网络云服务 - 虚拟专用网络

前言

- 本章主要讲述华为云服务中网络服务的虚拟专用网络（VPN）产品。

目标

- 学完本课程后，您将能够：
  - 了解VPN服务中的概念
  - 使用VPN的场景
  - 如何使用VPN

目录

VPN基本概念

- 虚拟专用网络即VPN（Virtual Private Network），用于在远端用户和虚拟私有云（VPC）之间建立一条安全加密的通信隧道。当您作为远端用户需要访问VPC的业务资源时，您可以通过VPN连通VPC。

VPN网关基本概念

- VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。

VPN连接基本概念

- VPN连接是一种基于Internet隧道技术，可帮您快速构建VPN网关和用户网关之间的安全、可靠的加密通道。当前VPN连接支持IPsec VPN协议。

VPN的分类

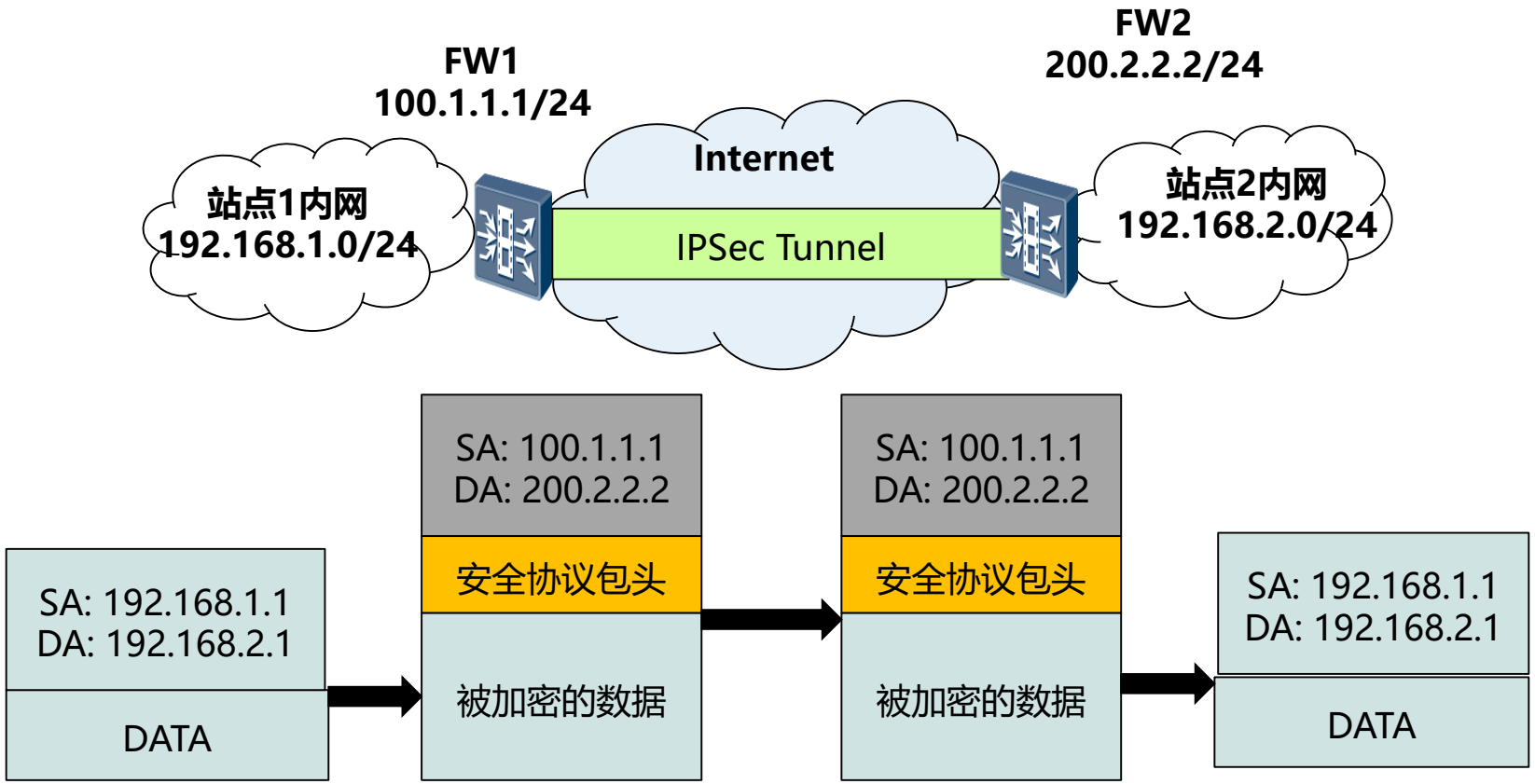
- 按业务用途分类
  - Access VPN

    远程拨入VPN，可以提供员工出差时的远程VPN拨入服务。
  - Intranet VPN

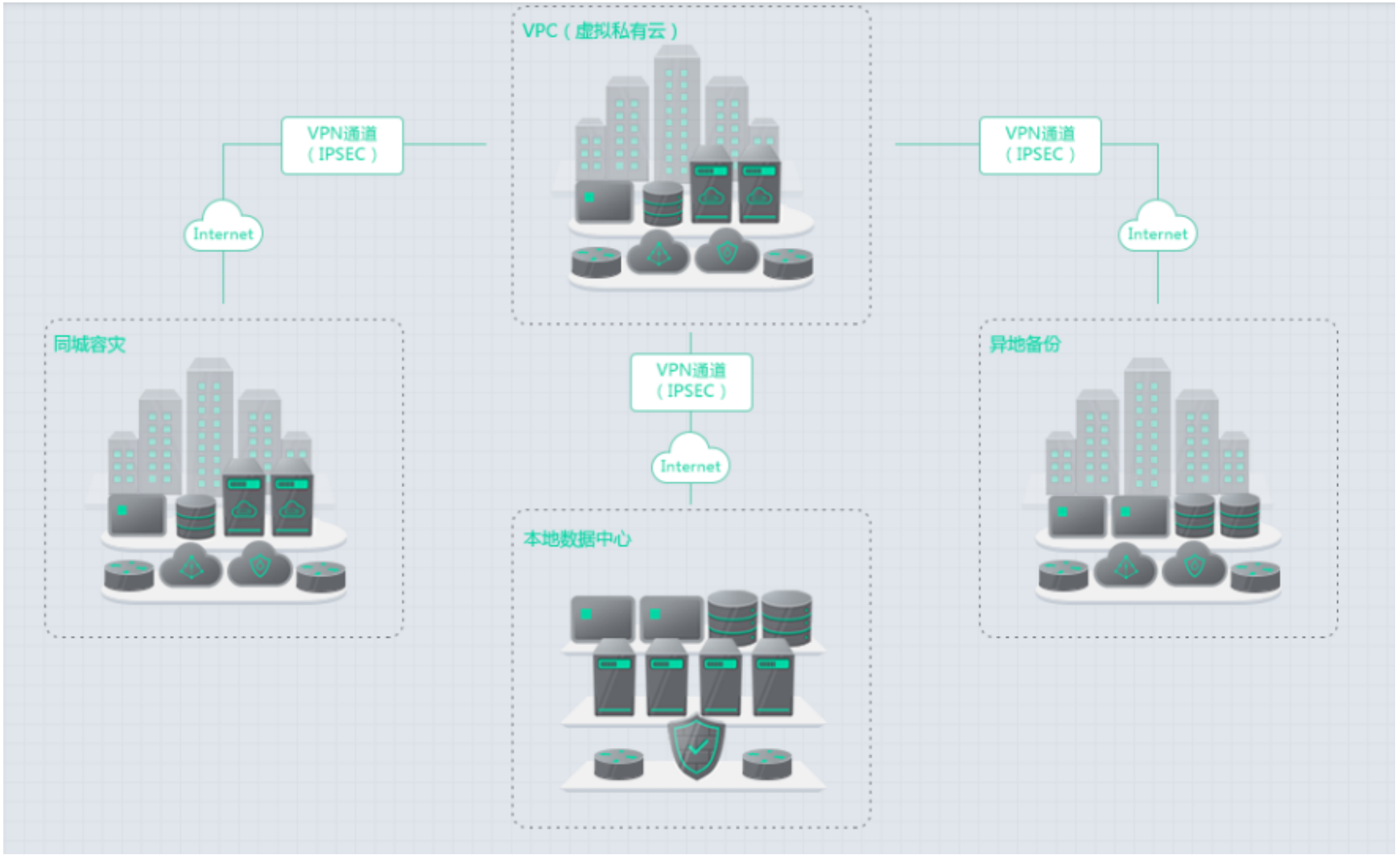
    这种VPN是利用VPN技术，实现在公网上使该企业的不同站点或办事处之间的私有通信。
  - Extranet VPN

    这种VPN实现企业内部网络与合作伙伴或授权机构之间的虚拟专用网络。

IPSec VPN示例



产品架构



计费

- 华为云VPN提供按量付费（按小时）的后付费购买方式，不用提前预估使用时长，灵活使用。
- 计费模式：按需计费
- 计费公式：VPN连接数使用费+公网带宽使用费
- VPN连接默认不包含公网带宽，需额外购买。

