# VPN 连接

# 操作指南

# 产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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



版权所有：腾讯云计算（北京）有限责任公司

# 操作指南
# VPN 网关
# IPSec VPN 网关
# 创建 IPSec VPN 网关

最近更新时间：2024-01-10 17:27:12

VPN 网关是 VPN 连接服务的功能实例，因此在使用 VPN 连接实现外部网络到腾讯云 VPC 的网络的安全访问之前，您必须先创建一个 IPsec VPN 网关，本文指导您如何在控制台创建 VPN 网关。

## 前提条件

如需创建 VPC 类型的 VPN 网关，请提前创建好同地域的 VPC 网络，详情请参考 创建私有网络。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 VPN 网关管理页面，单击 **+新建**。
4. 在弹出的**新建 VPN 网关**对话框中，配置如下网关参数。

**说明：**

200Mbps、500Mbps、1000Mbps和3000Mbps带宽仅支持新建网关，存量网关暂不支持。

如果 VPN 网关使用200Mbps、500Mbps、1000Mbps和3000Mbps规格的带宽，VPN 通道加密协议建议使用 AES128+MD5。

| 参数名称 | 参数说明 |
| --- | --- |
| 网关名称 | 填写 VPN 网关名称，不超过60个字符。 |
| 所在地域 | 展示 VPN 网关所在地域。 |
| 可用区 | 选择当前网关所在的可用区。 |
| 协议类型 | 支持 IPSec 和 SSL 两种协议类型。 |
| 带宽上限 | 请根据业务实际情况，合理设置 VPN 网关带宽上限。 |
| 关联网络 | 此处表示您将创建云联网类型 VPN 还是私有网络类型的 VPN，通常我们也称为 CCN 型 |

| | |
|---|---|
| | VPN 网关、VPC 型 VPN 网关。<br>如果您需要通过 VPN 连接实现与多 VPC 网络，或其他专线网络的互通，您可以勾选**云联网**。<br>**注意：**<br>暂不支持 CCN 类型 VPN 网关创建时直接关联云联网实例。请在完成 VPN 网关创建后，在详情页关联云联网实例。如您创建是策略型的 VPN 通道，您还需在 VPN 网关的 IDC 网段中启用发布至云联网的路由。<br>如果您需要通过 VPN 连接实现与单 VPC 网络的互通，您可以勾选私有网络。 |
| 所属网络 | 仅当关联网络为私有网络时，此处需要选择 VPN 网关将要关联的具体私有网络。 |
| 标签 | 标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。 |
| 计费方式 | 支持按流量计费。按流量计费适用于带宽波动较大的场景。 |

5. 完成网关参数设置后，单击**创建**启动 VPN 网关的创建，此时**状态**为**创建中**，等待约1～2分钟，创建成功的 VPN 网关状态为**运行中**，系统为 VPN 网关分配一个公网 IP。

# 配置腾讯云侧到用户侧路由策略

最近更新时间：2024-01-09 14:43:23

## 前提条件

在配置 VPN 路由策略前，请确保已完成 VPN 网关、对端网关及 VPN 通道的配置。

## 操作步骤

1. 登录 私有网络控制台。
2. 单击左导航栏中**VPN 连接** > **VPN 网关**。
3. 在“VPN 网关”页面，选择地域和私有网络，单击 VPN 网关实例 ID 进入详情页。
4. 在“实例详情”页面，单击**路由表**页签。
5. 单击**新增路由**，并配置路由策略。

| 配置项 | 说明 |
| --- | --- |
| 目的端 | 填写要访问的对端网络的网段。 |
| 下一跳类型 | 支持 **VPN 通道**和**云联网**类型。<br>说明：如果是 CCN 型 VPN 网关，且 VPN 网关已关联至云联网实例时，则下一跳到**云联网**的路由策略系统将自动学习到并展示在路由条目中，请勿手动配置重复路由。 |
| 下一跳 | 选择具体的下一跳实例 ID。<br>如果**下一跳类型**为 **VPN 通道**，则选择已创建的 VPN 通道。<br>如果**下一跳类型**为**云联网**，则系统自动展示该 VPN 网关关联的云联网实例。 |
| 权重 | 选择通道的权重值：<br>0：优先级高<br>100：优先级低 |
| 新增一行 | 可添加多条路由策略。 |
| 删除 | 可删除路由策略，最后一条不允许删除。 |

6. 完成路由策略的配置后，单击**确定**。
7. 其他可执行操作。

7.1 启动、或禁用路由策略。

7.2 已禁用的路由策略支持删除。

版权所有：腾讯云计算（北京）有限责任公司

# 绑定云联网实例

最近更新时间：2024-01-09 14:43:23

如果您创建的是 CCN VPN 网关，在完成 VPN 网关创建后，还需要在详情页关联云联网实例。

## 前提条件

已 创建 CCN 型 IPsec VPN 网关。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 单击需要查看的 VPN 网关 ID，进入 VPN 网关详情页。
4. 在网关实例详情页面的**基本信息**页签，单击**所属网络**所在行的编辑图标，然后在弹出的对话框中选择需要关联的云联网实例和相应的路由表。
5. 单击**保存**。

# 发布 IDC 网段至云联网

最近更新时间：2024-01-09 14:43:23

如果您需要打通 VPN 和云联网 CCN，可以发布网段至 CCN。

**说明：**

如果 VPN 通道的通信模式为“目的路由”，那么不需要发布 IDC 网段至云联网。

## 前提条件

已 创建 CCN 型 IPsec VPN 网关 且已 绑定云联网实例。

已在 VPN 通道配置 SPD 策略。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 单击需要查看的 VPN 网关 ID，进入 VPN 网关详情页。
4. 在详情页面的**发布网段**页签发布云联网方向的网段。

该处网段为 VPN 通道创建配置 SPD 策略时对端网关的网段。

版权所有：腾讯云计算（北京）有限责任公司

# 修改 IPSec VPN 网关

最近更新时间：2024-01-09 14:43:23

VPN 网关创建后支持修改 VPN 网关名称、标签、带宽上限。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在“VPN 网关”页面，修改网关名称。
单击 VPN 网关名称旁的编辑图标，可修改网关名称。
单击网关 ID，进入网关详情页，通过**更改**来进行名称修改。
4. 修改带宽上限。
**注意：**
带宽上限的修改会涉及费用的变更，请评估后再做修改。
VPN 网关带宽目前仅支持部分带宽范围内升降配，如[5,100]Mbps和[200,1000]Mbps，在各自带宽范围内可进行升降配，跨范围升降配暂不支持。请提前规划好您的需求。
按量计费
方式一： 在 VPN 网关实例列表页找到待升级的实例，并在**带宽上限**列单击编辑图标，并选择新的规格值。
方式二：进入实例详情页面，单击**带宽上限**旁的编辑图标，并选择新的规格值。
5. 在“网关列表”界面，单击**编辑标签**或进入网关详情页通过编辑图标进行标签修改。

