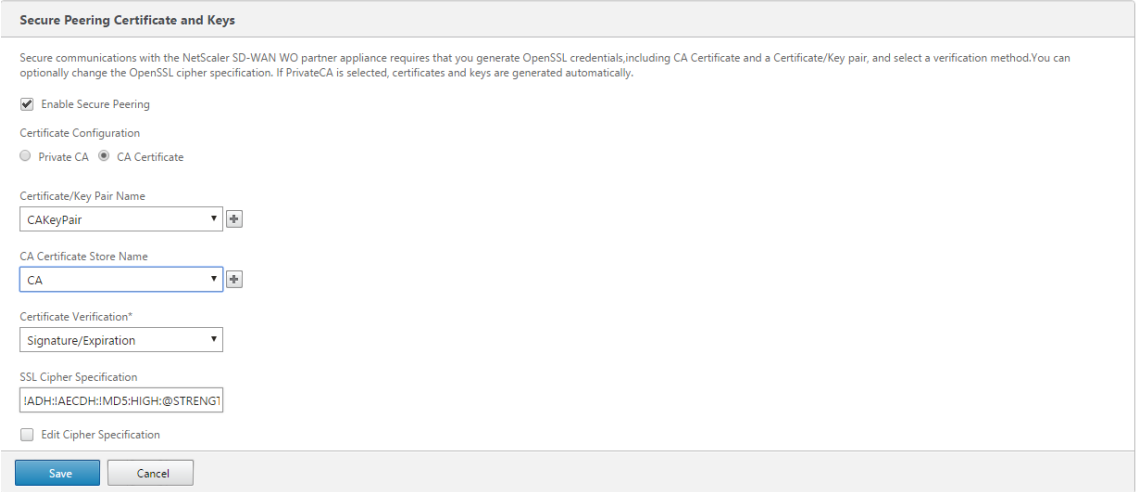


2. 在 DC 站点的新 PE 设备上，在 SD-WAN Web GUI 中，转到 配置 > 安全加速 > 安全对等。

3. 通过提供密钥库密码或禁用密 钥库来配置密钥库。



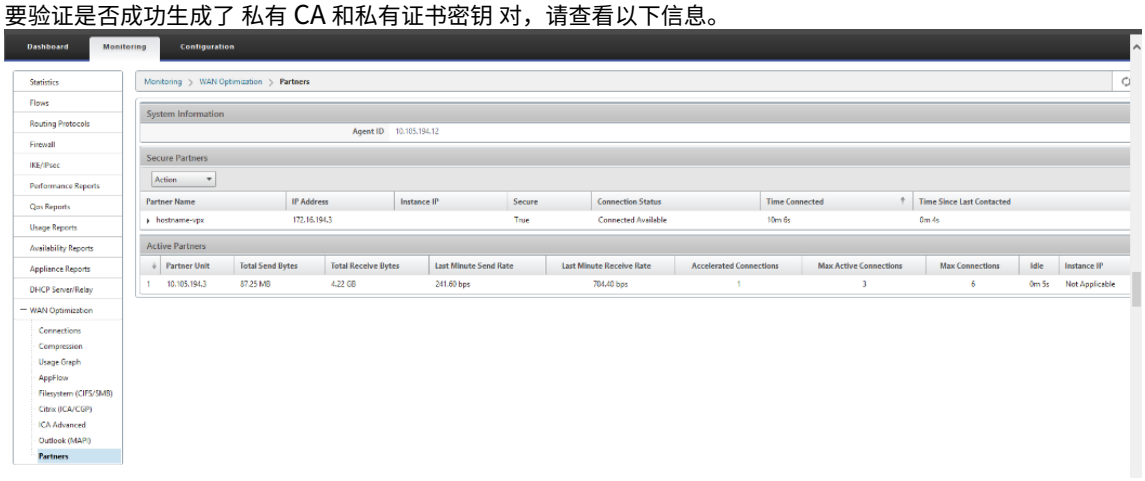
4. 通过选择 **CA** 证书 单选按钮并适当提供上载的 CA 和 CA 密钥对证书，启用安全对等，如下所示。



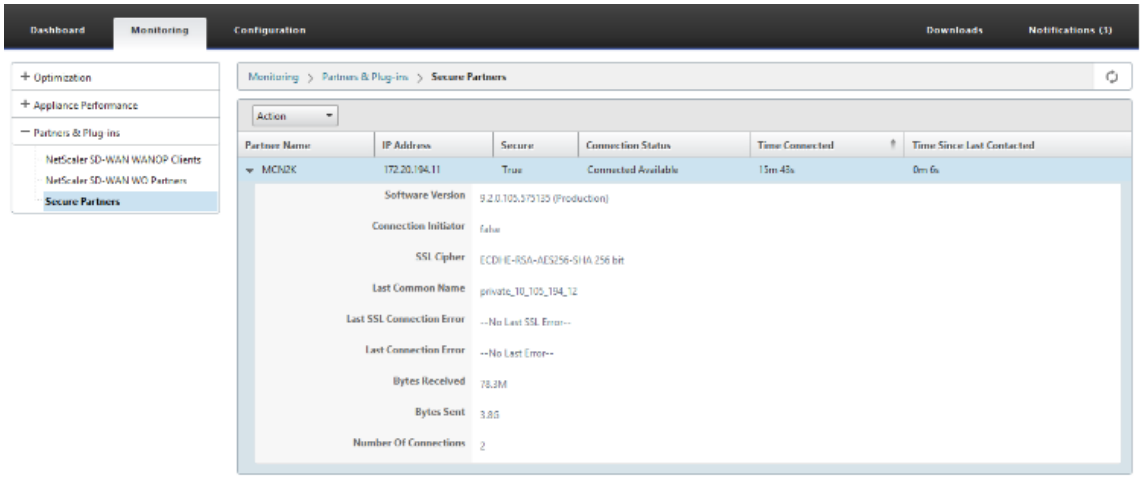
5. 提供远程计算机的虚拟 IP 以及端口 443，如下所示。

监视

1. 要验证是否成功生成了 私有 CA 和私有证书密钥 对，请查看以下信息。

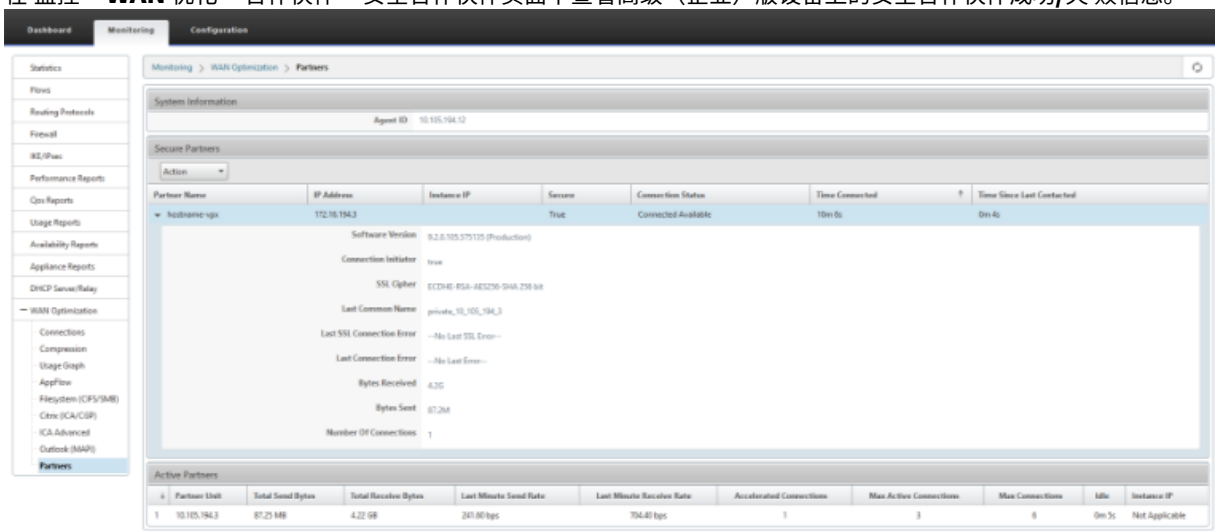


2. 在合作伙伴设备上，在“监视”>“合作 伙伴”>“安全合作伙伴”页面下，查看高级（企业）版设备上的安全合作伙伴信 息。



故障排除

在 监控 > **WAN** 优化 > 合作伙伴 > 安全合作伙伴页面下查看高级（企业）版设备上的安全合作伙伴成功/失 败信息。

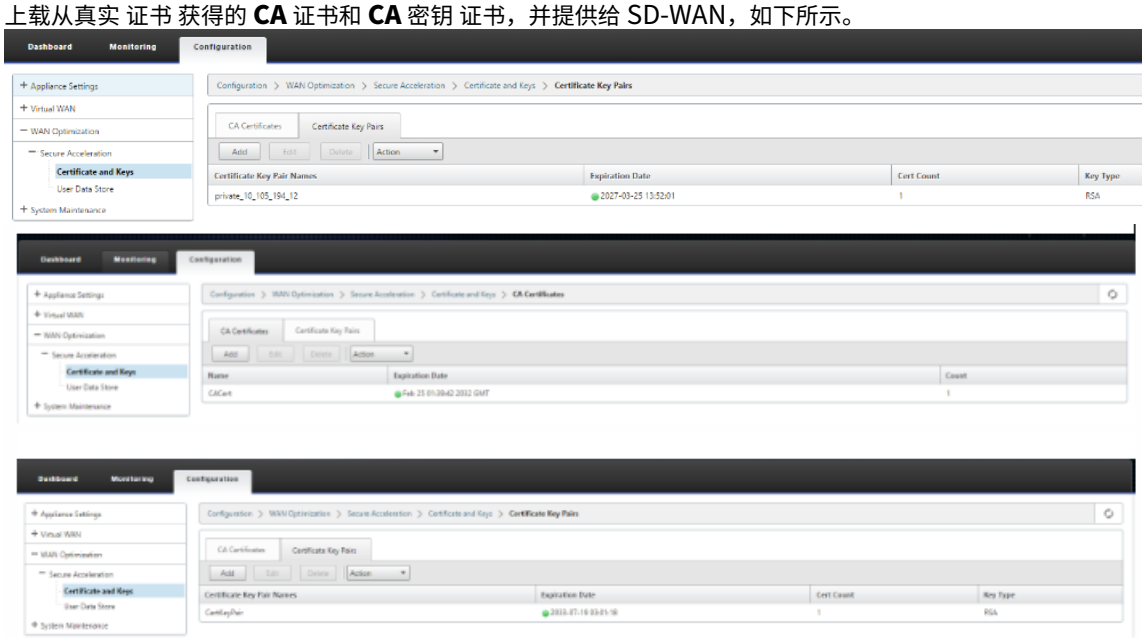


从直流站点的 **PE** 设备到分支机构独立 **SD-WAN SE** 和 **WANOP** 设备的手动安全对等

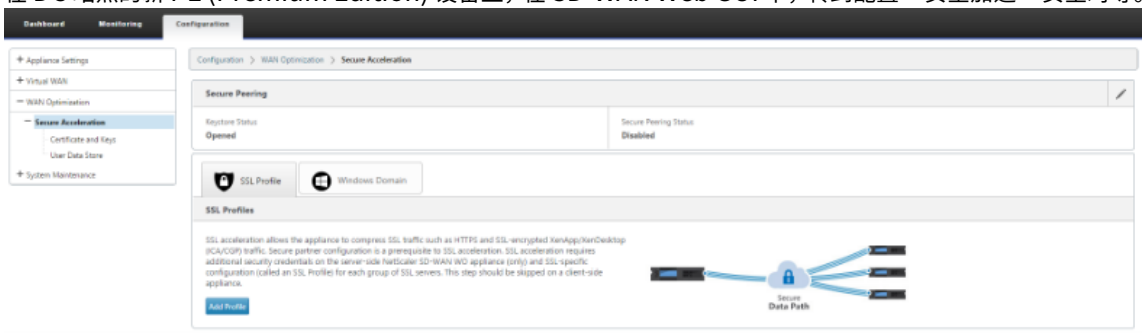
June 22, 2021

- PE 直流设备处于侦听开启模式（端口 443 上）。
- 分支 PE 设备处于连接至模式。
- PE 的 LISTEN-ON IP 位于与启用了“重定向到 WANOP”的路由域关联的接口 IP 中。
- 手动上载从证书颁发机构的真实来源获得的 CA 和证书密钥对证书。

1. 上载从真实 证书 获得的 **CA** 证书和 **CA** 密钥 证书，并提供给 SD-WAN，如下所示。

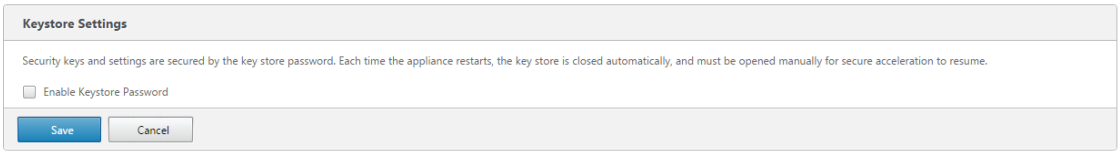


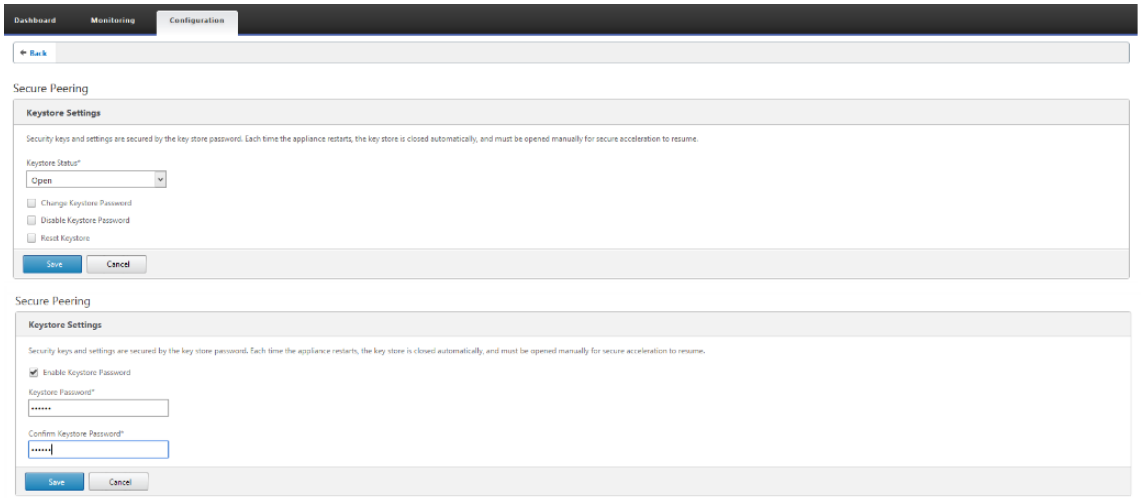
2. 在 DC 站点的新 PE (Premium Edition) 设备上，在 SD-WAN Web GUI 中，转到配置 > 安全加速 > 安全对等。



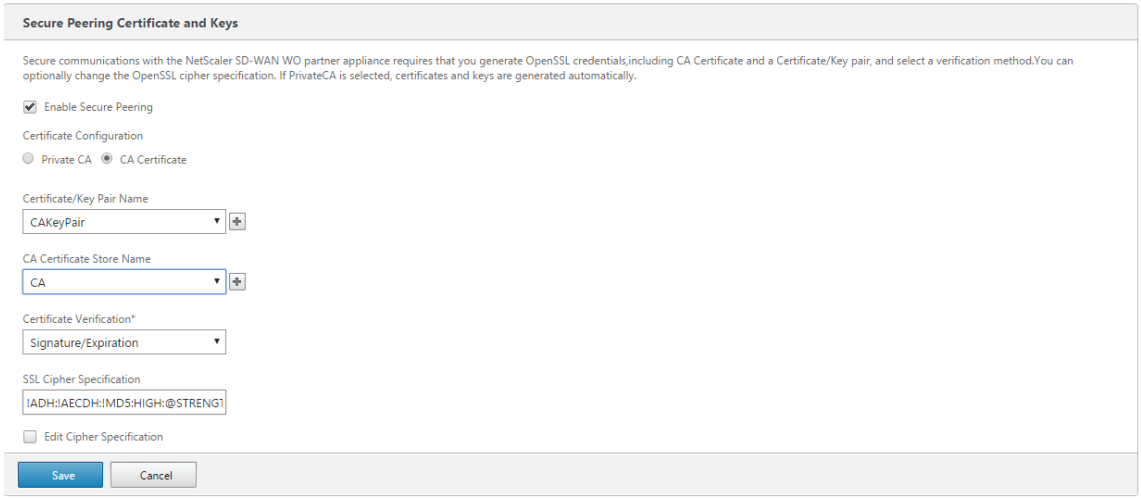
3. 通过提供密钥库 密码或禁用密钥库 来启用密钥库。

Secure Peering

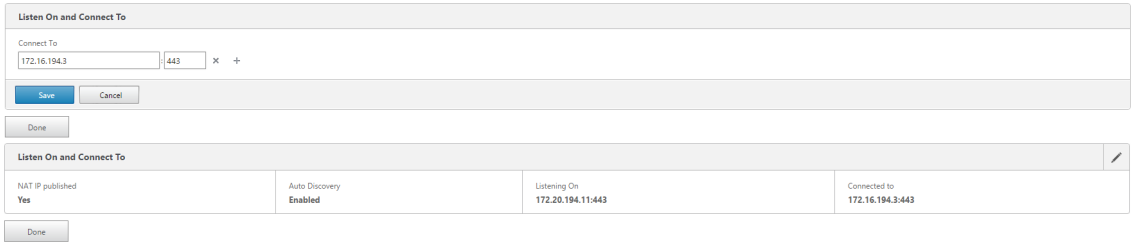




4. 通过选择 **CA** 证书 单选按钮并适当提供上载的 CA 和 CA 密钥对证书，启用安全对等，如下所示。



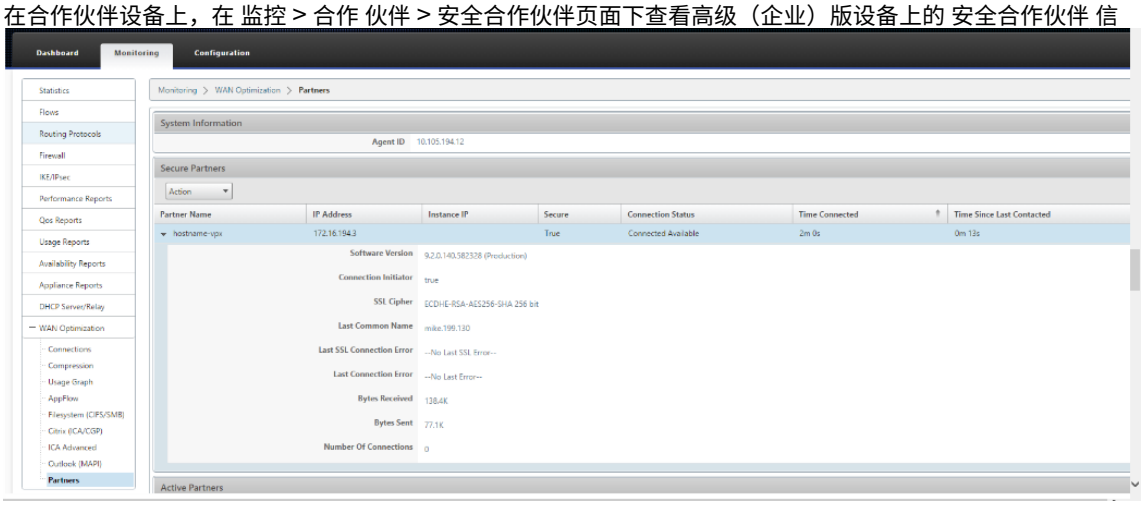
5. 提供远程计算机的虚拟 IP 以及端口 443，如下所示。



监视

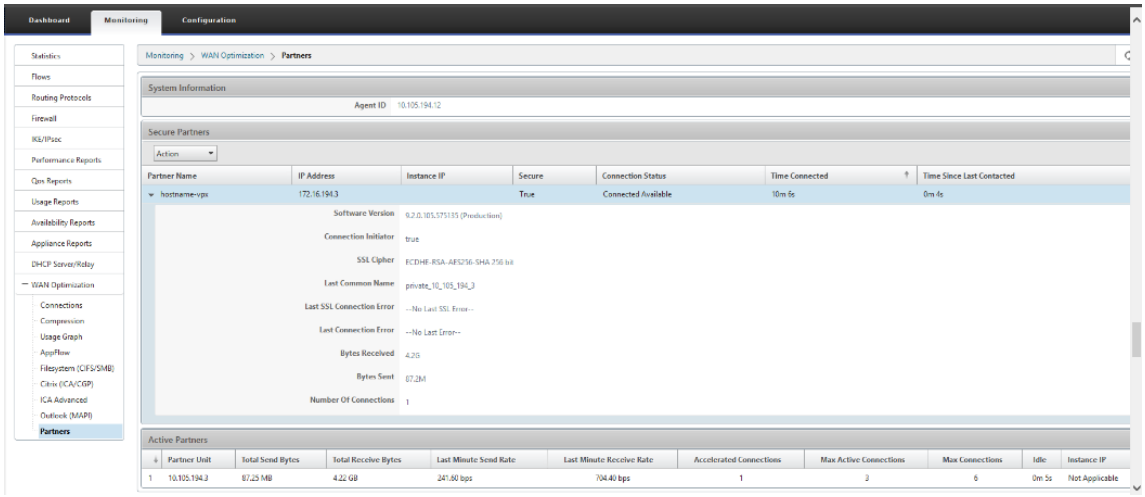
1. 在 监控 > **WAN** 优化 > 合作伙伴页面下查看高级（企业）版设备上的安全合作 伙伴 信息。

2. 在合作伙伴设备上，在 监控 > 合作 伙伴 > 安全合作伙伴页面下查看高级（企业）版设备上的 安全合作伙伴 信

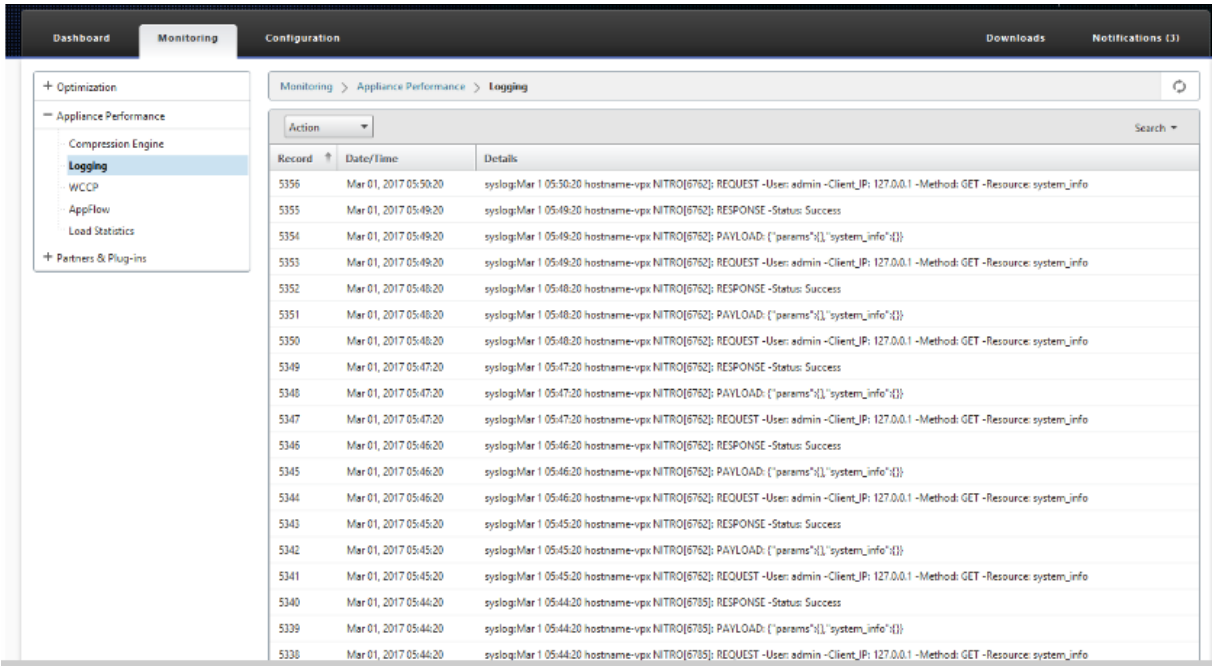


故障排除

1. 在监视 > **WAN** 优化 > 合作伙伴 > 安全合作伙伴页面下查看 Premium (Enterprise) Edition 设备上的安全合作伙伴成功/失败信息。



2. 在合作伙伴设备上，查看高级（企业）版设备上的 监视 > 设 备性能 > 日志记录 页面下的 安全合作伙伴信 息。

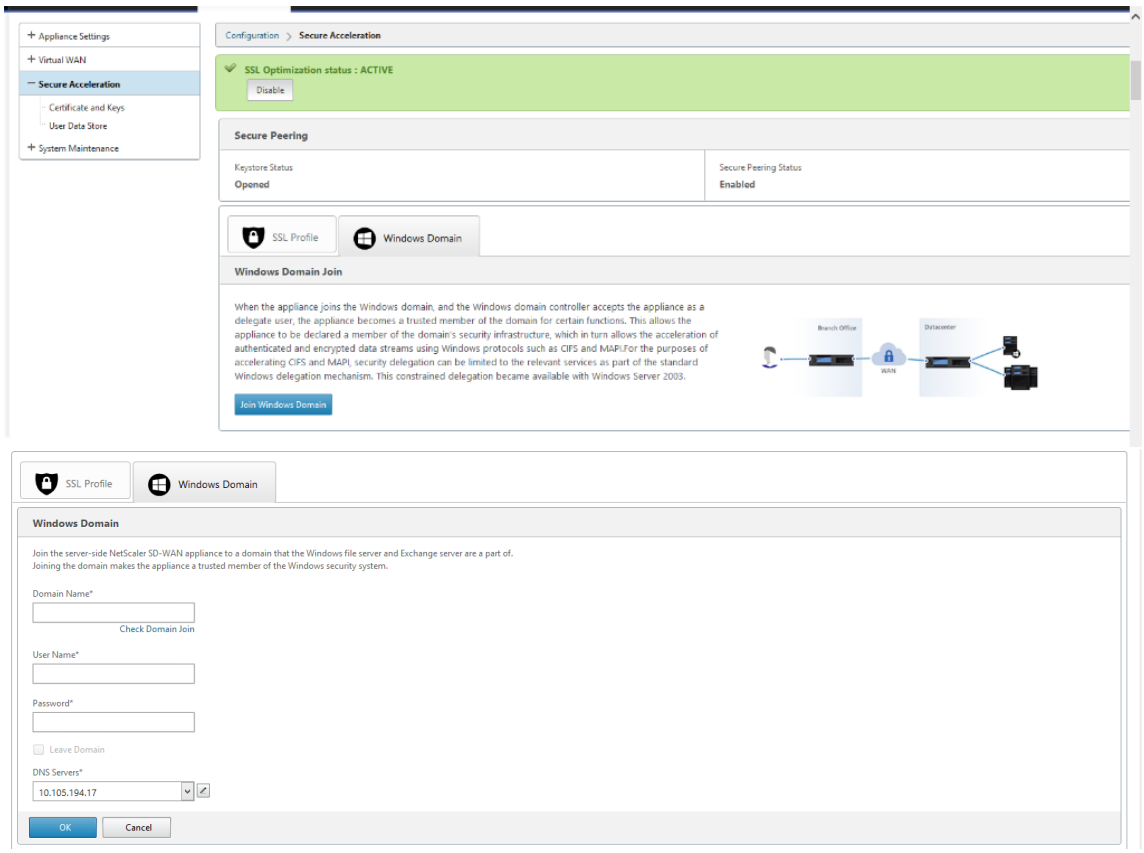


域加入和委托用户创建

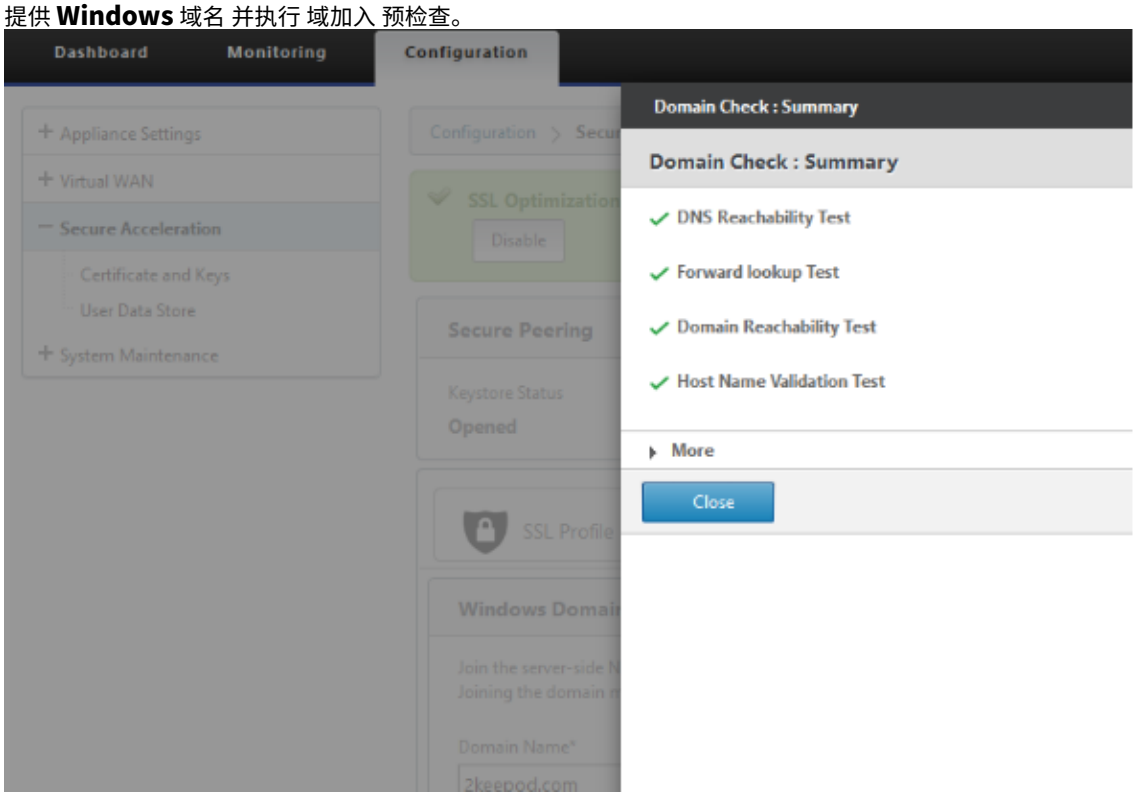
June 22, 2021

要在 **DC** 到 **Windows** 域中配置新的高级（企业）版 **(PE)** 设备，请执行以下操作：

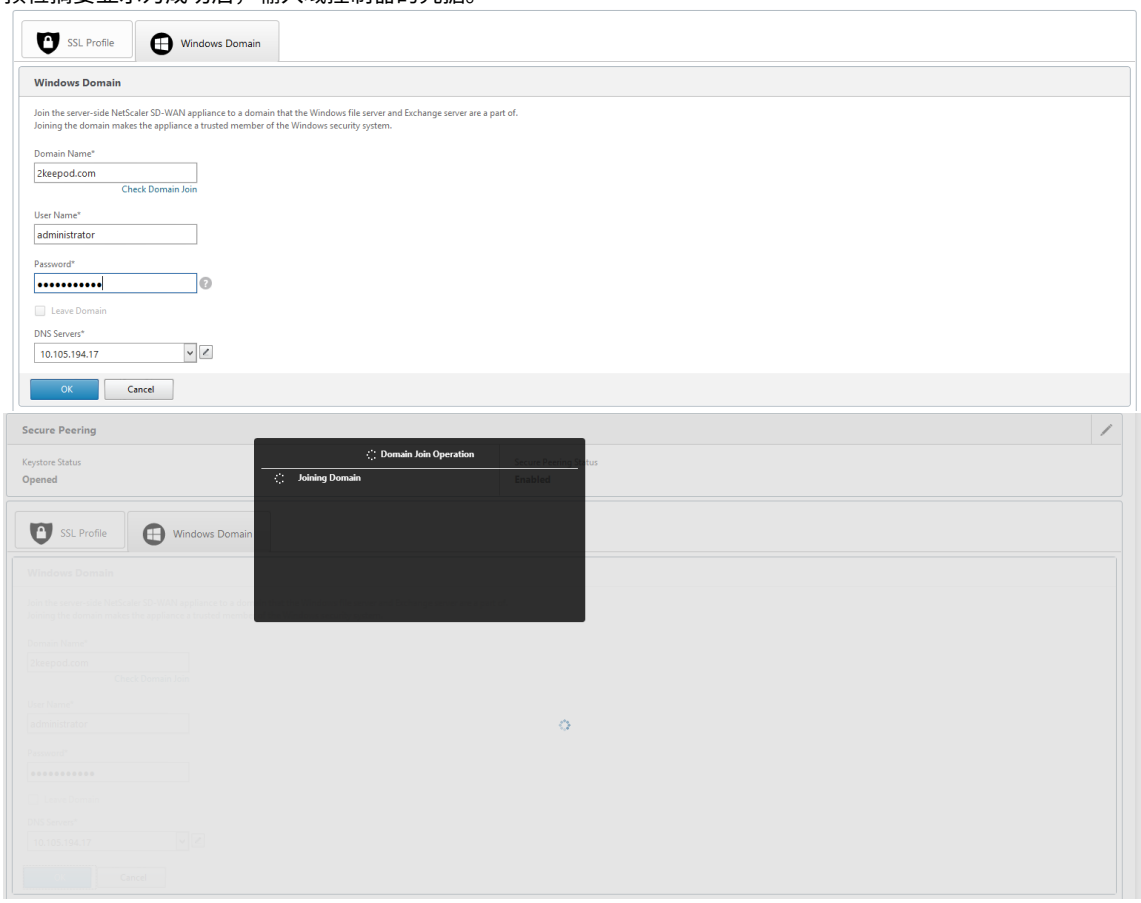
1. 转到 SD-WAN Web GUI 中的 Windows 域，导航到 配置 > 安全加速 >，然后单击加 入 **Windows** 域。



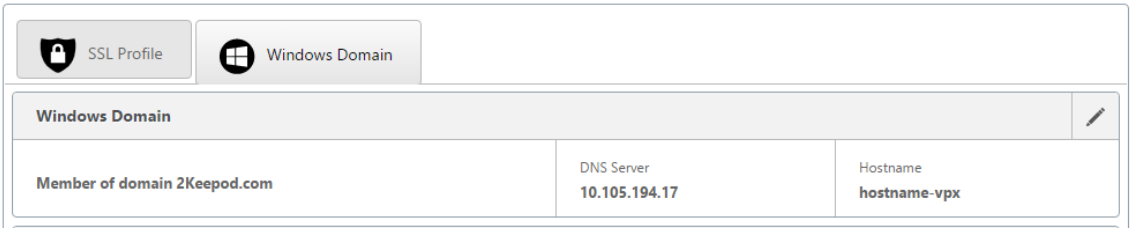
2. 提供 **Windows** 域名 并执行 域加入 预检查。



3. 预检摘要显示为成功后，输入域控制器的凭据。

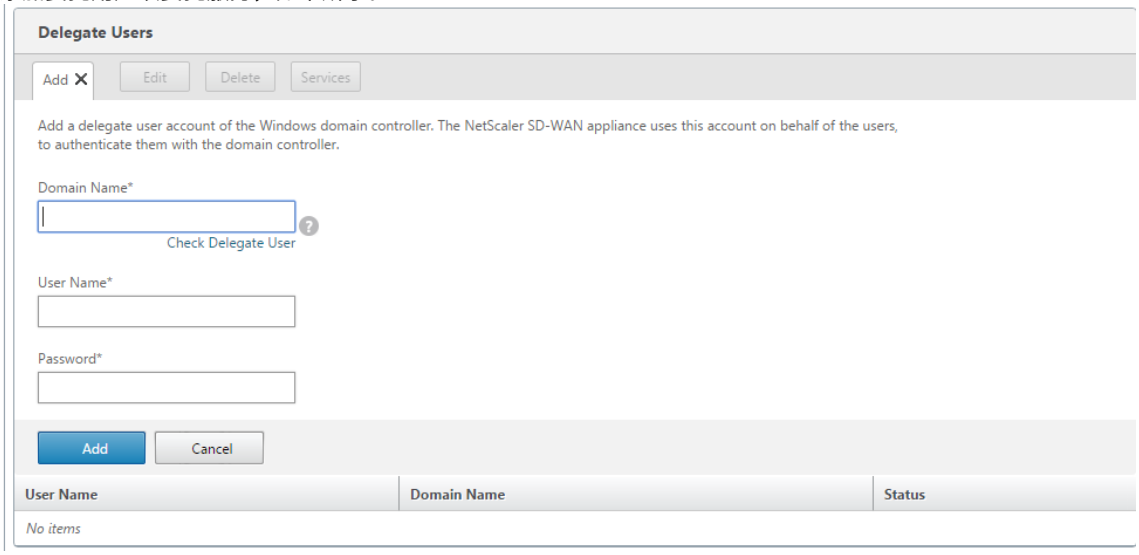


4. 在成功加入域时，您会得到以下输出。

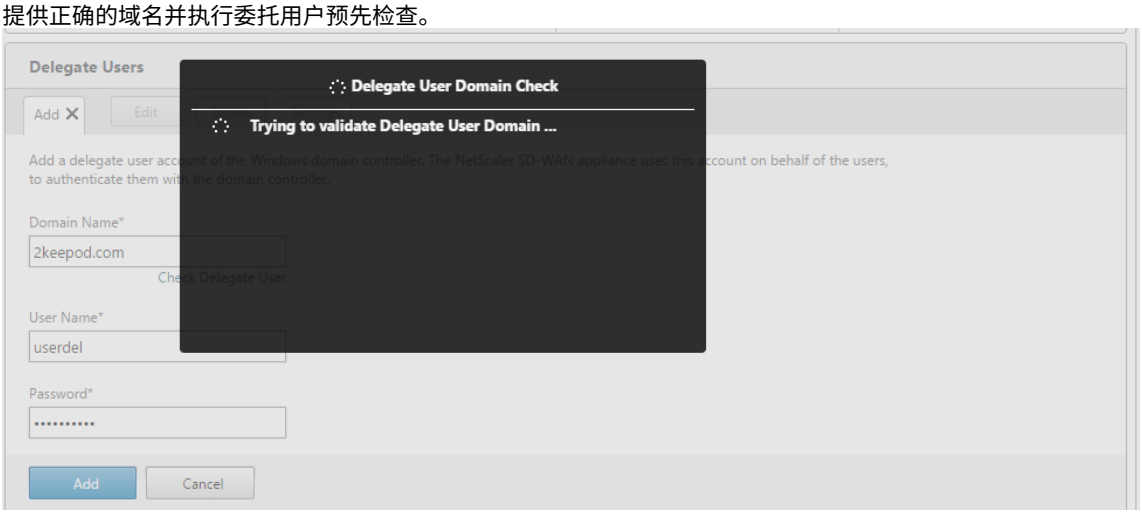


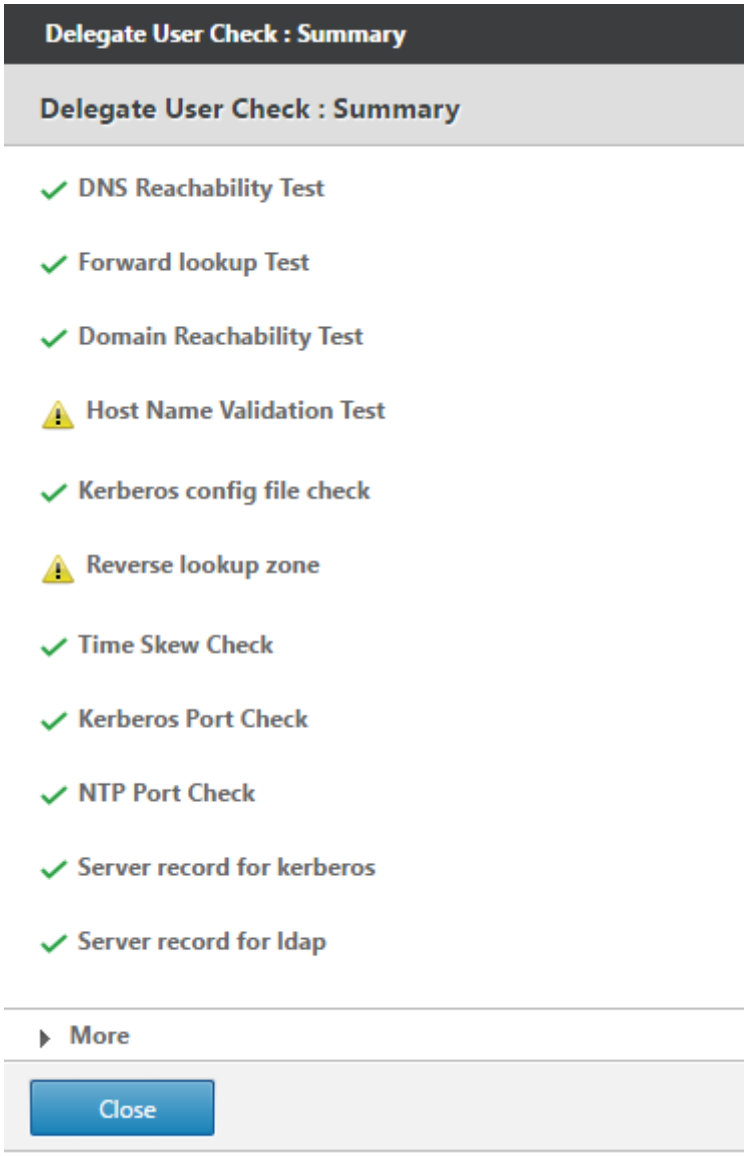
委托用户

1. 添加委托用户以委托服务，如下所示。



2. 提供正确的域名并执行委托用户预先检查。





3. 在委托用户预检成功后，请提供委托用户的有效凭据。

4. 委托用户成功添加到 SD-WAN 后，您会注意到一条成功消息。

5. 要检查委托用户委派的所有服务，请指向该用户并选择服务。

安全

June 22, 2021

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
- 网络安全性
- 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：

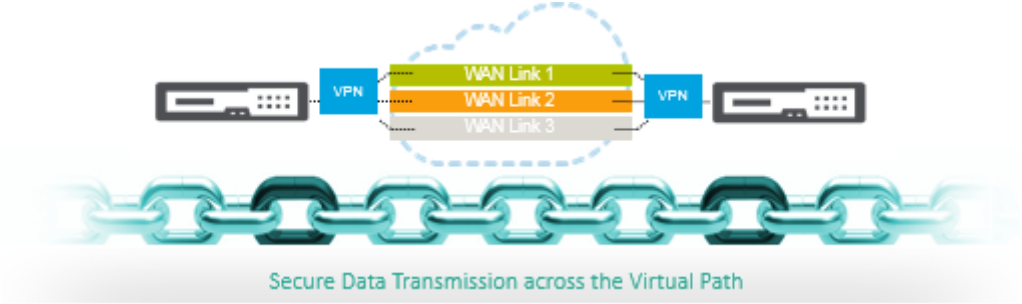
- IPsec 隧道
- 防火墙

IPsec 隧道终止

June 22, 2021

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 LAN 或 WAN 端的 IPsec VPN 隧道。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 隧道终止。

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。



Citrix SD-WAN 与 AWS 传输网关的集成

June 22, 2021

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。使用互联网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）。

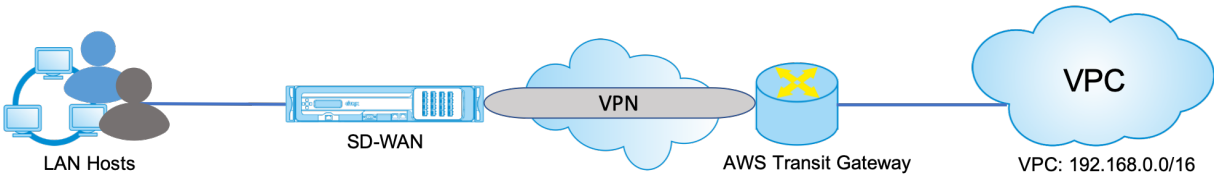
3. 将 VPN 连接到配置的传输网关，其中 VPN 所在的 SD-WAN 站点位于 PREM 或任何云（AWS、Azure 或 GCP）中。
4. 通过 IPsec 隧道与来自 Citrix SD-WAN 的 AWS 传输网关建立边界网关协议 (BGP) 对等，以了解连接到中转网关的网络 (VPC)。

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。

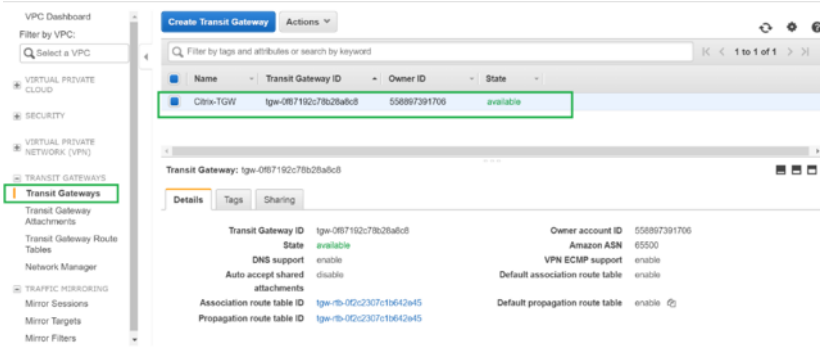


AWS 中转网关配置

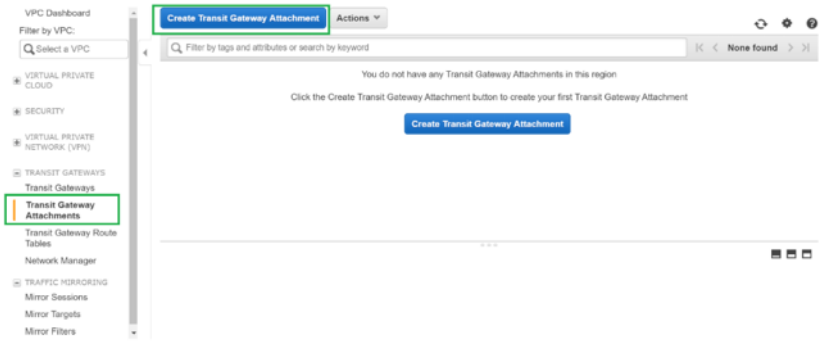
要创建 **AWS Transit Gateway**，请导航到 VPC 控制面板，然后转到中 转网关 部分。

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。

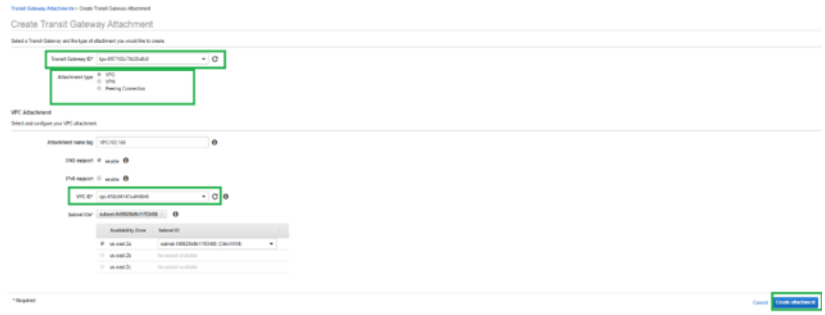
交通网关创建完成后，您可以看到状态为“可 用”。



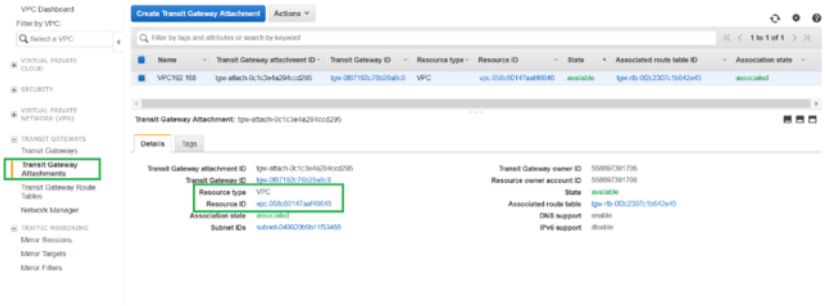
2. 要创建公 交网关附件，请导航到中 转网关 **>** 中转网关附件，然后单击 创建中转网关附件。



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。

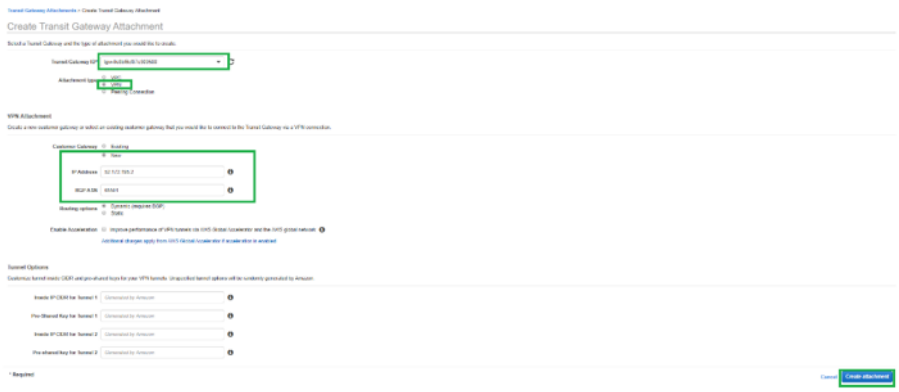


4. 将 VPC 连接到中转网关后，您可以看到 资源类型 **VPC** 已关联到中 转网关。

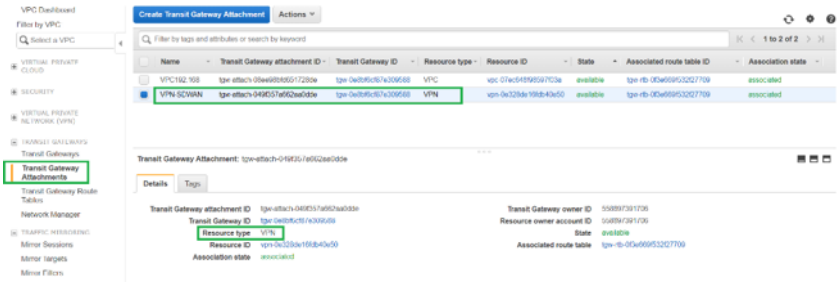


5. 要使用 VPN 将 SD-WAN 连接到中转网关，请从下拉列表中选择中 转网关 **ID** ，然后选择 附件类型 作为 **VPN**。确保您选择了正确的传输网关 ID。

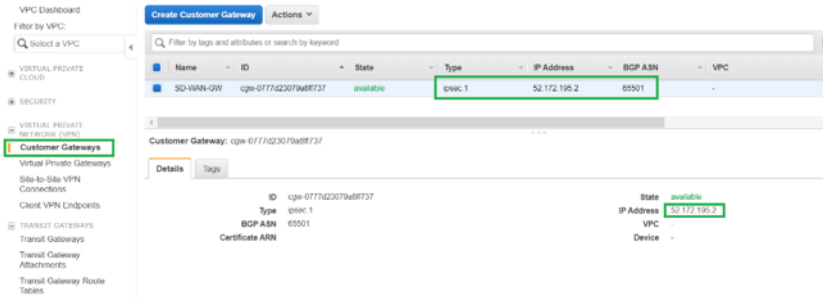
通过提供 SD-WAN 链路公有 IP 地址及其 BGP ASN 编号，连接新的 VPN 客户网关。单击 创建附件 以使用中转网关连接 VPN。



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：

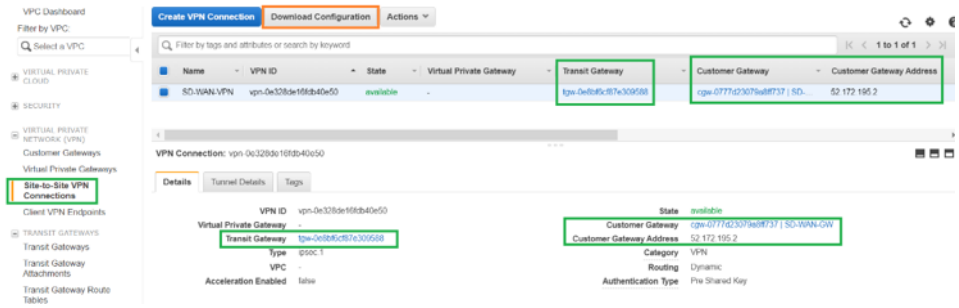


7. 在 客户网关下，SD-WAN 客户网关和站点到站点 VPN 连接是作为连接到中转网关的 VPN 的一部分创建的。您可以看到 SD-WAN 客户网关与此客户网关的 IP 地址一起创建，该地址代表 SD-WAN 的 WAN 链路公有 IP 地址。

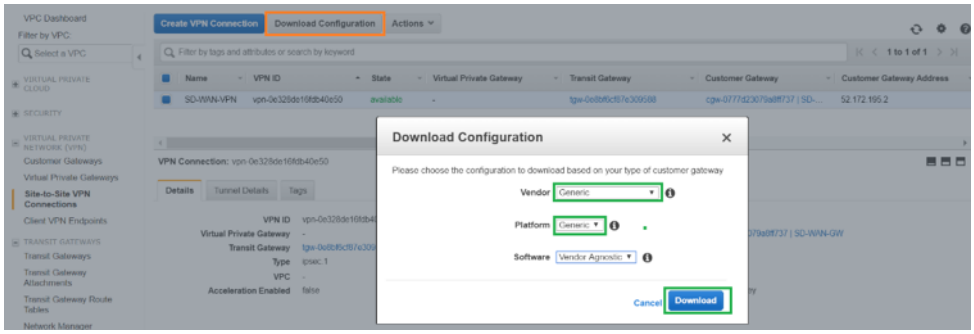


8. 导航 到站点到站点 **VPN** 连接 以下载 **SD-WAN** 客户网关 **VPN** 配置。此配置文件包含两个 IPSec 隧道详细信息以及 BGP 对等信息。从 SD-WAN 到传输网关之间创建两条隧道，以实现冗余。

   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：

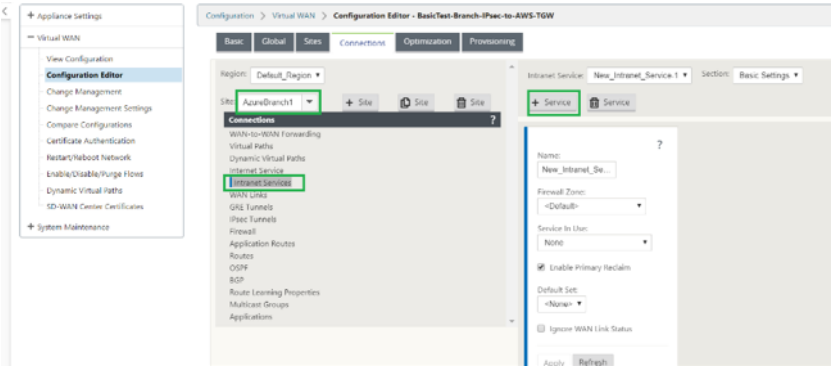
- IKE 配置
- AWS 中转网关的 IPSec 配置
- 隧道接口配置
- BGP 配置

此信息适用于两个 IPSec 隧道以实现高可用性 (HA)。在 SD-WAN 中配置这两个隧道端点时，请确保配置这两个隧道端点。请参阅以下屏幕截图以供参考：

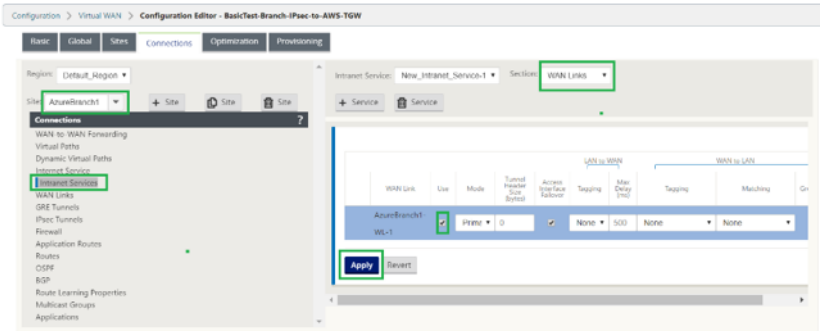
```
#3: Tunnel Interface Configuration

Your Customer Gateway must be configured with a tunnel interface that is
associated with the IPSec tunnel. All traffic transmitted to the tunnel
interface is encrypted and transmitted to the Virtual Private Gateway.


The Customer Gateway and Virtual Private Gateway each have two addresses that relate
to this IPSec tunnel. Each contains an outside address, upon which encrypted
traffic is exchanged. Each also contain an inside address associated with
the tunnel interface.

The Customer Gateway outside IP address was provided when the Customer Gateway
was created. Changing the IP address requires the creation of a new
Customer Gateway.

The Customer Gateway inside IP address should be configured on your tunnel
interface.

Outside IP Addresses:
  - Customer Gateway                  : 52.172.195.2
  - Virtual Private Gateway           : 3.133.37.22

Inside IP Addresses
  - Customer Gateway                  : 169.254.216.178/30
  - Virtual Private Gateway           : 169.254.216.177/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes
```


在 **SD-WAN** 上配置内部网服务

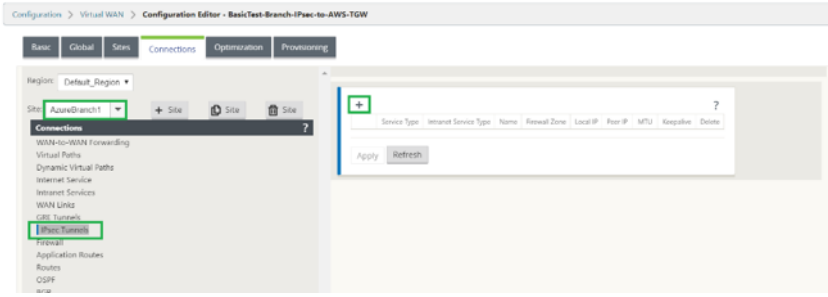
1. 要配置 SD-WAN 上的 IPsec 隧道配置中使用的 Intranet 服务，请导航到 配置编辑器 **>** 连接 **>**，从下拉列表中选择站点，然后选择 **Intranet** 服务。单击 **+** 服务 添加新的内联网服务。



2. 添加 Intranet 服务后，选择用于此服务的 WAN 链接（用于建立通向传输网关的隧道）。

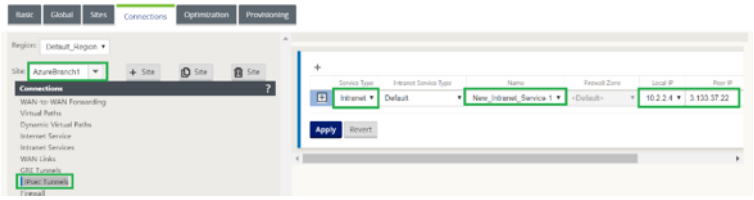


3. 要配置到 AWS Transit Gateway 的 IPsec 隧道，请导航到 配置编辑器 **>** 连接 **>** 从下拉列表中选择站点，然后单击 **IPsec** 隧道。单击 **+** 选项添加 IPsec 隧道。

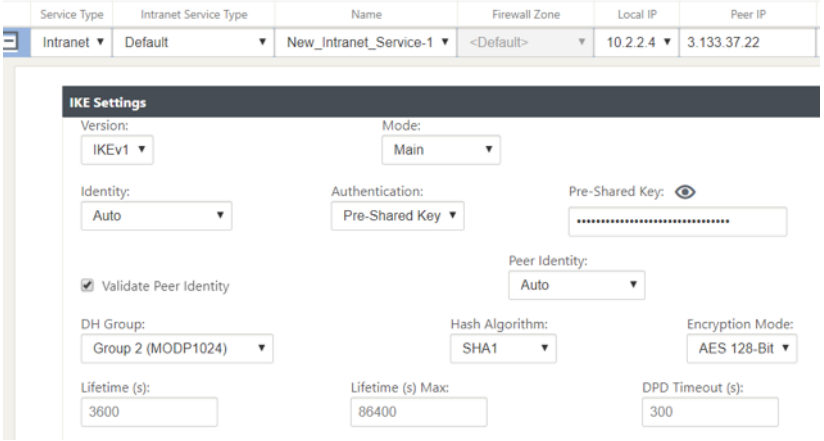


4. 选择 服务类型 作为 **Intranet** ，然后选择已添加的 **Intranet** 服务名称。选择本 地 **IP** 地 址作为 WAN 链路 IP 地址，选择 对等 地址作为中转网关虚拟专用网关 IP 地址。

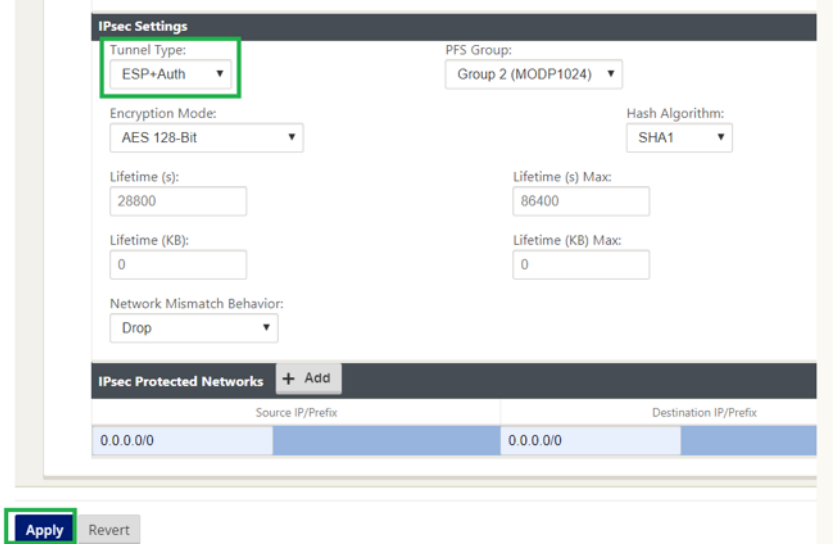
   单击 **Keepalive** 复选框可让 SD-WAN 在配置激活后立即启动隧道。



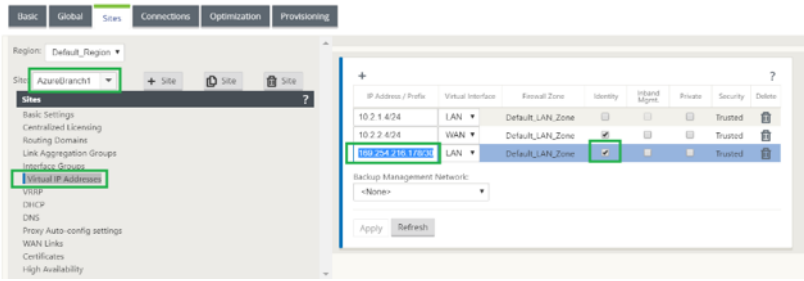
5. 根据您从 AWS 下载的 VPN 配置文件配置 IKE 参数。



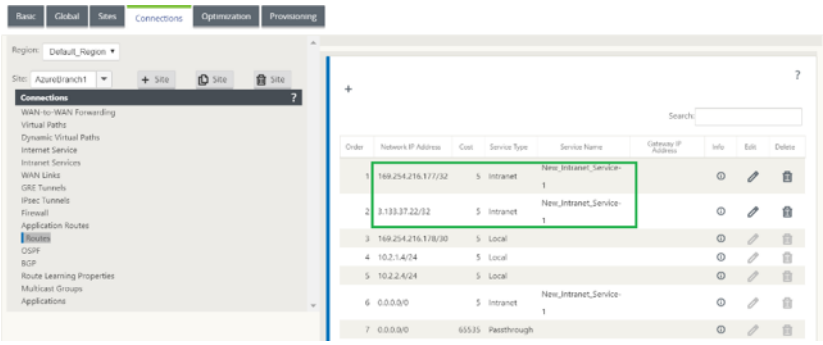
6. 根据您从 AWS 下载的 VPN 配置文件配置 IPSec 参数。还可以根据要通过隧道发送的网 络配置 **IPsec** 受保护的网络。您可以看到它已配置为允许通过 IPsec 隧道的任何流量。



7. 将 客户网关内部 **IP** 地址 配置为 SD-WAN 上的虚拟 IP 地址之一。从下载的 VPN 配置文件中，找到与 Tunnel-1 相关的 IP 地址内的客户 Gateway。将此客户网关在 IP 地址内配置为 SD-WAN 上的虚拟 IP 地址之一，然后启用 身份 复选框。

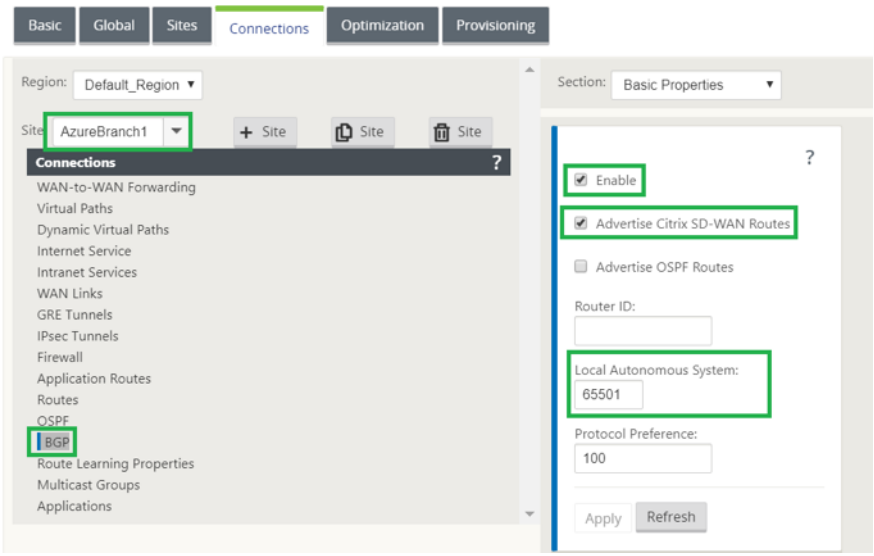


8. 在 SD-WAN 上添加 路由 以访问中转 网关的虚拟专 用网关。从下载的 VPN 配置文件中，找到与 Tunnel-1 相关的虚拟专用网关的内部和外部 IP 地址。将 服务类型 作为 **In** tranet 的虚拟专用网关的内部和外部 IP 地址添加路由，然后选择在上述步骤中创建的 Intranet 服务。



9. 在 SD-WAN 上配置 **BGP** 。使用适当的 ASN 编号启用 BGP。从下载的 VPN 配置文件中，找到与隧道-1 相关的 BGP 配置选项。使用这些详细信息在 SD-WAN 上添加 BGP 邻居。

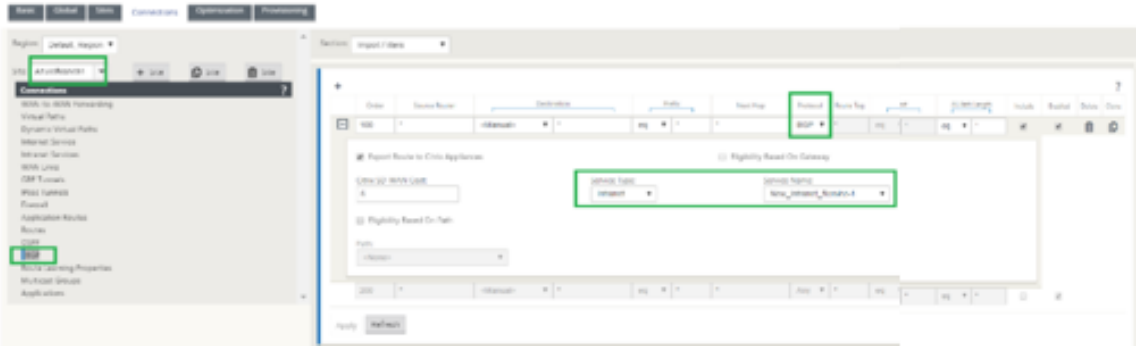
   要在 SD-WAN 上启用 BGP，请导航到 连接 从下拉列表中选择站点，然后选择 **BGP**。单击 启用 复选框以启用 BGP。单击 通告 **Citrix SD-WAN** 路由 复选框以向中转网关通告 SD-WAN 路由。使用 BGP 配置选项中的 客户网关 **ASN** 并将其配置为 本地自治系统。



10. 要在 SD-WAN 上添加 BGP 邻居，请导航到 连接 **>** 从下拉列表中选择站点，然后选择 **BGP**。单击 邻居 部分，然后单击 **+** 选项。

添加 邻居时，使用 **BGP** 配置选项中的邻居 **IP** 地址 和 虚拟专用网关 **ASN** 。源 **IP** 必须与从 AWS 下载的配置文件中的 IP 地址（配置为 SD-WAN 上的虚拟 IP 地址）内的 客户网 关匹配。添加在 SD-WAN 上启用了 多跳 的 BGP 邻居。

11. 要添加 导入筛 选器以将 BGP 路由导入 SD-WAN，请导航到 连接，从下拉列表中选择站点，然后选择 **BGP** 并单击 导入筛选器 部分。单击 **+** 选项添加导入过滤器。选择 协议 作为 **BGP** 并匹配任何协议以导入所有 BGP 路由。选择 服务类型 作为 **Intranet** ，然后选择创建的 Intranet 服务。这是将具有服务类型的 BGP 路由导入为内部网。

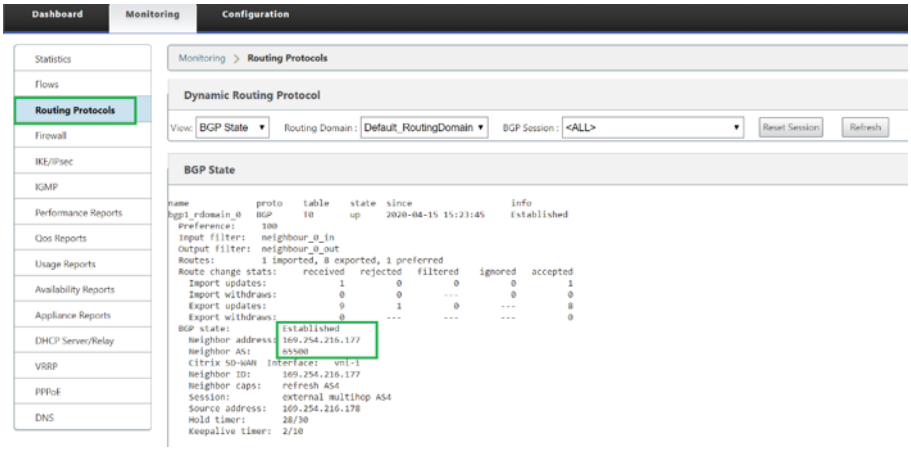


SD-WAN 上的监控和故障排除

1. 要验证 SD-WAN 上的 IPsec 隧道建立状态，请导航到 监控 **>** 统计 **> IPsec** 隧道。在以下屏幕截图中，您可以看到 IPsec 隧道是从 SD-WAN 向 AWS Transit Gateway 建立的，状态为 良好。
   此外，您还可以监视通过此 IPsec 隧道发送和接收的通信量。

   ！[SD-WAN 上的监控和故障排除] (/en-us/citrix-sd-wan/current-release/media/monitoring-and-troubleshooting-on-sdwan.png)

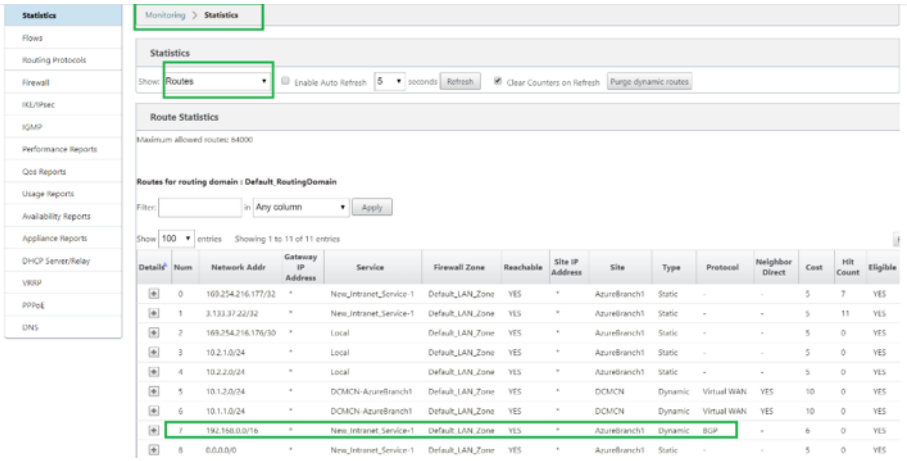
2. 要验证 SD-WAN 上的 **BGP** 对等互 连状态，请导航到 监视 **>** 路由协议，然后选择 **BGP** 状态。您可以看到 BGP 状态报告为 已建立，邻居 **IP** 地址 和 邻居 **ASN** 与 AWS BGP 邻居详细信息匹配。有了这一点，您可以确保通过 IPsec 隧道从 SD-WAN 到 AWS 传输网关建立 BGP 对等互连。



VPC (192.168.0.0) 连接到 AWS 中转网关。SD-WAN 已经通过 BGP

从 AWS Transit Gateway 了解此 VPC 网络 (192.168.0.0)，此路由根据上述步骤中创建的导入筛选器，安装在服务类型为 Intranet 的 SD-WAN 上。

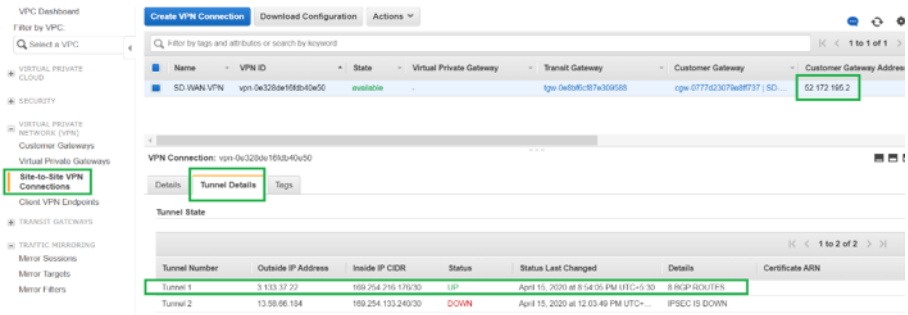
3. 要验证 SD-WAN 上的 BGP 路由安装，请导航到 监控 **>** 统计 **>** 路由，然后检查安装为 BGP 路由且服务类型为 Intranet 的网络 192.168.0.0/16。这意味着您可以了解连接到 AWS 传输网关的网络，并可以通过建立的 IPsec 隧道与这些网络进行通信。



AWS 上的监控和故障排除

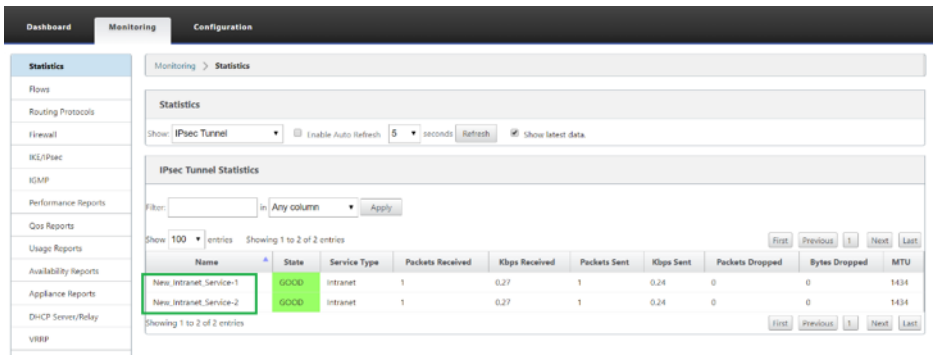
1. 要验证 AWS 上的 IPsec 隧道建立状态，请导航到 虚拟专用网络 **(VPN) >** 站点到站点 **VPN** 连接。在以下屏幕截图中，您可以看到客户网关地址代表 SD-WAN 链路公有 IP 地址，您已使用该地址建立了隧道。

   隧道状态显示为 **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 中转网关建立隧道，并能够通过 BGP 交换路由。

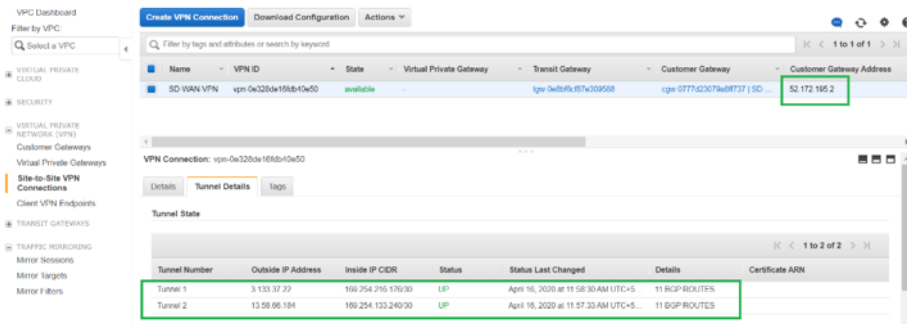


2. 根据 SD-WAN 上下载的配置文件，配置与第二条隧道相关的 IPSec 和 BGP 详细信息。

   可以在 SD-WAN 上监控与两条隧道相关的状态，如下所示：



3. 可以在 AWS 上监控与两个隧道相关的状态，如下所示：

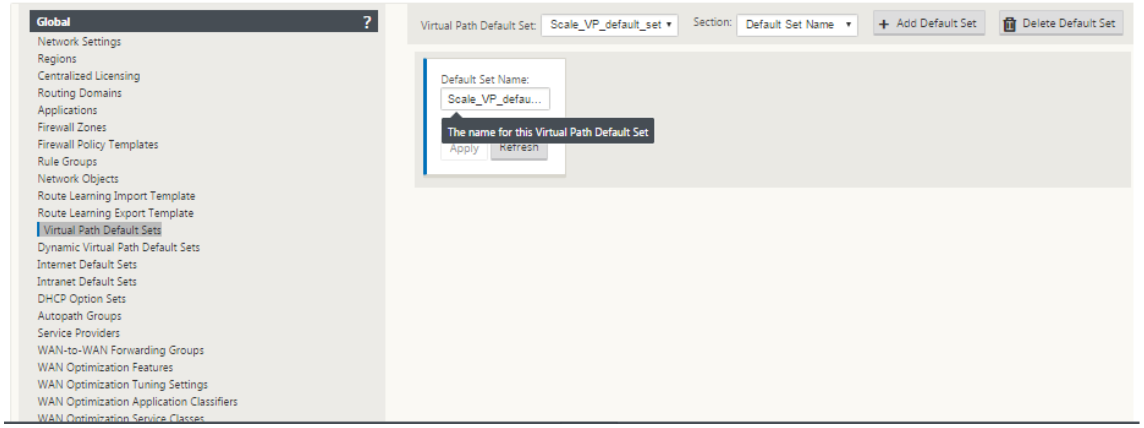


如何为虚拟和动态路径配置 **IPsec** 通道

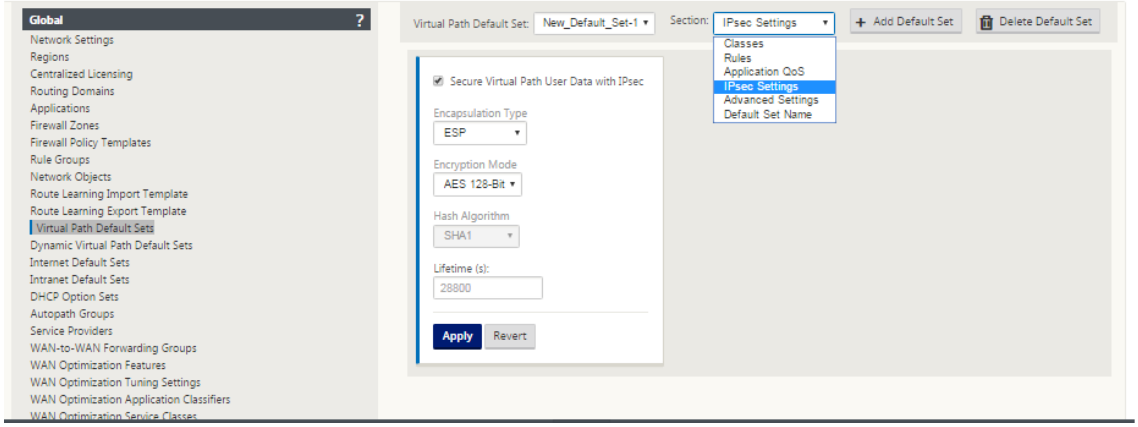
June 22, 2021

要为 Citrix SD-WAN 分支站点之间的虚拟和动态虚拟路径配置 IPsec 隧道，请执行以下操作：

1. 导航到 全局 **>** 虚拟路径默认集 或 动态虚拟路径默认集。



2. 创建新的默认集（虚拟或动态虚拟路径），并使用 **IPsec** 启用安全虚拟路径用户数据。
3. 选择 IPsec 加密的可用选项之一：
   - 封装类型：ESP、AH 或 ESP+AH
   - 加密模式：AES-CBC、AES 128 或 256 位
   - 哈希算法：SHA1 或 SHA-256
4. 将创建的虚拟路径默认集应用于 MCN 节点。这会自动将相同的默认设置应用到具有 MCN 虚拟路径的所有客户端节点。



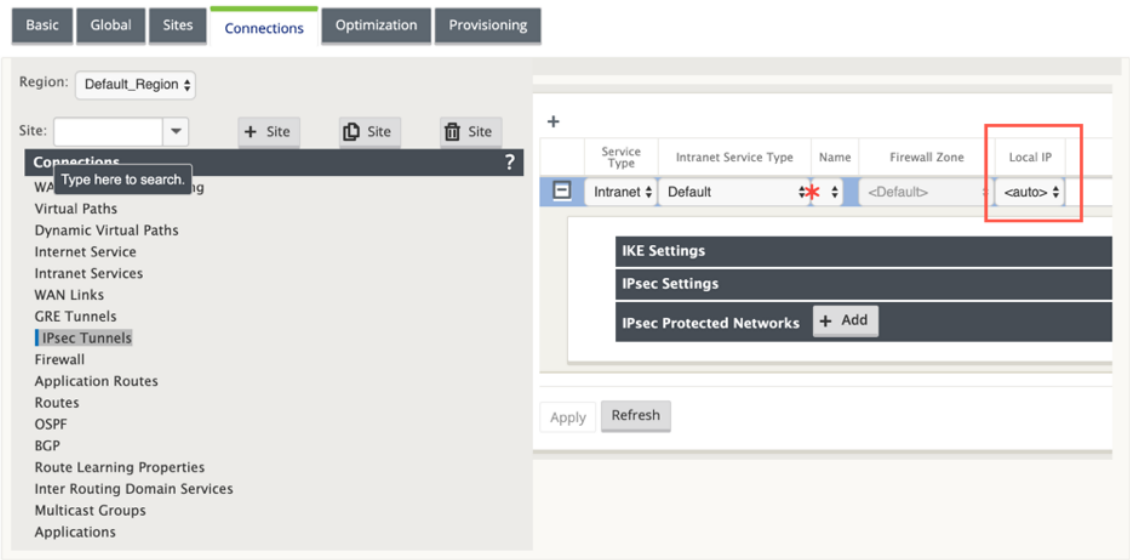
如何在 **SD-WAN** 和第三方设备之间配置 **IPsec** 隧道

November 1, 2021

要为内部网或局域网服务配置 IPsec 隧道，请执行以下操作：

1. 在 配置编辑器中，导航到 连接 > 查看站点 > **[**站点名称**]**> **IPsec** 隧道。选择 服务类型（局域网或内部网）。

2. 输入服务类型的 名称。对于 Intranet 服务类型，配置的 Intranet 服务器将确定哪些本地 IP 地址可用。



如果 WAN 链路在设备上直接终止，并且向 WAN 链路分配了动态 IP，Citrix SD-WAN 现在可以建立 IPsec 隧道。

在 11.1.0 版本中，当本地隧道 IP 地址不知道或无法知道时，必须可配置 Intranet IPsec 隧道。这有助于在通过 DHCP 分配地址的接口上创建 IPsec 隧道。

