远程办公场景最佳实践

本文旨在为 IT 管理员和网络安全专家提供 VPN 在企业网络管理中的多样化实际应用指南。通过飞连 VPN 的灵活配置选项，企业可以制定一套贴合特定需求的 VPN 网络解决方案。

**功能概述**

飞连 VPN 管理模块提供了一系列功能，包括 VPN 节点配置、权限管理、访问控制和极速模式设置。通过这些功能，企业可以为员工授权 VPN 使用权限，并控制连接 VPN 后的网络访问权限。飞连 VPN 优化了 VPN 隧道的稳定性和速度，支持一键连接和自动选择最优节点，确保远程办公和云业务系统的安全访问。

**###场景一：出差/居家办公员工远程办公**

**场景介绍**

本场景主要针对企业员工频繁出差且需要远程访问企业内网系统的需求。飞连 VPN 通过简化的客户端操作，仅需点击一键连接，即可轻松完成 VPN 连接，有效解决了这一难题。此外，飞连 VPN 还提供多种二次认证机制，进一步确保了 VPN 接入的安全性。  
在本场景中，我们添加了一个 VPN 节点，并通过配置使用和访问权限，将该节点默认开放给企业员工，企业员工只需登录飞连 VPN 客户端，即可一键连接至企业内网，实现远程办公。

**操作步骤**

1. 登录飞连管理后台。
2. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
3. 在**节点管理**页面的右上角，单击**添加节点**。  
   您需要根据企业实际情况，在飞连管理后台添加 VPN 节点。具体操作，请参见[添加节点](https://www.volcengine.com/docs/6427/158922#%E6%B7%BB%E5%8A%A0%E8%8A%82%E7%82%B9)。如果您已经添加了 VPN 节点，则可以跳过本步骤。
4. 配置极速模式的全局资源。
   1. 在左侧导航栏，选择 **VPN 管理** ＞ **高级配置**。
   2. 在 **VPN 高级配置**页面的**极速模式**区域，单击**新增资源**。
   3. 在**新增资源**界面，根据实际需要配置走 VPN 加密隧道的网络资源，并单击**确定**。  
      您可以选择只配置**域名**或者 **IP 地址**，也可以同时配置。例如，您只需要域名www.example.com走 VPN 加密隧道，则您在静态域名列表中添加www.example.com，并设置域名对应的 IP 列表。
5. 在 **VPN 节点管理**页面，找到已配置的 VPN 节点，单击节点卡片进入节点详情页。
6. 在节点详情页，单击**网络模式**页签，在页面右侧单击**编辑**，完成以下配置，并单击**保存**。

| **配置项** | **说明** |
| --- | --- |
| 网络模式 | 可以选择**全局模式**和**极速模式**。 |
| 极速模式下单节点资源 | 开启**极速模式下单节点资源**开关。  **说明**  开启该开关后，当前 VPN 节点仅使用极速模式单节点资源，而不会使用高级配置中的极速模式全局资源。 |
| 新增资源 | 单击**新增资源**，在右侧**新增资源**界面添加指定的单节点资源，并单击**确定**。 您可以选择只配置**域名**或者 **IP 地址**，也可以同时配置。例如，您只需要域名www.example.com走 VPN 隧道，则您在静态域名列表中添加www.example.com，并设置域名对应的 IP 列表。 |

1. 在左侧导航栏，选择 **VPN 管理** ＞ **使用权限**。
2. 在**使用权限**页签右上角，单击**添加权限**。  
   您需要根据企业实际情况，在飞连管理后台管理 VPN 权限。具体操作，请参见[添加 VPN 使用权限](https://www.volcengine.com/docs/6427/158923)。
3. 在左侧导航栏，选择 **VPN 管理** ＞ **访问权限**。  
   您需要根据企业实际情况，在飞连管理后台管理 VPN 权限。具体操作，请参见[管理 VPN 访问权限](https://www.volcengine.com/docs/6427/158925)。
4. 设置 VPN 访问权限为**默认开放模式**。
5. 在左侧导航栏，选择 **VPN 管理** ＞ **访问权限**。
6. 在 **VPN 访问权限**页面，选择**默认开放模式**。
   1. 如果您是首次配置，则需要在页面内单击**默认开放模式**，并单击**下一步**。  
      在创建网络资源页面，单击**跳出流程**。后续您可以自行添加网络资源以及访问策略。  
      