版权所有：腾讯云计算（北京）有限责任公司

# 删除 IPSec VPN 网关

最近更新时间：2024-01-09 14:43:23

当 VPN 网关不再使用时，您可以执行删除操作。

## 前提条件

已删除挂载的 VPN 通道，具体操作请参考 删除 VPN 通道。
已删除挂载的对端网关，具体操作请参考 删除对端网关。

## 操作步骤

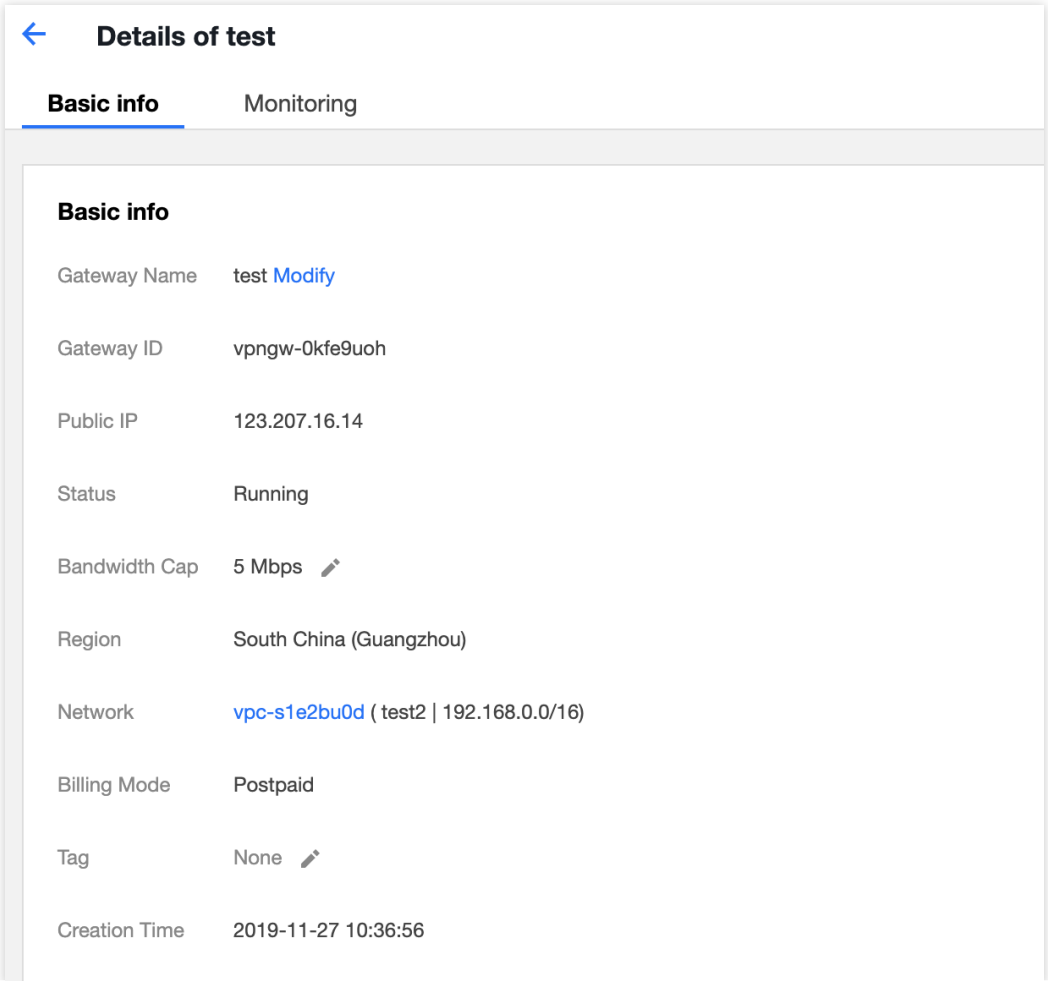
1. 登录 私有网络控制台。
2. 在左侧目录中选择 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在“VPN 网关”页面找到需要删除 VPN 网关，单击该网关右侧操作列的**删除**，并在弹出的对话框中单击**删除】**。

**说明：**
该 VPN 网关删除后，其关联的所有连接将立即中断，请务必确认后再进行操作。

# 查看 IPSec VPN 网关

最近更新时间：2024-01-09 14:43:23

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 单击需要查看的 VPN 网关 ID，即可进入 VPN 网关详情页。
4. 在该页面中，您可以看到 VPN 网关的详细信息。



# SSL VPN 网关
# 创建 SSL VPN 网关

最近更新时间：2024-01-09 14:43:23

SSL VPN 网关是 VPC 建立 SSL VPN 连接的出口网关，主要用于腾讯云 VPC 和客户移动端建立安全可靠的加密网络通信。

## 前提条件

已创建 VPC，详情请参考 创建私有网络。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 VPN 网关管理页面，单击**新建**。
4. 在弹出的**新建 VPN 网关**对话框中，配置如下网关参数。

| 参数名称 | 参数说明 |
| --- | --- |
| 网关名称 | 填写 VPN 网关名称，不超过60个字符。 |
| 所在地域 | 展示 VPN 网关所在地域。 |
| 可用区 | 选择当前网关所在的可用区。 |
| 协议类型 | 支持 IPSec 和 SSL 两种协议类型。 |
| 带宽上限 | 请根据业务实际情况，合理设置 VPN 网关带宽上限。 |
| 关联网络 | 此处表示您将创建云联网类型 VPN 还是私有网络类型的 VPN，通常我们也称为 CCN 型 VPN 网关、VPC 型 VPN 网关。如果您需要通过 VPN 连接实现与多 VPC 网络，或其他专线网络的互通，您可以勾选云联网。<br>**注意：**<br>暂不支持 CCN 类型 VPN 网关创建时直接关联云联网实例。请在完成 VPN 网关创建后，在详情页关联云联网实例。如您创建是策略型的 VPN 通道，您还需在 VPN 网关的 IDC 网段中启用发布至云联网的路由。<br>如果您需要通过 VPN 连接实现与单 VPC 网络的互通，您可以勾选私有网络。 |
| 所属网络 | 仅当关联网络为私有网络时，此处需要选择 VPN 网关将要关联的具体私有网络。云联网实例 |

| | |
|---|---|
| | 需要创建网关后在详情页进行绑定，详情请参见 绑定云联网实例。 |
| SSL 连接数 | “协议类型”选择 “SSL” 需要配置该项，SSL 连接所支持的数量与网关相关，具体请参见 使用限制。 |
| 标签 | 标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。 |
| 计费方式 | SSL VPN目前仅支持按流量计费。 |

5. 完成网关参数设置后，单击**创建**。

# 绑定云联网实例

最近更新时间：2024-01-09 14:43:23

如果您创建的是 CCN VPN 网关，在完成 VPN 网关创建后，还需在其详情页关联云联网实例。

## 前提条件

已创建 CCN 型 IPsec VPN 网关。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 单击需要查看的 VPN 网关 ID，进入 VPN 网关详情页。
4. 在网关实例详情页面的**基本信息**页签，单击**所属网络**所在行的编辑图标，然后在弹出的对话框中选择需要关联的云联网实例和相应的路由表。
5. 单击**保存**。

# 修改 SSL VPN 网关

最近更新时间：2024-01-09 14:43:23

SSL VPN 网关创建后支持修改网关名称、标签、带宽上限。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 **VPN 网关**页面，修改网关名称。

单击协议类型为 **SSL** 的 VPN 网关名称旁的编辑图标，可修改网关名称。

单击网关 ID，进入网关详情页，通过**更改**来进行名称修改。

4. 修改带宽上限。

**注意：**

带宽上限的修改会涉及费用的变更，请评估后再做修改。

VPN 网关带宽目前仅支持部分带宽范围内升降配，如[5,100]Mbps和[200,1000)Mbps，在各自带宽范围内可进行升降配，跨范围升降配暂不支持。请提前规划好您的需求。

1000Mbps暂不支持降配。

方式一： 在 VPN 网关实例列表页找到待调整带宽的实例，并在**带宽上限**列单击编辑图标，并选择新的规格值。

方式二：进入实例详情页面，单击**带宽上限**旁的编辑图标，并选择新的规格值。

# 删除 SSL VPN 网关

最近更新时间：2024-01-09 14:43:23

当 SSL VPN 网关不再使用时，您可以执行删除操作。

## 前提条件

已删除挂载的 SSL 服务端，具体操作请参考 删除 SSL 服务端。
已删除挂载的 SSL 客户端，具体操作请参考 删除 SSL 客户端。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中选择 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在“VPN 网关”页面找到需要删除的 SSL VPN 网关，然后单击操作列的**删除**，并在弹出的对话框中单击**删除**。

**说明：**
该 VPN 网关删除后，其关联的所有连接将立即中断，请务必确认后再进行操作。

# 查看 SSL VPN 网关

最近更新时间：2024-01-09 14:43:23

## 查看 VPN 网关

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
 该页面展示了 SSL VPN 网关 ID、名称、状态、公网 IP、所属网络、带宽上限等信息。
3. 单击具体的 SSL VPN 网关 ID，进入 SSL VPN 网关详情页。
4. 在该页面中，您可以查阅 SSL VPN 网关的详细信息。

## 设置 VPN 网关列表展示列

如果您需要对 VPN 网关列表展示列进行自定义设置，可单击右侧搜索框旁边的设置按钮，并选择需要展示的字段，然后单击**确定**。

# VPN 通道
# 创建 VPN 通道

最近更新时间：2024-01-09 14:43:23

VPN 通道是 VPN 连接中用来传输数据包的公网加密通道，腾讯云上的 VPN 通道在实现 IPsec 时，使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立会话。IKE 具有一套自我保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPSec 会话。本文介绍如何通过“控制台”创建 VPN 通道。您还可以通过 API、SDK 管理您的 VPN 通道，详情参见 API 文档。

VPN 通道的建立包括以下配置信息：

基本信息

通道模式

IKE 配置（选填）

IPsec 配置（选填）

## 背景信息

目的路由

本通信通过路由策略指定 VPN 网关所属网络可以和 IDC 中哪些网段通信，创建通道完成后需在 VPN 网关的路由表中配置对应路由策略，详情请参见 配置 VPN 网关路由 。

SPD 策略。

**说明：**

SPD（Security Policy Database）策略由一系列 SPD 规则组成，用于指定 VPC 或云联网内哪些网段可以和 IDC 内哪些网段通信。每条 SPD 规则包括一个本端网段 CIDR，和至少一个对端网段 CIDR。一个本端网段 CIDR 和一个对端网段 CIDR 构成一组匹配关系。一个 SPD 规则下可以有多组**匹配关系**。

腾讯云 VPN 网关会按照**匹配关系**依次和对端网关设备进行协商，您需要确保您的对端网关设备支持按照匹配关系进行协商，例如在 StrongSwan 配置中使用 also 关键字。