在为 IPsec 隧道配置接口时，必须提及本地隧道 IP。此接口被修改为允许在隧道类型为 **Intranet** 时选择空 IP。

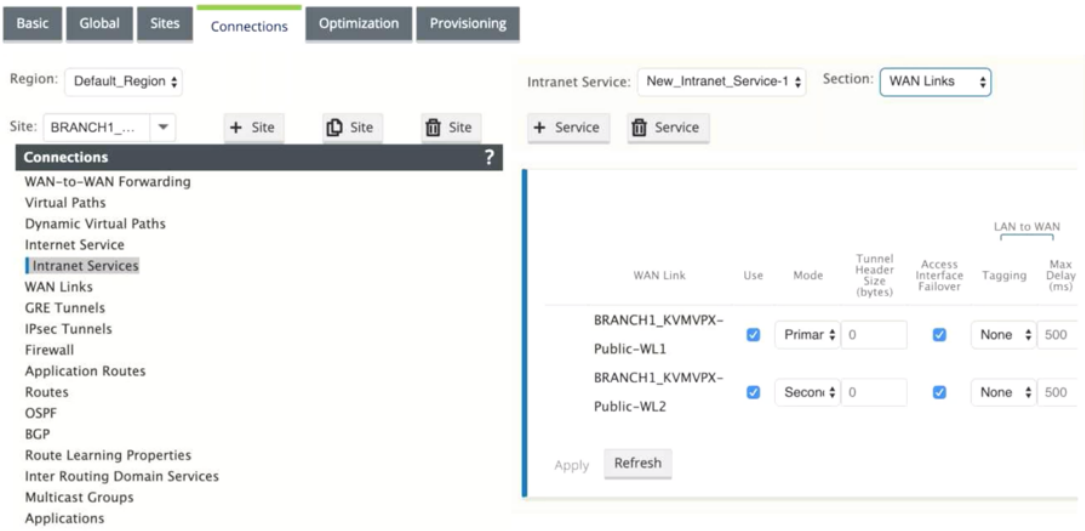
此外，当隧道类型为 **Intranet** 时，未设置地址的标签将更改为 自动。

如果本地 IP 设置为 自动，则它能够获取为该 WAN 链路上的接入接口合并的 IP 地址。该 WAN 链路访问接口可能会静态配置或从 DHCP 获取 IP。默认情况下，IPsec 隧道是使用主 WAN 链路访问接口建立的。

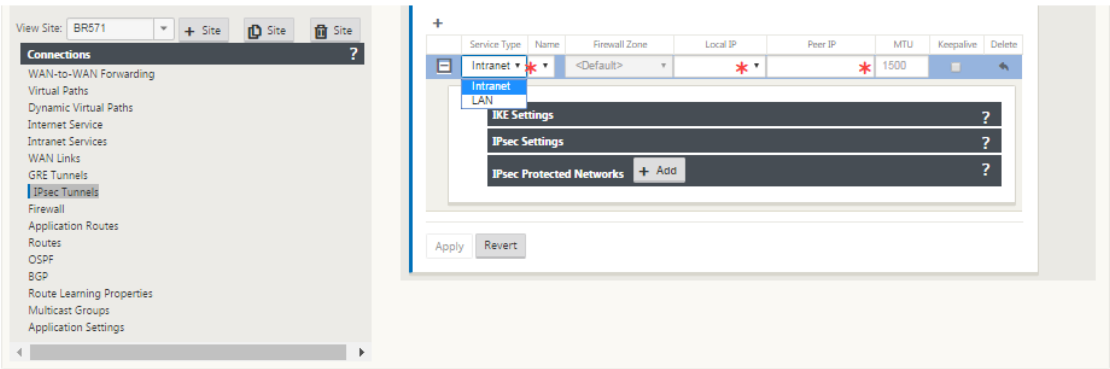
之前，您可以通过单个 WAN 链路建立 IPSec 隧道。这会使分支环境在完全链路故障期间以及在链路上的数据包丢失过高以实现可靠连接时出现服务丢失。

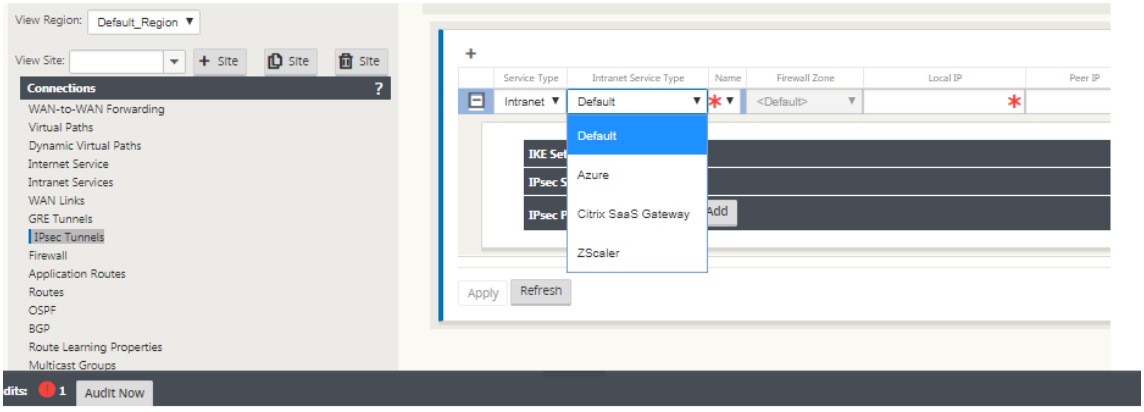
从 11.1.0 版本开始，您可以使用两个 WAN 链路建立 IPsec 隧道，以保护分支机构环境免受服务中断的影响。如果主链路断开，辅助链路会在毫秒内变为活动/向上。

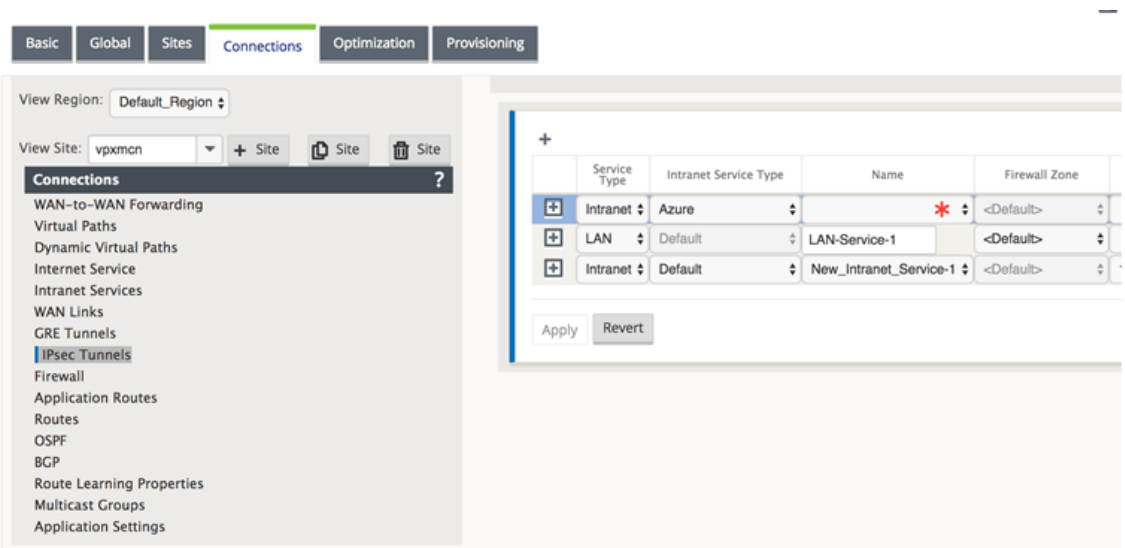
> 注意
>
> 如果选择 < 自动 > 选项，则使用主 WAN 链接访问接口建立 IPsec 隧道。如果主 WAN 链路关闭，则使用辅助 WAN 链路访问接口建立 IPsec 隧道。



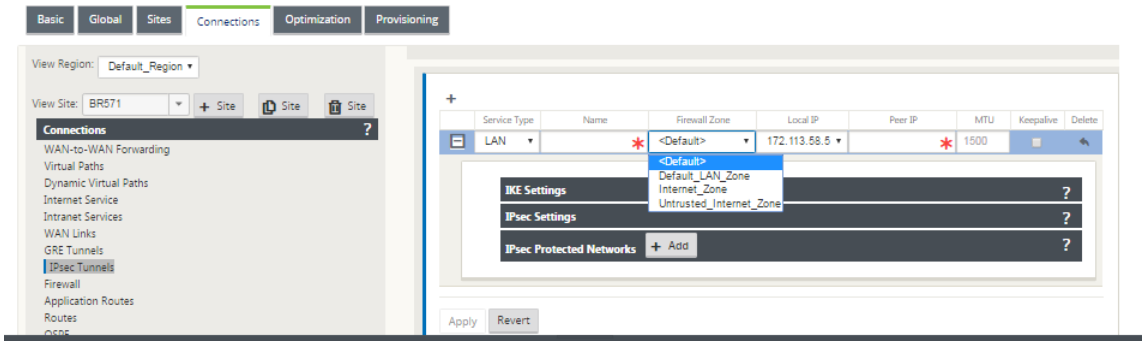
3. 选择可用的 本地 **IP** 地 址，然后输入 IPsec 隧道的 对等 **IP** 地址。







> 注意
>
> 如果服务类型是 Intranet，则 IP 地址由所选 Intranet 服务预先确定。

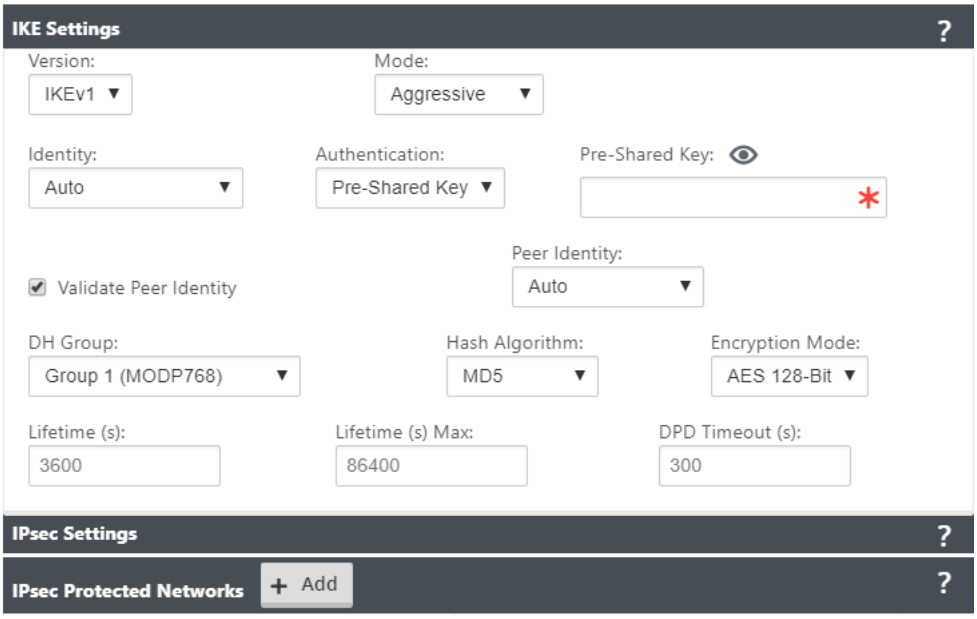


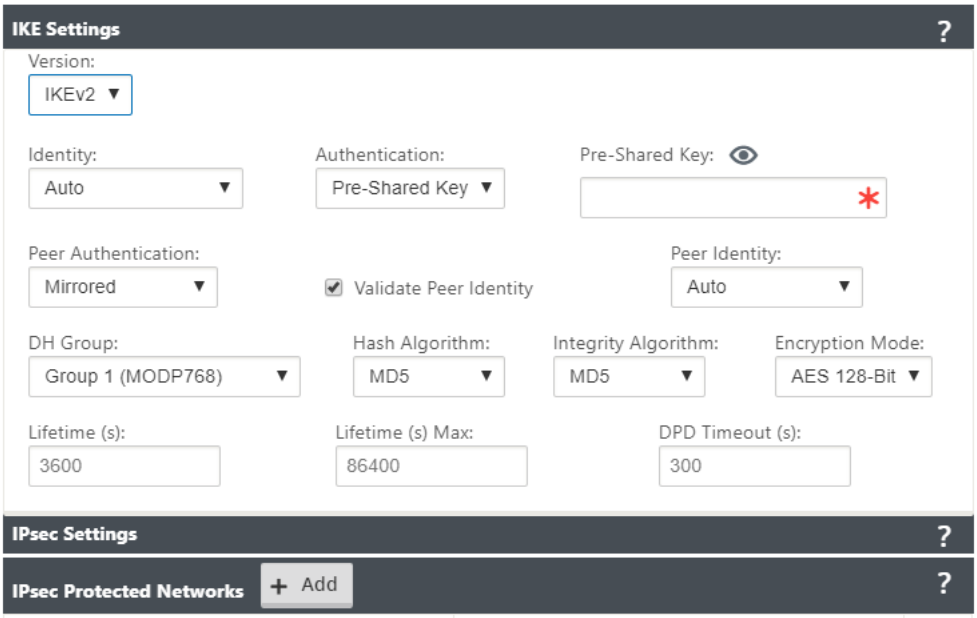
4. 通过应用下表中描述的条件来配置 IPsec 设置。完成后，单击 应用 以保存设置。

字段	说明	值
服务类型	从下拉菜单中选择服务类型	内联网、局域网
名称	如果服务类型为 Intranet，请从下拉菜单中的已配置 Intranet 服务列表中进行选择。如果服务类型为 LAN，请输入唯一名称	文本字符串
本地知识产权	从此站点配置的可用虚拟 IP 地址下拉菜单中选择 IPsec 隧道的本地 IP 地址	IP 地址
对等 IP	输入 IPsec 隧道的对等 IP 地址	IP 地址

字段	说明	值
MTU	输入 **MTU** 以对 IKE 和 IPSec 片段进行分段	默认值：1500
IKE 设置	版本：从下拉菜单中选择 IKE 版本	IKEv1 IKEv2
模式	从下拉菜单中选择模式	符合 FIPS 标准：主要、不符合 FIPS 标准：侵略性
身份	从下拉菜单中选择身份	自动 IP 地址手动 IP 地址用户 FQDN
身份验证	从下拉菜单中选择身份验证类型	预共享密钥：如果您使用的是预共享密钥，请将其复制并粘贴到此字段中。单击眼球 () 图标可查看预共享密钥。证书：如果您使用的是身份证书，请从下拉菜单中选择该证书。
验证对等标识	选中此复选框可验证 IKE 的对等项。如果对等体的 ID 类型不受支持，请不要启用此功能	无
DH Group	从下拉菜单中选择 Diffie-Hellman 组用于 IKE 密钥生成	不符合 FIPS 标准：组 1、FIPS 合规：组 2 组 5 组 14 组 15 组 16 组 19 组 20 组 21
哈希算法	从下拉菜单中选择一种算法来验证 IKE 消息	不符合 FIPS 要求：符合 MD5 FIPS 要求：SHA1 SHA-256
加密模式	从下拉菜单中选择 IKE 消息的 加密模式	AES 128 位 AES 192 位 AES 256 位
生命周期（秒）	输入 IKE 安全关联存在的首选持续时间（以秒为单位）	3600 秒（默认值）
最大使用寿命	输入允许存在 IKE 安全关联的最大首选持续时间（以秒为单位）	86400 秒（默认值）
DPD 超时	输入 VPN 连接的 死对等检测超时（以秒为单位）	300 秒（默认值）
IKEv2	对等验证：从下拉菜单中选择 对等身份验证	镜像预共享密钥证书
IKE2-预共享密钥	对等预共享密钥：将 IKEv2 对等预共享密钥粘贴到此字段中以进行身份验证。单击眼球 () 图标查看预共享密钥	文本字符串
完整性算法	从下拉菜单中选择一个算法作为用于 HMAC 验证的哈希算法	不符合 FIPS 要求：符合 MD5 FIPS 要求：SHA1 SHA-256

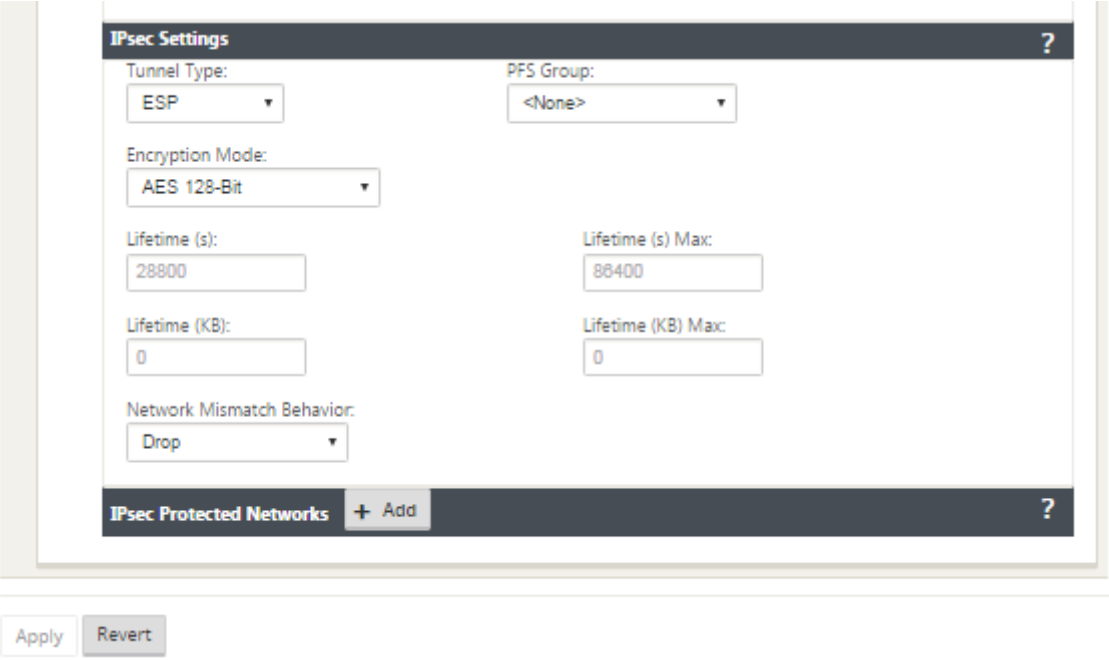
> 注意：
>
> 如果终止的 IPsec 路由器在配置中包含基于哈希的消息身份验证码 (HMAC)，请将 IPsec 模式更改为 **Exp+Auth**，并使用哈希算法作为 **SHA1**。





IPsec 和 IPsec 受保护的网络设置：

字段	说明	值
隧道类型	从下拉菜单中选择 隧道类型	ESP 环境保证 + 环境保证 + 环境保证 + 空 AH
PFS 组	从下拉菜单中选择 Diffie-Hellman 组用于完美的向前保密密钥生成	无 组 1 组 2 组 5 组 14 组 15 组 16 组 19 组 20 组 21
加密模式	从下拉菜单中选择 IPsec 消息的加 密模式	如果选择 ESP 或 ESP+ 身份验证，请选择以下任一项：AES 128 位、AES 192 位、AES 256 位、AES 128 位 GCM 64 位、AES 192 位 GCM 64 位、AES 256 位 GCM 64 位、AES 192 位 GCM 96 位、AES 192 位 GCM 96 位、AES 256 位 GCM 96 位、AES 256 位 GCM 96 位、AES 128 位 2 位 GCM 128 位、AES 256 位 GCM 128 位。AES 128/192/256 位受加拿大广播公司支持。
生命周期（秒）	输入允许 IPsec 安全关联存在的时间量（以秒为单位）	28800 秒（默认值）
最大寿命	输入允许 IPsec 安全关联存在的最长时间（以秒为单位）	86400 秒（默认值）
生命周期 (KB)	输入 IPsec 安全关联存在的数据量（以千字节为单位）	千字节
生命周期 (KB) 最大	输入允许 IPsec 安全关联存在的最大数据量（以千字节为单位）	千字节
网络不匹配行为	从下拉菜单中选择数据包与 IPsec 隧道的受保护网络不匹配时要采取的操作	删除，发送未加密，使用非 IPsec 路由
IPsec 保护网络	源 **IP/**前缀：单击添加 (+ 添加) 按钮后，输入 IPsec 隧道将保护的网络流量的 源 **IP** 和前缀	IP 地址
IPsec 保护网络	目标 **IP/**前缀：输入 IPsec 隧道将保护的网络流量的 目标 **IP** 和前缀	IP 地址



> 注意
>
> Citrix SD-WAN 支持通过 IPsec 连接到 Oracle 云基础设施 (OCI)。

监视 **IPsec** 隧道

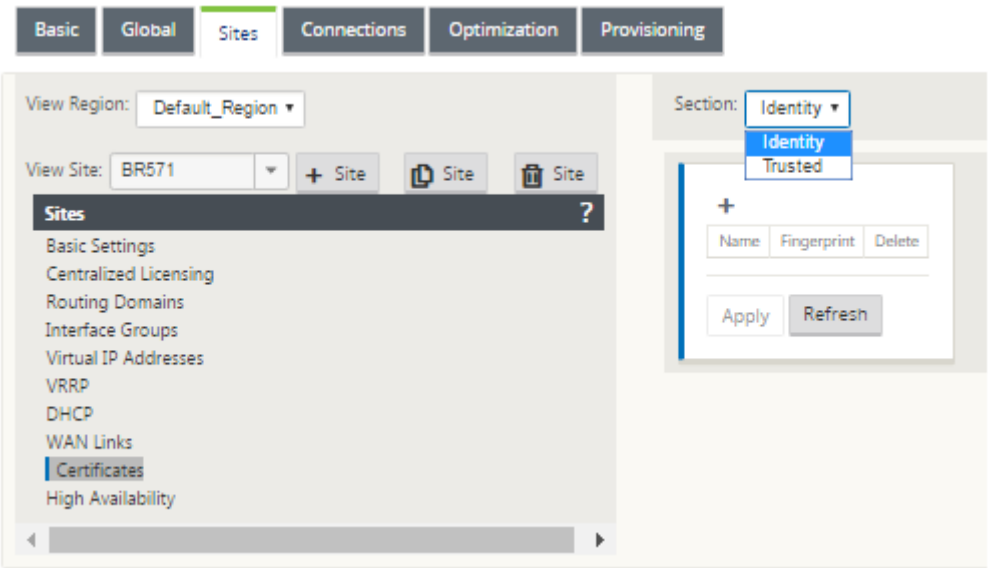
导航到 SD-WAN 设备 GUI 中的 监视 **> IKE/IPsec** ，以查看和监视 IPsec 隧道配置。

如何添加 **IKE** 证书

June 22, 2021

要实现 IKE 协商证书，请执行以下操作：

1. 导航到 站点 > 证书 并添加任何必要的证书。

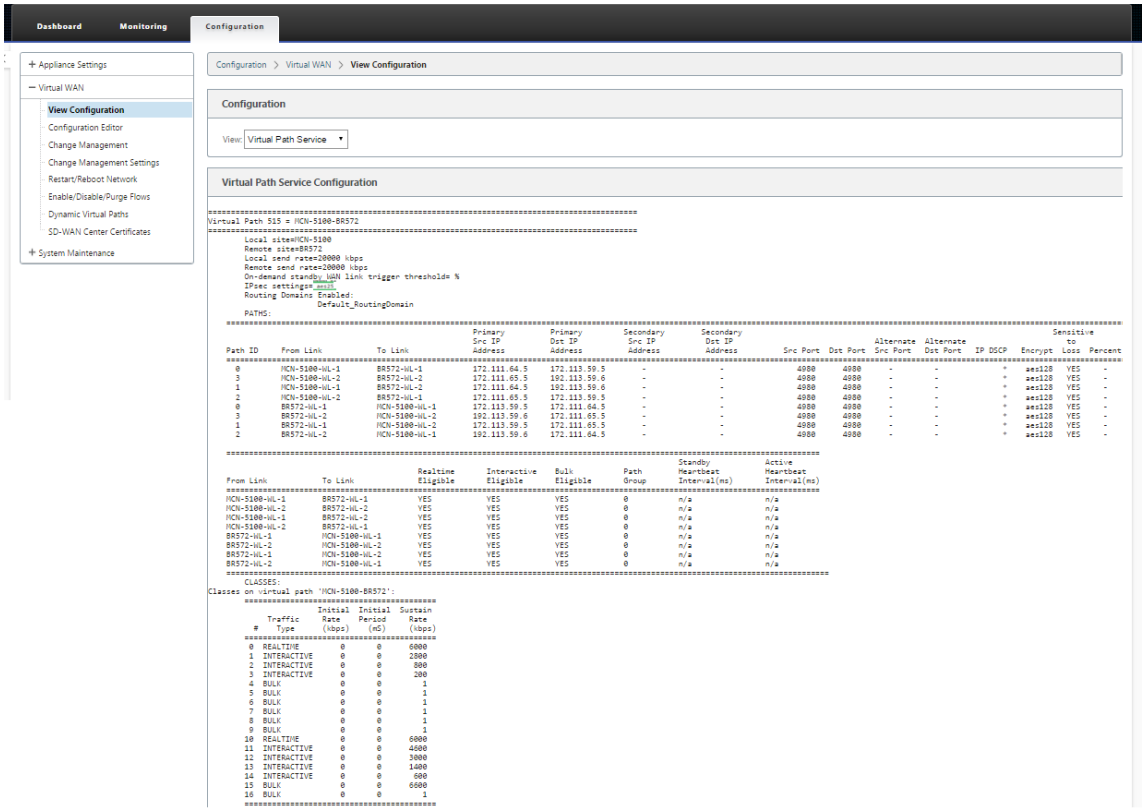


如何查看 **IPsec** 隧道配置

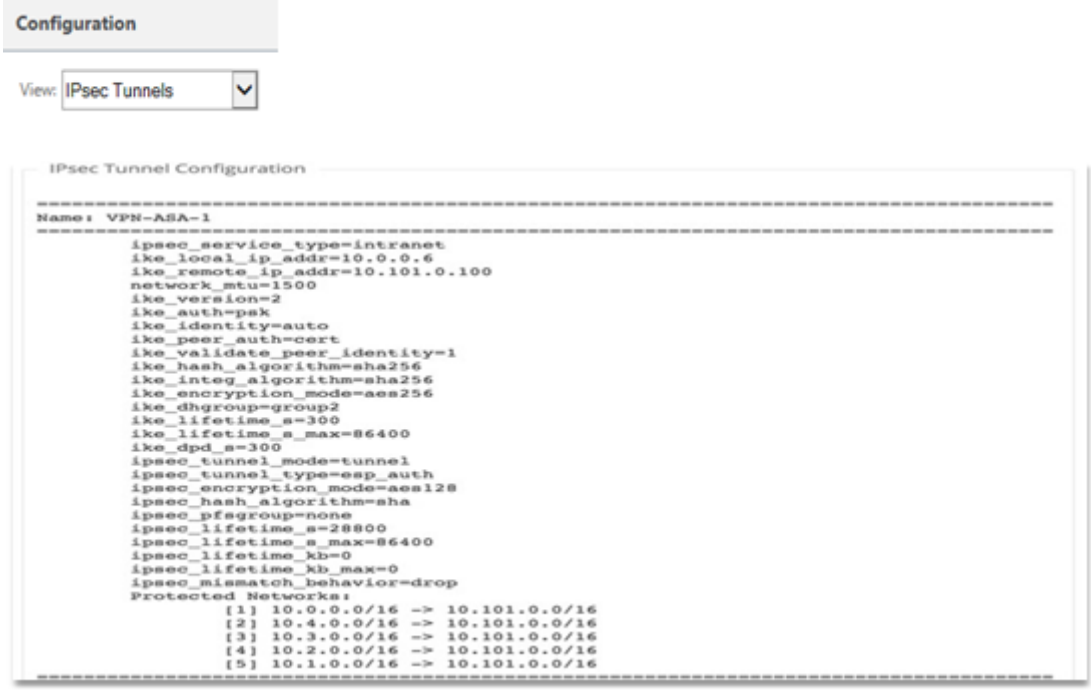
June 22, 2021

要查看 IPsec 隧道配置，请执行以下操作：

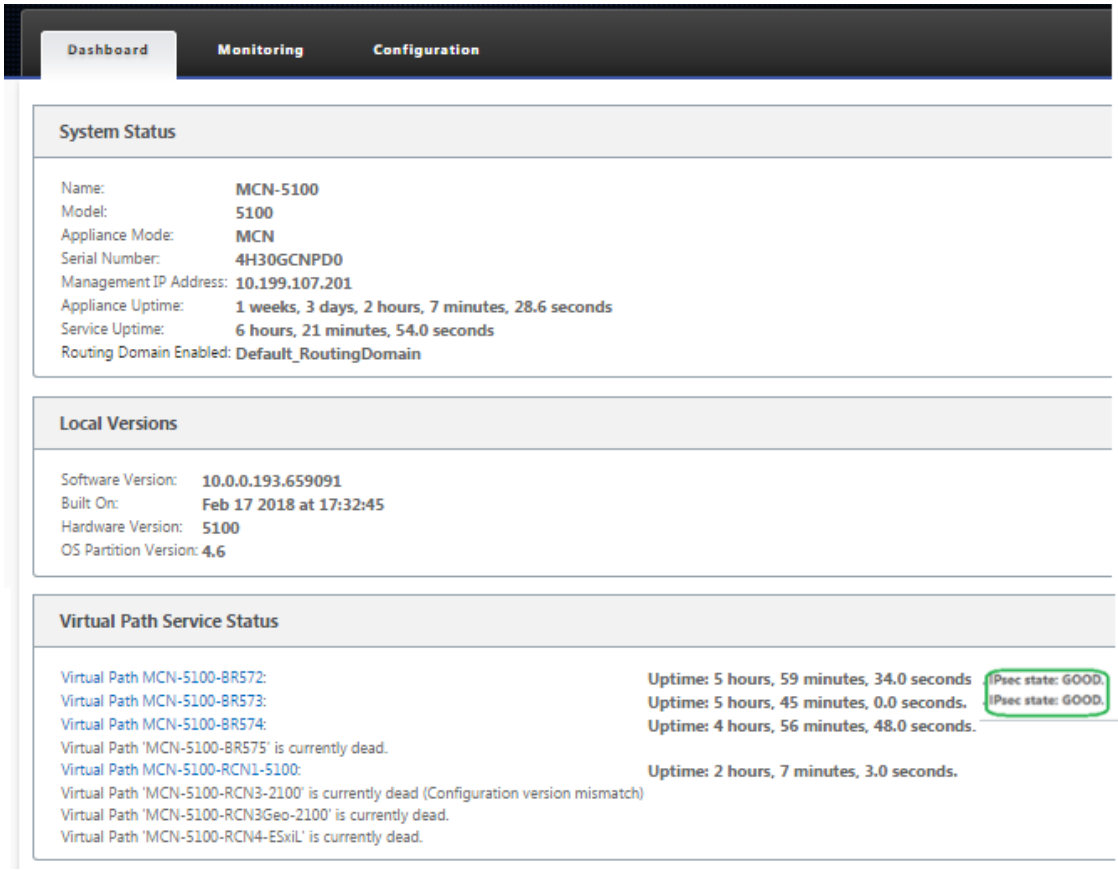
1. 导航到 配置 **>** 虚拟广域网 > 查看配置。
2. 从下拉菜单中选择 虚拟路径服务。只有在配置编辑器中启用 IPsec 时，才会显示 IPsec 设置。



3. 从下拉菜单中选择 **IPsec** 隧道 以查看 IPsec 隧道配置。



4. 每个虚拟路径将显示其自己的 IPsec 隧道状态，如下所示。

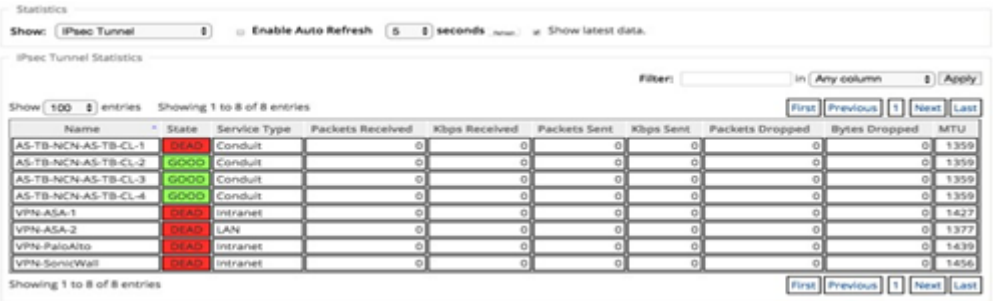


IPsec 监视和记录

June 22, 2021

要监视 IPsec 隧道统计信息，请执行以下操作：

1. 导航至 监视器 **>** 统计信息。从 显 示 下拉菜单中选择 **IPsec** 隧道，如下所示：

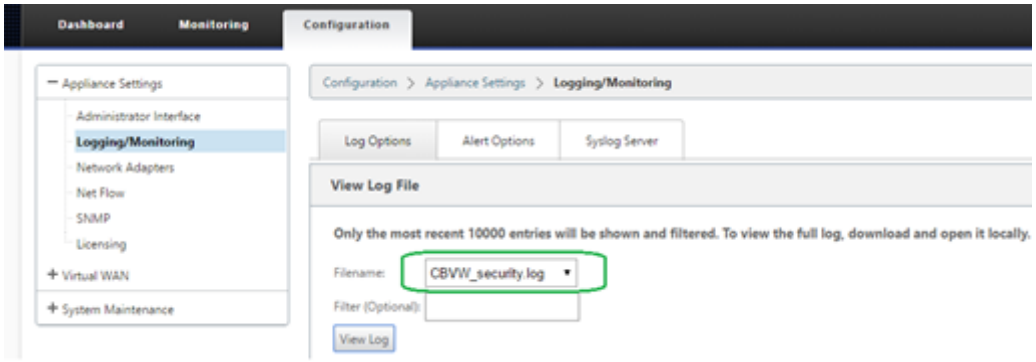


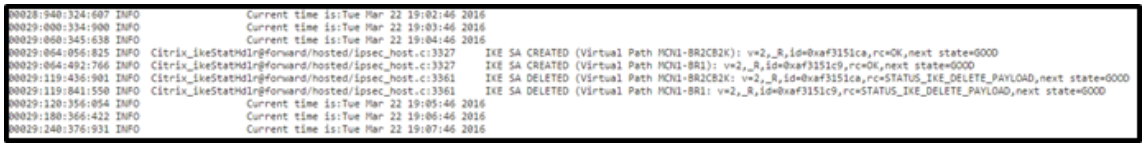
2. 导航到 监视器 > **IKE/IPsec**。观察在 SD-WAN 网络中配置的两个或模式 VPN 终端之间配置的 IPsec 隧道、IKE 和 IPsec 服务关联。

如何监测消除核心日志

1. 导航到 配置 > 设备设置 > 记录/监视。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 隧道的以下日志详细信息：

    - IPsec 隧道的创建与删除
    - IPsec 隧道状态更改

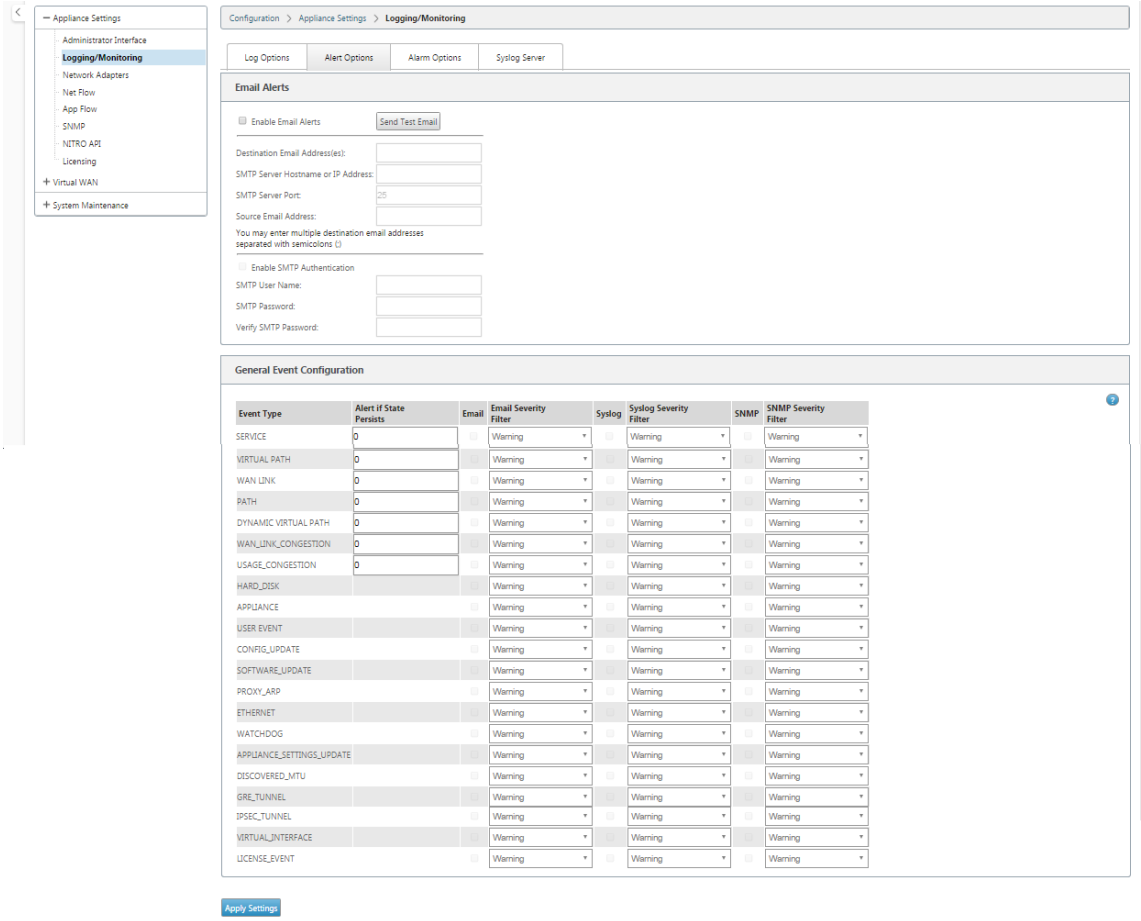




如何查看 **IPsec** 隧道警报

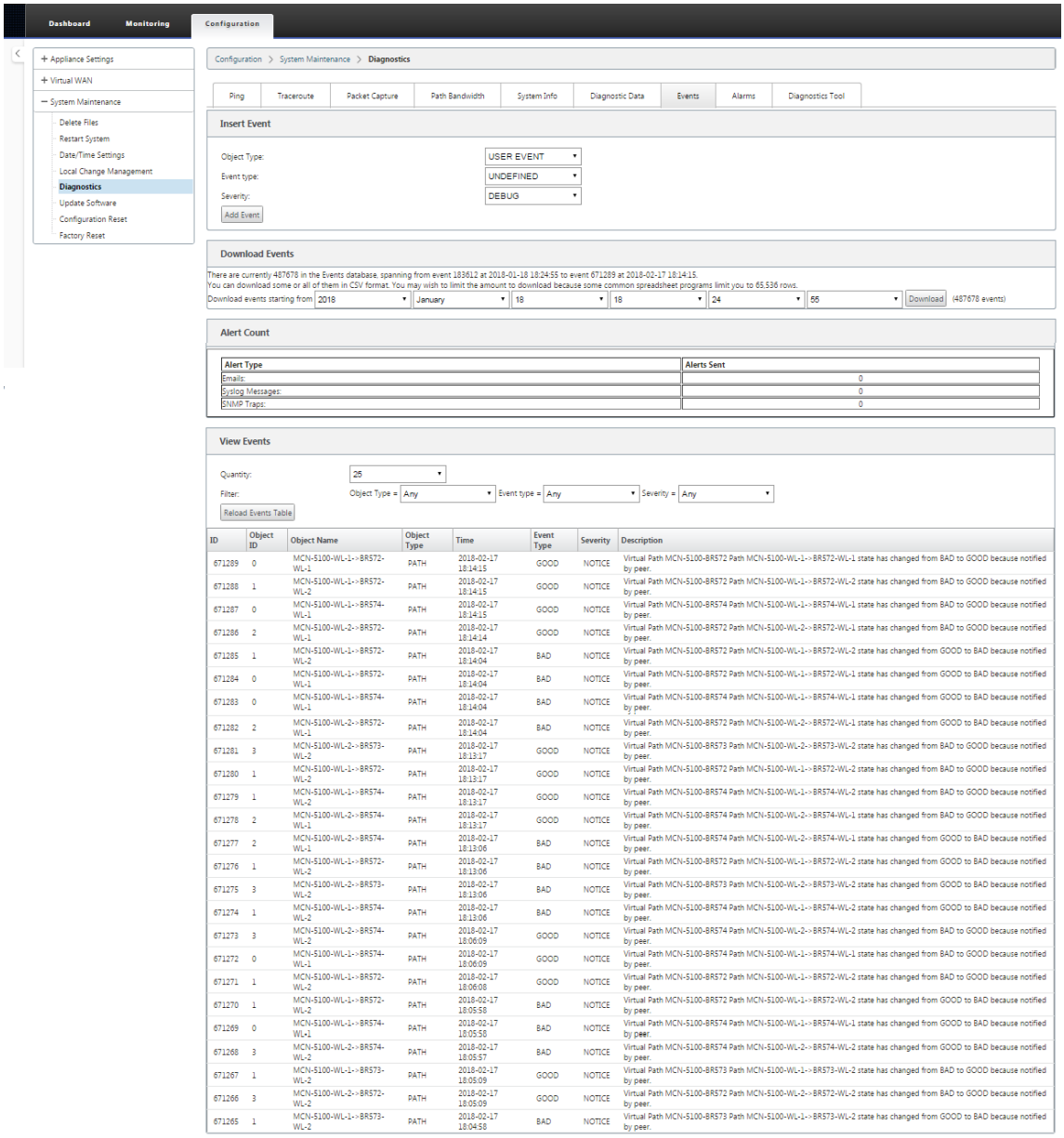
1. 导航至 配置 > 设备设置 **>** 记录/监视 > 警报选项。
2. 为 IPsec 隧道状态报告创建电子邮件和系统日志警报。

    - 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。



如何监视 **IPsec** 隧道事件

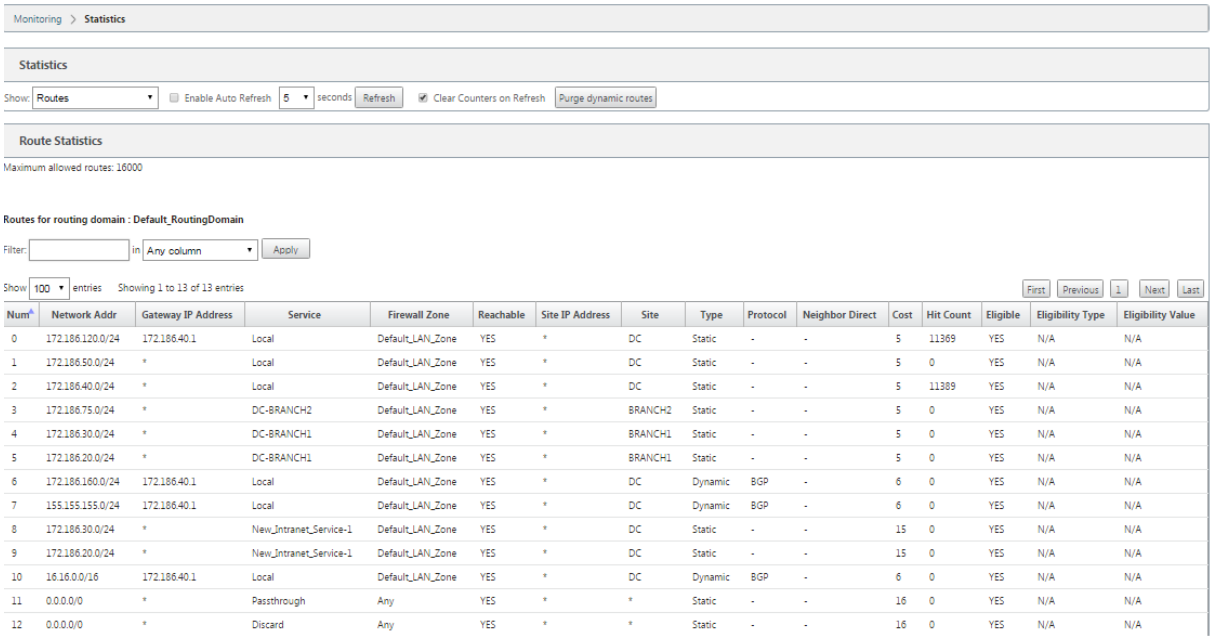
1. 导航到 配置 **>** 系统维护 > 诊断 > 事件。
2. 根据 **IPSEC_TUNDEN** D 对象类型添加事件。为所有 IPsec 相关事件创建过滤器。



IPsec 非虚拟路径路由的资格

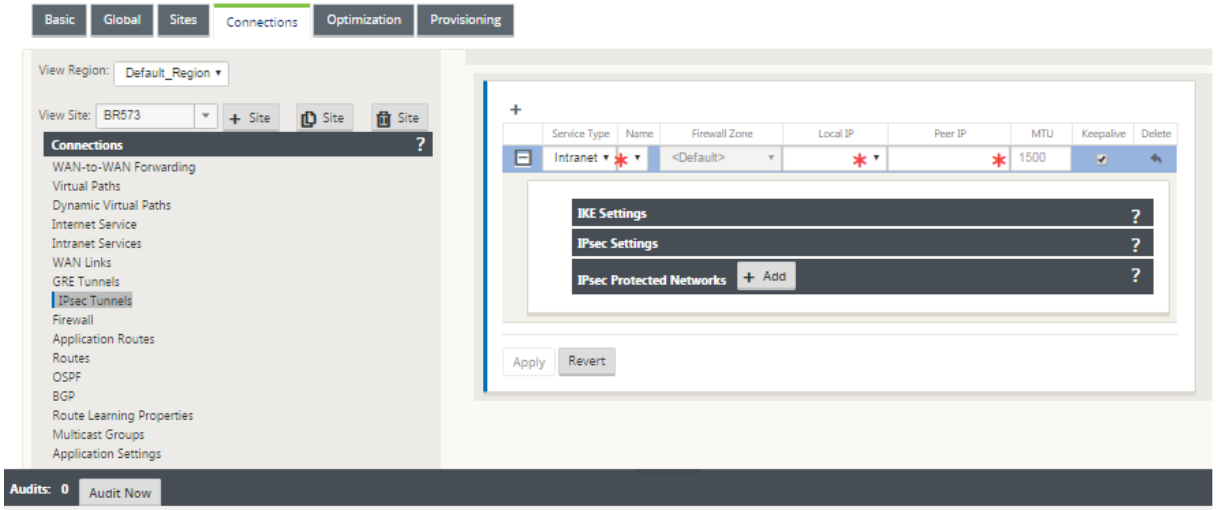
June 22, 2021

在以前的版本中，IPsec 隧道路由将保留在路由表中，即使隧道变为不可用。



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

使用 连接 [站点名称] > **IPsec** 隧道 下的 保持活动 选项可增强此行为，因此当 IPsec 隧道不再可用时，IPsec 非虚拟路径路由现在被视为不合格。启用 保持活动 选项后，将自动创建 SA，而不会通过隧道发送任何流量。

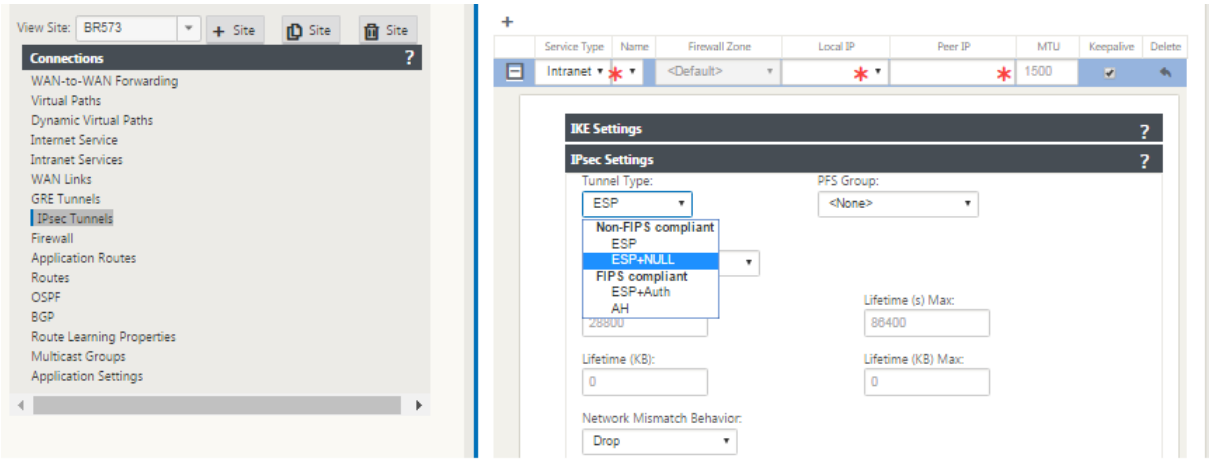


IPsec 空加密

June 22, 2021

在以前的版本中，引入了 ESP+NULL 的隧道类型。使用 IPsec ESP 协议时，通常会对流量进行加密和身份验证。但是，您可以选择不通过使用空加密使用加密。在 ESP + NULL 隧道类型中，数据包经过身份验证但未加密。

您可以在 配置编辑器 中的 **IPsec** 设置 部分中使用 **ESP+NULL** 隧道类型配置 **IPsec** 隧道。



FIPS 合规性

June 22, 2021

在 Citrix SD-WAN 中，FIPS 模式强制用户为其 IPsec 隧道配置 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 隧道类型
- 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 GUI 启用 FIPS 合规性，请执行以下操作：

1. 转到 配置 > 虚拟广域网 > 配置编辑器 > 全局，然后选择 启用 **FIPS** 模式。

启用 FIPS 模式会在配置期间强制执行检查，以确保所有与 IPsec 相关的配置参数都符合 FIPS 标准。系统会通过审核错误和警告提示您配置 IPsec。

要配置虚拟路径 IPsec 设置，请执行以下操作：

- 为需要 FIPS 合规性的所有虚拟路径启用虚拟路径 IPsec 隧道。虚拟路径的 IPsec 设置通过默认集进行控制。
- 通过将 IPsec 模式更改为 AH 或 ESP+ 身份验证来配置消息身份验证，并使用 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
- IPsec 生命周期应配置不超过 8 小时（28800 秒）。

虚拟广域网使用 IKE 版本 2 和预共享密钥通过虚拟路径协商 IPsec 隧道，使用以下设置：

- 卫生署 19 组：ECP256（256 位椭圆曲线）密钥协商

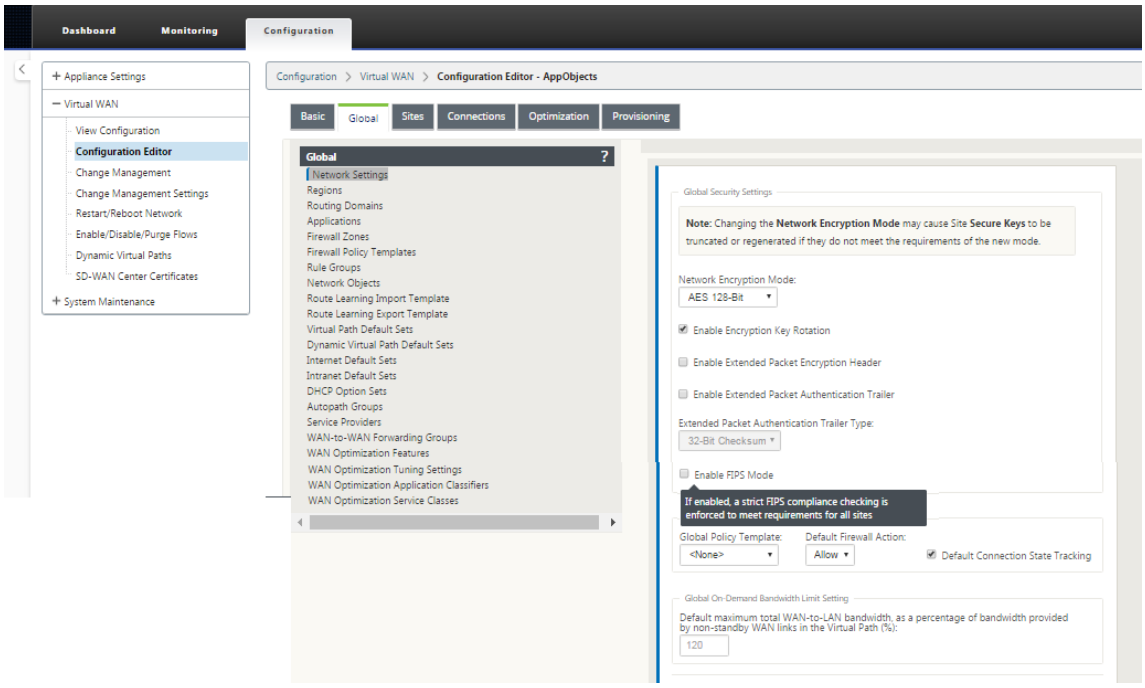
- 256 位 AES-CBC 加密
- 用于消息身份验证的 SHA256 哈希
- 用于消息完整性的 SHA256 哈希
- DH 组 2：完全向前保密的 MODP-1024

要为第三方配置 IPsec 隧道，请使用以下设置：

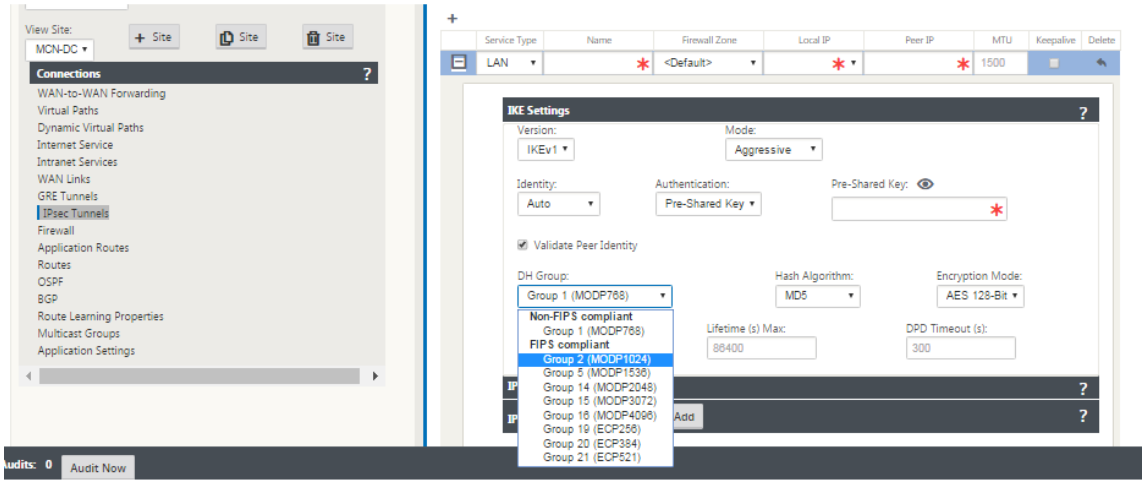
1. 配置 FIPS 批准的 DH 组。根据 FIPS，第 2 组和第 5 组是允许的，但强烈推荐 14 组及以上组。
2. 配置 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
3. 如果使用 IKEv2，请配置 FIPS 批准的完整性功能。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
4. 将 IKE 生命周期和最大生命周期配置为不超过 24 小时（86,400 秒）。
5. 通过将 IPsec 模式更改为 AH 或 ESP+ 身份验证来配置 IPsec 消息身份验证，并使用 FIPS 批准的哈希函数。SHA1 被 FIPS 接受，但强烈推荐使用 SHA256。
6. 将 IPsec 生命周期和最大生命周期配置为不超过 8 小时（28800 秒）。

要配置 IPsec 隧道，请执行以下操作：

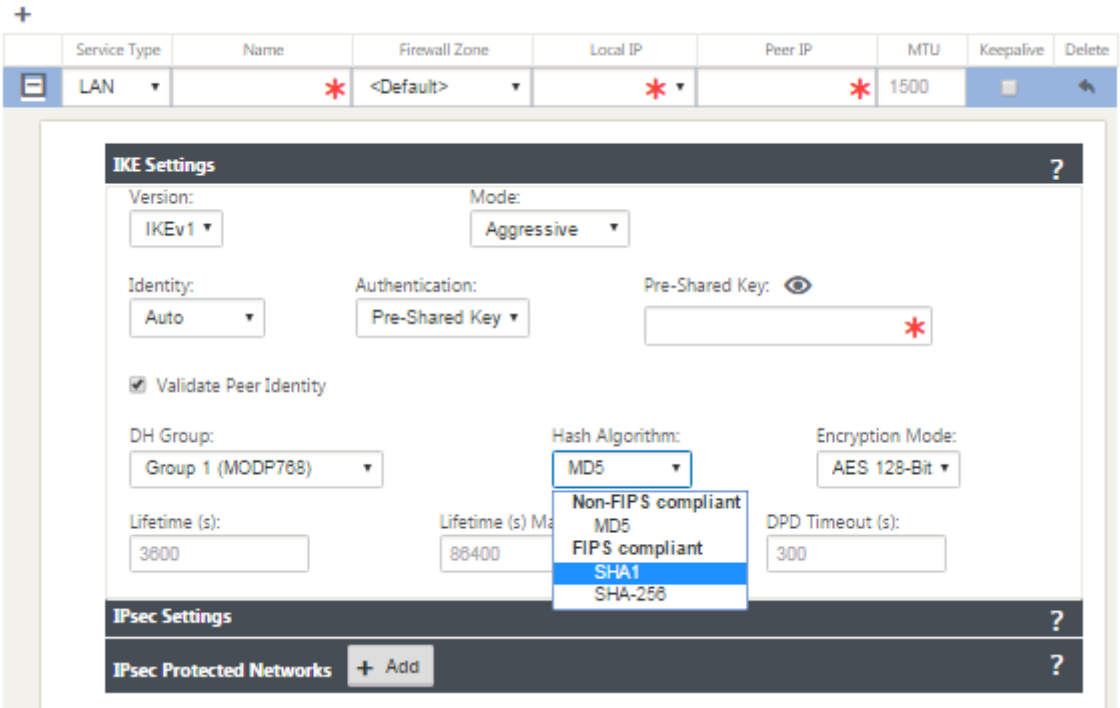
1. 在 MCN 设备上，转到 配置 > 虚拟 **WAN** > 配置编辑器。打开现有配置包。转到 连接 > **IPsec** 隧道。



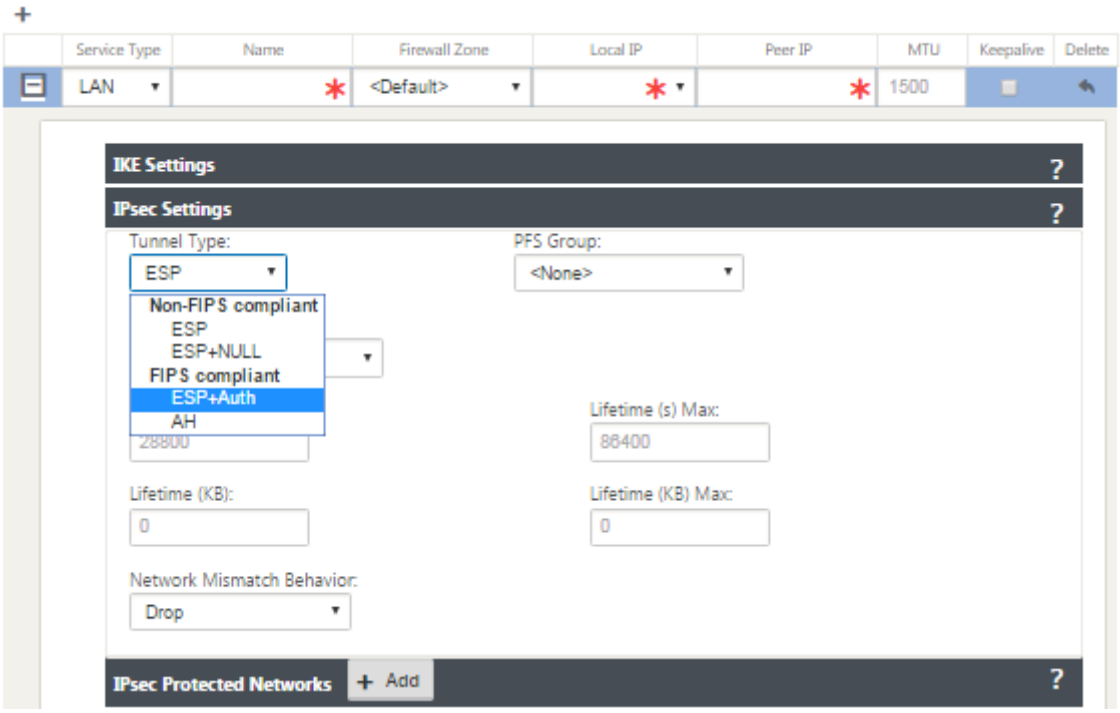
2. 转到 连接 > **IPsec** 隧道。选择 **LAN** 或 **Intranet** 隧道 后，屏幕将 IKE 设置中的 FIPS 兼容组与不兼容的组区分开来，以便您可以轻松配置 FIPS 合规性。



屏幕还指示哈希算法是否符合 FIPS 标准，如下图所示。



IPsec 设置的 FIPS 合规性选项：



如果 IPsec 配置在启用时不符合 FIPS 标准，则可能会触发审核错误。以下是 GUI 中显示的审核错误类型。

- 启用 FIPS 模式并选择不符合 FIPS 标准的选项。
- 启用 FIPS 模式时，输入不正确的生命周期值。
- 启用 FIPS 模式并启用虚拟路径默认设置的 IPsec 设置，并选择不正确的隧道模式（ESP vs ESP_Auth /AH）。
- 启用 FIPS 模式时，虚拟路径默认集的 IPsec 设置也会启用，并输入不正确的生命周期值。

Citrix SD-WAN Secure Web Gateway

June 22, 2021

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强化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 云安全平台。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（目标 NAT 的透明代理）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 1, 2021

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。通过简单地将您的互联网流量重定向到 Zscaler，您可以立即保护您的商店、分支机构和远程位置。Zscaler 连接用户和互联网，检查每个字节的流量，即使它是加密或压缩。

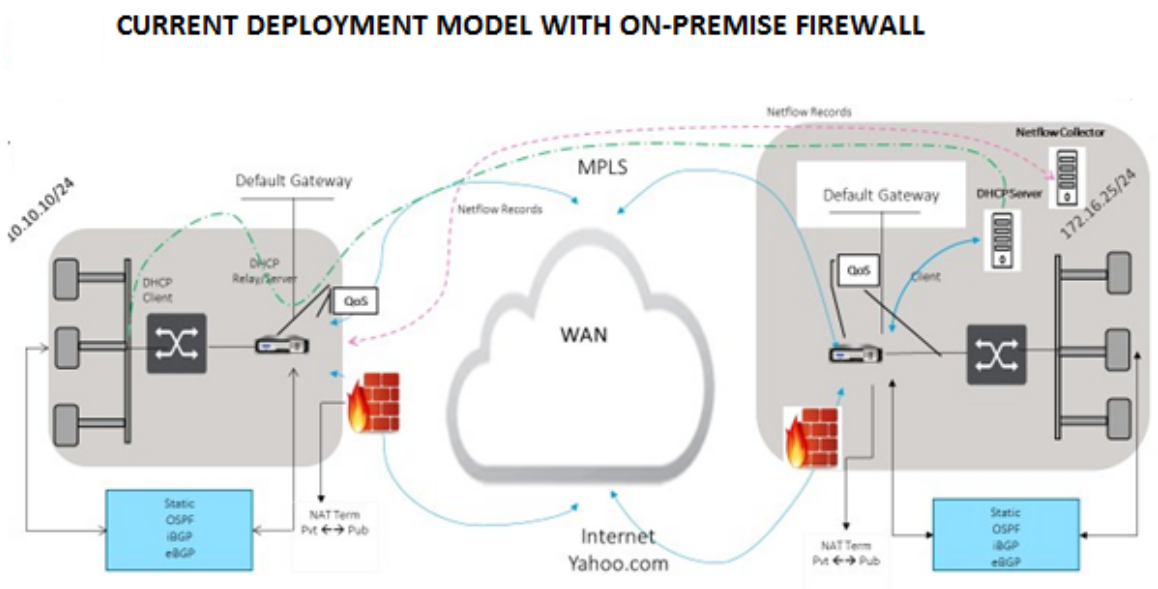
Citrix SD-WAN 设备可以通过客户现场的 GRE 隧道连接到 Zscaler 云网络。使用 SD-WAN 设备的 Zscaler 部署支持以下功能：

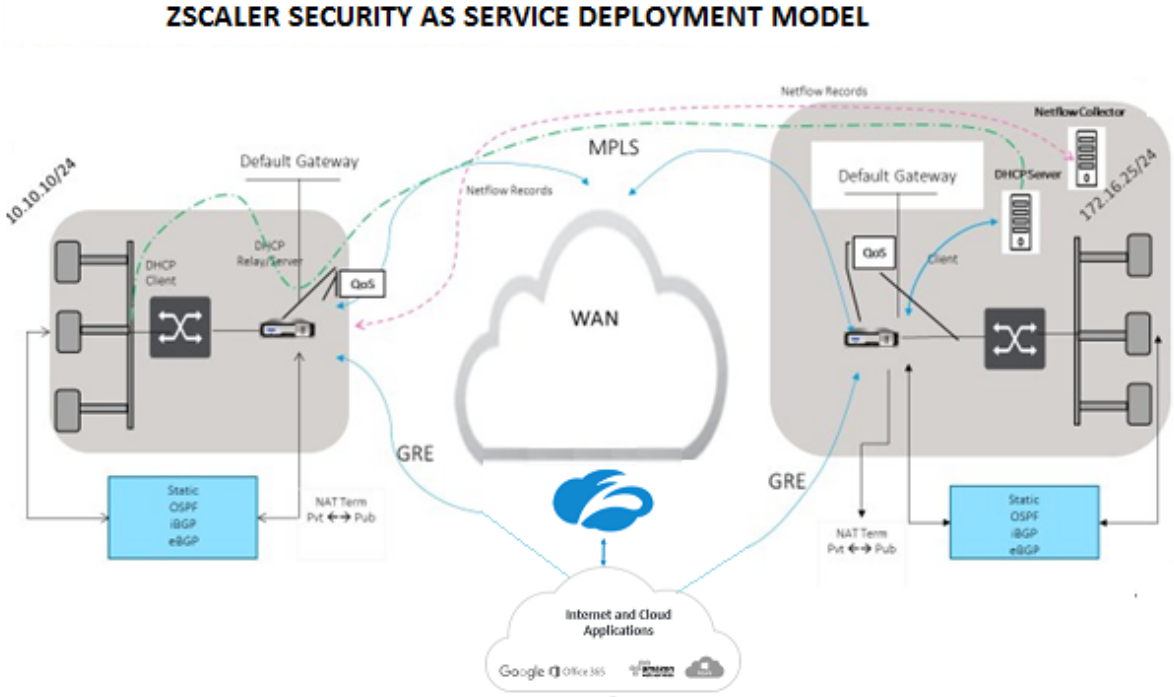
- 转发所有 GRE 流量 Zscaler, 从而使直接互联网突破.
- 基于每个客户站点使用 Zscaler 进行直接互联网访问（DIA)。
  - 在某些站点上，您可能希望向 DIA 提供本地安全设备，而不使用 Zscaler。
  - 在某些站点上，您可能会选择回程线路流量（另一个客户站点）以访问 Internet。
- 虚拟路由和转发部署。
- 一个 WAN 链接，作为 Internet 服务的一部分。

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互联网服务.
- 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 隧道或 IPsec 隧道流量转发：

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 隧道或 IPsec 隧道源 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隧道的健康.

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 使用两个要将流量重定向到的 ZEN IP 地址 [DR1] 进行响应。GRE 保持活动的消息可以用来确定隧道的健康。

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

要配置 Internet 服务，请执行以下操作：

1. 导航到连接 - **Internet** 服务。配置 Internet 服务。
2. 选择 **+** 服务 并根据需要启用设置（基本设置、WAN 链接和规则）。
3. 选择应用。

有关为站点启用 Internet 服务的详细信息，请参阅 具有集成防火墙的分支机构的直接互联网突破。

您可以在 Internet 服务上配置以下设置：

- 基本设置
- WAN 链接
- 规则

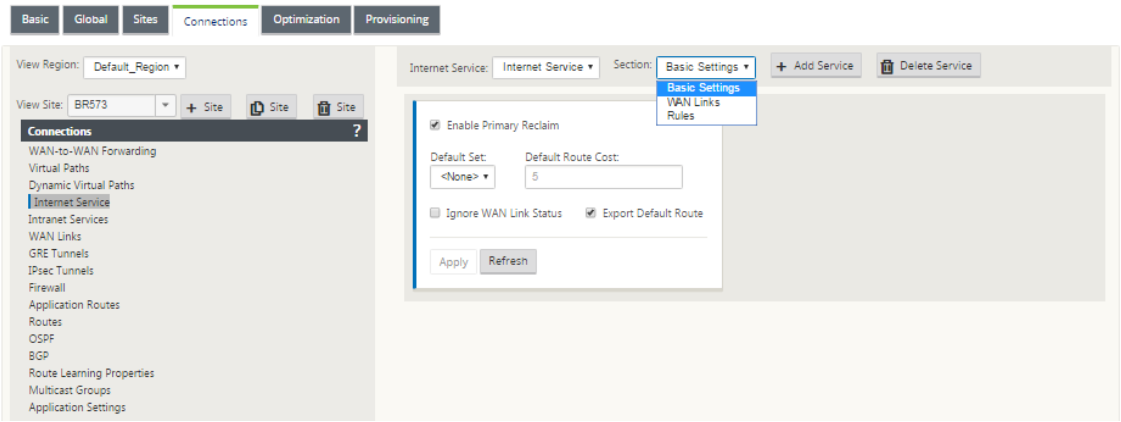
基本设置

无法为 Internet 服务配置防火墙区域设置。如果互联网服务受信任，则会将其分配给 **Internet_Zone**。如果 Internet 服务不受信任，则会将其分配给 **Untrusted_Internet_Zone**。

可配置的基本设置如下所述：

- 启用主回收：如果启用，则 WAN 链接上与此服务关联的（使用 = 主要）使用情况将强制恢复为该 WAN 链接上的活动服务的状态。

- 默认集：用于填充站点上 Internet 服务规则的 Internet 默认集的名称。
- 默认路由成本：与默认 (0.0.0.0/0) 互联网路由关联的路由成本。
- 忽略 **WAN** 链接状态：如果启用，即使该服务的所有 WAN 链路都不可用，发往此服务的数据包仍会选择此服务。
- 导出默认路由：如果启用，则如果启用了 WAN 到 WAN 转发，则 Internet 服务的默认路由 0.0.0.0/0 将导出到其他站点。



WAN 链接

可配置的 WAN 链接设置如下所述：

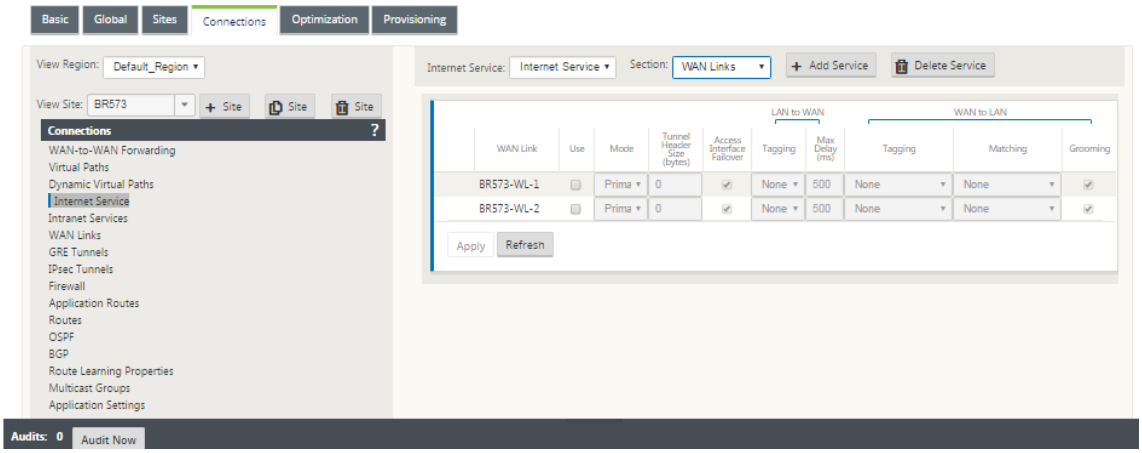
- 使用：允许服务使用此 WAN 链接。禁用“使用”时，所有其他选项都不可用。
- 模式：服务模式—主要、辅助或平衡，用于流量冗余或负载平衡。
- 通道头大小（字节）：通道报头的大小（以字节为单位）（如果适用）。
- 访问接口故障切换：如果启用，具有不匹配 VLAN 的 Internet 或 Intranet 数据包仍然可以使用该服务。

局域网到 **WAN**

- 标记：应用于服务上的 LAN 到 WAN 数据包的 DSCP 标记。
- 最大延迟 **(**毫秒**)**：超出 WAN Link 带宽时缓冲数据包的最长时间（以毫秒为单位）。

WAN 到局域网

- 标记：应用于服务上的 WAN 到 LAN 数据包的 DSCP 标记。
- 匹配：将匹配此标记的 Internet WAN 到 LAN 数据包分配给服务。
- 整理：如果启用，则会随机丢弃数据包，以防止 WAN 到 LAN 的流量超出服务的预配置带宽。



规则

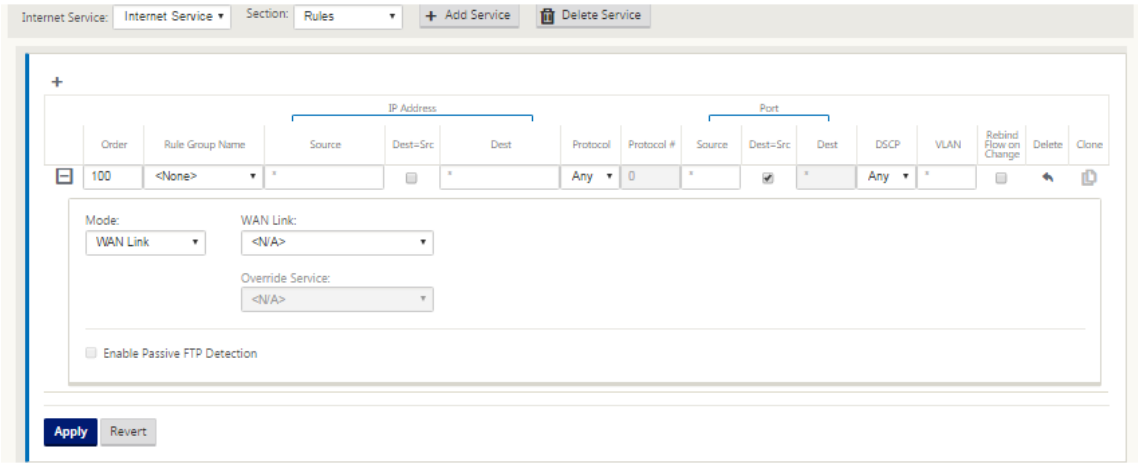
互联网流量是根据定义的规则进行识别的。规则定义用于匹配特定的通信流。匹配后，您必须定义要申请流量的操作。

下面介绍了可用规则的列表：

- 顺序：应用规则并自动重新分配规则的顺序。
- 规则组名称：为规则指定的名称，该名称允许在显示规则统计信息时按组汇总。可以一起查看具有相同规则组名称的规则的所有统计信息。
- 来源：与规则匹配的源 IP 地址和子网掩码。
- **Dest-Src**：如果启用，则源 IP 地址也将用作目标 IP 地址。
- **Dest**：与规则匹配的目标 IP 地址和子网掩码。
- 协议：与过滤器匹配的协议名称。
- 协议编号：与过滤器匹配的协议编号。
- **DSCP**：IP 报头中与规则匹配的 DSCP 标记。

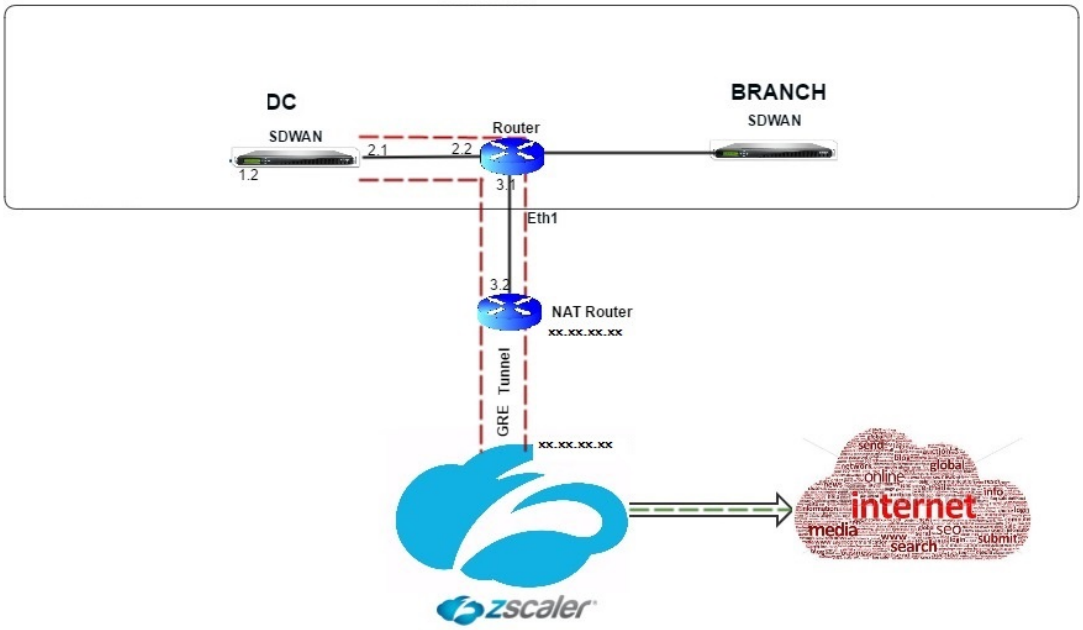
下面介绍了可用操作的列表：

- **WAN** 链接：启用 Internet 负载平衡后，与规则匹配的流量将使用的 WAN 链接。
- 覆盖服务：与规则匹配的流的目标服务。
  - 丢弃：丢弃流量。
  - 直通：将流映射到直通，并允许流量不变地通过设备。



配置 **GRE** 隧道

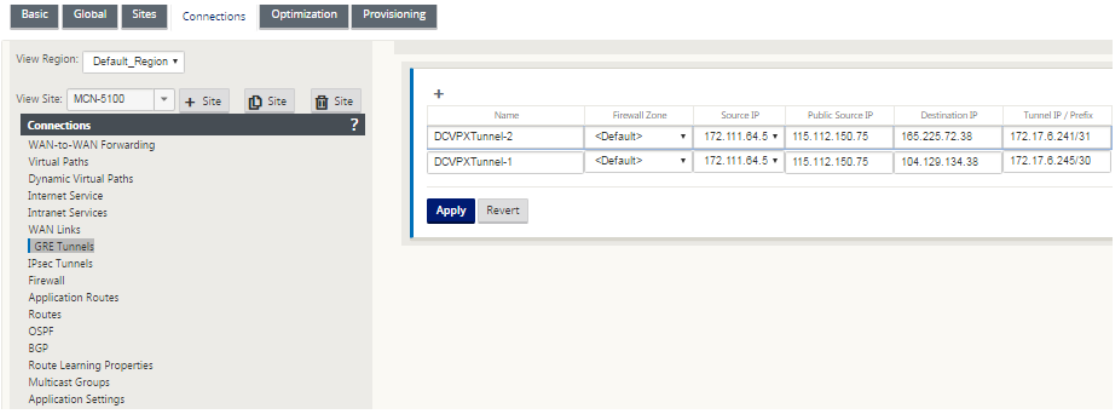
1. 源 IP 地址是隧道源 IP 地址。如果隧道源 IP 地址已执行 NAT，则公共源 IP 地址是公共隧道源 IP 地址，即使其在不同的中间设备上执行了 NAT 也是如此。
2. 目标 IP 地址是 Zscaler 提供的 ZEN IP 地址。
3. 源 IP 地址和目标 IP 地址是原始负载封装时路由器 GRE 头.
4. 隧道 IP 地址和前缀是 GRE 隧道本身的 IP 地址。这对于通过 GRE 隧道路由流量非常有用。流量需要此 IP 地址作为网关地址。



要配置 GRE 隧道：

1. 在配置编辑器中，导航到“连接”> “站点”> “**GRE** 通道”，然后配置路由以将 Internet 前缀服务转发到 Zscaler GRE 通道。

   只能从受信任链接上的虚拟网络接口中选择源 IP 地址。请参阅 如何配置 GRE 通道。



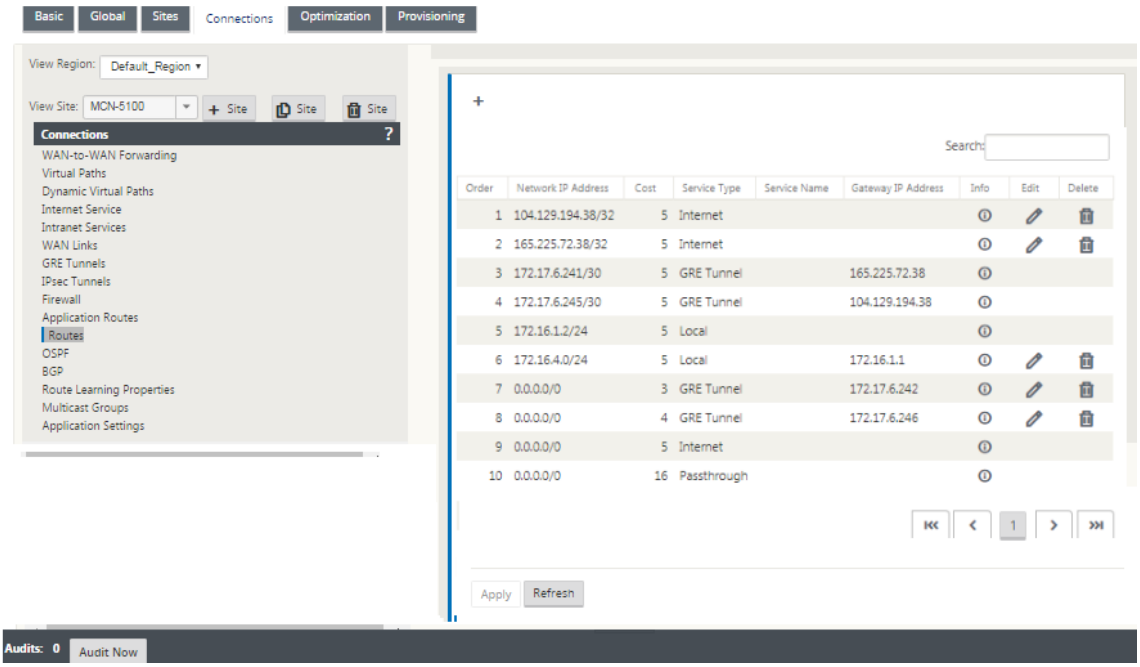
为 **GRE** 隧道配置路线

配置路由以将互联网前缀服务转发到 Zscaler GRE 隧道.