   2. 如果您之前已创建过网络资源以及访问策略，则需要在页面左上角单击**切换模式**，并在弹出的对话框中选择**默认开放模式**。  
      

**操作结果**

当企业员工通过个人设备登录飞连 VPN 客户端并成功建立连接后，他们便能够访问公司内网资源，实现远程办公。

**###场景二：限制指定部门访问指定资源**

**场景介绍**

本场景主要为了应对小型企业在云上部署业务时面临的网络安全挑战。由于云服务的公网访问特性，企业需要关注来自不同 IP 地址的安全威胁。为此，建议将访问云业务系统的流量通过 VPN 节点进行统一代理转发，从而减少公网对云业务系统的直接暴露，仅允许 VPN 节点的 IP 地址访问，有效提升业务访问的安全性和信任度。  
在本场景中，我们配置了一个 VPN 节点，该节点仅开启极速模式，以提供快速且安全的访问通道。此外，通过设置访问控制策略，可以限制指定部门的员工在连接 VPN 后能够访问的网络资源范围。

**操作步骤**

1. 登录飞连管理后台。
2. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
3. 在**节点管理**页面的右上角，单击**添加节点**。  
   您需要根据企业实际情况，在飞连管理后台添加 VPN 节点。具体操作，请参见[添加节点](https://www.volcengine.com/docs/6427/158922#%E6%B7%BB%E5%8A%A0%E8%8A%82%E7%82%B9)。如果您已经添加了 VPN 节点，则可以跳过本步骤。
4. 配置极速模式的全局资源。
   1. 在左侧导航栏，选择 **VPN 管理** ＞ **高级配置**。
   2. 在 **VPN 高级配置**页面的**极速模式**区域，单击**新增资源**。
   3. 在**新增资源**界面，根据实际需要配置走 VPN 加密隧道的网络资源，并单击**确定**。  
      您可以选择只配置**域名**或者 **IP 地址**，也可以同时配置。例如，您只需要域名www.example.com走 VPN 加密隧道，则您在静态域名列表中添加www.example.com，并设置域名对应的 IP 列表。
5. 设置 VPN 节点仅开启极速模式。
   1. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
   2. 在 **VPN 节点管理**页面，找到已配置的 VPN 节点，单击节点卡片进入节点详情页。
   3. 在节点详情页，单击**网络模式**页签。
   4. 在页面右侧单击**编辑**，并在**网络模式**区域仅选中**极速模式**，并单击**保存**。

**说明**

选中**极速模式**后，页面内会出现**极速模式下单节点资源**开关，本示例场景中不需要开启该开关。如果您开启该开关，则当前 VPN 节点需要设置独立的路由资源，且您在步骤 3 配置的极速模式全局资源不会下发至该 VPN 节点。

1. 配置访问策略，限制指定部门的网络访问权限。
   1. 在左侧导航栏，选择 **VPN 管理** ＞ **访问权限**。
   2. 在 VPN 访问权限页面，将模式配置为**默认开放模式**。
      * 如果您是首次配置，则需要在页面内单击**默认开放模式**，并单击**下一步**。  
        在创建网络资源页面，单击**跳出流程**。后续您可以自行添加网络资源以及访问策略。  
        
      * 如果您之前已创建过网络资源以及访问策略，则需要在页面左上角单击**切换模式**，并在弹出的对话框中选择**默认开放模式**。  
        
   3. 在**网络资源**页签，单击**新增资源**，在**新增资源**对话框，完成以下配置，并单击**确定**。

**说明**

此处创建的网络资源仅用于后续添加访问策略时的资源配置。

| **配置项** | **说明** |
| --- | --- |
| 资源名称 | 自定义名称，用于标识该网络资源。 |
| 资源标签 | 网络资源支持通过标签进行分类，后续在配置访问策略时，您可以通过选择资源标签来批量设置网络资源。 |
| 资源类型 | 选择配置**域名**或者 **IP 地址**。例如，您需要将域名www.example.com添加为网络资源，则您在**资源类型**配置项选择**域名**，并在**域名列表**中添加www.example.com即可。 |
| 协议栈 | 选择域名对应协议，支持选择**全部**、**https** 或者 **http**，或者 IP 地址遵循的协议，支持选择**全部**、**tcp**、**udp** 或者 **icmp**，支持多选。 |
| 域名列表 | * + - 设置该网络资源包含的域名，需要包含端口信息（默认添加 80 和 443 端口），格式示例：www.example.com:80。添加多个域名时需要使用逗号或者空格间隔。     - 设置网络资源所需的端口范围，支持单端口（例如，80）、端口范围（例如，0-65535）。添加多个端口时需要使用逗号或者空格间隔。 |
| 端口列表 | 设置网络资源所需的端口范围，支持单端口（例如，80）、端口范围（例如，0-65535）。添加多个端口时需要使用逗号或者空格间隔。 |

