**路特斯科技有限公司**

数据防泄漏项目

Azure ESG\_S2S站点部署SOP

**苏州璞泰信息科技有限公司**

2022年4月

**目 录**

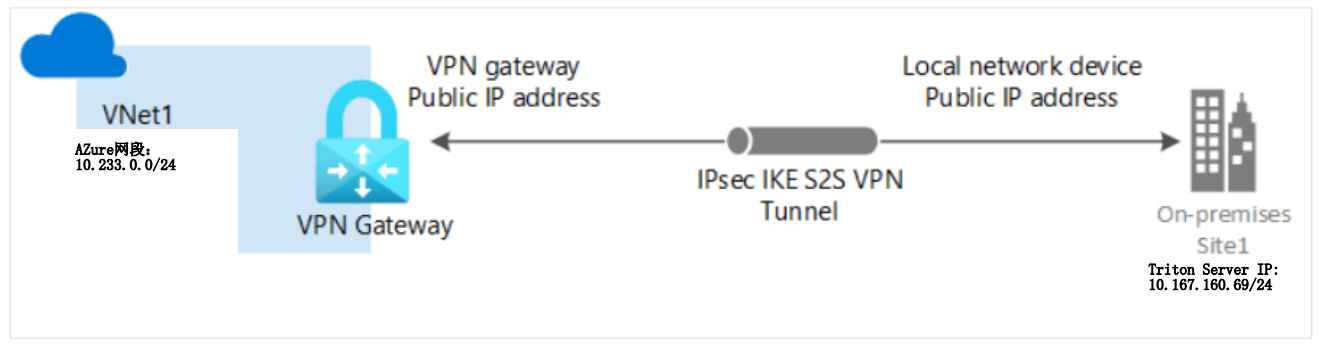
[1. 部署背景 2](#_Toc101901636)

[2. Azure 配置 4](#_Toc101901637)

[3. 百度私有云IPSecVPN设备配置 9](#_Toc101901638)

[4. 联系我们 12](#_Toc101901639)

## 部署背景



DLP Triton Server 10.167.160.69/24需与Azure 上服务器所在10.233.0.0/24网段建立内网

路特斯端 使用百度私有云品台产品，非硬件设备 与Azure 建立ipsec vpn，使用基于路由的vpn。

双方公网信息：IDC: 115.236.146.52 Azure : 20.239.65.147

内网互访信息：IDC: 10.167.160.69/24 Azure : 10.233.0.0/24

预共享密钥：Lotus@DLP2022 IKE版本v2

Azure VPN配置

第一阶段

! [6] Phase 1/Main Mode:

! IKE encryption algorithm

! IKE hashing algorithm

! IKE Diffie-Hellman group

! IKE SA lifetime (seconds)

! IKE SA data size (Kilobytes)

/Data/IKE\_ENCRYPTION\_1 = aes256

/Data/IKE\_INTEGRITY\_1 = sha2-256

/Data/IKE\_DHGROUP\_1 = group2

/Data/IKE\_SALIFETIME\_1 = 28800

第二阶段

! [7] Phase 2/Quick Mode:

! IPsec encryption algorithm

! IPsec hashing algorithm

! PFS Group (Perfect Forward Secrecy)

! IPsec SA (QMSA) lifetime (seconds)