- ZEN IP 地址（隧道目标 IP，如上图 104.129.194.38 所示）必须设置为服务类型的互联网。这是必需的，以便从互联网服务中计入发往 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 隧道传输。确保 GRE 隧道 [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 隧道 Zscaler 必须具有比主 GRE 隧道更高的成本.
- 确保 ZEN IP 地址存在非递归路由。

要配置 **GRE** 隧道路由：

1. 导航到“连接”> “站点”> “路由”，然后按照 配置路由 中所述的步骤操作，以获取有关创建路



注意

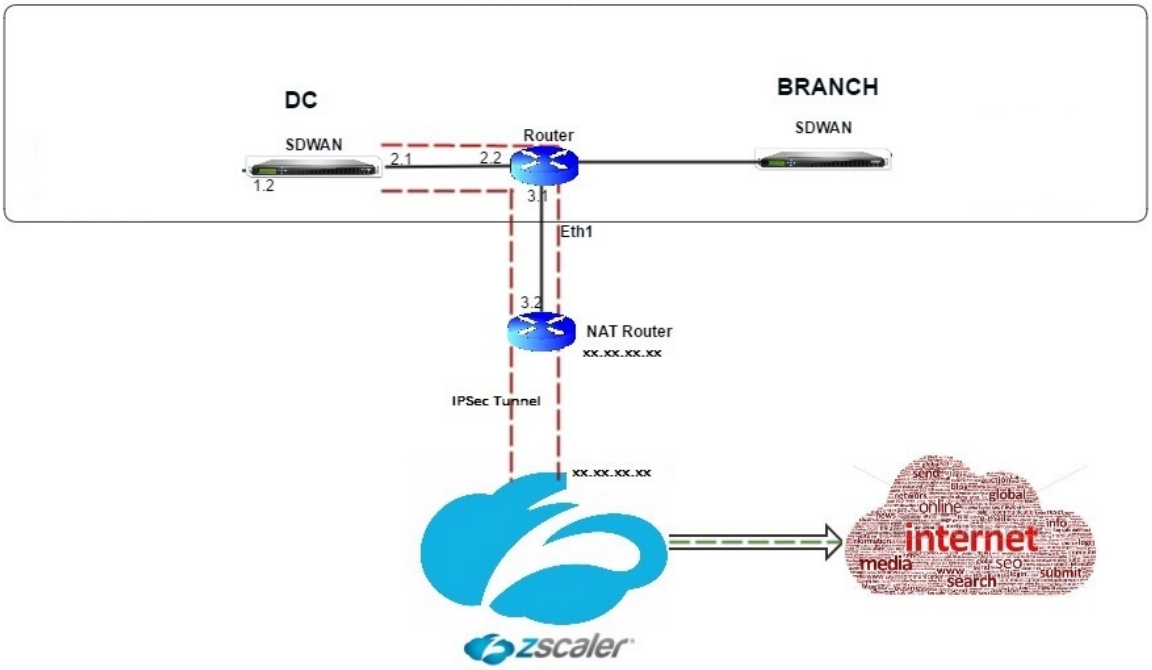
如果您没有 Zscaler IP 地址的特定路由，请配置路由前缀 0.0.0.0/0 以匹配 ZEN IP 地址，并通过 GRE 隧道封装循环路由。此配置使用主动备份模式下的隧道。如上图所示的值，流量会自动切换到 Gateway 关 IP 地址 172.17.6.242 的隧道。如果需要，请配置回程虚拟路径路由。否则，将备份隧道的保持活动时间间隔设置为零。这使得安全的互联网访问网站，即使两个隧道 Zscaler 失败。

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 设备的隧道源由中间设备 NATE 时，该字段提供 GRE 源地址的 NAT 地址。

限制

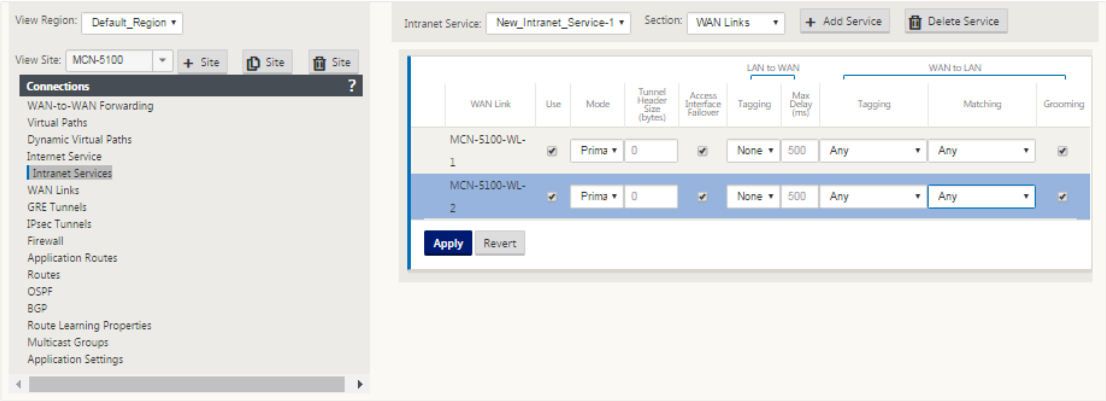
- 不支持多个 VRF 部署。
- 主备份 GRE 隧道仅支持高可用性设计模式。

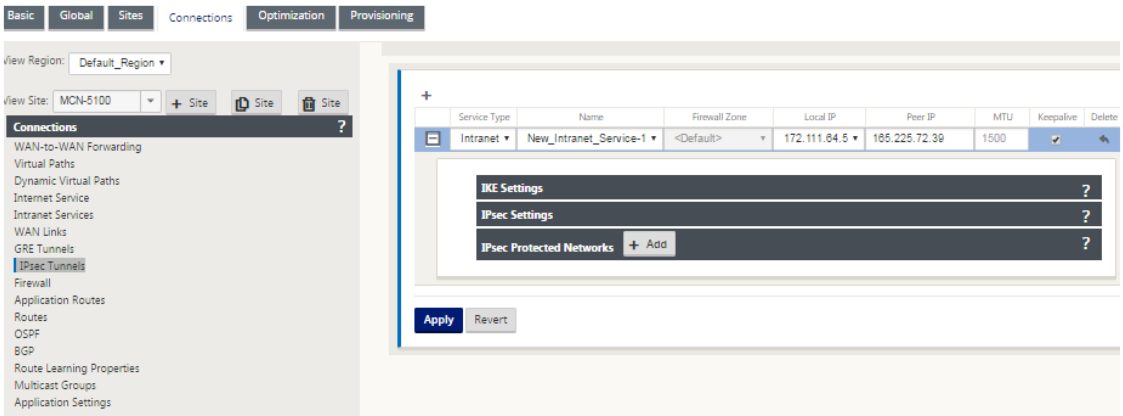
配置 **IPsec** 隧道



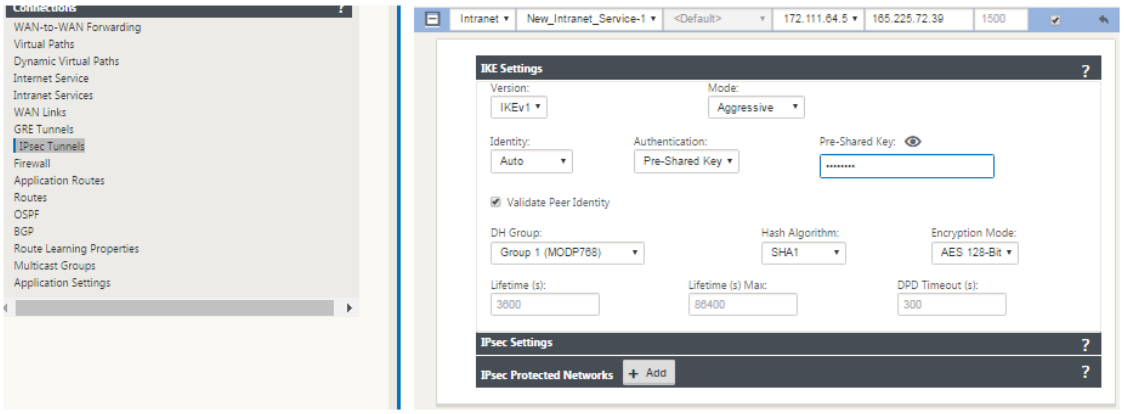
要在 Citrix SD-WAN 设备 GUI 中为 Intranet 或 LAN 服务配置 IPsec 隧道，请执行以下操作：

1. 在配置编辑器中，导航到 连接 > < S**iteName**> > **IPsec** 通道，然后选择一种服务类型（局域网或内部网）。
2. 输入服务类型的 名称。对于 Intranet 服务类型，配置的 Intranet 服务器确定哪些本地 IP 地址可用。
3. 选择可用的本地 IP 地址，然后输入远程对等的虚拟路径的对等 IP 地址。



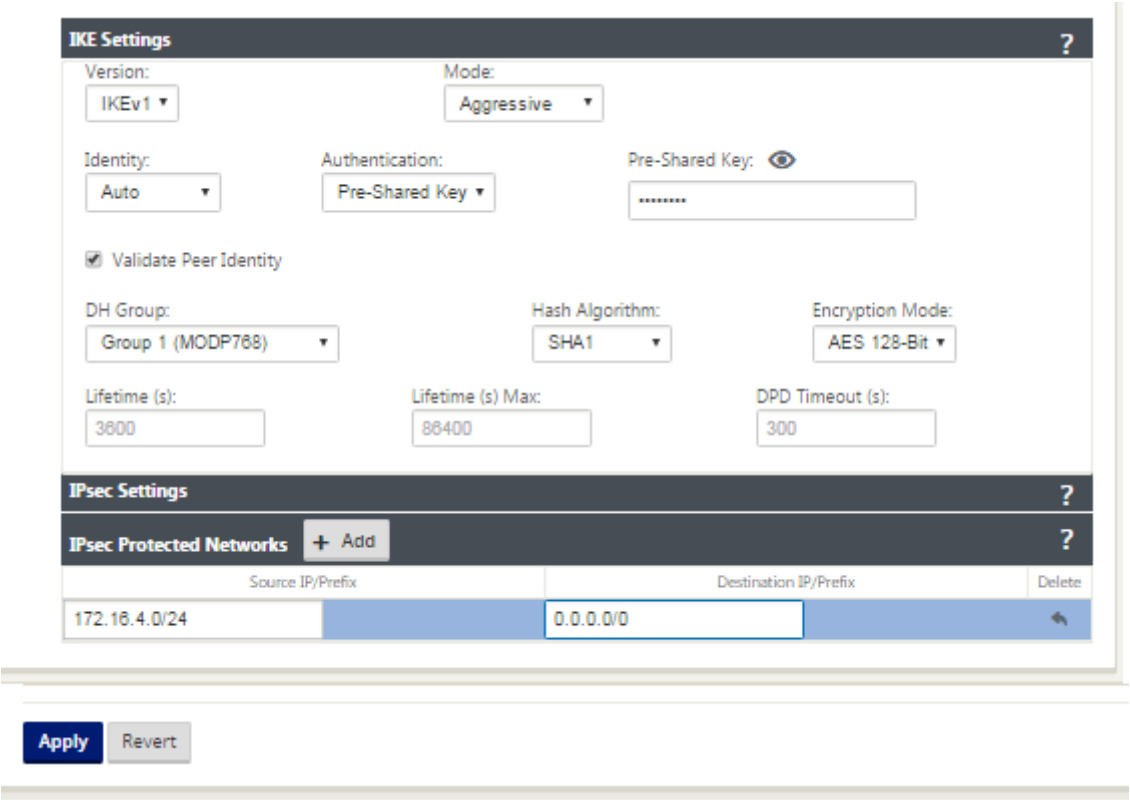


4. 为 **IKE** 设置选择 **IKEv1**。Zscaler 仅支持 IKEv1。



5. 在 IPsec 设置下，为 隧道类型 选择 **ESP-NULL**，以通过 IPsec 隧道将流量重定向到 Zscaler。IPsec 隧道不会对流量进行加密。

6. 由于互联网流量被重定向，因此目标 IP/前缀可以是任何 IP 地址。

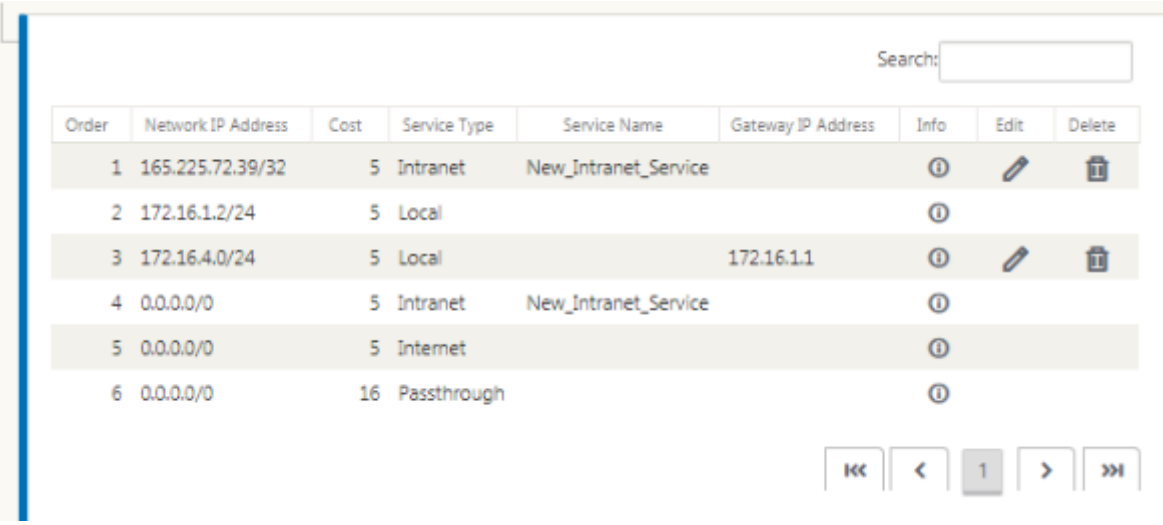


有关使用 Citrix SD-WAN Web 界面配置 IPsec 隧道的更多信息，请参阅；IPsec 隧道 主题。

配置 **IPsec** 隧道的路由

要配置 **IPsec** 路由，请执行以下操作：

1. 导航到“连接” > “**DC** ” > “路由”，然后按照 配置路由 中所述的步骤操作，以获取有关创建



要监视 GRE 和 IPsec 隧道统计信息：

在 SD-WAN Web 界面中，导航到 监控 > 统计信息 > [**GRE** 通道] **IPsec** 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

June 22, 2021

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）

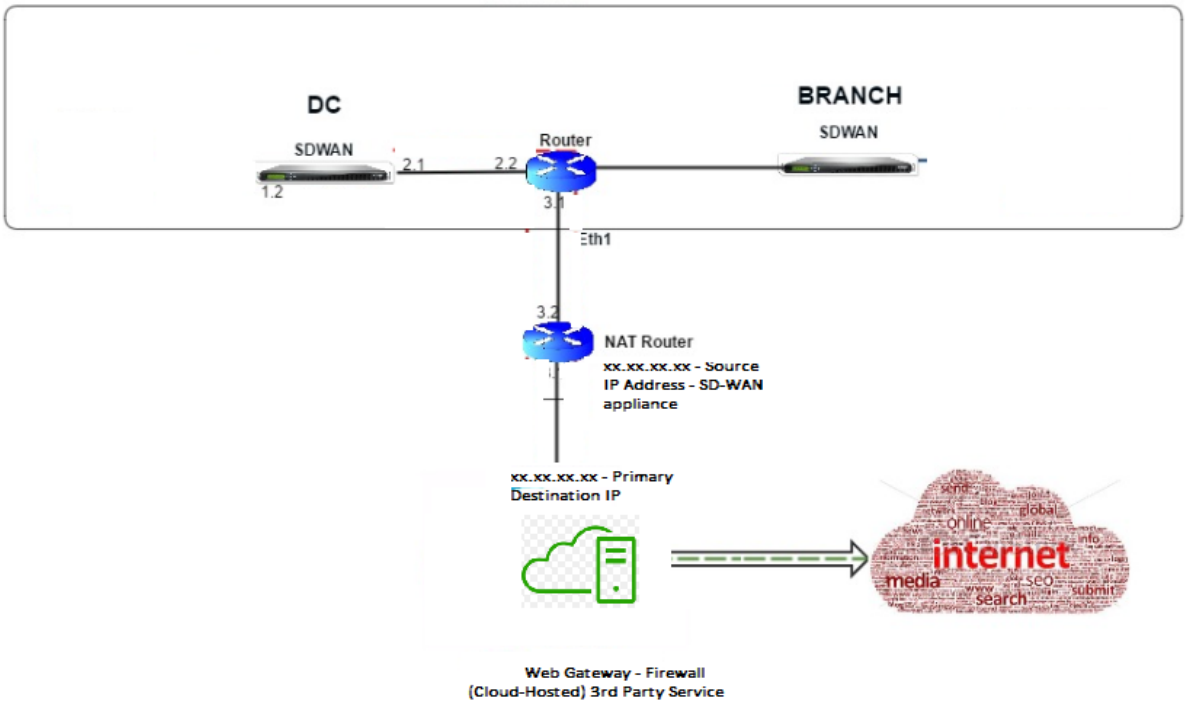
目标 NAT 策略使企业能够使用 ForcePoint 通过云托管安全服务路由互联网流量。

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. 登录到Forcepoint 门户网站。通过提供企业公有 IP 地址来创建策略，互联网流量需要重定向到 Forcepoint。获取互联网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 使用互联网流量的目标 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) 内的互联网 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。

有关 Citrix SD-WAN 中的 NAT 支持的其他信息，请参阅以下主题配置 NAT



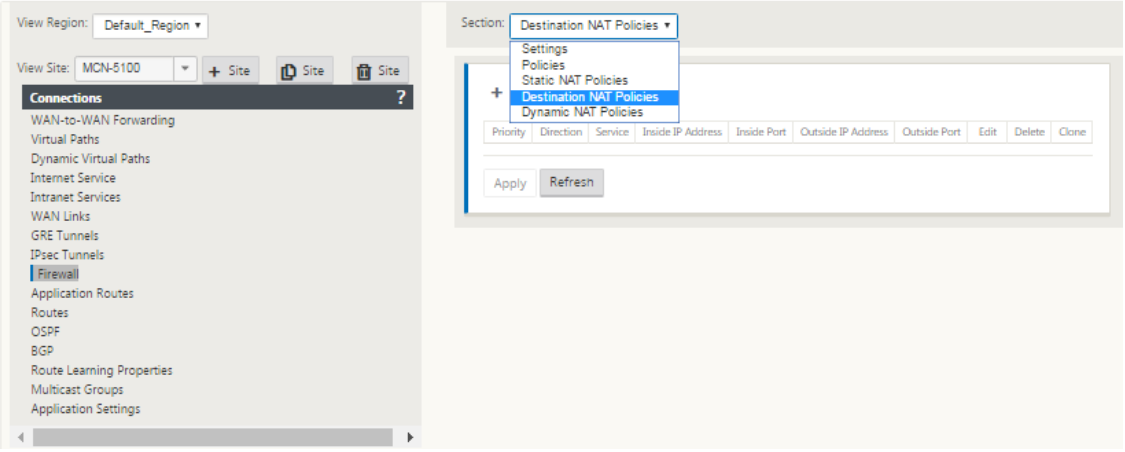
配置目标 **NAT (DNAT)**

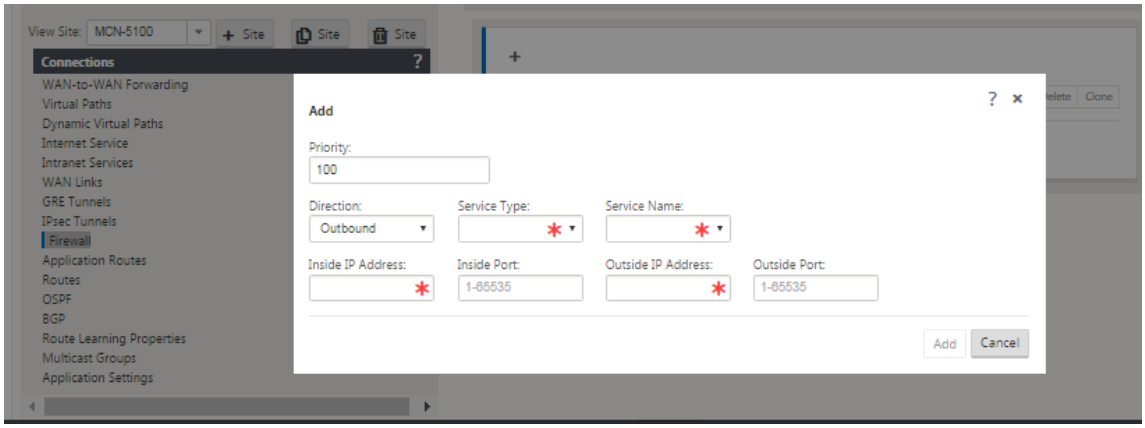
使用 Citrix SD-WAN GUI 配置目标 NAT (DNAT)。在配置中，添加一个或多个 DNAT 策略，用于重定向与特定目标 IP 地址和端口匹配的流量。

要配置目标 NAT，请执行以下操作：

在 SD-WAN SE/VPX GUI 中，转到 配置 -> 虚拟 **WAN** -> 配置编辑器。单击 打开 以打开现有软件包。选择已保存的配置包。您还可以在构建网络配置时创建 DNAT 规则。

1. 在 DC (MCN) 中，配置 Internet 服务。转到 连接 -> 防火墙。
2. 单击 **+** 添加以 添加 DNAT 策略。
3. 在 添加目标 **NAT** 策略 对话框中，提供以下信息：
   - 优先级
   - 方向
   - 服务类型
   - 服务名称
   - IP 地址内部
   - 在端口内
   - 外部 IP 地址
   - 端口外





4. 为防火墙流量重定向设置目标 NAT 规则，类似于静态 NAT。
5. 输入匹配条件和要 NNated 的目标 IP/端口。
6. 执行 DNAT 规则与统计数据的连接匹配。

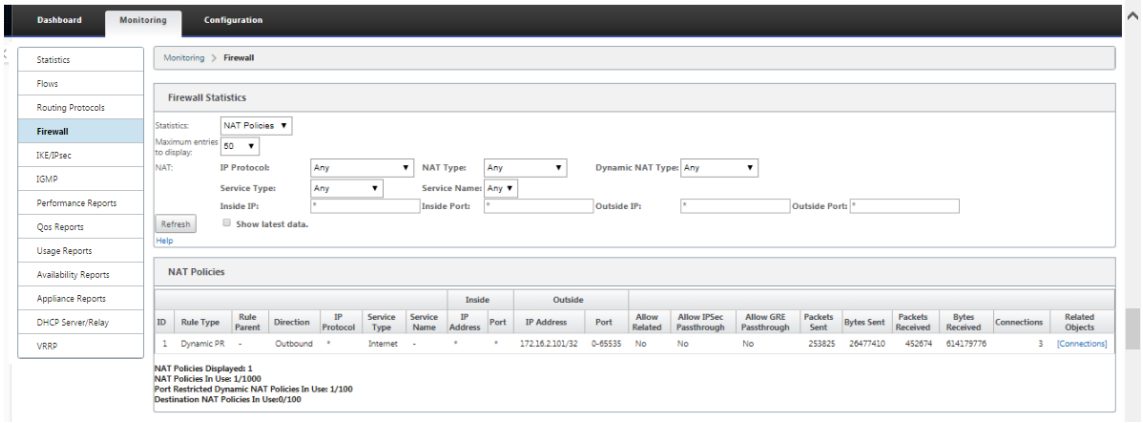
7. 在配置更新期间删除或更新 DNAT 规则。

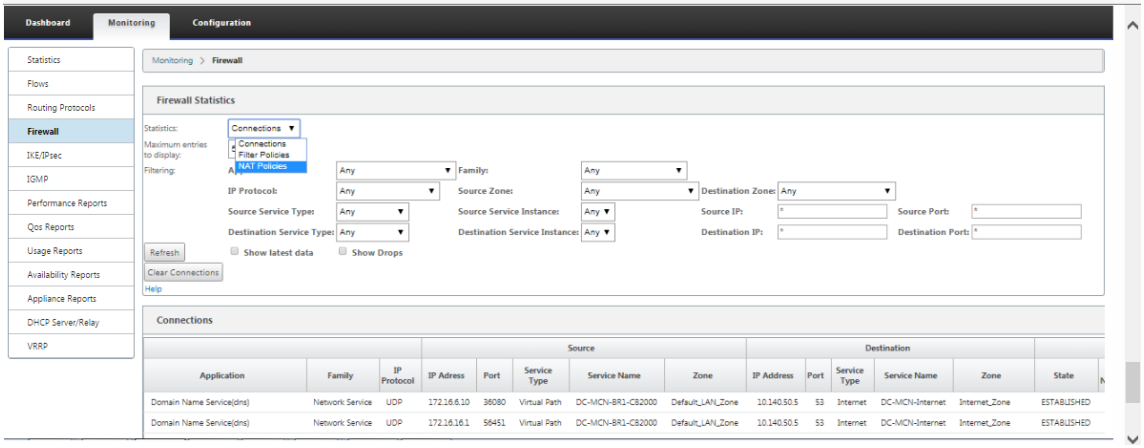
监视目标 **NAT** 策略（防火墙）

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 监视 > 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** 隧道的 **Palo Alto** 集成

June 22, 2021

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，可以使用 Palo Alto 网络下一代防火墙或符合 IPsec 标准的第三方设备（包括
SD-WAN），该设备可以建立到该服务的 IPsec 隧道。

- 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 隧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。可以在 Citrix SD-WAN Center 中配置 Palo Alto 网络。

在开始为远程网络配置 Prisma Access 服务之前，请确保已准备好以下配置，以确保您能够成功启用该服务并为远程网络位置中的用户强制执行策略：

1. 服务连接—如果您的远程网络位置需要访问公司总部的基础设施以验证用户身份或启用对关键网络资产的访问，则必须设置对您的企业网络的访问，以便总部和远程网络位置连接。

如果远程网络位置是自主的，并且不需要访问其他位置的基础设施，则无需设置服务连接（除非您的移动用户需要访问）。

1. 模板—Prisma Access 服务自动为远程网络的 Prisma Access 服务创建模板堆栈(Remote_Network_Template_Stack)和热门模板（Remote_Network_Template）。要为远程网络配置 Prisma Access 服务，请从头开始配置热门模板或利用现有配置（如果您已在本地运行 Palo Alto 网络防火墙）。

   该模板需要设置来建立 IPsec 隧道和 Internet 密钥交换 (IKE) 配置，用于远程网络位置与 Prisma Access 服务之间的协议协商，您可以在安全策略中引用的区域，以及日志转发配置文件，以便您可以将日志从远程网络的 Prisma Access 服务转发到日志记录服务。

2. 父设备组—远程网络的 Prisma Access 服务要求您指定包含安全策略、安全配置文件和其他策略对象（如应用程序组和对象以及地址组）的父设备组以及身份验证策略，以便远程网络的 Prisma Access 服务可以一致地对通过 IPSec 隧道路由到远程网络的 Prisma Access 服务的流量实施策略。您需要在 Panorama 上定义策略规则和对象，或使用现有设备组来保护远程网络位置中的用户的安全。

   > 注意：
   >
   > 如果您使用引用区域的现有设备组，请确保将定义区域的相应模板添加到远程网络 _ 模板 _ 堆栈中。

这允许您在配置远程网络的 Prisma Access 服务时完成区域映射。

3. **IP** 子网—为了使 Prisma Access 服务将流量路由到您的远程网络，您必须为要使用 Prisma Access 服务保护的子网提供路由信息。您可以在远程网络位置定义指向每个子网的静态路由，或者在服务连接位置和 Prisma Access 服务之间配置 BGP，或者使用两种方法的组合。

   如果配置两个静态路由并启用 BGP，则静态路由优先。虽然如果远程网络位置只有几个子网，则使用静态路由可能会很方便，但在具有多个具有重叠子网的远程网络的大型部署中，BGP 可以让您更轻松地扩展。

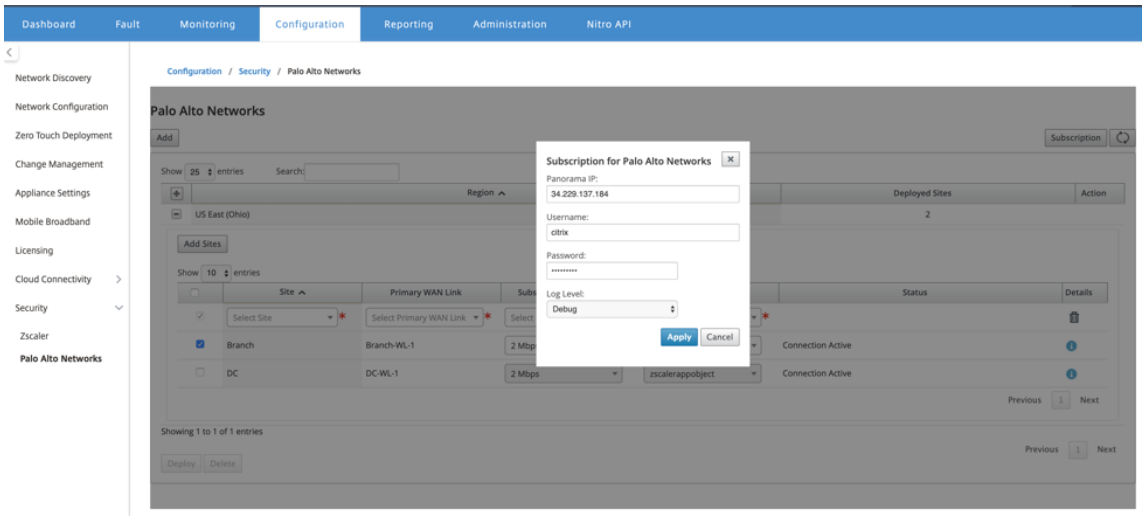
SD-WAN Center 中的 Palo Alto 网络

确保满足以下先决条件：

- 从 PRISMA ACCESS 服务获取全景 IP 地址。
- 在 PRISMA Access 服务中获取用户名和密码用户。
- 在 SD-WAN 设备 GUI 中配置 IPsec 隧道。
- 确保该网站没有登录到一个地区，该地区已经有一个不同的网站配置了不同的 IP/IPSec 配置文件，而不是 Citrix-IKE 加密默认值/Citrix-IPSec-加密默认值。
- 请确保 Prisma Access 配置不会手动更改配置时由 SD-WAN Center 更新。

在 Citrix SD-WAN Center GUI 中，提供 Palo Alto 订阅信息。

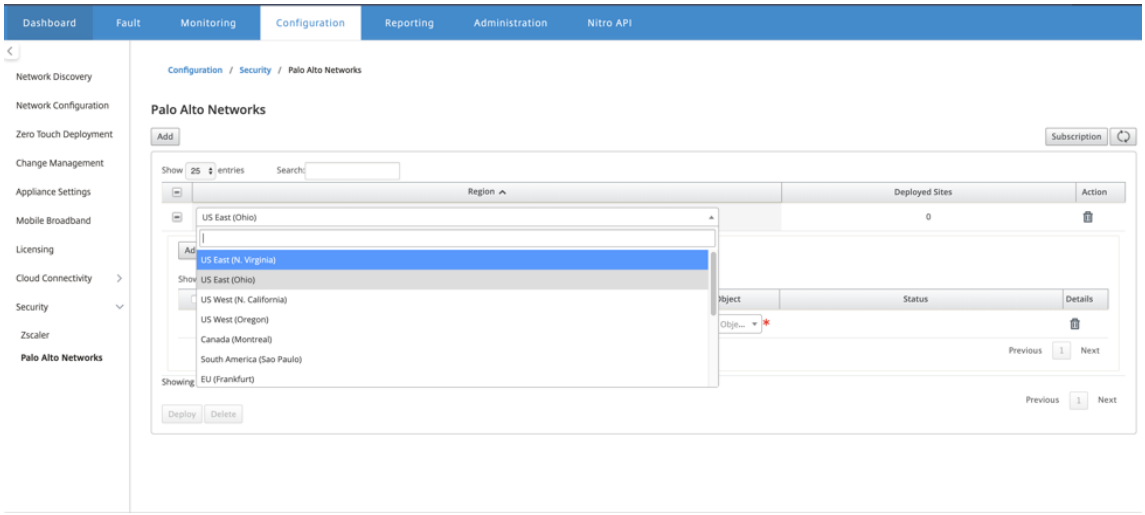
- 配置全景 IP 地址。您可以从 Palo Alto 获得此 IP 地址（PRISMA ACCESS 服务）。
- 配置 PRISMA ACCESS 服务中使用的用户名和密码。

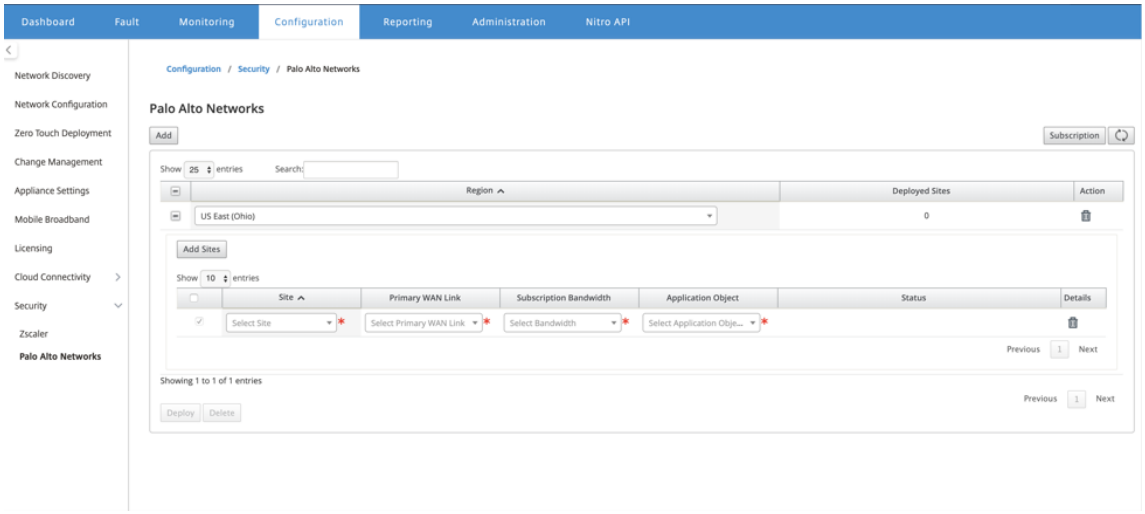


添加和部署站点

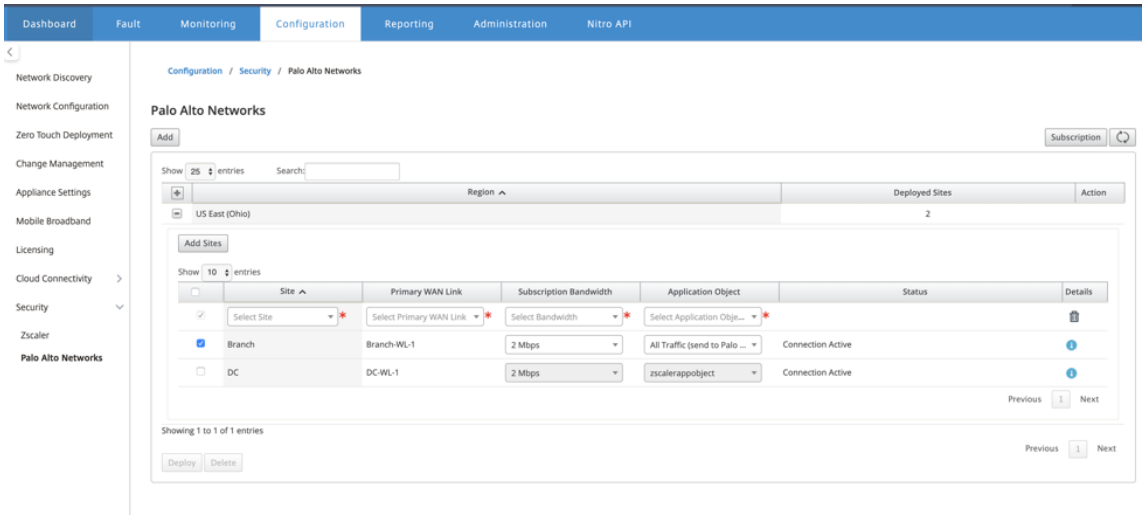
1. 若要部署站点，请选择要为 Prisma Access 区域配置的 PRISMA ACCESS 网络区域和 SD-WAN 站点，然后选择站点 WAN 链接、带宽和应用程序对象进行流量选择。

> 注意：
>
> 如果所选带宽超过可用带宽范围，则流量会受到影响。
>
> 通过选择 应用程序对象选择 下的 所有流量 选项，可以选择将 所有 **Internet** 绑定的流量 重定向到 PRISMA ACCESS 服务。

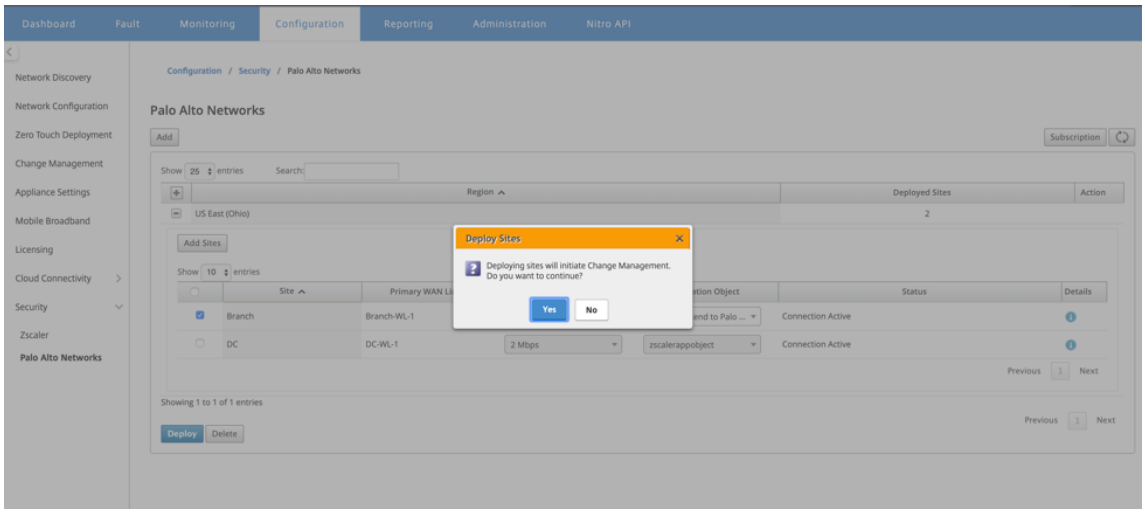




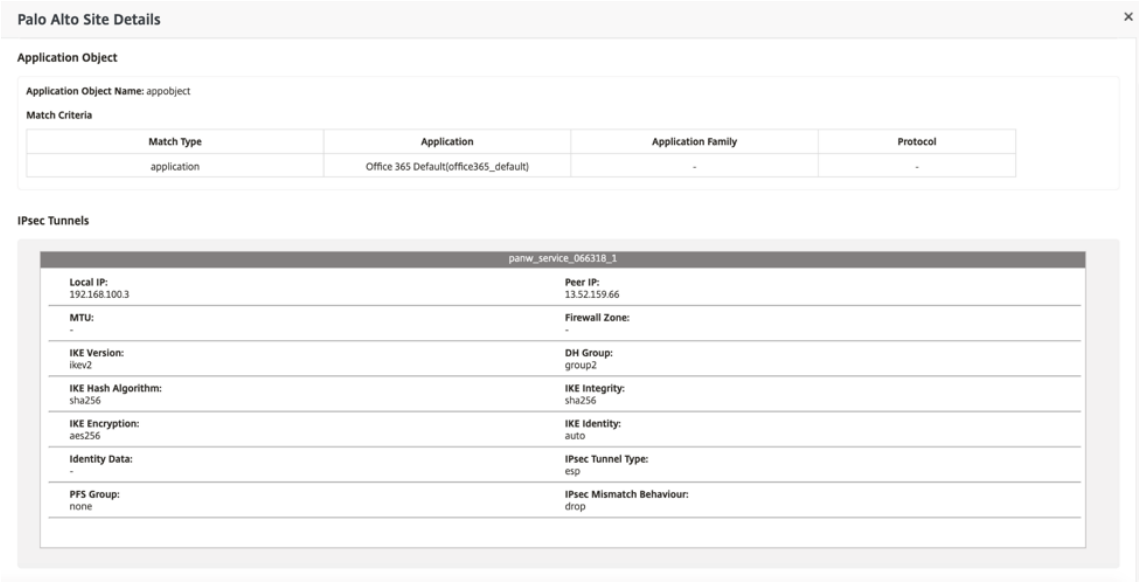
2. 您可以根据需要继续添加更多 SD-WAN 分支站点。



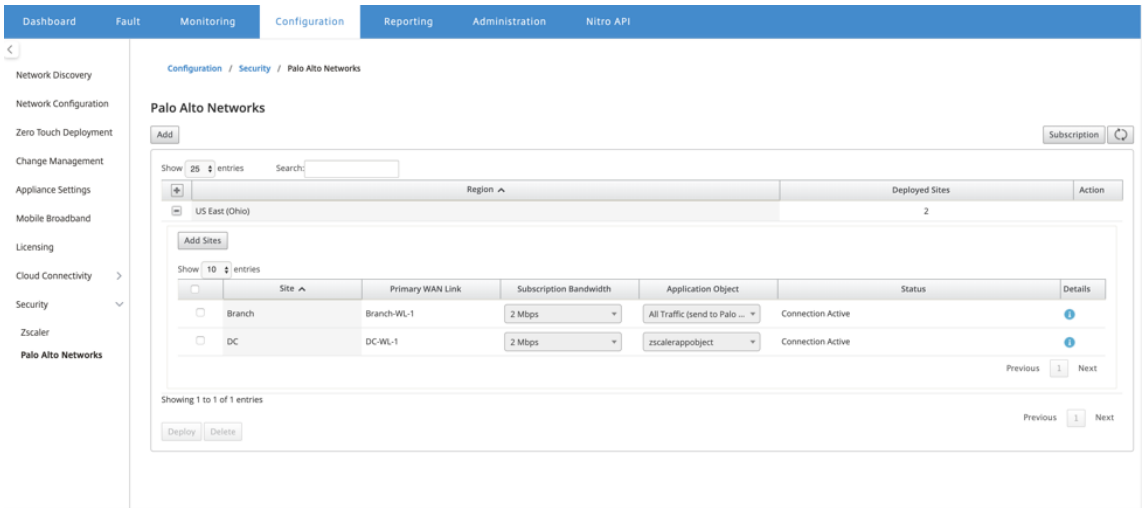
3. 单击部署。启动更改管理流程。单击“是”继续。



部署后，用于建立隧道的 IPsec 隧道配置如下。



登录页面显示在不同 SD-WAN 区域中配置和分组的所有站点的列表。



验证端到端流量连接：

- 从分支机构的 LAN 子网访问互联网资源。
- 验证流量是否通过 Citrix SD-WAN IPsec 隧道进入 Palo Alto Prisma Access。
- 验证是否在“监视”选项卡下对流量应用了 Palo Alto 安全策略。
- 验证从互联网到分支中的主机的响应是通过的。

有状态防火墙和 NAT 支持

June 22, 2021

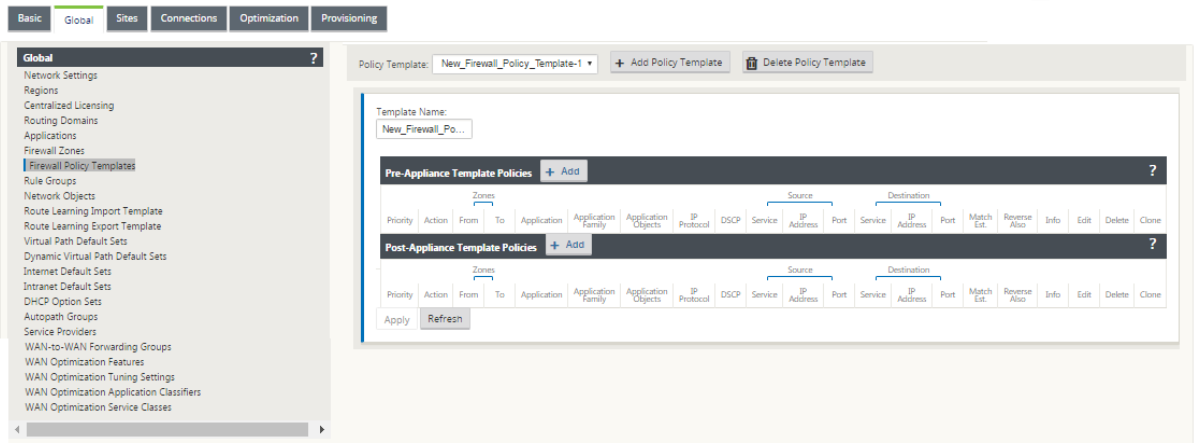
此功能提供内置于 SD-WAN 应用程序中的防火墙。防火墙允许服务和区域之间的策略，并支持静态 NAT、动态 NAT (PAT) 和带端口转发的动态 NAT。更多防火墙功能包括：

- 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

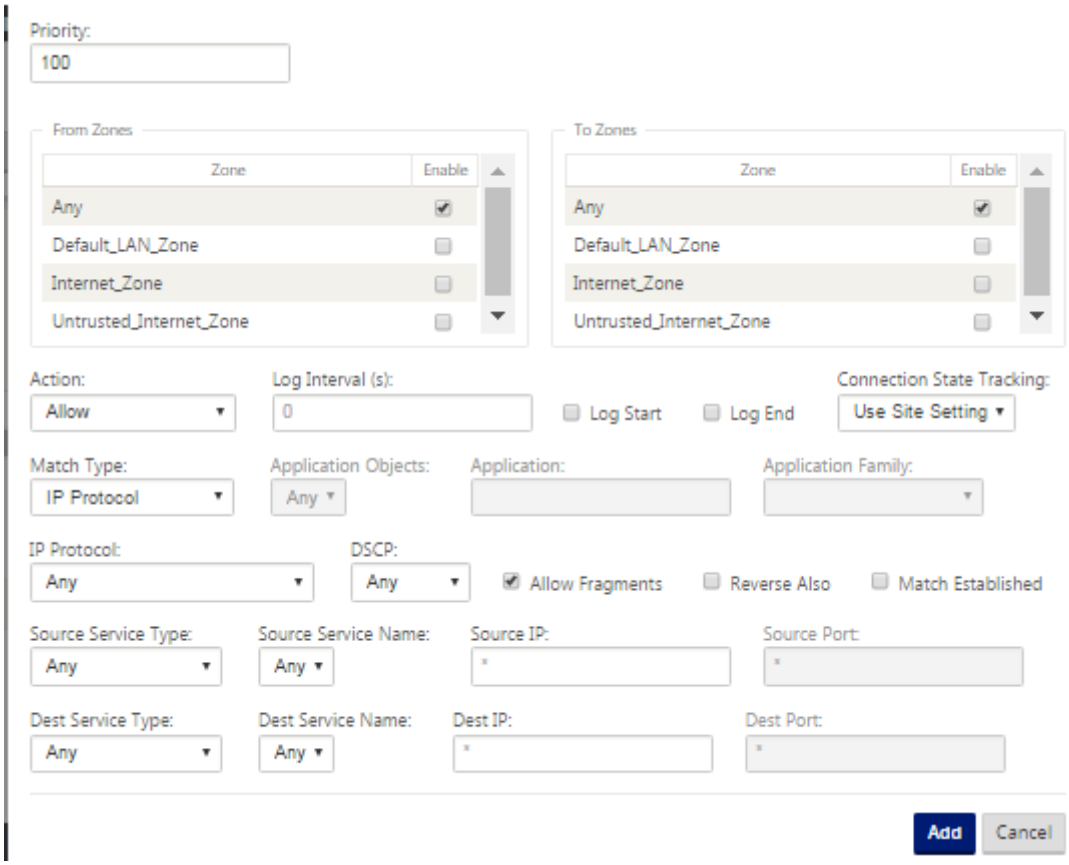
为了简化配置过程，将在全局配置级别创建防火墙策略。此全局配置由设备前站点和设备后站点策略模板组成，可应用于 SD-WAN 网络中的所有站点。

> 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。

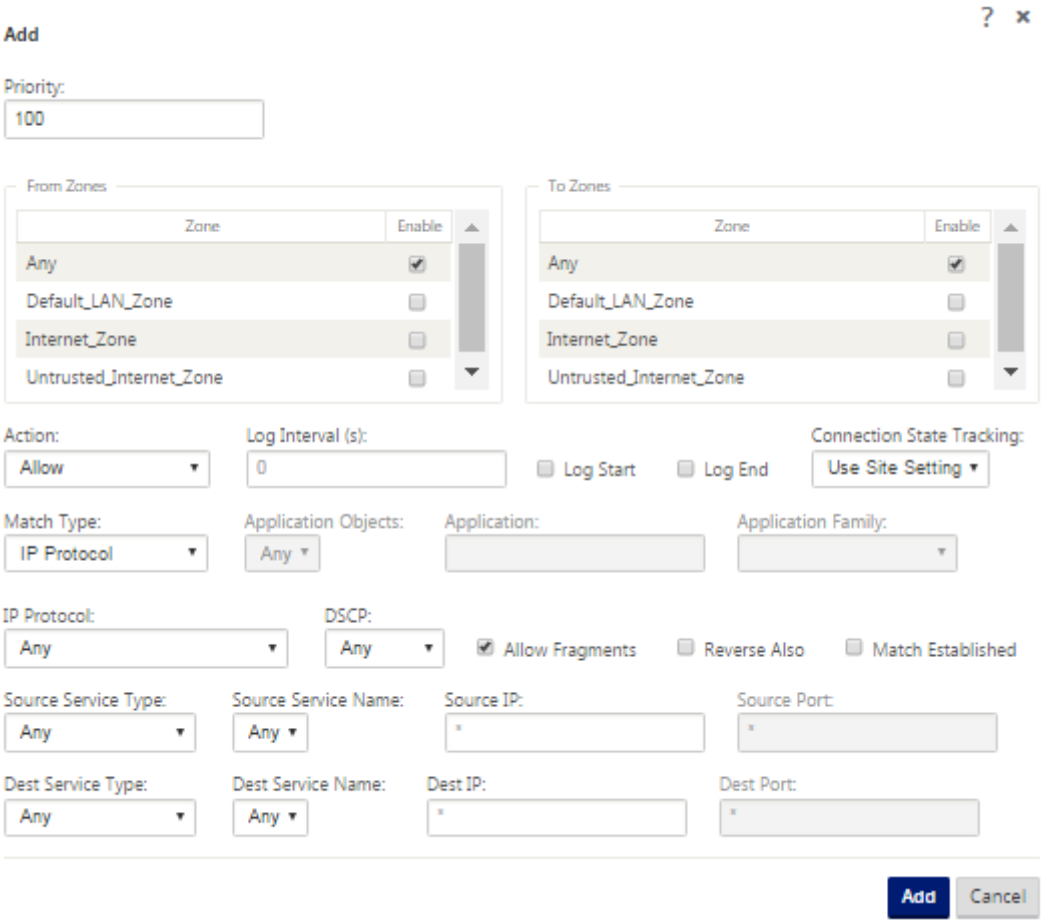
全球策略模板



策略前模板



政策后模板



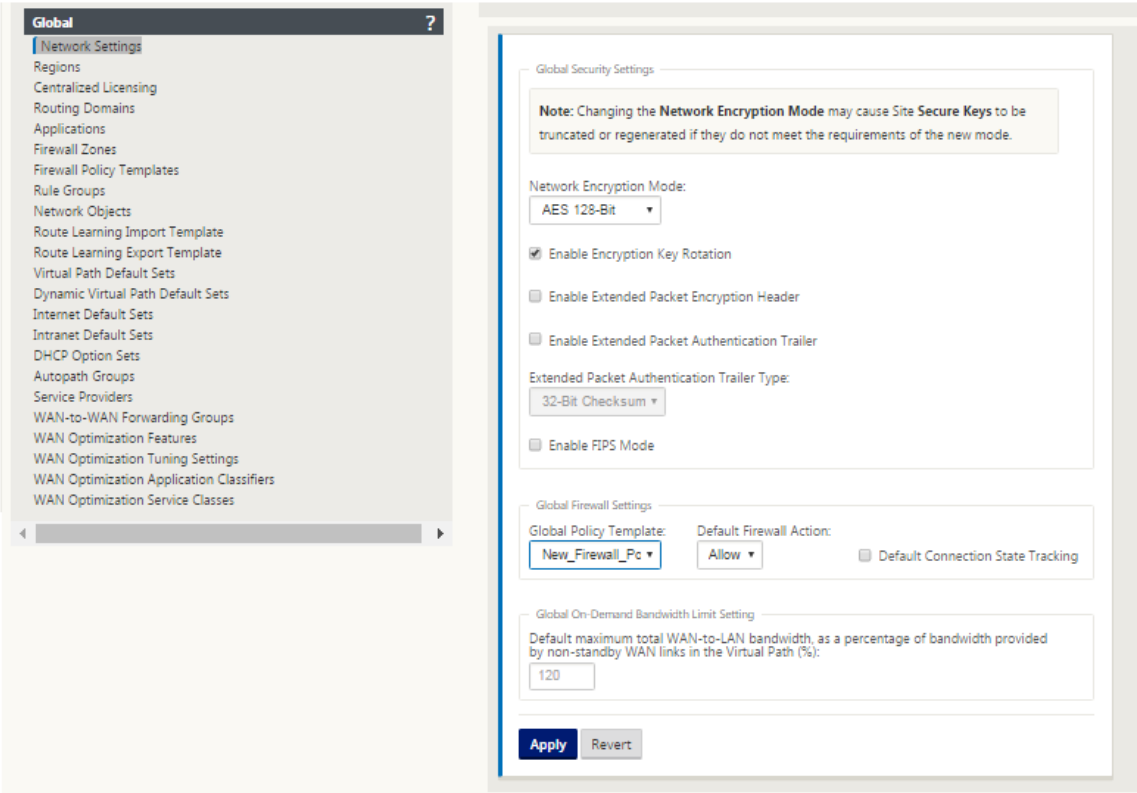
全局防火墙设置

June 22, 2021

创建防火墙策略模板后，您可以使用此策略配置 NetScaler SD-WAN 网络的防火墙设置。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。

要配置全局防火墙设置，请执行以下操作：

1. 在 配置编辑器中，导航到 全局 > 网络设置，然后单击编辑图标。



2. 在“全局防火墙设置”部分中，为以下选项选择值：
   - 全局策略模板 -选择要应用于 SD-WAN 网络中所有设备的防火墙策略模板，默认防火墙操作 -选择允许以允许数据包与筛选器策略不匹配。选择 删除，以删除与筛选器策略不匹配的数据包，默认连接状态跟踪-这将启用与筛选器策略或 NAT 规则不匹配的 TCP、UDP 和 ICMP 流的定向连接状态跟踪。这会阻止非对称流，即使没有定义防火墙策略也是如此。
3. 单击应用。

> 注意
>
> 您也可以在站点级别配置这些设置，这将覆盖全局设置。

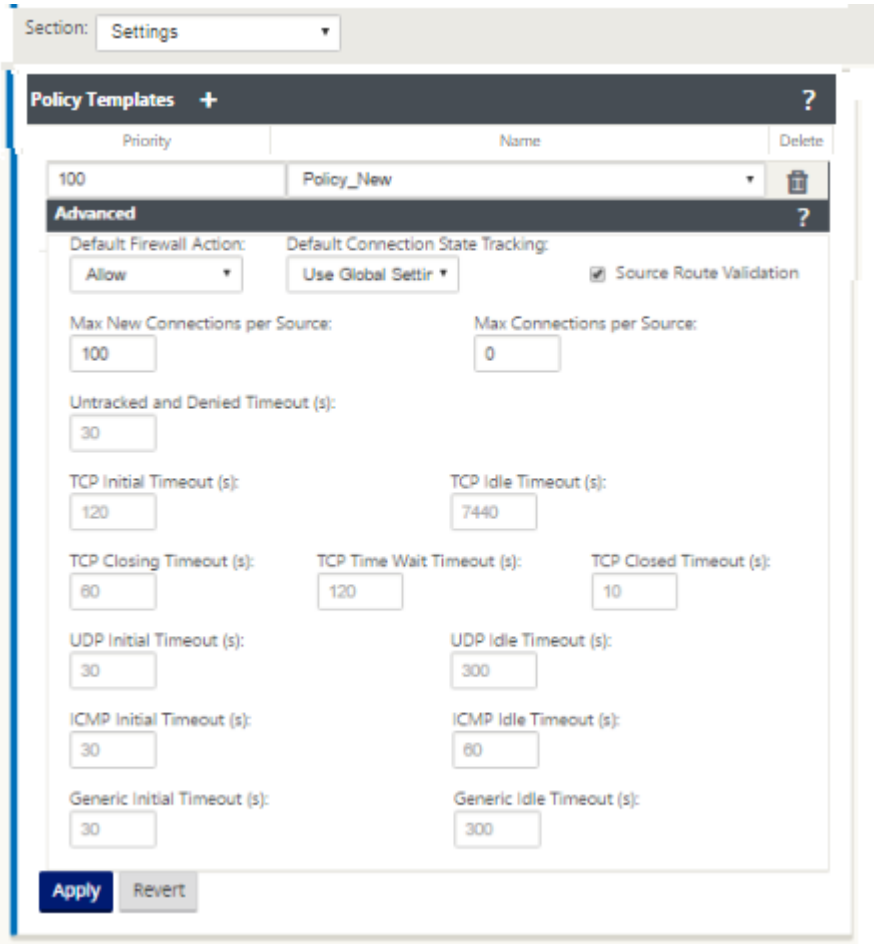
高级防火墙设置

June 22, 2021

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。

要配置高级防火墙设置，请执行以下操作：

1. 在 配置编辑器中，导航到 连接 > 查看站点 > 防火墙 > 设置。



2. 在 策略模板 部分，单击 添加。输入以下参数的值。
   - 优先级 -策略在站点上应用的顺序。
   - **Name** -要在站点上使用的策略模板的名称。
3. 单击高级。输入以下参数的值：
   - 默认防火墙操 作-选择以下选项之一。
     - 使用全局设置-使用 NetScaler SD-WAN 设置中配置的全局设置
     - 允许-允许不匹配任何筛选器策略的数据包。
     - **Drop**-删除与任何筛选器策略不匹配的数据包。
   - 默认连接状态跟踪—选择以下选项之一。
     - 使用全局设置 -使用 NetScaler SD-WAN 设置中配置的全局设置
     - 无跟踪 -不会对不匹配任何筛选策略的数据包执行双向连接状态跟踪
     - **Track** -将对不匹配任何筛选器策略或 NAT 规则的 TCP、UDP 和 ICMP 数据包执行双向连接状态跟踪。这会阻止非对称流，即使没有定义防火墙策略也是如此。

- 源路由验证：如果启用，则在接口上与数据包的路由不同（由源 IP 地址决定）接收数据包时，数据包将被丢弃。仅考虑数据包当前匹配的路由。
- 每个源的最大新连接数：每个源 IP 地址允许的最大未建立连接数。0 表示无限。使用此设置可帮助防止防火墙上的拒绝服务攻击。
- 每个源的最大连接数：每个源 IP 地址允许的最大连接数。0 表示无限。使用此设置可帮助防止防火墙上的拒绝服务攻击。

4. 配置各种超时设置，然后单击 应用。

区域

June 22, 2021

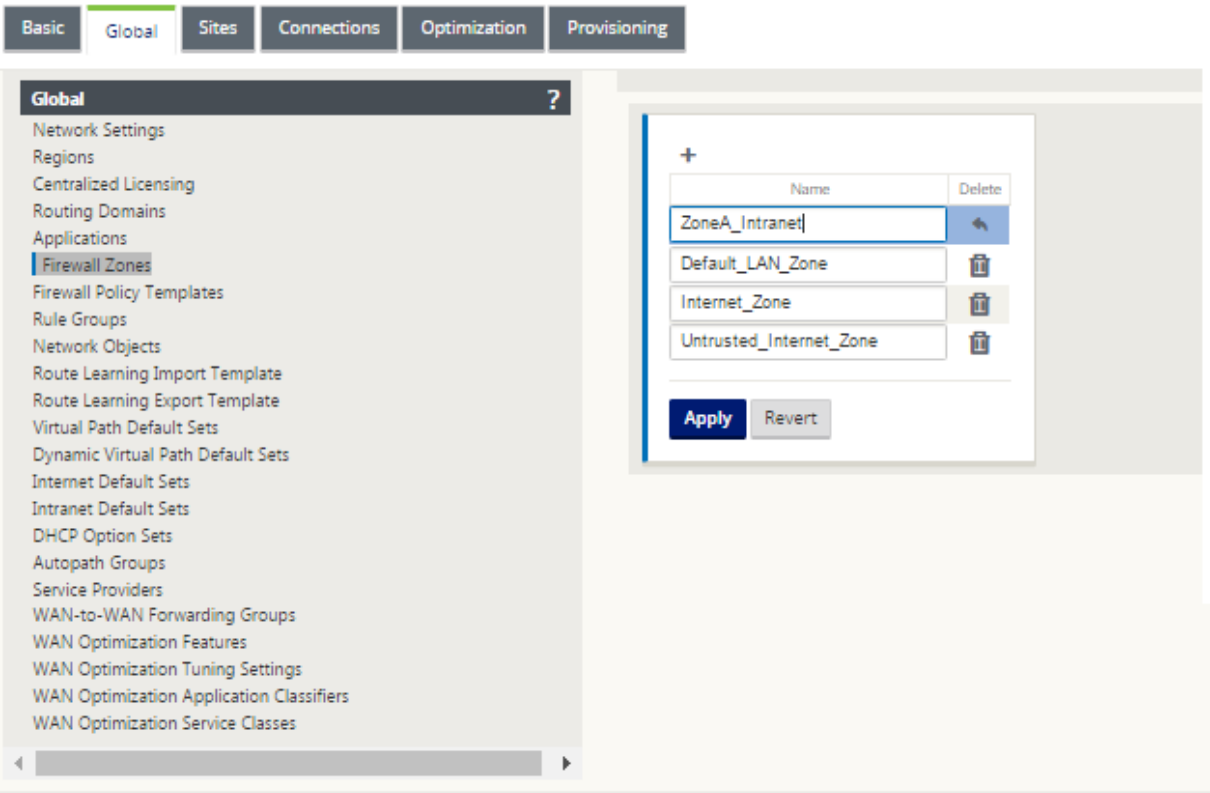
您可以在网络中配置区域并定义策略以控制流量进出区域的方式。默认情况下，将创建以下区域：

- 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：

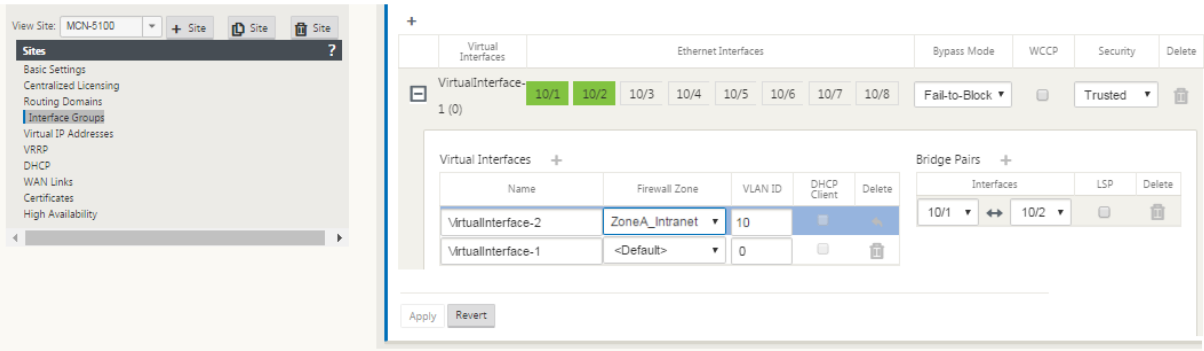
- 虚拟网络接口 (VNI)
- 内联网服务
- GRE 通道
- 局域网 IPsec 隧道

下图显示了预配置的三个区域。此外，您可以根据需要创建自己的区域。在此示例中，区域“Zonea_Intranet”是用户创建的区域。它被分配到 SD-WAN 设备旁路段（端口 1 和端口 2）的虚拟接口。



数据包的源区域由接收数据包的服务或虚拟网络接口决定。这种情况的例外是虚拟路径流量。当流量进入虚拟路径时，数据包将标记为源自流量的区域，并通过虚拟路径传输该源区域。这允许虚拟路径的接收端在进入虚拟路径之前根据原始源区域做出策略决策。

例如，网络管理员可能需要定义策略，以便只允许站点 A 的 VLAN 30 的流量进入站点 B 的 VLAN 10。管理员可以为每个 VLAN 分配一个区域，并创建允许这些区域之间的流量并阻止来自其他区域的流量的策略。下面的屏幕截图显示了用户如何将 ZoneA_Intranet 区域分配给 VLAN 10。在此示例中，ZoneA_Intranet 区域之前由用户定义，以便将其分配给虚拟接口 VirtualInterface-2。



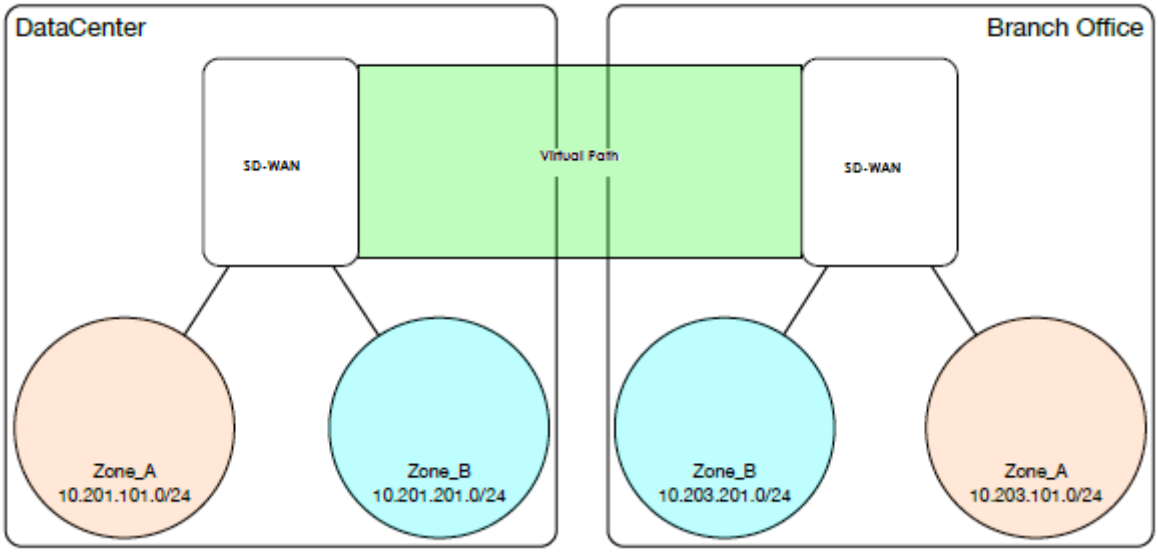
数据包的目标区域根据目标路由匹配确定。SD-WAN 设备在路由表中查找目标子网时，数据包将匹配一个路由，路由分配了一个区域。

- 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。



下面的屏幕截图显示了虚拟 IP (VIP) 从其分配的虚拟网络接口 (VNI) 继承的区域。

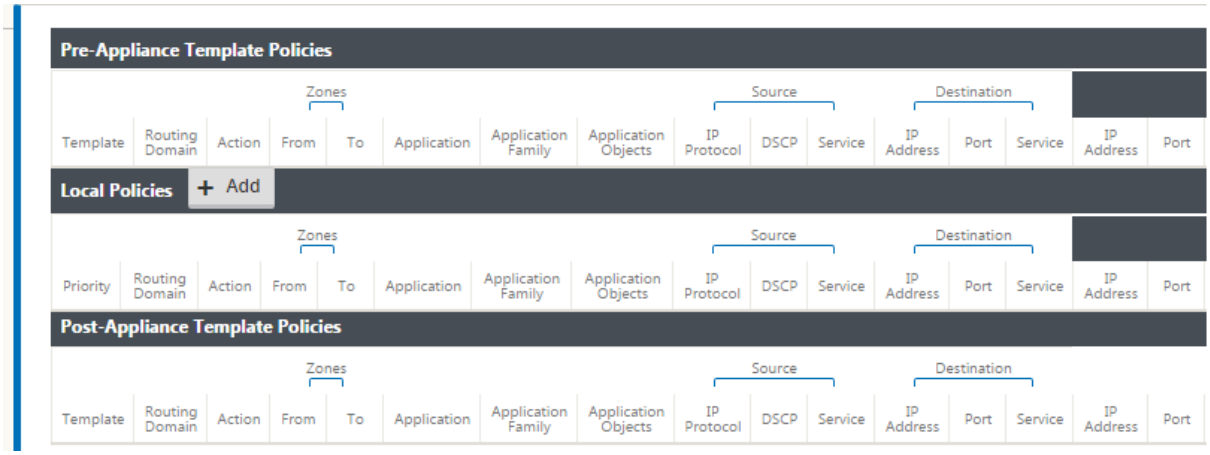
IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
172.16.187.11/24	VirtualInterface-1	Default_LAN_Zone	✔		Trusted	🗑
172.16.187.12/24	VirtualInterface-1	Default_LAN_Zone			Trusted	

策略

June 22, 2021

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。随着 SD-WAN 网络的发展，将难以将这些策略单独应用到每个站点。若要解决此问题，可以使用防火墙策略模板创建防火墙筛选器组。防火墙策略模板可以应用于网络中

的所有站点，也可以仅应用于特定站点。这些策略按设备前模板策略或设备后模板策略进行排序。网络范围的前设备和后设备模板策略均在全局级别进行配置。本地策略在 连接 下的站点级别配置，并仅应用于该特定站点。



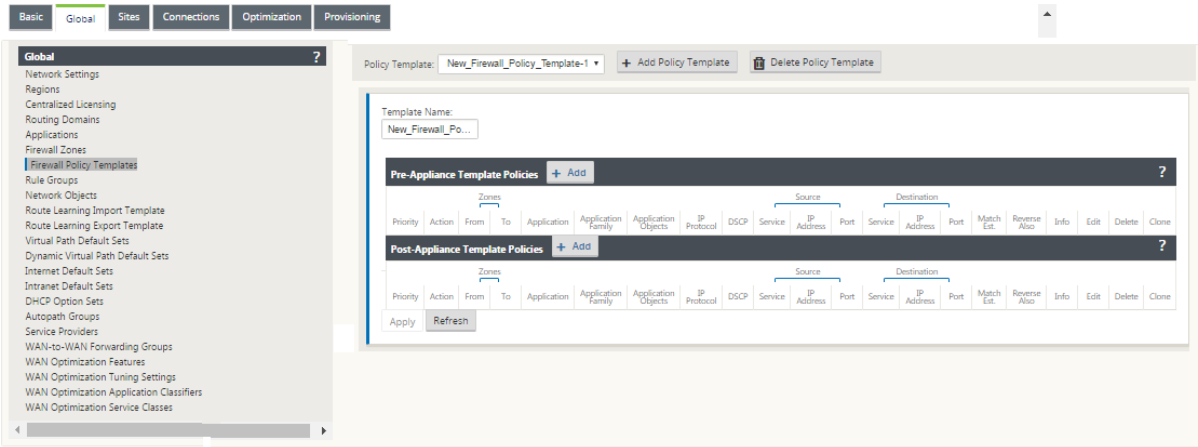
设备前模板策略应用于任何本地站点策略。接下来应用本地站点策略，后面是设备后模板策略。目标是通过允许您应用全局策略，同时保持应用特定于站点的策略的灵活性，从而简化配置过程。

筛选策略评估顺序

1. 预模板—从所有模板“PRE”部分编译的策略。
2. 全局前—从全球“PRE”部分编译的策略。
3. 本地—设备级策略。
4. 本地自动生成—自动本地生成的策略。
5. 后模板—从所有模板“POST”部分编译的策略。
6. 后全局—从全局“POST”部分编译的策略。

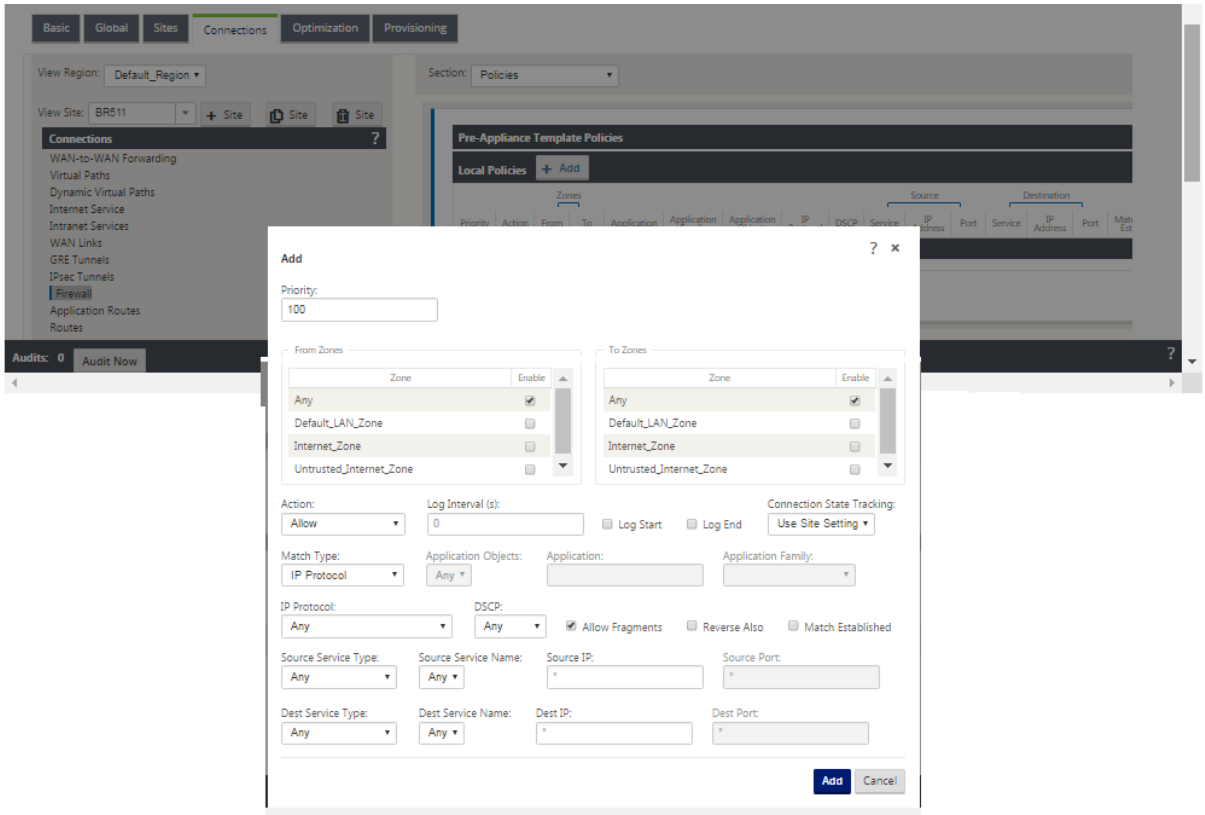
政策定义-全局和本地（站点）

您可以在全局级别配置设备前和设备后模板策略。本地策略在设备的站点级别应用。



以上屏幕截图显示了将应用于全局 SD-WAN 网络的策略模板。要将模板应用到网络中的所有站点，请导航到全局 > 网络设置 **>** 全局策略模板，然后选择特定策略。在站点级别，您可以添加更多策略模板，以及创建特定于站点的策略。

策略的特定可配置属性显示在下面的屏幕截图中，这些属性对于所有策略都是相同的。



策略属性

- 优先级—在所有定义策略中应用策略的顺序。优先级较低的策略在优先级较高的策略之前应用。
- 区域—流具有源区域和目标区域。

  - 来自区域—策略的源区域。
  - 到区域—策略的目标区域。

- 操 作—在匹配的流程上执行的操作。
  - 允许—允 许流经防火墙。
  - **Drop** —通过删除数据包来拒绝通过防火墙的流。
  - 拒绝—拒绝 通过防火墙的流，并发送特定于协议的响应。TCP 将发送重置，ICMP 将发送错误消息。
  - 计数并继续—计算此流的数据包和字节数，然后继续下去策略列表。
- 日志间隔—记录与防火墙日志文件或 syslog 服务器匹配的数据包数（如果已配置）之间的时间（以秒为单位）。
  - 日志开始—如果选中，则会为新流创建一个日志条目。
  - 日志结束—在删除流时记录流的数据。

> 注意
>
> 默认的日志间隔值为 0 表示没有日志记录。

- **Track** —允许防火墙跟踪流的状态，并在 监视 > 防火墙 > 连接 表中显示此信息。如果未跟踪流，状态将显示 NOT_TRACKED。请参阅下表，了解基于协议的状态跟踪。使用 防火墙 > 设置 **> **** 高 级 > 默认跟踪 下的站点级别定义的设置 **。
  - 无跟踪—未启用流状态。
  - **Track** —显示流的当前状态（与此策略匹配）。
- 匹配类型—选择以下匹配类型之一
  - **IP** 协议—如果选择了此匹配类型，请选择筛选器将与之匹配的 IP 协议。选项包括任何，TCP，UDP ICMP 等
  - 应用程序—如果选择了此匹配类型，则指定用作此筛选器匹配条件的应用程序。
  - 应用程序系 列—如果选择了此匹配类型，请选择用作此筛选器匹配条件的应用程序系列。
  - 应用程序对象—如果选择了此匹配类型，则选择用作此筛选器的匹配条件的应用程序系列。

有关应用程序、应用程序系列和应用程序对象的更多信息，请参阅应用分类。

- **DSCP** —允许用户在 DSCP 标签设置上进行匹配。
- 允许片段—允许匹配此筛选器策略的 IP 片段。

> 注意
>
> 防火墙不会重新组装碎片框架。

- 另外反向—自动添加此筛选器策略的副本，同时源和目标设置已反转。

- 匹配已建立—将允许传出数据包连接的传入数据包匹配。
- 源服务类型—参考 SD-WAN 服务—本地（到设备）、虚拟路径、Intranet、IPhost 或 Internet 是服务类型的示例。
- **IPhost** 选项 -这是防火墙的新服务类型，用于 SD-WAN 应用程序生成的数据包。例如，从 SD-WAN 的 Web UI 运行 ping 会产生来自 SD-WAN 虚拟 IP 地址的数据包。为此 IP 地址创建策略需要用户选择 IPhost 选项。
- 源服务名称—与服务类型关联的服务名称。例如，如果为源服务类型选择了虚拟路径，则这将是特定虚拟路径的名称。这并不总是必需的，取决于所选服务类型。
- 源 **IP** 地址—筛选器将使用的典型 IP 地址和子网掩码进行匹配。
- 源端口—特定应用程序将使用的源端口。
- 目标服务类型 -参考 SD-WAN 服务-本地（到设备）、虚拟路径、Intranet、IPhost 或 Internet 是服务类型的示例。
- 目标服务名 称-与服务类型关联的服务名称。这并不总是必需的，取决于所选服务类型。
- 目标 **IP** 地址 -筛选器将使用的典型 IP 地址和子网掩码进行匹配。
- 目标端口—特定应用程序将使用的目标端口（即 TCP 协议的 HTTP 目标端口 80）。

轨道选项提供了有关流程的更多详细信息。状态表中跟踪的状态信息如下所示。

轨道选项的状态表

只有几个状态是一致的：

- **INIT-** 连接创建，但初始数据包无效。
- **O_DENIED-** 创建连接的数据包将被筛选器策略拒绝。
- 来自响应程序的 **R_DENIED** 数据包被筛选策略拒绝。
- **NOT_TRACKED-** 连接没有状态跟踪，但被允许。
- **CLOSED-** 连接已超时，否则由协议关闭。
- **DELETED-** 正在删除连接。DELETED 状态几乎永远不会被看到。

所有其他状态都是特定于协议的，并且需要启用状态跟踪。

TCP 可以报告以下状态：

- **SYN_SENT** - 看到第一个 TCP SYN 消息。
- **SYN_SENT2** - 在两个方向上看到的 SYN 消息，没有 SYN+ACK（AKA 同时打开）。
- **SYN_ACK_RCVD** - 已收到 SYN+ACK。
- 建立**-** 第二 ACK 接收, 连接完全建立.