* 1. 在**访问策略**页签，单击**新增策略**，在**新增访问策略**对话框，完成以下配置，并单击**确定**。

| **配置项** | **说明** |
| --- | --- |
| 切换权限 | 单击**切换**，设置**限制员工访问权限**。 |
| 策略名称 | 自定义名称，用于标识该策略。 |
| 选择资源 | 在**选择资源**配置项，选择已创建好的www.example.com网络资源。 |
| 匹配优先级 | 设置为 100。数值越高则策略生效的优先级越高。 |
| 生效对象 | 选择**部门**，并选取指定的部门范围（例如选择A部门）。在部门范围内的成员将是当前策略的生效对象。 |
| 生效时长 | 设置为**永久生效**。 |

**操作结果**

企业内A部门下的员工登录飞连客户端并连接 VPN 后，无法访问www.example.com。其他部门员工登录飞连客户端并连接 VPN 后，可正常访问www.example.com。

**###场景三：允许指定部门访问指定资源**

**场景介绍**

本场景主要为了实现对 VPN 访问权限的精细控制，确保员工仅能访问与其工作职责相关的网络资源，飞连区分了两种 VPN 访问模式：**默认开放模式**和**默认拒绝模式**。

* 默认开放模式是指员工可以访问全部网络资源，配置的访问策略用于限制不可访问的网络资源范围。
* 默认拒绝模式是指员工禁止访问全部网络资源，配置的访问策略用于开放员工可以访问的网络资源范围。

在本场景中，我们选择将 VPN 访问模式设置为**默认拒绝模式**，通过访问策略，我们确保员工在连接 VPN 后只能访问到他们工作所需的特定网络资源。这种模式下，未经授权的访问将被自动阻止，从而有效降低了潜在的安全风险。同时，这种策略也有助于简化网络管理，因为管理员只需定义允许访问的资源，而不是逐一限制每个资源的访问。

**操作步骤**

1. 登录飞连管理后台。
2. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
3. 在**节点管理**页面的右上角，单击**添加节点**。  
   您需要根据企业实际情况，在飞连管理后台添加 VPN 节点。具体操作，请参见[添加节点](https://www.volcengine.com/docs/6427/158922#%E6%B7%BB%E5%8A%A0%E8%8A%82%E7%82%B9)。如果您已经添加了 VPN 节点，则可以跳过本步骤。
4. 为 VPN 的主备 DNS 的 53 端口配置放行的访问策略。  
   在设置默认拒绝模式之前，您需要先添加一个访问策略，放行 VPN 主备 DNS 的 53 端口。否则在设置为默认拒绝模式之后将导致域名资源无法访问。
   1. 在左侧导航栏，选择 **VPN 管理** ＞ **访问权限**。
   2. 单击**网络资源**页签，并单击**新增资源**。
   3. 在**新增资源**对话框，完成以下配置，并单击**确定**。

| **配置项** | **说明** |
| --- | --- |
| 资源名称 | 自定义名称，用于标识该网络资源。 |
| 资源标签 | 网络资源支持通过标签进行分类，后续在配置访问策略时，您可以通过选择资源标签来批量设置网络资源。 |
| 资源类型 | 选择 **IP 地址**。 |
| 协议栈 | 选择域名对应协议，支持选择**全部**、**https** 或者 **http**，或者 IP 地址遵循的协议，支持选择**全部**、**tcp**、**udp** 或者 **icmp**，支持多选。 |
| 域名列表 | IP 列表中添加 VPN 节点下 DNS 主备服务器的 IP 地址。 |
| 端口列表 | 端口列表中添加 53 端口。 |

1. 在 **VPN 访问权限**页面，单击**切换模式**。
2. 在**切换默认模式**对话框，单击**默认拒绝模式**，并单击**确定**。  
   
3. 添加放行的访问策略。  
   当 VPN 的访问模式切换为**默认拒绝模式**后，默认情况下员工无法访问任何网络资源，您需要根据企业实际需求添加访问策略放行指定的网络资源。后续员工通过 VPN 连接企业内网后即可访问策略生效范围内的网络资源。
   1. 在 **VPN 访问权限**页面，单击**网络资源**页签，在页签内单击**新增资源**。
   2. 在**新增资源**对话框，配置网络资源，并单击**确定**。