目录

VPN快速入门

- VPN快速入门流程
  - 购买VPN网关
  - 购买VPN连接

购买VPN网关 (1/4)

- 购买VPN网关流程：
  - 注册并登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
  - 在“VPN网关”界面，单击“购买VPN网关”。
  - 根据界面提示配置参数，并单击“立即购买”。
  - 阅读并勾选服务协议后，单击“提交”。

购买VPN网关 (2/4)

购买VPN网关 (3/4)

- 购买VPN网关参数配置：

参数	说明	取值样例
计费模式	VPN网关支持按需计费。 按需计费网关费用分为网关配置费用以及带宽使用费用。	按需计费
区域	区域指VPN网关所在的物理位置。	华北-北京一
虚拟私有云	VPN接入的VPC名称。	vpc-001
名称	VPN网关名称。	vpngw-001
类型	VPN类型。默认为选择“IPsec”。	IPsec
可靠性	当前环境下仅支持“单活”。 单活即一个VPN网关对应一个IP地址，不支持主备模式。	单活

购买VPN网关 (4/4)

- 购买VPN网关参数配置：

参数	说明	取值样例
计费方式	支持两种计费方式：按带宽计费/按流量计费 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。	按流量计费
带宽大小	本地VPN网关的带宽大小（单位Mbit/s），为所有基于该网关创建的VPN连接共享的带宽，VPN连接带宽总和不超过VPN网关的带宽。 • 在VPN使用过程中，当网络流量超过VPN带宽时有可能造成网络拥塞导致VPN连接中断，请用户提前做好带宽规划。 • 可以在CES监控中配置告警规则对带宽进行监控。	100
描述	VPN网关的描述信息	-

购买VPN连接 (1/2)

- 购买VPN连接流程：
  - 注册并登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
  - 在“VPN连接”界面，单击“购买VPN连接”。
  - 根据界面提示配置参数，并单击“立即购买”。
  - 阅读并勾选服务协议后，单击“提交”。
  - 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行IPSec VPN隧道配置。

购买VPN连接 (2/2)

购买VPN连接 (1/6)

- 购买VPN连接参数配置：

参数	说明	取值样例
计费模式	VPN连接支持按需计费。	按需计费
区域	区域指虚拟私有云所在的物理位置。同一区域内可用分区间内网互通，不同区域间内网不互通。	华北-北京一 -
名称	VPN连接名称。	vpn-001
VPN网关	VPN连接挂载的VPN网关名称	vpcgw-001
本端子网	VPC内需要与您的数据中心或者私有网络互通的子网。支持以下方式设置本端子网 •选择子网 •手动输入网段	192.168.1.0/24, 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-

购买VPN连接 (2/6)

- 购买VPN连接参数配置：

参数	说明	取值样例
远端子网	您的数据中心或私有网络中需要与VPC通信的子网地址。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段重合。	192.168.3.0/24, 192.168.4.0/24
预共享密钥	预共享密钥（Pre Shared Key），取值范围为6～128位。此项配置在VPC的VPN和您的数据中心的VPN中，配置需要一致。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	•默认配置 •自定义配置：自定义配置IKE策略和IPsec策略。	自定义配置

购买VPN连接 (3/6)

- 购买VPN连接IKE策略参数配置：

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：sha1、sha2-256、sha2-384、sha2-512、md5。 默认配置为：sha1。	sha1
加密算法	加密算法，支持的算法：aes-128、aes-192、aes-256、3des（有安全风险不推荐）。 默认配置为：aes-128。	aes-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法：group2，group5，group14。 默认配置为：group5。 协商双方的dh算法必须一致，否则会导致协商失败。	group5
版本	IKE密钥交换协议版本，支持的版本：v1、v2。 默认配置为：v1。	v1

购买VPN连接 (4/6)

- 购买VPN连接IKE策略参数配置：

参数	说明	取值样例
生命周期（秒）	安全联盟（SA—Secuity Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400
协商模式	选择IKE策略版本未“v1”时，可以配置协商模式，取值支持main、aggressive。 默认配置为：main	main

购买VPN连接 (5/6)

- 购买VPN连接Ipsec Policy策略参数配置：

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法：sha1、sha2-256、sha2-384、sha2-512、md5。 默认配置为：sha1。	sha1
加密算法	加密算法，支持的算法：aes-128、aes-192、aes-256、3des（有安全风险不推荐） 默认配置为：aes-128。	aes-128
DH算法	Diffie-Hellman密钥交换算法，开启该功能后会在二阶段协商时再次进行dh密钥交换，可以提高密钥的安全性。支持的算法：group2，group5，group14等。 协商双方的dh算法必须一致，否则会导致协商失败。 默认配置为：group5。	group5