- **FIN_WAIT** - 看到第一个 FIN 消息。
- **CLOSE_WAIT** - 在两个方向上看到的 FIN 消息。
- **TIME_WAIT** - 在两个方向上看到的最后一个 ACK。连接现在已关闭，等待重新打开。

所有其他 IP 协议（尤其是 ICMP 和 UDP）都具有以下状态：

- **NEW** - 在一个方向上看到的数据包。
- 建立 -在两个方向上看到的数据包。

网络地址转换 (NAT)

June 22, 2021

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 网络能够连接到互联网。Citrix SD-WAN 上的 NAT 功能将您的私有 SD-WAN 网络与公共互联网连接起来。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互联网，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
>
> NAT 功能只能在站点级别进行配置。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。

静态 NAT

June 8, 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，互联网服务到局域网服务—对于接收的数据包（互联网到局域网），将转换源 IP 地址。对于传输的数据包（LAN 到互联网），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，局域网服务到互联网服务—对于传输的数据包（局域网到互联网），将转换源 IP 地址。对于接收的数据包（互联网到局域网），将转换目的 IP 地址。

区域派生

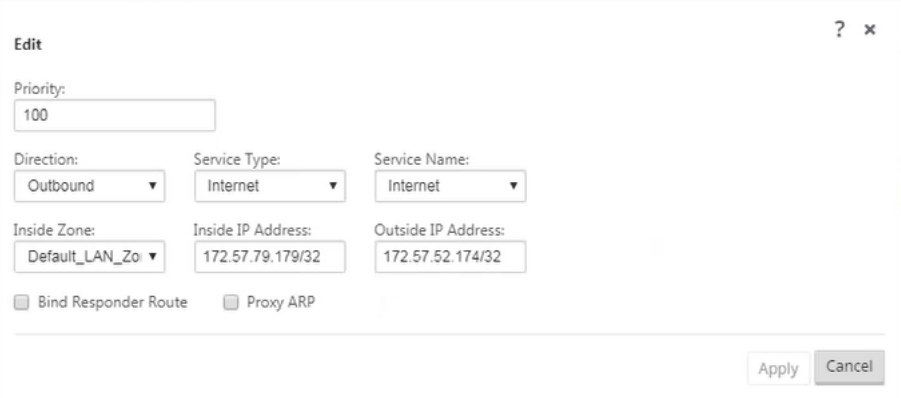
入站或出站流量的源和目标防火墙区域不应相同。如果源防火墙区域和目标防火墙区域相同，则不会对流量执行 NAT。

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，受信任的互联网链接上的 Internet 服务与受信任的互联网区域相关联。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。

配置静态 **NAT** 策略

要配置静态 NAT 策略，请在配置编辑器中导航到 连接 > 防火墙 > 静态 **NAT** 策略。



- 优先级：在所有定义的策略中应用策略的顺序。优先级较低的策略在优先级较高的策略之前应用。
- 方向：从虚拟接口或服务的角度来看，流量的流动方向。它可以是入站流量，也可以是出站流量。
- 服务类型：应用 NAT 策略的 SD-WAN 服务类型。对于静态 NAT，支持的服务类型包括本地、虚拟路径、Internet、Intranet 和路由间域服务
- 服务名称：选择与服务类型相对应的已配置服务名称。
- 内部区域：数据包必须来自的内防火墙区域匹配类型才能进行转换。
- 外部区域：数据包必须来自的外部防火墙区域匹配类型才能进行转换。

- 内部 **IP** 地址：满足匹配条件时必须转换为的内部 IP 地址和前缀。
- 外部 **IP** 地址：如果满足匹配条件，则内部 IP 地址转换为的外部 IP 地址和前缀。
- 绑定响应方路由：确保响应流量通过接收响应流量的同一服务发送，以避免非对称路由。
- 代理 **ARP**：确保设备响应外部 IP 地址的本地 ARP 请求。

IPv6 互联网服务的静态 **NAT** 策略

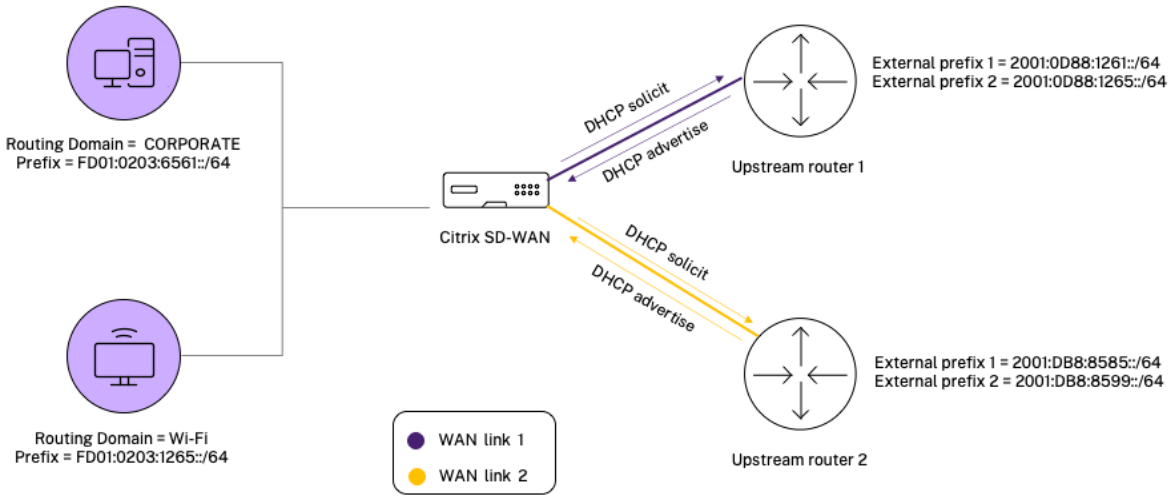
Citrix SD-WAN 从 11.4.0 版开始支持 IPv6 互联网服务的静态 NAT 策略。IPv6 Internet 服务的静态 NAT 策略指定将内部网络前缀映射到外部网络前缀。所需的静态 NAT 策略的数量取决于内部网络的数量和外部网络（WAN 链路）的数量。如果有 **M** 个内部网络和 **N** 个 WAN 链路，则所需的静态 NAT 策略数为 **M x N**。

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：

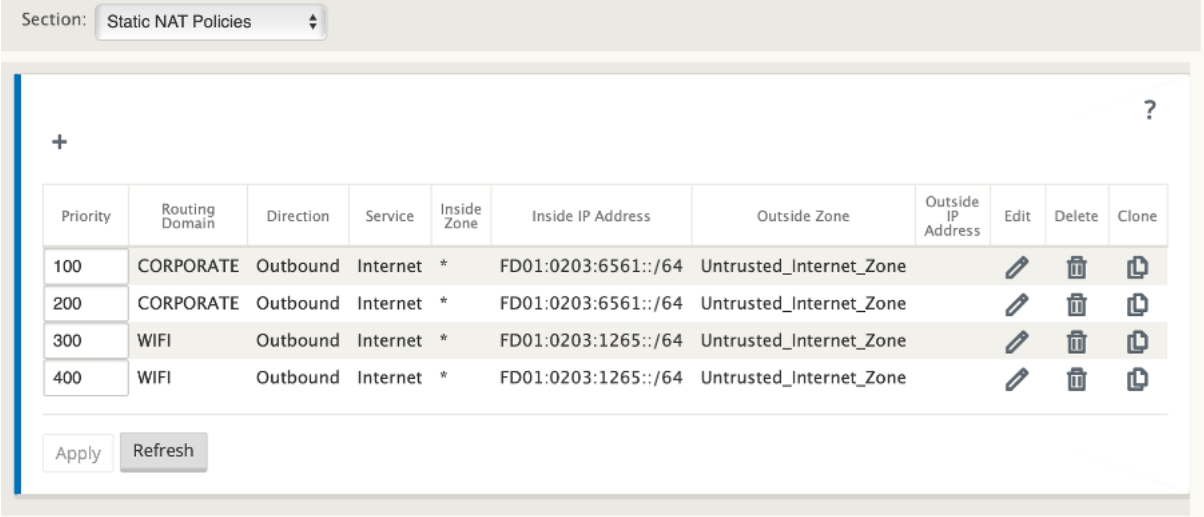
- 内部网络 1 驻留在具有网络前缀 FD 01:0203:6561⊠ /64 的企业路由域中
- 内部网络 2 驻留在 Wi-Fi 路由域中，网络前缀为 FD 01:0203:1265⊠ /64
- 通过 WAN Link 1，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001：0 D 88:1261⊠ /64 和 2001:0 D 88:1265⊠ /64 从上游委派路由器接收。当来自内部网络的流量通过 WAN link 1 时，这两个委派的前缀将用作外部网络前缀。
- 通过 WAN Link 2，SD-WAN 设备通过 DHCPv6 前缀委派、2 个委派前缀 2001：DB 8:8585⊠ /64 和 2001:DB 8:8599⊠ /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 互联网服务所需的静态 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：

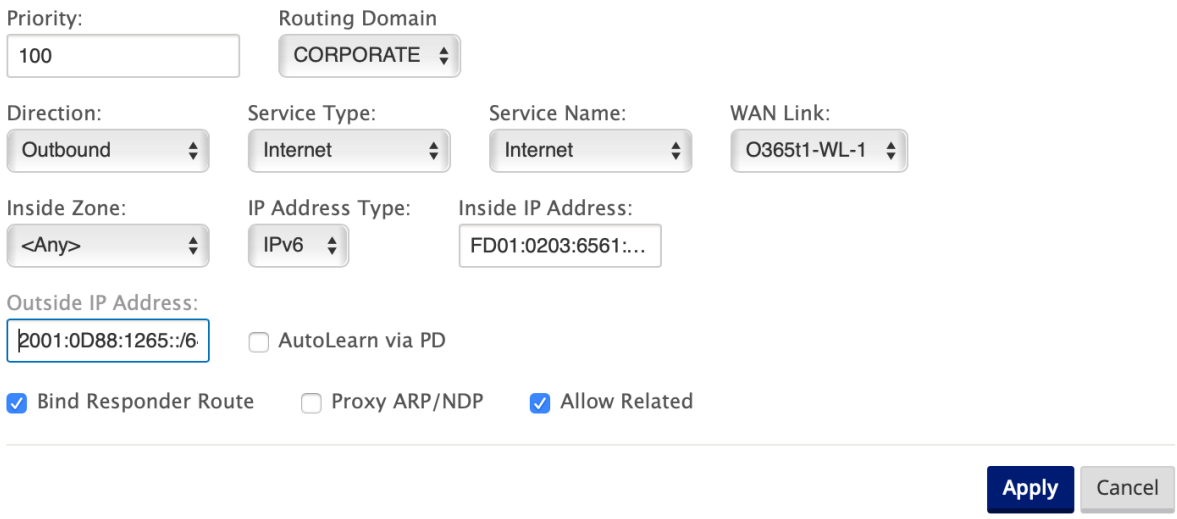
- 通过 WAN 链路 1 在网络 1 内部
- 在网络 1 内部通过 WAN 链路 2
- 通过 WAN 链路 1 在网络 2 内部
- 通过 WAN 链路 2 在网络 2 内部

要配置这些静态 NAT 策略，请在配置编辑器中导航到 连接 **>** 防火墙 **>** 静态 **NAT** 策略。



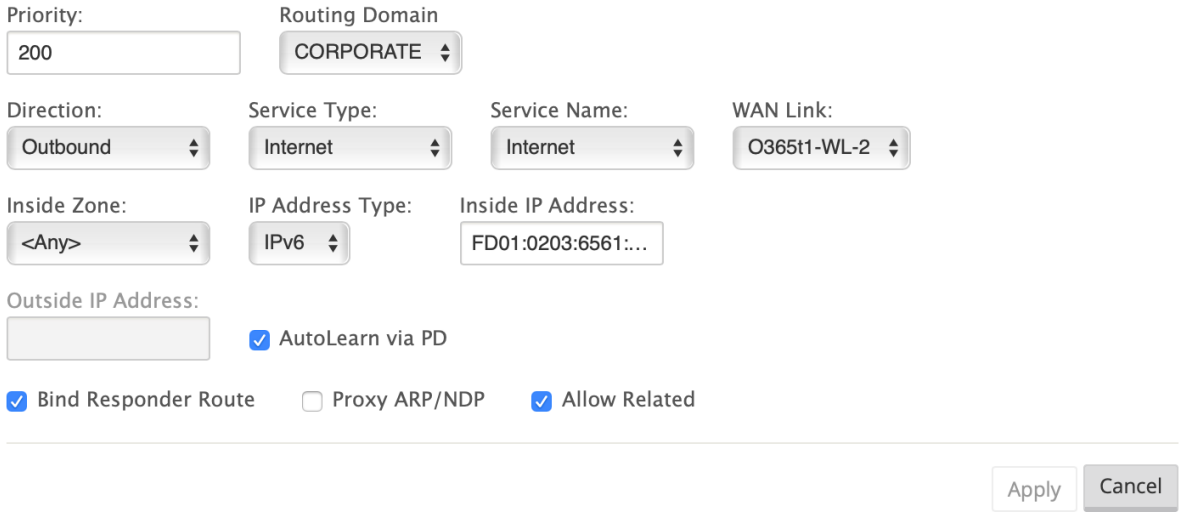
创建 NAT 策略时，请确保选择 服务类型 作为 互联网，将 **IP** 地址 类型选择为 **IPv6**。选择 WAN 链接，然后在 内部 **IP** 地址 字段中输入内部网络前缀（仅允许使用 /64 前缀）。在 外部 **IP** 地址 字段中，您可以手动输入外部网络前缀或选中 通过 **PD** 自动学习 复选框。

以下是在静态 NAT 策略中手动输入外部 IP 地址的示例。



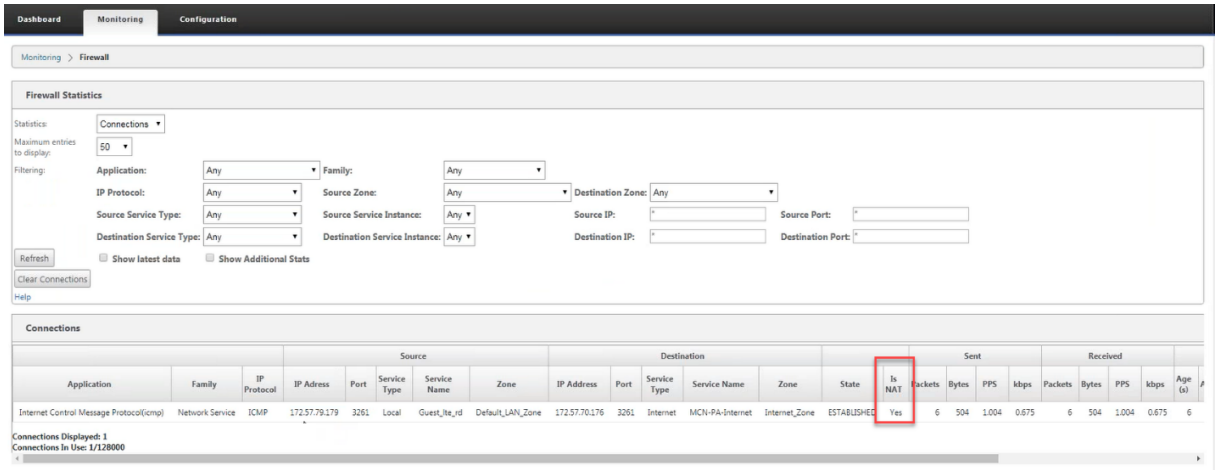
如果选中 通过 **PD** 自动学习 复选框，请确保上游路由器支持 DHCPv6 前缀委派。Citrix SD-WAN 向上游委派路由器请求前缀，委派路由器会向 Citrix SD-WAN 使用前缀进行响应。Citrix SD-WAN 使用此委派前缀将内部 IP 地址转换为外部 IP 地址。

以下是启用 了通过 **PD** 自动学习 的示例，以便通过 DHCPv6 前缀委派获取外部网络前缀。

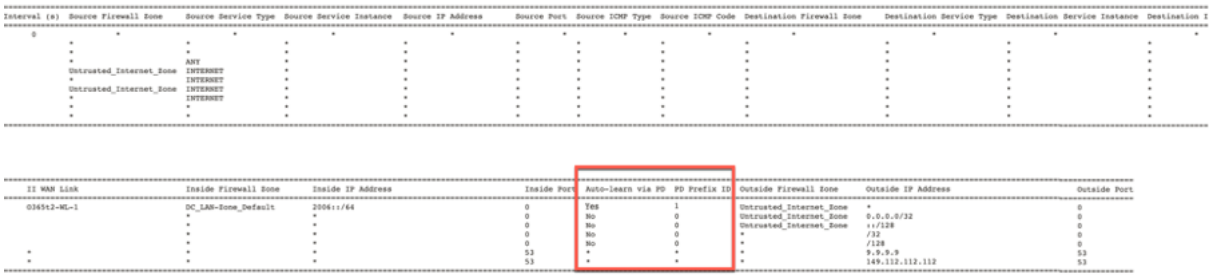


监视

要监控 NAT，请导航到 监 控 > 防火墙统计 > 连接。对于连接，你可以看到 NAT 是否完成。

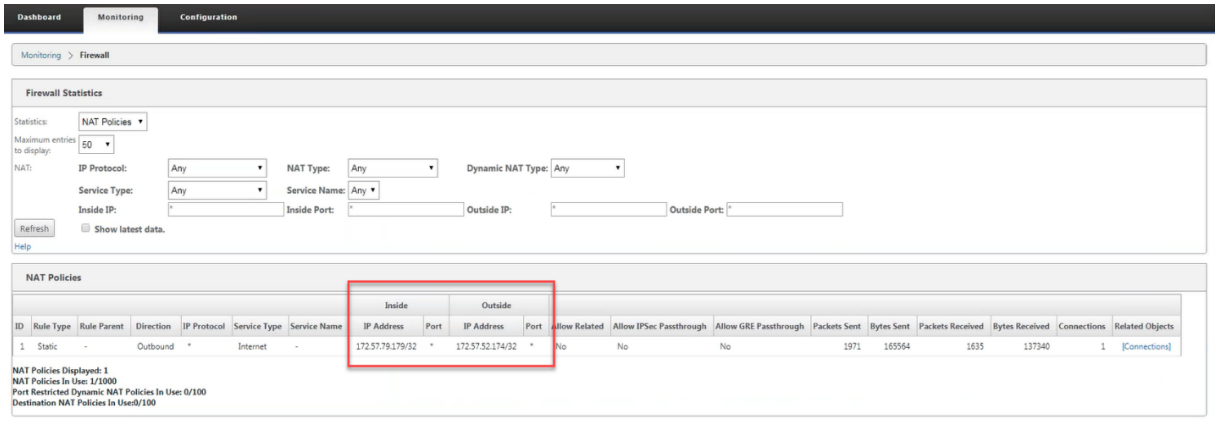


要检查是否为任何 NAT 规则配置了通过 PD 自动学习，请导航到 配置 **>** 虚拟 **WAN >** 查看配置，然后从视 图 下拉列表中选择 防火墙。通过 **PD** 自动学习 和 **PD** 前缀 **ID** 列显示详细信息。

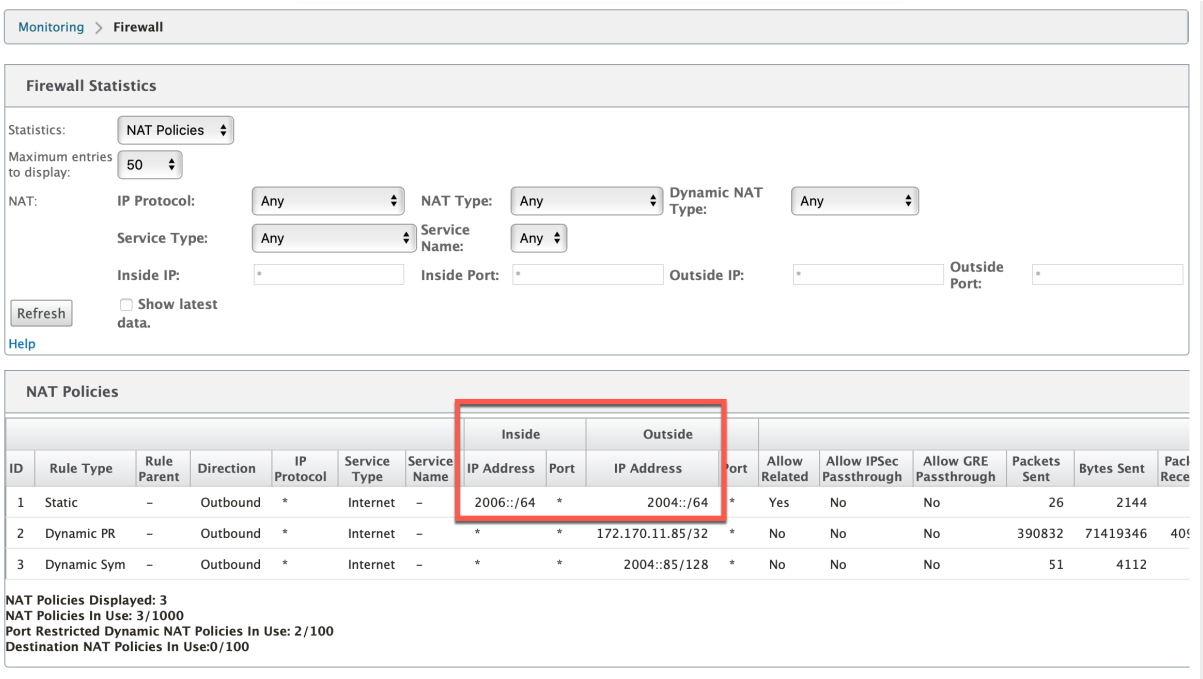


要进一步查看内部 IP 地址到外部 IP 地址的映射，请单击 相关对象 下的 路由后 **NAT** ，或导航到 监控 > 防火墙统计 > **NAT** 策略。

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。



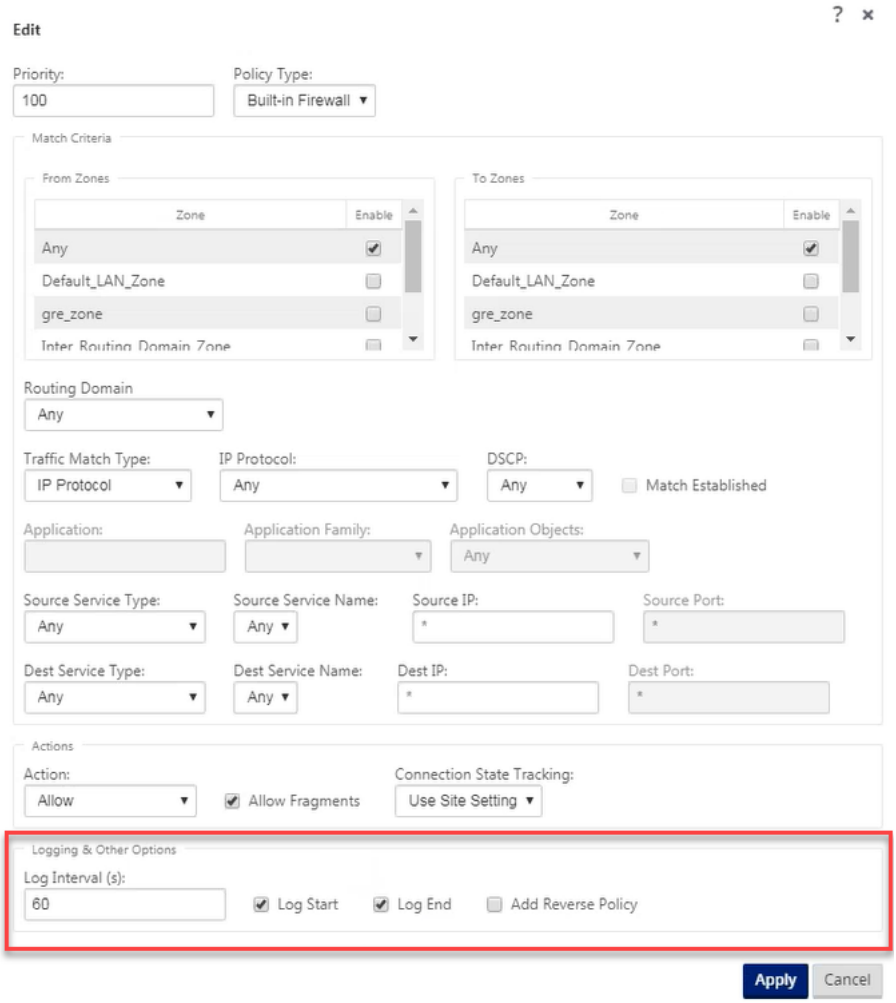
以下屏幕截图显示了 IPv6 静态 NAT 策略中内部地址与外部地址的映射。



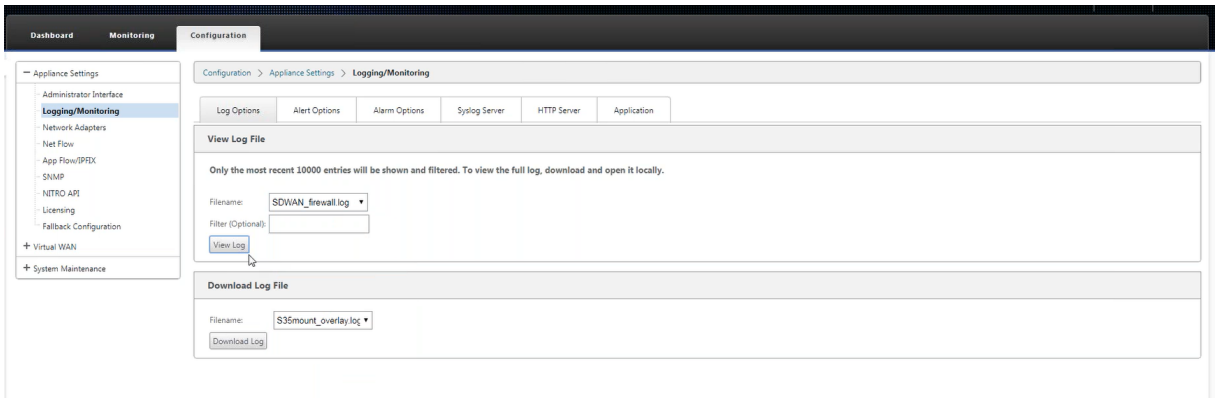
日志

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:8704      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**

June 8, 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 地址连接到互联网。

- 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互联网 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。

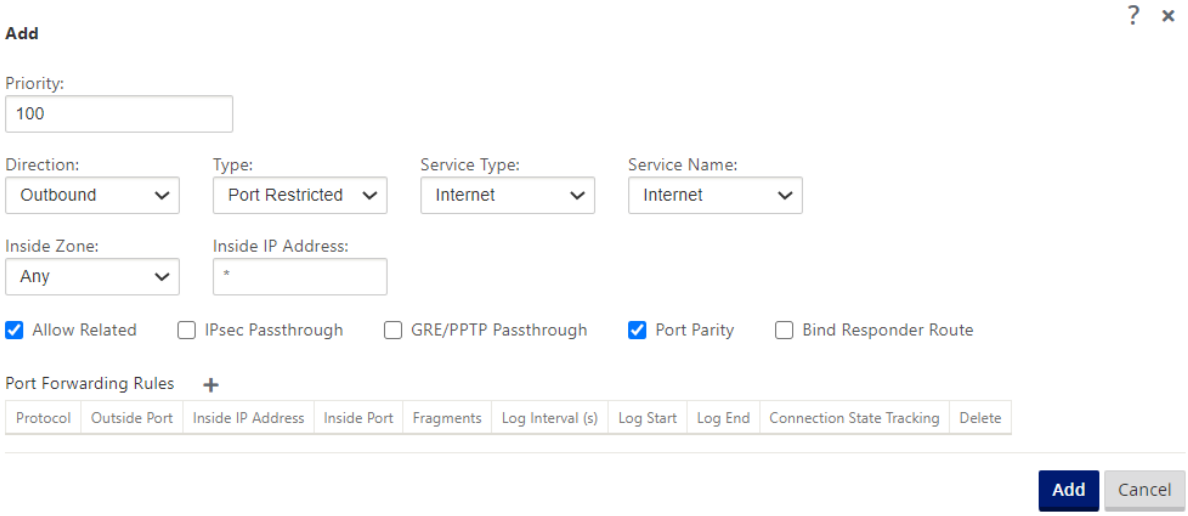
- 出站：对于在服务上接收的数据包，将转换目标地址。对于在服务上传输的数据包，将转换源地址。本地、Internet、内部网和路由间域服务支持出站动态 NAT。对于 WAN 服务（如 Internet 和内部网服务），配置的

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 地址安全地访问互联网。

- 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（如互联网和内部网）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。

配置动态 **NAT** 策略

要配置动态 NAT 策略，请在配置编辑器中导航到 连接 > 防火墙 > 动态 **NAT** 策略。

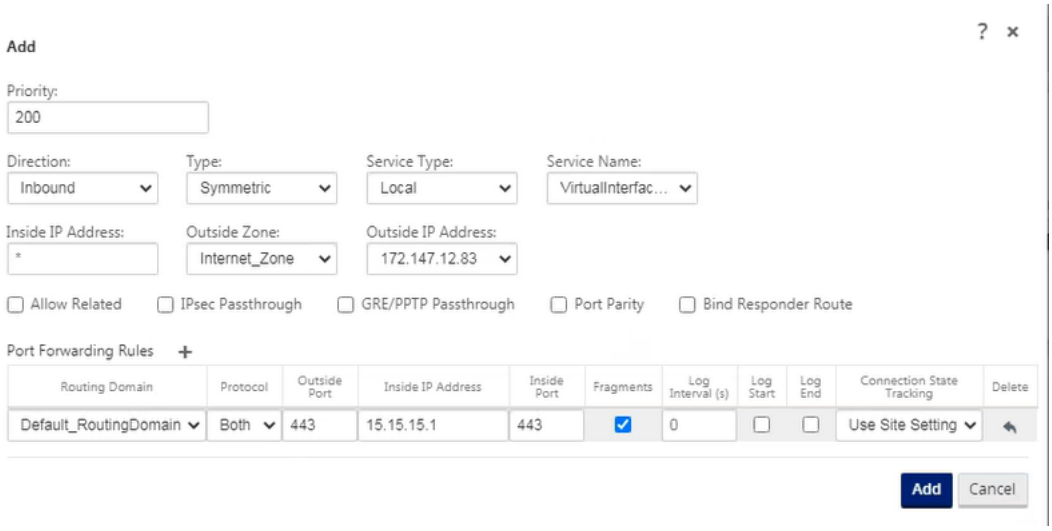


- 优先级：在所有定义的策略中应用策略的顺序。优先级较低的策略在优先级较高的策略之前应用。
- 方向：从虚拟接口或服务的角度来看，流量的流动方向。它可以是入站流量，也可以是出站流量。
- 类型：要执行的动态 NAT 的类型、端口限制或对称。
- 服务类型：应用动态 NAT 策略的 SD-WAN 服务类型。本地和路由间域服务支持入站动态 NAT。本地、Internet、内部网和路由间域服务支持出站动态 NAT
- 服务名称：选择与服务类型对应的已配置服务名称。
- 内部区域：数据包必须来自的内防火墙区域匹配类型才能进行转换。
- 外部区域：对于入站流量，请指定数据包必须来自的外部防火墙区域匹配类型才能进行转换。
- 内部 **IP** 地址：满足匹配条件时必须转换为的内部 IP 地址和前缀。输入“*”表示任何内部 IP 地址。
- 外部 **IP** 地址：如果满足匹配条件，则内部 IP 地址转换为的外部 IP 地址和前缀。对于使用 Internet 和内部网服务的出站流量，已配置的 WAN 链路 IP 地址将动态选择为外部 IP 地址。
- 允许相关：允许与规则匹配的流量相关的流量。例如，如果存在与该策略相关的某种类型的错误，则 ICMP 重定向与该策略匹配的特定流相关。
- **IPSec** 通过：允许翻译 IPsec (AH/ESP) 会话。
- **GRE/PPTP** 通过：允许翻译 GRE/PPTP 会话。

- 端口奇偶校验：如果启用，NAT 连接的外部端口将保持奇偶校验（即使内部端口是偶数，如果外部端口为奇数，则为奇数）。
- 绑定响应程序路由：确保响应流量通过接收响应流量的同一服务发送，以避免非对称路由。

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。



- 协议：TCP、UDP 或两者兼而有。
- 外部端口：转发到内部端口的外部端口。
- 内部 **IP** 地址：转发匹配数据包的内部地址。
- 内端口：外部端口将被转发到的内部端口。
- 片段：允许转发碎片数据包。
- 日志时间间隔：记录与 syslog 服务器匹配策略的数据包数之间的秒钟。默认的日志间隔值为 0 表示没有日志记录。
- 日志开始：如果选择此选项，将为新流程创建一个新的日志条目。
- 日志结束：删除流程时记录流程的数据。
- 跟踪：对与规则匹配的 TCP、UDP 和 ICMP 数据包执行 双向连接状态跟踪。此功能可阻止由于非对称路由或校验和失败、协议特定验证而看起来不合法的流。状态详细信息显示在
  监视 > 防火墙 > 连接下。
- 无跟踪：不对匹配规则的数据包执行双向连接状态跟踪。

每个端口转发规则都有一个父 NAT 规则。外部 IP 地址取自父 NAT 规则。

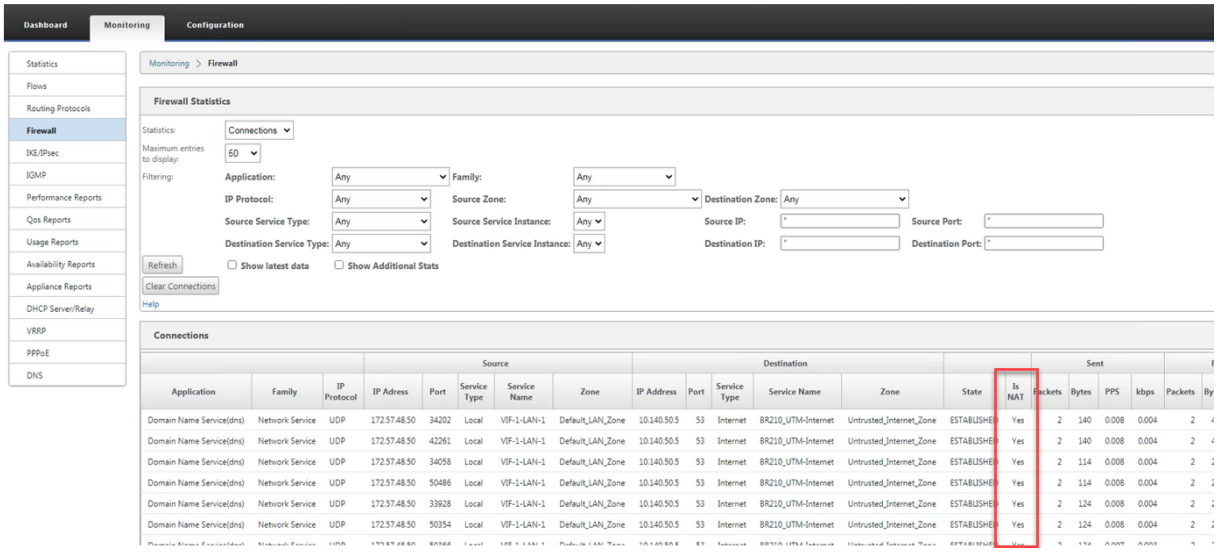
自动创建的动态 **NAT** 策略

在以下情况下，将自动创建互联网服务的动态 NAT 策略：

- 在不受信任的接口（WAN 链接）上配置互联网服务。
- 在单个 WAN 链路上启用所有路由域的互联网访问。有关更多详细信息，请参阅 配置防火墙分段。
- 在 SD-WAN 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。

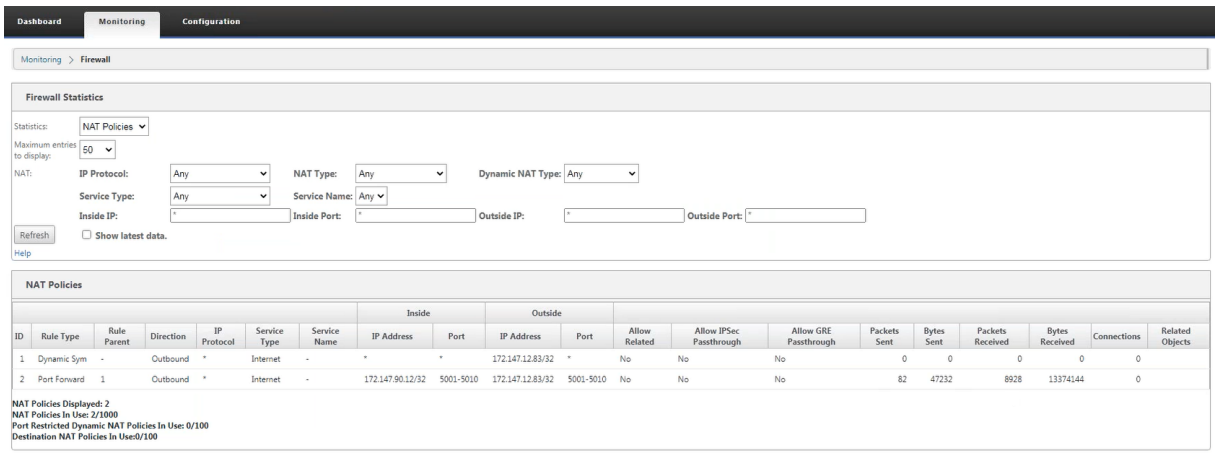
监视

要监视动态 NAT，请导航到 监 控 > 防火墙统计 > 连接。对于连接，你可以看到 NAT 是否完成。

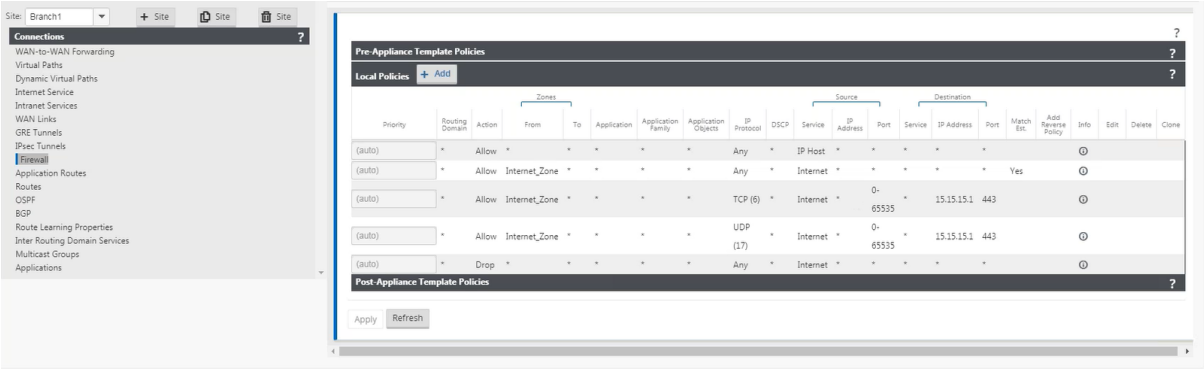


要进一步查看内部 IP 地址到外部 IP 地址的映射，请单击 相关对象 下的 预路由 **NAT** 或路由后 NAT，或导航到监控 > 防火墙统计 >**NAT** 策略。

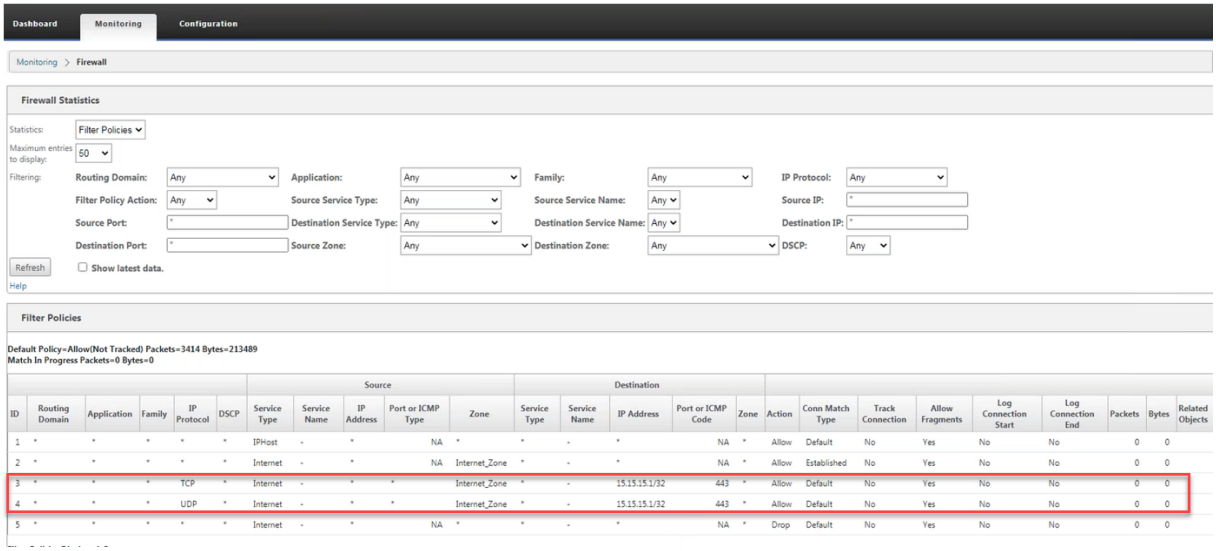
以下屏幕截图显示了对称类型的动态 NAT 规则及其相应的端口转发规则的统计信息。



创建端口转发规则时，也会创建相应的防火墙规则。



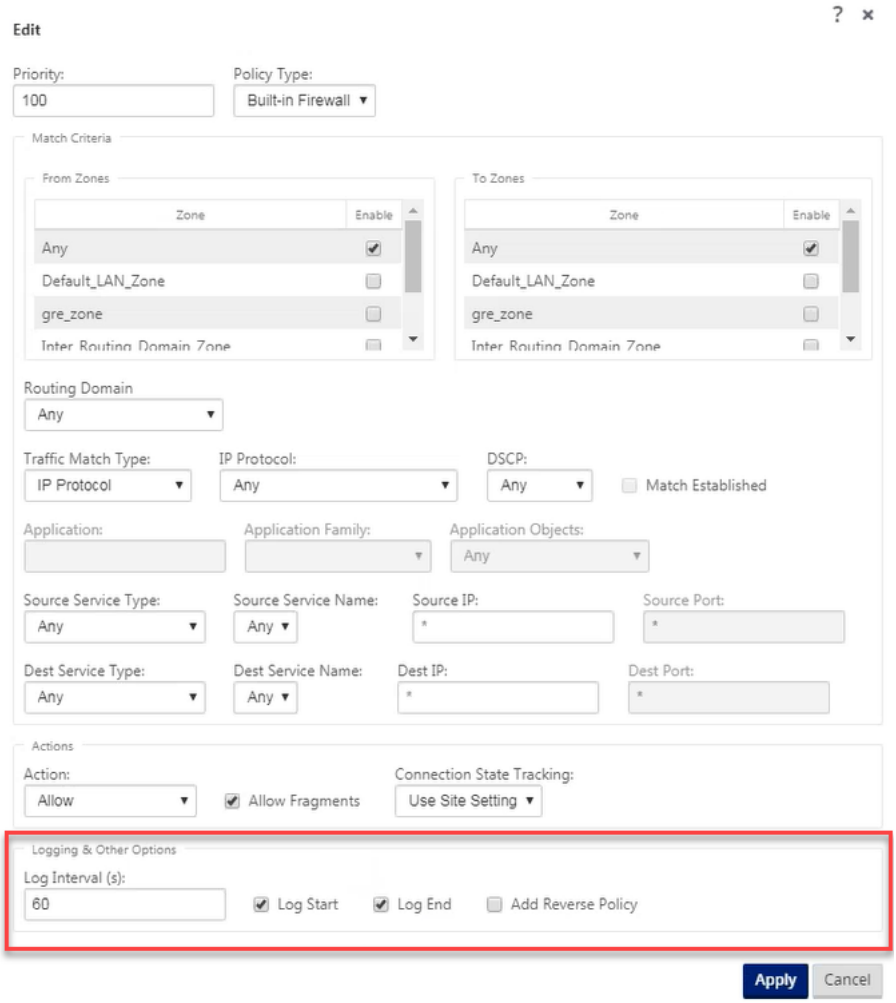
您可以通过导航到 监视 > 防火墙统计信息 **>** 筛选器策略来查看筛选器策略统计信息



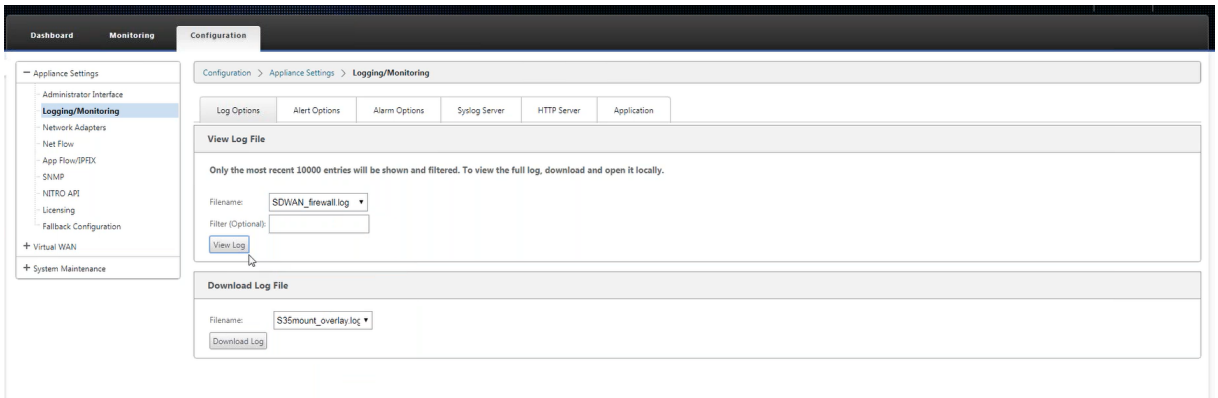
日志

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。


```
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:8704      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)
```

配置虚拟广域网服务

June 22, 2021

Citrix SD-WAN 配置描述并定义了 Citrix SD-WAN 网络的拓扑。必须先定义虚拟 WAN 配置，然后才能部署 SD-WAN 网络。要执行此操作，请在 MCN 设备上的 Citrix SD-WAN 管理 Web 界面中使用配置编辑器。

安全和加密

启用 SD-WAN（对于虚拟路径）的加密是可选的。有关配置此功能的说明，请参阅启用和配置虚拟 WAN 安全和加密（可选）部分

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。您可以使用管理控制节点 (MCN) 上的管理 Web 界面中的配置编辑器来选择、启用和配置这些和其他加密选项。您必须具有 MCN 上的管理访问权限才能修改配置，并在 SD-WAN 网络中分发更改。一旦 MCN 被安全保护，加密设置及其分发也是安全的。

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。

启用虚拟广域网服务

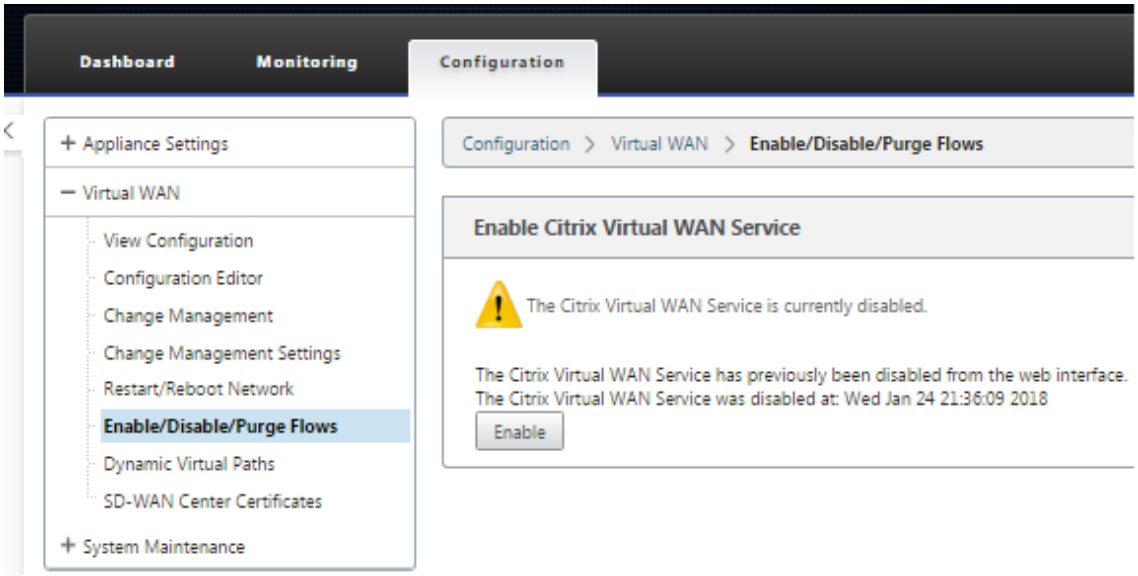
如果这是初始安装和配置，最后一步，您需要在网络中的每个 SD-WAN 设备上手动启用虚拟 WAN 服务。启用该服务可启用并启动虚拟 WAN 守护进程。

> 注意
>
> 如果要重新配置现有部署，MCN 会在将更新的设备包分发到客户端站点时自动启用该服务。在这种情况下，您可以跳过最后一步。

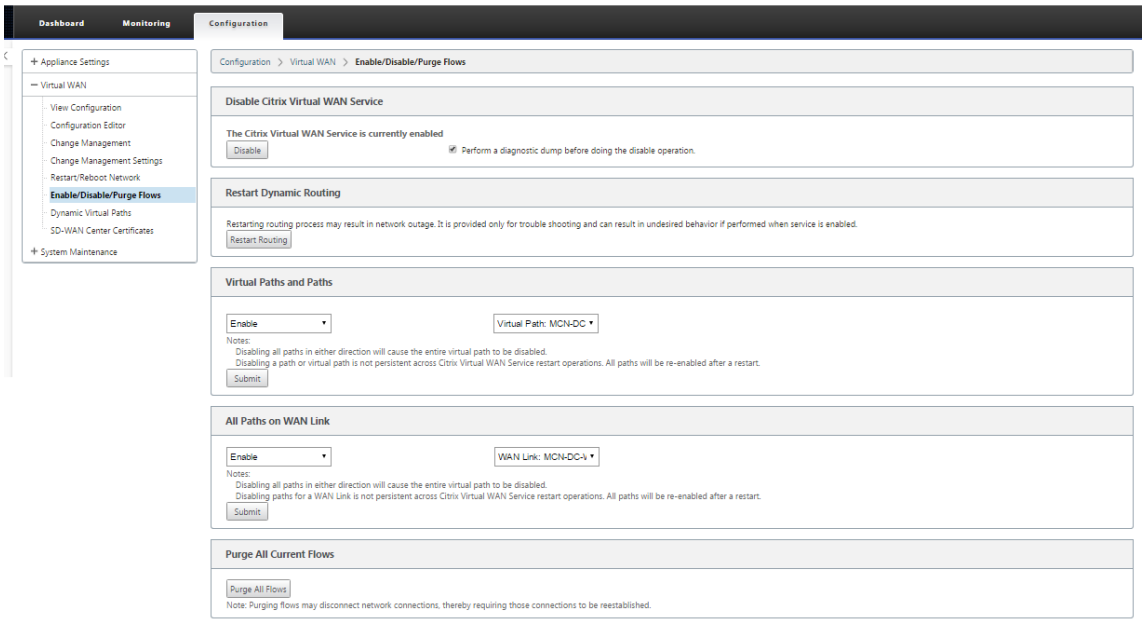
要在设备上手动启用虚拟 WAN 服务，请执行以下操作：

1. 登录到要激活的设备上的管理 Web 界面。
2. 选择 配置 选项卡。
3. 在导航窗格中，打开虚拟 WAN 分支并选择 启用/禁用/清除流。

   如果禁用了虚拟广域网服务，则会显示 启用虚拟广域网服务 页面，如下所示。如果服务已启用，则会显示 启用/禁用/清除流 页面。



4. Click **Enable**。这将启用该服务，并显示 启用/禁用/清除流 页面。



启用虚拟 WAN 服务后，页面顶部会显示一条具有该效果的状态消息。

> 注意
>
> 此页面还提供了用于启用/禁用网络中特定路径和虚拟路径的选项，以及用于清除所有流的选项。

这将完成 MCN 和分支站点客户端设备上 SD-WAN 的安装和激活。现在，您可以使用 监视 页面验证激活并诊断任何现有或潜在的配置问题。

配置防火墙分割

June 22, 2021

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互联网，而无需访问彼此的流量。

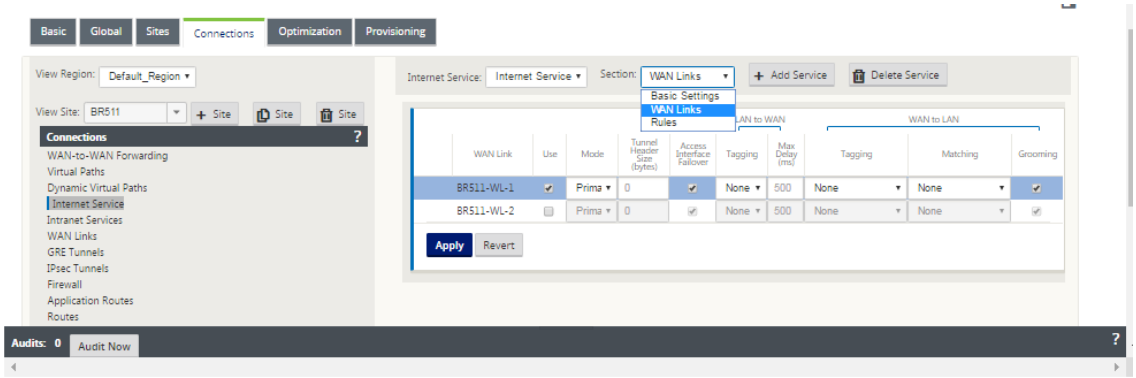
- 本地访客用户互联网接入
- 定义应用程序的员工-用户互联网访问
- 员工-用户可以继续将所有其他流量固定到 MCN
- 允许用户为特定路由域添加特定路由。
- 启用后，此功能将应用于所有路由域。

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。

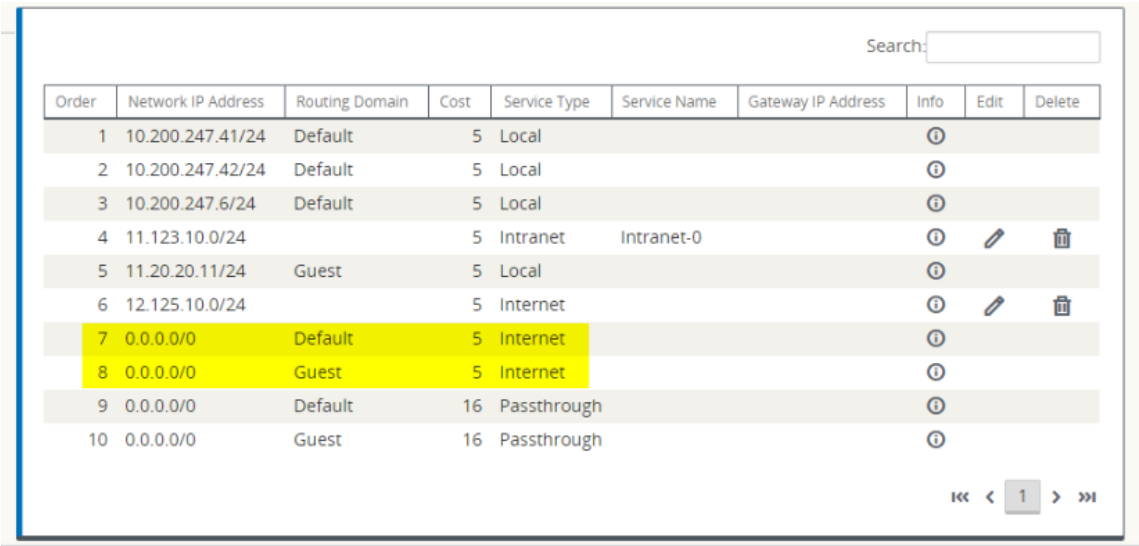
> 注意
>
> 有关更多信息，请参阅如何操作配置 VRF。

要为所有路由域配置 Internet 服务，请执行以下操作：

1. 为网站创建互联网服务。导航到连接 > 查看区域 > 查看网站 > [站点名称] > **Internet** 服务 **>** 部分 **> WAN** 链接，然后在 WAN 链接下选择使用复选框。



> 注意
>
> 您应该看到在连接 > 查看区域 > 查看站点 > [站点名称] > 路由下添加了 0.0.0.0/0 路由，每个路由域一个路由。



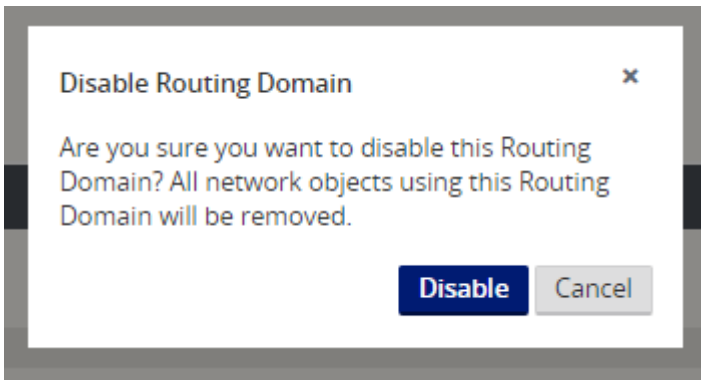
Search:

Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local					
2	10.200.247.42/24	Default	5	Local					
3	10.200.247.6/24	Default	5	Local					
4	11.123.10.0/24		5	Intranet	Intranet-0				
5	11.20.20.11/24	Guest	5	Local					
6	12.125.10.0/24		5	Internet					
7	0.0.0.0/0	Default	5	Internet					
8	0.0.0.0/0	Guest	5	Internet					
9	0.0.0.0/0	Default	16	Passthrough					
10	0.0.0.0/0	Guest	16	Passthrough					

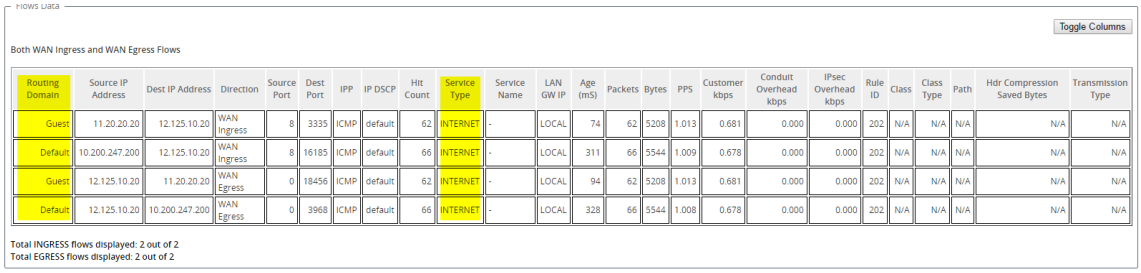
1

不再需要在 MCN 上启用所有路由域。

2. 如果在 MCN 上禁用路由域，则如果分支站点正在使用域，则会显示以下消息：



3. 您可以通过在监视器 **>** 流程 下检查 **Web** 管理界面的 流量 表中的 路由域 列来确认每个路由域正在使用 **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

4. 您还可以在 监视器 > 统计信息 > 路由 下检查每个路由域的 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互联网（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。
- 不同路由域的互联网接入。

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：

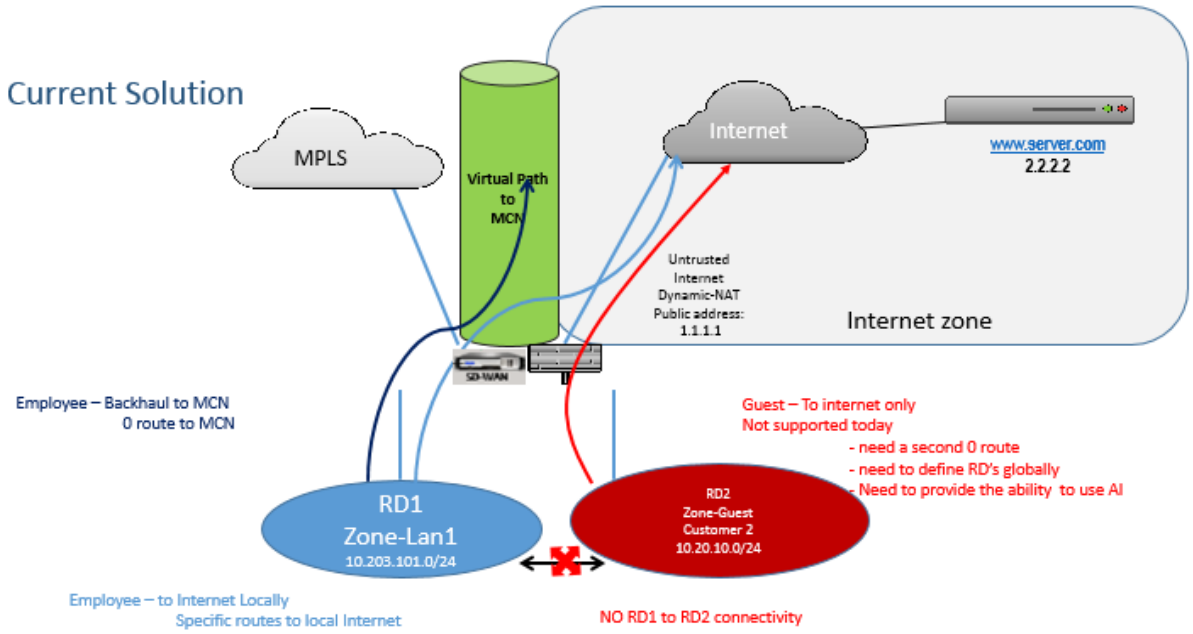
- 在分支站点提供支持至少两个用户组（如员工和来宾）的安全连接的基础结构。该基础架构最多可支持 16 个路由域。
- 隔离每个路由域的流量与任何其他路由域的流量。
- 为每个路由域提供互联网接入，
  - 一个通用的访问接口是必需的，并且可以接受
  - 具有单独面向公众的 IP 地址的每个组的访问接口
- 员工的流量可以直接路由到本地互联网（特定应用程序）
- 员工的流量可以路由或回溯到 MCN 进行广泛筛选（0 路由）
- 路由域的流量可以直接路由到本地互联网（0 路由）
- 如有必要，支持每个路由域的特定路由
- 路由域基于 VLAN 的路由域
- 删除 RD 必须驻留在 MCN 的要求
- 现在只能在分支站点配置路由域

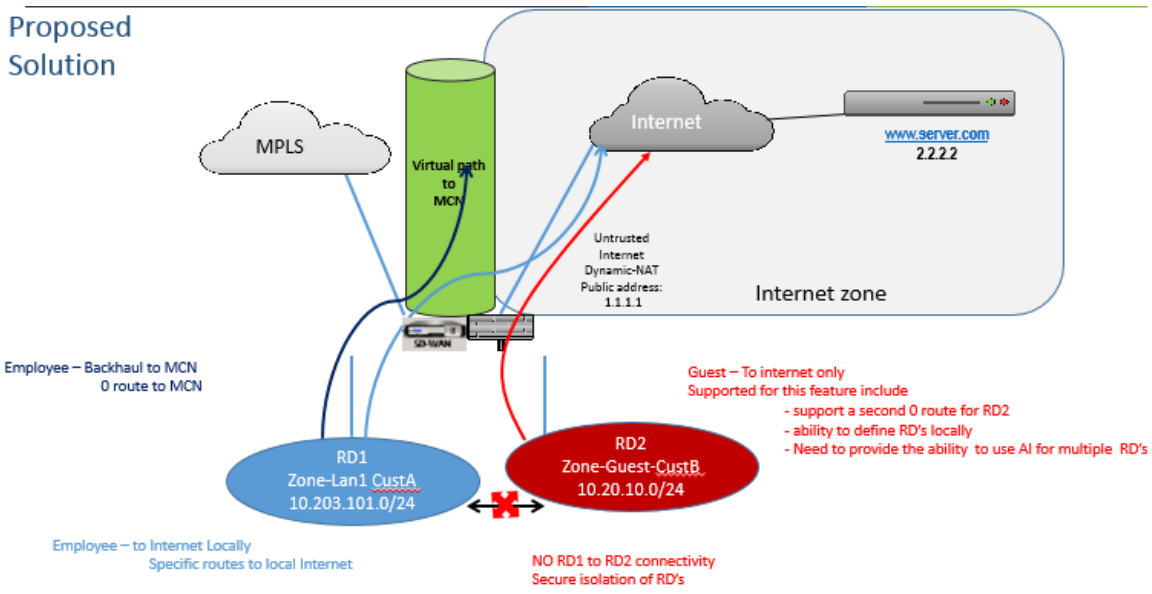
- 允许您将多个 RD 分配给访问接口（一旦启用）
- 为每个 RD 分配一条 0.0.0.0 路径
- 允许为 RD 添加特定路由
- 允许来自不同 RD 的流量使用相同的接入界面退出到互联网
- 允许您为每个 RD 配置不同的访问接口
- 必须是唯一的子网（RD 分配给 VLAN）
- 每个 RD 可以使用相同的 FW 默认区域
- 通过路由域隔离流量
- 出站流将 RD 作为流头的组成部分。允许 SD-WAN 将返回流映射到正确的路由域。

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。
- 在 站点 > 站点名称 > W **AN** 链接 > WL2 [名称] > 访问接口 中，确保复选框可用且已正确定义 Internet 服务。如果无法选中该复选框，则 Internet 服务不会定义或分配给该站点的 WAN 链接。

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，以便访问互联网。
- 每个路由域没有 QoS；先到先得。

证书身份验证

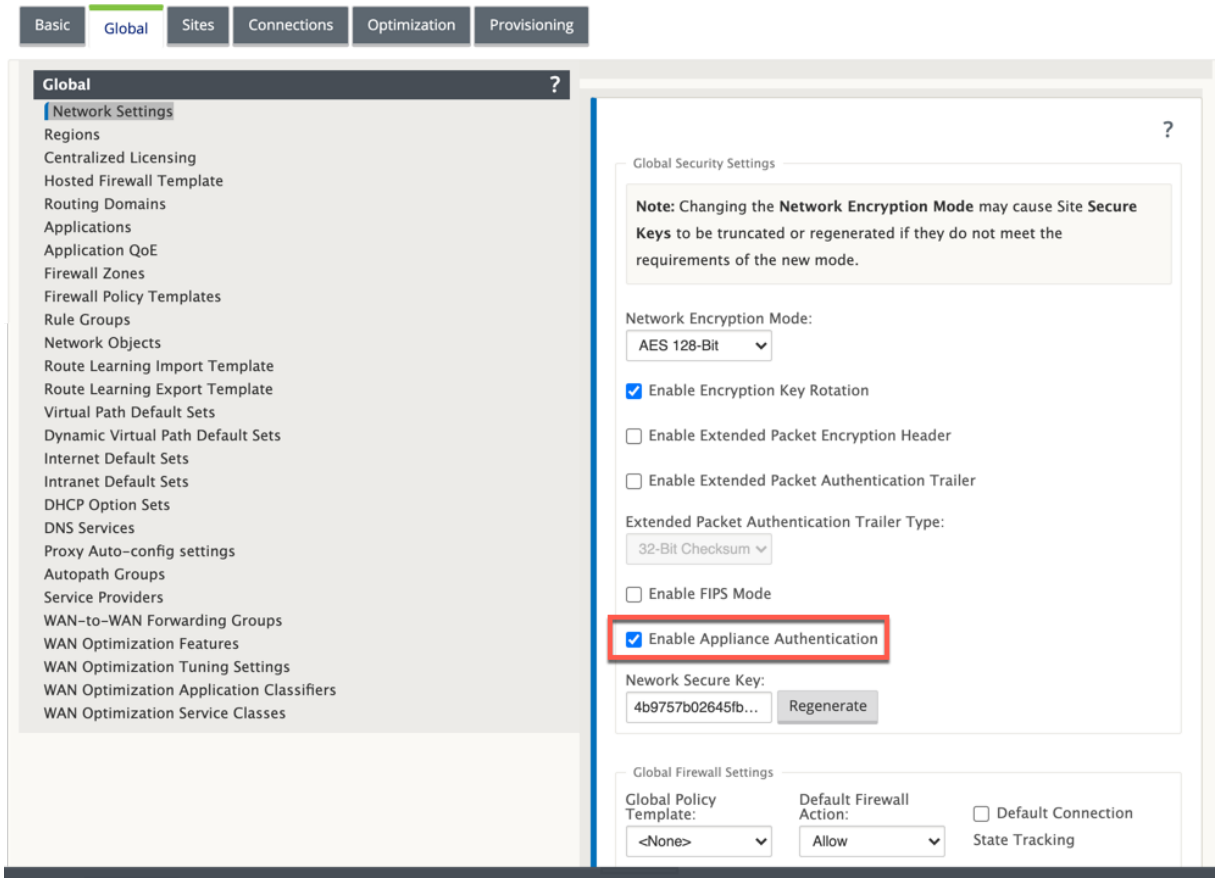
June 22, 2021

Citrix SD-WAN 通过使用网络加密和虚拟路径 IPsec 隧道等安全技术，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专用证书颁发机构 (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。

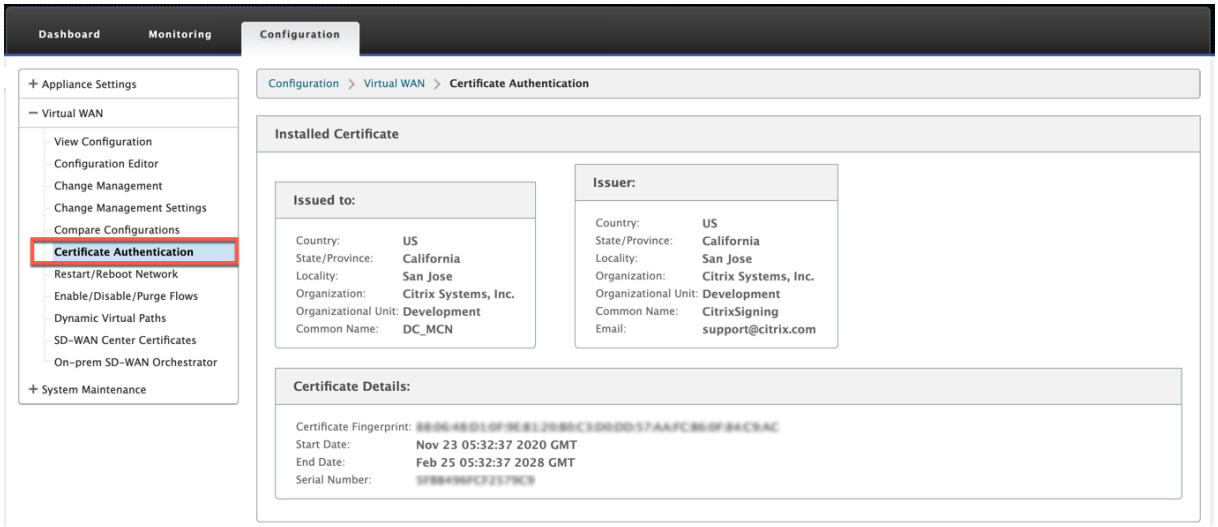
CA 颁发的证书将公钥绑定到设备名称。公钥与证书标识的设备所拥有的相应私钥一起工作。

要启用设备身份验证，请在配置编辑器中导航到 全局 > 网络设置，然后选择 启用设备身份验证。



在暂存和应用配置后，配 置 > 虚拟 **WAN** 下会列出新的 证书身份验证 选项。

您可以从 证书身份验证 页面管理用于虚拟路径身份 验证 的所有证书。

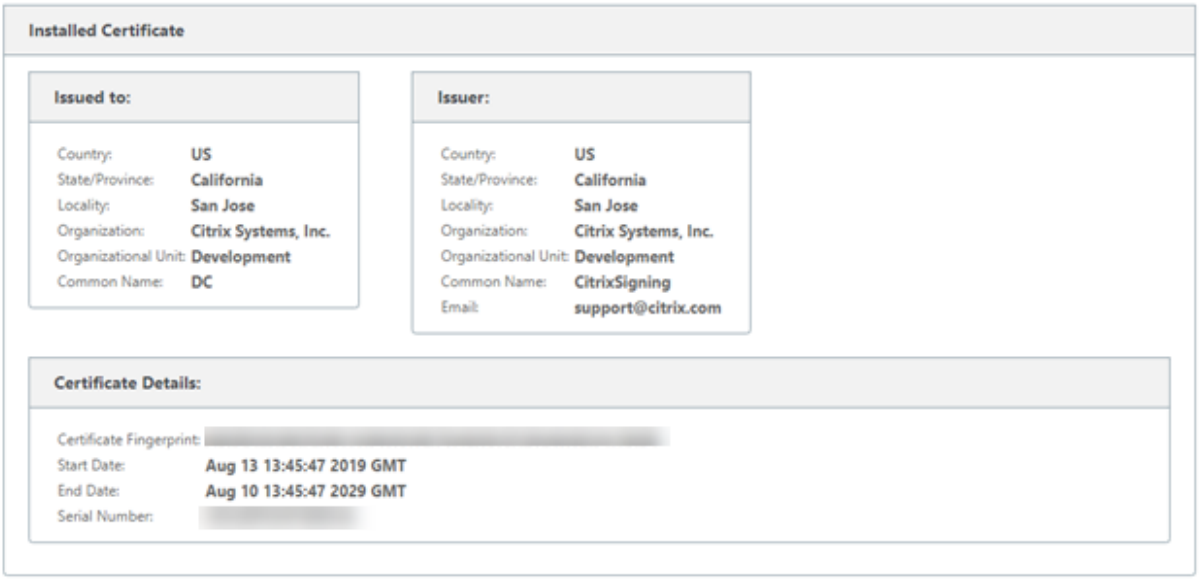


> 注意
>
> 如果要将装置软件从 SD-WAN 版本 11.0 升级到 11.1 或更高版本，请取消选中 启用设备身份验证 选项并执行软件升级。升级过程完成后，选择 启用设备身份验证 选项。

已安装的证书

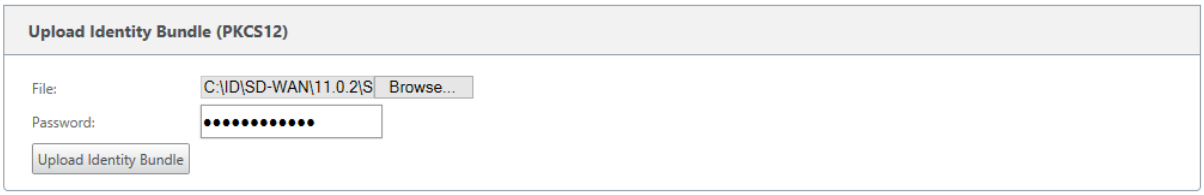
已安装的证书 部分提供设备上安装的证书的摘要。设备使用此证书在网络中标识自身。

颁发给 部分提供了有关证书颁发给谁的详细信息。证书中的公 用名 称与设备名称相匹配，因为证书绑定到设备名称。颁发 者部分提供证书签名颁发机构的详细信息，用于签名证书。证书详细信息包括证书的指纹、序列号和证书的有效期。



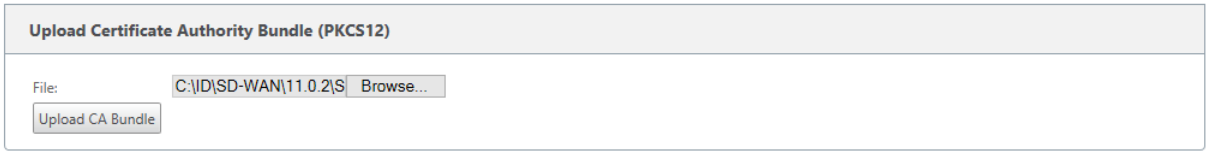
上载身份包

身份包包括私钥和与私钥关联的证书。您可以将 CA 颁发的设备证书上载到设备中。证书捆绑包是一个 PKCS 12 文件，扩展名为.p12。您可以选择使用密码保护它。如果将密码字段留空，则将被视为没有密码保护。



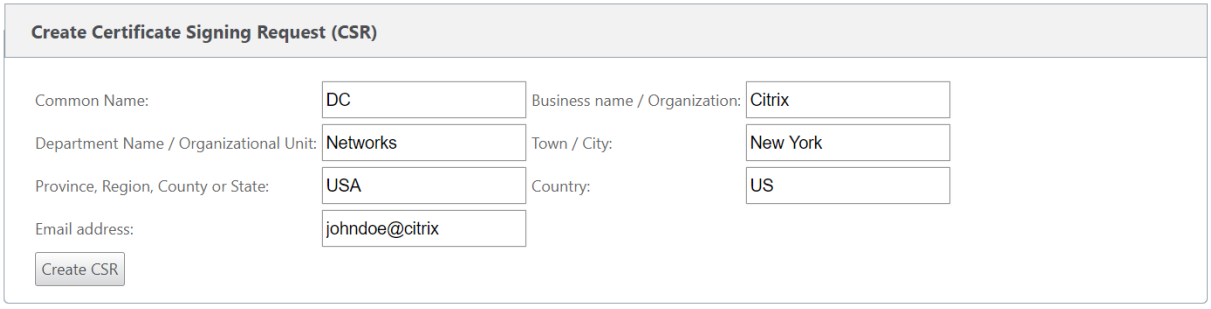
上载证书颁发机构包

上载与证书签名颁发机构对应的 PKCS 12 捆绑包。证书颁发机构捆绑包括完整的签名链、根签名机构和所有中间签名机构。



创建认证签名请求

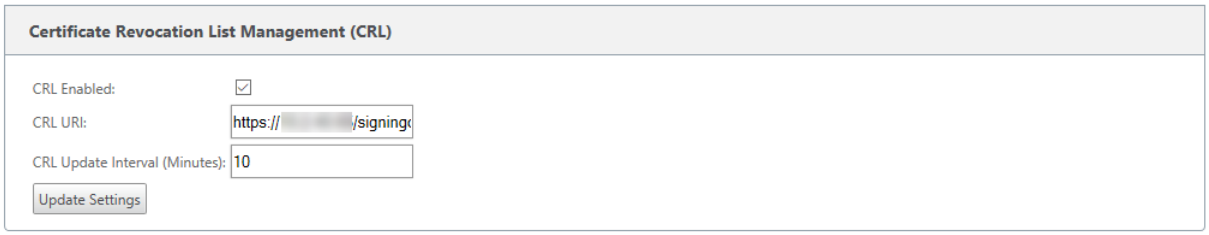
设备可以生成未签名证书并创建证书签名请求 (CSR)。然后，CA 可以从设备下载 CSR，对其进行签名，然后以 PEM 或 DER 格式将其上传回设备。这用作设备的身份证书。要为设备创建 CSR，请提供设备公用名称、组织详细信息和地址。



证书吊销列表管理器

证书吊销列表 (CRL) 是在网络中不再有效的证书序列号的已发布列表。CRL 文件定期下载并在本地所有设备上存储。当验证证书时，响应程序会检查 CRL 以查看启动程序证书是否已被吊销。Citrix SD-WAN 目前支持 PEM 和 DER 格式的版本 1 CRL。

要启用 CRL，请选择启用 CRL 选项。提供 CRL 文件的维护位置。支持 HTTP、HTTPS 和 FTP 位置。指定检查和下载 CRL 文件的时间间隔，范围为 1—1440 分钟。



> 注意
>
> virtua1 路径的重新身份验证期可以介于 10-15 分钟之间，如果 CRL 更新间隔设置为较短的持续时间，则更新的 CRL 列表可能包括当前活动的序列号。使主动吊销的证书在网络中短时间内可用。

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。仅针对 HDX 数据集提供的 TCP多跳数据。HDX 数据集提供HDX 洞察数据。

> 注意
>
> HDX 模板仅适用于 Citrix SD-WAN PE 版和双盒设备。应在数据中心设备上启用此功能。

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

模板编号**-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	
导出进程编号	出口加工 d，144	Unsigned32, 4	
流程编号	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	
最后的时间（以微秒为单位）	流动微秒，155	日期时间微秒, 8	

信息元素 **(IE)**	**IE** 名称和 **ID**	类型和莱恩	说明
知识产权服务	分类管理服务, 5	Unsigned8, 1	
流标志	TCPS 控制位，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
应用程序 ID	应用程序编号，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|
| 导出进程编号 | 出口加工 d，144|Unsigned32, 4|
| 流程编号 | 弗洛伊德，148|Unsigned64, 8|
|Ipv6 SRC IP|sourceIPv6Address, 27|Ipv6address, 16|
|IPv6 DST IP|destinationIpv6Addres, 28|Ipv6address, 16|
|IP 版本 |IPVersion, 60| UNSIGNed8, 1| 设置为 6| | |
IP 协议号 | 协议代码,4| UNSIGNed8, 1| | |
填充 |N/A | Unsigned16, 2| |

|SRC 端口 | sourceTranportport, 7| Unsigne
d16, 2| |DST PortPort, 11| UNSIGNed16, 2| |
|PktCount|packetdeltaCount, 2| unsigned64, 8| | |
字节计数 |octetdeltaCount, 1
|unsigned64, 8| | | 第一个 pkt 的
时间以微秒为单位 | flowstart 微秒,154| datetime 微秒,154| datetime 秒，8| |
|IPTOS|IPCLASSOFService, 5| UNSIGNED8, 1| | |
流标志 |TCPControlBITS, 6| UNSIGNED8, 2| 目前设置为 0.| |
流向 | 流向,61|unsigned8, 1|0x00: 入口流量 0x01: 出口流量 WAN-WAN 和 LAN-LAN 可能出口 |
| 输入接口 | ingress 接口，10|Unsigned32, 4| Citrix SD-WAN 负载均衡数据流经多个成员路径，因此单个数据流可以有多个输入/输出接口组合。| |
输出接口 |egressInterface, 14| Unsigned32, 4| Citrix SD-WAN 负载均衡数据流通过多个成员路径，因此单个数据流可以有多个输入/输出接口组合。| | 输
入 Vlan ID|vlanID，58| 未签名 16，2| | | |
输出 Vlan ID|postvlanid，59| 未签名 16，2| |
|VRF ID|ingresSVRFID，234| unsigned32，4| | | |
流量键指示器，173| 未签名到 0x64 1E037f.| | 应用程序 ID | 应
用程序 ID，95|OctetarRay，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	应用程序编号，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。
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	
知识产权服务	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|
|IP 版本 |IP 版本,60| UNSIGNed8, 1| 设置为 6| | |
IP 协议编号 | 协议编号 | 协议编号,4| UNSIGNed8, 1| |
|IP TOS|IPCLASSOFService ,5| UNSIGNed8, 1| | |
流方向 | 61|unsigned8, ing000 ress flow0x01：出口 FlowWan-WAN 和局域网流是一种可能性 SDWAN|
|SRC 端口 | sourceTranportport, 7| unsigned16, 2| |

|DST 端口 | 目的地传输港口,11| unsigned16, 2| |
Pkt Count|Pkt Count|packetdeltaCount, 2|unsigned64, | |
字节计数 |OctetdeltaCount, 1unsid64, 8| | |
输入接口 | ingress 界面，10| UNSIGNed32，4| Citrix SD-WAN 负载均衡数据流经多个成员路径，因此单个数据流可以有多个输入/输出接口组合。| |
输出接口 |egressInterface, 14| Unsigned32, 4| Citrix SD-WAN 负载均衡数据流通过多个成员路径，因此单个数据流可以有多个输入/输出接口组合。| |
输入 Vlan ID|vlanID，58| 未签名 16，2| | | |
输出 Vlan ID|postvlanID，59| UNSIGNed16，2| |

限制

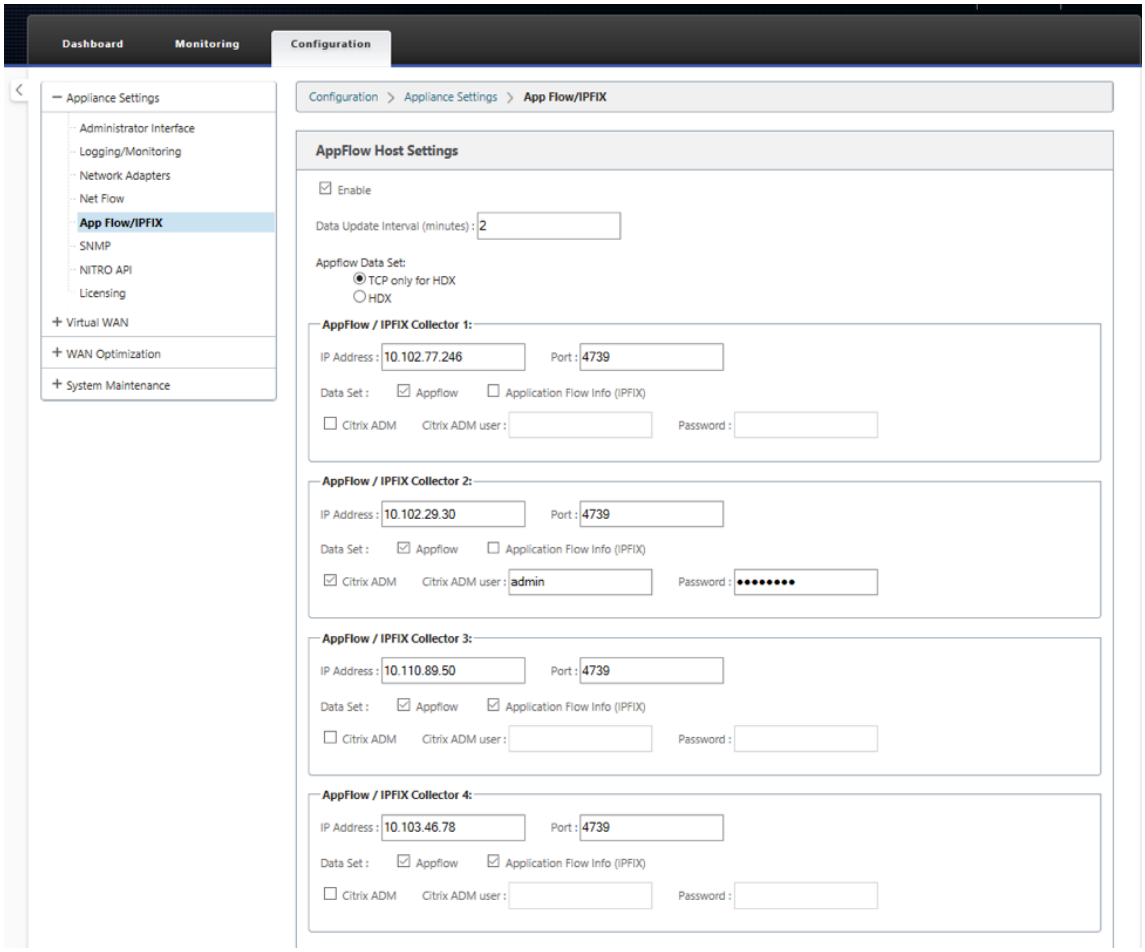
- AppFlow 不支持 IPv6 收集器和流记录。
- 净流的导出间隔从 15 秒增加到 60 秒。
- AppFlow /IPFIX 流通过 UDP 传输，连接丢失不是所有的数据都被重新传输。如果导出间隔设置为 X 分钟，则设备仅存储 X 分钟的数据。连接损失 X 分钟后重新传输。
- 在 Citrix SD-WAN 中，版本 10 版本 2 中，**AppFlow** 设置将设置为每台设备的本地设置，而在以前的版本中，该设置为全局设置。如果 SD-WAN 软件版本降级为以前的任何版本，并且如果 AppFlow 在任何一台设备上配置，则该版本将在全球范围内应用于所有联盟。

配置 **AppFlow/IPFIX**

可以在各个 SD-WAN 设备上配置 AppFlow /IPFIX，也可以在 SD-WAN Center 进行配置，并将配置推送到一组设备。

若要在 SD-WAN 设备上配置 AppFlow/IPFIX：

1. 在 Citrix SD-WAN SE/PE Web 界面中，导航到配置 **> AppFlow/IPFIX**。
2. Click **Enable**。



3. 在数据更新时间间隔字段中，指定流报告导出到 AppFlow/IPFIX 收集器的时间间隔（以分钟为单位）。最大间隔为 10 分钟。

4. 选择 **AppFlow** 数据集模板，您可以选择以下数据集模板之一：

   - **TCP** 仅适用于 **HDX (AppFlow)**：用于收集 ICA 连接的多跃点数据并将其发送到 AppFlow 收集器的 AppFlow 数据集模板。
   - **HDX (AppFlow)**：用于收集 ICA 连接的 HDX 洞察数据并将其发送到 AppFlow 收集器的 AppFlow 数据集模板。

   > 注意
   >
   > **HDX** 模板仅适用于 Citrix SD-WAN PE 和双盒设备。

5. 您最多可以配置四个 AppFlow/IPFIX 收集器。为每个收集器指定以下参数：

   - **IP** 地址：外部 AppFlow/IPFIX 收集器系统的 IP 地址。
   - 端口：外部 AppFlow/IPFIX 收集器系统侦听的端口号。默认值为 4739。您可以根据使用的收集器更改端口号。
   - 应用程序流程信息 **(IPFIX)**：根据 IPFIX 模板 611、615 和 612 向 IPFIX 收集者发送流记录。

- 基本属性 **(IPFIX)**：根据 IPFIX 模板 613 和 616 向 IPFIX 收集器发送流记录。
- **Citrix ADM**：选择此选项可将 Citrix ADM 用作 AppFlow 收集器。

> 注意
>
> - Citrix ADM 目前不支持 IPFIX 集合。
> - Citrix ADM 不支持 AppFlow 和 IPFIX 的 IPv6 地址。

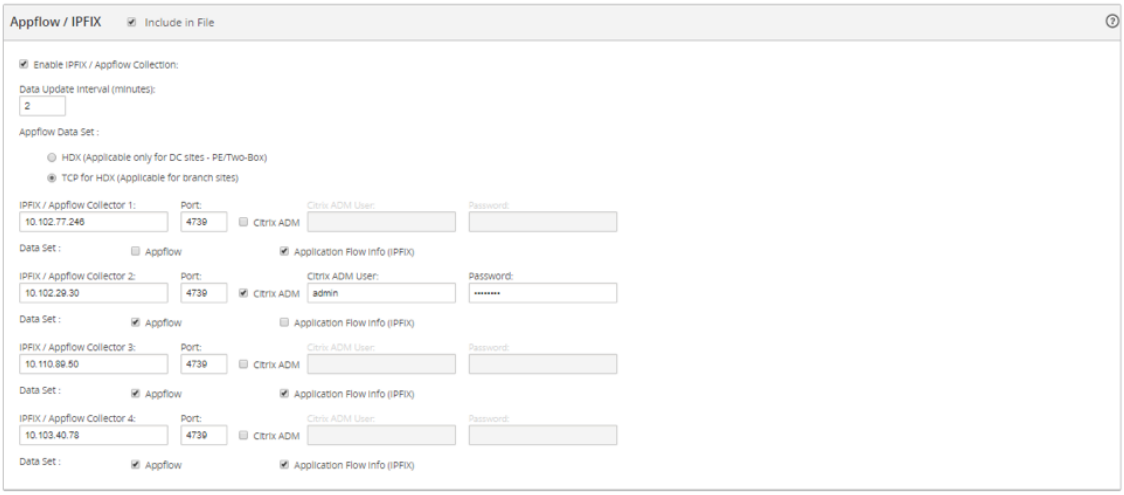
- **Citrix ADM** 用户：Citrix ADM 收集器的用户名
- 密码: Citrix ADM 收集器密码.