| **配置项** | **说明** |
| --- | --- |
| 资源名称 | 自定义名称，用于标识该网络资源。 |
| 资源标签 | 网络资源支持通过标签进行分类，后续在配置访问策略时，您可以通过选择资源标签来批量设置网络资源。 |
| 资源类型 | 选择配置**域名**或者 **IP 地址**。例如，您需要将域名www.example.com添加为网络资源，则您在**资源类型**配置项选择**域名**，并在**域名列表**中添加www.example.com即可。 |
| 协议栈 | 选择域名对应协议，支持选择**全部**、**https** 或者 **http**，或者 IP 地址遵循的协议，支持选择**全部**、**tcp**、**udp** 或者 **icmp**，支持多选。 |
| 域名列表 | * + - 设置该网络资源包含的域名，需要包含端口信息（默认添加 80 和 443 端口），格式示例：www.example.com:80。添加多个域名时需要使用逗号或者空格间隔。     - 设置网络资源所需的端口范围，支持单端口（例如，80）、端口范围（例如，0-65535）。添加多个端口时需要使用逗号或者空格间隔。 |
| 端口列表 | 设置网络资源所需的端口范围，支持单端口（例如，80）、端口范围（例如，0-65535）。添加多个端口时需要使用逗号或者空格间隔。 |

* 1. 在 **VPN 访问权限**页面，单击**访问策略**页签，在页签内单击**新增策略**。
  2. 在**新增访问策略**对话框，完成以下配置，并单击**确定**。

| **配置项** | **说明** |
| --- | --- |
| 切换权限 | 单击**切换**，设置**授予员工访问权限**。 |
| 策略名称 | 自定义**策略名称**。 |
| 选择资源 | 在**选择资源**下拉列表，选择需要放行的www.example.com网络资源。 |
| 匹配优先级 | 设置为 100。数值越高则策略生效的优先级越高。 |
| 生效对象 | 选择**部门**，并选取指定的部门范围（例如选择A部门）。在部门范围内的成员将是当前策略的生效对象。 |
| 生效时长 | 设置为**永久生效**。 |

**操作结果**

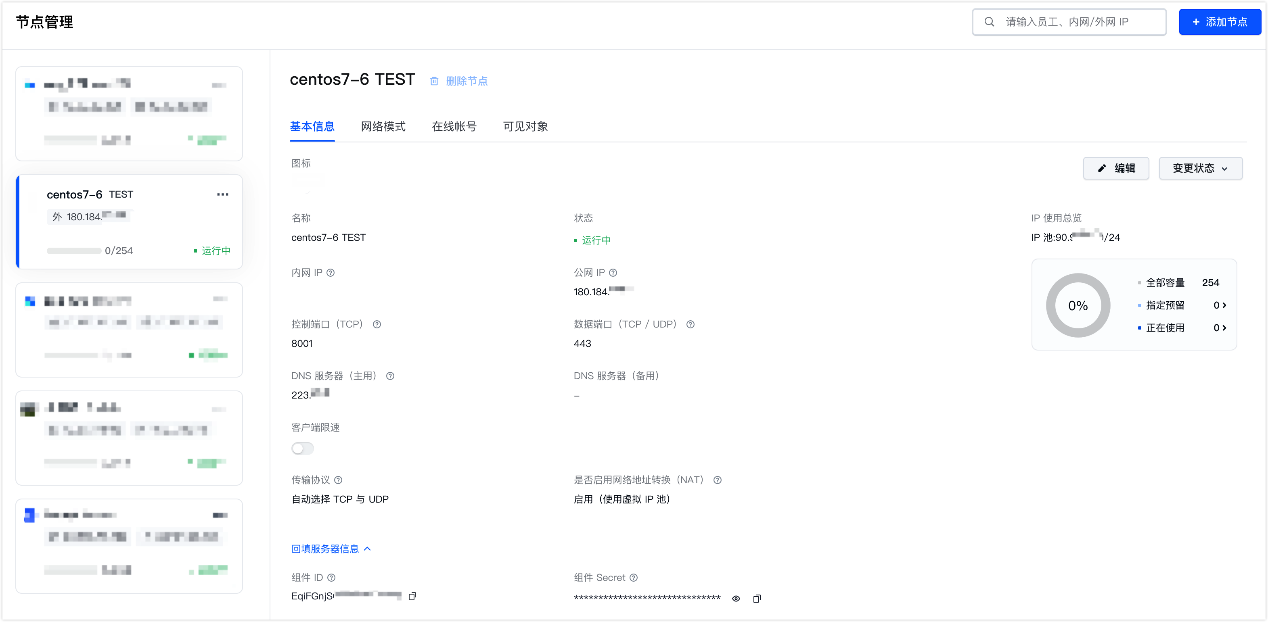
企业内A部门下的所有员工登录飞连客户端并连接 VPN 后，可访问www.example.com。其他部门的员工登录飞连客户端并连接 VPN 后，无法访问网络资源。