购买VPN连接 (6/6)

- 购买VPN连接Ipsec Policy策略参数配置：

参数	说明	取值样例
传输协议	IPSec传输和封装用户数据时使用的安全协议，目前支持的协议：ah、esp、ah-esp。 默认配置为：esp。	esp
生命周期（秒）	安全联盟（SA—Secuity Associations）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

目录

VPN的使用管理

- 查看已购买的VPN网关
- 修改已购买的VPN网关
- 删除VPN网关
- 查看已购买的VPN连接
- 修改已购买的VPN连接
- 删除VPN连接

查看已购买的VPN网关

- **操作场景**
  - 用户购买VPN网关后，可以查看已购买的VPN网关。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
  - 在“VPN网关”界面，即可看到已购买的VPN网关。

修改已开通的VPN网关

- **操作场景**
  - 当购买的VPN网关信息需要根据最新网络环境调整时，可通过修改VPN网关的方式进行调整。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
  - 在所需修改的VPN网关所在行，单击“修改”。
  - 根据界面提示配置参数，单击“确定”。

删除VPN网关

- **操作场景**
  - 当无需使用VPN网络时，可删除VPN网关。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN网关”。
  - 在所需删除的VPN网关所在行，单击“删除”。

查看已购买的VPN连接

- **操作场景**
  - 用户购买VPN连接后，可以查看已购买的VPN连接。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
  - 在“VPN网关”界面，即可看到已购买的VPN连接。

修改已开通的VPN连接

- **操作场景**
  - 当购买的VPN连接信息需要根据最新网络环境调整时，可通过修改VPN连接的方式进行调整。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
  - 在所需修改的VPN连接所在行，单击“修改”。
  - 根据界面提示配置参数，单击“确定”。

删除VPN连接

- **操作场景**
  - 当无需使用VPN网络时，可删除VPN连接。
- **操作步骤**
  - 登录管理控制台。
  - 在系统首页，单击“网络 > 虚拟专用网络”。
  - 在左侧导航栏选择“虚拟专用网络 > VPN连接”。
  - 在所需删除的VPN连接所在行，单击“删除”。

目录

VPN常见问题 (1/3)

- VPN支持哪些类型?
  - 当前仅支持IPSec VPN。
- 一个用户支持多少个VPN连接?
  - 每个账号默认最多申请2个VPN网关。
  - 每个账号默认2个VPN连接，可申请配额扩容至20个。如需更多连接数需咨询管理员方案。
- IPSec VPN是否会自动协商?
  - 支持自动协商。

VPN常见问题 (2/3)

- 为什么VPN连接成功后状态显示未连接?
  - VPN对接成功后两端的服务器或者虚拟机之间需要进行通信，VPN的状态才会刷新为正常。
  - IKE v1版本：如果VPN连接经历了一段无流量的空闲时间，则需要重新协商。协商时间取决于IPsec Policy策略中的“生命周期（秒）”取值。“生命周期（秒）”取值一般为3600（1小时），会在第54分钟时重新发起协商。若协商成功，则保持则保持连接状态至下一轮协商。若协商失败，则在1小时内将状态设置为未连接，需要VPN两端重新进行通信才能恢复为连接状态。可以使用网络监控工具（例如 IP SLA）生成保持连接的Ping信号来避免这种情况发生。
  - IKE v2版本：如果VPN连接经历了一段无流量的空闲时间，VPN保持连接状态。

VPN常见问题 (3/3)

- VPN支持将两个VPC互连吗?
  - 如果两个VPC位于同一区域内，可以使用VPC对等连接互连。
  - 如果两个VPC位于不同区域，可以通过VPN连接，分别把这两个VPC的CIDR作为本端子网和远端子网。

更多信息

- **缩略语**

缩写	全称	释义
GRE	Generic Routing Encapsulation	路由封装协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
PPTP	Point-to-Point Tunneling Protocol	点到的隧道协议
IKE	Internet Key Exchange	因特网密钥交换协议
SA	Security Associations	安全盟
AH	Authentication Header	认证报头协议
ESP	Encapsulated Security Payload	负载安全封装协议

学习推荐

- 华为Learning网站
  - http://support.huawei.com/learning/Index!toTrainIndex
- 华为Support案例库
  - http://support.huawei.com/enterprise/servicecenter?lang=zh


谢 谢
www.huawei.com