/Data/IPsec\_ENCRYPTION\_1 = 3des

/Data/IPsec\_INTEGRITY\_1 = sha2-256

/Data/IPsec\_PFSGROUP\_1 = None

/Data/IPsec\_SALIFETIME = 3600

! [8] Connection pre-shared key

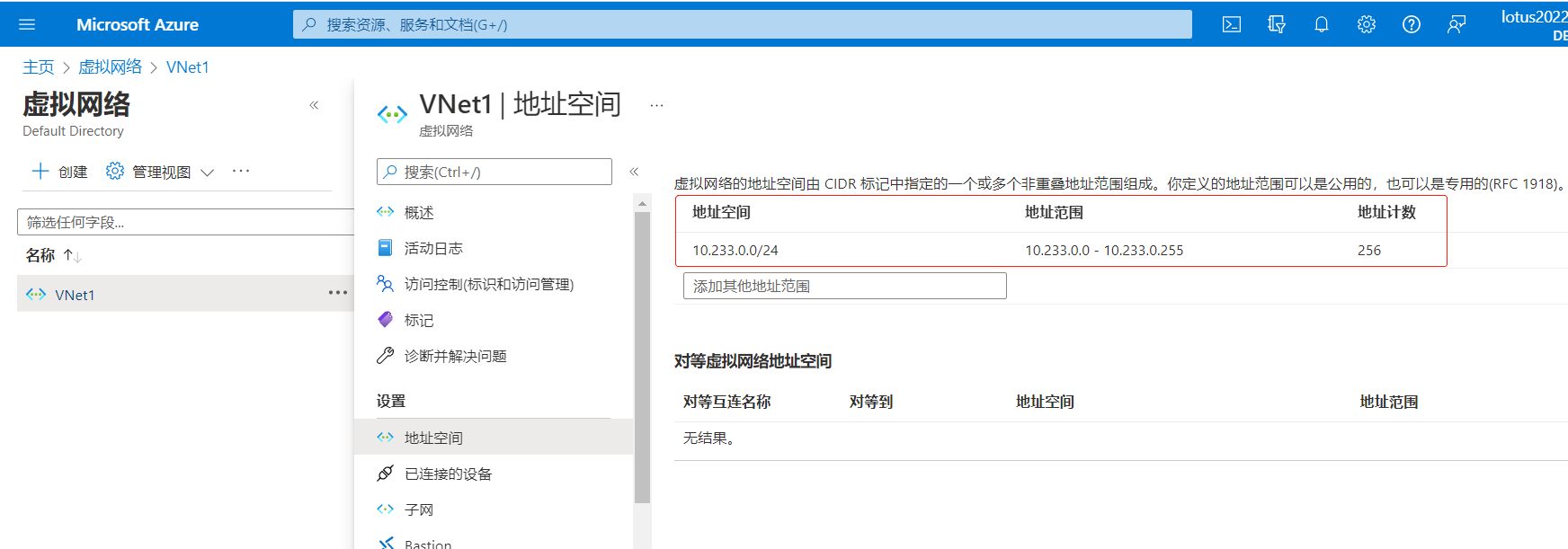
/Data/CONNECTION\_PSK = Lotus@DLP2022

## Azure 配置

1. 登录<https://portal.azure.com/#home>



1. 在“搜索资源、服务和文档(G+/)”中，键入“虚拟网络”。

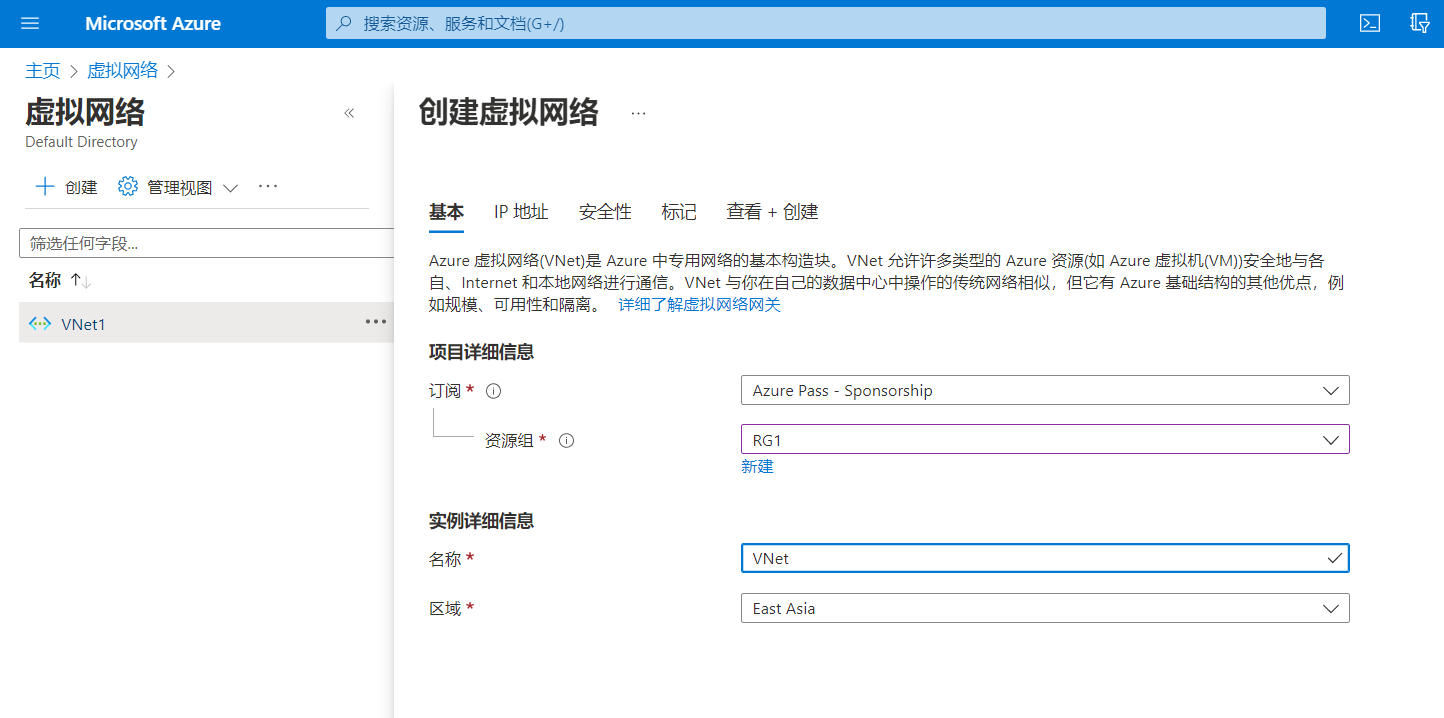


1. 从“市场”结果中选择“虚拟网络”，在“虚拟网络”页上选择“创建”。

在“基本信息”选项卡上，配置“项目详细信息”和“实例详细信息”VNet 设置。

资源组：选择“新建”，名称为“RG1”

名称：实例名称为“VNet1”



1. 在“IP 地址”选项卡上配置值。 根据所需的设置调整这些值。

IPv4地址空间范围：10.233.0.0/24

**子网不添加即使用默认IPv4地址空间范围**



1. 安全性和标记保持默认选项，验证完成后创建完成虚拟网络。
2. 从Azure 门户，搜索资源、服务和文档（G+/）类型的**虚拟网络网关**。在搜索结果中找到虚拟网络网关并将其选中。
3. 在“基本”选项卡上，填写虚拟网络网关的值。

名称：“VNet1GW”