用户名和密码用于无缝登录 Citrix ADM 并存储流数据。

6. 单击 应用设置。

要使用 Citrix SD-WAN Center 配置 **AppFlow/IPFIX** 收集器，请执行以下操作：

1. 在 Citrix SD-WAN Center 管理 UI 中，导航到 配置 **>** 设备设置。
2. 导航到 **AppFlow/IPFIX** 部分，然后选择包含在文件中。
3. 选择启用 **IPFIX/AppFlow** 集合。



4. 在数据更新时间间隔字段中，指定将 AppFlow 报告导出到 AppFlow/IPFIX 收集器的时间间隔（以分钟为单位）。
5. 选择 **AppFlow** 数据集模板，您可以选择以下数据集模板之一：
   - **TCP** 仅适用于 **HDX**：用于收集 ICA 连接的多跃点数据并将其发送到 AppFlow 收集器的 AppFlow 数据集模板。
   - **HDX**：用于收集 ICA 连接的 HDX 洞察数据并将其发送到 AppFlow 收集器的 AppFlow 数据集模板。

> 注意
>
> **HDX** 模板仅适用于 Citrix SD-WAN PE 和双盒设备。

6. 您最多可以配置四个 AppFlow/IPFIX 收集器。为每个收集器指定以下参数：
   - **IPFIX/AppFlow** 收集器：外部应用流量/IPFIX 收集器系统的 IP 地址。
   - 端口：外部 AppFlow/IPFIX 收集器系统侦听的端口号。默认值为 4739。您可以根据使用的收集器更改端口号。
   - 应用程序流程信息：根据 IPFIX 模板 611、615 和 612 向 IPFIX 收集者发送流程记录。
   - 基本属性 **(IPFIX)**：根据 IPFIX 模板 613 和 616 向 IPFIX 收集器发送流记录。
   - **Citrix ADM**：选择此选项可将 Citrix ADM 用作 AppFlow 收集器。

     > 注意
     >
     > Citrix ADM 目前不支持 IPFIX 集合。

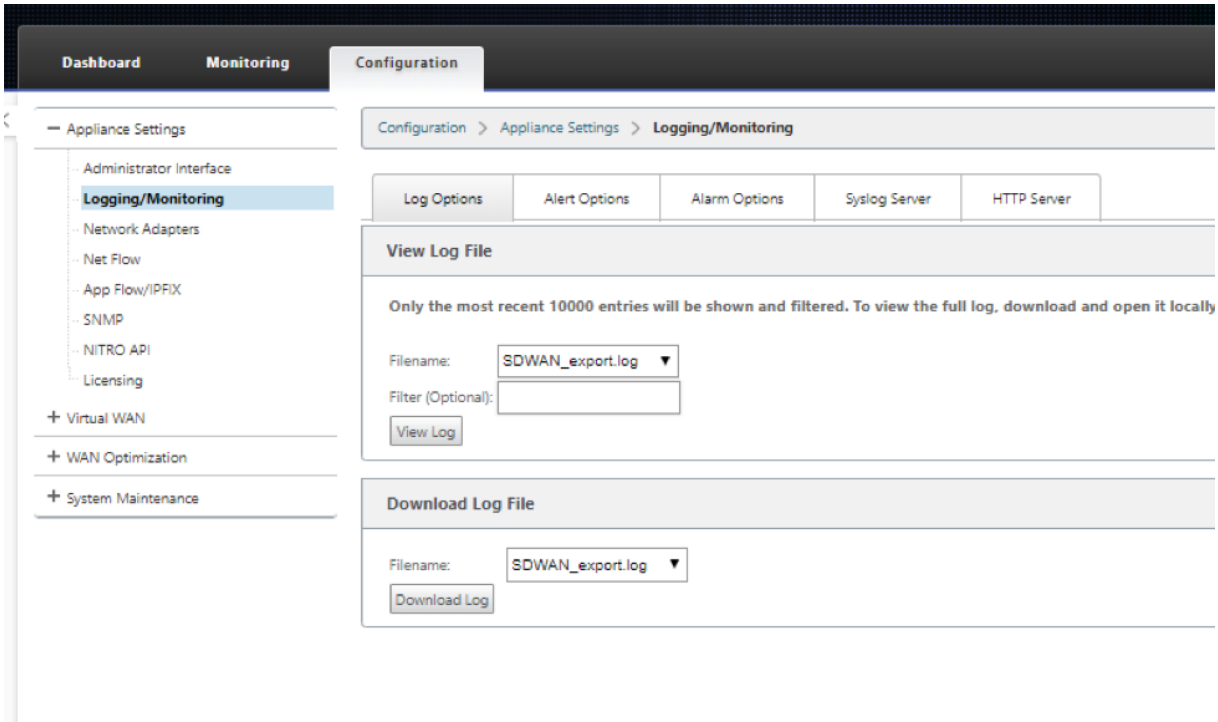
   - **Citrix ADM** 用户：Citrix ADM 收集器的用户名。
   - 密码: Citrix ADM 收集器密码.

     用户名和密码用于无缝登录 Citrix ADM 并存储流数据。
7. 将配置保存 并 导出 到受管设备。

> 注意
>
> 如果 SD-WAN Center 版本低于 10.2，SD-WAN 设备版本为 10.2 及更高版本，则您可以遵守以下条件。
>
> - 如果在设备上启用了本地收集器，则从 SD-WAN Center 推送的 AppFlow/IPFIX 配置不会影响现有配置。
> - 如果未在设备上启用本地收集器，则从 SD-WAN Center 推送的 AppFlow/IPFIX 配置将应用于设备。
> - 如果在 SD-WAN Center 配置中启用了全局 AppFlow/IPFIX 配置，则在设备上启用所有本地收集器。

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

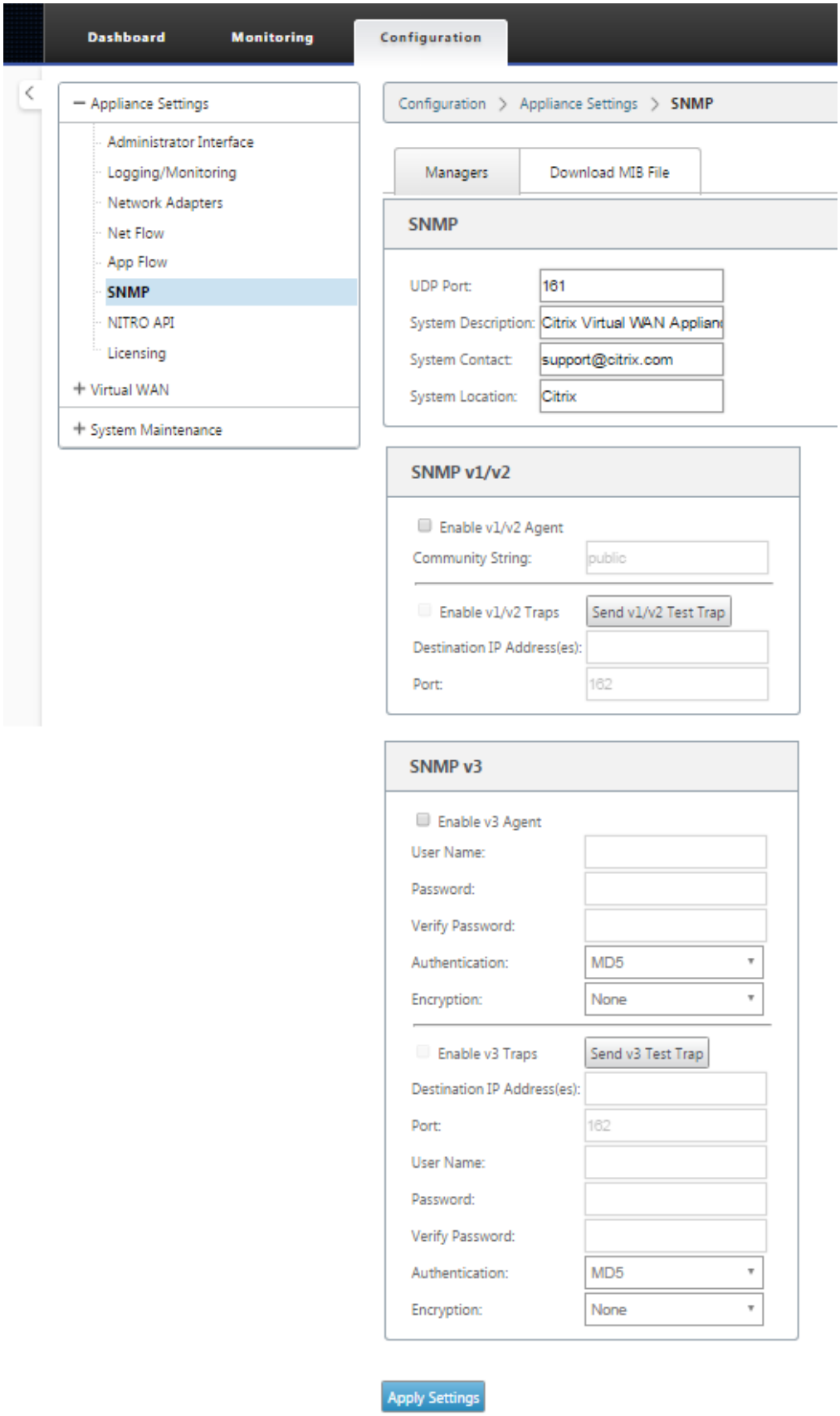
November 16, 2022

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：

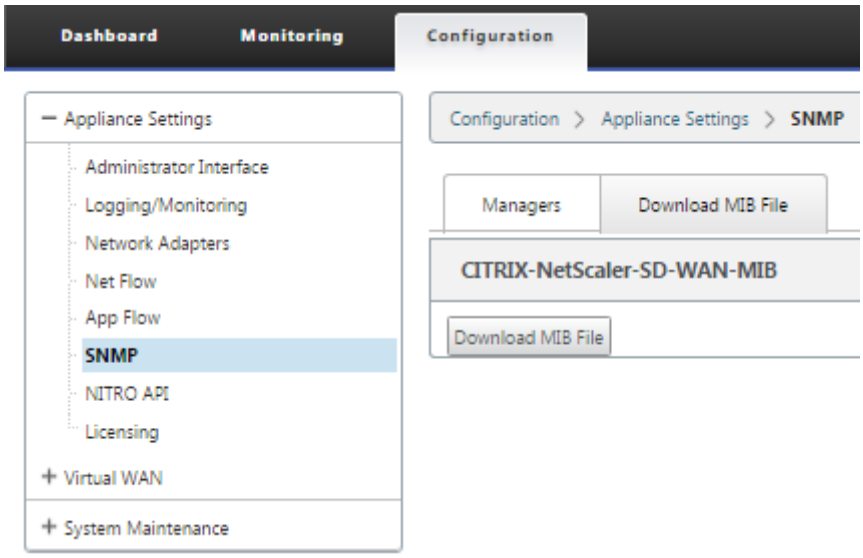
- CITRIX-COMMON-MIB.txt
- APPACCELERATION-SMI.txt
- APPACCELERATION-PRODUCTS-MIB.txt
- APPACCELERATION-TC.txt
- APPACCELERATION-STATUS-MIB.txt
- APPCACHE-MIB.txt
- SDX-MIB-smiv2.mib

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 **IF**Table 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

June 22, 2021

您可以使用以下管理选项管理和维护 Citrix SD-WAN 设备：

- 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：

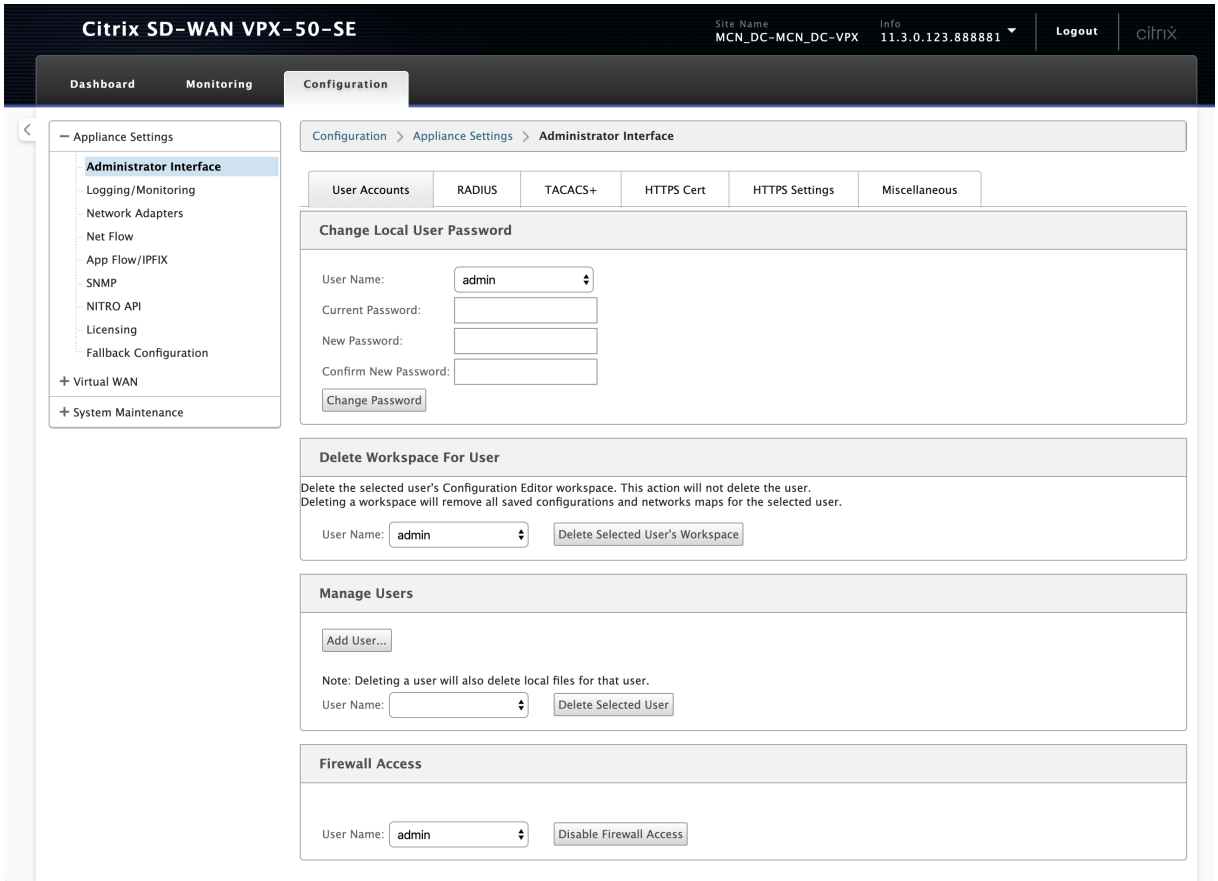
- 查看者：查看者帐户是一个只读帐户，可以访问控制面 板、报告和 监 控页面。
- 管理员：管理员帐户对所有部分具有管理权限和读写权限。

  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：安全管理员仅对 配置编辑器中的防火墙和安全相关设置具有读写访问权限，同时对其余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：网络管理员对所有区域具有读写权限，并且可以完全配置分支，但 配置编辑器中的防火墙和安全相关设置除外。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。

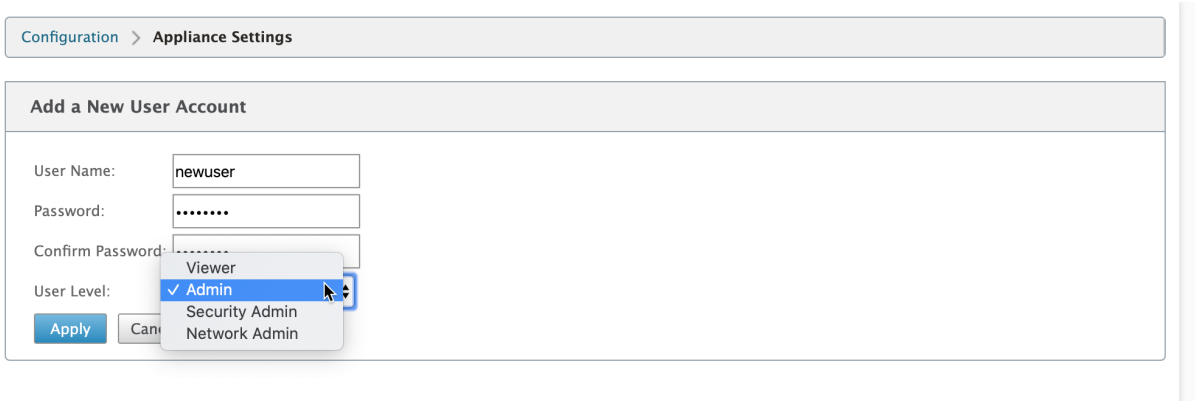
> 注意：
>
> 网络管理员和安全管理员无法添加或删除用户帐户。他们只能编辑自己的帐户密码。



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”。

为用户删除工作区

您可以删除用户的“配置编辑器”工作区。删除工作区不会删除用户帐户。它会删除所选用户的所有保存的配置和网络映射。

要删除用户的工作区，请在“删除用户的工作区”部分下，从“用 户名”下拉列表中选择该用户。单击 删除选定用户的工作区。

禁用对防火墙的访问

您可以禁用防火墙对用户帐户的访问。要禁用，请从用户 名下拉列表中选择用户，然后单击 禁用防火墙访问。

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。

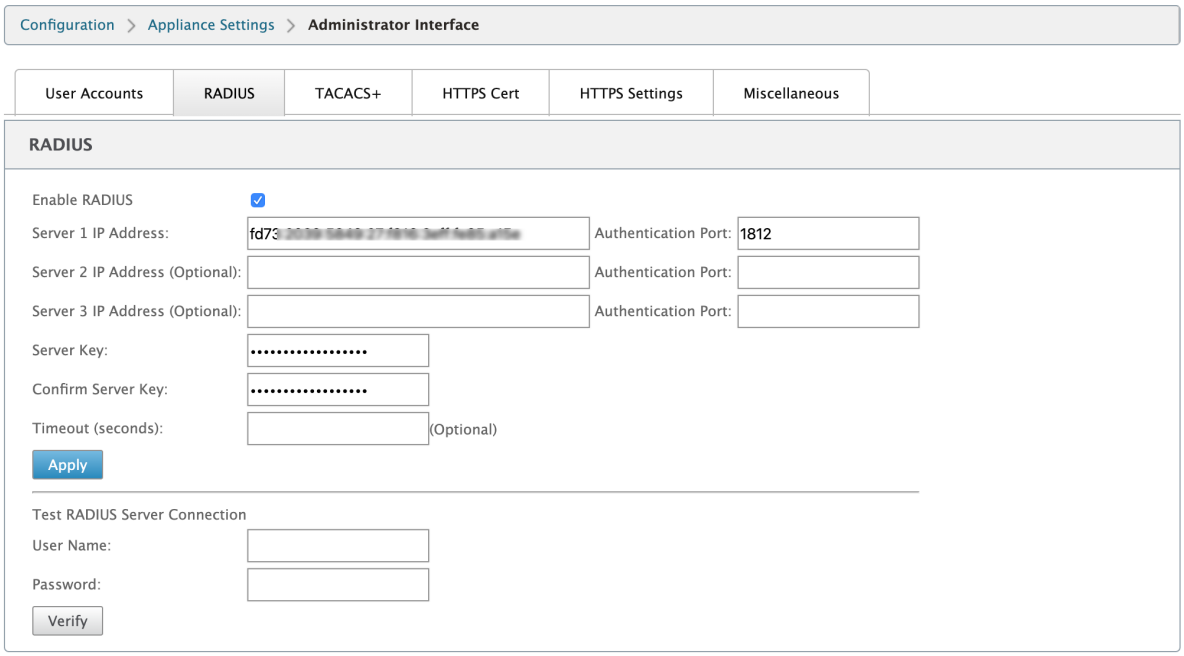
要配置 RADIUS 服务器：

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+ 使用私有密钥、IP 地址和端口号。默认端口号为 49。

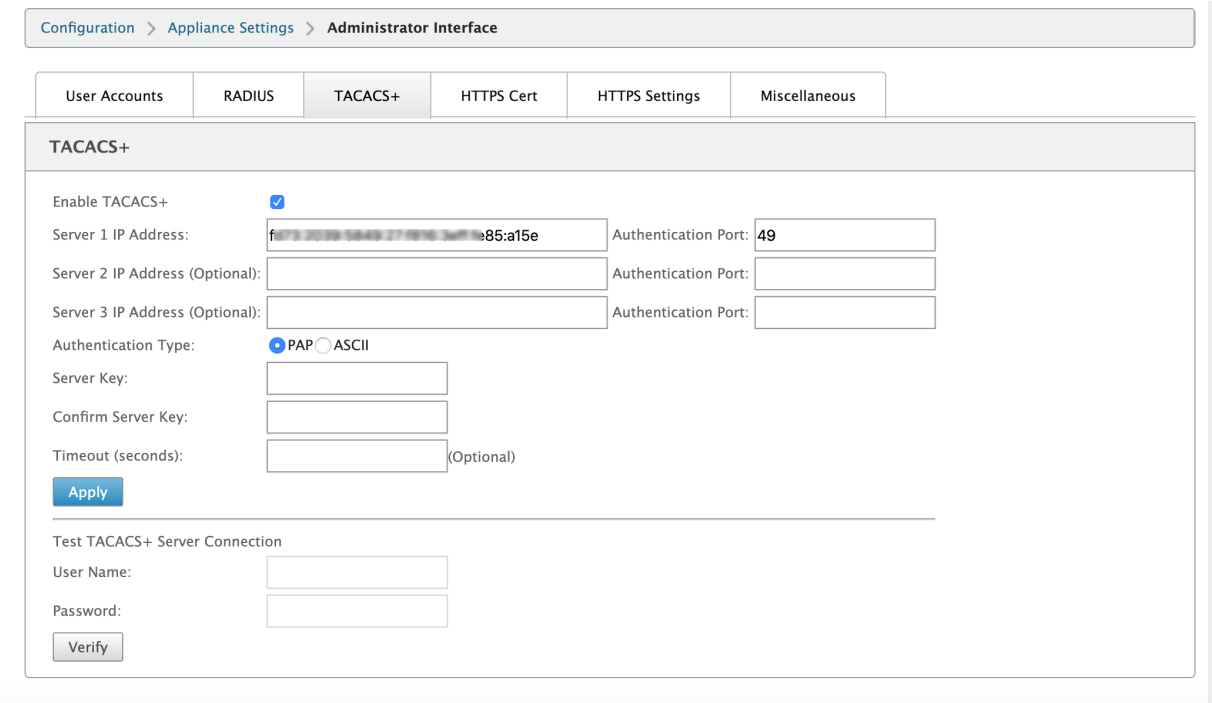
要配置 TACACS+ 服务器，请执行以下操作：

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

June 22, 2021

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。

要配置 NDP 路由器通告，

1. 在配置编辑器中，导航到 站点 **> NDP** 路由器通告。
2. 单击 **+**，然后从虚拟接口下拉列表中选择一个已配置的 虚拟接口。
3. 选中 启用通告 复选框以启用定期发送路由器通告并响应所选虚拟接口的路由器请求。
4. 指定最大、最小和路由器的生命周期间隔。
    - 最大间隔：发送定期未经请求的多播路由器通告之间允许的最长时间（以秒为单位）。
    - 最小间隔：发送定期未经请求的多播路由器通告之间允许的最短时间（以秒为单位）。

- 路由器寿命：主机认为路由器有效的时间（以秒为单位）。0 表示无法将路由器用作默认路由器。

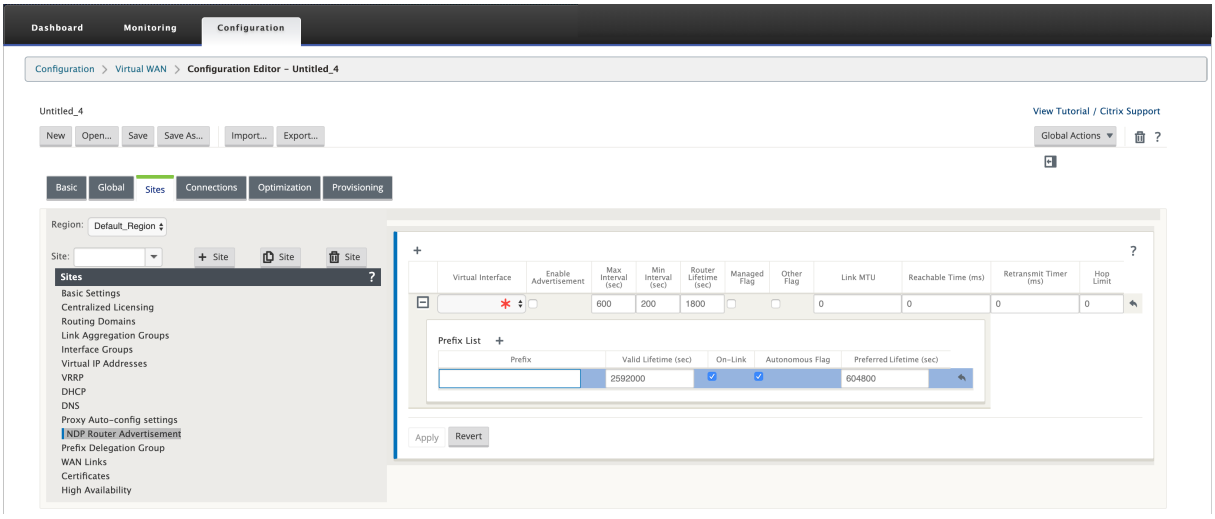
5. 如果 IP 地址可通过 DHCPv6 协议获得，请选择 托管标记 复选框。
6. 如果配置信息（不包括 IP 地址）可通过 DHCPv6 协议获得，请选择其他 标 志复选框。
7. 为所选接口指定以下值。

   - 链路 **MTU**：接口推荐的最大传输单元 (MTU)。
   - 可达时间：**NDP** 协议保持在可达状态的时间（以毫秒为单位）。
   - 重传计时器：解析 IP 地址或探测邻居时，重新传输邻居请求消息的间隔时间（以毫秒为单位）。
   - 跳数限制：路由器通告中包含的最大跳数。

8. 输入与前缀关联的详细信息。

   - 前缀：无类域间路由 (CIDR) 表示法中的前缀和前缀长度。
   - 有效生命周期：前缀有效的时间（以秒为单位）。-1 表示无穷大，这意味着前缀永久保留。
   - **ON-Link**：选中此前缀将被视为网络的本地前缀。
   - 自治标志：启用后，主机的无状态地址自动配置 (SLAAC) 将使用该前缀生成 IP 地址。
   - 前缀生命周期：前缀被视为首选的时间（以秒为单位）。

9. 单击应用。
10. 要为 NDP 路由器通告配置更多虚拟接口，请单击 **+**。



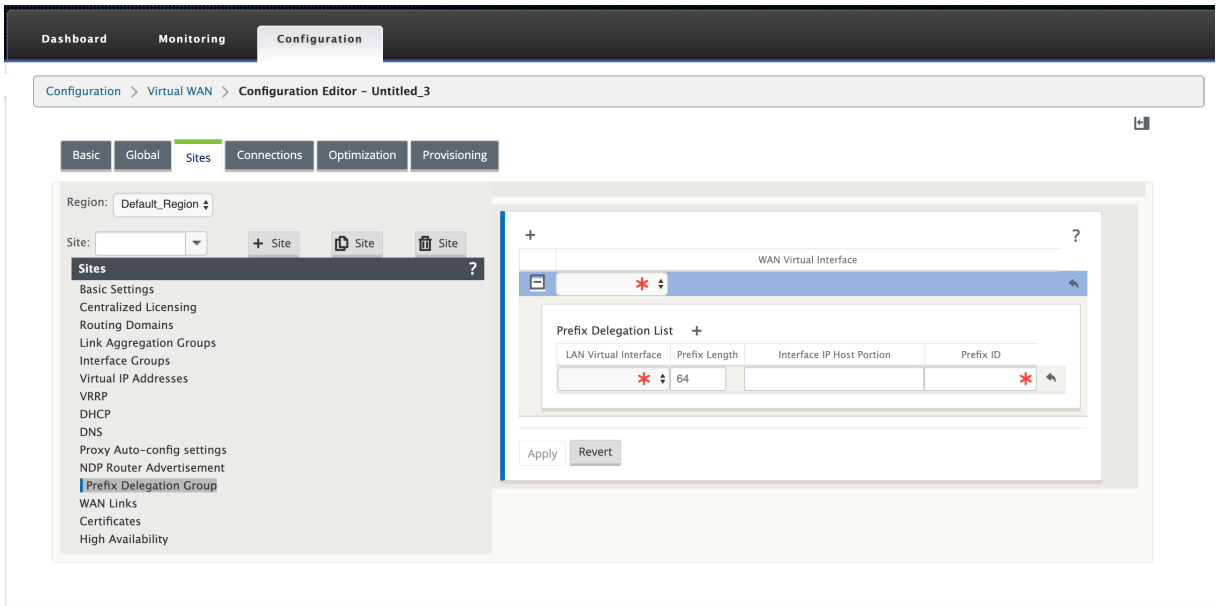
前缀委派组

> 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。

要配置前缀委派，

1. 在配置编辑器中，导航到 站点 **>** 前缀委派组。
2. 单击 **+**，然后选择一个已配置的 WAN 虚拟接口，该接口是从 ISP 请求前缀的。
3. 提供以下详细信息：
   - 局域网虚拟接口：选择要求前缀的已配置 LAN 虚拟接口之一。
   - 前缀长度：作为前缀一部分的全局单播 IPv6 地址的位数。
   - 接口 **IP** 主机部分：用于接口 IP 地址的主机部分。
   - 前缀 **ID**：用于标识局域网接口的前缀委派请求的唯一标识符。
4. 单击应用。
5. 要将更多 WAN 虚拟接口配置为前缀委派组的一部分，请单击 **+**。



广域网优化

June 22, 2021

Citrix SD-WAN WANOP 设备可优化 WAN 链接，确保最大的响应能力和吞吐量。Citrix SD-WAN WANOP 设备成对工作，每一端都有一个设备，以加快链路上的流量。以下是 Citrix SD-WAN WANOP-

- 压缩
- TCP 协议加速
- 通信管理
- 应用程序加速
- Citrix XenApp/XenDesktop (HDX) 加速
- 集成
- 监测和管理

有关 Citrix SD-WAN WANOP 10.2 安装、部署和功能配置的信息，请参阅 Citrix SD-WAN WANOP 文档。Citrix SD-WAN WANOP 10.2 的功能和过程与 Citrix SD-WAN WANOP 版本中记录的过程类似。

您可以在 Citrix SD-WAN Premium Edition 上启用和配置 WAN 优化功能。有关详细信息，请参阅 Citrix SD-WANPremium Edition。

您可以使用 WANOP 客户端插件软件在任何远程 Windows 笔记本电脑或工作站上实现网络加速。有关详细信息，请参阅WANOP 客户端插件。

Citrix SD-WAN Premium Edition

June 22, 2021

本节提供了有关为虚拟 WAN 启用和配置 SD-WAN 高级（企业）版 WAN 优化功能的分步说明。若要执行此操作，请在 MCN 上的 Web 管理界面的 配置编辑器 中使用 优化 部分窗体。

> 注意
>
> 您必须安装 SD-WAN 高级（企业）版许可证才能访问、启用、配置和激活虚拟 WAN 优化功能。SD-WAN 标准版不支持这些功能。

配置 优化 部分集和参数有两个顶级步骤。这些按依赖顺序列出如下：

1. 启用 WAN 优化并自定义 默认 配置，或接受默认值。

   默认 配置用作所有符合 WAN 优化 条件的站点的基本优化配置。默 认配置是预先配置的，并且可以自定义。

   > 注意
   >
   > 有关说明，请参阅启用优化和配置默认设置。

2. （可选）为每个分支站点自定义 WAN 优化配置，或接受 每个分支站点的默认设置和设置。

默认情况下，默认配置最初应用于符合 **WAN** 优化条件的每个分支站点。仅支持 1000-EE (Premium Edition) 和 2000-EE (Premium Edition) 硬件设备的 WAN 优化。对于每个支持的分支站点，您可以选择接受或修改默认 设置和设置的任意组合，或这些设置的任何子集。相关说明，请参阅配置分支站点的优化。

要完成这些步骤，您可以使用配置窗体配置编辑器的优化部分。优化 部分的组织方式如下：

- 默认值—默认值 分支包含以下子分支，这些子分支又包含一个或多个用于配置各自集合和设置的表单：
  - 默认功能
  - 默认调整设置
  - 默认应用程序分类器（集）
  - 默认服务类（设置）
- ****<Client Site Name>—**** 优化 部分配置树包含支持 WAN 优化的每个客户端节点（分支站点）的分支。如果客户端节点是不受支持的设备型号，则该站点将不包含在 优化 部分配置树中。树中的每个分支都包含以下子分支，这些子分支又包含一个或多个用于配置各自集合和设置的表单：
  - 默认功能
  - 默认调整设置
  - 默认应用程序分类器（集）
  - 默认服务类（设置）

以下部分提供有关为虚拟 WAN 启用 WAN 优化以及配置 默认 设置和设置的说明。

启用优化并配置默认功能设置

June 22, 2021

在虚拟 WAN 中启用 WAN 优化需要执行以下步骤：

1. 在“优化”部分的“功能”设置中启用 **WAN** 优化。

   本节提供了有关这一部分流程的说明。

2. 在 服务类 表中为每个适用的服务类配置加速策略设置。

   在完成 优化 配置的其余部分后，此过程将进一步执行。说明在配置优化默认服务类部分中提供。此时，您的配置中已启用 WAN 优化，但尚未在您的虚拟 WAN 中启用和激活。要在虚拟 WAN 中启用和激活 WAN 优化，您必须完成虚拟 WAN 配置，然后在部署中符合条件的站点上生成、暂存和激活虚拟 WAN 设备包，如本指南后续章节所述。

   要启用 WAN 优化并配置 默认 设置 部分 功 能设置，请执行以下操作：

a) 如有必要，请重新登录管理 Web 界面，然后打开 配置编辑器。

要打开 配置编辑器，请执行以下操作：

i. 选择页面顶部的 配置 选项卡以打开 配置 导航树（左窗格）。

ii. 在导航树中，单击 **Virtual WAN** 分支左侧的 **+** 以 打开该分支。

iii. 在 虚拟 **WAN** 分支中，选择 配置编辑器。

b) 打开要修改的配置包。

单击 打开 以显示 打开配置包 对话框，然后从 保存的包 下拉菜单中选择包。

这会将选定的软件包加载到 配置编辑器 中，并打开它进行编辑。
如果您拥有包含 WAN 优化功能的有效且当前的许可证，则“优化”部分可在 配置编辑器中找到。

> 注意
>
> 如果“优化”部分不可用，请检查您是否在虚拟 WAN 中安装了 SD-WAN 高级（企业）版许可证。SD-WAN 标准版不支持 WAN 优化功能。

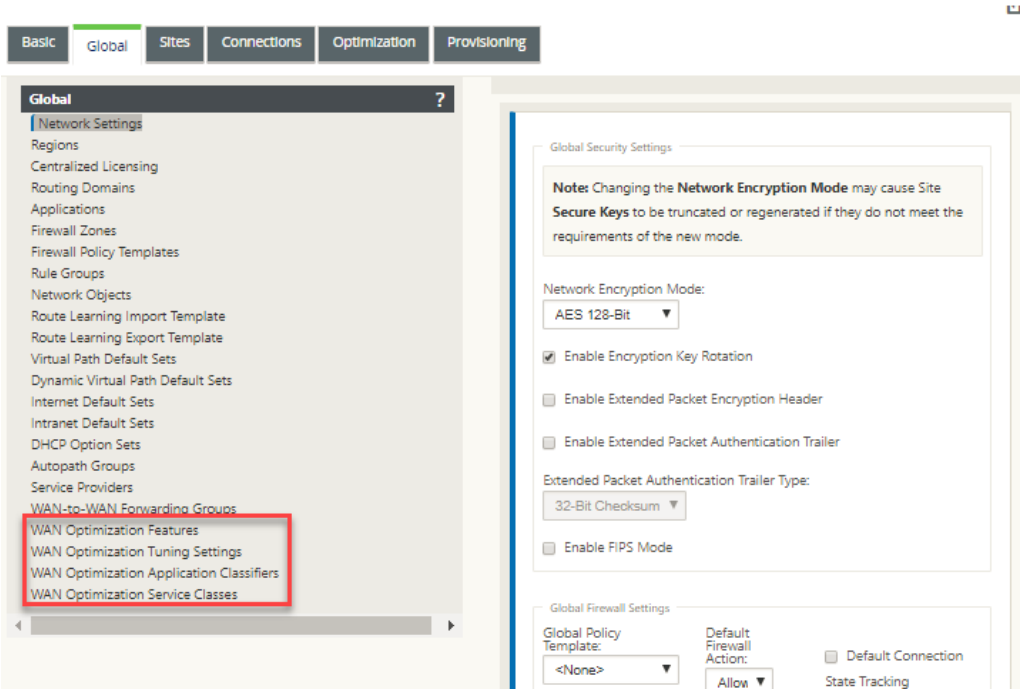
有关详细信息和说明，请参阅以下部分：

- SD-WAN 版本
- 许可

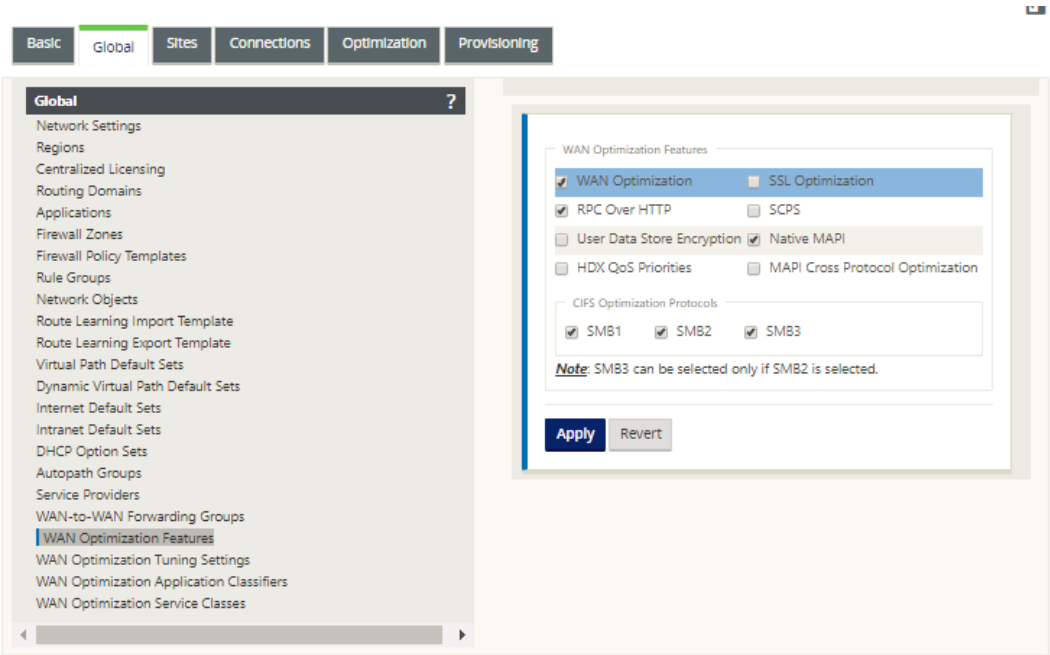
c) 单击 全局 选项卡。

您可以从 全 局 选项卡为 WAN 优化配置以下默认设置。

- 广域网优化功能
- WAN 优化调整设置
- WAN 优化应用程序分类器
- WAN 优化服务类



d) 单击 **WAN** 优化功能。



e) 选中 **WAN** 优化 复选框。

WAN 优化 复选框位于 **WAN** 优化 功能 部分的左上角。这将启用窗体进行编辑，并显示 应用 和 恢复 按钮。

> 注意
>
> 这只选择此功能用于启用。完成功能配置后，在您单击应用之前才能在优化部分或配置包中启用

> WAN 优化。此外，还必须按照 优 化配置过程中的进一步说明，在 服务类 表中为每个适用的服务类配置 加 速 设置。（部分提供了说明配置优化默认服务类）最后，在您完成整个虚拟 WAN 配置之前，将不会启用和激活 WAN 优化，然后在您的虚拟 WAN 中符合条件的站点上生成、暂存、分发和激活虚拟 WAN 设备包。

f) 配置 功能 设置。

单击复选框以选择或取消选择一个选项。您可以接受窗体中预先选择的默认设置，或自定义设置。

> 注意
>
> 默认情况下，您在 全局 选项卡中配置的设置会自动应用到树中包含的每个分支站点。但是，您可以自定义特定分支的 优化 配置，如本节所述配置分支站点的优化。

功能配 置窗体包含两个部分：

- 广域网优化功能
- **CIFS** 优化协议

WAN 优化功能 设置如下所示：

- **WAN** 优化—选中该复选框可为此配置启用 WAN 优化。这还可以实现压缩、重复数据消除和 TCP 协议优化。

  > 注意
  >
  > 必须选择 WAN 优化选项才能使其他 优化 部分选项可用。

- **SCPS** —选中该复选框可为卫星链路启用 TCP 协议优化。
- **HDX QoS** 优先级—选中该复选框以启用基于 HDX 子通道的优先级优化 ICA 流量的优先级。
- **MAPI** 跨协议优化—选中该复选框可启用 Microsoft Outlook (MAPI) 流量的跨协议优化。
- **SSL** 优化—选中该复选框可启用 SSL 加密对流量流进行优化。
- **RPC Over HTTP** —选中该复选框可启用使用 RPC Over HTTP 的 Microsoft Exchange 流量的优化。
- 用户数据存储加密—选中该复选框可通过 WAN 优化压缩历史记录加密来增强数据的安全性。
- 本机 **MAPI** —选中该复选框可启用 Microsoft Exchange 流量的优化。

  CIFS 优化协议 选项如下所示：

  - **SMB1** —选中该复选框以启用 Windows 文件共享优化 (SMB1)
  - **SMB2** —选中该复选框以启用 Windows 文件共享优化 (SMB2)
  - **SMB3** —选中该复选框以启用 Windows 文件共享的优化 (SMB3)。必须先选择 **SMB2** 选项，然后才能选择 **SMB3**。

g) 单击应用以启用选定的默认功能并将其添加到配置包中。

下一步是配置 优化 默认 调整设置。

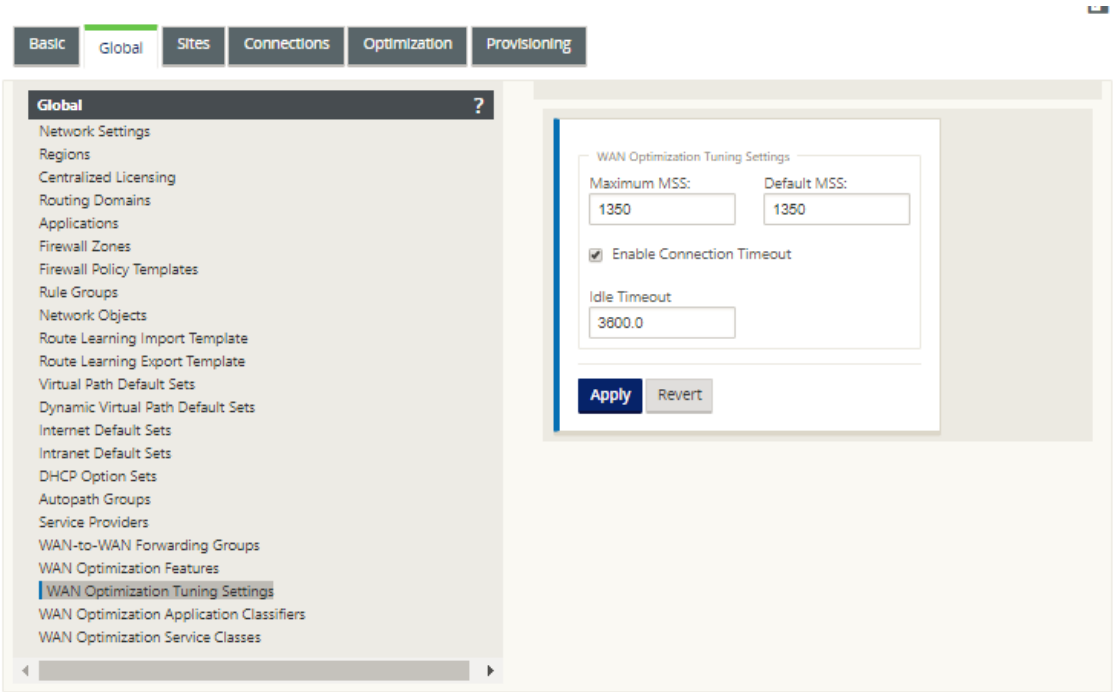
配置优化默认调谐设置

June 22, 2021

您可以在 全 局 选项卡中配置 WAN 优化默认调整设置。

要配置 WAN 优化默认 调整设置，请执行以下操作：

1. 在 全 局选项卡中，单击 **WAN** 优化调整设置。



2. 选择并配置调 整设置。

   调 谐设置 选项如下所示：

   - 最大 **MSS** —输入 TCP 段的最大分段大小 (MSS) 的最大大小（以字节 为单位）。
   - 默认 **MSS** —输入 TCP 数据段 MSS 的默认大小（以八位字节为单位）。
   - 启用连接超时—选择此选项可在超过空闲阈值时启用连接自动终止。
   - 空闲超 时—输入阈值（以秒为单位），以指定空闲连接终止之前允许的空闲时间。必须先选择 启用连接超时，然后才能配置此字段。

3. 单击应用。

   这会将修改后的 调谐设置 应用于全局配置。

   下一步是配置 WAN 优化应用程序分类器的默认集。

配置优化默认应用程序分类器

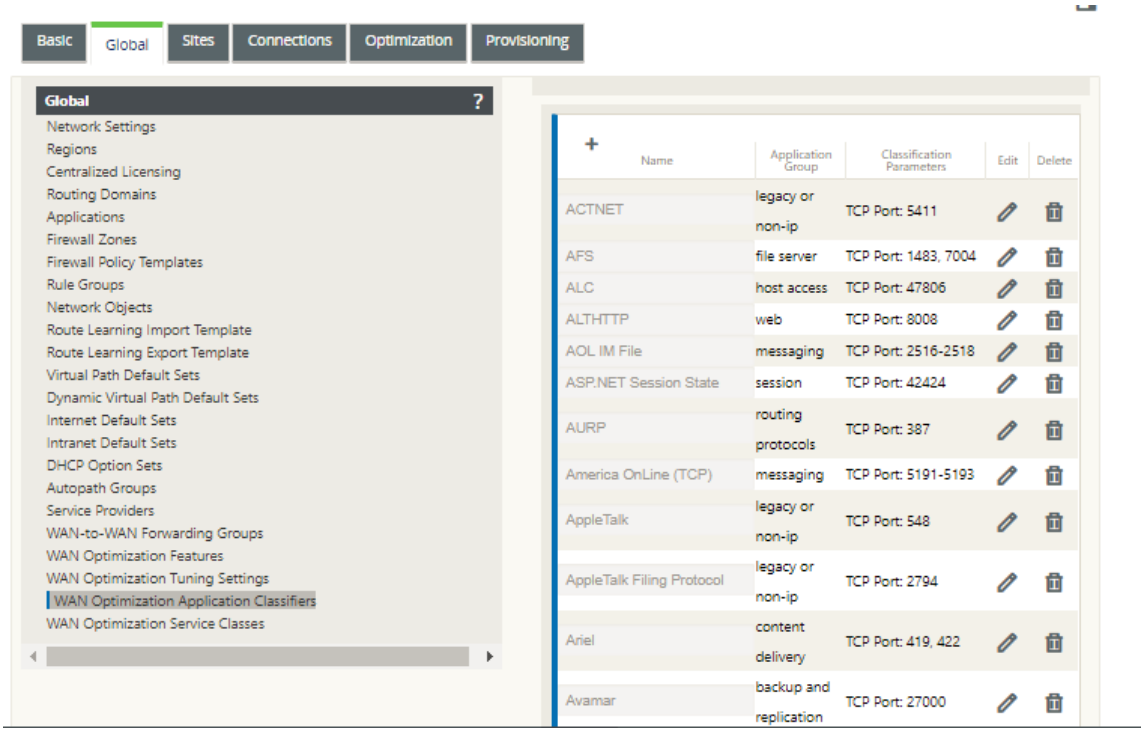
June 22, 2021

您可以在“全 局”选项卡中配置 WAN 优化默认应用程序分类器设置。

要配置 WAN 优化应用程序分类器的默认集，请执行以下操作：

1. 在“全 局”选项卡中，单击 **WAN** 优化应用程序分类器。

   此操作将打开 应用程序分类器 表，显示默认的应用程序分类器集。



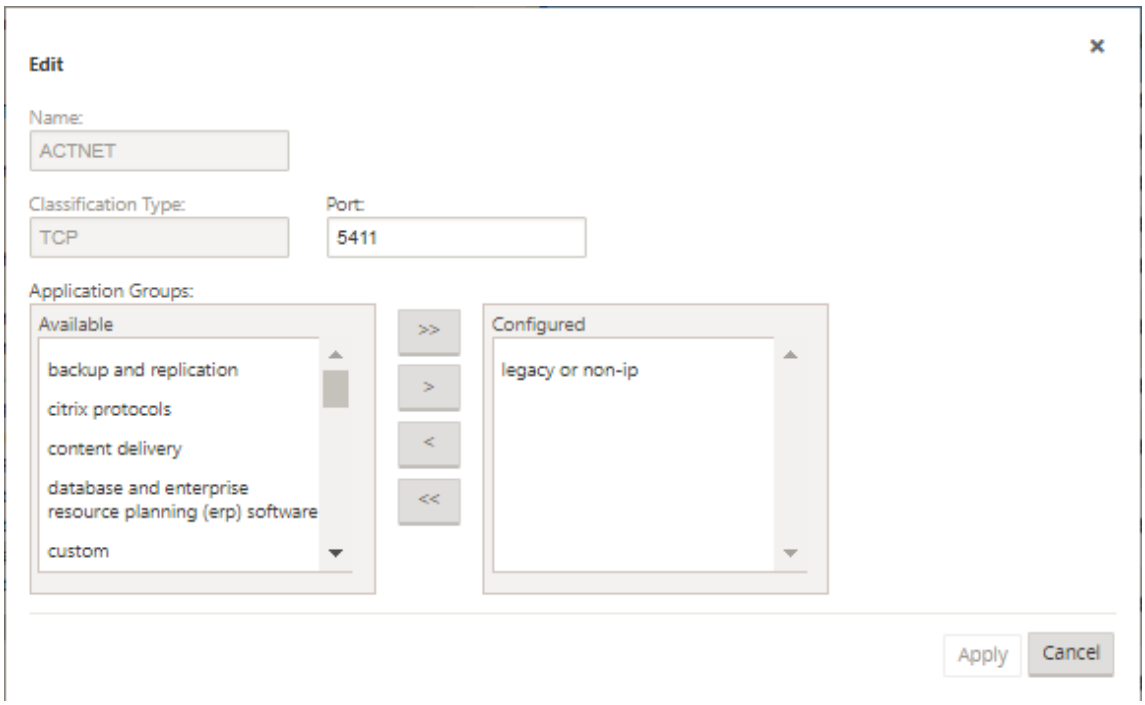
   此表也是一个配置窗体。您可以使用此窗体配置（编辑）、删除和添加应用程序分类器以创建自定义默认集。修改后的默认 应用程序分类器 集和您配置的单个应用程序分类器设置将自动作为默认值应用到 优化 部分树中包含的任何分支站点。

   > 注意

> 您还可以为每个特定 分支站点自定义应用程序分类器 集和设置。有关说明，请参阅部分配置分支站点的优化。

2. 要配置现有的应用程序分类器，请单击该分类器条目的 编辑 列中的编辑（铅笔图标）。

   此操作将打开弹出式 编辑 设置 窗体，用于配置选定的应用程序分类器。



3. 在 端口 字段中，输入应用程序分类器的端口号，或接受默认值。
4. 在 已配置 列表中添加或删除应用程序组，或接受默认值。
   - 将应用程序组添加到列表中：在左侧的 应用程序组 列表中选择该应用程序组，然后单击 添加右箭头 (>) 将该组添加到右侧的 已配置 列表中。要将所有 应用程序组 一次添加到列表中，请单击 添加全部 双向右箭头 (»)。
   - 要从列表中删除应用程序组：在右侧的 已配置 列表中选择该应用程序组，然后单击 删除左箭头 (<)。要同时从列表中删除所有 应用程序组，请单击 删除全部 左双箭头 («)。
5. 单击应用。

   这将您的更改应用于应用程序分类器，并取消编 辑 配置窗体。
6. （可选）自定义默认的 应用程序分类器 集。

   您可以添加或删除应用程序分类器以自定义默认集，如下所示：

   - 要从集中删除应用程序分类器：

   单击 应用程序分类器 条目的 删除 列中的垃圾扫雷图标，从表中删除该条目。

   - 要将应用程序分类器添加到集合中：

a) 单击 应用程序分类器分 支标签右侧的 **+**。

这将显示 添加 配置窗体。

b) 分别在 名称 和 端口 字段中输入应用程序分类器的 名称 和 端口 号。

c) 在 已 配置 列表中添加或删除应用程序组。

将应用程序组添加到列表中：在左侧的 应用程序组 列表中选择该应用程序组，然后单击 添加右箭头 (>) 将该组添加到右侧的 已配置 列表中。要将所有 应用程序组 一次添加到列表中，请单击 添加全部 双向右箭头 (»)。

要从列表中删除应用程序组：在右侧的 已配置 列表中选择该应用程序组，然后单击 删除左箭头 (<)。要同时从列表中删除所有 应用程序组，请单击 删除全部 左双箭头 («)。

d) 单击应用。

这会将新的应用程序分类器添加到集合中，并取消 添 加配置窗体。

下一步是配置 WAN 优化服务类的默认集。

配置优化默认服务类

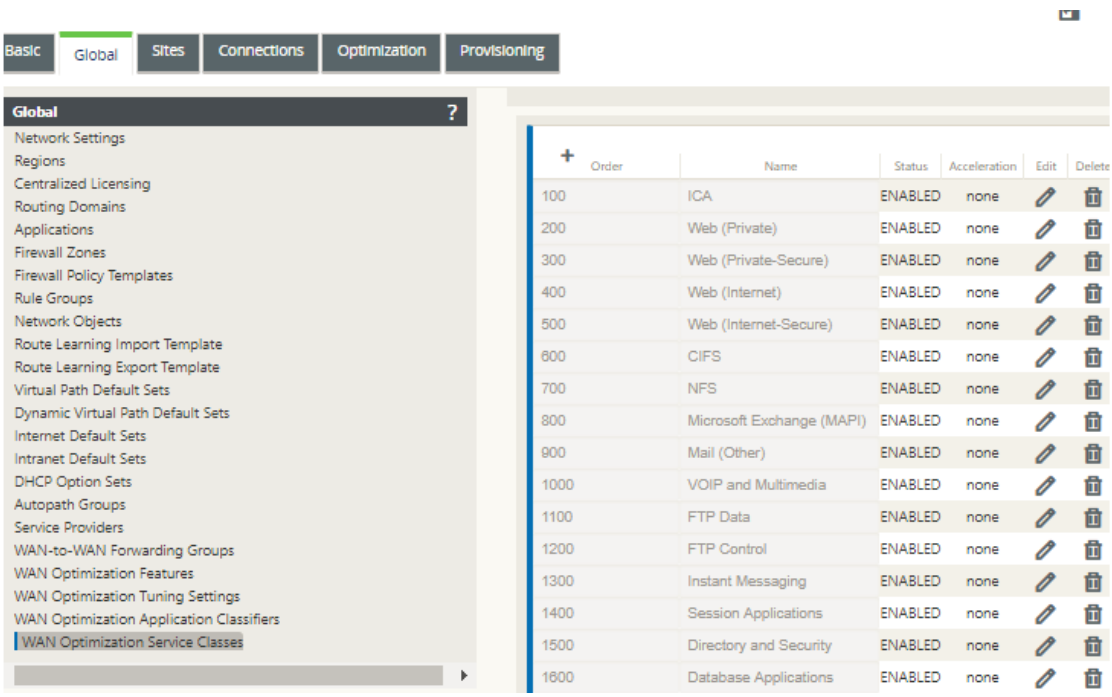
June 22, 2021

您可以在“全局”选项卡中配置 WAN 优化默认服务类设置。

要配置 WAN 优化服务类的默认集，请执行以下操作：

1. 在 全 局选项卡中，单击 **WAN** 优化服务类。

   此操作将打开 服务类 表，显示默认的服务类集。

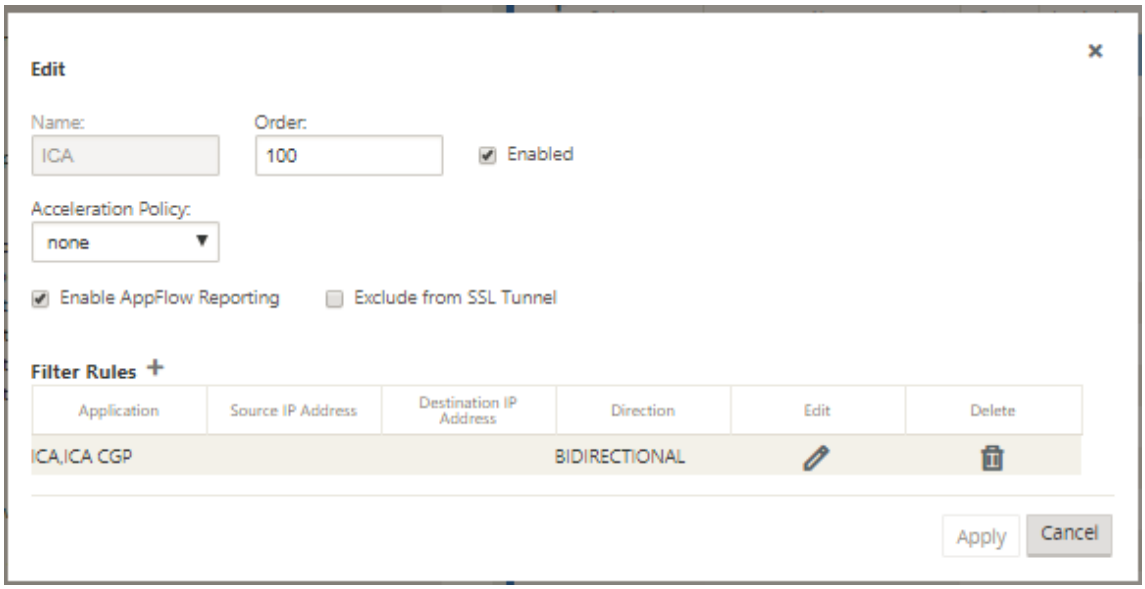


此表也是一个配置窗体。您可以使用此窗体配置（编辑）、删除和添加服务类以创建自定义默认集。修改后的默认服务类 集和您配置的单个服务类设置将自动作为默认值应用到 优化 部分树中包含的任何分支站点。

> 注意
>
> 您还可以自定义每个特定分支站点的 服务类 集和设置。有关为分支站点自定义 优化 配置的说明，请参阅部分配置分支站点的优化。

2. 要配置现有服务类，请单击 服务类 表中该类条目的 编辑 列中的 编辑（铅笔图标）。

   此操作将打开弹出 编辑 设置 窗体，用于配置所选服务类



3. 配置服务类的基本设置。

   基本设置如下：

   - 已启用—选择此选项以启用新的服务类。默认情况下，该类处于启用状态。
   - 加速策略—从加 速策略下拉菜单中选择一个策略。选项包括：
     - **disk** —选择此策略可将设备磁盘指定为存储用于压缩的流量历史记录的位置。这将为此服务类启用基于磁盘的压缩 (DBC) 策略。一般来说，磁盘 策略通常是最好的选择，因为设备会自动选择 磁盘 或内存 作为存储位置，具体取决于哪个位置更适合流量。
     - **none** —如果不想为此服务类启用加速策略，请选择此选项。无策略通常仅用于不可压缩的加密流量和实时视频。
     - 仅限流量控制—选择此策略可禁用压缩，但启用流量控制加速。为始终加密的服务和 FTP 控制通道选择此选项。
     - 内存—选择此策略可指定内存作为存储用于压缩的流量历史记录的位置。
   - 启用 **AppFlow** 报告—选择此选项可为此服务类启用 AppFlow 报告。AppFlow 是解锁由网络基础设施处理的应用事务数据的行业标准。WAN 优化 AppFlow 界面与任何 AppFlow 收集器一起工作，以生成报告。收集器使用 AppFlow 开放标准 (`http://www.appflow.org`) 从设备接收详细信息。

     有关 AppFlow 的更多信息，请参阅 Citrix 文档门户网站 `http://docs.citrix.com/` 上提供的 Citrix CloudBridge 7.4 产品文档。

     > 注意
     >
     > 要查看 WAN 优化 AppFlow 报告，请选择“监视”选项卡 **，** 然后在导航树（左窗格）中打开 **WAN** 优化 分支，然后选择 **AppFlow**。另请参阅 监视虚拟广域网。

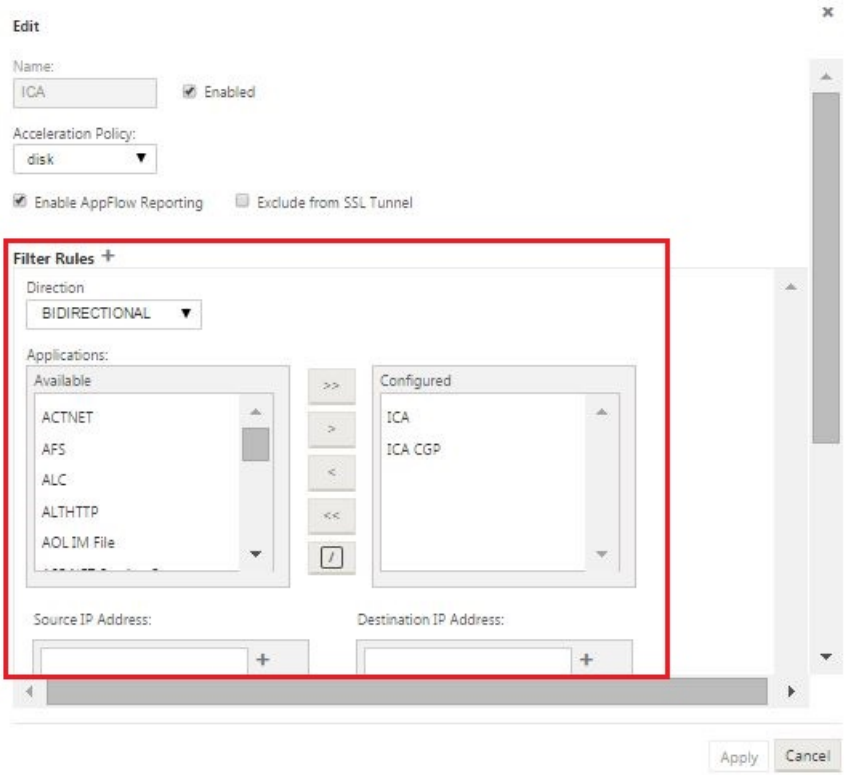
   - 从 **SSL** 隧道中排除—选择此选项可从 SSL 隧道中排除与服务类关联的流量。

4. 配置服务类的 筛选器规则。

   要编辑现有规则，请执行以下操作：

   a) 在筛选规则表（窗体底部）中，单击要编辑的规则的编辑列中的编辑（铅笔图标）。

      这将显示所选筛选器规则的筛选器规则设置。



b) 从 方向 下拉菜单中选择过滤器方向。

选择以下选项之一：

- 双向
- 单向

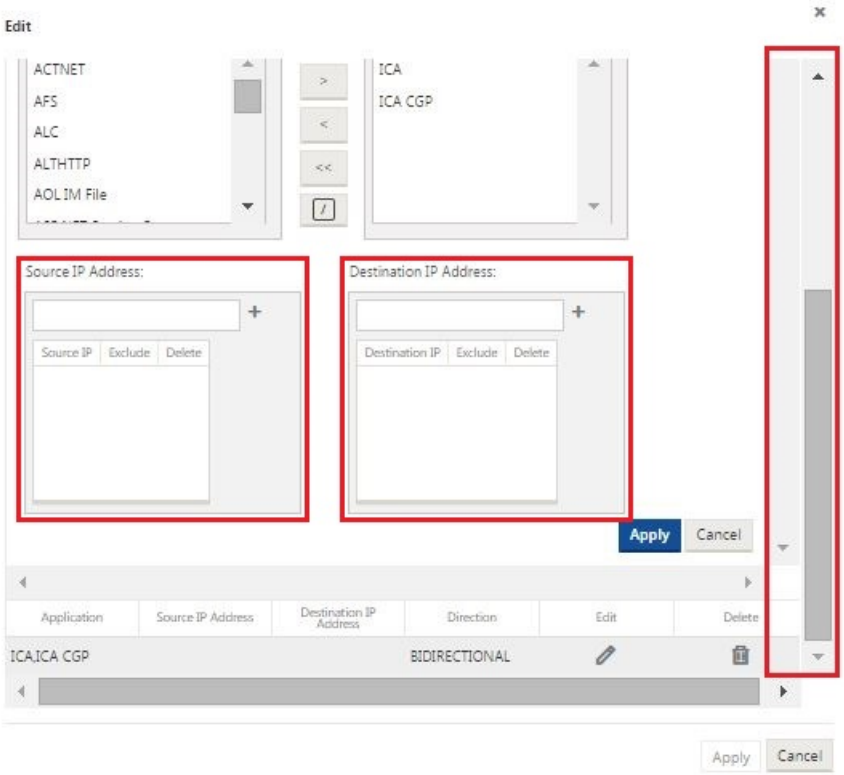
c) 在 已配置 列表中添加或删除应用程序。

将 应用程序添加到列表中：在左侧的 应用程序 列表中选择该应用程序，然后单击 添加右箭头 (**>**) 以将组添加到右侧的 已配置 列表中。若要一次将所有 应用程序 添加到列表中，请单击添加全部右箭头 (**»**)。

要从列表中删除应用程序：在右侧的 已配置 列表中选择该应用程序，然后单击 删除左箭头 **(<**)。要同时从列表中删除所有 应用程序，请单击 全部删除 左双箭头 (**«**)。

d) 向下滚动以显示窗体的截断部分。

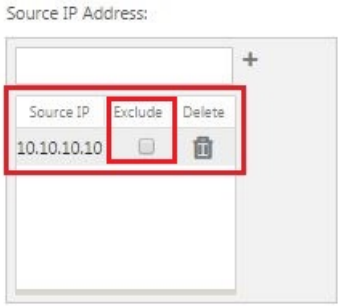
筛选规则 设置部分有点长，因此您需要使用滚动条来显示窗体的截断部分。



e) 在源 IP 地址字段中输入 源 **IP** 地址。

f) 单击您刚输入的源 IP 地址右侧的 **+**。

这会将指定的 IP 地址添加到 源 **IP** 地址 表中。



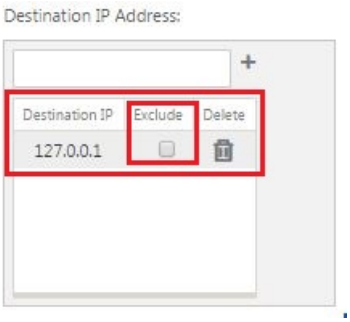
g) 指定是包括还是排除此筛选器规则的源 IP 地址。

选中 排除 复选框可从此筛选器规则中排除指定的源 IP 地址。取消选中复选框以包含地址。

h) 在目标 IP 地址字段中输入 目标 **IP** 地址。

i) 单击您刚刚输入的目标 IP 地址右侧的 **+**。

这会将指定的 IP 地址添加到 源 **IP** 地址 表中。



j) 指定是包括还是排除此筛选器规则的目标 IP 地址。

选中 排除 复选框可从此筛选器规则中排除指定的目标 IP 地址。取消选中复选框以包含地址。

k) 单击应用。

这将应用您对规则的修改并隐藏 筛选规则 设置部分。

5. （可选）自定义默认 服务类 集。

您可以添加或删除服务类以自定义默认集，如下所示：

- 要从集中删除服务类，请执行以下操作：

  单击表中某个服务类条目的 删除 列中的垃圾扫雷图标以删除该条目。

- 要将服务类添加到集合中：

  a) 单击 服务类 分支标签右侧的 **+**。

  这将显示 添加 配置窗体。

  b) 在“名称”字段中输入新服务类的 名称。

  c) 配置新的服务类。

  配置新服务类的步骤与修改现有服务类的步骤相同。有关说明，请参阅本节前面的以下步骤：

  “3. 配置服务类的基本设置。

  “4. 配置服务类的筛选器规则。

  d) 单击 添加 以将新的服务类添加到默认集，然后取消 添 加配置 窗体。

6. （可选，推荐）保存 配置包。

现在，您已完成全局 WAN 优化配置，并可以开始为分支站点配置 优化 集和设置。

配置分支站点的优化

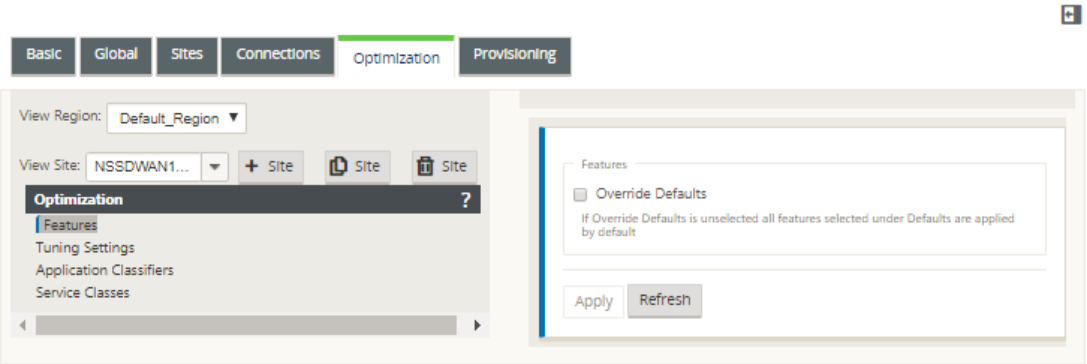
June 22, 2021

完成默认全局配置后，您可以选择为每个分支站点自定义集和设置。

您刚刚配置的全局设置会自动应用到 优化 部分中包含的每个分支站点。您可以选择接受默认值，或者自定义任何给定分支的配置。配置分支站点的 优化 集和设置的过程与配置全局默认值的过程相同，只有一些小区别。

要自定义分支站点的 优化 配置，请执行以下操作：

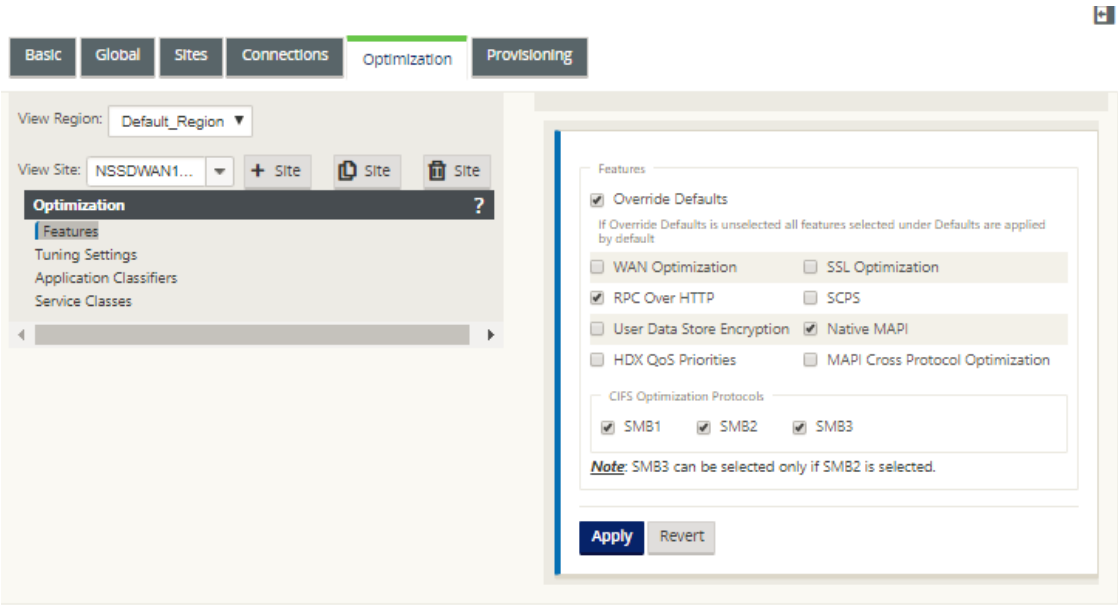
1. 单击 优化 选项卡，在查看站点字段中，选择一个站点。



2. 选中 覆盖默认值 复选框。

   这将显示该配置类别的顶级配置窗体，并将其打开以进行编辑。

   下图显示了一个示例顶级设置配置窗体，在本例中为 功能 集。



3. 输入您的配置更改。

   从此开始，每个分支站点 优化 类别的配置过程与对应的全局区域类别的配置过程相同。有关配置特定类别集或设置的说明，请参阅下面列出的相应部分：

   - 启用优化和配置默认功能设置。

- 配置优化默认调谐设置。
- 配置优化默认应用程序分类器。
- 配置优化默认服务类。

4. （可选，推荐）保存 配置包。

   您现在已完成配置虚拟广域网的 优化 部分集和设置。

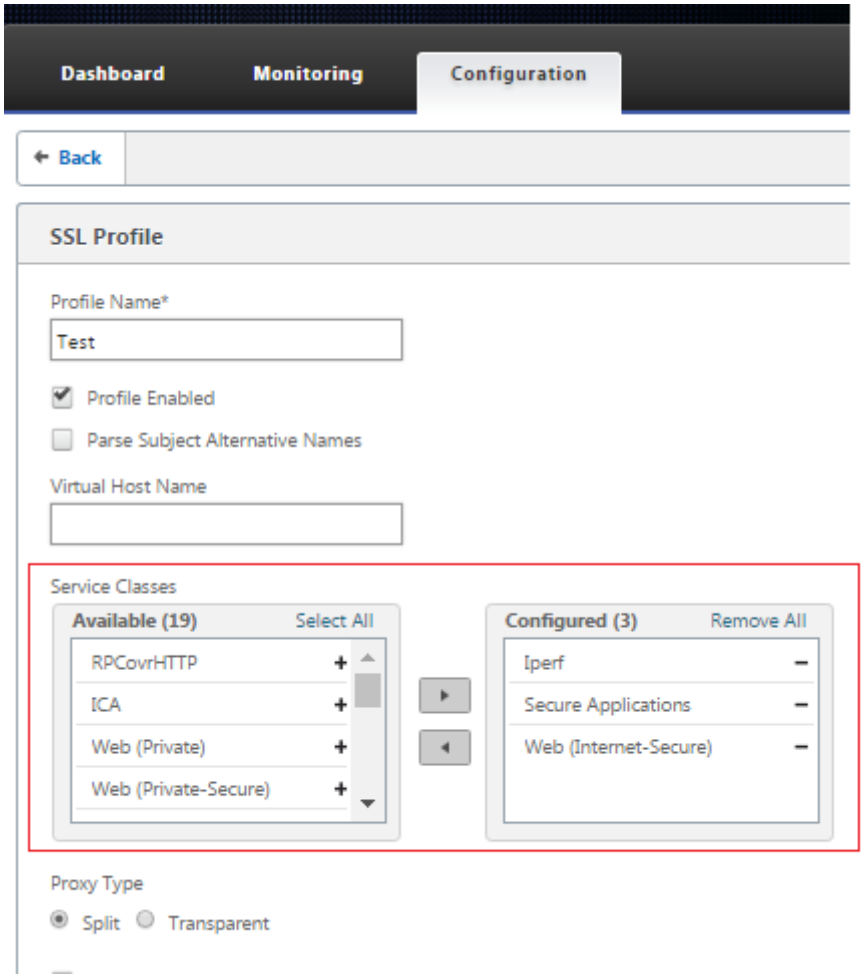
配置 SSL 配置文件

June 22, 2021

所有与 SSL 相关的配置都可以通过设备的新配置编辑器获取，以确保安全性和可用性。在 SD-WAN 高级版（企业版）和双盒部署中，服务类是从配置编辑器配置的，因此您无法附加任何 SSL 配置文件。为了容纳 SSL 配置文件映射到服务类的表达式，SSL 配置文件的工作流将更改为允许在配置文件节点中附加服务类。

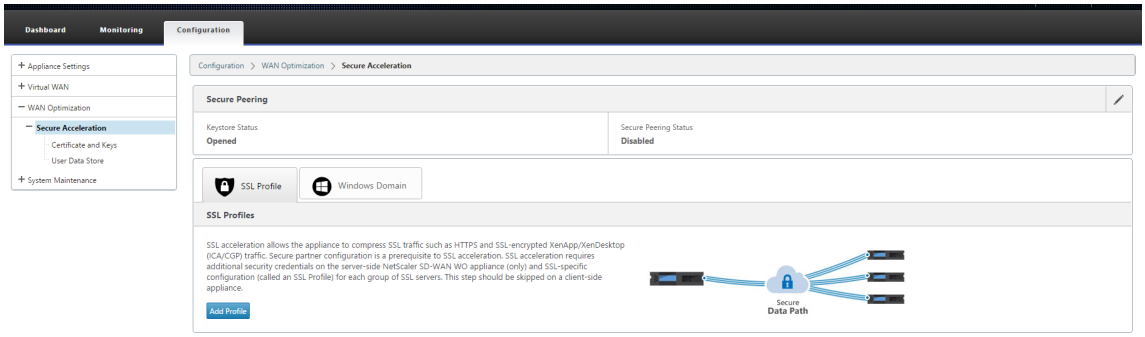
其中一个限制是 SSL 配置文件将附加到服务类中的所有规则。如果您需要选择性地将 SSL 配置文件附加到特定规则，则服务类配置将被拆分为详细规则以供进一步选择。

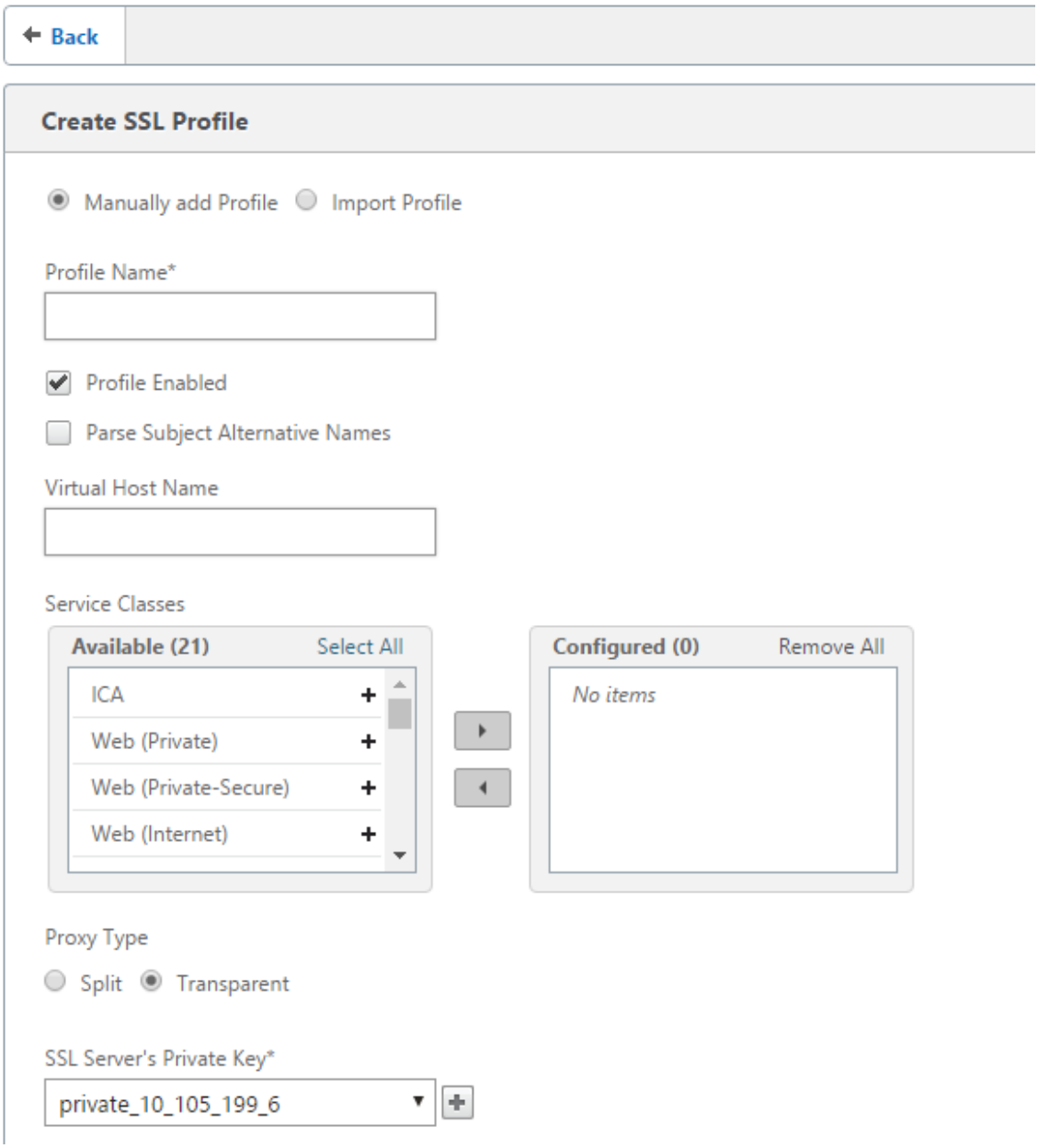
> 注意
>
> 只有将其筛选规则方向设置为单向的服务类才能与 SSL 配置文件相关联。