同一 VPN 网关下所有 SPD 规则形成匹配关系的数量最多为**200**个，否则建议您使用**路由型 VPN 连接**。

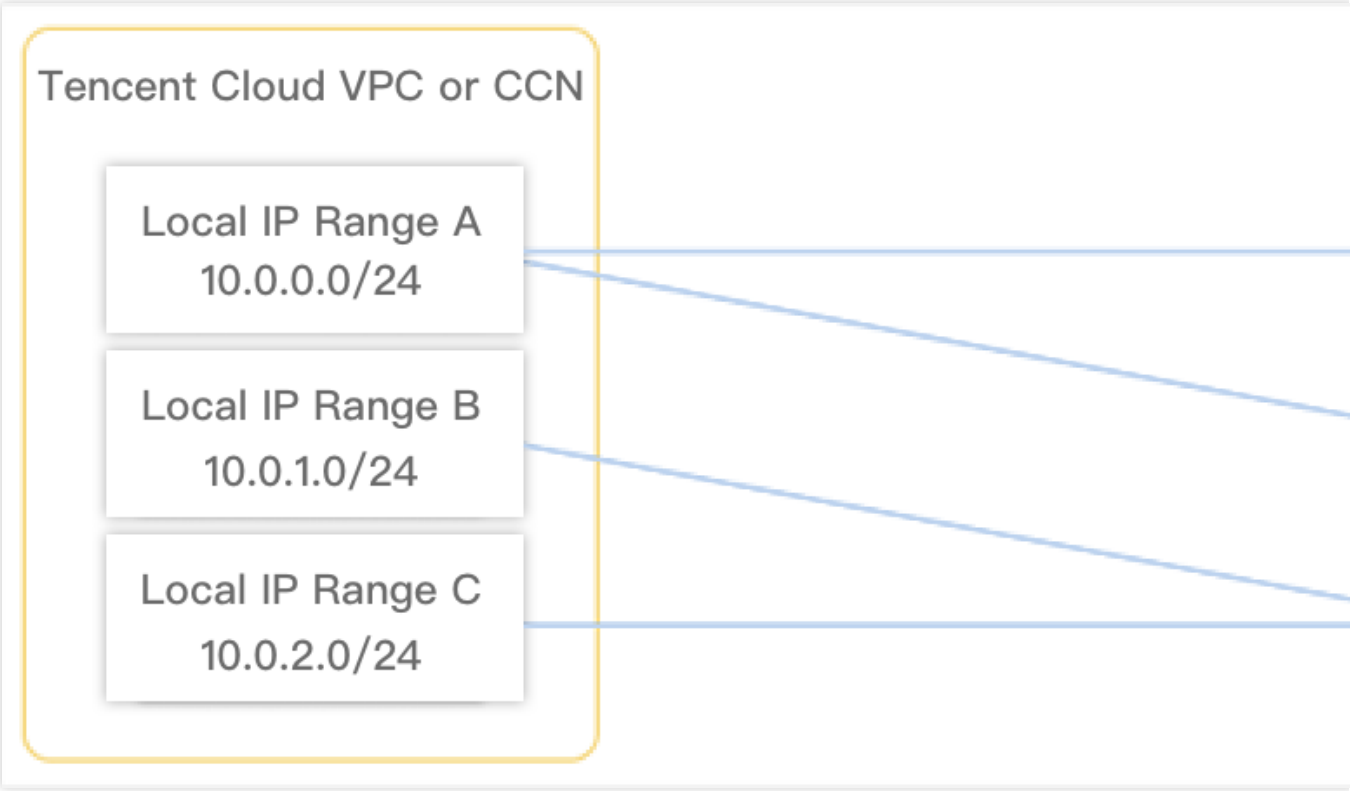
同一 VPN 网关下所有通道内的规则，匹配关系不能重叠，即一组的匹配关系中，本端网段和对端网段不能同时重叠。

在腾讯云配置的 **SPD 策略建议与对端网关设备配置的 SPD 策略对称**，即在腾讯云配置 SPD 策略中本端网段为 `10.11.12.0/24` ，对端网段为 `192.168.1.0/24` ；对端网关设备配置 SPD 策略中本端网段为 `192.168.1.0/24` ，对端网段为 `10.11.12.0/24` 。

配置 SPD 策略后，VPN 网关会自动下发路由，无需在 VPN 网关添加路由。

**示例：**

如下图所示，某 VPN 网关下已经存在以下 SPD 规则：




SPD 规则1本端网段 `10.0.0.0/24` ，对端网段为 `192.168.0.0/24` 、 `192.168.1.0/24` ，有两组匹配关系。
SPD 规则2本端网段 `10.0.1.0/24` ，对端网段为 `192.168.2.0/24` ，有一组匹配关系。
SPD 规则3本端网段 `10.0.2.0/24` ，对端网段为 `192.168.2.0/24` ，有一组匹配关系。
他们的匹配关系分别是：
`10.0.0.0/24` ----- `192.168.0.0/24`
`10.0.0.0/24` ----- `192.168.1.0/24`
`10.0.1.0/24` ----- `192.168.2.0/24`
`10.0.2.0/24` ----- `192.168.2.0/24`
这四组匹配关系相互不能重叠，即他们的本端网段和对端网段不能同时重叠。
如果新增一个 `10.0.0.0/24` ----- `192.168.1.0/24` 匹配关系，则会因为和已有匹配关系重叠，而无法添加 SPD 规则。
如果新增一个 `10.0.1.0/24` ----- `192.168.1.0/24` 匹配关系，和已有的3个匹配关系均不重叠，则可以加入 SPD 规则。

## 前提条件

已 创建 VPN 网关 和 对端网关。
请确保您已创建的 VPN 通道没有超出配额，调整配额请参考 使用限制。

# 操作步骤

1. 登录 私有网络控制台。
2. 单击左侧导航栏中 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在 **VPN 通道**管理页面，单击**新建**。
4. 在弹出的新建对话框中，配置 VPN 通道基本信息。

**4.1 基本信息配置**

本步骤主要配置通道名称、所属网络、关联 VPN 网关、对完网关、共享密钥、协商类型、通信模式等基本配置。

| 参数名称 | 说明 |
| --- | --- |
| 通道名称 | 自定义通道名称，字符长度为60个。 |
| 地域 | 您要创建的 VPN 通道关联的 VPN 网关所在的地域。 |
| VPN 网关类型 | VPN 网关类型有私有网络型 VPN 和云联网型 VPN。关于两种 VPN 网关类型的详细说明请参考 IPsec VPN。 |
| 私有网络 | 仅当 **VPN 网关类型**为**私有网络**时，需要在此处选择 VPN 网关所属的私有网络。云联网类型无此参数。 |
| VPN 网关 | 在列表中选择 VPN 网关。 |
| 对端网关 | 选择已创建的对端信息，如果没有，可选择新建。 |
| 对端网关 IP | 对端网关的公网 IP 地址。 |
| 预共享密钥 | 用于本端和对端网关之间的身份认证，本端和对端须使用相同的预共享密钥。 |
| 协商类型 | 流量协商：创建通道完成之后，当本端有流量进入时，开始与对端协商。<br>主动协商：通道创建后主动向对端发起协商。<br>被动协商：等待对端发起协商。 |
| 通信模式 | 支持目的路由和 SPD 策略两种类型，推荐使用目的路由。 在使用 SPD 策略模式前，您可先了解 SPD 策略原则。 |

4.2 高级配置

本步骤主要配置 DPD 检测、健康检查、IKE 和 IPSec 等。

| 参数名称 | 说明 |
| --- | --- |
| 开启 DPD 检测 | DPD 检测开启/关闭开关，用于检测对端是否存活，默认开启。<br>本端主动向对端发送 DPD 请求报文，若在指定超时时间内未收到对端的回应报文，则认为对端离线，进行超时后对应操作。 |
| DPD 超时时 | DPD 探测总体超时时间。默认30秒，取值范围30秒~60秒。 |

| | |
|---|---|
| 间 | |
| DPD 超时操作 | 断开：清除当前 SA，且当前 VPN 通道断开。<br>重试：重新与对端建立连接。 |

4.3 健康检查配置

| 参数名称 | 说明 |
|---|---|
| 开启健康检查 | 健康检查用于主备通道的场景，具体请参考 IDC 与单个腾讯云 VPC 实现主备容灾。如果您不涉及，无需开启此开关（默认不开启），否则请开启本开关，并完成下面的健康检查本端及对端地址的配置，详情请参见配置健康检查。<br>**说明：**<br>一旦您开启健康检查并创建通道完成，系统立即开始通过 NQA 检测 VPN 通道健康状况，如果 VPN 通道未联通或您配置的对端地址不响应 NQA 探测，则系统会在多次探测失败后判定为不健康，并临时中断业务流量，直到 VPN 通道恢复健康。 |
| 健康检查本端地址 | 仅当开启健康检查功能时，需要设置此参数。您可以使用系统为您分配的 IP 地址或者指定。<br>**说明：**<br>指定地址不能与 VPC 或 CCN 以及 IDC 通信私网地址或网段冲突，也不能与健康检查对端地址冲突。不能使用多播、广播及本地环回地址。 |
| 健康检查对端地址 | 仅当开启健康检查功能时，需要设置此参数。您可以使用系统为您分配的 IP 地址或者指定。<br>**说明：**<br>指定地址不能与 VPC 或 CCN 以及 IDC 通信私网地址或网段冲突，也不能与健康检查本端地址冲突。不能使用多播、广播及本地环回地址。 |