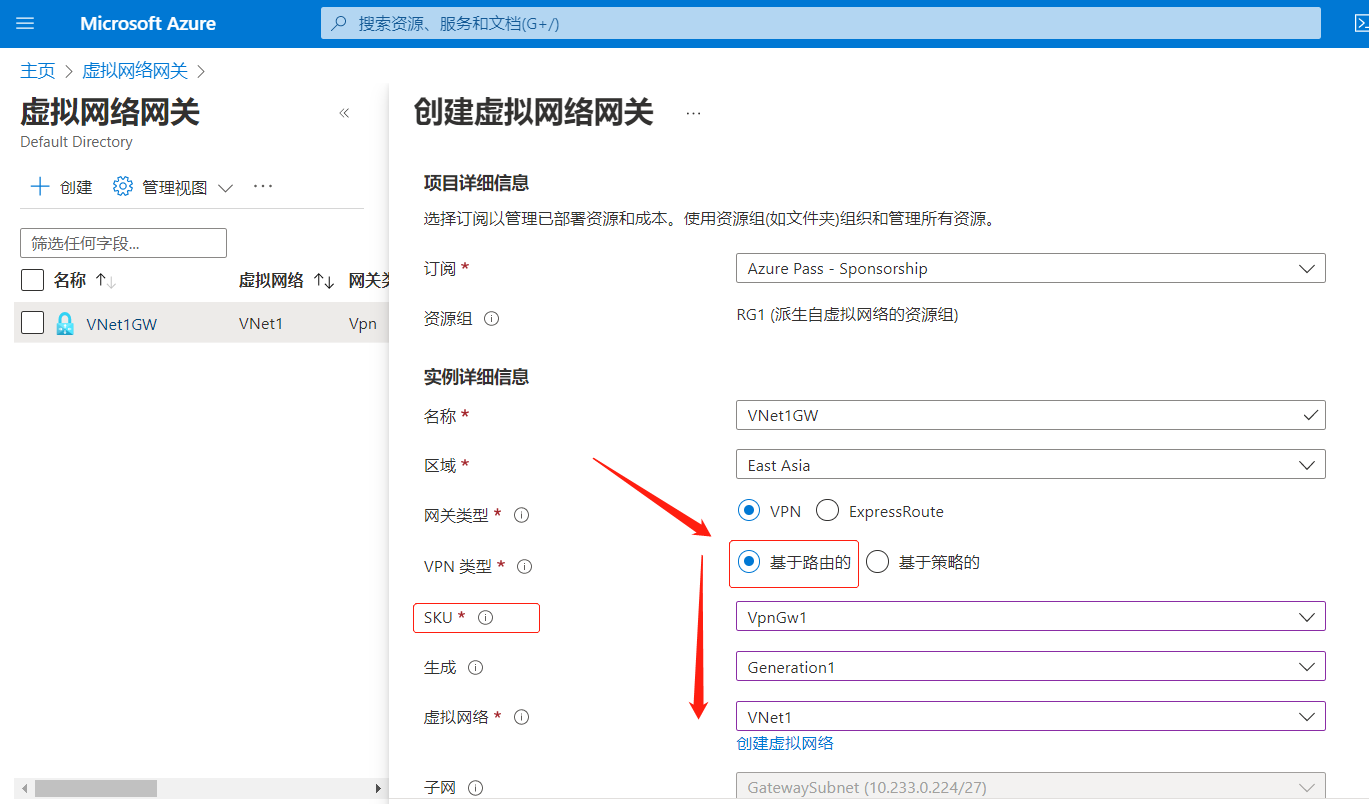
网关类型：“VPN”

VPN类型：“基于路由的”