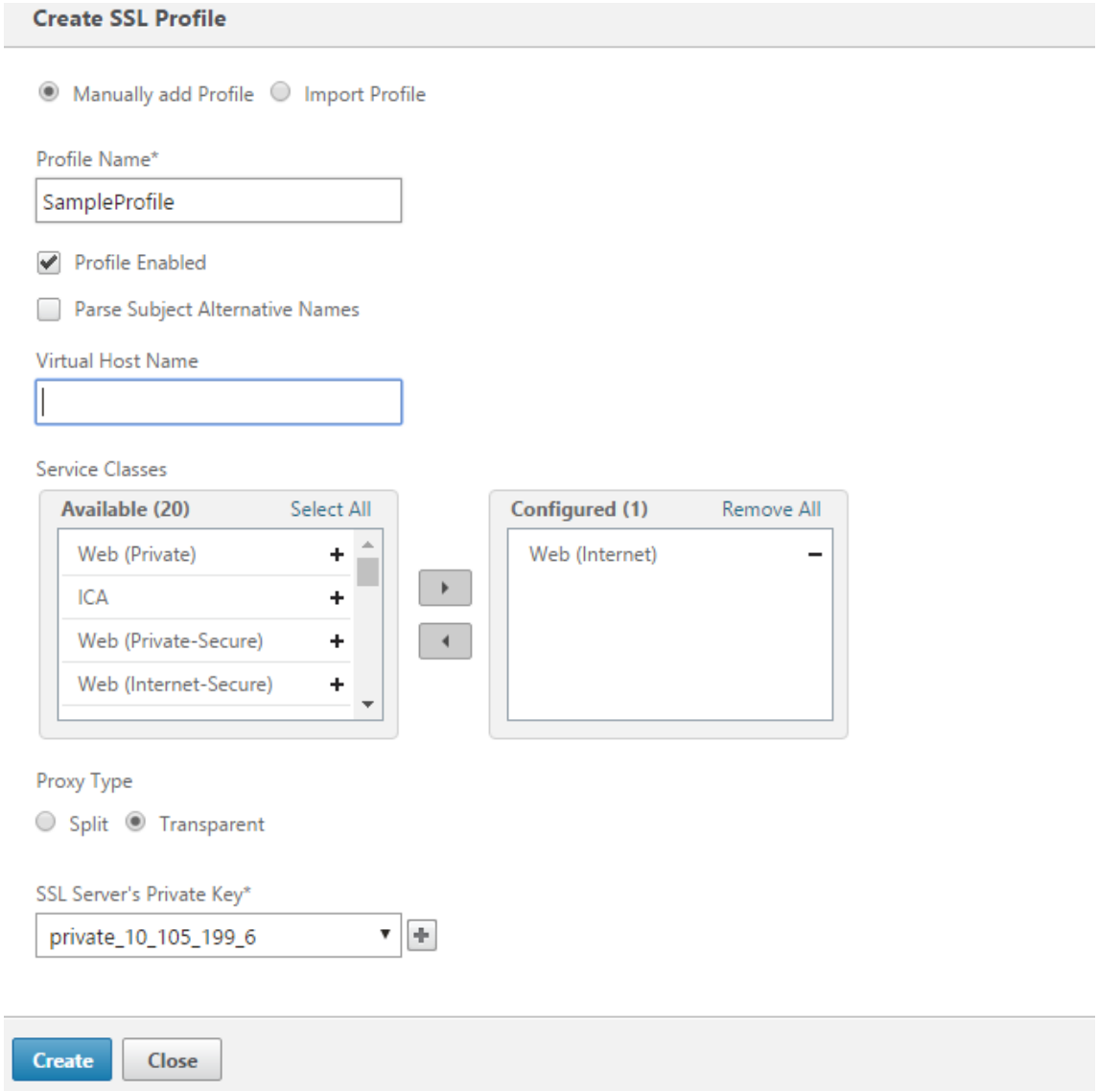
要在数据中心的新高级（企业）版设备上创建 SSL 配置文件，请执行以下操作：

1. 在 SD-WAN Web GUI 中，转到 配置 > 安全加速 页面。单击 添加配置文件。创建 **SSL** 配置文件。

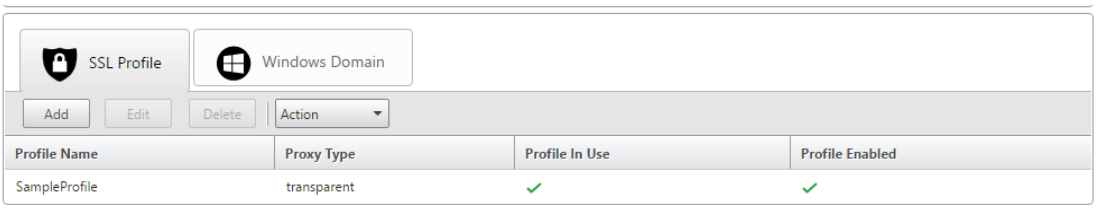




2. 在 创建 **SSL** 配置文件 页面中，提供配置文件名称，然后选择将与此配置文件关联的 服务类。选择 代理类型 并提供相关数据，然后单击 创建。



3. 成功创建 SSL 配置文件并关联服务类后，请查看 SSL 配置文件信息，如下所示。



Citrix 广域网优化客户端插件

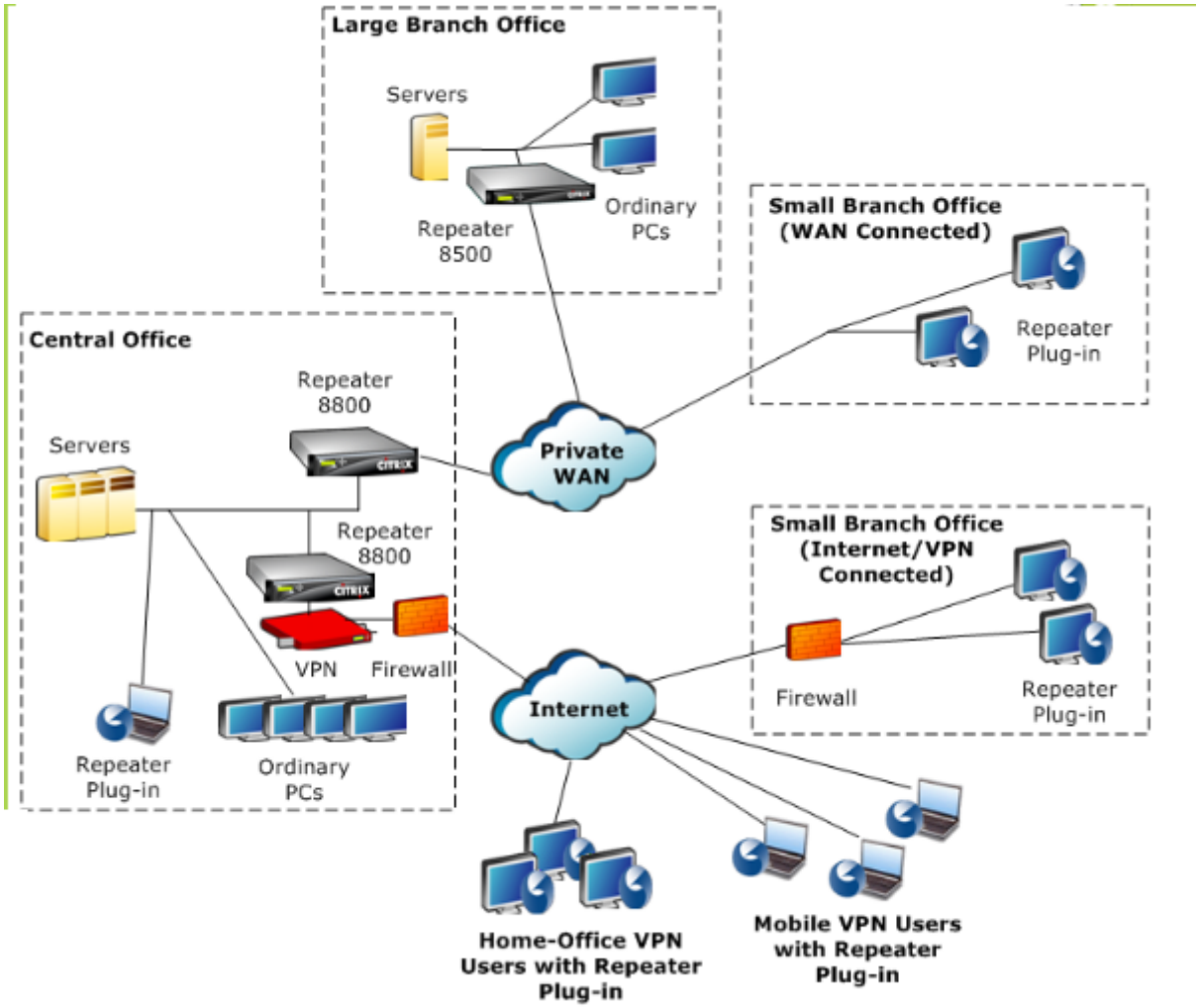
June 22, 2021

Citrix WANOP 客户端插件是一种基于软件的网络加速器，可在 Windows 笔记本电脑和工作站上运行，在任何地方提供加速，而不仅仅是在具有 WANOP 客户端插件设备的办公室。它连接到链接另一端的 Citrix WANOP 客户端插件设备。

WANOP 客户端插件操作的原理通常与 WANOP 客户端插件设备的原理相同。有关插件文档中未包含的主题，请参阅较大的文档集。

该插件作为标准的微软安装文件 (MSI) 分发。插件部署需要在链接的另一端对 WANOP 客户端插件设备进行某些特定于插件的配置。如果使用 WANOP 客户端插件设备的 DNS 或 IP 地址以及其他一些参数自定义 MSI 文件，则用户在其 Windows 计算机上安装插件时不必输入任何配置信息。

图 1. 显示 WANOP 客户端插件的典型 WANOP 客户端插件网络



> 注意
>
> 该插件受 Citrix Receiver 1.2 或更高版本的支持，并且可由 Citrix Receiver 分发和管理。

硬件和软件要求

June 22, 2021

在加速链接的客户端，Windows 台式机和笔记本电脑系统支持
WANOP 客户端插件，但不支持上网本或瘦客户端。Citrix 建议运行 WANOP 客户端插件的计算机遵循以下最低硬件规范：

- Pentium 4 级 CPU
- 2 GB RAM
- 2 GB 可用磁盘空间

Windows 10 平台支持 WANOP 客户端插件，需要以下系统要求：

- 4 GB 内存
- 10GB 可用磁盘空间

以下操作系统支持 WANOP 客户端插件：

- Windows XP Home
- Windows XP Professional
- Windows Vista（Home Basic、Home Premium、Business、Enterprise 和 Ultimate 的所有 32 位版本）
- Windows 7（Home Basic、Home Premium、Professional、Enterprise 和 Ultimate 的所有 32 位和 64 位版本）
- Windows 8（32 位和 64 位版本的高级版（企业版）
- Windows 10（32 位和 64 位版本的高级版（企业版）

在服务器端，以下设备当前支持 WANOP 客户端插件部署：

- 直放站 8500 系列
- 直放站 8800 系列
- WANOP 客户端插件 VPX
- WANOP 客户端插件 2000
- WANOP 客户端插件 3000
- WANOP 客户端插件 4000
- WANOP 客户端插件 5000

WANOP 插件的工作原理

June 22, 2021

WANOP 客户端插件产品使用您现有的 WAN/VPN 基础设施。安装插件的计算机将继续访问 LAN、WAN 和 Internet，就像安装插件之前一样。无需更改路由表、网络设置、客户端应用程序或服务器应用程序。

Citrix 接入网关 VPN 需要少量的 WANOP 客户端插件特定配置。

插件和设备处理连接的方式有两种变化：透明模式 和 重定向模式。重定向器是新部署不推荐使用的旧模式。

- 插件到设备加速的透明模式 与设备到设备加速非常相似。WANOP 客户端插件设备在插件和服务器之间传输时必须位于数据包所采用的路径中。与设备到设备的加速一样，透明模式可作为透明代理工作，从连接的一端保留源和目标 IP 地址以及端口号。
- 重定向器模式（不推荐）使用显式代理。插件将传出的数据包重新定向器 IP 地址。设备将数据包重新地址到服务器，同时将返回地址更改为指向自身而不是插件。在此模式下，设备不必物理上与 WAN 接口和服务器之间的路径内联（尽管这是理想的部署）。

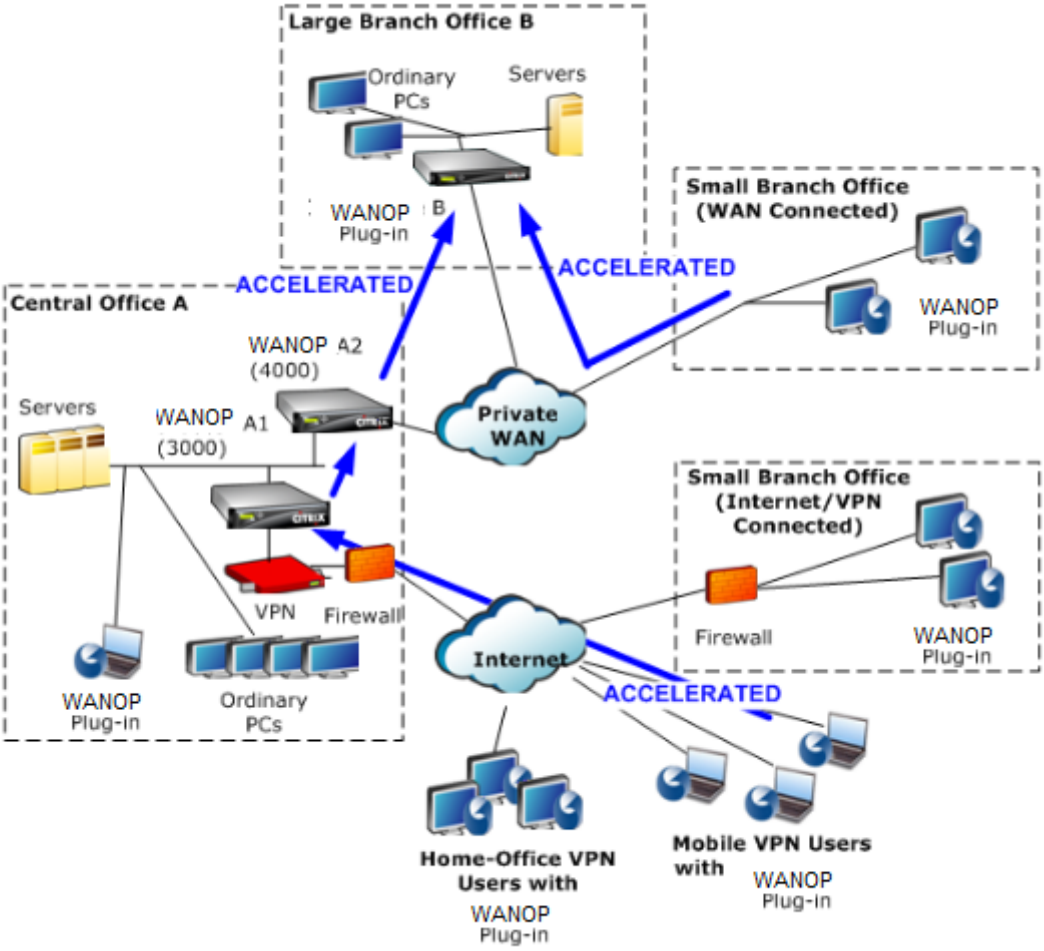
  最佳实践：当你可以使用透明模式，当你必须使用重定向模式。

透明模式

在透明模式下，用于加速连接的数据包必须通过目标设备，就像在设备到设备的加速中一样。

插件配置为可用于加速的设备列表。它尝试联系每个设备，打开信号连接。如果信令连接成功，插件会从设备下载加速规则，从而发送设备可加速的连接的目标地址。

图 1. 透明模式，突出显示三个加速路径



> 注意
>
> - 流量流-透明模式可加速 WANOP 客户端插件与启用插件的设备之间的连接。
> - 许可-设备需要许可证才能支持所需数量的插件。在图中，中继器 A2 不需要为插件加速许可，因为中继器 A1 提供了站点 A 的插件加速。
> - 菊花链-如果连接在通往目标设备的路上通过多个设备，则中间的设备必须启用“菊花链”，否则加速被阻止。在图中，中继器 B 加速了来自家庭办公室和移动 VPN 用户的流量来自大型分支机构 B 的流量。为此，中继器 A1 和 A2 必须启用菊花链。

每当插件打开新连接时，它都会查看加速规则。如果目标地址与任何规则匹配，插件会尝试通过将加速选项附加到连接中的初始数据包（SYN 数据包）来加速连接。如果插件已知的任何设备将加速选项附加到 SYN-ACK 响应数据包，则会与该设备建立加速连接。

应用程序和服务器不知道已建立加速连接。只有插件软件和设备知道正在发生加速。

透明模式类似于设备到设备的加速，但与其不完全相同。不同之处是：

- 仅客户端启动的连接—透明模式仅接受由配备插件的系统启动的连接。如果将配备插件的系统用作服务器，则不

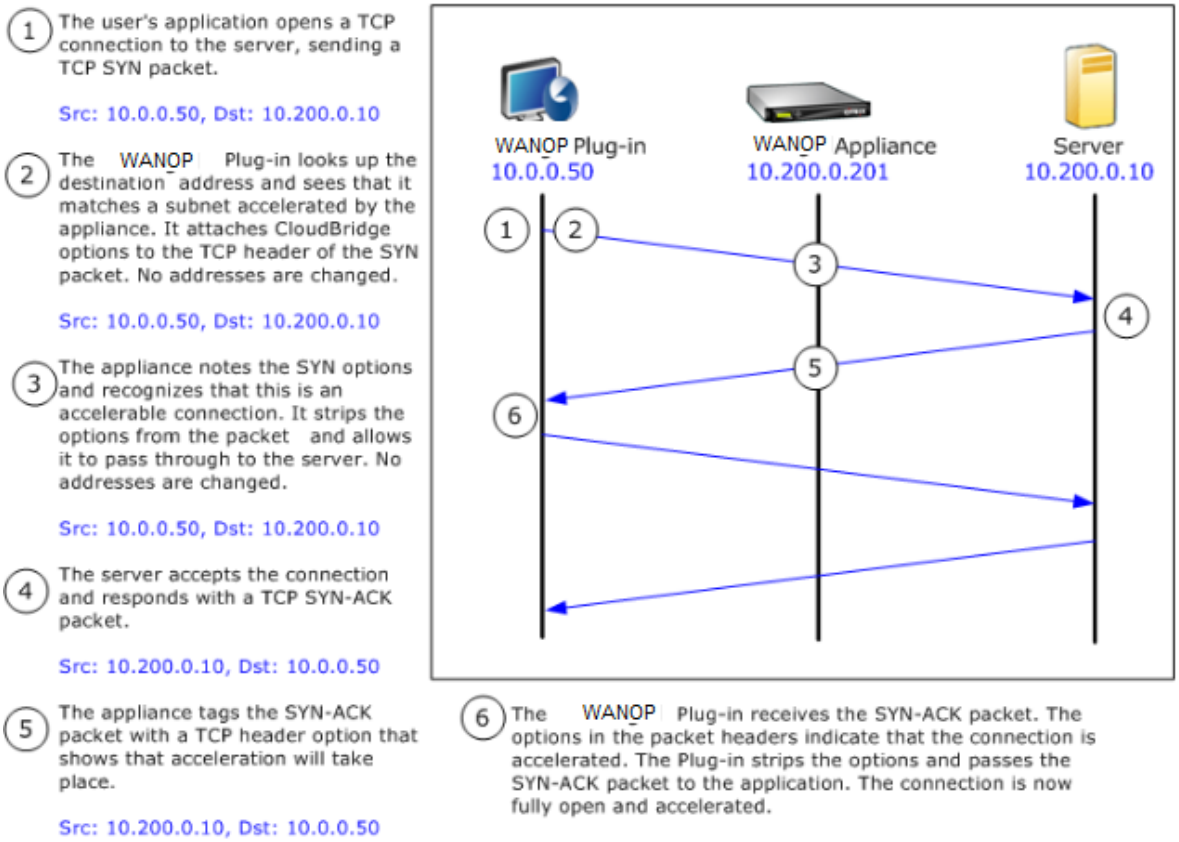
会加速服务器连接。另一方面，无论哪一端是客户端，哪一端是服务器，设备到设备的加速都会起作用。（主动模式 FTP 被视为特殊情况，因为启动插件请求的数据传输的连接是由服务器打开的。）

- 信令连接-透明模式使用插件和设备之间的信令连接传输状态信息。设备到设备加速不需要信令连接，但安全对等关系除外，默认情况下处于禁用状态。如果插件无法打开信令连接，则不会尝试通过设备加速连接。
- 菊花链-对于位于插件与其所选目标设备之间路径中的设备，必须在 配置：调整 菜单上启用菊花链。

透明模式通常与 VPN 一起使用。WANOP 客户端插件与大多数 IPsec 和 PPTP VPN 以及 Citrix Access Gateway VPN 兼容。

下图显示了透明模式下的数据包流。此数据包流几乎与设备到设备的加速相同，只是决定是否尝试加速连接是基于通过信令连接下载的加速规则。

图 2. 透明模式下的数据包流



重定向器模式

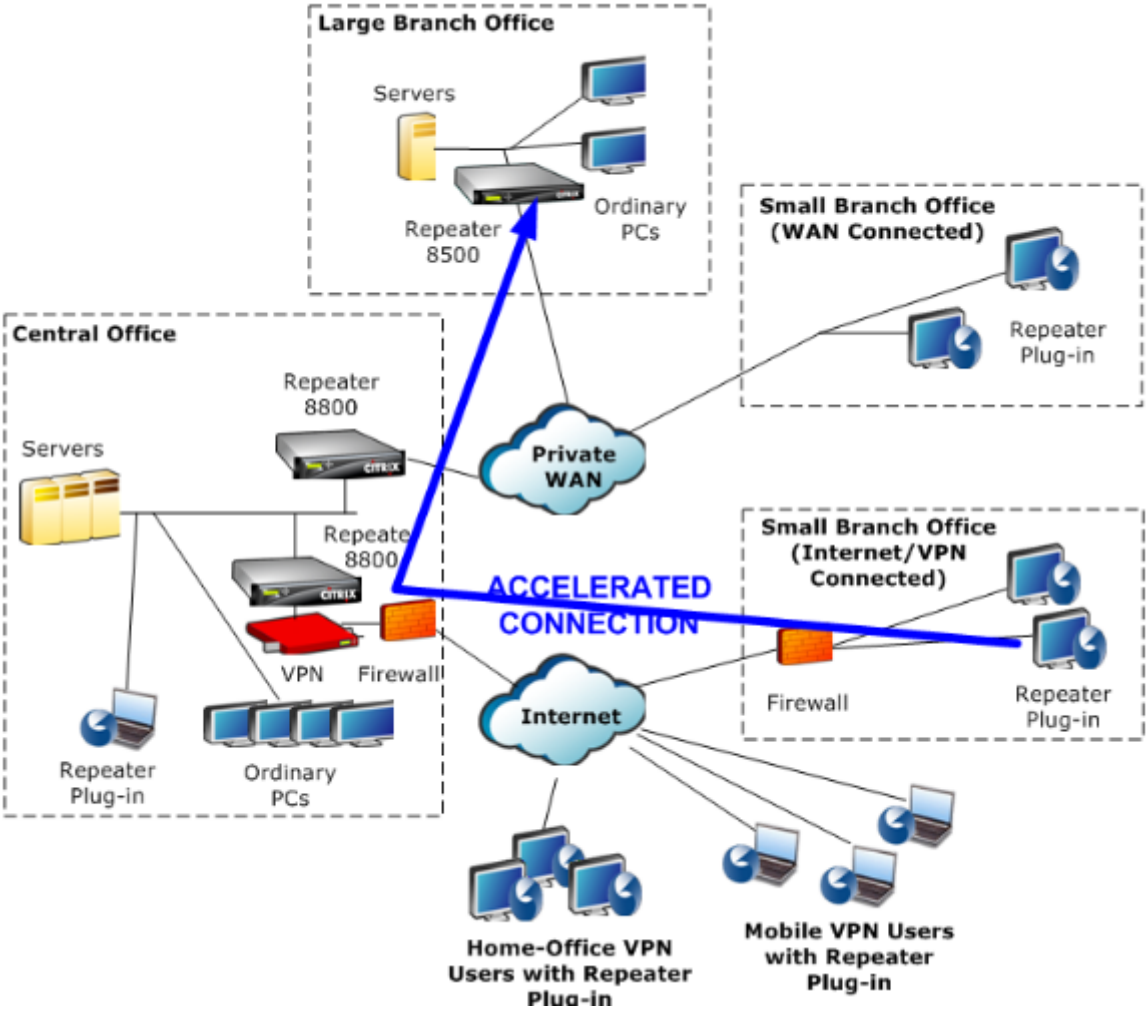
重定向器模式的工作方式与透明模式有所不同：

- WANOP 客户端插件软件通过将数据包明确地寻址到设备来重定向数据包。
- 因此，重定向器模式设备不必拦截所有 WAN-Link 流量。由于加速连接是直接给它的，因此只要插件和服务器都能到达，它就可以放置在任何地方。

- 设备执行其优化，然后将输出数据包重定向到服务器，将数据包中的源 IP 地址替换为自己的地址。从服务器的角度来看，连接始于设备。
- 来自服务器的返回流量会发送到设备，该设备在返回方向上执行优化，并将输出数据包转发到插件。
- 目标端口号不会更改，因此网络监视应用程序仍然可以对流量进行分类。

下图显示了重定向器模式的工作原理。

图 1. 重定向器模式



下图显示了 重定向器模式下的数据包流和地址映射。

图 2. 重定向器模式下的数据包流

1. The user's application opens a TCP connection to the server, sending a TCP SYN packet.

   Src: 10.0.0.50, Dst: 10.200.0.10

2. The Repeater Plug-in looks up the dst address and decides to redirect the connection to the appliance at 10.200.0.201.

   Src: 10.0.0.50, Dst: 10.200.0.201

   (10.200.0.10 is preserved in a TCP option field. Options 24-31 are used for various parameters.)

3. The appliance accepts the connection and forwards the packet to the server (using the dst address from the TCP options field), and giving itself as the src.

   Src: 10.200.0.201, Dst: 10.200.0.10

4. The server accepts the connection and responds with a TCP SYN-ACK packet.

   Src: 10.200.0.10, Dst: 10.200.0.201

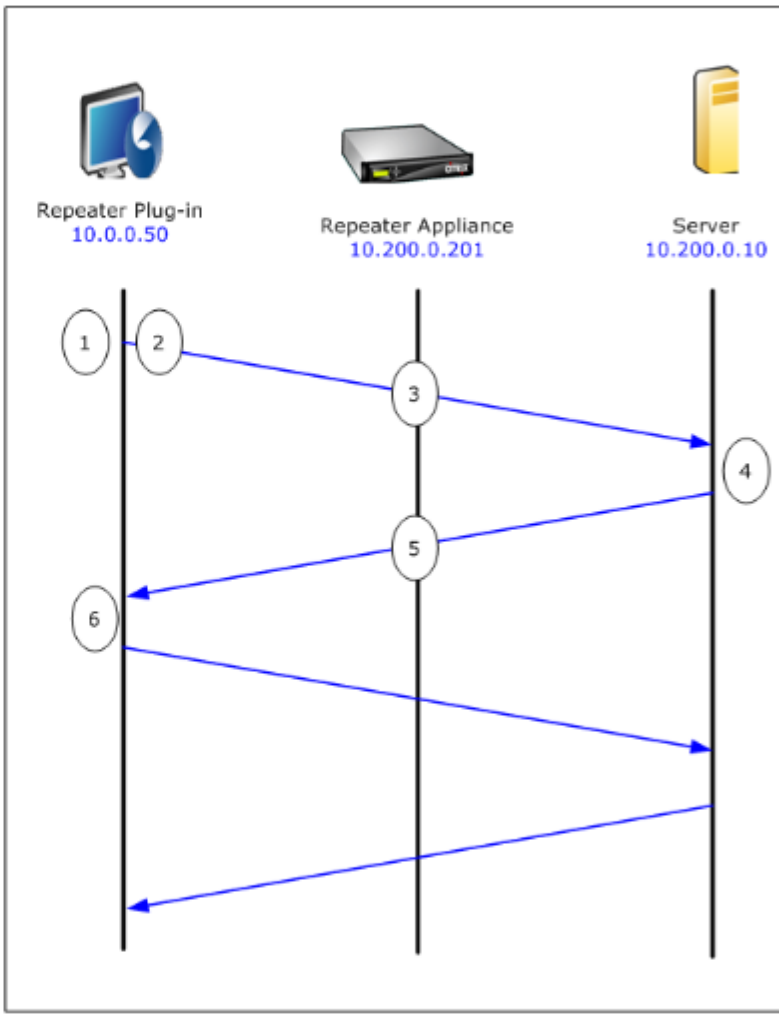
5. The appliance rewrites the addresses and forwards the packet to the Plug-in (placing the server address in an option field).

   Src: 10.200.0.201, Dst: 10.0.0.50

6. The connection is now fully open. The client and server send packets back and forth via the appliance.

   While the addresses are altered in Redirector mode, the destination port numbers are not (though the ephemeral port number may be). The data is not encapsulated. Redirector mode is a proxy, not a tunnel.

   There is no 1:1 relationship between packets (though in the end, the data received is always identical to the data sent). Compression may reduce many input packets into a single output packet. CIFS acceleration will perform speculative read-ahead and write-behind operations. Also, if packets are dropped between appliance and the Repeater Plug-in, the retransmission is handled by the appliance, not the server, using advanced recovery algorithms.



插件如何选择设备

每个插件都配置了它可以联系以请求加速连接的设备列表。

每个设备都有 加速规则列表，该列表是设备可以建立加速连接的目标地址或端口的列表。插件从设备下载这些规则，并将每个连接的目标地址和端口与每个设备的规则集匹配。如果只有一台设备提供加速给定连接，则选择非常简单。如果多个设备提供加速连接，则插件必须选择其中一个设备。

设备选择的规则如下所示：

- 如果提供加速连接的所有设备都是重定向模式设备，则会选择插件的设备列表中最左侧的设备。（如果将设备指定为 DNS 地址，并且 DNS 记录具有多个 IP 地址，则这些地址也会从左到右扫描。）
- 如果提供加速连接的某些设备使用重定向器模式，而有些设备使用透明模式，则忽略透明模式设备，并从重定向器模式设备中进行选择。
- 如果提供加速连接的所有设备都使用透明模式，则插件不会选择特定设备 *。* 它会启动使用 WANOP 客户端插件 SYN 选项的连接，并且任何候选设备都会将适当的选项附加到返回的 SYN-ACK 数据包。这允许实际上与流量一致的设备标识到插件中的自身。但是，插件必须与响应设备具有开放的信号连接，否则不会发生加速。
- 某些配置信息被视为全局信息。此配置信息取自可以打开信令连接的列表中最左侧的设备。

部署设备以便与插件一起使用

June 22, 2021

客户端加速需要在 WANOP 客户端插件设备上进行特殊配置。其他注意事项包括设备放置。插件通常部署用于 VPN 连接。

尽可能使用专用设备

尝试将同一设备用于插件加速和链路加速通常很困难，因为这两种用途有时要求设备位于数据中心的不同点，而这两种用途可以调用不同的服务类规则。

此外，单个设备可以用作插件加速的端点节点或用作站点到站点加速的端点节点，但不能同时用于同一连接。因此，当您将设备用于 VPN 的插件加速和站点到站点加速到远程数据中心时，插件用户不会接收站点到站点加速。此问题的严重程度取决于插件用户使用的数据有多少来自远程站点。

最后，由于专用设备的资源不会在插件和站点到站点需求之间划分，因此它们可为每个插件用户提供更多的资源，从而提高性能。

尽可能使用内联模式

应将设备部署在与其支持的 VPN 单元相同的站点上。通常情况下，这两个单位是相互一致的。内联部署提供最简单的配置、最多的功能和最高的性能。为了获得最佳效果，设备应直接与 VPN 单元保持一致。

但是，设备可以使用除组模式或高可用性模式之外的任何部署模式。这些模式适用于设备到设备和客户端到设备加速。它们可以单独使用（透明模式）或与重定向器模式组合使用。

将设备置于网络的安全部分

设备依赖于您的现有安全基础结构，与服务器相同。它应该与服务器放置在防火墙（和 VPN 单元，如果使用）的同一侧。

避免 **NAT** 问题

插件端的网络地址转换 (NAT) 是透明处理的，不是一个问题。在设备方面，NAT 可能会很麻烦。应用以下准则以确保顺利部署：

- 将设备放在与服务器相同的地址空间中，以便用于访问服务器的任何地址修改也应用于设备。
- 切勿使用设备未与其自身关联的地址访问设备。
- 设备必须能够通过使用插件用户访问相同服务器的相同 IP 地址来访问服务器。
- 简而言之，请勿将 NAT 应用于服务器或设备的地址。

选择软提升模式

在配置设置：带宽管理页面上，选择 Softboost 模式。Softboost 是唯一支持 WANOP 客户端插件插件的加速类型。

定义插件加速规则

设备维护一个加速规则列表，用于告知客户端要加速哪些流量。每个规则都指定一个地址或子网以及设备可以加速的端口范围。

加速什么-加速什么流量的选择取决于设备的使用情况：

- VPN 加速器-如果设备被用作 VPN 加速器，所有 VPN 流量都通过设备，则无论目的地如何，所有 TCP 流量都应加速。
- 重定向器模式-与透明模式不同，处于重定向器模式的设备是显式代理，导致插件将其流量转发到重定向器模式设备，即使这样做是不可取的。如果客户端将流量转发到远离服务器的设备，特别是如果此“三角形路由”引入了缓慢或不可靠的链接，则加速可能会起反作用。因此，Citrix 建议将加速规则配置为允许给定设备仅加速其自己的站点。

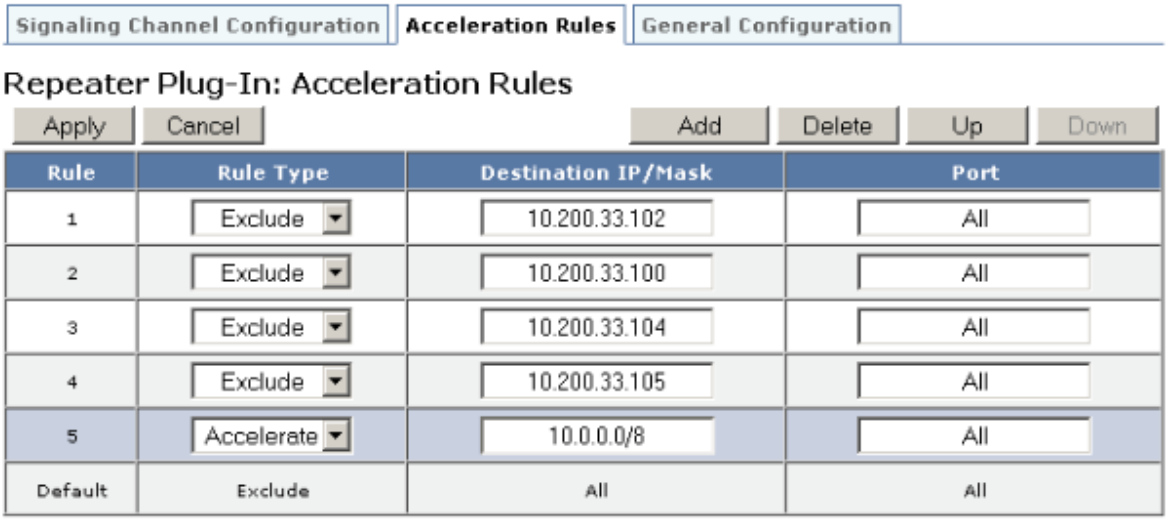
- 其他用途-当插件既不用作 VPN 加速器，也不用于重定向器模式时，加速规则应包括远程用户和数据中心本地的地址。

在 配置：**WANOP** 客户端插件：加速规则选项卡上定义规则-在设备上定义加速规则。

按顺序计算规则，并从第一个匹配规则执行操作（加速或排除）。要加速连接，它必须与加速规则匹配。

默认操作是不加速。

图 1. 设置加速规则



1. 在配置：WANOP 插件：加速规则选项卡上：
   - 为设备可以访问的每个本地 LAN 子网添加加速规则。也就是说，单击 添加”，选择“加 速”，然后键入子网 IP 地址和掩码。
   - 对设备本地的每个子网重复此操作。
2. 如果您需要排除包含范围的某些部分，请添加“排除”规则并将其移动到更常规的规则之上。例如，10.217.1.99 看起来像一个本地地址。如果它实际上是 VPN 单元的本地端点节点，请在 10.217.1.0/24 的加速规则上方的行上创建一个排除规则。
3. 如果要仅对单个端口（不推荐）使用加速，例如 HTTP 端口 80，请将“端口”字段中的通配符替换为特定端口号。您可以通过添加额外的规则（每个端口一个）来支持其他端口。
4. 一般来说，在一般规则之前列出狭窄的规则（通常是例外）。
5. 单击应用。如果您在应用更改之前离开此页面，则不会保存更改。

IP 端口使用情况

对于 IP 端口使用，请使用以下指南：

- 用于与 **WANOP** 客户端插件进行通信的端口—插件通过信令连接维护与设备的对话框，默认情况下，信令连接位于端口 443 (HTTPS) 上，这是通过大多数防火墙允许的。
- 用于与服务器通信的端口—WANOP 客户端插件插件与设备之间的通信使用的端口与客户端用于与服务器通信的端口相同（如果插件和设备不存在）。也就是说，当客户端在端口 80 上打开 HTTP 连接时，它会连接到端口 80 上的设备。设备依次与端口 80 上的服务器联系。

  在重定向器模式下，只保留已知端口（即 TCP SYN 数据包上的目标端口）。临时端口不会被保留。在透明模式下，保留两个端口。

  设备假定它可以在客户端请求的任何端口上与服务器通信，而客户端假定它可以在任何所需端口上与设备通信。如果设备遵守与服务器相同的防火墙规则，则此功能很好。在这种情况下，在直接连接中成功的任何连接都会在加速连接中成功。

TCP 选项使用和防火墙

WANOP 客户端插件参数在 TCP 选项中发送。TCP 选项可以出现在任何数据包中，并保证存在于建立连接的 SYN 和 SYN-ACK 数据包中。

防火墙不得阻止 24-31（十进制）范围内的 TCP 选项，否则无法进行加速。大多数防火墙不会阻止这些选项。但是，默认情况下，具有版本 7.x 固件的思科 PIX 或 ASA 防火墙可能会这样做，因此您可能需要调整其配置。

自定义插件 **MSI** 文件

June 22, 2021

您可以更改
WANOP 客户端插件分发文件中的参数，该文件采用标准的 Microsoft 安装程序 (MSI) 格式。自定义需要使用 MSI 编辑器。

> 注意
>
> 已编辑过的参数中已更改。MSI 文件仅适用于新安装。当现有插件用户更新到新版本时，其现有设置将保留。因此，更改参数后，您应该建议用户在安装新版本之前卸载旧版本。

最佳实践：

创建解析到最近已启用插件的设备的 DNS 条目。例如，定义“Repeater.mycompany.com”，并将其解析为您的设备（如果您只有一个设备）。或者，假如您有五台设备，将 Repeater.mycompany.com 解析为您的五台设备中的一台，选择设备是根据靠近客户端或 VPN 单元的程度进行的。例如，使用与特定 VPN 关联的地址的客户端应看到 Repeater.mycompany.com 解析为连接到该 VPN 的 WANOP 客户端插件设备的 IP 地址。使用 MSI 编辑器（如 Oorca）将此地址构建到插件二进制文件中。添加、移动或删除设备时，更改 DNS 服务器上的此单个 DNS 定义会自动更新插件上的设备列表。

您也可以将 DNS 条目解析为多个设备，但除非所有设备的配置相同，否则这是不可取的，因为插件从列表中最左侧的设备获取其中一些特征，并在全局范围内应用它们（包括 SSL 压缩特征）。这可能会导致不希望的和令人困惑的结果，尤其是当 DNS 服务器为每个请求旋转 IP 地址的顺序时。

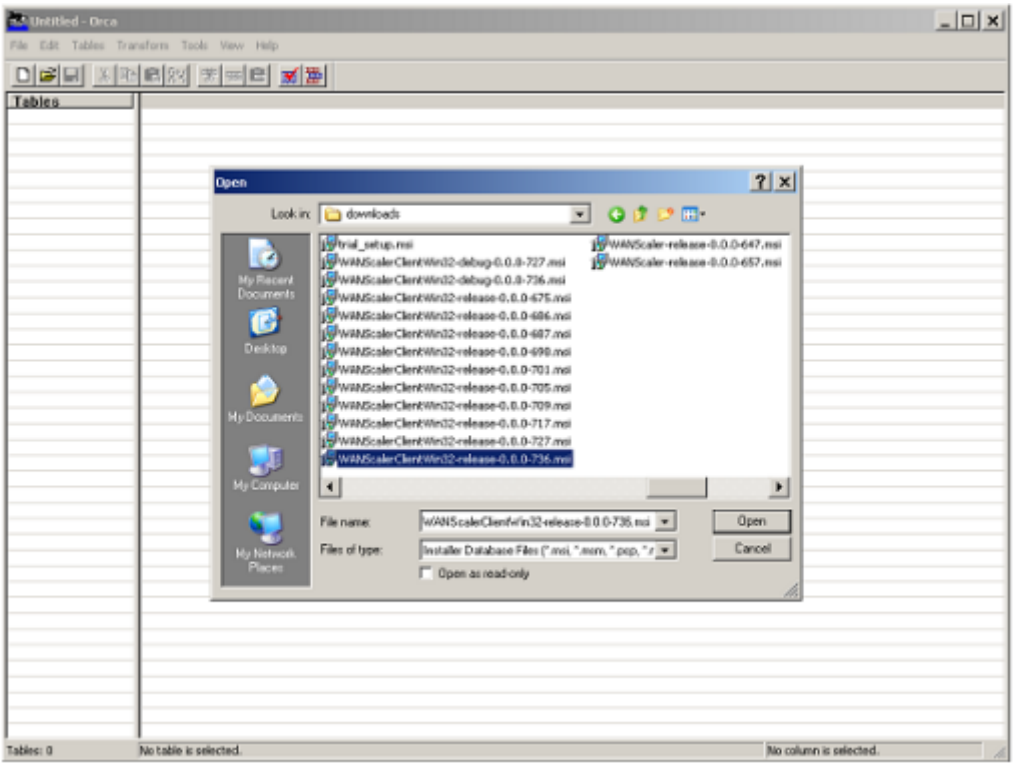
安装略卡 **MSI** 编辑器：

有许多 MSI 编辑器，如 Oorca，它是微软免费平台 SDK 的一部分，可以从微软下载。

- 安装 Orca MSI 编辑器的步骤

  1. 下载软件开发工具包的 PSDK-x86.exe 版本并执行它。按照安装说明进行操作。
  2. 安装 SDK 后，必须安装 Orca 编辑器。它将在 Microsoft 平台 SDK\Bin\Orca.Msi 下进行。启动 Orca.msi 以安装实际的逆戟鲸编辑器 (orca.exe)。
  3. 运行逆戟—微软提供其在线的逆戟鲸文档。以下信息介绍了如何编辑最重要的 WANOP 客户端插件参数。
  4. 启动逆戟鲸与 开始 **>** 所有程序 **>** 逆戟鲸。当出现空白的 Orca 窗口时，打开 WANOP 客户端插件 MSI 文件，其中包含“文 件” **>** “打开”。

     图 **1.** 使用奥卡岛

  5. 在表菜单上，单击属性。此时将显示.MSI 文件的所有可编辑属性的列表。编辑下表中显示的参数。要编辑参数，请双击其值，键入新值，然后按 En **ter** 键。

参数	说明	默认值	注意
WSAPPLIANCES	设备列表	无	以逗号分隔的列表形式在此处输入您的 WANOP 设备的 IP 或 DNS 地址，即 { appliance1, appliance2, appliance3 }。如果用于信号连接的端口与默认端口 (443) 不同，请使用 Appliance1:port_number 格式指定端口。
DBCMINSIZE	用于压缩的最小磁盘空间量（以兆字节为单位）	250	将其更改为较大的值（例如，2000）可提高压缩性能，但如果磁盘空间不足，则会阻止安装。除非您为 DBCMINSIZE 指定的值之外，还有至少 100 MB 的可用磁盘空间，否则不会安装插件。
EKEYPEM	插件的私钥。使用 SSL 压缩的证书/钥钥对的部分	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的私钥（开头为—-BEGIN RSA PRIVATE KEY—-)
X509CERTPEM	插件的证书。使用 SSL 压缩的证书/钥钥对的部分	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的证书（开头为—-BEGIN CERTIFICATE —-)
CACERTPEM	插件的证书颁发机构证书。与 SSL 压缩一起使用	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的证书（开头为—-BEGIN CERTIFICATE —-)

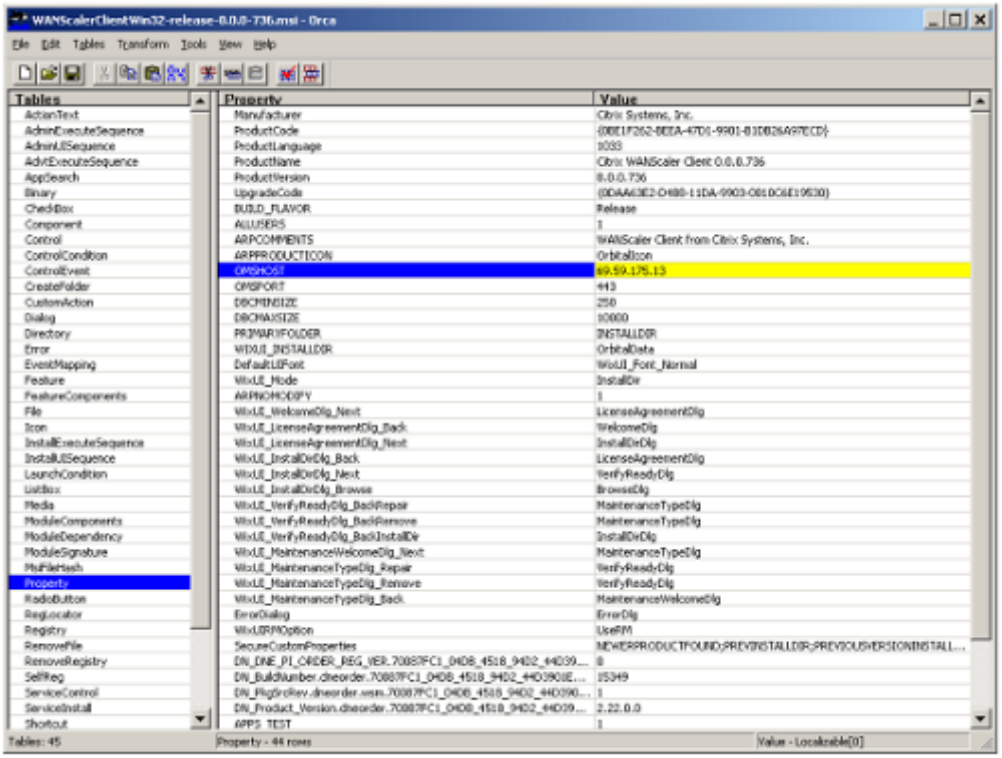
6. 在表菜单上单击属性。此时将显示.MSI 文件的所有可编辑属性的列表。编辑下表中显示的参数。要编辑参数，请双击其值，键入新值，然后按 En **ter** 键。

参数	说明	默认值	注意
WSAPPLIANCES	设备列表	无	以逗号分隔的列表形式在此处输入您的 WANOP 客户端插件设备的 IP 或 DNS 地址，即 *{ appliance1, appliance2, appliance3 }*。如果用于信令连接的端口与默认端口 (443) 不同，请以 *Appliance1*：*Port_Number* 格式指定端口。
DBCMINSIZE	用于压缩的最小磁盘空间量（以兆字节为单位）	250	将其更改为较大的值（例如，2000）可提高压缩性能，但如果磁盘空间不足，则会阻止安装。除非您为 DBCMINSIZE 指定的值之外，还有至少 100 MB 的可用磁盘空间，否则不会安装插件。
PRIVATEKEYPEM	插件的私钥。使用 SSL 压缩的证书/钥钥对的部分	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的私钥（开头为—–BEGIN RSA PRIVATE KEY—–)
X509CERTPEM	插件的证书。使用 SSL 压缩的证书/钥钥对的部分	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的证书（开头为—–BEGIN CERTIFICATE —–)

参数	说明	默认值	注意
CACERTPEM	插件的证书颁发机构证书。与 SSL 压缩一起使用	无	使用逆戟鲸的粘贴单元格命令。正常的粘贴函数不会保留键的格式。应该是 PEM 格式的证书（开头为—-BEGIN CERTIFICATE—-）

7. 完成后，使用 文件：另存为”命令以 新文件名保存已编辑的文件；例如 test.msi。

   图 **2**：在 **Orca** 中编辑参数：



8. 完成后，使用 文件：另存为”命令以 新文件名保存已编辑的文件；例如 test.msi。

   您的插件软件现已定制。

   > 注意
   >
   > 一些用户在 orca 中看到一个错误，导致它将文件截断为 1 MB。检查保存的文件的大小。如果已截断，请创建原始文件的副本，然后使用“保存”命令覆盖原始文件。

   使用 Orca 自定义设备列表并将自定义 MSI 文件分发给用户后，用户在安装软件时无需键入任何配置信息。

在 **Windows** 系统上部署插件

June 22, 2021

WANOP 客户端插件是一个可执行的 Microsoft 安装程序 (MSI) 文件，您可以下载和安装与任何其他 Web 分布式程序一样。从 Citrix.com Web 站点的 MyCitrix 部分获取此文件。

> 注意：
>
> WANOP 客户端插件用户界面将自身称为 **Citrix** 加速插件管理器。

插件所需的唯一用户配置是设备地址列表。此列表可以由逗号分隔的 IP 或 DNS 地址列表组成。这两种形式可以混合。您可以自定义分发文件，以便默认情况下列表指向您的设备。安装后，操作是透明的。通过适当的设备发送到加速子网的流量，并将所有其他流量直接发送到服务器。用户应用程序不知道任何这种情况正在发生。

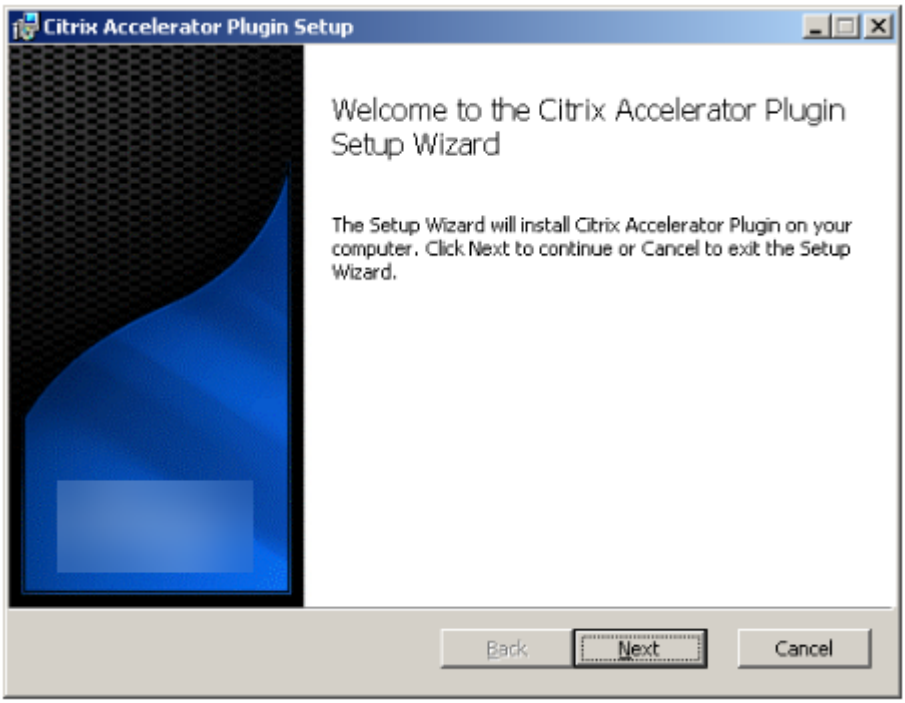
安装

> 必备条件：
>
> Windows 10 要求所有驱动程序具有有效的数字签名才能执行安装而不会出现任何错误。

要在 Windows 系统上安装 WANOP 客户端插件插件加速器，请执行以下操作：

1. Repeater*.msi 文件是一个安装文件。关闭所有应用程序和可能打开的任何窗口，然后按常规方式启动安装程序（在文件窗口中双击，或使用 run 命令）。

   图 **1.** 初始安装屏幕：



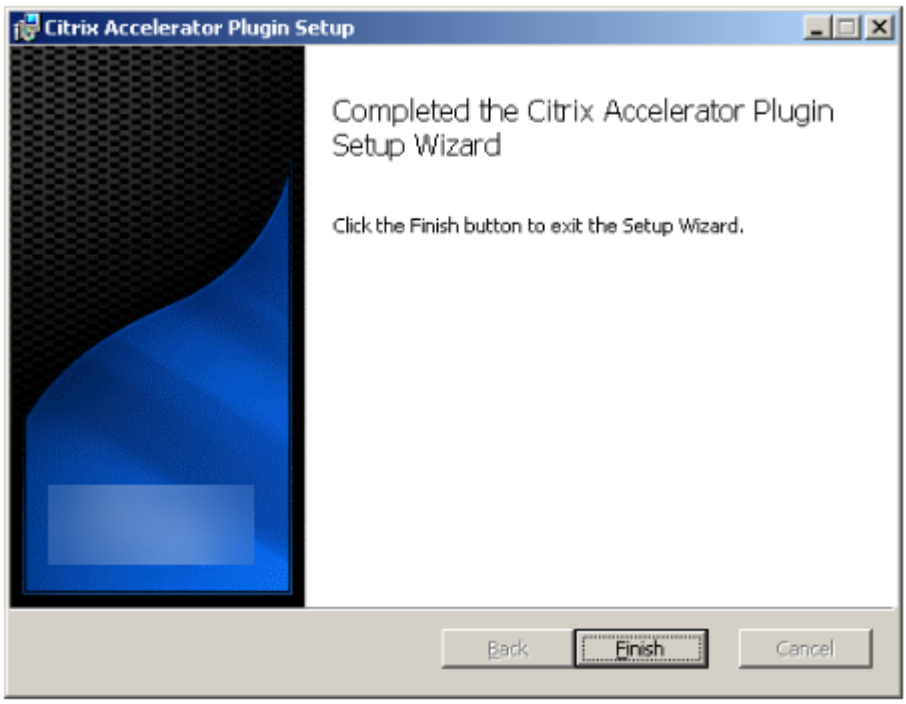
以下步骤适用于交互式安装。可以使用以下命令执行静默安装：

客户端 **_msi_** 文件**/qn**

2. 安装程序会提示输入安装软件的位置。您指定的目录用于客户端软件和基于磁盘的压缩历史记录。它们总共需要最低 500 MB 的磁盘空间。

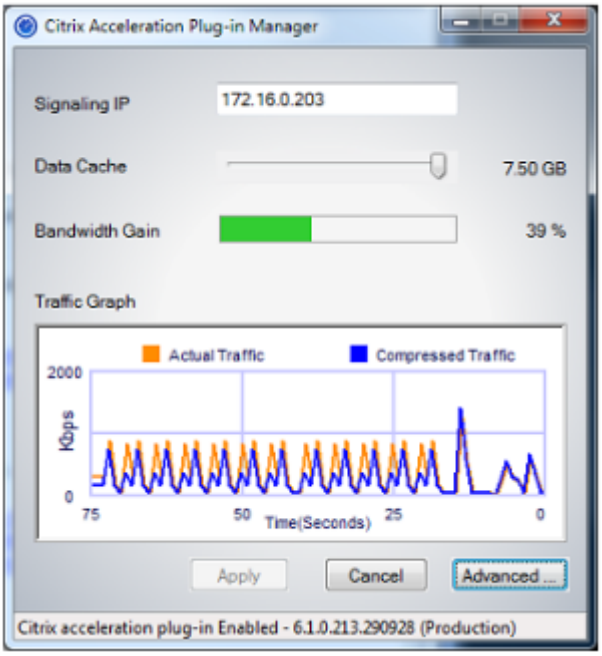
3. 安装程序完成后，它可能会要求您重新启动系统。重新启动后，WANOP 客户端插件插件将自动启动。

图 **2.** 最终安装屏幕



4. 右键单击任务栏中的加速器图标，然后选择 管理加速 以启动 Citrix 插件加速器管理器。

图 **3. Citrix** 加速器插入管理器，初始（基本）显示



5. 如果尚未为用户自定义.MSI 文件，请指定信令地址和用于压缩的磁盘空间量：

   - 在设备：信令地址字段中，键入设备的信令 IP 地址。如果您有多个启用了插件的设备，请将它们全部列出，并以逗号分隔。IP 地址或 DNS 地址均可接受。
   - 使用“数据缓存”滑块，选择用于压缩的磁盘空间量。更多更好。7.5 GB 是不是太多，如果你有那么多的磁盘空间可用。
   - 按“应用”。

     WANOP 客户端插件加速器现在正在运行。未来与加速子网的所有连接都将加速

     在插件的“高级规则”选项卡上，“加速规则”列表应将每个设备显示为“已连接”，并将每个设备的加速子网显示为“已加速”。如果没有，请检查信令地址 IP 字段和一般网络连接。

插件故障排除

插件安装通常顺利。如果没有，请检查以下问题：

常见问题：

- 如果您不重新启动系统，WANOP 客户端插件将无法正常运行。
- 如果磁盘碎片过多，会导致压缩性能低下。
- 加速失败（诊断 选项卡上未列出加速连接）通常表示某些事情阻止了与设备的通信。检查插件上的 配置：加速规则 列表，以确保已成功联系设备，并且目标地址包含在其中一个加速规则中。连接故障的典型原因包括：
  - 设备未运行，或者加速已禁用。

- 防火墙正在剥离插件和设备之间的某个时候剥离 WANOP 客户端插件 TCP 选项。
- 该插件正在使用不受支持的 VPN。

确定性网络增强器锁定错误

在极少数情况下，安装插件并重新启动计算机后，将出现两次以下错误消息：

确定性的网络增强器安装需要首先重新启动，以释放锁定的资源。请在重新启动计算机后再次运行此安装。

如果发生上述情况，请执行以下操作：

1. 转到 添加/删除程序 并删除 WANOP 客户端插件（如果存在）。
2. 转到 控制面板 > 网络适配器 > 局域连接 > 属性，找到确定性网络增强器的条目，清除其复选框，然后单 击 确定。（您的网络适配器可能由“本地连接”以外的名称调用。）
3. 打开命令窗口并转到 c:windowsinf（或者如果您在非标准位置安装了 Windows，则该等效目录）。
4. 键入以下命令：

   find “dne2000.cat” oem*.inf
5. 找到返回匹配行的 highest-numbered oem*.inf 文件（匹配行是为 CatalogFile= dne2000.cat）并对其进行编辑。例如：

   notepad oem13.inf
6. 删除除顶部以分号开头的三行之外的所有内容，然后保存文件。这将清除任何不适当或过时的设置，下次安装将使用默认值。
7. 重试安装。

其他安装问题

安装 WANOP 客户端插件时出现的任何问题通常都是由于现有网络、防火墙或防病毒软件干扰安装。通常，一旦安装完成，就没有进一步的问题。

如果安装失败，请尝试以下步骤：

1. 确保插件安装文件已复制到本地系统。
2. 断开任何活动的 VPN/远程网络客户端。
3. 暂时禁用任何防火墙和防病毒软件。
4. 如果其中一些是困难的，做你可以。
5. 重新安装 WANOP 客户端插件。
6. 如果这不起作用，请重新启动系统并重试。

WANOP 插件 GUI 命令

June 22, 2021

右键单击 **Citrix** 加速器插件图标并选择 管理 加速时，将显示 WANOP 客户端插件 GUI。首先显示 GUI 的基本显示。还有一个高级显示器，可以根据需要使用。

基本显示器

在“基本”页面上，您可以设置两个参数：

- “信令地址”字段指定插件可连接到的每个设备的 IP 地址。Citrix 建议仅列出一个设备，但您可以创建逗号分隔的列表。这是一个有序列表，最左侧的设备优先于其他设备。尝试使用可以建立信号连接的最左侧设备加速。您可以同时使用 DNS 地址和 IP 地址。

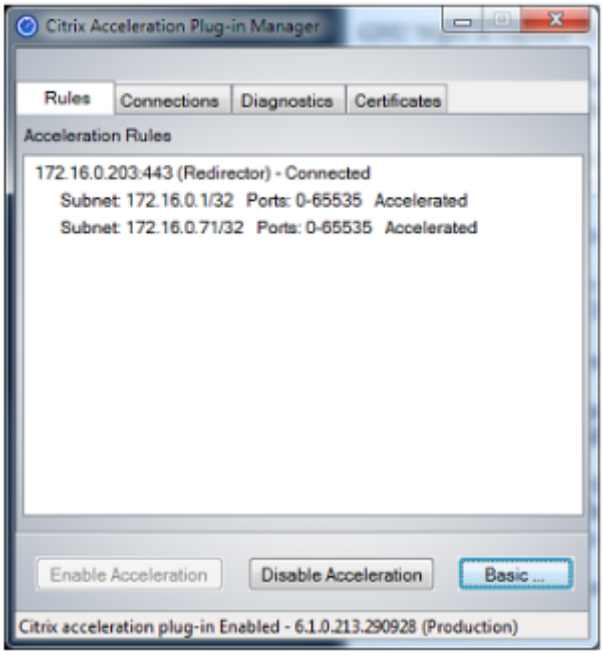
  示例：10.200.33.200、ws.mycompany.com、ws2.mycompany.com

- “数据缓存”滑块可调整分配给插件基于磁盘的压缩历史记录的磁盘空间量。更多更好。

  此外，还有一个按钮移动到高级显示屏。

高级显示器

“高级”页面包含四个选项卡：规则、连接、诊断和证书。



显示屏底部有按钮，用于启用加速、禁用加速和返回到基本页面。

规则选项卡

“规则”选项卡显示从设备下载的加速规则的缩写列表。每个列表项显示设备的信令地址和端口、加速模式（重定向器或透明）和连接状态，后面是设备规则摘要。

连接选项卡

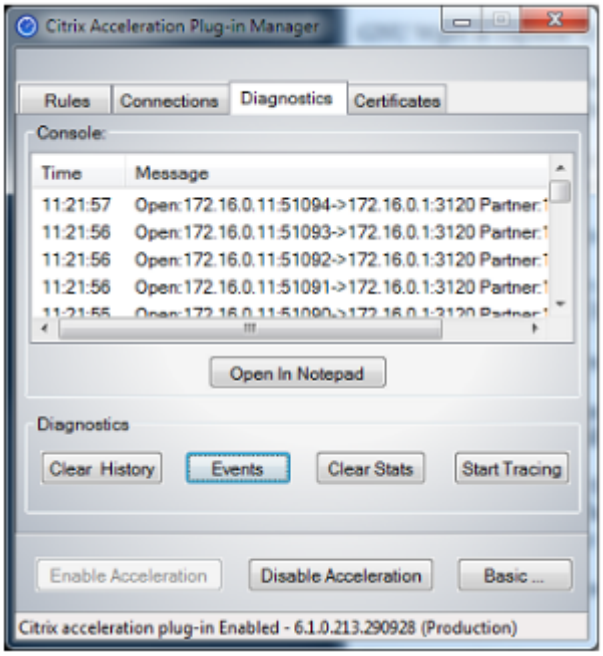
连接 选项卡列出了不同类型的打开连接的数量：

- 加速连接—WANOP 客户端插件插件与设备之间的打开连接数。此数字包括每个设备的一个信令连接，但不包括加速 CIFS 连接。单击“更多”将打开一个窗口，其中包含每个连接的简要摘要。（所有“更多”按钮允许您将窗口中的信息复制到剪贴板，如果您想与支持部门共享。）
- 加速 **CIFS** 连接—与 CIFS（Windows 文件系统）服务器的打开、加速连接的数量。这通常与挂载的网络文件系统的数量相同。单击“更多”将显示与加速连接相同的信息，以及在使用 WANOP 客户端插件的特殊 CIFS 优化运行 CIFS 连接时报告活动状态字段。
- 加速的 **MAPI** 连接 - 打开的加速 Outlook/Exchange 连接的数量。
- 加速 **ICA** 连接-使用 ICA 或 CGP 协议的打开、加速的 XenApp 和 XenDesktop 连接的数量。
- 未加速连接—打开未加速的连接。您可以单击“更多”以显示连接未加速的简要说明。通常情况下，原因是没有任何设备会加速目标地址，该地址作为服务策略规则报告。
- 打开**/**关闭连接—未完全打开但正在打开或关闭的连接（TCP “半打开”或“半关闭”连接）。“更多”按钮显示有关这些连接的一些附加信息。

诊断选项卡

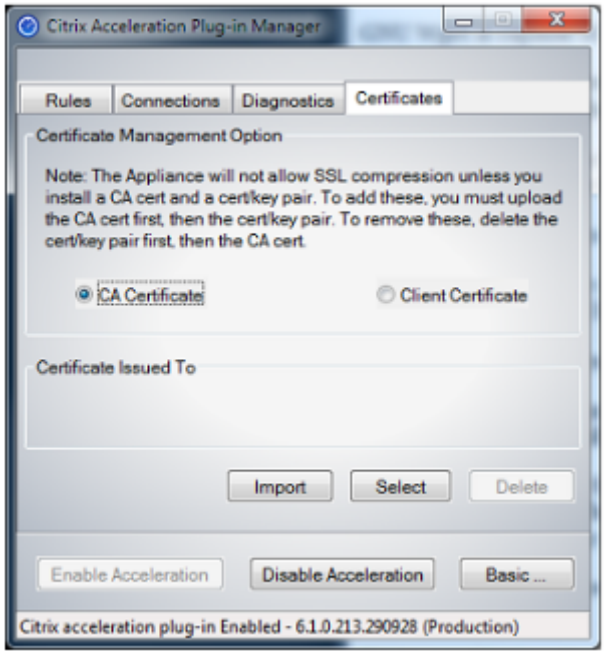
“诊断”页面报告不同类别中的连接数以及其他有用信息。

- 开始跟踪**/**停止跟踪—如果您报告问题，Citrix 代表可能会要求您执行连接跟踪以帮助确定问题。此按钮启动和停止追踪。停止跟踪时，弹出窗口会显示跟踪文件。按照您的 Citrix 代表推荐的方式将其发送给他或她。
- 清除历史记录-不应使用此功能。
- 清除统计信息—按此按钮可清除“性能”选项卡上的统计信息。
- 控制台-带有最近状态消息的可滚动窗口，主要是连接打开和连接关闭消息，但也有错误消息和其他状态消息。



证书选项卡

在“证书”选项卡上，您可以为可选的安全对等功能安装安全凭据。这些安全证书的目的是使设备能够验证插件是否是受信任的客户端。



要上载 CA 证书和证书密钥对，请执行以下操作：

1. 选择 CA 证书管理。

2. 单击导入。
3. 上载 CA 证书。证书文件必须使用支持的文件类型之一（.pem、.crt、.cer 或.spc）。可能会出现一个对话框，要求您选择要使用的证书存储区并向您显示关键字列表。选择列表中的第一个关键字。
4. 选择 客户端证书管理。
5. 单击导入。
6. 选择证书密钥对的格式（PKCS12 或 PEM/DER）。
7. 单击 **Submit**（提交）。

> 注意
>
> 对于 PEM/DER，证书和密钥有单独的上载框。如果您的证书密钥对合并在一个文件中，请为每个框指定两次文件。

更新 **WANOP** 插件

June 22, 2021

要安装更新版本的 WANOP 客户端插件，请按照首次安装插件时使用的相同步骤操作。

卸载 **WANOP** 客户端插件

若要卸载 WANOP 客户端插件，请使用 Windows 添加/删除程序实用程序。WANOP 客户端插件在当前安装的程序列表中列为 **Citrix** 加速插件。选择它并单击 删除。

您必须重新启动系统才能完成卸载客户端。

对 **WANOP** 插件进行故障排除

June 22, 2021

- 问题：我面临信号通道连接问题。如何解决这些问题？

  解决方法：要解决信令通道连接问题，请执行以下故障排除步骤：

  - 验证您是否已正确配置信令 IP 地址。您可以通过 ping 信令 IP 地址并验证响应来执行此操作。
  - 验证 WANOP 设备上是否启用了信号状态。
  - 验证网络上安装的防火墙不会删除 WANOP TCP 选项。

  - 验证 WANOP 设备上是否安装了有效的 WANOP 插件许可证。
  - 验证信令通道源筛选配置不阻止客户端源 IP 地址。
  - 如果您已启用 LAN 检测，请验证 WANOP 插件和 WANOP 设备之间的往返时间是否为可接受的值。

- 问题：在 WANOP 4000 设备上，我无法禁用 WANOP 插件。

  原因：这是一个已知的问题。

  决议：无。您不能禁用 WANOP 4000 设备上的 WANOP 插件。

- 问题：使用 WANOP 插件连接到 WANOP 设备时，“警报”选项卡上会记录以下错误消息条目：

  <Number> 尝试连接到此设备的 WANOP 插件超过当前限制。

  原因：与 WANOP 设备的连接数已超过许可用户限制。

  解决方法：等待用户断开连接或终止连接。

- 问题：在 WANOP 4000 或 5000 设备上配置了错误的信令 IP 地址。

  解决方法：要更新 WANOP 4000 或 5000 设备上的信令 IP 地址，请完成以下步骤：

  1. 登录到 WANOP 设备的 NetScaler 实例。
  2. 导航到流量管理 > 负载平衡 > 虚拟服务器 > BR_LB_VIP_SIG 页面。
  3. 更新信令 IP 地址。
  4. 保存配置。

- 问题：CIFS 和 ICA 流量没有加速。

  解决方法：要解决此问题，请执行以下故障排除步骤：

  - 验证是否为 WANOP 插件正确定义了 IP 地址和端口号的加速规则。
  - 验证是否在信令连接成功后建立了 CIFS 或 ICA 连接。
  - 验证正在使用的服务类的加速策略。

SMB 3.1.1 连接

June 22, 2021

服务器消息块 (SMB) 协议是一种网络文件共享协议。定义协议特定版本的消息数据包称为方言。通用互联网文件系统 (CIFS) 协议是中小型企业的一种方言。

在 Citrix SD-WAN 版本 10 版本 1 中，在 Citrix SD-WAN WANOP 和 Premium Edition 平台上引入了 SMB 3.1.1 协议。

Citrix SD-WAN ANOP 支持 SMB 3.1.1 连接。当客户端是 Windows 10 和服务器是 Windows 服务器 2016 年时，SMB 3.1.1 连接适用。

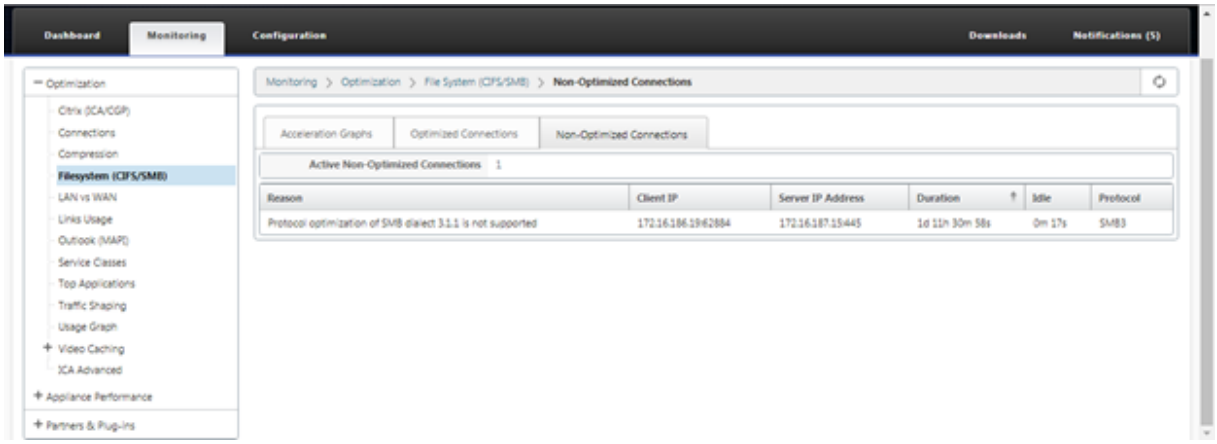
当 SMB 3.1.1 流量通过 WANOP 模块时：

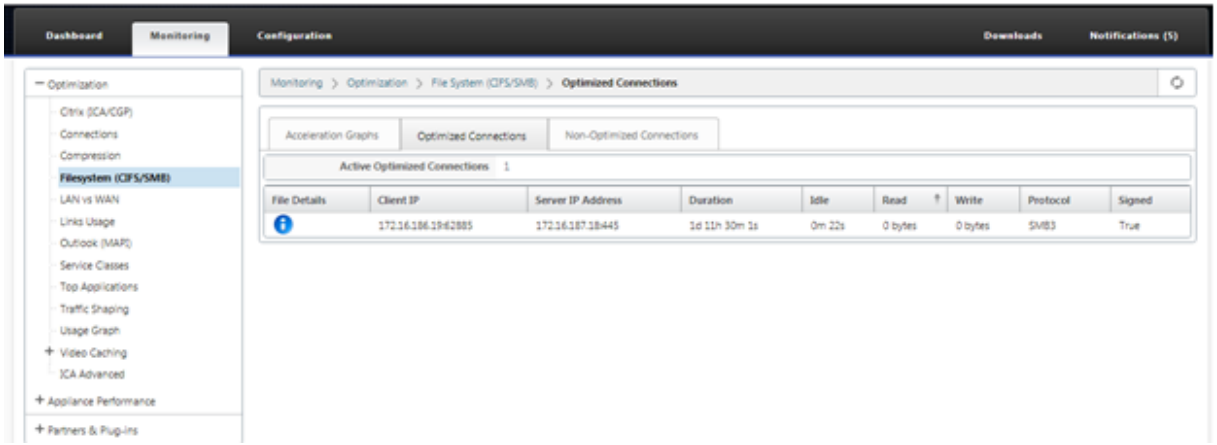
- 它被计数/可见作为 SMB 3.1 CIFS 未优化连接的一部分
- 将显示以下跟踪消息：“不支持 SMB 3.1.1 通过此连接”。

客户端	服务器	SMB 版本
Windows 10	Win 2016、2012R2	SMB 3.1.1、3.0.2
Windows 8.1	SMB 3.0	SMB 3.0
Windows 7	SMB 3.0	SMB 3.0

对于未优化的连接，Citrix SD-WAN WANOP 设备 GUI 将显示 SMB 3.1.1 的消息。

在 Citrix SD-WAN WANOP 设备 GUI 中，导航到 监视 > 文件系统 **(CIFS/SMB)**。单击 未优化的连接 选项卡，将显示以下消息，不支持 *SMB 方言 3.1.1* 的协议优化。没有可用的日志条目，SD-WAN WANOP 中不需要新的配置来支持这一点。





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 隧道
- 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
- 安全对等和手动安全对等
- 零接触部署
- 双盒模式部署

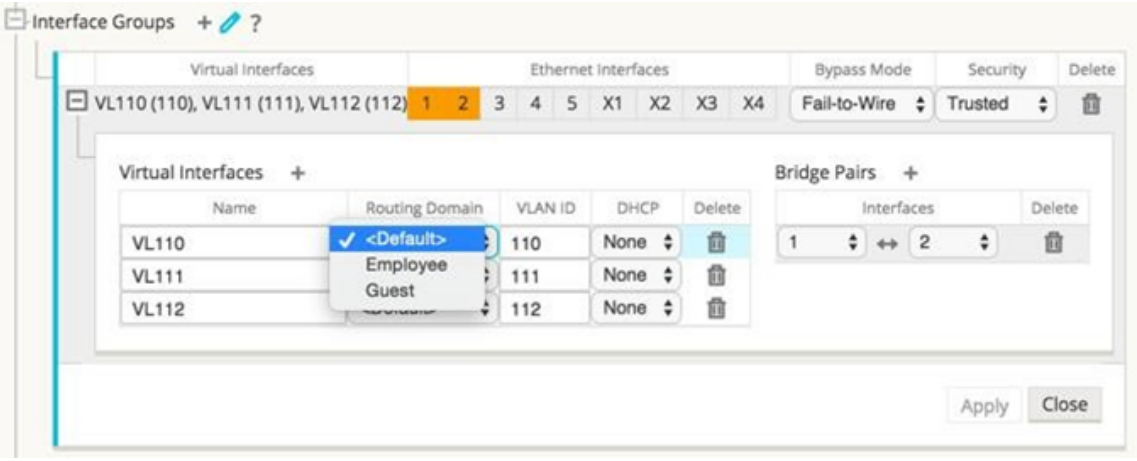
接口组

June 22, 2021

要配置接口组，请执行以下操作：

1. 在 配置编辑器中，导航到 站点 > [客户端站点名称]> 接 口组，在配置虚拟接口时从下拉菜单中选择 路由域。有关详细说明，请参阅 配置接口组。

   > 注意
   >
   > 虚拟接口与特定路由域关联后，使用该路由域时只有这些接口才可用。



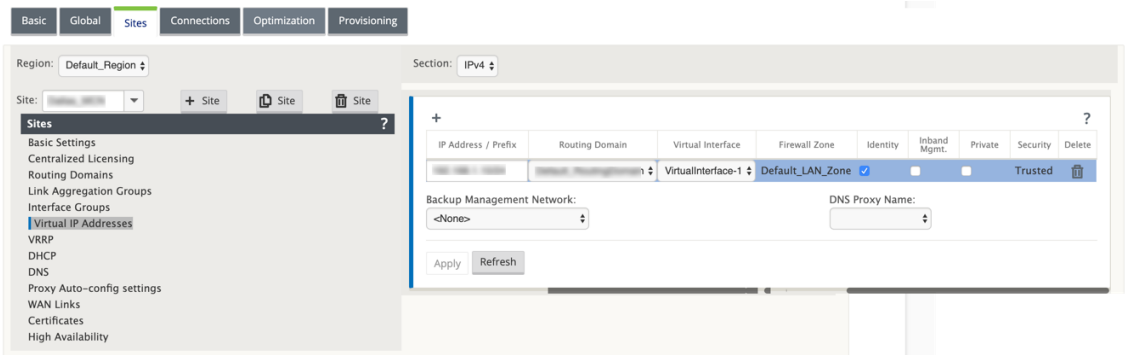
配置虚拟 IP 地址标识

June 22, 2021

虚拟网络接口可以托管相同或不同子网中的多个 IP 地址。但是，您只能选择一个标识设置为 true 的虚拟 IP，该虚拟 IP 可用于动态路由协议，如 BGP/OSPF、DHCP 服务器/中继和带内管理。

要配置虚拟 IP 地址标识，请执行以下操作：

1. 在 配置编辑器中，导航到 站点 > [站点名称] > 虚拟 **IP** 地址。
2. 单击虚拟 IP 地址的 身份 复选框以将其用于 IP 服务。



配置访问接口

September 26, 2023

要配置访问接口，请执行以下操作：

1. 在 配置编辑器中，导航到 站点 > **[**客户端站点名称**]** > **WAN** 链 接 > **[WAN** 链接名称**]** > 访问接口。
2. 配置访问接口时，从下拉菜单中选择 路由域。

   有关详细说明，请参阅 配置 MCN 主题中 的如何配置访问接口 部分。

配置虚拟 **IP** 地址

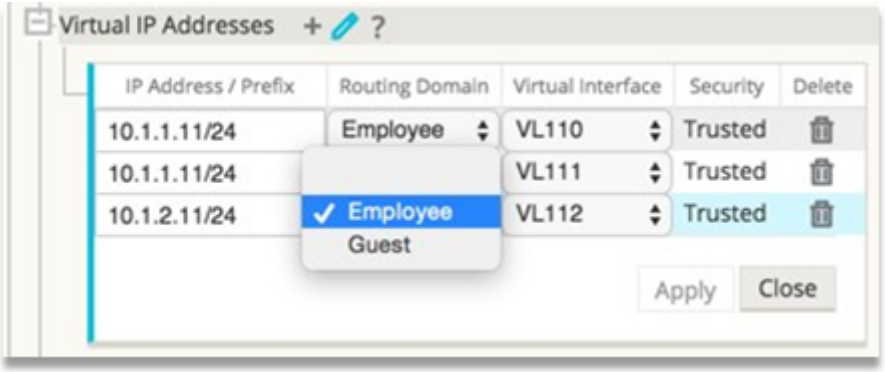
June 22, 2021

要配置虚拟 IP 地址，请执行以下操作：

1. 在 配置编辑器中，导航到 站点 **>** **[**客户端站点名称**]** **>** 虚拟 **IP** 地址。
2. 配置虚拟 IP 地址时，从下拉菜单中选择 路由域。

   有关详细说明，请参阅 配置虚拟 IP 地址。

您选择的路由域决定从下拉菜单中可用哪些虚拟接口。



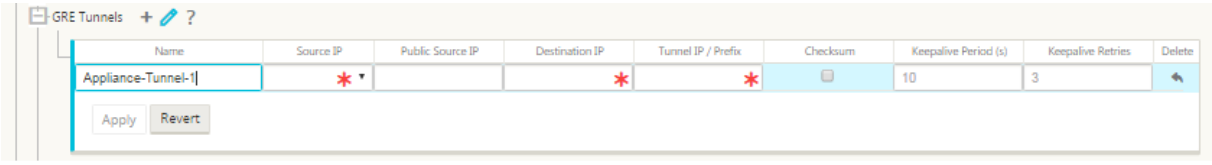
配置 GRE 隧道

June 22, 2021

要配置 GRE 隧道：

1. 在配置编辑器中，导航到 连接 > 站点 > **GRE** 隧道。只能从受信任链接上的虚拟网络接口中选择源 IP 地址。
2. 输入 GRE 隧道的名称.
3. 从下拉菜单中选择可用的 源 **IP** 地址。路由域从下拉菜单中确定哪些源 IP 地址可用。
4. （可选）选择 公共源 **IP**。如果此地址与源 IP 相同，则此字段可以为空。
5. 输入 GRE 隧道的 目标 **IP** 地 址。
6. 输入 GRE 隧道的隧道 **IP/**前缀 地址。
7. 单击 校验和，如果要在 GRE 隧道标题中使用校验和。
8. 为 保持活动期间 输入一个值（以秒为单位）。如果配置 0，则不会传输保持活动状态数据包，但 GRE 隧道将处于活动状态。
9. 为 保持活动重试 输入一个值。此值确定在 SD-WAN 设备停用 GRE 隧道之前尝试保持活动状态重试的次数。

有关详细信息，请参阅 MCN 网站上的配置 GRE 隧道。



有关使用 GRE 隧道保护 Web 网关的更多信息，请参阅Secure Web Gateway。

设置分支到分支通信的动态路径

June 22, 2021

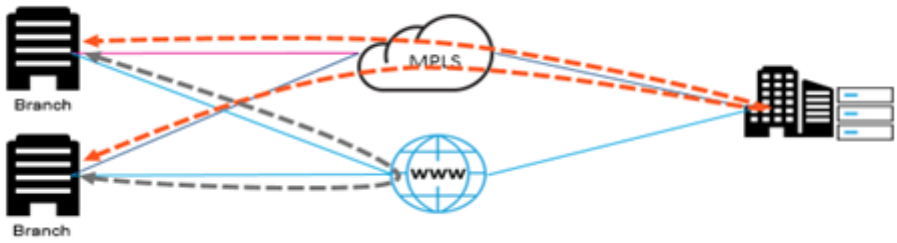
随着对 VoIP 和视频会议的需求，办公室之间的流量越来越多。通过数据中心设置完整的网状连接效率低下，这可能会很耗时。