4.4 IKE 配置

| 配置项 | 说明 |
|---|---|
| 版本 | IKE V1、IKE V2。 |
| 身份认证方法 | 加密算法支持 AES-128、AES-192、AES-256、3DES、DES、SM4，推荐使用 AES-128。 |
| 认证算法 | 身份认证算法，支持 MD5、SHA1、SHA256、AES-383、SHA512、SM3，推荐使用 MD5。 |
| 协商模式 | 支持 main（主模式）和 aggressive（野蛮模式）二者的不同之处在于，aggressive 模式可以用更少的包发送更多信息，可以快速建立连接，但是是以清晰的方式发送安全网关的身份。使用 aggressive 模式时，配置参数如 Diffie-Hellman 和 PFS 不能进行协商，要求两端拥有兼容的配 |

版权所有：腾讯云计算（北京）有限责任公司

| | |
|---|---|
| | 置。 |
| 本端标识 | 支持 IP Address 和 FQDN（全称域名），默认 IP Address。 |
| 对端标识 | 支持 IP Address 和 FQDN，默认 IP Address。 |
| DH group | 指定 IKE 交换密钥时使用的 DH 组，密钥交换的安全性随着 DH 组的扩大而增加，但交换的时间也增加了。<br>DH1：采用 768-bit 模指数（Modular Exponential，MODP ）算法的 DH 组。<br>DH2：采用 1024-bit MODP 算法的 DH 组。<br>DH5：采用 1536-bit MODP 算法的 DH 组。<br>DH14：采用 2048-bit MODP 算法，不支持动态 VPN 实现此选项。<br>DH24：带 256 位的素数阶子群的 2048-bit MODP 算法 DH 组。 |
| IKE SA Lifetime | 单位：s<br>设置 IKE 安全提议的 SA 生存周期，在设定的生存周期超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时后，将被自动清除。 |

4.5 IPSec 配置(选配)

| 配置项 | 说明 |
|---|---|
| 加密算法 | 加密算法支持 AES-128、AES-192、AES-256、3DES、DES、SM4。 |
| 认证算法 | 身份认证算法，支持 MD5、SHA1、SHA256、SHA384、SHA512、SM3。 |
| 报文封装模式 | Tunnel。 |
| 安全协议 | ESP。 |
| PFS | 支持 disable、DH-GROUP1、DH-GROUP2、DH-GROUP5、DH-GROUP14 和 DH-GROUP24。 |
| IPsec SA lifetime(s) | 单位：s。 |
| IPsec SA lifetime(KB) | 单位：KB。 |

5. 单击**下一步**，进入通信模式配置界面。

**说明：**

如果需要输入多个对端网段，请使用换行隔开。

6. 单击**下一步**，进入 **IKE 配置（选填）**界面，如不需要高级配置，可直接单击**下一步**。

| | |
|---|---|
| | |

| 配置项 | 说明 |
| --- | --- |
| 版本 | IKE V1、IKE V2。 |
| 身份认证方法 | 默认预共享密钥。 |
| 加密算法 | 加密算法支持 AES-128、AES-192、AES-256、3DES、DES、SM4，推荐使用 AES-128。 |
| 认证算法 | 身份认证算法，支持 MD5、SHA1、SHA256、AES-383、SHA512、SM3，推荐使用 MD5。 |
| 协商模式 | 支持 main（主模式）和 aggressive（野蛮模式）<br>二者的不同之处在于，aggressive 模式可以用更少的包发送更多信息，可以快速建立连接，但是是以清晰的方式发送安全网关的身份。使用 aggressive 模式时，配置参数如 Diffie-Hellman 和 PFS 不能进行协商，要求两端拥有兼容的配置。 |
| 本端标识 | 支持 IP Address 和 FQDN（全称域名），默认 IP Address。 |
| 对端标识 | 支持 IP Address 和 FQDN，默认 IP Address。 |
| DH group | 指定 IKE 交换密钥时使用的 DH 组，密钥交换的安全性随着 DH 组的扩大而增加，但交换的时间也增加了。<br>DH1：采用 768-bit 模指数（Modular Exponential，MODP ）算法的 DH 组。<br>DH2：采用 1024-bit MODP 算法的 DH 组。<br>DH5：采用 1536-bit MODP 算法的 DH 组。<br>DH14：采用 2048-bit MODP 算法，不支持动态 VPN 实现此选项。<br>DH24：带 256 位的素数阶子群的 2048-bit MODP 算法 DH 组。 |
| IKE SA Lifetime | 单位：s<br>设置 IKE 安全提议的 SA 生存周期，在设定的生存周期超时前，会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时后，被自动清除。 |

7. 进入 **IPsec配置（选填）**界面，如果不需要高级配置，可直接单击**完成**。

| 配置项 | 说明 |
| --- | --- |
| 加密算法 | 加密算法支持 AES-128、AES-192、AES-256、3DES、DES、SM4 |
| 认证算法 | 身份认证算法，支持 MD5、SHA1、SHA256、SHA384、SHA512、SM3 |
| 报文封装模式 | Tunnel |
| 安全协议 | ESP |
| PFS | 支持 disable、DH-GROUP1、DH-GROUP2、DH-GROUP5、DH-GROUP14 和 DH-GROUP24 |
| | |

| | |
|---|---|
| IPsec SA lifetime(s) | 单位：s |
| IPsec SA lifetime(KB) | 单位：KB |

# 查看 VPN 通道

最近更新时间：2024-01-09 14:43:23

VPN 通道创建后，您可以在 VPN 通道管理页面查看通道详情。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在“VPN 通道”管理页面，单击通道实例进入 VPN 通道详情页面。

版权所有：腾讯云计算（北京）有限责任公司

# 配置健康检查

最近更新时间：2024-01-09 14:43:23

腾讯云 VPN 为您的业务高可用性提供完整的解决方案，除网关本身支持高可用外，也支持主备通道。VPN 网关通过健康检查判定通道状况，从而触发进行主备通道的流量切换。本文介绍如何进行健康检查配置。

**说明：**

健康检查推荐使用路由型通道，若为 SPD 策略型通道，需配置 `0.0.0.0/0` 的 SPD 策略。

## 健康检查原理

VPN 通道的监控检查使用了 NQA 机制，并默认使用 Ping 方式。即 VPN 网关会周期性使用健康检查的本端地址 Ping（通道内加密）对端地址，从而判定其连通性。连续多次 Ping 失败后，VPN 网关判定通道连通性异常，会将主通道流量切换到备通道，此时，也需要对端网关实现类似的机制，同步将流量切换到备用通道。为此，您需要为健康检查配置或采用系统自动分配两个可以在通道内相互 Ping 的 IP 地址。两个地址所属网段不应与 VPC、IDC 网段冲突。

## 前提条件

已 创建 VPN 网关 和 对端网关的配置，且 VPN 网关为3.0及以上版本。

业务场景需要主备通道。

已规划健康检查地址或计划使用系统自动分配地址。

## 方式一：VPN 通道创建时配置健康检查

该处仅介绍健康检查参数配置和参数说明，VPN 通道创建其他步骤请参考 创建 VPN 通道 。

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在 **VPN 通道**管理页面，单击**新建**。
4. 在弹出的新建对话框中，完成基本配置后，在**高级配置**中开启健康检查并配置健康检查 IP。
5. 继续完成 VPN 通道创建，通道创建完成后健康检查配置立即生效。

## 方式二：VPN 通道创建后配置健康检查

如果在 VPN 通道创建过程中没有配置健康检查，您可以在创建完成在 VPN 通道详情页进行配置。

版权所有：腾讯云计算（北京）有限责任公司

**说明：**

本方式配置健康检查后，您的业务可能会产品短暂的业务中断，建议使用方式一。

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在 **VPN 通道**管理页面，找到需要配置健康检查的 VPN 通道实例，然后单击具体的实例名称，并在**基本信息**页签单击**编辑**。
4. 开启健康检查，并配置健康检查参数。

| 参数 | 说明 |
| --- | --- |
| 健康检查本端地址 | 默认分配`169.254.128.0/17`网段地址，也可填写 VPC 外可用内网 IP 地址，但该 IP 必须为非 VPC 内、`224.0.0.0`-`239.255.255.255`，以及`0.0.0.0`地址。 |
| 健康检查对端地址 | 默认分配`169.254.128.0/17`网段地址，也可填写 IDC 内可用 IP 地址。 |

5. 推荐您在通信模式中选择**目的路由**方式。如果没有**目的路由**方式可选，则建议将 SPD 本端及对端填写为 `0.0.0.0/0`，确保本端健康检查 IP 和对端健康检查 IP 基于 VPN 通道加密通信。
6. 单击**保存**。