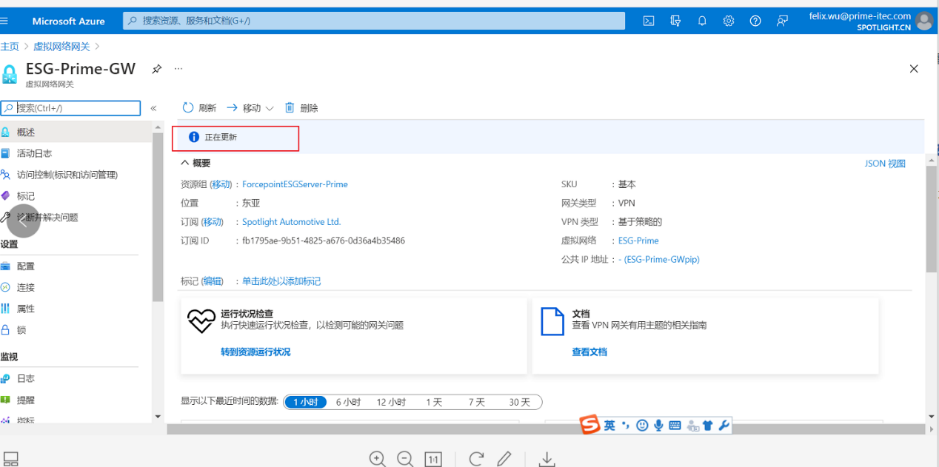
虚拟网络：下拉框中选择之前创建的VNet1

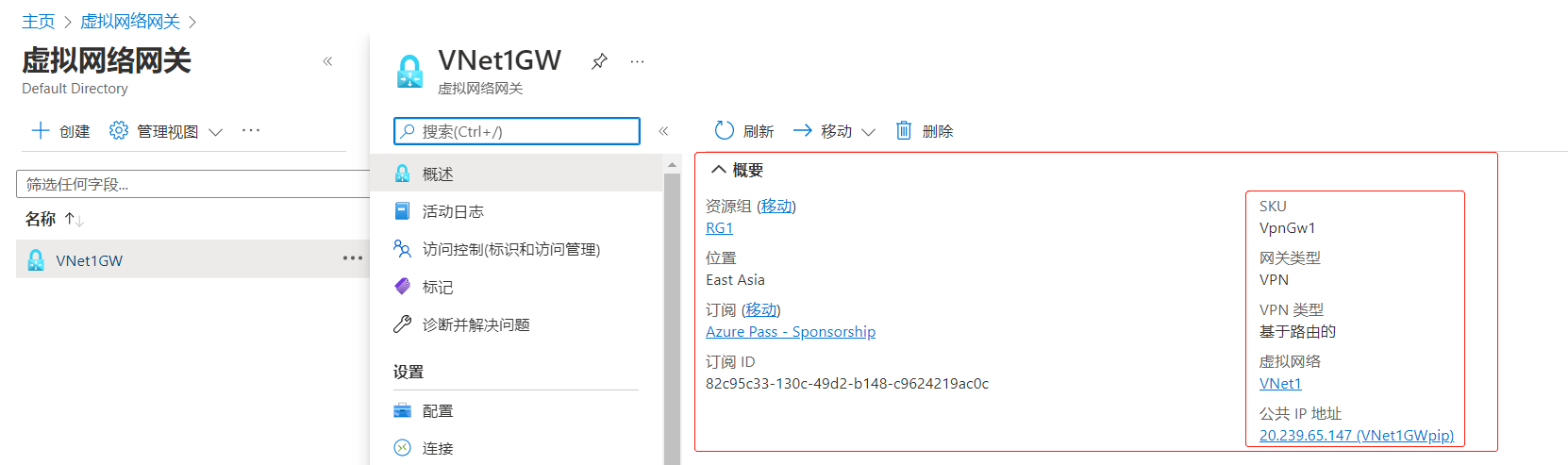
公共IP地址：选择“新建”

公共IP地址名称：“VNet1GWpip”



1. 选择“查看+创建”，确认后，点击“创建”，耗时较长，需要等待几十分钟。