

VPN 连接

故障处理

产品文档





【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有,未经腾讯云事先书面许可,任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况,部分产品、服务的内容可能有所调整。您 所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则, 腾讯云对本文档内容不做任何明示或默示的承诺或保证。



文档目录

故障处理

VPN 通道未联通

VPN 通道已联通但实际内网不通



故障处理 VPN 通道未联通

最近更新时间:2024-01-09 14:41:10

现象描述

使用 VPN 连接建立 VPC 与 IDC 的通信,完成配置后,发现 VPN 通道状态为未联通。

可能原因

通道状态异常,一般有如下可能原因: 无流量激活通道 VPN 网关公网 IP 不通 安全策略配置不正确 协商参数、协商模式不一致

处理方案

1. 登录 VPC 中的一台服务器, ping 对端 IDC 侧服务器的内网 IP 来激活通道。

说明:

登录VPC中云服务器请参考 登录Linux实例 或 登录Windows实例。 如果 ping 通,表示通道已激活,查看 VPN 通道状态是否已联通,如已联通,则问题解决,结束。 如果 ping 不通,请直接执行 步骤2。

2.

请登录 IDC 侧

的 VPN 设备, ping 腾讯云侧 VPN 网关的公网 IP(本例假设 VPN 网关公网 IP 为139.186.120.129), 查看是否可以 ping 通。

若是,请执行步骤4。

若否,请执行 步骤3。



[IDC_IPSec] ping 139.186.120.129 PING 139.186.120.129: 56 data bytes, press CTRL_C to Reply from 139.186.120.129: bytes=56 Sequence=1 ttl Reply from 139.186.120.129: bytes=56 Sequence=2 ttl Reply from 139.186.120.129: bytes=56 Sequence=3 ttl Reply from 139.186.120.129: bytes=56 Sequence=4 ttl Reply from 139.186.120.129: bytes=56 Sequence=5 ttl --- 139.186.120.129 ping statistics ---5 packet(s) transmitted 5 packet(s) received 0.00% packet loss round-trip min/avg/max = 30/58/80 ms

DC 侧公网

网络连接状态,是否可以正常连接到互联网。

若是,请执行 步骤4。

若否,请修复本地网络后,再查看 VPN 通道状态是否已联通,如已联通,则问题解决,结束;如未联通,则继续执行 步骤4。

4. 查看 ID

C 侧 VPN 设备的安全策略

,是否放通了腾讯云侧 VPN 网关的公网 IP 地址以及需要互通的内网地址。





display current-configuration configuration security-policy //此处以华为防火墙为例

若是,请执行步骤5。

若否,请修改安全策略,放通腾讯云侧 VPN 网关的 IP 以及对应 SPD 策略,再查看 VPN 通道状态是否已联通,如 已联通,则问题解决,结束;如未联通,则继续执行 步骤5。

5. 比对腾讯

云侧 VPN 网关与

对端 IDC 的 VPN 设备协商参数(IKE、IPsec 配置)及协商模式(主模式 main/野蛮模式 aggressive)是否一致。 **注意**:



任何一个参数不一致, VPN 通道都无法建立。 不同厂家设备、公有云服务提供商的默认 VPN 配置不尽相同。 进入 VPN 通道控制台,单击实例 ID,进入详情页,在"高级配置"页签中查看。 IDC 侧设备配置参数可通过如下命令获取(此处以华为防火墙为例):



display current-configuration configuration ike profile display current-configuration configuration ipsec policy

若是,请执行步骤6。



若否,请修改相应参数,确保两端配置一致,然后再查看 VPN 通道状态是否已联通,如已联通,则问题解决,结束;如未联通,则继续执行 步骤6。

6. 请收集以

上检查信

息,并提交工单或联系设备厂商跟进处理。



VPN 通道已联通但实际内网不通

最近更新时间:2024-01-09 14:41:10

现象描述

使用 VPN 连接建立 VPC 与 IDC 的通信, VPN 通道显示为已联通状态, 但内网无法联通,

[root@UM-1-11-centos ~]# ping 10...0.7 PING 10...0.7 (10.0 →.7) 56(84) bytes of data.