# 下载配置文件

最近更新时间：2024-01-09 14:43:23

本端 VPN 通道配置完成后，您可以下载 VPN 通道配置，将该配置加载到 IDC 侧的本地网关设备中。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在“VPN 通道”管理页面，单击通道实例右侧的**更多** > **下载配置文件**。
4. 在弹出的下载对话框中，选择对端网关设备的类型、下载平台、版本、接口名称，然后单击**下载**。

版权所有：腾讯云计算（北京）有限责任公司

# 查看通道日志

最近更新时间：2024-01-09 14:43:23

VPN 通道管理界面，提供日志查询功能，通过日志信息可排查 VPN 通道连接过程中的故障。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > VPN 通道，进入管理页。
3. 在“VPN 通道”管理页面，单击通道实例右侧的**更多** > **日志**，进入日志检索页面。
4. 在“日志检索”页面，您可以查看日志详情，且可以选择不同时间段的日志进行查看。

# 修改 VPN 通道

最近更新时间：2024-01-09 14:43:23

VPN 通道创建后，您可以修改通道基本信息中的名称、预共享密码、标签信息、SPD 策略，以及高级配置中的 IKE 配置和 IPsec 配置，也可以重置通道的所有配置。

## 对系统的影响

重置操作会中断现有 VPN 通道数据传输并重新建立连接，请提前做好网络变更准备。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在“VPN 通道”管理页面，单击需要修改的 VPN 通道实例 ID，进入详情页。
4. 在“基本信息”页面，单击图中的编辑图标，可修改 VPN 通道名称、预共享密码、标签信息、以及 SPD 策略规则，修改后单击**保存**即可。
 其中，通道名称和预共享密钥也可以在 VPN 通道列表界面单击编辑图标直接修改，如下图所示。
5. 单击**高级配置**选项卡，可在高级配置中修改 IKE 配置 和 IPsec 配置，修改后单击**保存**即可。
6. 单击**重置**将重置所有通道配置，请知悉风险并谨慎操作。

版权所有：腾讯云计算（北京）有限责任公司

# 删除 VPN 通道

最近更新时间：2024-01-09 14:43:23

当 VPN 通道不再使用时，您可以执行删除操作。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **VPN 通道**，进入管理页。
3. 在“VPN 通道”管理页面，单击通道实例右侧的**更多** > **删除**。
4. 在确认对话框中，单击**删除**即可完成操作。

# 对端网关

# 创建对端网关

最近更新时间：2024-01-09 14:43:23

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **对端网关**，进入管理页。
3. 在“对端网关”管理页面，选择地域，单击**+新建**。
4. 填写对端网关名称，公网 IP 填写对端 IDC 侧的 VPN 网关设备的静态公网 IP ，根据需要设置标签。
5. 单击**创建**即可，创建成功的对端网关如下图所示。

版权所有：腾讯云计算（北京）有限责任公司

# 查看对端网关

最近更新时间：2024-01-09 14:43:23

创建对端网关后，您可以查看对端网关详情。

## 操作步骤.

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **对端网关**，进入管理页。
 可通过搜索框查看需要的对端网关信息，包括 ID/名称、公网 IP、通道个数等信息。

# 修改对端网关

最近更新时间：2024-01-09 14:43:23

创建对端网关后，您可以修改对端网关的名称和描述信息。

## 操作步骤.

1. 登录 私有网络控制台。
2. 在左侧目录中单击**VPN 连接 > 对端网关**，进入管理页。
3. 在“对端网关”管理页面，单击对端网关名称右侧的修改图标可进行修改，修改后，单击**保存**即可。
4. 单击右侧的**编辑标签**，可以修改标签信息。

版权所有：腾讯云计算（北京）有限责任公司

# 删除对端网关

最近更新时间：2024-01-09 14:43:23

如果您的对端网关不再使用，且未创建任何通道，则您可以执行删除操作。

## 操作步骤.

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > 对端网关，进入管理页。
3. 在“对端网关”管理页面，单击待删除的对端网关实例右侧的**删除**。
4. 在确认对话框中，单击删除即可完成操作。

# SSL 服务端
# 创建 SSL 服务端

最近更新时间：2024-01-09 14:43:23

SSL VPN 网关创建完成后，需要在腾讯云侧创建 SSL 服务端，为用户侧提供 SSL 服务。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。

**说明：**

一个 VPN 网关仅支持关联一个 SSL 服务端，详情请参见 使用限制。

3. 在 SSL 服务端管理页面，单击 **+新建** 。
4. 在弹出的 **新建 SSL 服务端**对话框中，配置如下参数。

**说明：**

在 Windows 系统下，如果您的客户端 OpenVPN 是3.4.0及以上版本，那么 SSL 服务端配置时需要配置加密和认证算法，其中认证算法仅支持 SHA1。

| 参数名称 | 参数说明 |
| --- | --- |
| 名称 | 填写 SSL 服务端名称，不超过60个字符。 |
| 地域 | 展示 SSL 服务端所在地域。 |
| VPN 网关 | 选择创建好的 SSL VPN 网关。 |
| 本端网段 | 客户移动端访问的云上网段。 |
| 客户端网段 | 分配给用户移动端进行通信的网段，该网段请勿与腾讯侧 VPC CIDR 冲突，同时也不能与您本地的网段冲突。 |
| 协议 | 服务端传输协议。 |
| 端口 | 填写 SSL 服务端用于数据转发的端口。 |
| 认证算法 | 目前支持 SHA1 和 MD5 两种认证算法。 |
| 加密算法 | 目前支持 AES-128-CBC、AES-192-CBC 和 AES-256-CBC 加密算法。 |
| 是否压缩 | 否。 |
| 认证方式 | **证书认证**和**证书认证 + 身份认证**两种方式，本示例以**证书认证**为例。 |

版权所有：腾讯云计算（北京）有限责任公司

| | |
|---|---|
| | 证书认证：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问。<br>证书认证 + 身份认证：该认证方式仅允许在控制策略中的访问策略连接，您可选择为特定用户组或全部用户配置访问策略，勾选后需要选择对应的 EIAM 应用。 |

5. 完成网关参数设置后，单击**创建**。

# 查看 SSL 服务端

最近更新时间：2024-01-09 14:43:23

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页。
 该页面展示了 SSL 服务端 ID、名称、状态、VPN 网关、本端网段、客户端网段等信息。
3. 单击具体的 SSL 服务端 ID，进入 SSL 服务端详情页。
在该页面中，您可以查 SSL 服务端基本信息和配置信息。

版权所有：腾讯云计算（北京）有限责任公司

# 删除 SSL 服务端

最近更新时间：2024-01-09 14:43:23

当 SSL 服务端不再使用时，您可以执行删除操作。

## 前提条件

已删除挂着 SSL 服务端的 SSL 客户端。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中选择 **VPN 连接** > **SSL 服务端**，进入管理页。
3. 在 **SSL 服务端**页面找到需要删除的 SSL 服务端，然后单击操作列的**删除**，并在弹出的对话框中单击**删除**。

**说明：**

该 SSL 服务端删除后，其关联的所有连接将立即中断，请务必确认后再进行操作。

# 导出 SSL 服务端列表

最近更新时间：2024-01-09 14:43:23

SSL 服务端创建完成后，如果您需要导出 SSL 服务端配置信息，可在 SSL 服务端操作。本文介绍如何导出 SSL 服务端配置信息。

## 前提条件

已 创建 SSL 服务端。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页。
3. 在 SSL 服务端管理页面单击搜索框旁的导出按钮。