可以进入创建的虚拟网关的“概述”中，查看状态，如果是“正在更新”，则说明还在创建中。





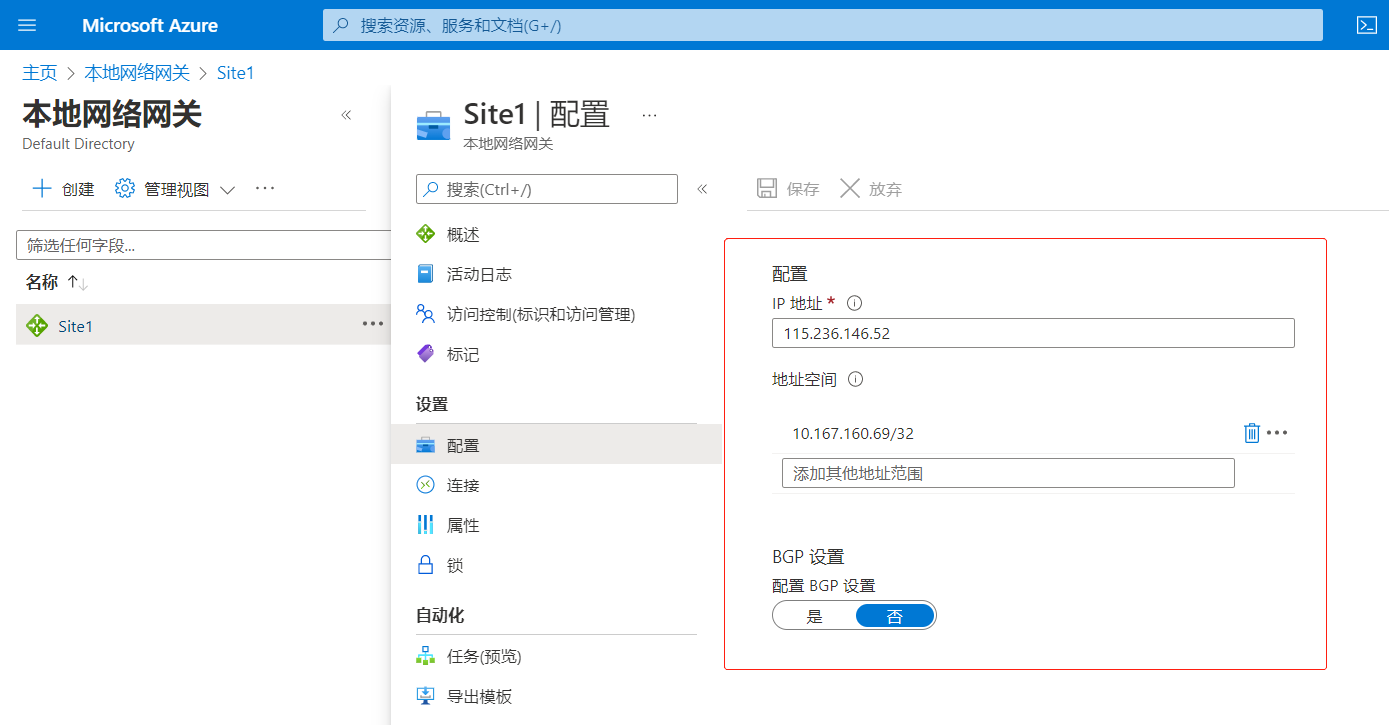
1. 在 Azure 门户的“搜索资源、服务和文档(G+/)”中，键入“本地网关” 。 在搜索结果中找到“市场”下的“本地网关”，并选择它 。 此操作将打开“创建本地网关”页。
2. 在“创建本地网络网关”页上，指定本地网络网关的值 。