可能原因

通道状态正常但内网却无法联通,可能原因如下: VPC 子网路由表未添加指向 IDC 侧内网网段的路由 VPC/IDC 侧的安全策略未放通对应源 IP、目的 IP VPN 网关未添加指向 IDC 侧内网网段的通道(路由型) VPC/IDC 侧的内网服务器操作系统的防火墙未放行对端网段 VPC/IDC 侧的 SPD 策略未包含该源 IP、目的 IP VPN 网关未配置路由策略

处理步骤

检查 VPC 子网路由表中,是否有目的地址为 IDC 侧内网网段,下一跳地址为对应 VPN 网关的路由,同时检查 IDC 侧是否有目的地址为 VPC 网段,下一跳地址为对应 VPN 隧道的路由。
进入 VPC 子网路由表,单击路由表 ID,进入详情界面检查。
IDC 侧执行命令检查路由情况(以华为设备为例):





display ip routing-table //查看是否有对应目的地址为云上 VPC 网段,下一跳为对应 VPN 隧道

若是,请执行步骤3。

若否,请根据业务需求,补全相应路由信息,再执行步骤2。

2. 检查通信是否恢复正常,即登录 VPC/IDC 中的一台服务器,ping 对端服务器内网 IP。

说明:

登录VPC中云服务器请参考登录Linux实例 或登录Windows实例。

若是,通信正常,问题解决,结束。

若否,请执行步骤3。



3. 检查

VPC 中服务器关

联的安全组和子网关联的网络 ACL 是否放通来自云下 IDC 的流量,同时检查 IDC 侧是否放通来自云上 VPC 的流量。

进入 VPC 中服务器安全组 界面,单击安全组 ID,进入"安全组规则"页检查:

进入 VPC 子网 ACL 规则,单击网络 ACL ID,进入"基本信息"页,单击"入站规则"页签检查:

IDC 侧安全策略检查(此处以华为防火墙为例):



display current-configuration configuration security-policy

若是,请执行 步骤5。

∽ 腾讯云

若否,请放通安全组/网络 ACL/IDC 侧安全设备需要互通的内网地址段,再执行 步骤4。

4. 检查通信是否恢复正常,即登录 VPC/IDC 中的一台服务器, ping 对端服务器内网 IP。

若是,通信正常,问题解决,结束。

若否,请执行步骤5。

5. 分别检查 VPC 中云服务器和 IDC 侧内网服务器操作系统自带防火墙,是否有放通对端网段的策略。

Linux 服务器查看防火墙: iptables --list

Windows 服务器查看防火墙:控制面板/系统和安全/Windows 防火墙/允许的应用

若是,请执行步骤7。

若否,请在内网机器防火墙中放通需要联通的业务网段,再执行步骤6。

6. 检查通信是否恢复正常,即登录 VPC/IDC 中的一台服务器,ping 对端服务器内网 IP。

若是,通信正常,问题解决,结束。

若否,请执行步骤7。

7. 分别检查 VPC 和 IDC 侧的 VPN 通道的感兴趣流(SPD 策略)是否包含需要互通的内网网段。

进入 VPC 侧 SPD 策略, 单击 VPN 通道 ID, 进入"基本信息"页, 即可检查 SPD 策略:

IDC 侧 SPD 策略检查(此处以华为防火墙为例):





display current-configuration configuration acl

若是,请执行步骤8。

若否,请补充缺失的 SPD 策略,再执行 步骤8。

8. 检查 VPN 网关的路由表中是否包含对应的路由策略。进入 VPN 网关,单击 VPN 网关 ID,进入"路由表"页,即可 检查路由策略。

若是,请执行步骤9。

若否,请在 VPN 网关 > 路由页签指定下一跳,再执行 步骤9。

9. 检查通信是否恢复正常,即登录 VPC/IDC 中的一台服务器,ping 对端服务器内网 IP。



若是,通信正常,问题解决,结束。 若否,请执行步骤10。

10. 请收集以上检查信息,并提交工单或联系设备厂商跟进处理。