版权所有：腾讯云计算（北京）有限责任公司

# SSO 认证

最近更新时间：2024-01-09 14:43:23

若您通过 自助 Portal 下载 SSL 客户端配置，可以在 SSL 服务端开启 SSO 认证。

**说明：**

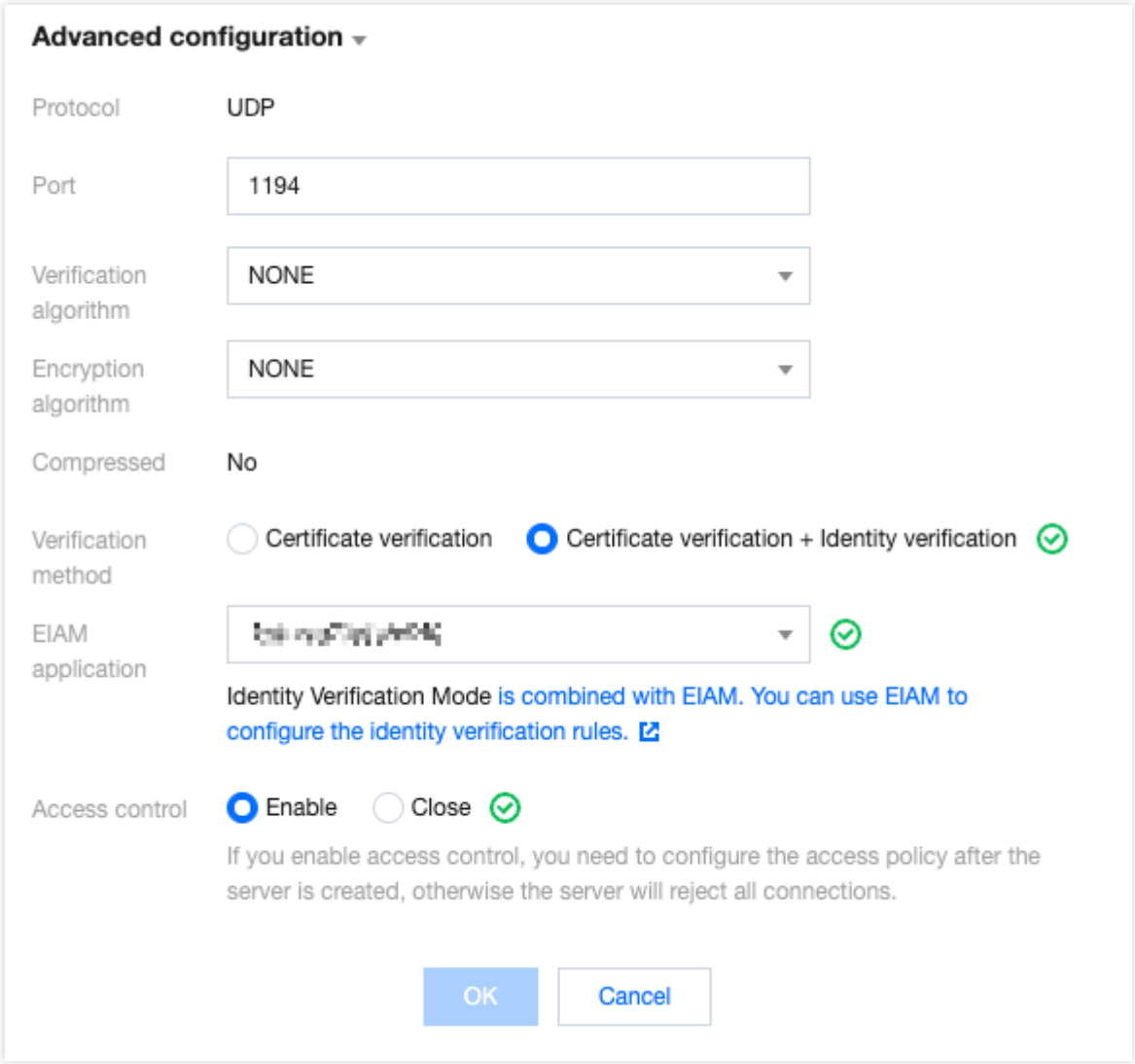
目前 SSO 身份认证功能灰度中，仅支持新加坡地域，如有需要，请提交 工单申请。

## 前提条件

在数字身份管控平台已创建用户组，添加了相应的用户并为用户组配置应用授权。

## 在创建 SSL 服务端过程中开启

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击**新建**。
4. 在弹出的**新建 SSL 服务端**对话框中，**认证方式**选择**证书认证 + 身份认证**，然后选择 EIAM 应用。

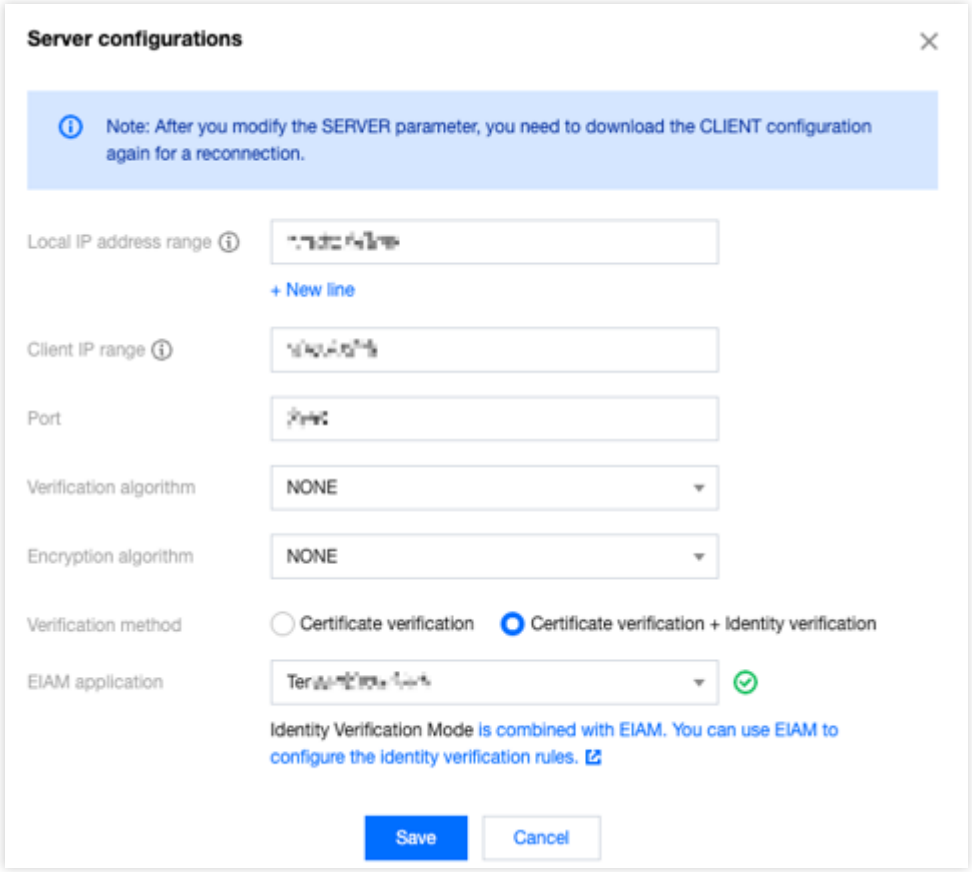



| 参数名称 | 参数说明 |
| --- | --- |
| 协议 | 服务端传输协议 |
| 端口 | 填写 SSL 服务端用于数据转发的端口 |
| 认证算法 | 目前支持 SHA1 和 MD5 两种认证算法 |
| 加密算法 | 目前支持 AES-128-CBC、AES-192-CBC 和 AES-256-CBC 加密算法 |
| 是否压缩 | 否 |
| 认证方式 | 证书认证：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问<br>证书认证 + 身份认证：该认证方式仅允许在控制策略中的访问策略连接，您可选择为特定用户组或全部用户配置访问策略，勾选后需要选择对应的 EIAM 应用 |
| EIAM 应用 | EIAM 是在 数字身份管控平台 所创建的用于访问控制的应用 |
| 访问控制 | SSL 服务端访问控制开关 |

5. **访问控制**按需**开启**，详情请参见 开启访问控制。

## 在 SSL 服务端创建完成后开启

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击具体的实例名称。
4. 在实例详情页的**基本信息**页签的**服务端配置**区域单击**编辑**。
5. **认证方式**选择**证书认证 + 身份认证**，并选择 EIAM 应用，然后单击**保存**。



# 开启访问控制

最近更新时间：2024-01-09 14:43:23

为了确保您的业务的安全性，SSL VPN 提供了SSL 服务端访问控制功能，让您的链路安全性更高。

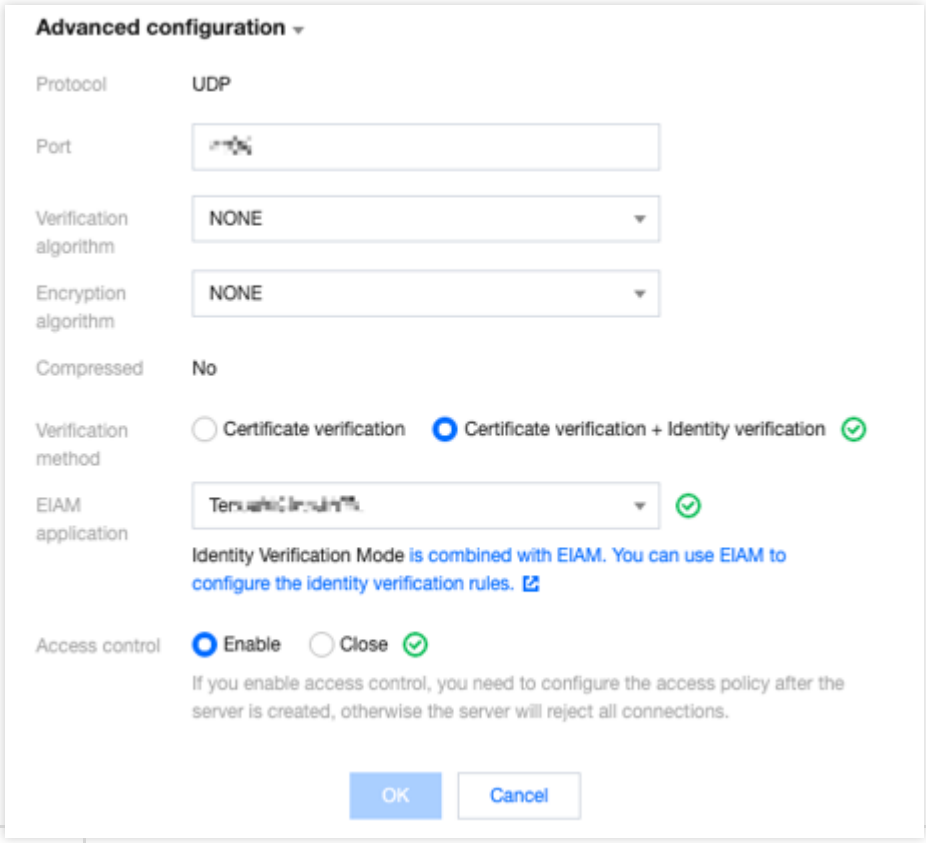
## 注意事项

开启访问控制后，在服务端创建完成之后您需要配置对应访问策略，否则服务端将拒绝所有连接。
如果认证方式仅选择了**证书认证**，默认该 SSL 服务端将接受所有连接。
**说明：**
目前只有支持 SSO 身份认证 SSL VPN 支持访问控制功能，详情见 SSO 认证。