资源组：选择之前创建的“RG1”

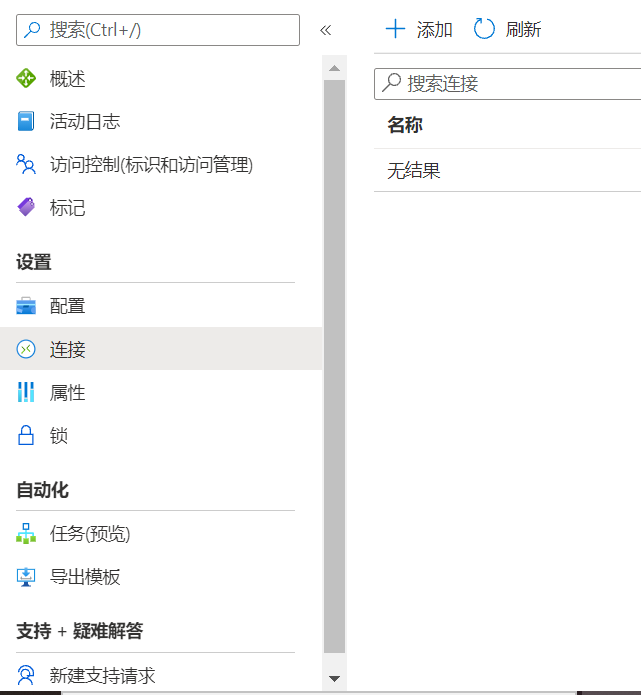
名称：“Site1”

终结点：选择IP地址

IP地址：输入本地防火墙的公网IP地址



1. 选择“查看+创建”，确认后，点击“创建”即可创建完成本地网关
2. 打开虚拟网络网关的页面。 可通过转到你的 VNet 名称 ->“概述”->“已连接的设备”-> 你的网关名称来导航到网关（但也可以通过多种其他方法进行导航，也可以选择本地网关进行配置）。
3. 在网关的页面上，选择“连接”。 在“连接”页的顶部，选择“+添加”打开“添加连接”页。



1. 在“添加连接”页上，配置连接的值。

名称：“VNet1ToSite1”

连接类型：“站点到站点”

虚拟网络网关：选择VNet1GW

本地网络网关：选择Site1

共享密钥：输入防火墙对端配置的密码

IKE协议根据实际情况填写。

其余保持默认，点击“确定”，完成创建。





## 百度私有云IPSecVPN设备配置

1. 配置一阶段





1. 配置二阶段。
2. 配置对端网关。
3. 配置gateway。
4. 配置静态路由。
5. 配置安全策略。



1. 配置交换机路由

核心配置路由 ip route

## 联系我们

苏州璞泰信息科技有限公司

中国·苏州市工业园区东旺路18号N度空间A座2楼

电话：0512-62816238