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。

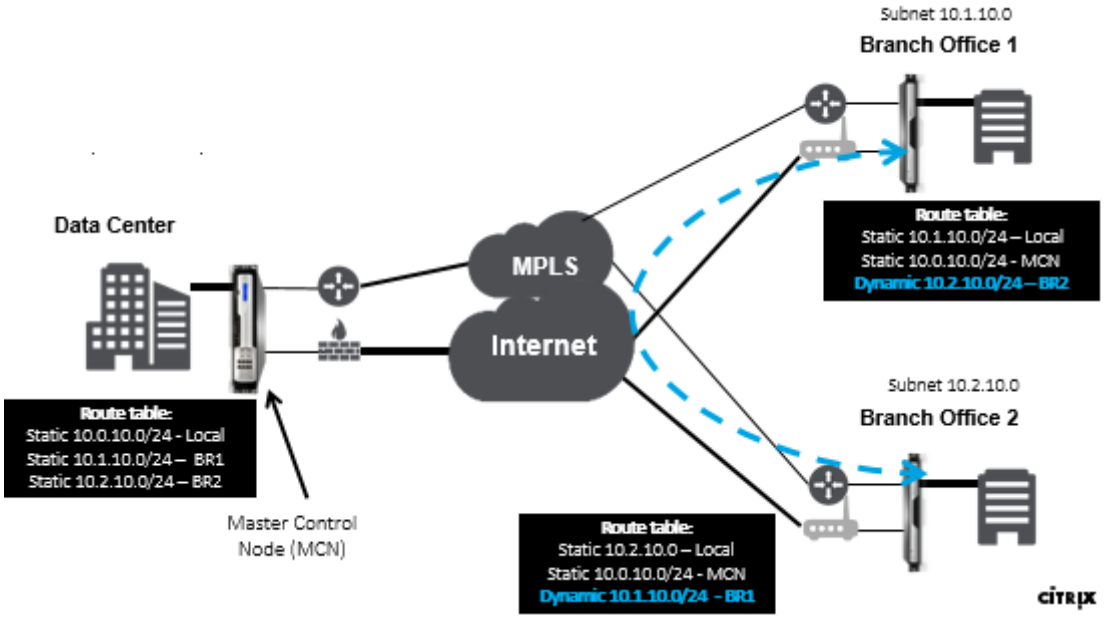
SD-WAN 网络的其他优势包括：

- 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：

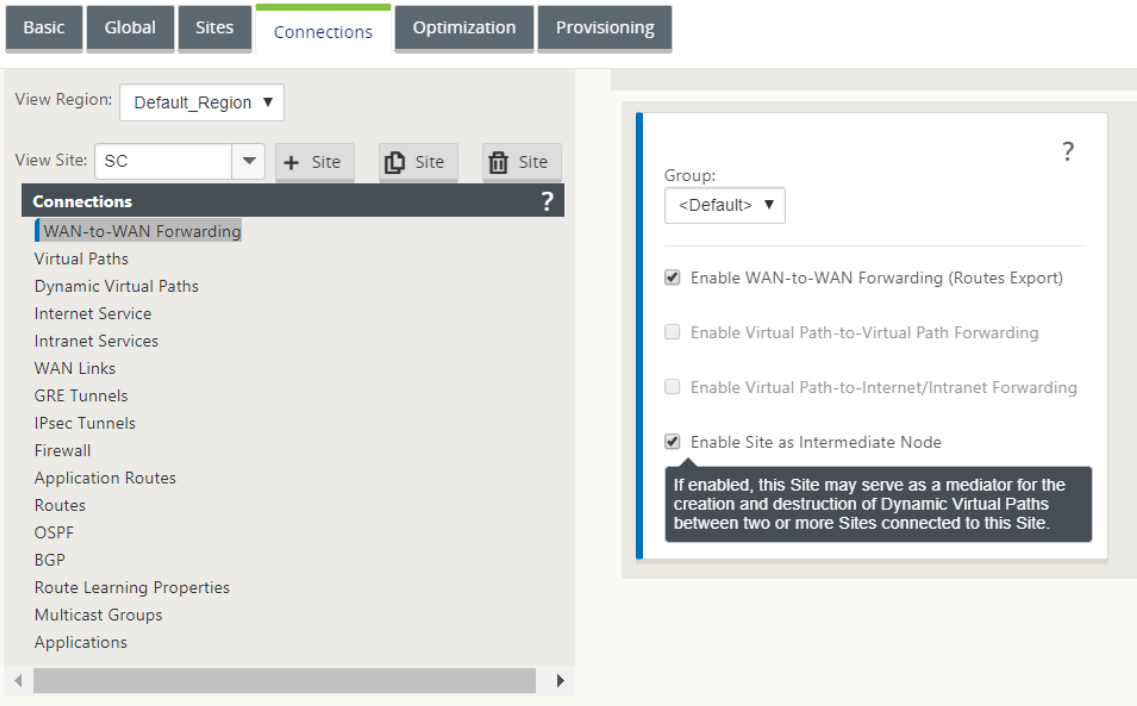


- 动态虚拟路径用于大规模部署，例如企业
- 较小的部署使用静态虚拟路径和任何到任何虚拟路径
- 始终使用两个数据中心（DC 到 DC）之间的静态虚拟路径
- 并非所有 WAN 路径都需要配置为使用动态虚拟路径
- 每个 SD-WAN 设备都具有可配置的动态虚拟路径数量有限（8 个动态最低限值，8 个静态最低限值 = 共 16 个）。

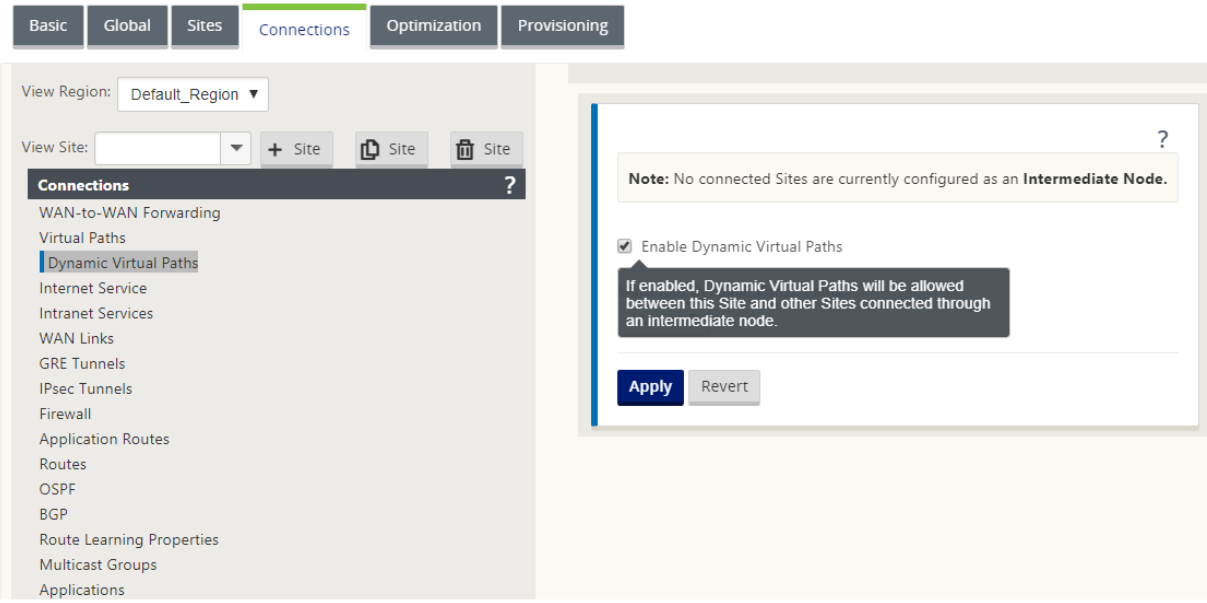
如何在 **SD-WAN GUI** 中启用动态虚拟路径

要启用动态虚拟路径，请执行以下操作：

1. 在 Citrix SD-WAN GUI 中的 连接 窗格下，创建一个 WAN 到 WAN 转发组。
2. 导航到 连接 **>** [客户端站点名称] **> WAN** 到 **WAN** 转发。
3. 启用 **WAN** 到 **WAN** 转发 以使站点能够充当多跳站点到站点的代理。
4. 启用 站点作为中间节点
5. 导航到 连接 **>** 远程站点 **> WAN** 到 **WAN** 转发。
6. 启用 WAN 到 WAN 转发，以使站点能够作为多跃点站点到站点的代理。

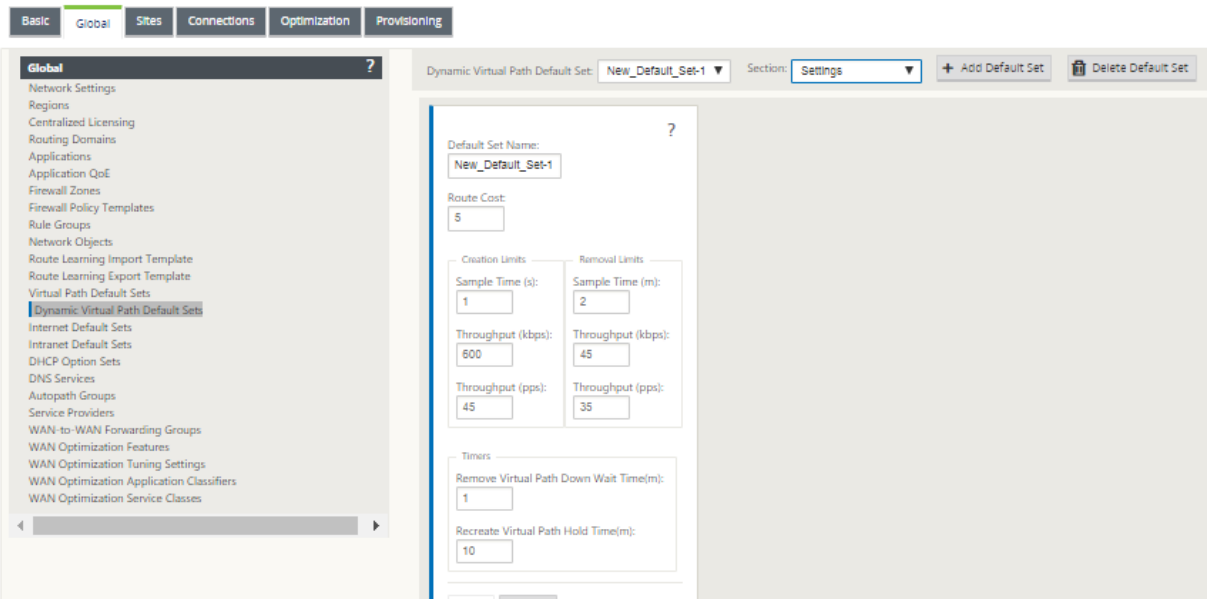


7. 导航到 连接 **>** 远程站点 **>** 虚拟路径 **>** 动态虚拟路径。
8. 启用 动态虚拟路径。
9. 设置动态路径的最大数量。



如何创建动态虚拟路径

- 配置确定动态虚拟路径何时处于活动状态或关闭状态。
- 在时间范围内配置样本数据包计数 (pps) 或带宽 (kbps)。
- 可以在全局设置，也可以在中间节点上配置 WAN 链接。



监视和故障排除

June 22, 2021

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

June 22, 2021

查看设备的基本信息

使用浏览器连接到要监视的设备的管理 Web 界面，然后单击 控制板 选项卡以显示该设备的基本信息。

控制板 页面显示本地设备的以下基本信息：

系统状态：

- 名称—这是您在将设备添加到系统时分配给设备的名称。
- 模型—这是虚拟 WAN 设备型号。
- 设备模式—指示此设备是否已配置为主 MCN 或辅助 MCN，还是客户端设备。
- 管理 **IP** 地址—这是设备的管理 IP 地址。
- 设备正常运行时间—指定自上次重新启动以来设备运行的持续时间。

- 服务正常运行时间—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。

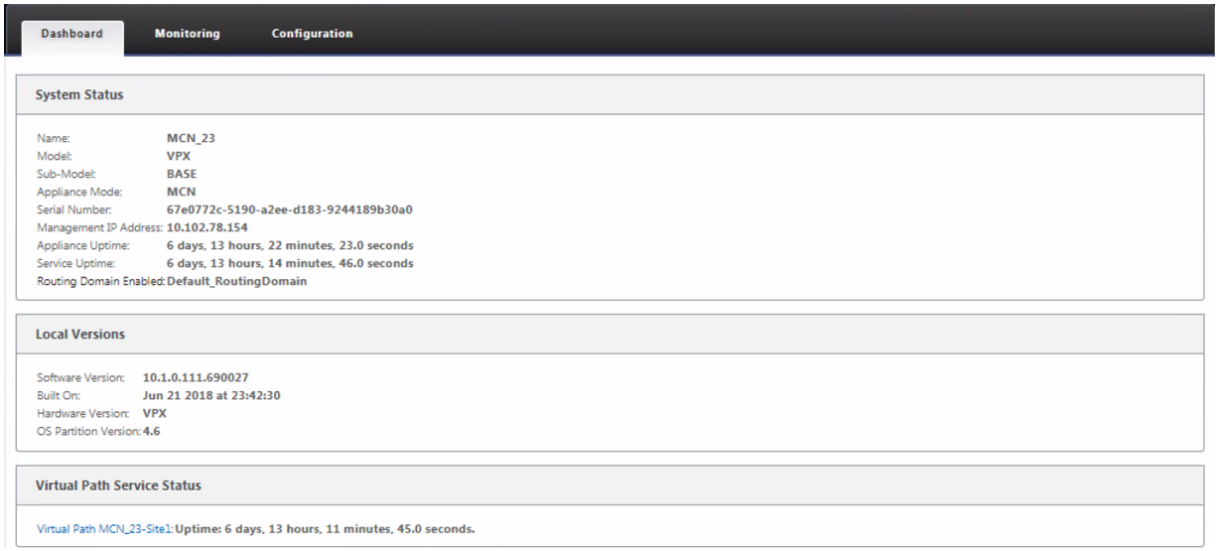
虚拟路径服务状态：

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—这是当前在设备上激活的 CloudBridge 虚拟路径软件包的版本。
- 基于 生成—这是当前在本地设备上运行的产品版本的生成日期。
- 硬件版本—这是设备的硬件型号和版本。
- **OS** 分区版本—这是设备上当前处于活动状态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

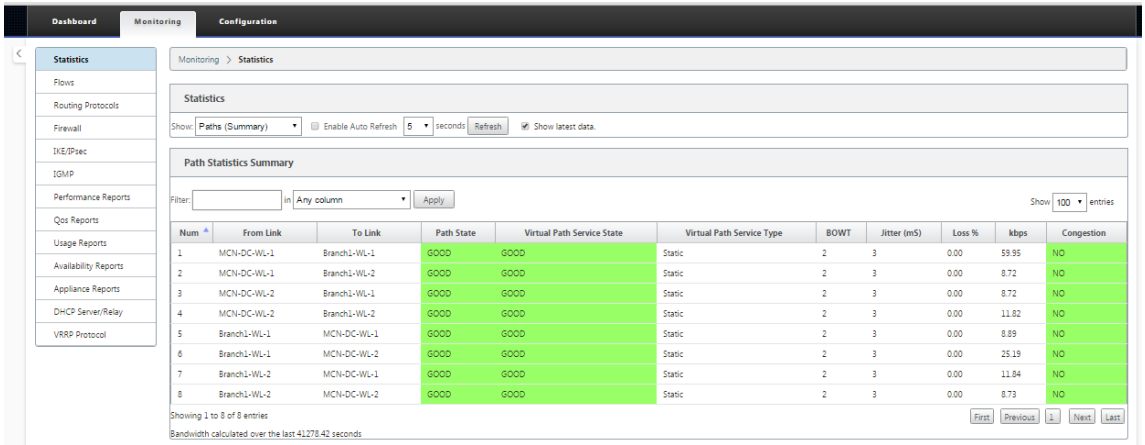
June 22, 2021

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。

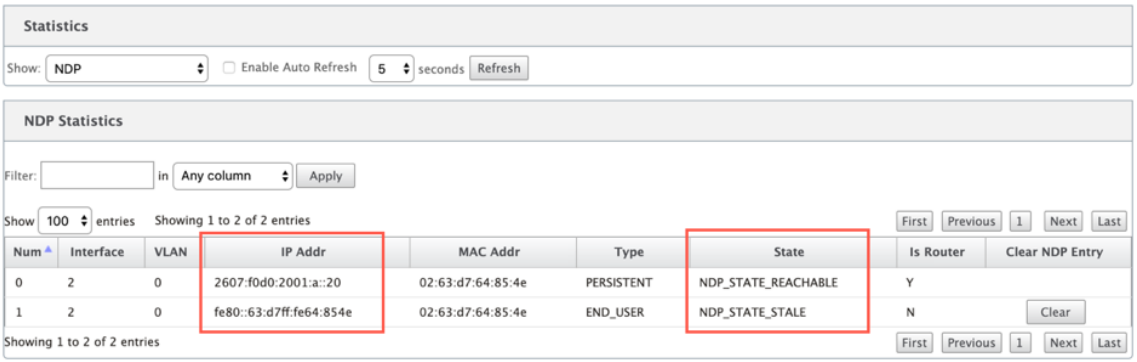
   这将在左窗格中打开 监视 导航树。默认情况下，此操作还会显示 显 示 字段中预先选择的 路径 的 统计信息 页面。这包含路径统计信息的详细表。

> 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。

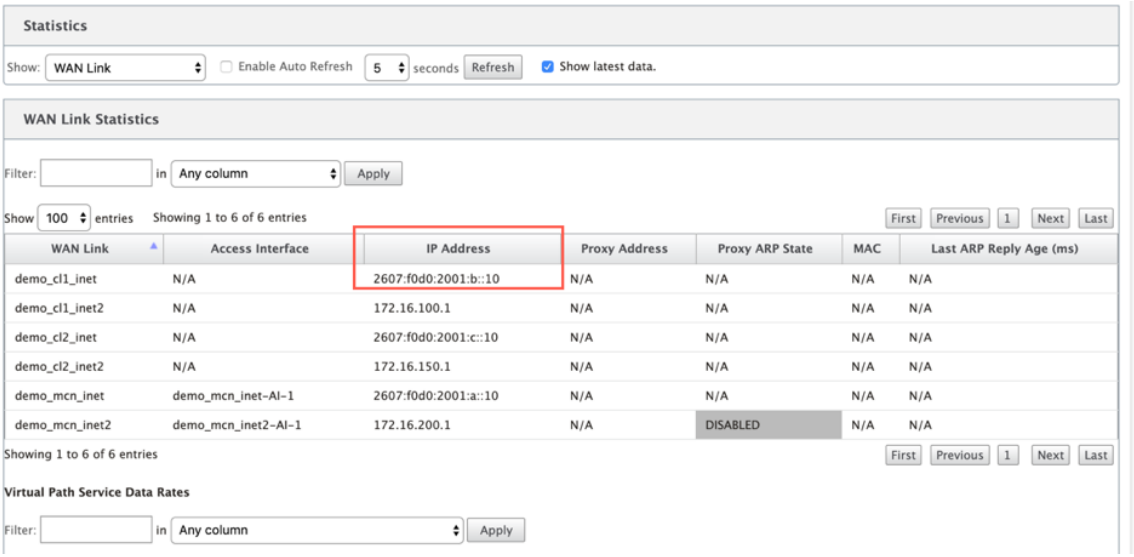


在 11.1.0 版本中，添加了邻居发现协议 (NDP) 选项以调试邻居发现问题。

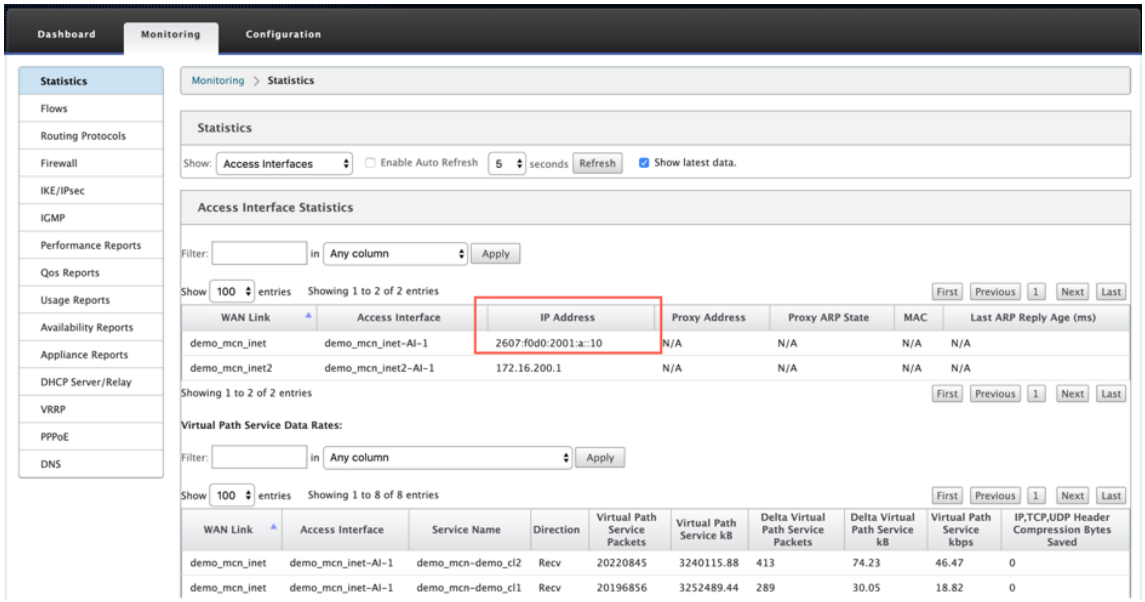
1. 从“显示”下拉菜单中选择“NDP”选项，您可以查看 NDP 的状态以及 IPv6 地址。



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。

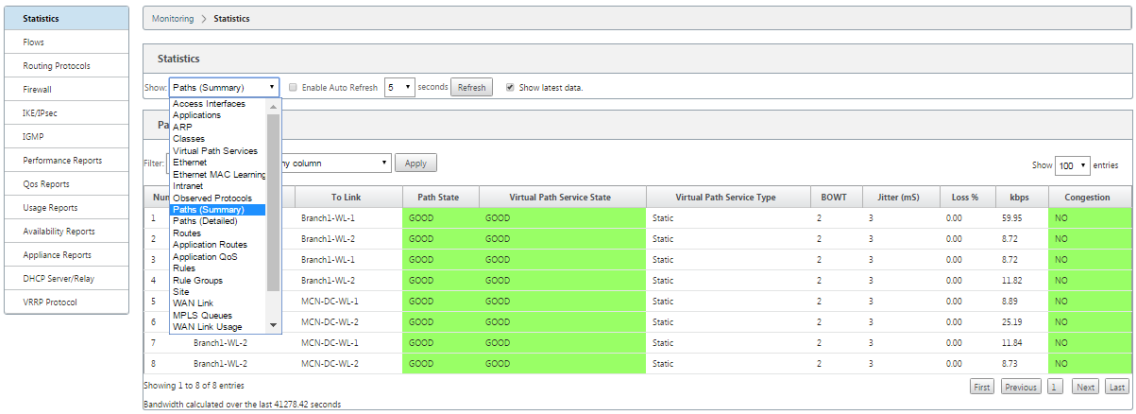


3. 您还可以查看接入接口统计信息。



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。

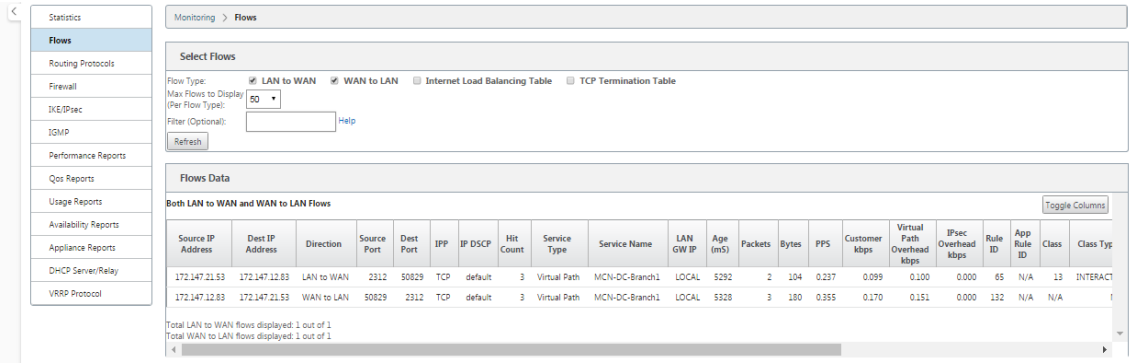
查看流信息

February 10, 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：

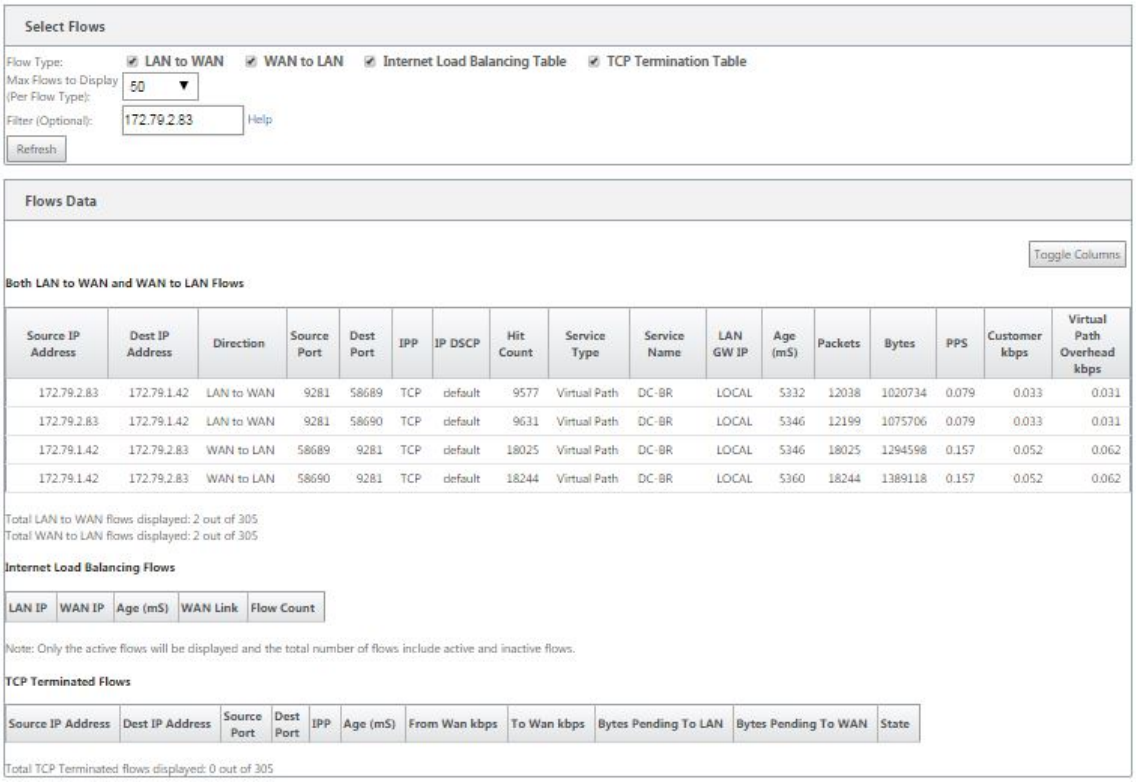
1. 登录到 MCN 的管理 Web 界面，然后选择 监视 选项卡。它会在左侧窗格中打开“监控”导航树。
2. 在导航树中选择 流量 分支。它显示流量页面，其中包含在流程类型字段中预先选择了 **LAN** 到 **WAN**。



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”。

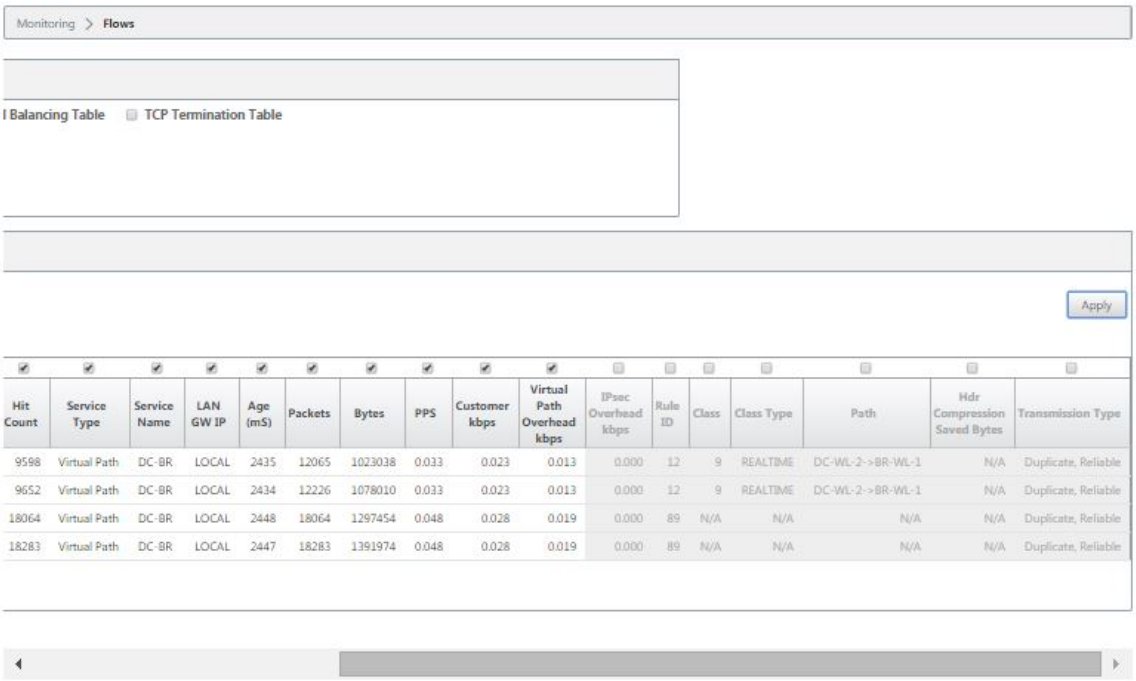
7. 单击刷新以显示筛选结果。图中显示了一个已过滤的流量页面示例，其中选择了所有流程类型。



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。



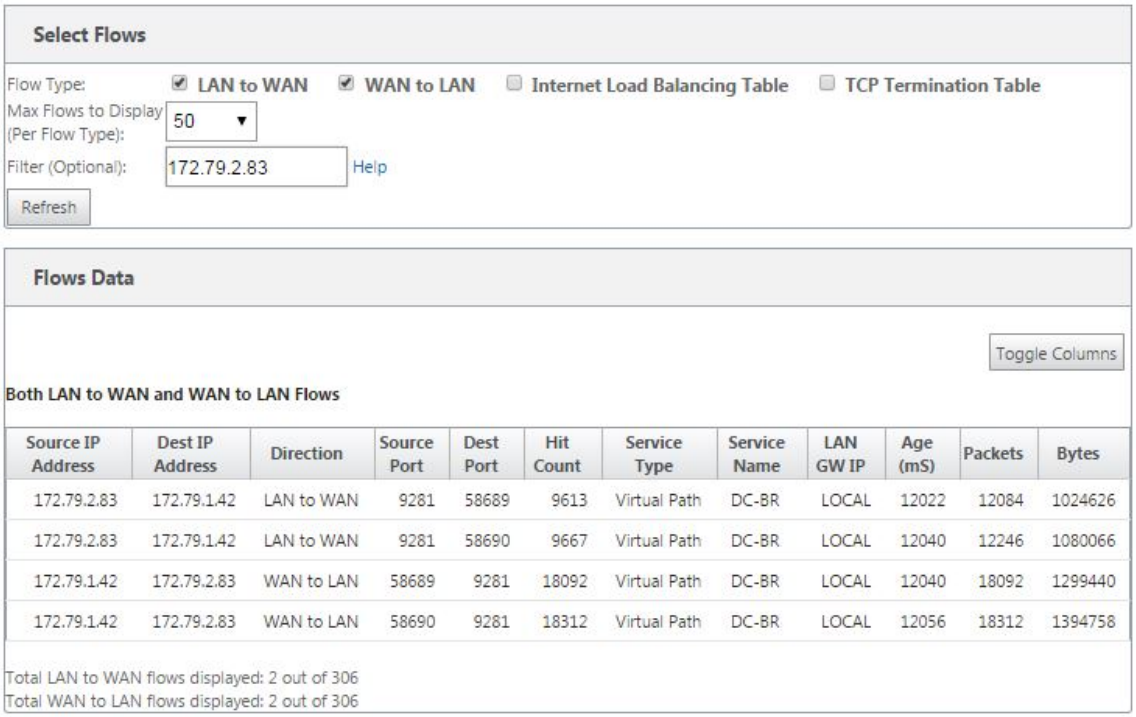
Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
9598	Virtual Path	DC-BR	LOCAL	2435	12065	1023038	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
9652	Virtual Path	DC-BR	LOCAL	2434	12226	1078010	0.033	0.023	0.013	0.000	12	9	REALTIME	DC-WL-2->BR-WL-1	N/A	Duplicate, Reliable
18064	Virtual Path	DC-BR	LOCAL	2448	18064	1297454	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable
18283	Virtual Path	DC-BR	LOCAL	2447	18283	1391974	0.048	0.028	0.019	0.000	89	N/A	N/A	N/A	N/A	Duplicate, Reliable

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

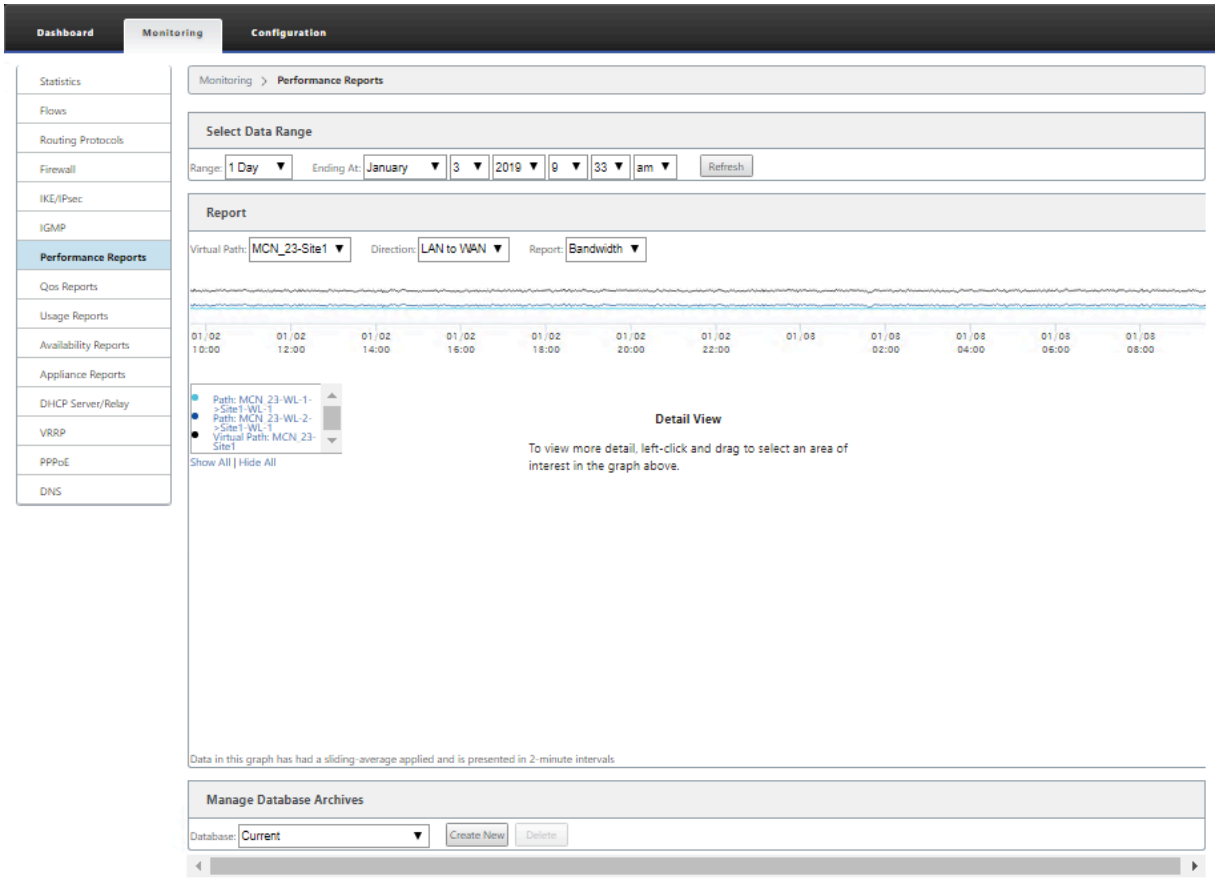
在 早期版本中，可以识别约 4,000 个应用程序，并配置为 800 个服务（550 个虚拟路径、256 个内联网服务）。存储此数据会影响整体系统性能（存储数据所需的 CPU 周期和磁盘空间）。如果支持按使用量或路径报告数据，它也会产生影响。

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

June 22, 2021

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。

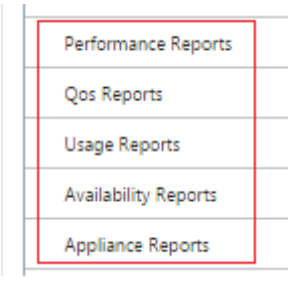
要生成和查看虚拟 WAN 报表，请执行以下操作：

1. 登录到 MCN 的管理 Web 界面，然后选择 监视 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：

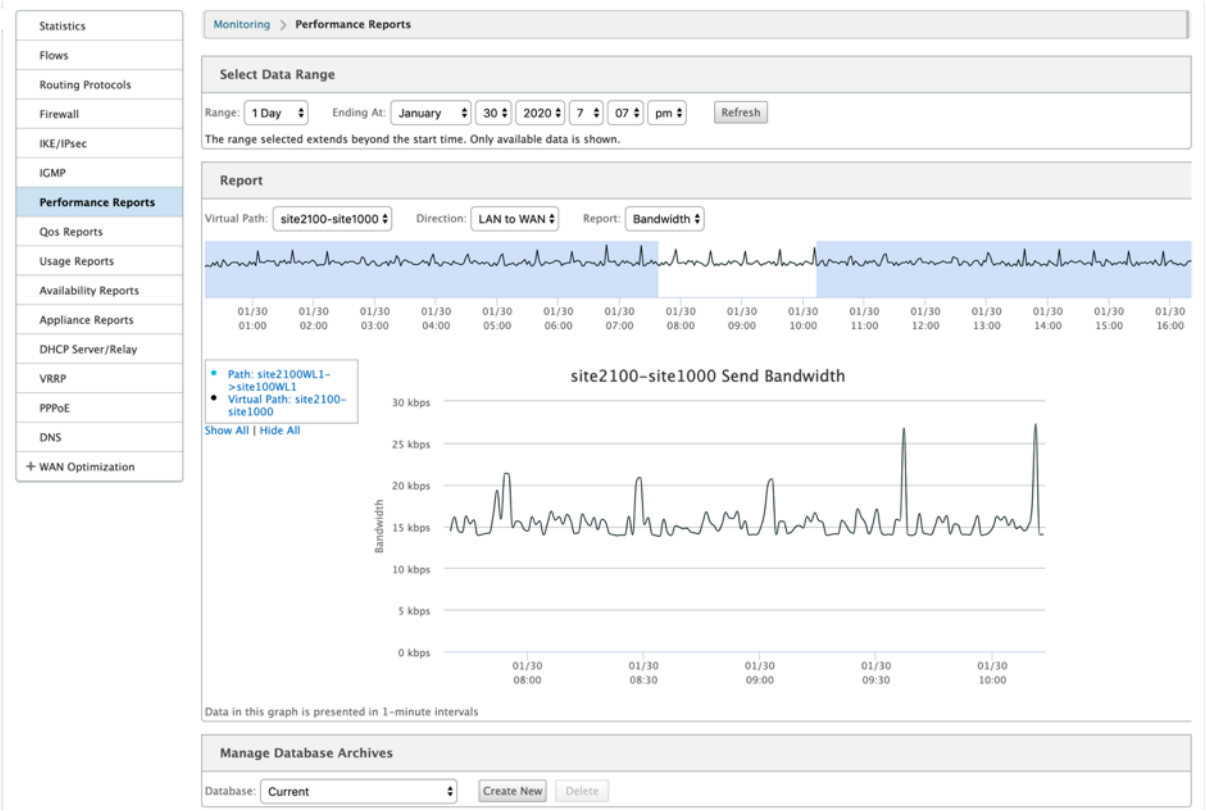
- 绩效报告
- **QoS** 报告
- 使用情况报告
- 可用性报告
- 设备报告

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。



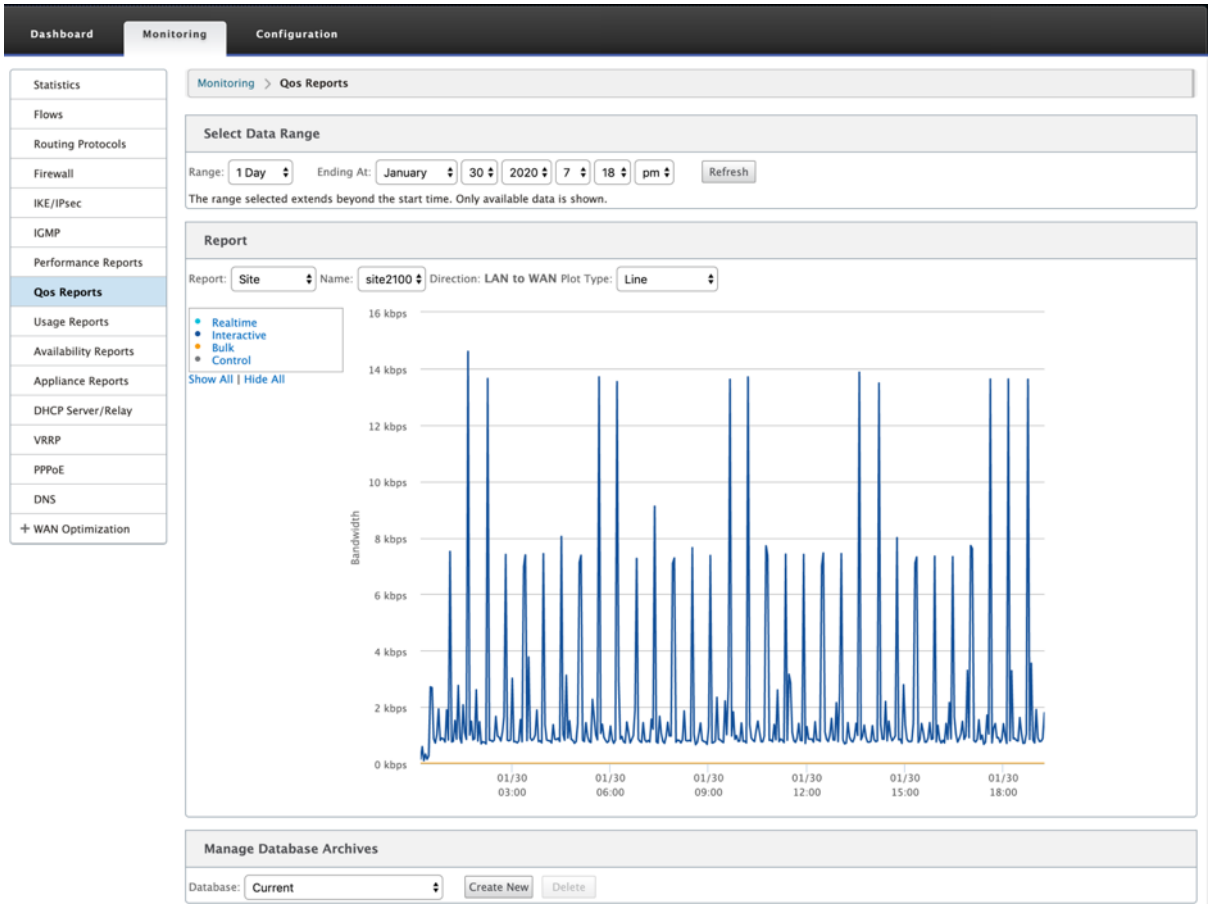
您可以根据需要使用以下字段选择数据范围以查看性能报告：

- 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。



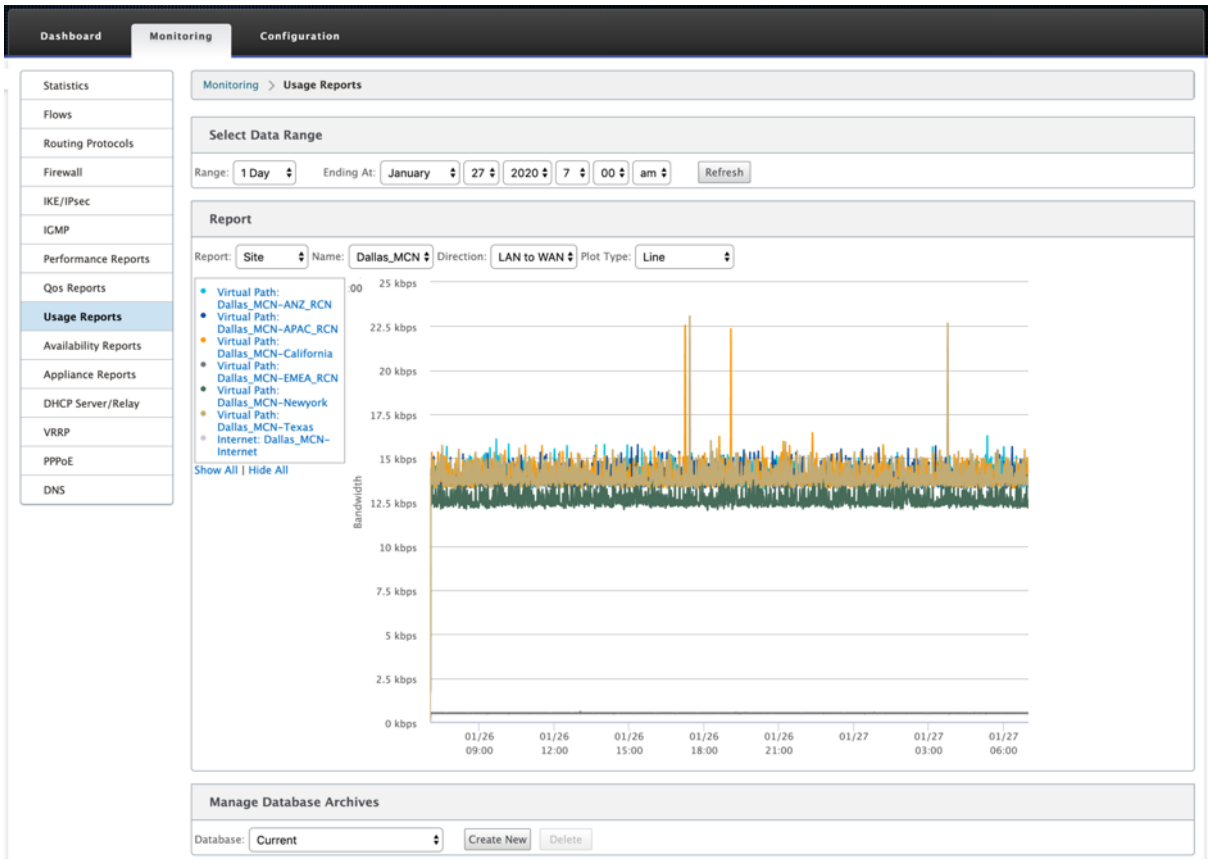
您可以查看以下指标：

- 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

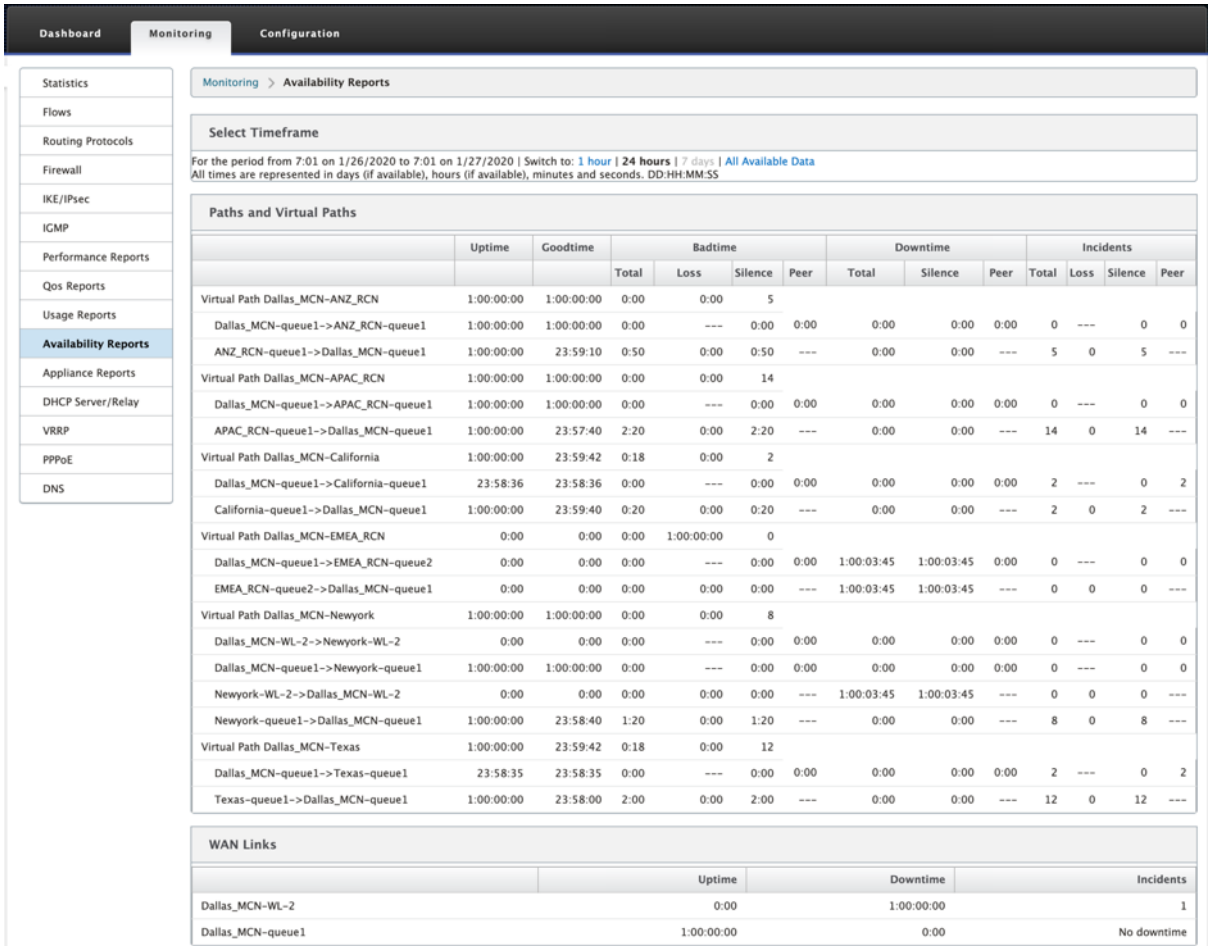
使用情况报告提供虚拟路径使用情况信息。



- 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）。

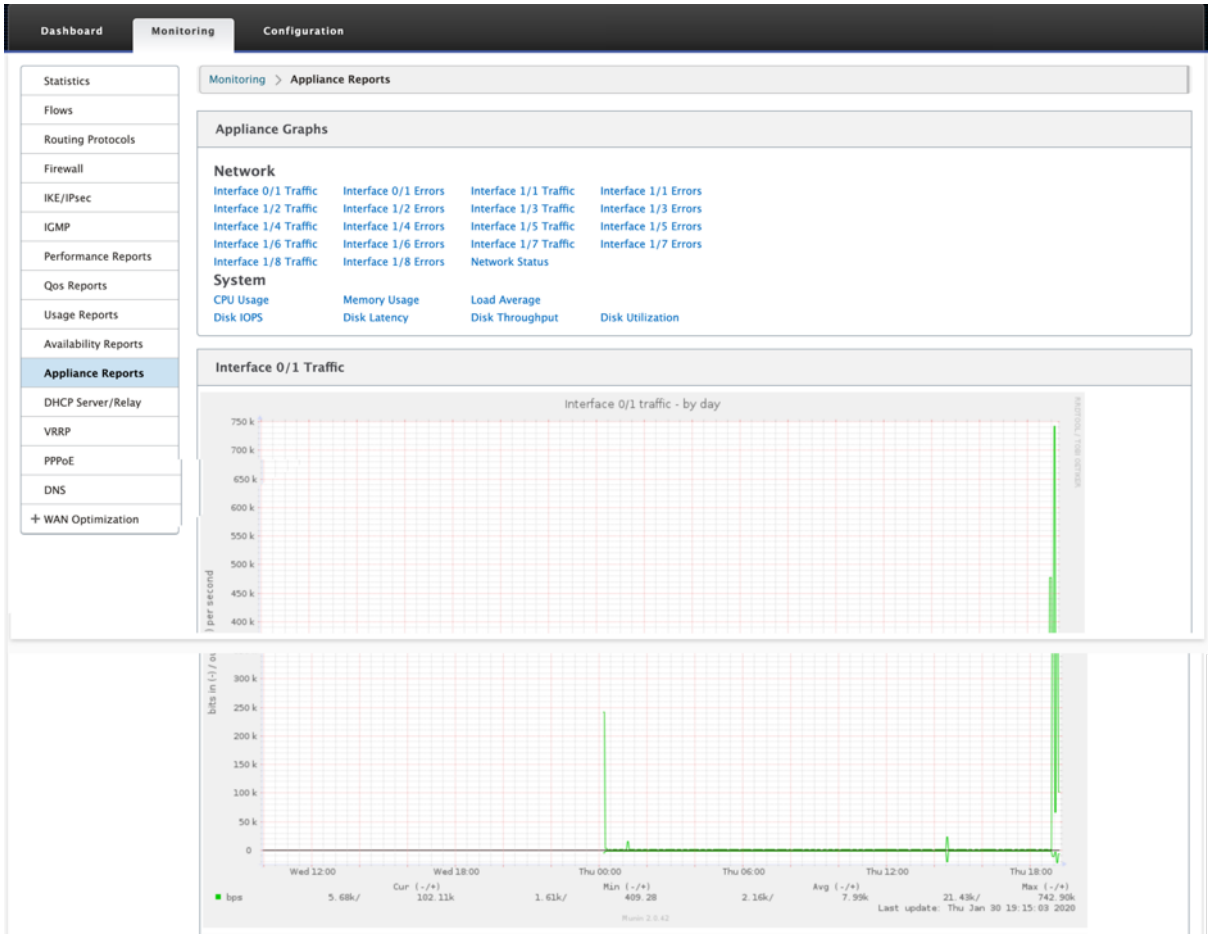
可用性报告

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

June 22, 2021

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。

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。

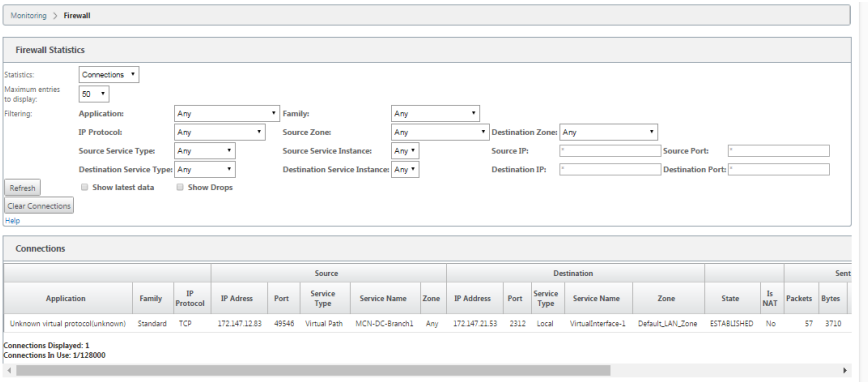
NAT 策略

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。

要查看防火墙统计信息，请执行以下操作：

1. 导航到监视 > 防火墙。
2. 在“统计”字段中，根据需要选择连接、筛选器策略或 **NAT** 策略。
3. 根据需要设置筛选条件。



4. 单击 刷新。

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：

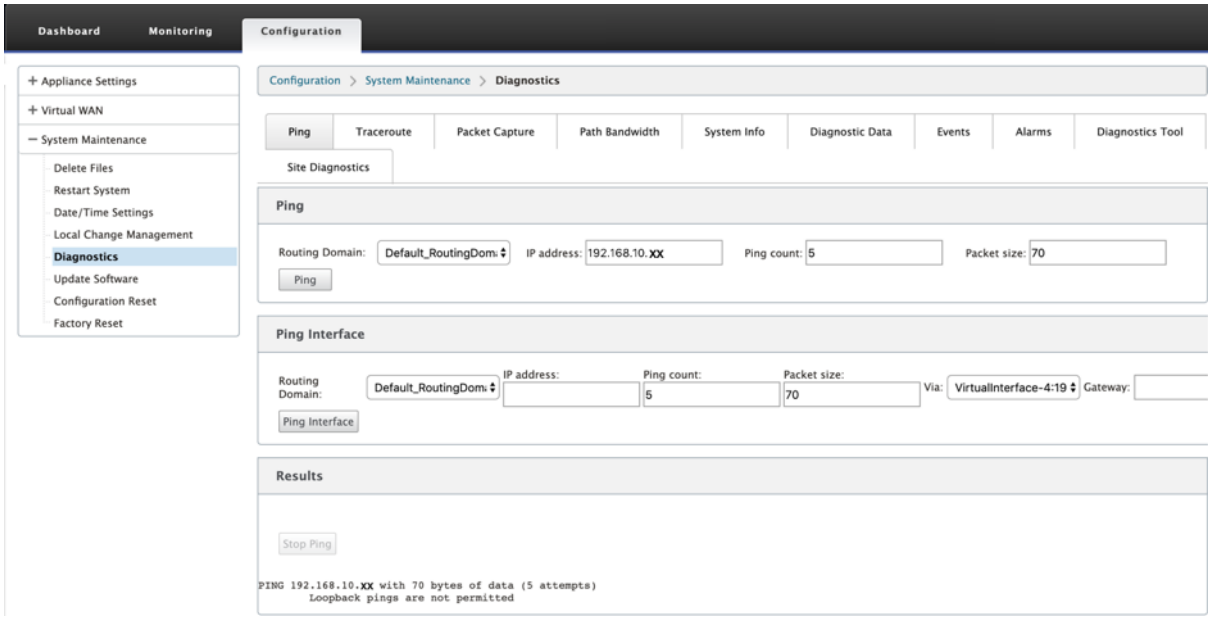
- Ping
- Traceroute
- 数据包捕获
- 路径带宽
- 系统信息
- 诊断数据

- 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。

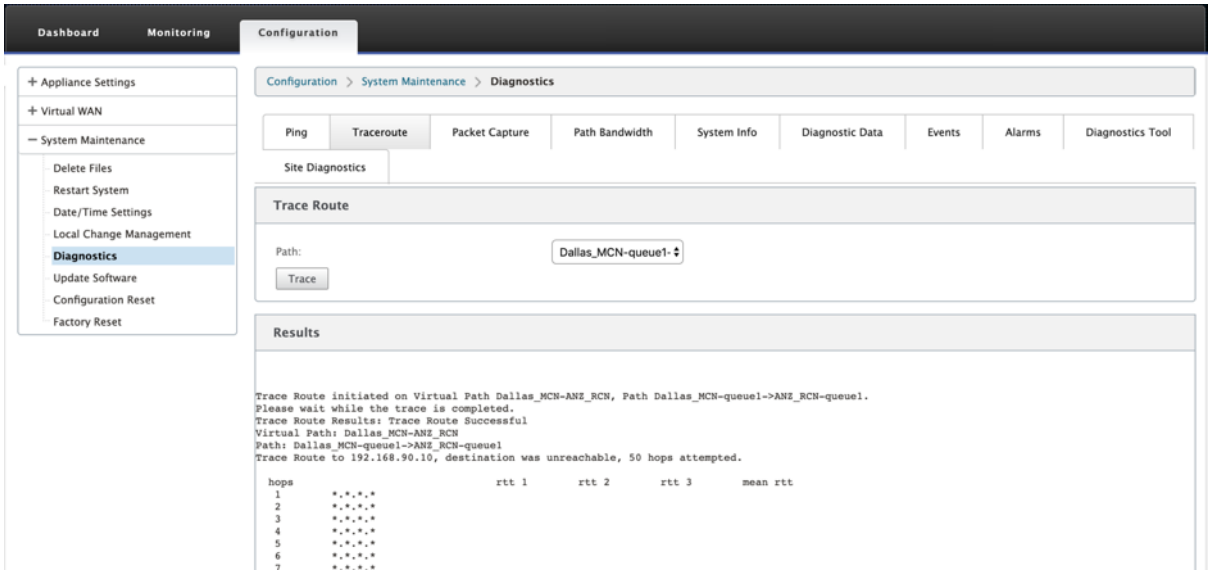


选择路由域。提供有效的 IP 地址、ping 计数次数（发送 ping 请求的次数）和数据包大小（数据字节数）。单击 停止 **Ping** 可停止正在进行的 ping 搜索。

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**。

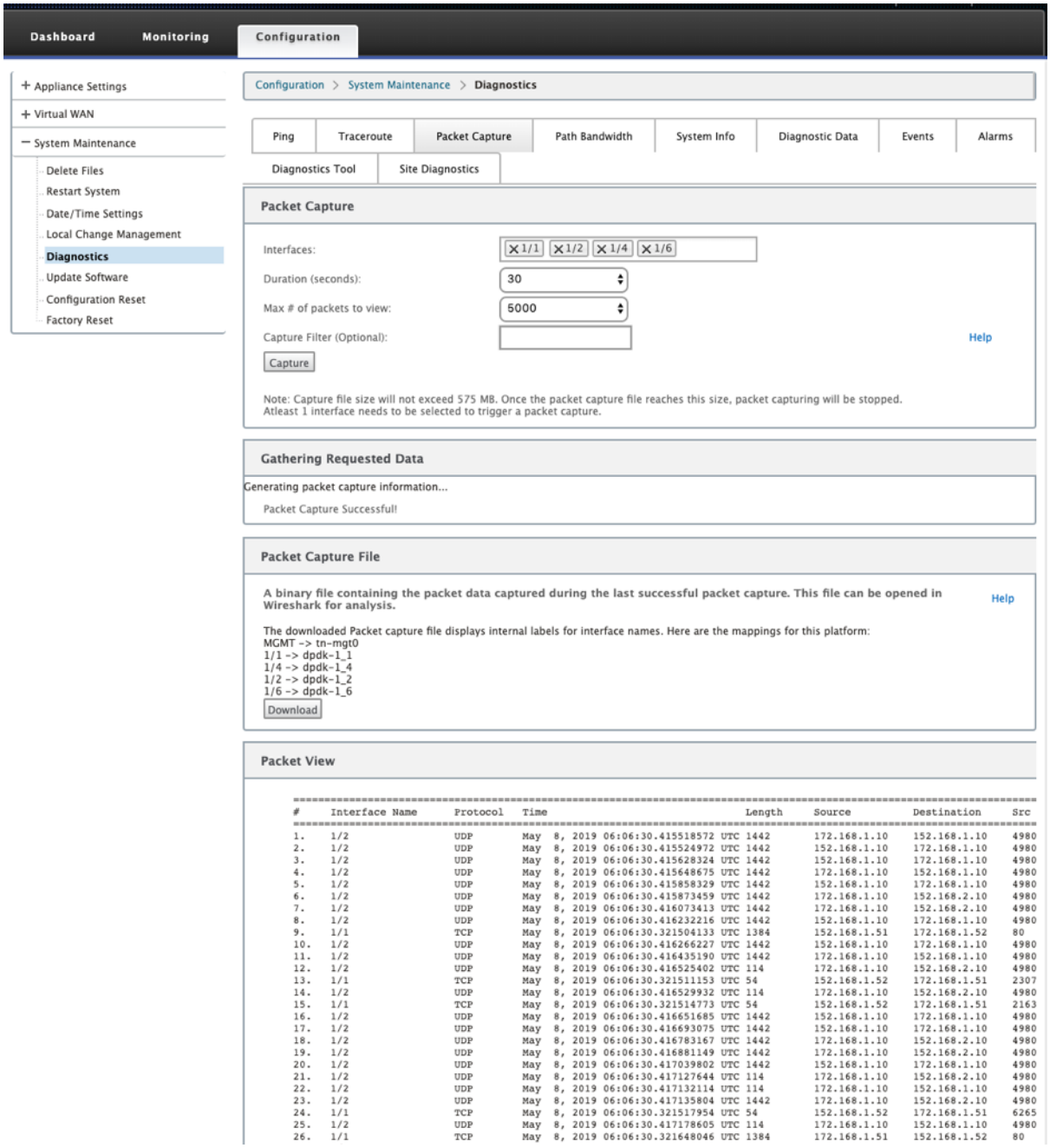


Traceroute 有助于发现并显示通往远程服务器的路径或路由。使用 **Traceroute** 选项作为调试工具来检测网络中的故障点。

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。

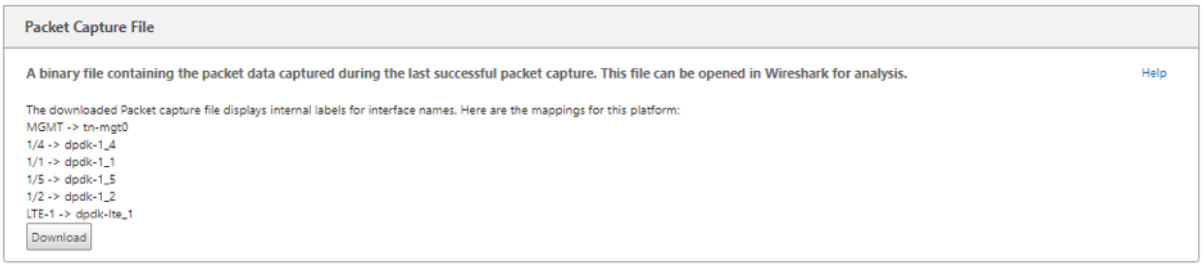
单击 捕获 查看数据包捕获结果。您还可以下载包含上次成功捕获数据包期间捕获的数据包数据的二进制文件。

收集所要求的数据

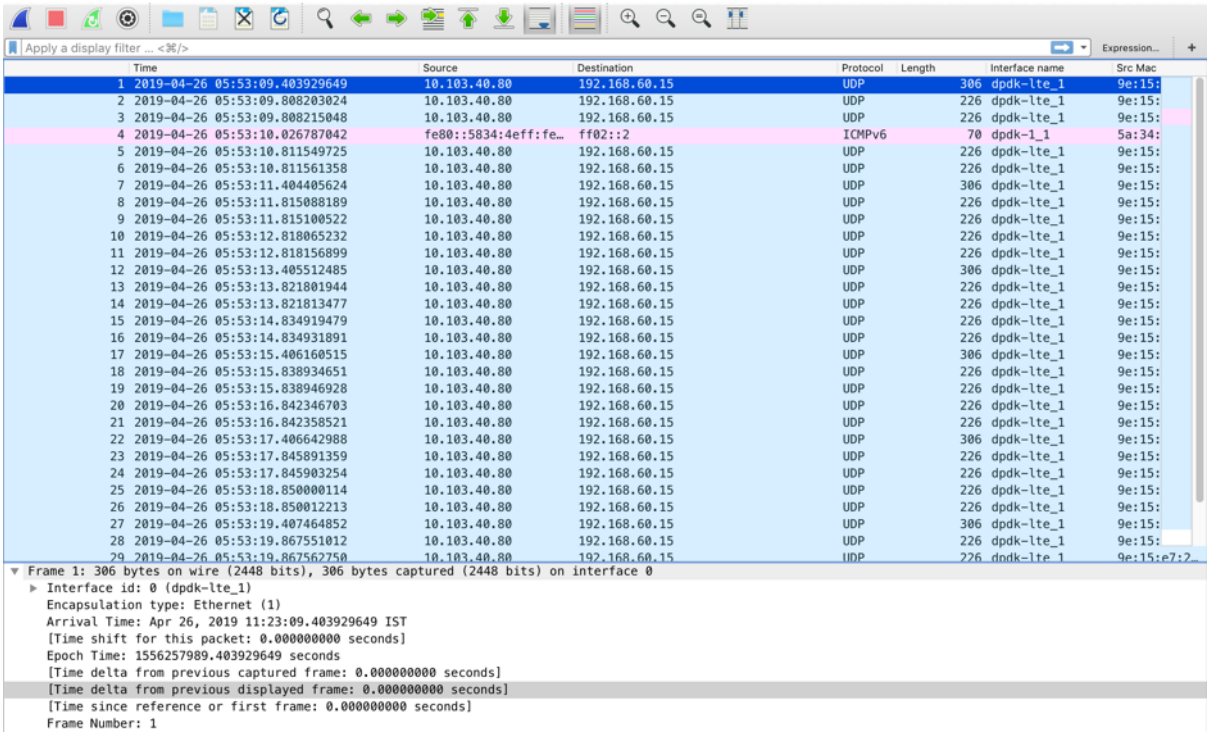
您可以在此表中查看生成数据包捕获信息的状态（数据包捕获是成功还是没有数据包捕获）。

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。



你需要 **Wireshark** 软件 2.4.13 版或更高版本才能打开和读取二进制文件。

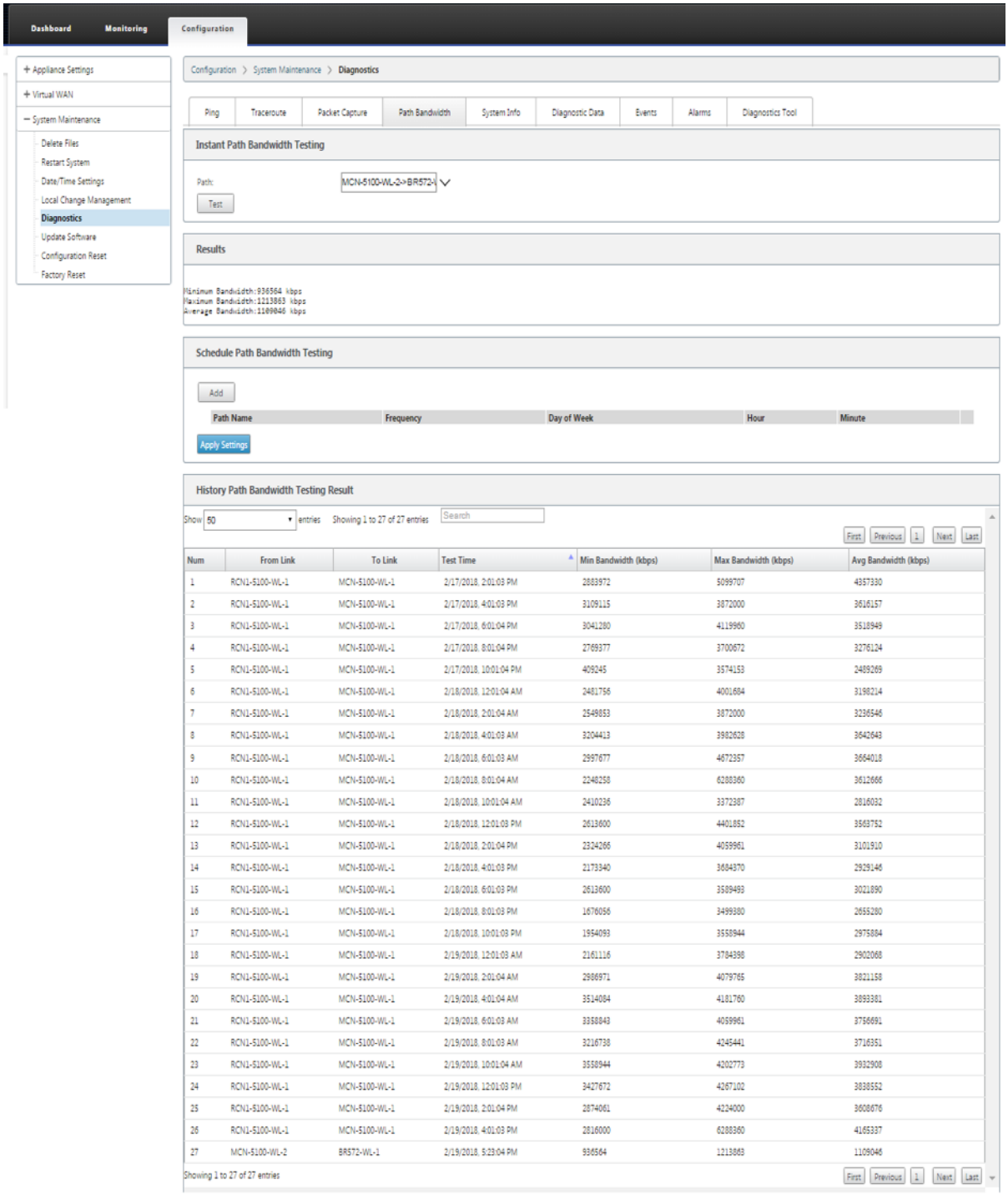


数据包视图

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。



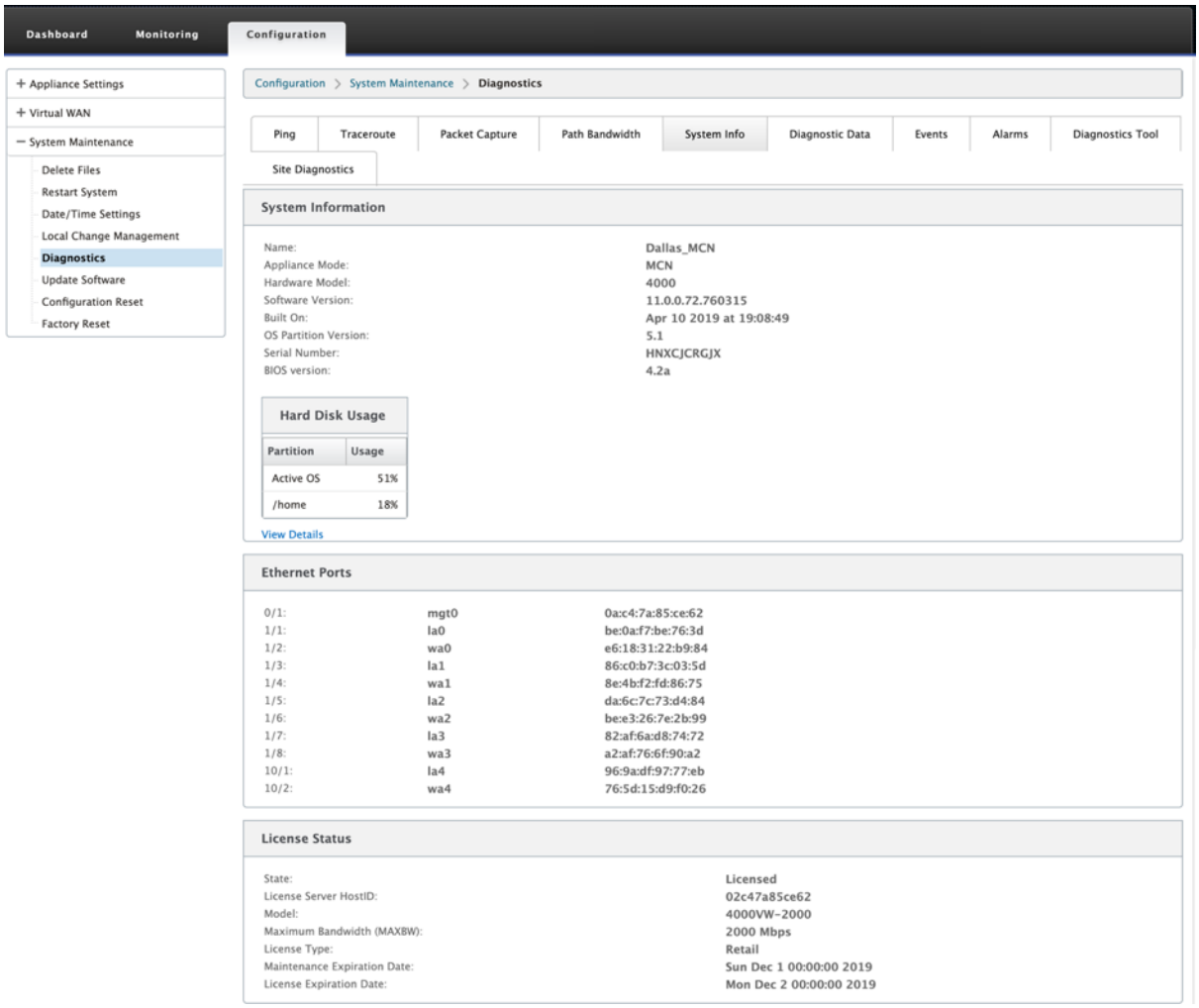
主动带宽测试使您能够通过公共 Internet WAN 链接发出即时路径带宽测试，或安排公共 Internet WAN 链接带宽测试在特定时间定期完成。

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。

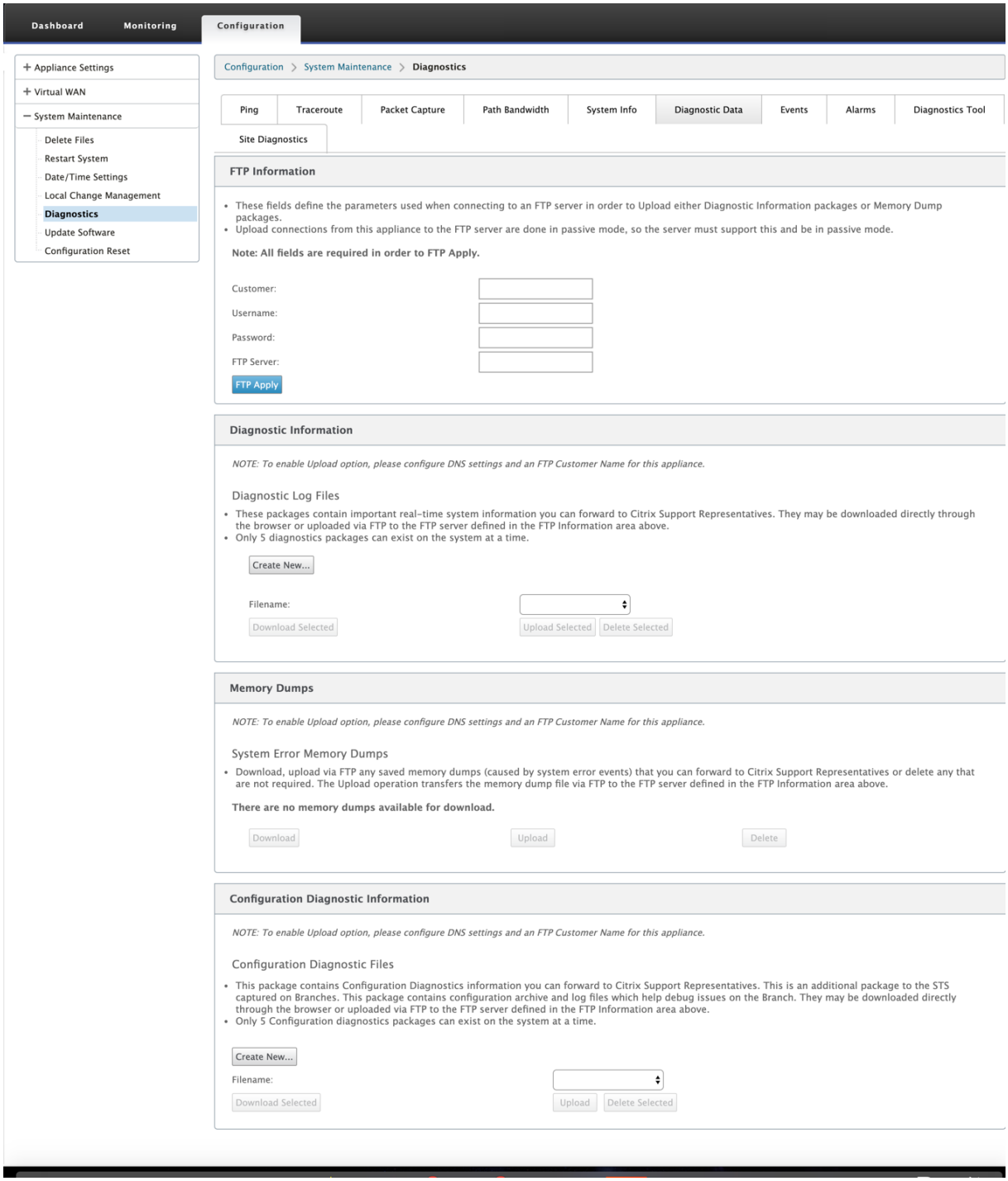


系 统信息 列出了所有未设置为默认值的参数。此信息为只读信息。如果怀疑存在某种错误配置，则由支持部门使用。当您报告问题时，系统可能会要求您检查此页面上的一个或多个值。

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。



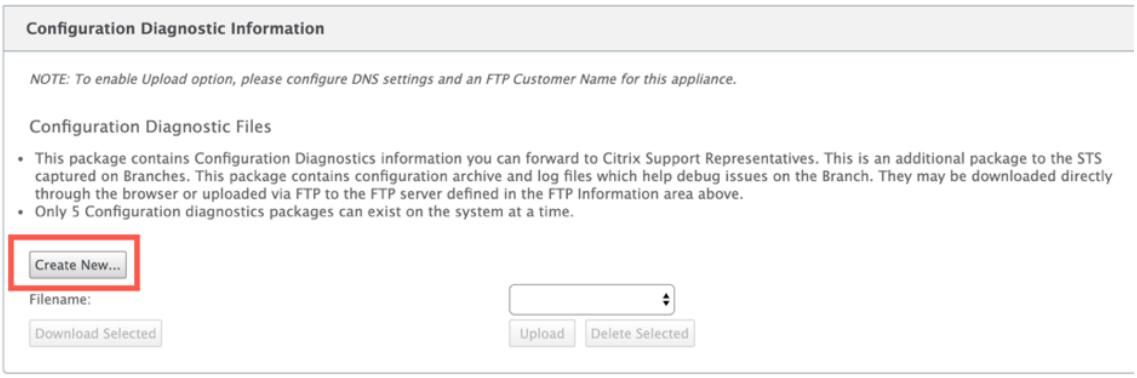
诊断数据 包括：

- **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。

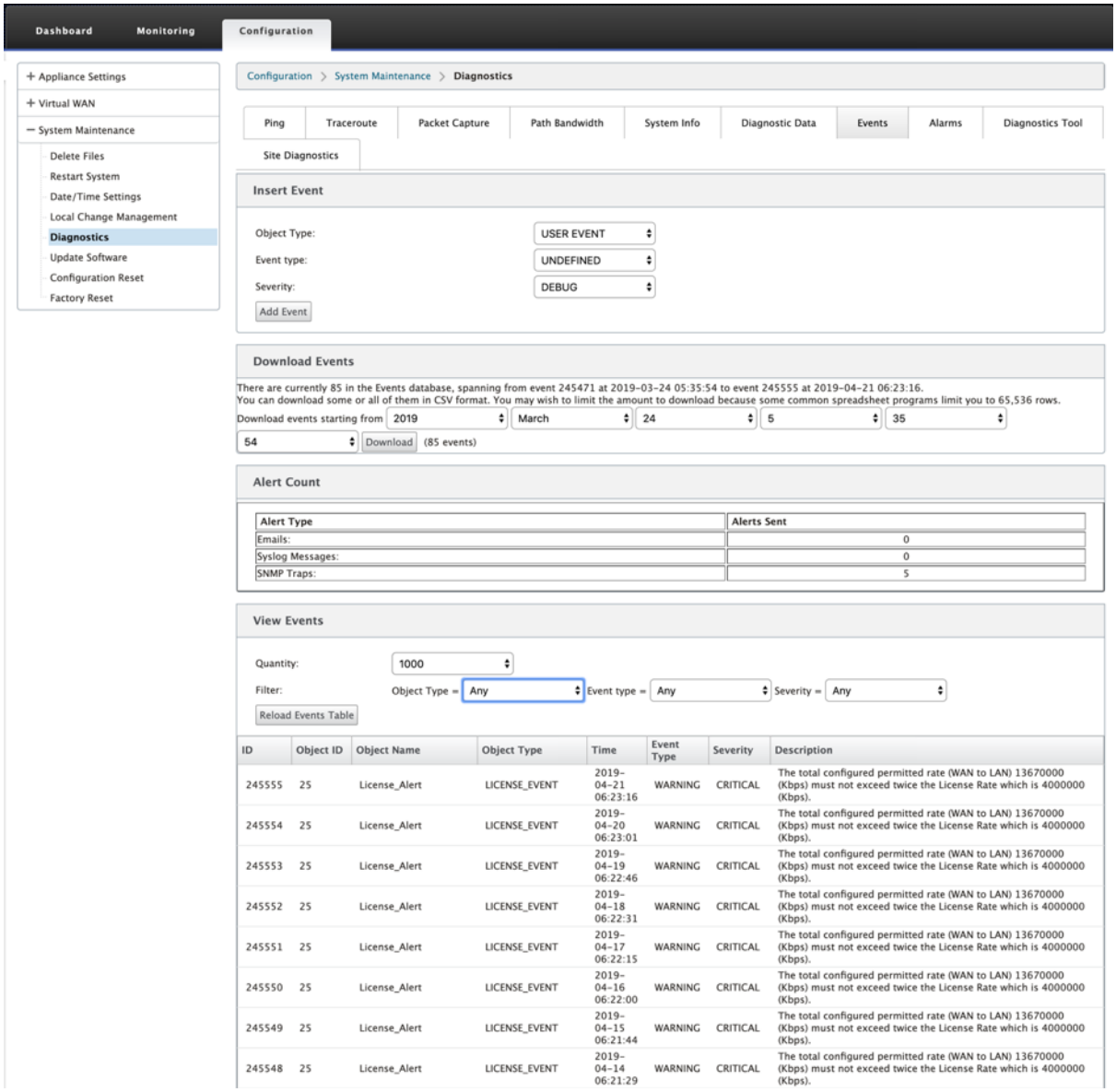
> 注意：
>
> 默认情况下，上传 选项处于禁用模式。要启用它，请为此设备配置 **DNS** 设置和 **FTP** 客户名称。