## 在创建 SSL 服务端时开启访问控制

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击**+新建**。
4. 在弹出的**新建 SSL 服务端**对话框中，开启身份认证时同步开启访问控制并配置相关参数。

**说明：**
如您开启访问控制，在服务端创建完成之后您需要 配置访问控制策略，否则服务端将拒绝所有连接。



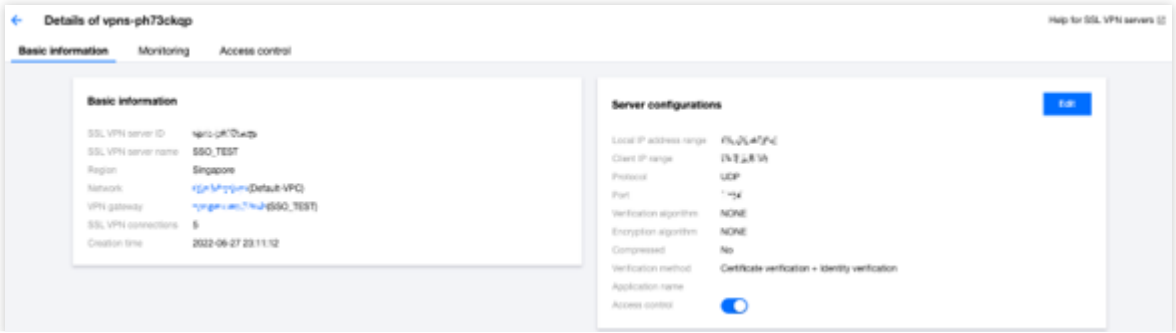

| 参数名称 | 参数说明 |
| --- | --- |
| 认证方式 | 证书认证：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问。<br>证书认证 + 身份认证：该认证方式仅允许在控制策略中的访问策略连接，您可选择为特定用户组或全部用户配置访问策略，勾选后需要选择对应的 EIAM 应用。 |
| EIAM 应用 | EIAM 是在 数字身份管控平台 所创建的用于访问控制的应用。 |
| 访问控制 | SSL 服务端访问控制开关。 |

# 在创建 SSL 服务端后开启访问控制

**说明：**

如您开启访问控制，在服务端创建完成之后您需要配置对应访问策略，否则服务端将拒绝所有连接。

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击具体的实例名称。
4. 在实例详情页的**基本信息**页签的服务端配置开启认证策略。


Details of vpns-ph73ckqp
Help for SSL VPN servers
Basic information
Monitoring
Access control
Basic information
SSL VPN server ID
SSL VPN server name
SSO_TEST
Region
Singapore
Network
(Default-VPC)
VPN gateway
(SSO_TEST)
SSL VPN connections
5
Creation time
2022-06-27 23:11:12
Server configurations
Edit
Local IP address range
Client IP range
Protocol
UDP
Port
Verification algorithm
NONE
Encryption algorithm
NONE
Compressed
No
Verification method
Certificate verification + identity verification
Application name
Access control

# 关闭访问控制

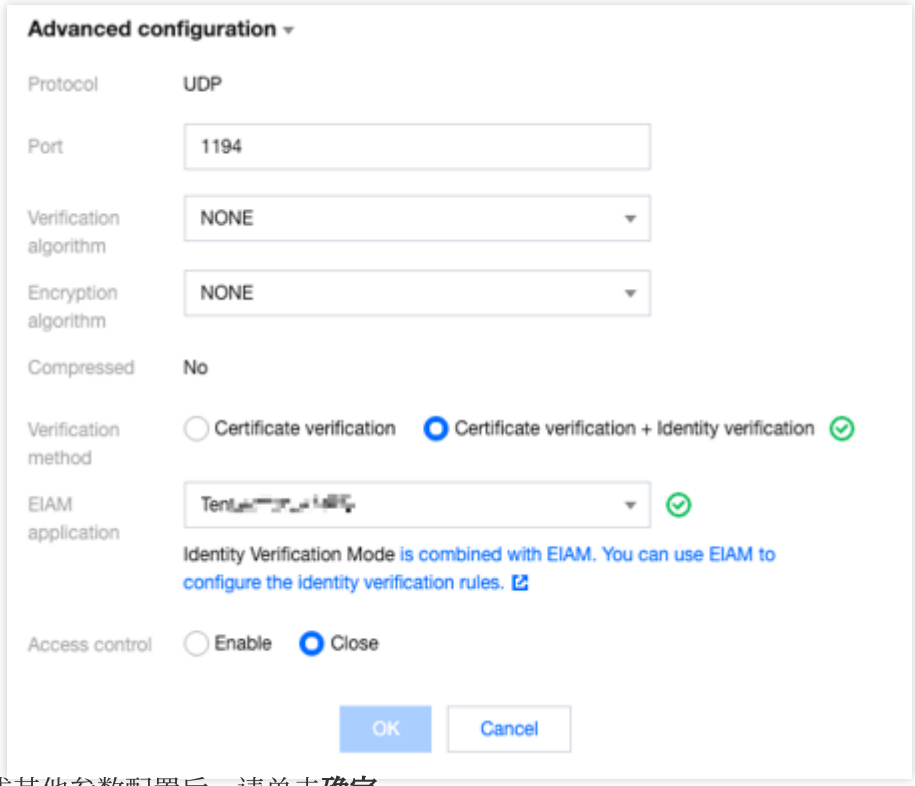
最近更新时间：2024-01-09 14:43:23

**说明：**

如您关闭访问控制，您所配置的访问策略条目将全部清空，服务端将默认接受所有连接。

## 创建 SSL 服务端时关闭

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击**+新建**。
4. 在弹出的**新建 SSL 服务端**对话框中，完成其他参数配置时将**访问控制**选择**关闭**。