**###场景四：不同部门/员工使用不同 VPN 节点**

**场景介绍**

本场景主要为了解决企业在部署多个飞连 VPN 节点时面临的权限管理问题。由于不同节点具有不同的用途，企业希望实现对员工访问权限的精确控制，确保员工只能连接到与其工作职责相关的 VPN 节点，而其他节点则对其不可见。  
在本场景中，我们通过飞连 VPN 的管理功能，为每个部门、员工或角色配置了相应的 VPN 节点访问权限。如果您购买了多个 VPN 节点配额，则可以在 VPN 管理功能中添加这些节点。当员工使用飞连客户端连接 VPN 时，他们可以从多个节点中选择适合自己的节点进行连接。

**操作步骤**

1. 在飞连管理后台，添加多个 VPN 节点。  
   具体的配置操作，请参见[场景一：出差/居家办公员工远程办公](https://www.volcengine.com/docs/6427/1277476#412e1e32)。您需要重复场景一中的操作创建多个 VPN 节点。
2. 在飞连管理后台，设置节点可见策略。  
   具体的配置操作，请参见[配置 VPN 节点的可见对象](https://www.volcengine.com/docs/6427/486945)。
3. 检查并确保各个 VPN 节点的运行状态均为运行中。
   * 在 **VPN 管理** ＞ **节点管理**页面，查看各个节点运行状态。  
     
   * 在**集成管理** ＞ **组件管理**页面，查看 VPN 组件的运行状态。  
     

**操作结果**

企业员工登录飞连客户端，在连接 VPN 时支持选择不同的节点进行连接。即使有 VPN 节点出现故障导致连接超时，员工也可以选择其他正常运行的 VPN 节点进行连接。

**###场景五：为 VPN 节点配置独立极速模式单节点资源**

**场景介绍**

本场景主要为了展示如何在飞连 VPN 管理中为特定 VPN 节点配置独立的极速模式单节点资源。这种配置允许特定 VPN 节点访问特定的网络资源，而不是全局资源，从而实现更精细化的网络资源管理和优化。  
在本场景中，我们将详细介绍如何为 VPN 节点配置独立的极速模式单节点资源。通过遵循本场景中的操作步骤，您可以为多个 VPN 节点进行类似的配置，以实现每个节点的最优性能和资源访问。例如，如果您有两个 VPN 节点，您可以按照以下示例配置，实现每个节点访问特定网络资源的目的。以下是两个 VPN 节点的示例配置以及最终效果的说明：

| **VPN 节点** | **示例配置** | **最终效果** |
| --- | --- | --- |
| 节点 A | * 开启极速模式 * 将域名 A 添加为极速模式单节点资源 | 员工在飞连客户端选择节点 A 进行 VPN 连接，即可通过企业内网流量访问域名 A。 |
| 节点 B | * 开启极速模式 * 将域名 B 添加为极速模式单节点资源 | 员工在飞连客户端选择节点 B 进行 VPN 连接，即可通过企业内网流量访问域名 B。 |

**操作步骤**

1. 登录飞连管理后台。
2. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
3. 在**节点管理**页面的右上角，单击**添加节点**。  
   您需要根据企业实际情况，在飞连管理后台添加 VPN 节点。具体操作，请参见[添加节点](https://www.volcengine.com/docs/6427/158922#%E6%B7%BB%E5%8A%A0%E8%8A%82%E7%82%B9)。如果您已经添加了 VPN 节点，则可以跳过本步骤。
4. 在左侧导航栏，选择 **VPN 管理** ＞ **节点管理**。
5. 在 **VPN 节点管理**页面，找到已配置的 VPN 节点，单击节点卡片进入节点详情页。
6. 在节点详情页，单击**网络模式**页签，在页面右侧单击**编辑**，完成以下配置，并单击**保存**。

| **配置项** | **说明** |
| --- | --- |
| 网络模式 | 仅选择**极速模式**。 |
| 极速模式下单节点资源 | 开启**极速模式下单节点资源**开关。  **说明**  开启该开关后，当前 VPN 节点仅使用极速模式单节点资源，而不会使用高级配置中的极速模式全局资源。 |
| 新增资源 | 单击**新增资源**，在右侧**新增资源**界面添加指定的单节点资源，并单击**确定**。 您可以选择只配置**域名**或者 **IP 地址**，也可以同时配置。例如，您只需要域名www.example.com走 VPN 隧道，则您在静态域名列表中添加www.example.com，并设置域名对应的 IP 列表。 |

**操作结果**

员工必须通过飞连客户端连接至指定的 VPN 节点，将通过 VPN 加密隧道才能访问www.example.com资源。若连接至非指定的 VPN 节点，将无法访问该资源。