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。

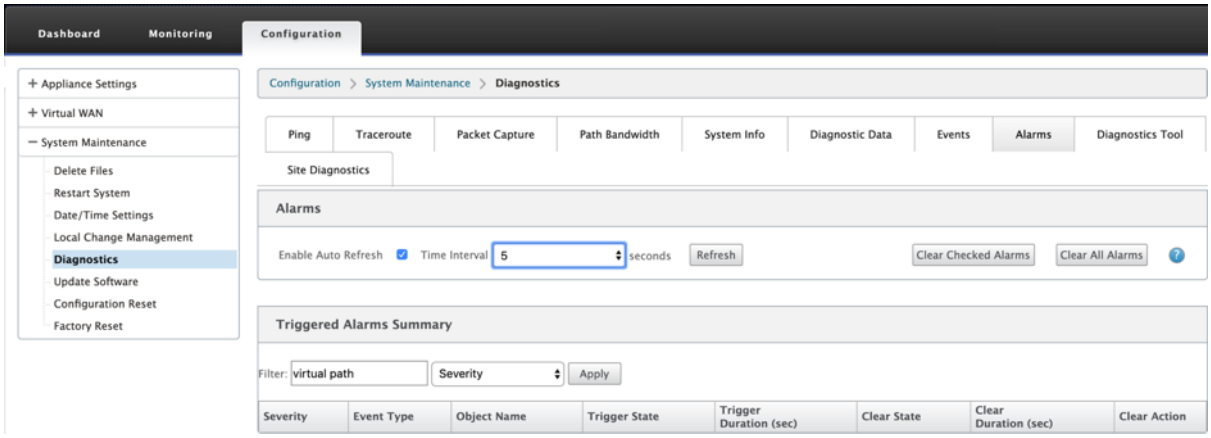
您可以在“查看事件”表格下 查看事件 详细信息。活动详情包括以下信息。

- **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。

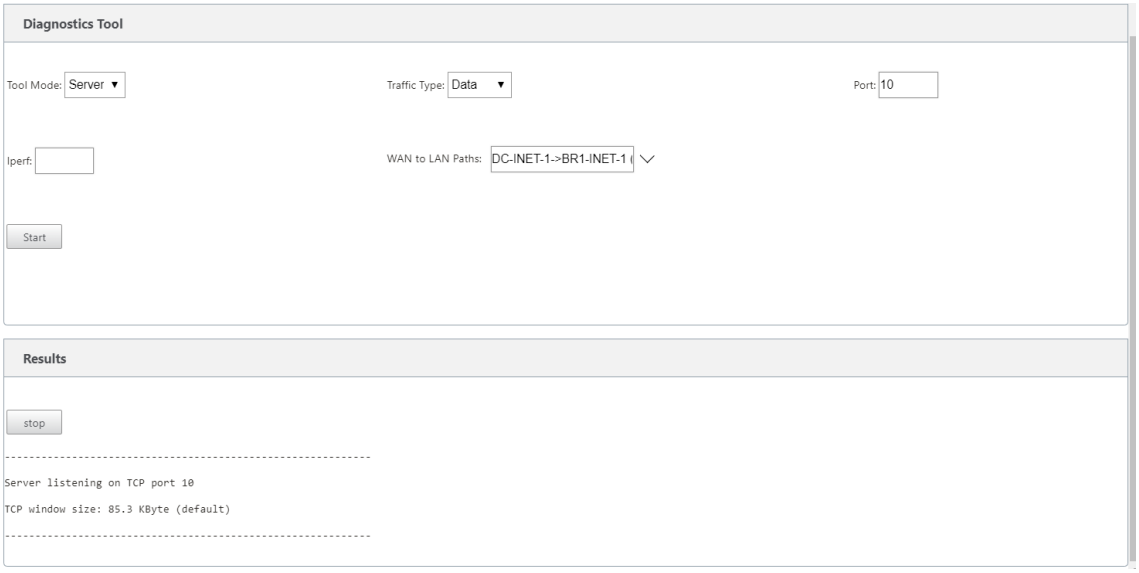
诊断工具允许生成以下两种类型的流量：

- 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。



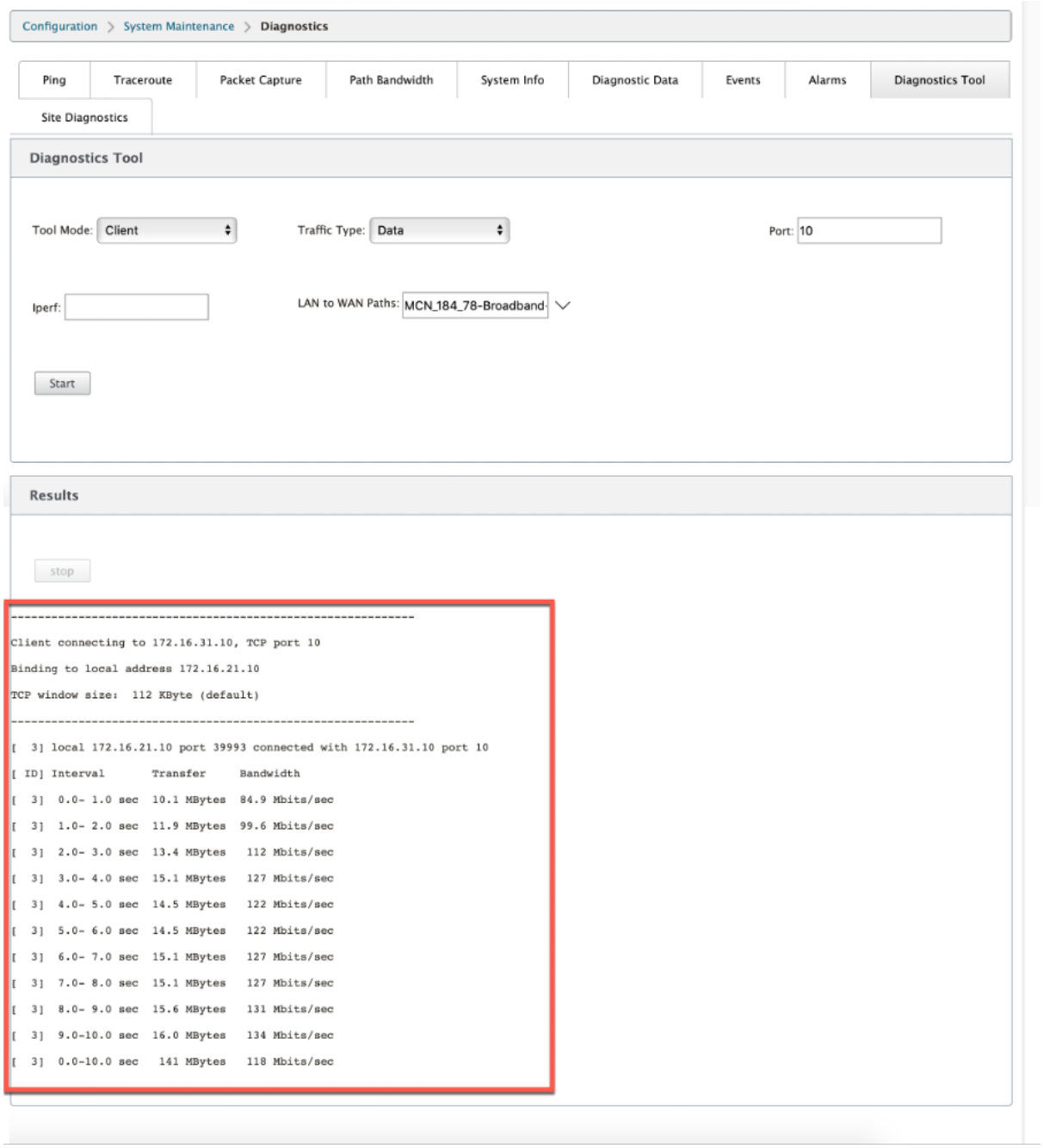
2. 在工具模式字段中，选择一台设备上的服务器，然后选择位于所选路径远程端的设备上的客户端。
3. 在“流量类型”字段中，选择诊断流量的类型，即“控制”或“数据”。在两个设备上选择相同的流量类型。
4. 在“端口”字段中，指定发送诊断流量的 **TCP /UDP** 端口号。在两个设备上指定相同的端口号。
5. 在 **Iperf** 字段中，指定 IPPERF 命令行选项（如果有）。

> 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”。

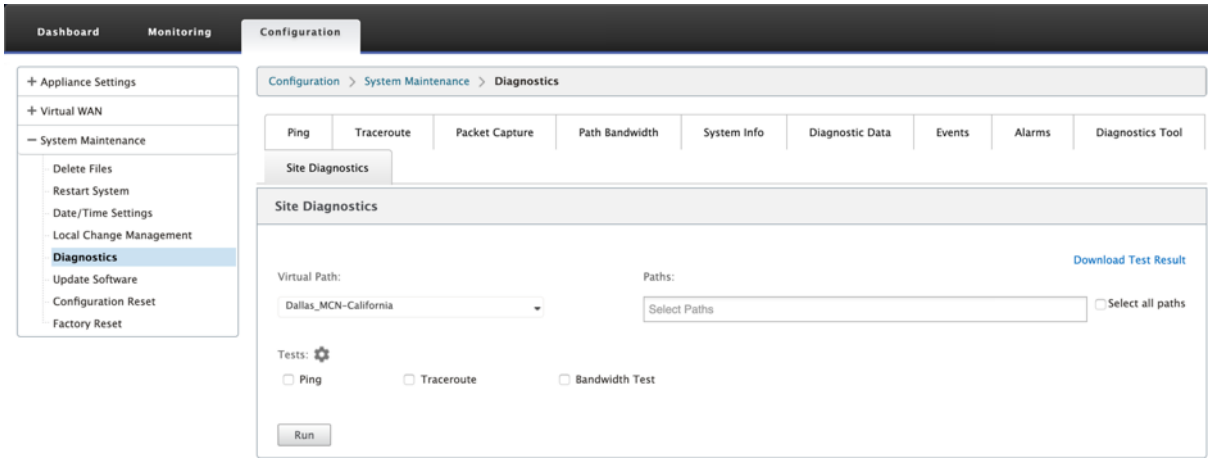
结果将显示所选设备的模式（客户端或服务器）以及运行测试的 TCP 或 UDP 端口。它会定期显示在指定时间间隔内传输的数据和占用的带宽，直到达到测试的总持续时间。



站点诊断

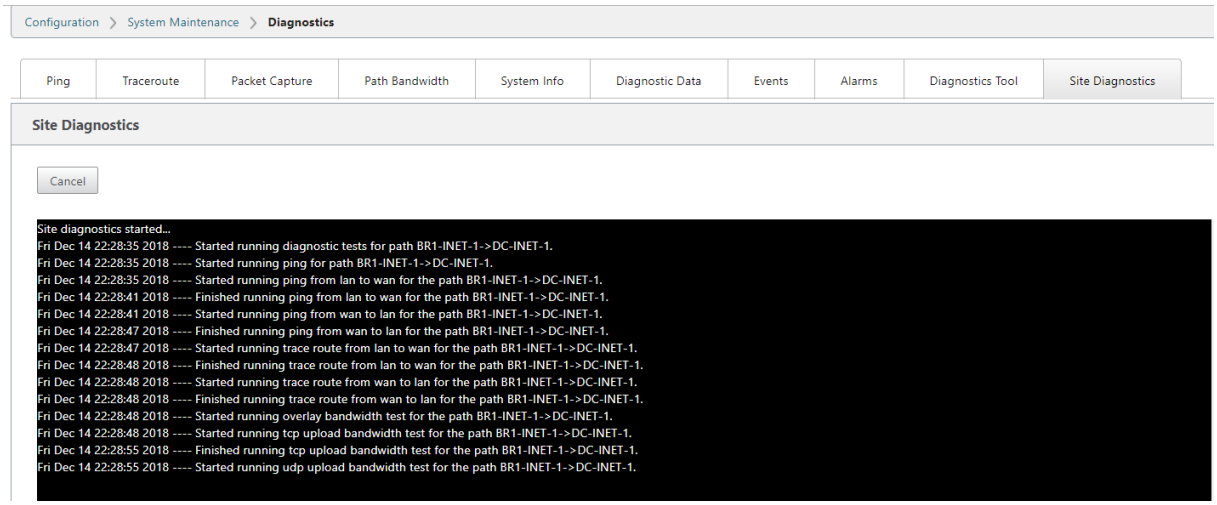
您可以对在 Citrix SD-WAN 网络中的不同站点配置的 WAN 链接测试带宽使用情况、ping 和执行 traceroute。它提供的信息有助于对现有配置中的问题进行故障排除。

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

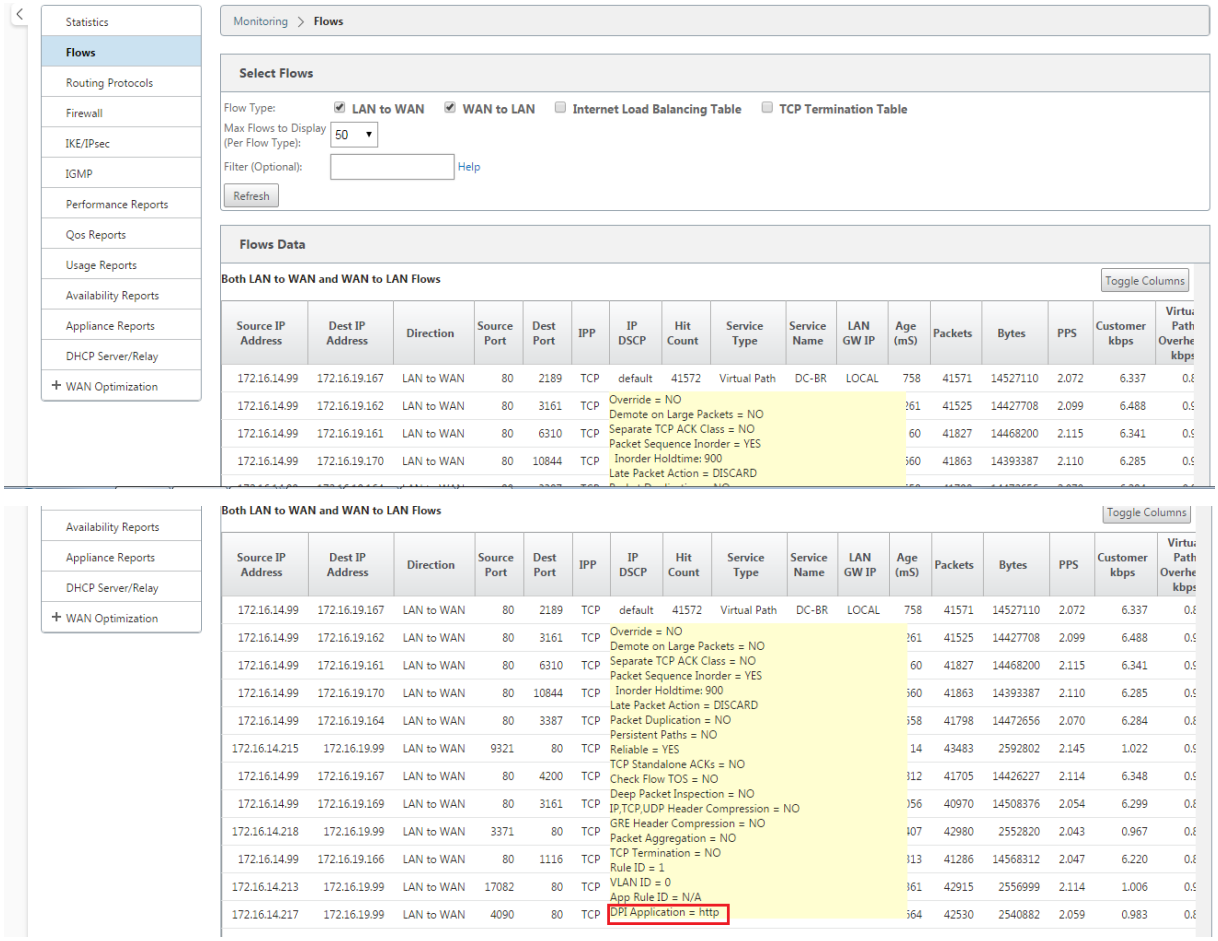
June 22, 2021

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

监视流上的 DPI 应用程序对象名称存储并显示在 SD-WAN GUI 监视 -> 流页面中。将显示一个工具提示来标识 DPI 应用程序。



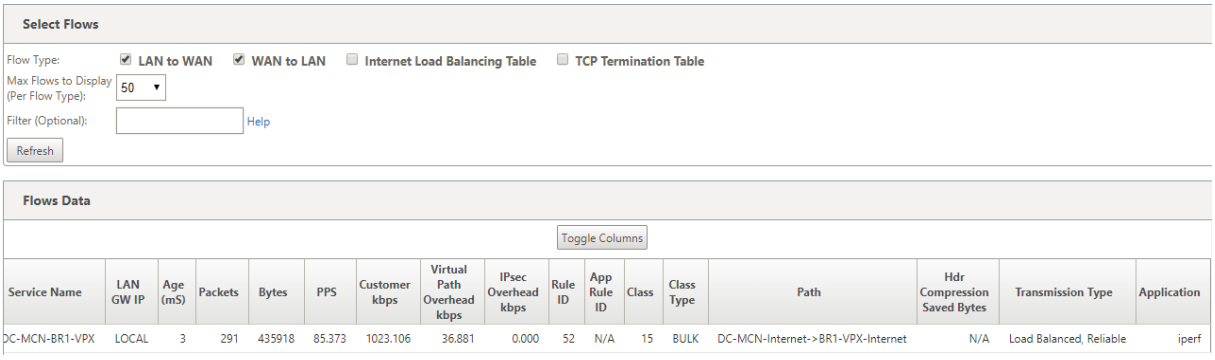
SD-WAN GUI 中交通流量的路径信息监视

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：

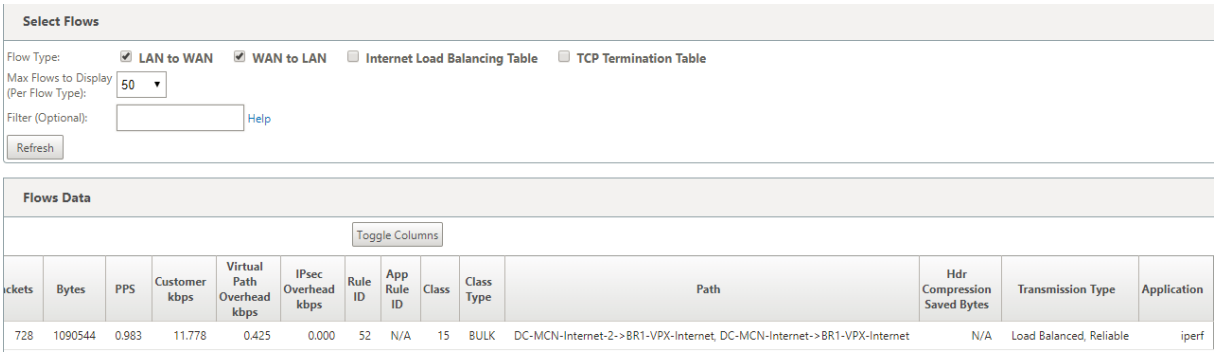
下图说明了启动流量且所有路径均良好的情况，选择一条最佳路径，因为带宽需求足以满足一条路径。您注意到只选择一个路径 **DC-MCN-Internet** -> **BR1-VPX-Internet**，并且传输类型显示为负载均衡。



Service Name	LAN GW 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
DC-MCN-BR1-VPX	LOCAL	3	291	435918	85.373	1023.106	36.881	0.000	52	N/A	15	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

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为 **DC-MCN-Internet2 -> BR1-VPX-Internet**，处理流量的最后一个最佳路径为 **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。

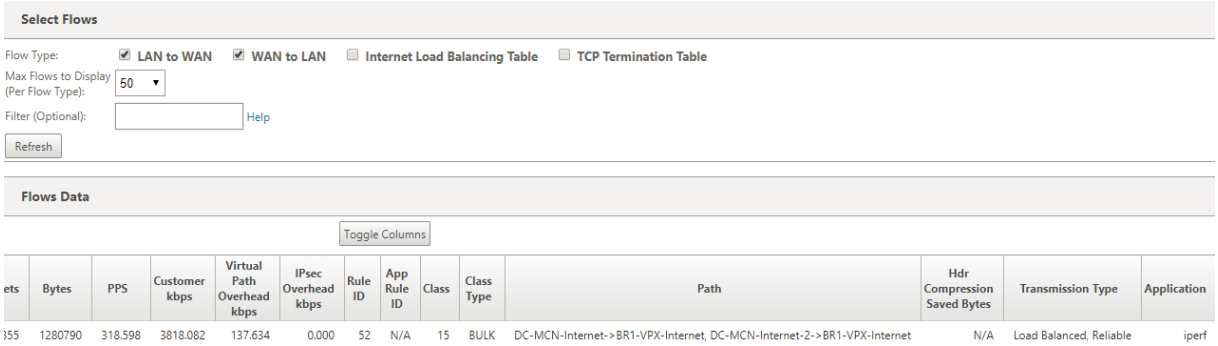


ckets	Bytes	PPS	Customer kbps	Virtual Path Overhead kbps	IPsec Overhead kbps	Rule ID	App Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type	Application
728	1090544	0.983	11.778	0.425	0.000	52	N/A	15	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-Internet->BR1-VPX-Internet	N/A	Load Balanced, Reliable	iperf

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。

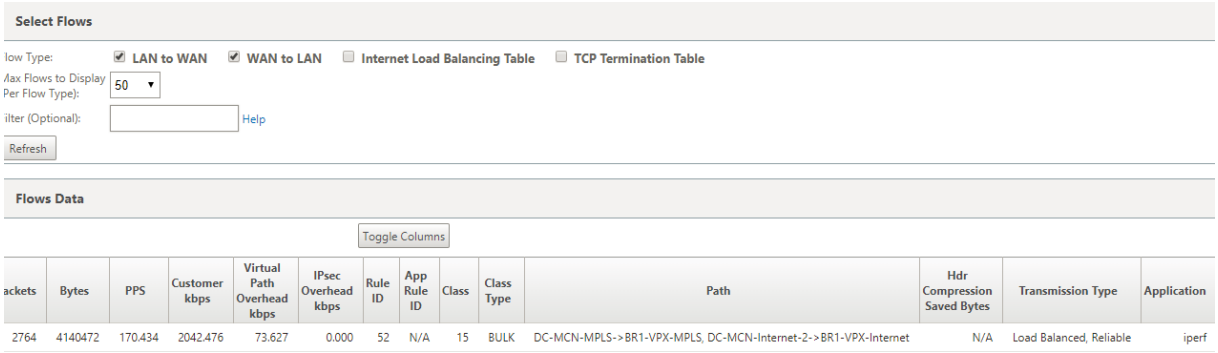
观察流数据表中显示的两条路径为 **DC-MCN-Internet->BR1-VPX-Internet**、**DC-MCN-Internet2->BR1-VPX-Internet**。

> 注意
>
> 如上所示，只显示流表中最多两个路径。



下图说明当流量仍在流动时，如果当前最佳路径 **DC-MCN-Internet-> BR1-VPX-Internet** 在 WAN 属性中不可用/不活动/降级，则所选的当前最佳路径将首先出现在 流量数据 表的路径部分其次是服务于流量的最佳路径。

由于 **DC-MCN-Internet->BR1-VPX-Internet** 不再是最好的，因此，系统选择了一个新的当前最佳路径作为 **DC-MCN-MPLS->BR1-VPX-MPLS**，最后一个主动提供连接的最佳路径与当前最佳路径为 **DC-MCN-Internet2->BR1-VPX-Internet**，因为这两者都是当前的带宽流量需求所需的。



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。

您注意到在下图中，流数据表的路径部分中的两个路径 **DC-MCN-Internet2->BR-VPX-Internet**、**DC-MCN-MPLS->BR1-VPX-MPLS**。

Select Flows

Flow Type: ☑ LAN to WAN ☑ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

Flows Data

Toggle Columns

e S)	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
3	551	32640	88.836	42.100	38.377	0.000	0	N/A	9	BULK	DC-MCN-Internet-2->BR1-VPX-Internet, DC-MCN-MPLS->BR1-VPX-MPLS	N/A	Duplicate, Reliable	iperf
4	1651	2362062	262.860	3008.560	113.555	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable	iperf

下图说明流量流动时，如果其中一个当前最佳路径变为非活动状态，则会选择另一个路径，并且仍有两个路径作为 流量数据 表中路径部分的一部分。

Select Flows

Flow Type: ☑ LAN to WAN ☑ WAN to LAN ☐ Internet Load Balancing Table ☐ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional): Help

Refresh

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
CAL	10	9692	530732	75.025	32.705	32.411	0.000	0	N/A	9	BULK	DC-MCN-MPLS->BR1-VPX-MPLS, DC-MCN-Internet->BR1-VPX-Internet	N/A	Duplicate, Reliable
CAL	0	34213	49055970	267.264	3066.058	115.458	0.000	72	N/A	N/A	N/A	N/A	N/A	Duplicate, Reliable

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。目前只有一个最好的路径，这是 **DC-MCN-Internet->BR1-VPX-Internet**。

Flows Data

Toggle Columns

rvice Type	Service Name	LAN GW 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
ual Path	DC-MCN-BR1-VPX	LOCAL	662	3	4494	1.127	13.511	0.487	0.000	4	N/A	9	BULK	DC-MCN-Internet->BR1-VPX-Internet	N/A	Persistent	iperf

下图说明，如果路径 **DC-MCN-Internet-> BR1-VPX-Internet** 变得容易延迟或禁用，则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。所采用的两种路径如下：**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

假设最好的路径之一 **DC-MCN-Internet** 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

June 22, 2021

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、WANOP 和高级（企业）版（物理和虚拟设备）的所有平台型号。

> 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

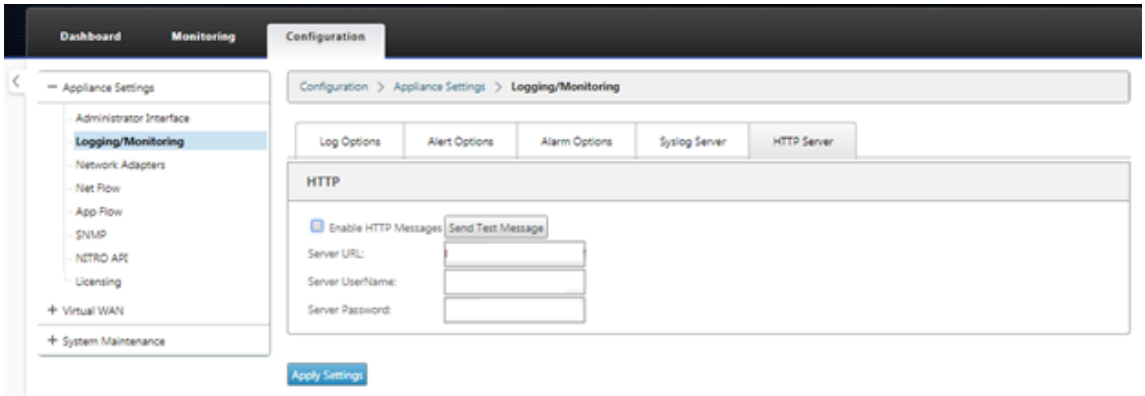
June 22, 2021

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。

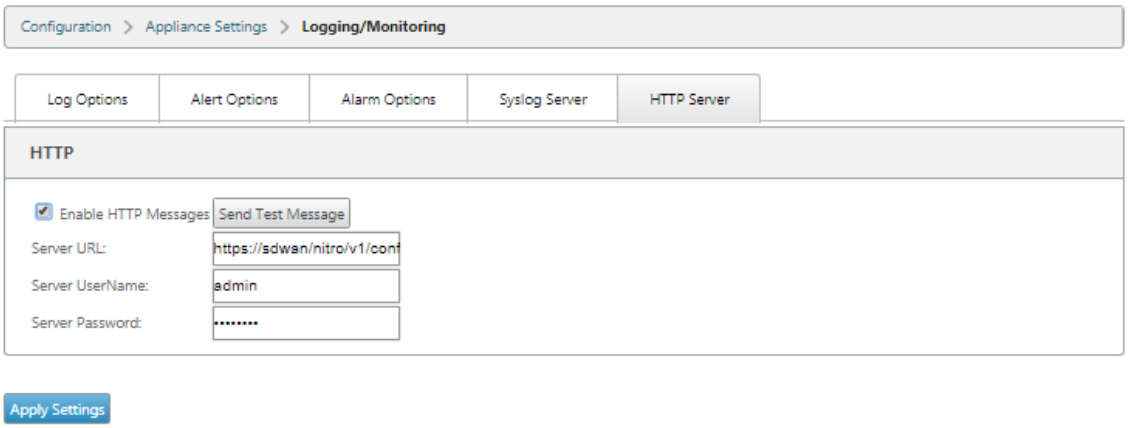
基于会话的 HTTP Post 通知会发送到外部服务，如立即服务。可以在 Citrix SD-WAN 设备 GUI 和 Citrix SD-WAN Center 中配置 HTTP 服务器的事件通知。

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 > 记录**/**监视 > **HTTP** 服务器。



2. 单击 启用 **HTTP** 消息。
3. 输入要接收通知的 HTTP 服务器的服务器 **URL**。输入 服务器用户名 和 服务器密码。

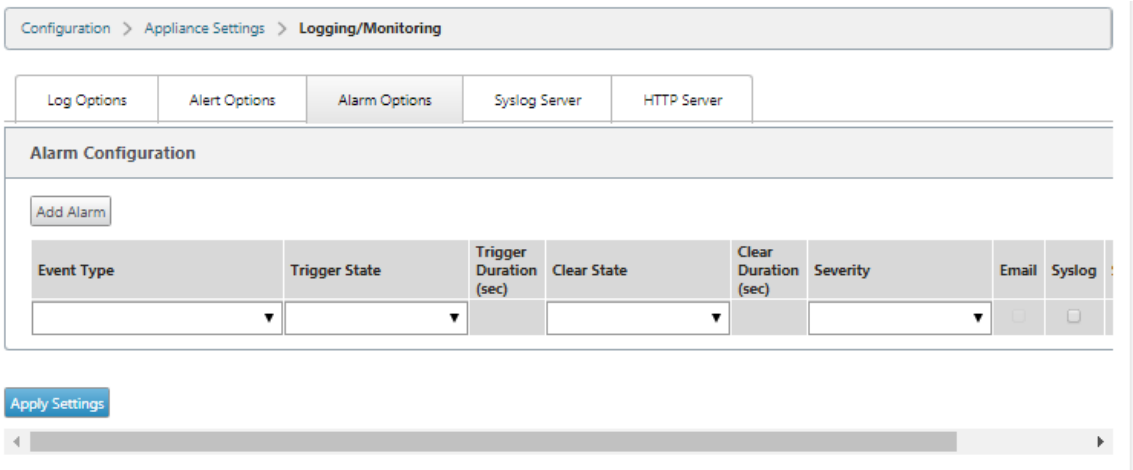


4. 单击 应用设置。应用 HTTP 服务器通知设置后，页面将刷新。

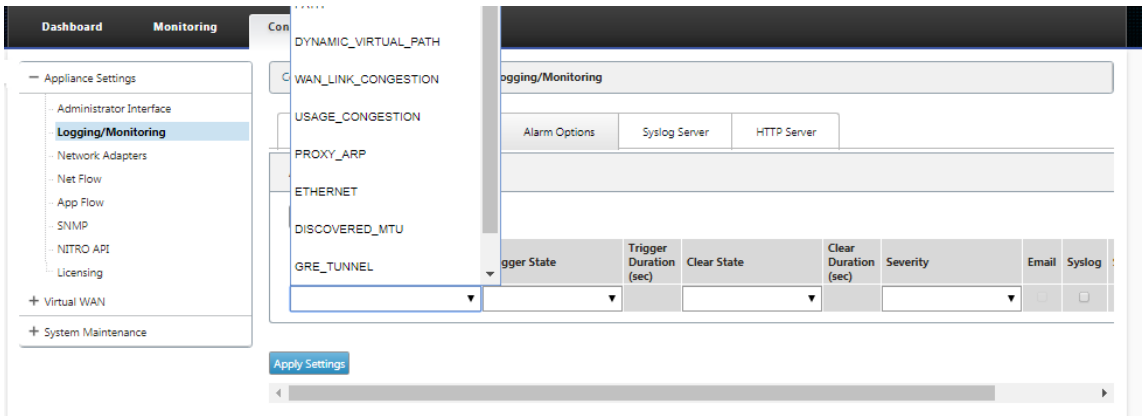
> 注意
>
> 使用 发 送测试消息 选项验证 HTTP 服务器连接是否成功。

要为 HTTP 服务器会话添加警报通知：

1. 在 记录/监视 页面中，转到 警报选项 选项 卡页面。
2. 单击 添加警报。

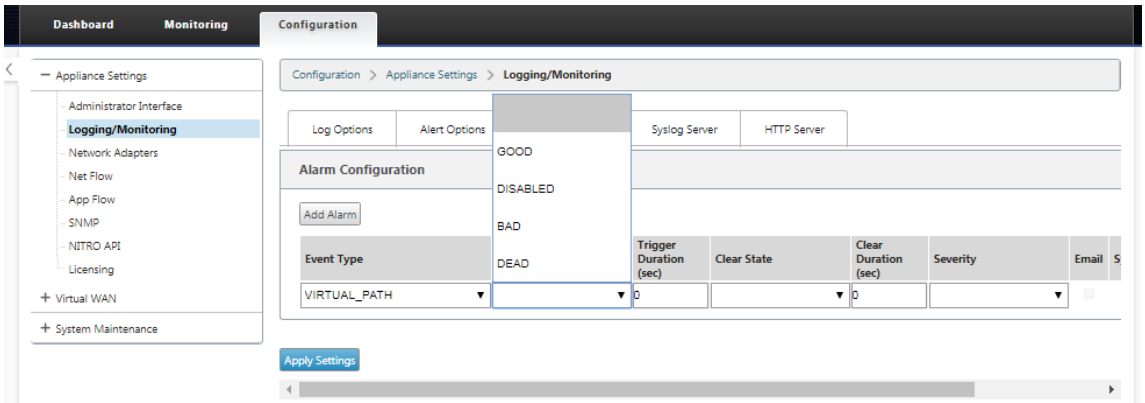


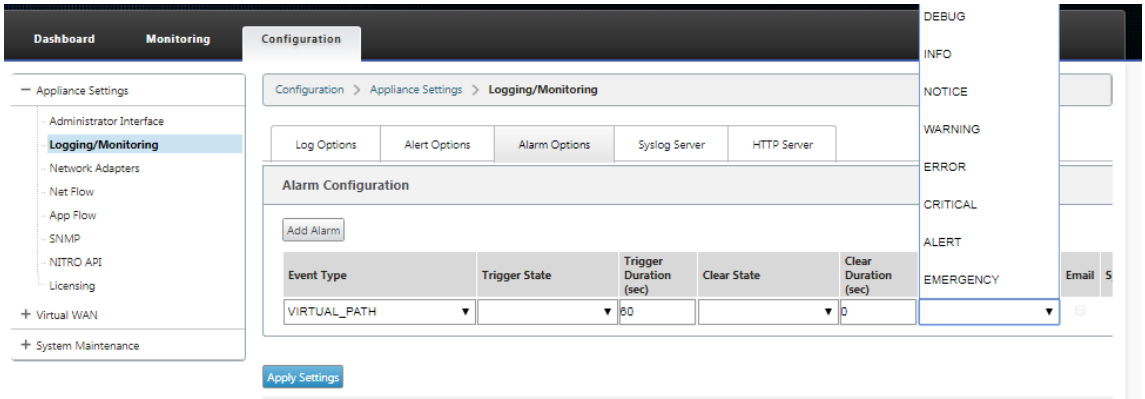
3. 从下拉列表中选择 事件类型。



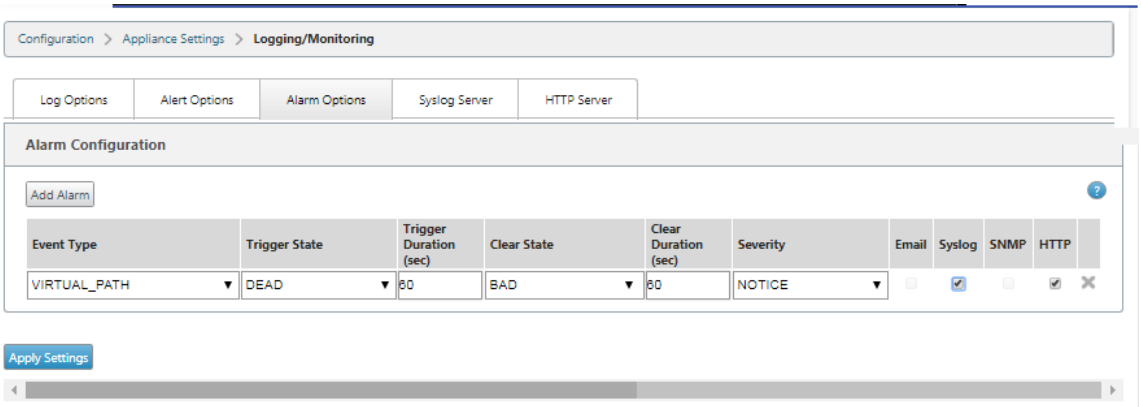
4. 为所选 事件类型选择以下警报通知状态。触发器状态和清除状态根据选定的事件类型发生变化。

- 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





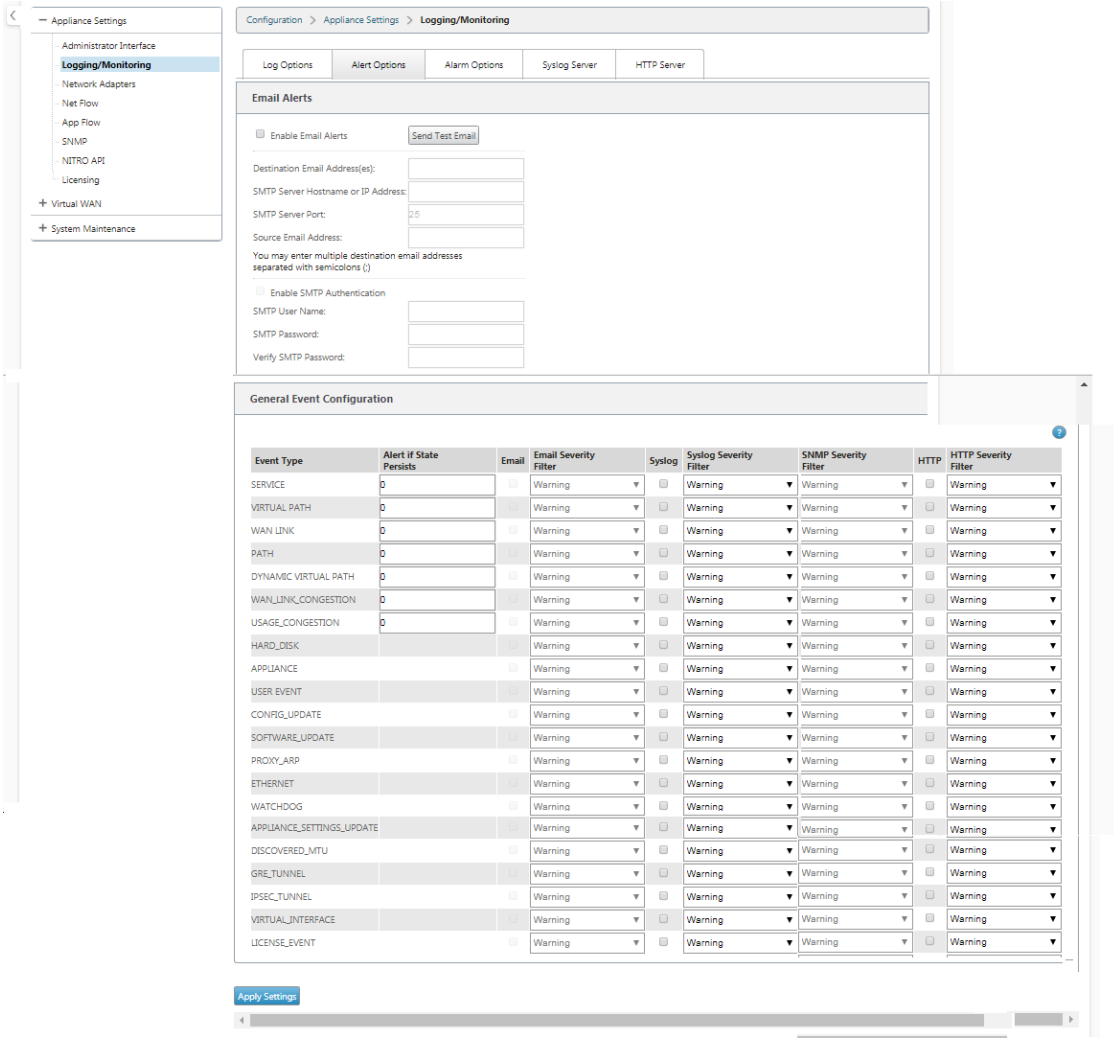
5. 选择 系统日志 和 **HTTP** 复选框以接收特定于系统日志和 HTTP 服务器事件的通知。单击 应用设置。



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 页面下；为事 件类型 选择 HTTP 服务器通知筛选器，然后单击 应用设置。

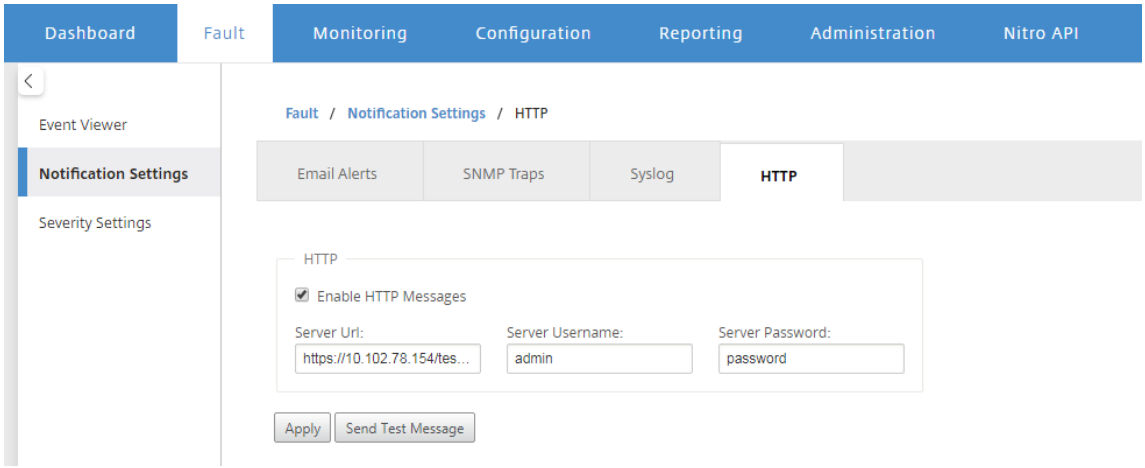
- HTTP
- HTTP 严重性筛选器



在 **Citrix SD-WAN Center** 中配置 **HTTP** 通知

要配置 HTTP 通知，请执行以下操作：

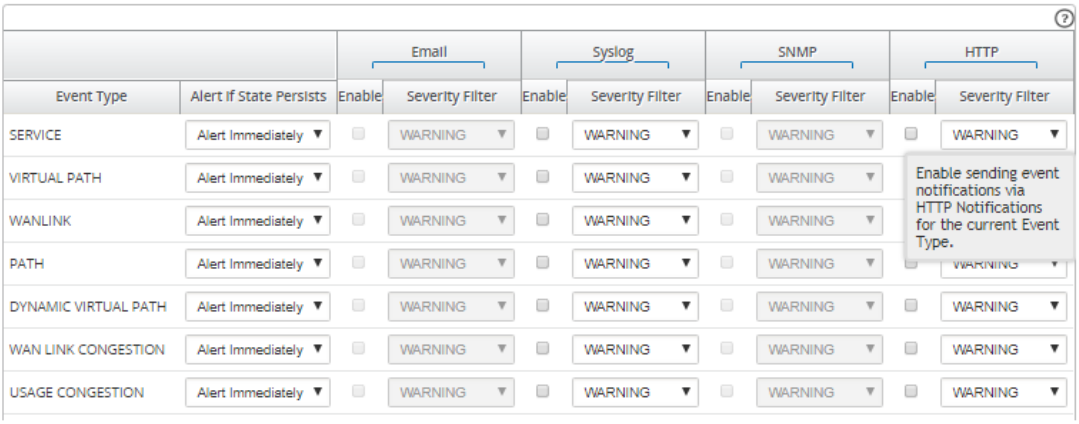
1. 导航到 故障 > 通知设置 > **HTTP**。



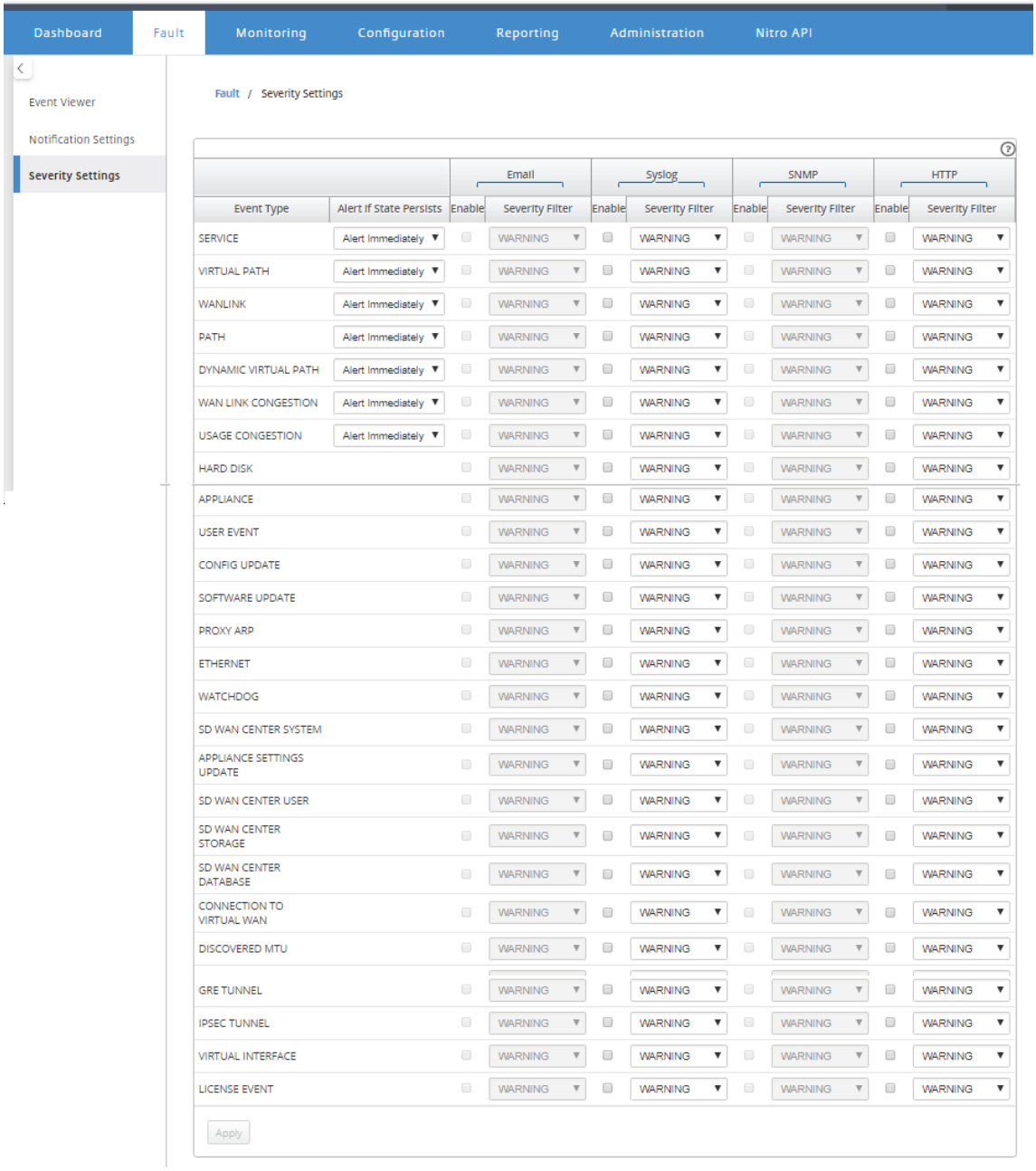
2. 输入 HTTP 服务器的服务器 **URL**、服务器用户名和服务器密码。
3. 单击 应用

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 以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。



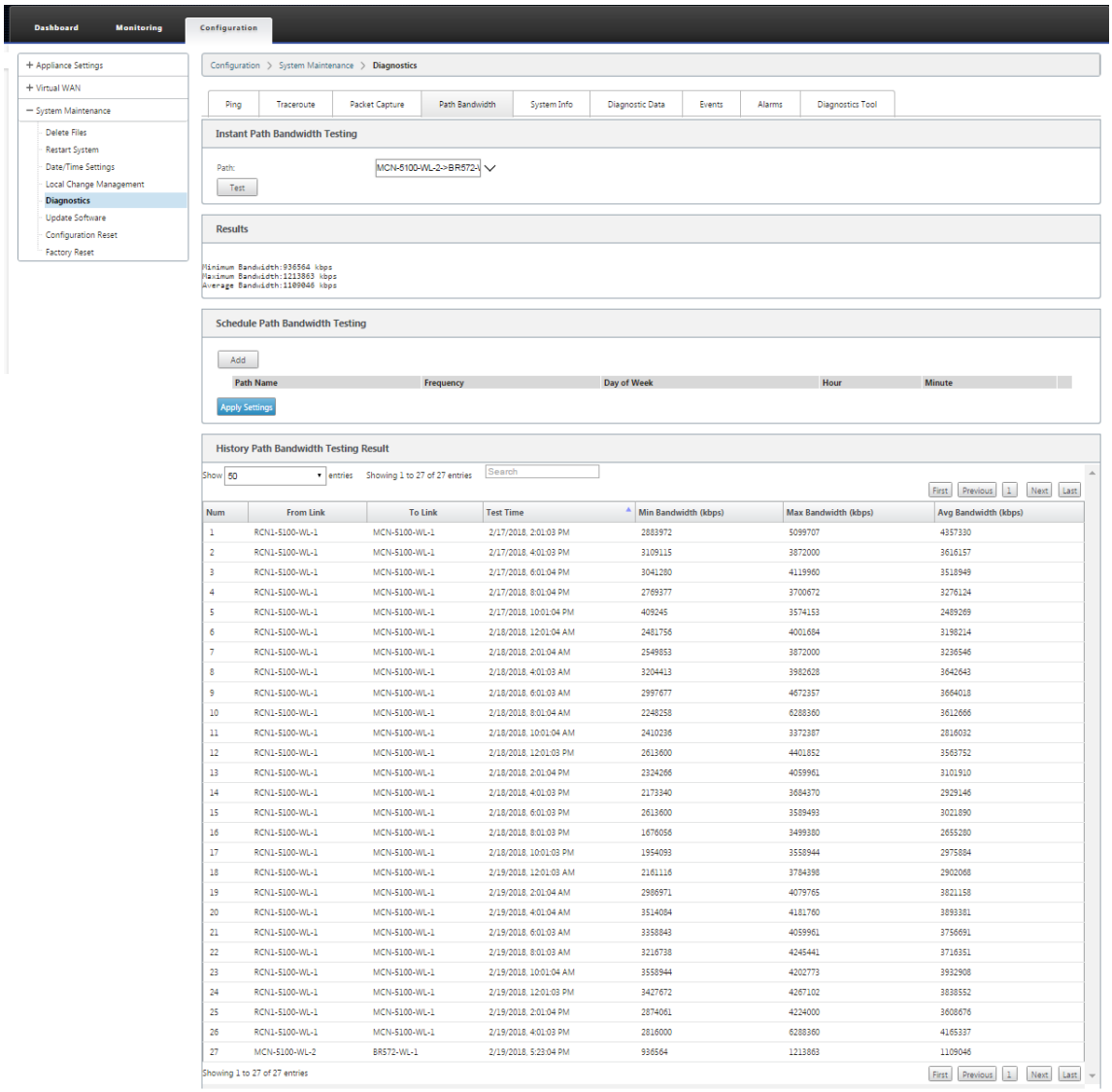
主动带宽测试

June 22, 2021

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。

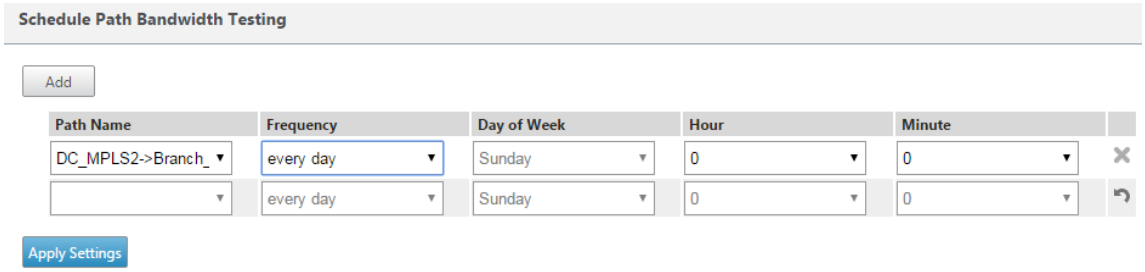
要使用主动带宽测试功能，请执行以下操作：

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。



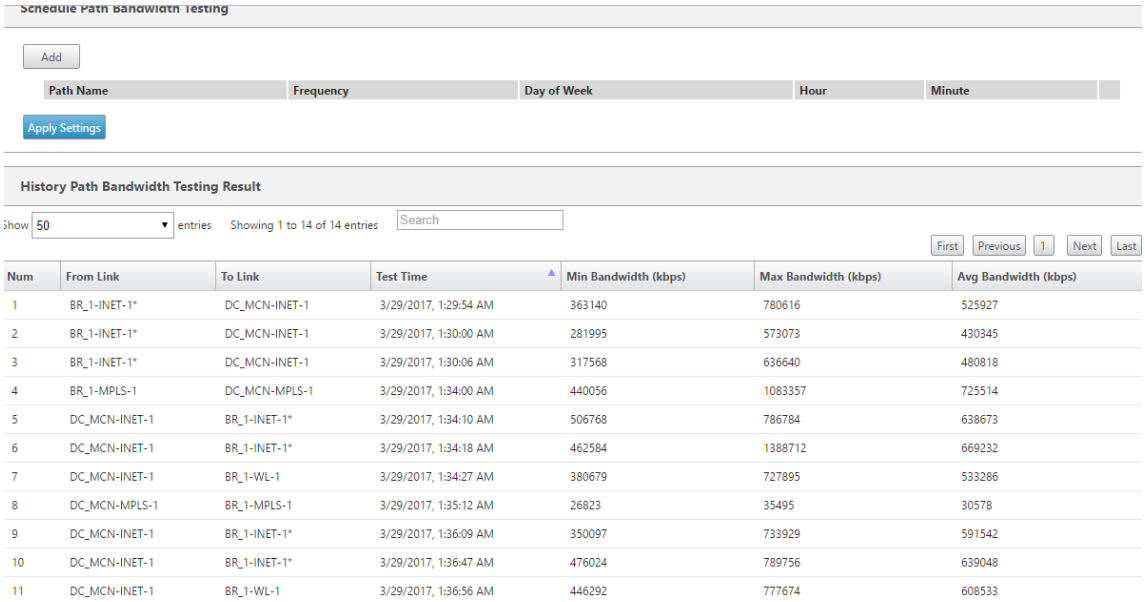
输出显示用作值的平均带宽，以设置为测试的 WAN Link 最小和最大带宽结果的允许速率。除了测试带宽的功能外，您现在可以更改配置文件以使用学习的带宽。这是通过“自动学习”选项在站点 > [站点名称] > **WAN** 链接 > [WAN 链接名称] > 设置下完成的，如果启用，系统将使用学习的带宽。

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。



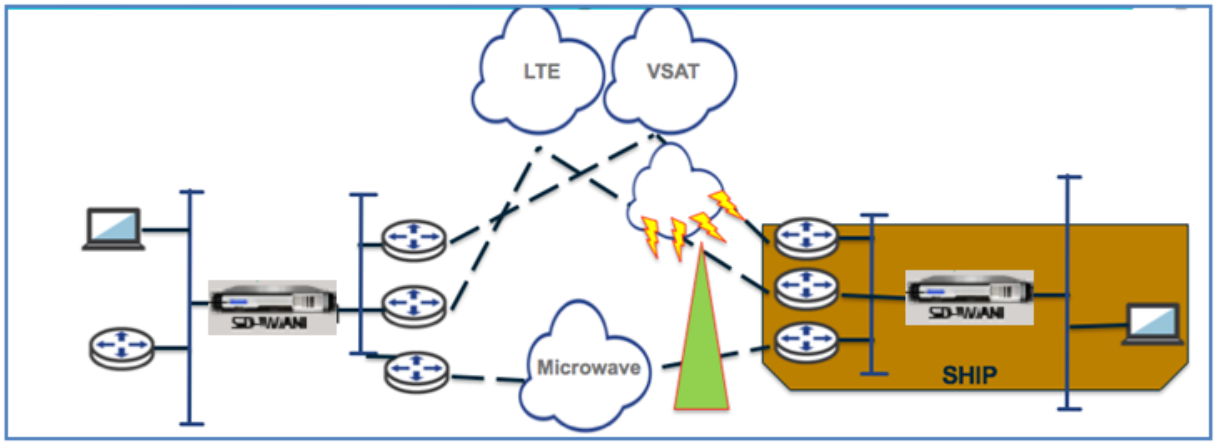
Num	From Link	To Link	Test Time	Min Bandwidth (kbps)	Max Bandwidth (kbps)	Avg Bandwidth (kbps)
1	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:29:54 AM	363140	780616	525927
2	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:00 AM	281995	573073	430345
3	BR_1-INET-1*	DC_MCN-INET-1	3/29/2017, 1:30:06 AM	317568	636640	480818
4	BR_1-MPLS-1	DC_MCN-MPLS-1	3/29/2017, 1:34:00 AM	440056	1083357	725514
5	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:10 AM	506768	786784	638673
6	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:34:18 AM	462584	1388712	669232
7	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:34:27 AM	380679	727895	533286
8	DC_MCN-MPLS-1	BR_1-MPLS-1	3/29/2017, 1:35:12 AM	26823	35495	30578
9	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:09 AM	350097	733929	591542
10	DC_MCN-INET-1	BR_1-INET-1*	3/29/2017, 1:36:47 AM	476024	789756	639048
11	DC_MCN-INET-1	BR_1-WL-1	3/29/2017, 1:36:56 AM	446292	777674	608533

自适应带宽检测

June 22, 2021

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。

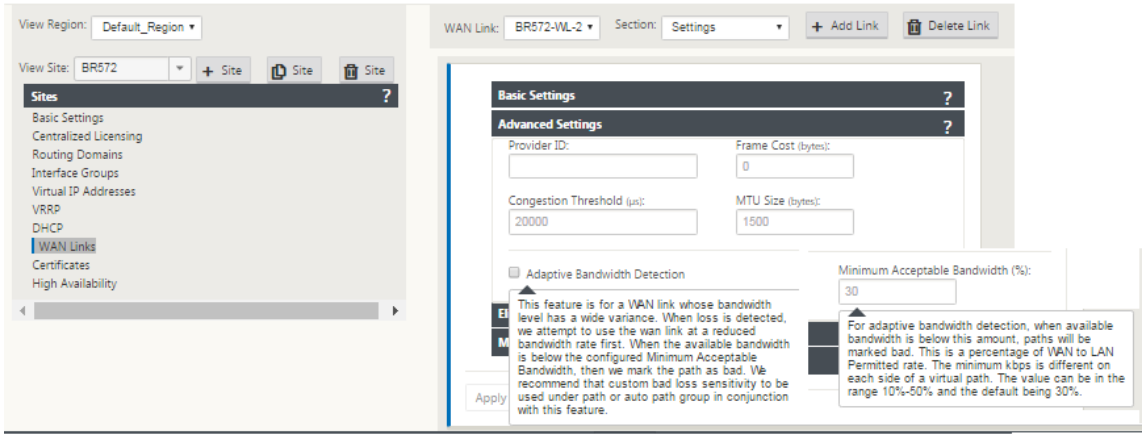
- 更高的带宽可靠性（通过 VSAT、Microwave、3G/4G 和 LTE）
- 与用户配置设置相比，自适应带宽可预测性更高



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。您可以在 全局 > 自动解决组 > [自动分配组名称] > 不良损失敏感 下启用它。

1. 在 全局 > 自动解析组 > 不良损失敏感 > [自动分配组名称] > 下启用自适应带宽检测。
2. 导航到 配置编辑器 > 站点 > [站点名称] > **WAN** 链接 > [**WAN** 链接名称] > 设置 > 高级设置。



3. 选中 自适应带宽检测 框，并在 最小可接受带宽 字段中输入一个值。
4. 通过导航到 监视 > 统计 > **WAN** 链接使用率 > 使用率和允许费率，查看使用率和允许费率 表。

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

最佳做法

June 22, 2021

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实践。

安全

路由

QoS

WAN 链接

安全性

February 10, 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
- 网络安全性
- 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。

网络安全性

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

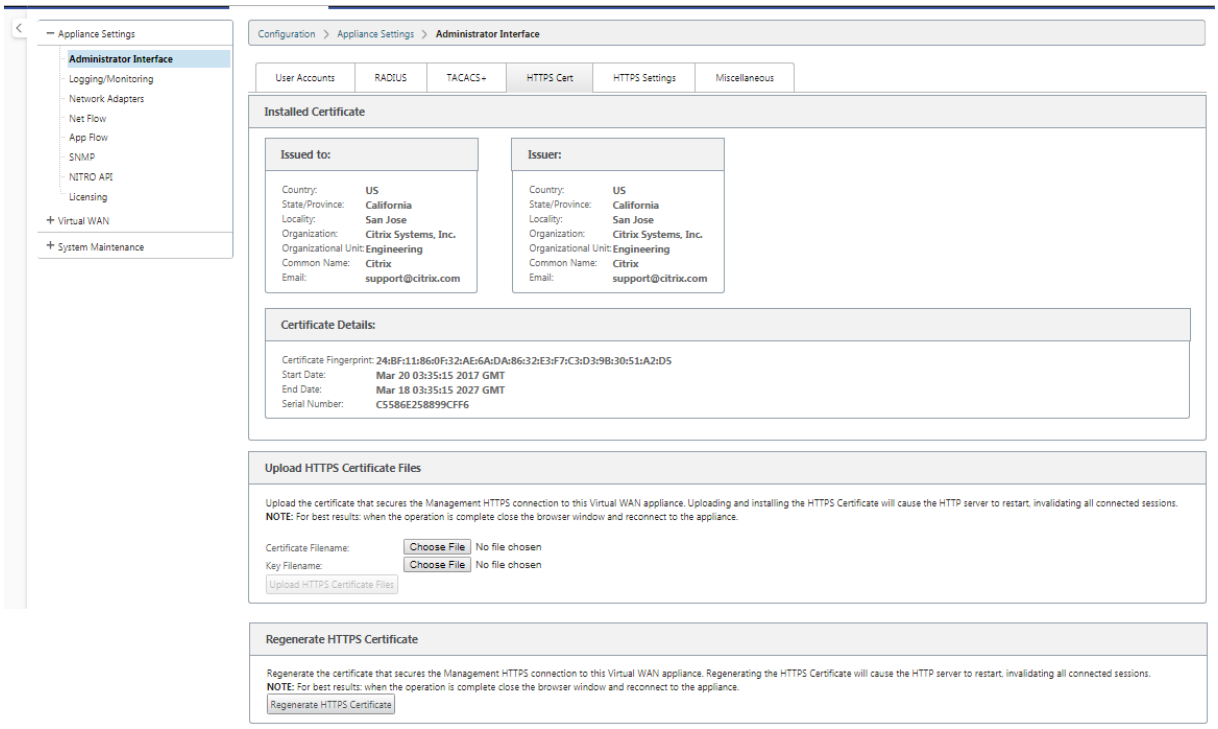
HTTPS 证书：

- 证书

- 键

杂项：

- Web 控制台超时



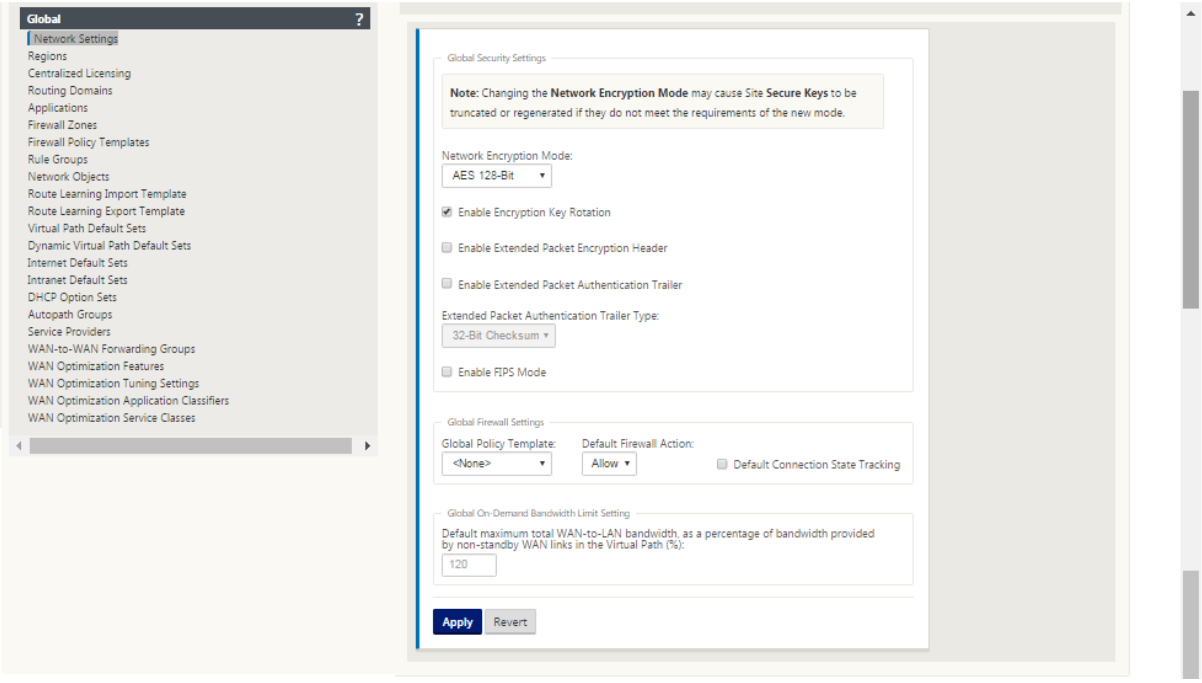
配置编辑器 > 全局 > 网络设置

全局防火墙设置：

- 全局策略模板
- 默认防火墙操作
- 默认连接状态跟踪

全局虚拟路径加密设置：

- AES 128 位（默认值）
- 加密密钥轮换（默认）
- 扩展数据包加密标头
- 扩展数据包认证拖车



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 应用程序防火墙简介。

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

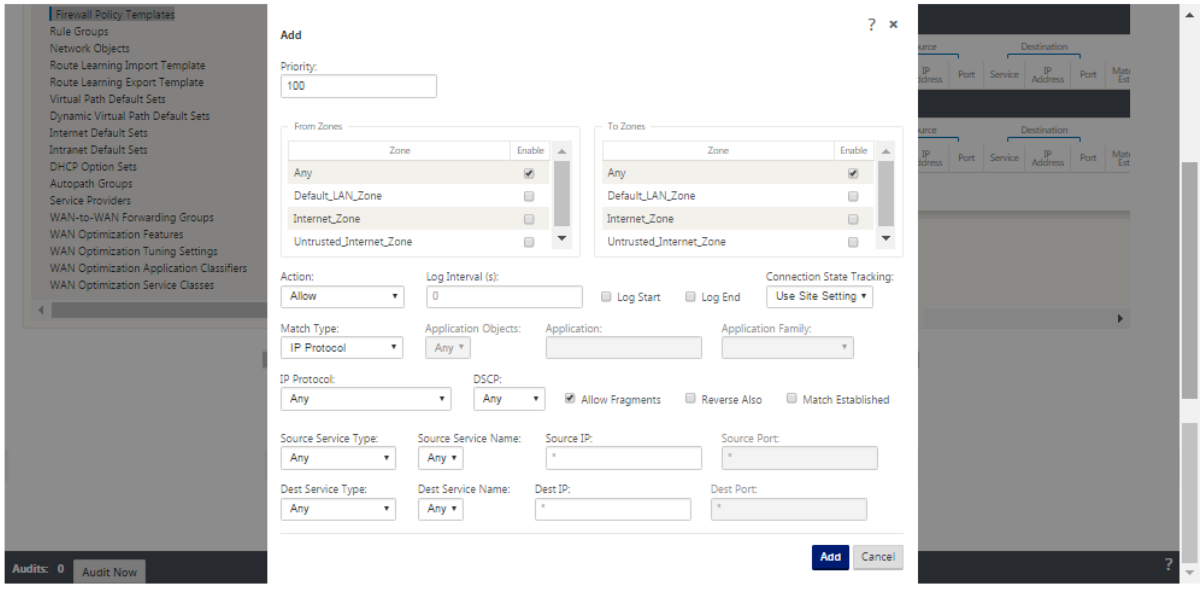
建议的防火墙配置首先使用默认防火墙操作作为全部拒绝，然后添加例外。在添加任何规则之前，记录并查看防火墙规则的用途。尽可能使用状态检查和应用级别检查。简化规则并消除冗余规则。定义并遵守更改管理流程，以跟踪并允许审查对 防火墙 设置的更改。将所有设备的防火墙设置为使用全局设置跟踪通过设备的连接。跟踪连接验证数据包是否正确形成，并且是否适合连接状态。创建适合组织网络或功能区域逻辑层次结构的区域。请记住，区域在全球范围内具有重要意义，可以将不同地理位置的网络视为同一个安全区域。创建最具体的策略，以降低安全漏洞的风险，避免在允许规则中使用任意。配置和维护全局策略模板，为网络中的所有设备创建基本安全级别。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 隧道和 LAN IPsec 隧道。



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。

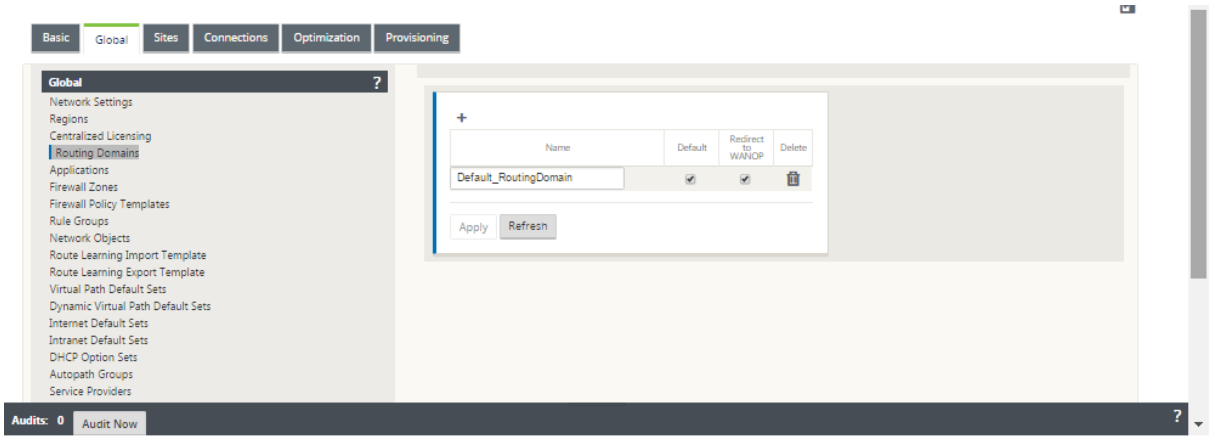
配置编辑器 > 全局

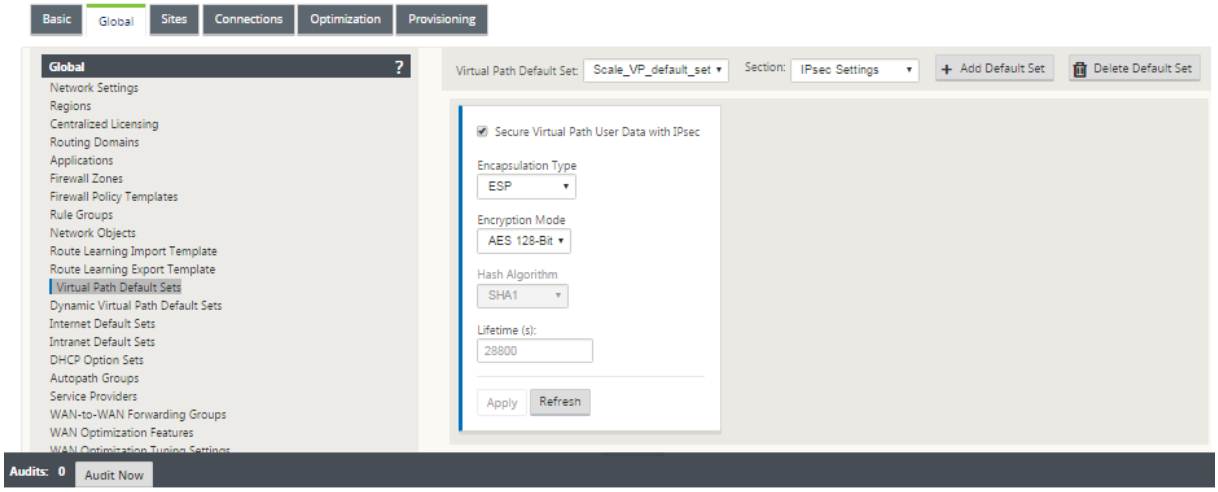
路由域

- Default_RoutingDomain

IPsec 隧道

- 默认集
- 使用 IPsec 保护虚拟路径用户数据





IPsec 隧道

IPsec 隧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 隧道。对于 LAN 上的 IPsec 隧道，必须选择路由域。如果 IPsec 隧道使用 Intranet 服务，则路由域由所选的 Intranet 服务预先确定。

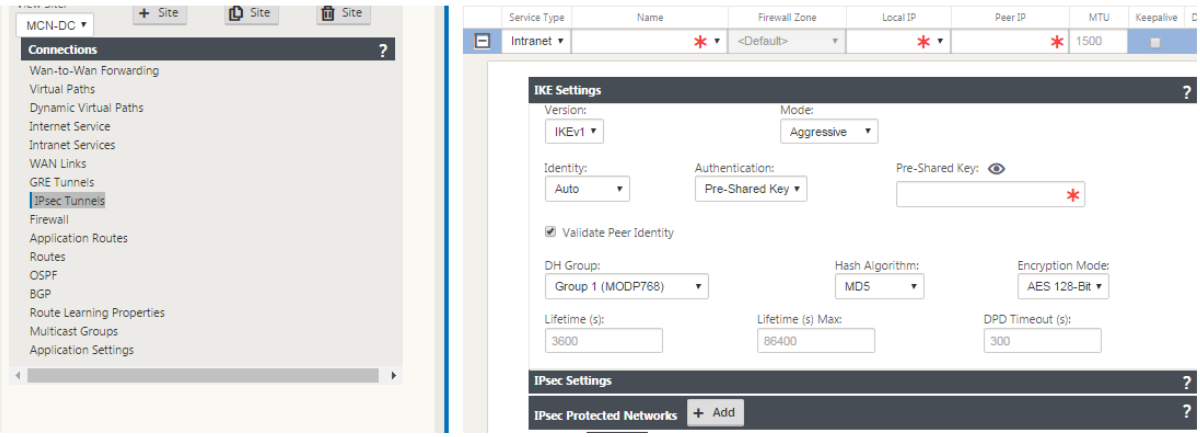
在数据可以通过 SD-WAN 覆盖网络流动之前，跨虚拟路径建立 IPsec 隧道。

- 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

互联网密钥交换 (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

June 22, 2021

本文概述了 Citrix SD-WAN 解决方案的路由最佳实践。

互联网/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、互联网、内联网、直通
- 路线成本

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

June 8, 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

June 22, 2021

Citrix SD-WAN 平台支持多达 8 个公共互联网连接和 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 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 速率。
- 当您不确定带宽并且链接不可靠时，您可以启用 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。
- 如果基础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 检查链接的运行状况/容量。
- 如果 SD-WAN 以 单臂 模式部署，请确保您不会超出基础链路的物理容量。

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

June 22, 2021

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* 软件包从我的当前版本（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?

不会，操作系统软件的更新/升级将通过单步升级 *.zip* 软件包进行处理，并根据您在各自站点的 更改管理设置 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* 软件包从 9.3 升级到 9.3.x，为什么不直接使用 9.3.x 的 *.zip* 软件包?

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。当单步升级 *.zip* 程序包上载到更改管理收件箱时，系统会引发错误，指出无法识别该程序包。因此，首先将 SD-WAN 软件升级到 9.3 或更高版本，然后使用执行更改管理。拉链 包装。

如何通过单步升级安装操作系统组件, 如果.*UPG* 升级不执行?

使用单步升级 *.zip* 软件包完成更改管理后，MCN 将根据设备型号传输/阶段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** ‘，以便即时安装操作系统组件。

> 注意
>
> 只有当设备收到站点所需的所有软件包时才开始安装，即使 维护窗口 值设置为 **0** 也是如此。

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 页面显示默认的调度信息，即 *“”start”：“2016-05-21 21:20:00,”“window”：1,“repeat”：1,“unit”：“days”’*。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 at 21:20:00 (Maintenance window of 1 hour and repeated every 1 day)’*。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？

使用单步升级 *.zip* 包升级到任何更高版本，当当当前的软件版本 9.3.x 或更高版本。

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？

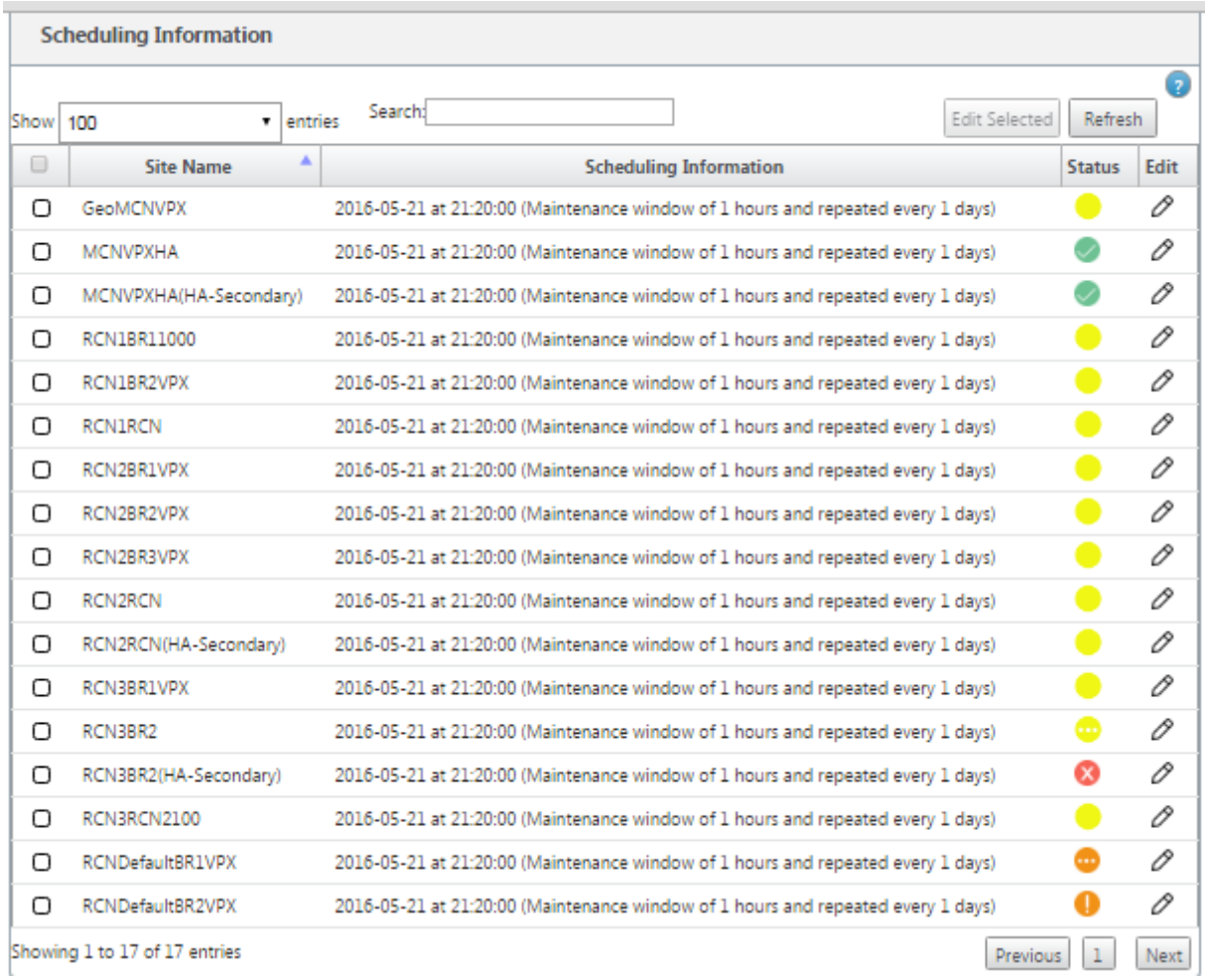
RCN 的计划从 MCN 更改管理设置 页面执行。对于 RCN 分支机构，您需要登录相应的 RCN 并设置计划详细信息。

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。



Scheduling Information

Show 100 entries Search: Edit Selected Refresh

Site Name	Scheduling Information	Status	Edit
GeoMCNVPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
MCNVPXHA(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR11000	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN1RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2BR3VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN2RCN(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3BR2(HA-Secondary)	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCN3RCN2100	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR1VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		
RCNDefaultBR2VPX	2016-05-21 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 days)		

Showing 1 to 17 of 17 entries Previous 1 Next

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，但不建议使用，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。从版本 9.3 版本 1 中，更新操作系统软件 页将折旧。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* 包再次执行更改管理。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?

当当前软件版本为 9.3.x 或更高版本时，请使用单步升级包 *ns-sdw-sw-<release-version>.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。

上载 *ns-sdw-sw-<release-version>.zip* 文件后，我只看到当前软件下的一个平台模型?

从 10.0 版开始，引入了对扩展架构的支持，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。当您选择验证或阶段设备按钮时，会列出/显示/处理其他设备包。

对于 VPX/VPXL/裸机设备，哪些软件包是为 RCN 上演?

软件包被分配到 RCN，因为 RCN 分支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，而分支是需要这些软件包的设备，则 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? 当选择此按钮时，它对尚未完成分段的网站有什么影响?

是的，您可以单击忽略未完成。这将启用下一步按钮，并显示进度栏。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 中转储更新版本的 10.x 版本，并在选定的站点/分支机构的本地更改管理页面激活暂存软件版本。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。用户必须通过在配置 > 更改管理设置页面上启用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 期待从更改管理的激活页面单击“激活暂存”选项。您可以选择通过单击激活暂存按钮激活网络，或单击更改准备以通过接受确认取消状态。

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，如果软件升级与配置同时执行，并且遇到回滚方案，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。

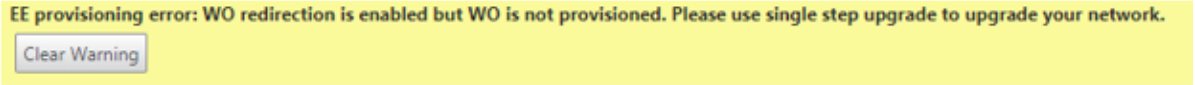
当我有多层网络时，回滚如何与部分软件升级进行交互？

- 如果禁用了部分软件升级，并且如果某个区域（或 RCN）中的站点回滚，则出现问题的区域将回滚，并且回滚完成后将向上载播到 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。

2100 高级版（企业版）

当 2100 EE 设备升级到版本 10.0 时，以下消息指示什么？



设备具有 EE 许可证或从 MCN 启用 WANOP 重定向。您 可以安排 WANOP 组件的安装，以便 在此平台上开始 Provisioning WANOP 功能。

相关信息

- 基于 LTE 的零接触部署
- 在 HA 中配置辅助 MCN

参考资料

June 22, 2021

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。