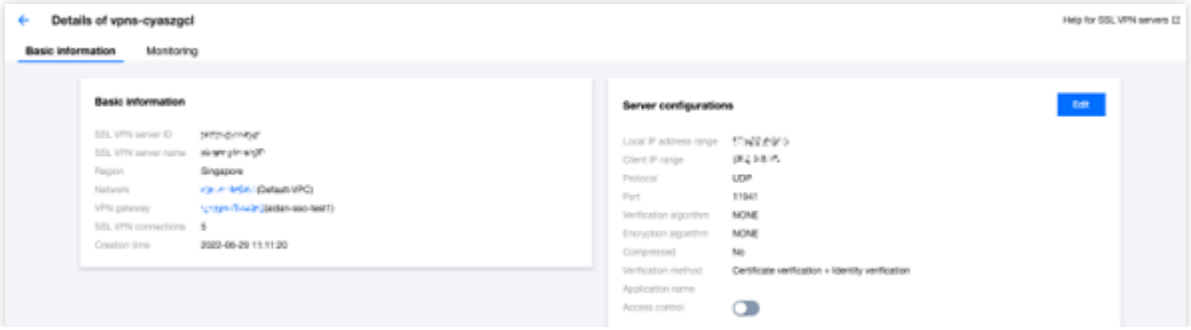



5. 完成其他参数配置后，请单击**确定**。

## 在 SSL 服务端创建完成后关闭

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击具体的实例名称。

4. 在实例详情页的**基本信息**页签的**服务端配置**区域关闭**访问策略**。



# 配置访问控制策略

最近更新时间：2024-01-09 14:43:23

为了确保您的业务的安全性，SSL VPN 提供了 SSL 服务端访问控制功能，精细化管理您的 SSL VPN。

**说明：**

目前只有支持 SSO 身份认证 SSL VPN 支持访问控制功能，详情请参见 SSO 认证。

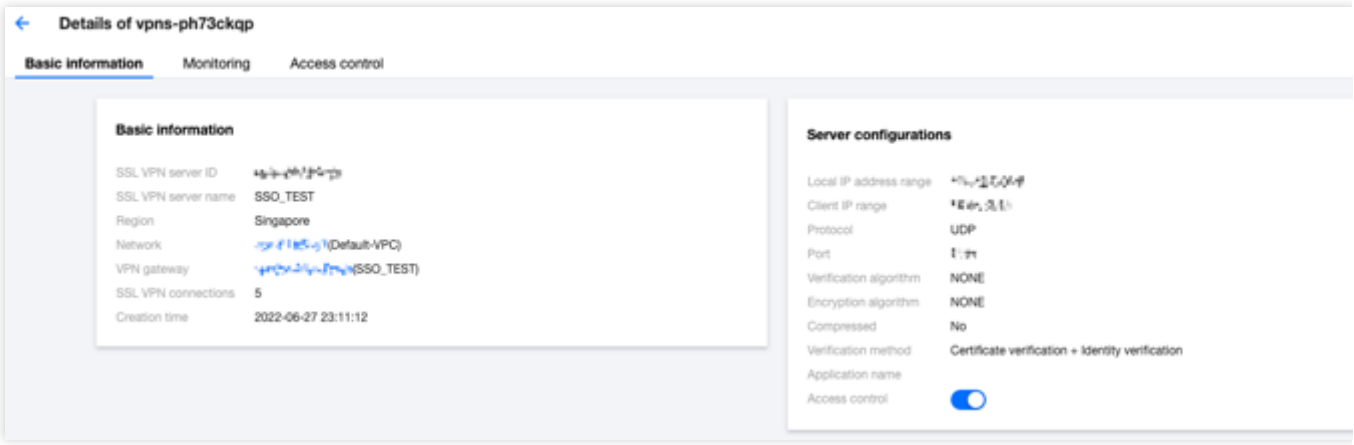
## 前提条件

在 数字身份管控平台 已创建用户组、添加了相应的用户并配为用户组配置应用授权。

在 VPN 控制台 已开启 SSL 服务端“证书认证 + 身份认证”，同步开启访问控制。

方式一：SSL 服务端创建过程中开启。


方式二：在 SSL 服务端创建完后开启。



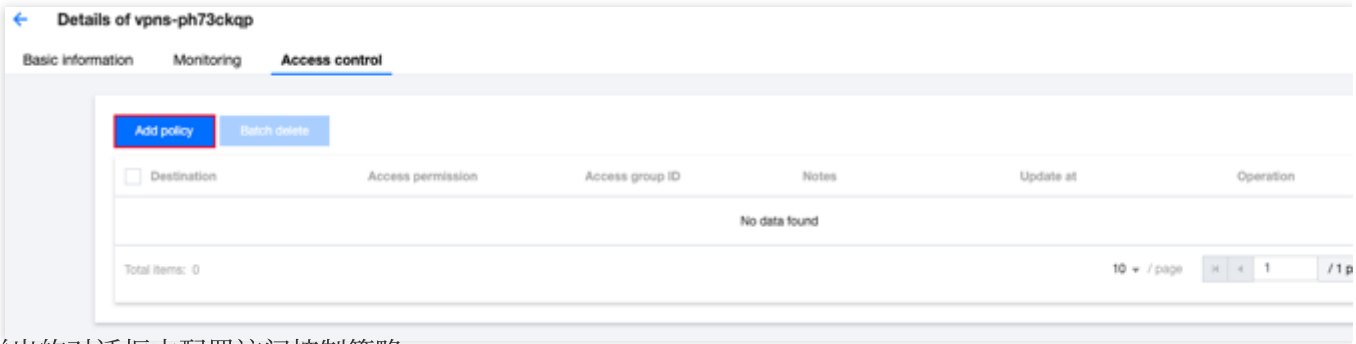

**注意：**

如果认证方式仅选择了**证书认证**，默认该 SSL 服务端可以被全量访问，即可以被任何客户端连接。

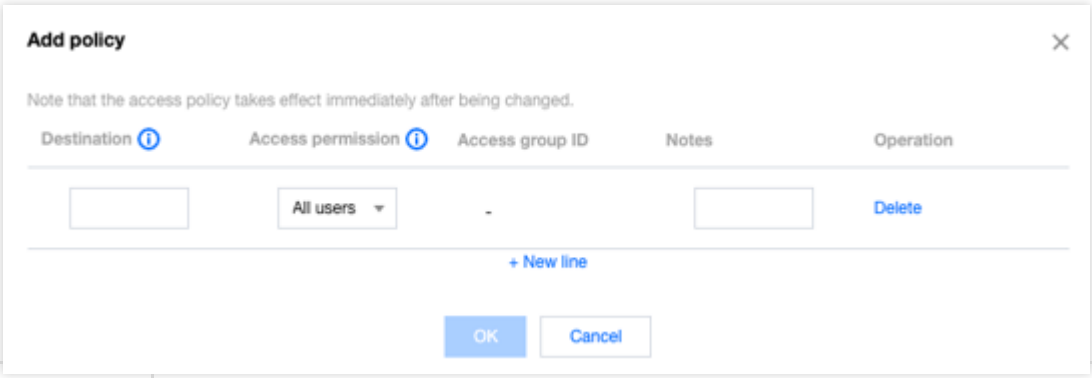
开启访问控制后，需要为 SSL 服务端配置访问控制策略，否则 SSL 服务端将拒绝所有连接访问。

# 配置访问控制策略

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击具体的实例名称。
4. 在实例详情页面单击**访问控制**，并单击**新增策略**。




5. 在弹出的对话框中配置访问控制策略。




| 参数名称 | 参数说明 |
| --- | --- |
| 目的端 | 填写需要本端 IP 网段，即访问云上的 IP 网段。<br>**说明：**<br>目的端网段需要与本端网段在同一网段内，若更改本端网段，需主动修改访问控制的目的端地址。 |
| 访问权限 | 特定用户组：该访问控制策略针对于指定的特定用户组生效，选择该项后需要配置访问组 ID。<br>全部用户：该访问控制策略针对于全部用户生效。<br>**说明：**<br>您可选择为特定用户组或全部用户配置访问策略，特定用户组可来自 身份认证平台 中用户组配置。 |
| 访问组 ID | 访问组 ID 为对应 EIAM 应用中用户组，支持多选。选择访问组 ID 后，该访问控制策略针对于特定用户组生效。 |
| 备注 | 必填，填写策略的备注信息，方便您后续识别策略信息。 |

6. 单击**确定**。

配置完成后，该 SSL 服务端将接受该用户组中用户的连接。

# 删除访问控制策略

**注意：**

访问控制策略删除后本策略中的用户组的客户端无法访问该 SSL 服务端。

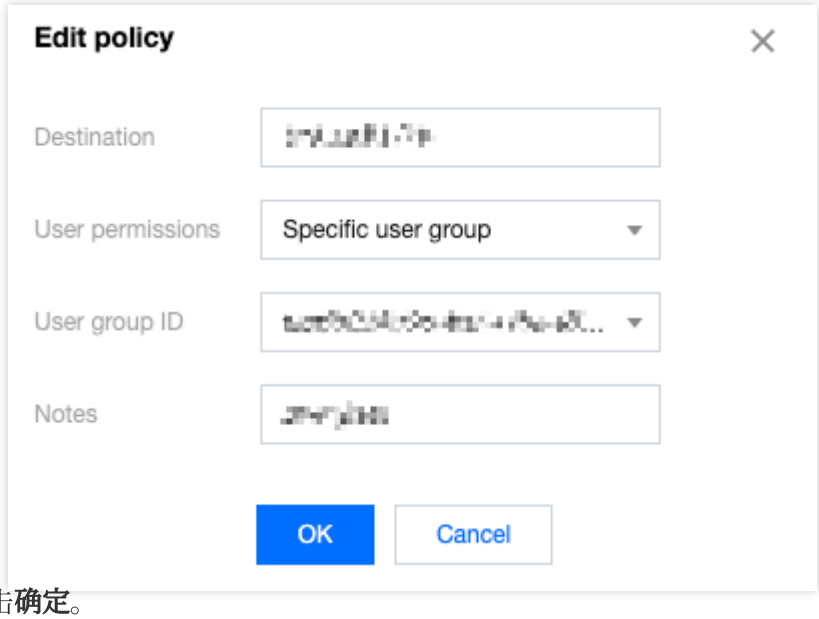
如果访问控制策略全部删除，该 SSL 服务默认拒绝所有客户端访问，如需被访问可继续配置访问策略或者认证方式改为**证书认证**。

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。

3. 在 SSL 服务端管理页面，单击具体的实例名称，在**访问控制**页签中删除对应的策略。
批量删除：在策略列表中选择需要删除的策略，然后单击**批量删除**。
单个删除：在待删除策略的操作列单击**删除**。
4. 在弹出的对话中单击**确定**。

# 编辑访问控制策略

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。
3. 在 SSL 服务端管理页面，单击具体的实例名称，在**访问控制**页签具体的策略操作列单击**编辑**，并依据实际情况修改相应的参数。




4. 单击**确定**。

# SSL 客户端
# 创建 SSL 客户端

最近更新时间：2024-01-09 14:43:23

SSL VPN 网关和 SSL 服务端创建完成后，您还需要在腾讯云侧创建 SSL 客户端证书。SSL 客户端证书记录了腾讯云分配给用户的 SSL 证书信息，即用于服务端和客户移动端进行双向认证的 SSL 证书。您可以下载该证书至移动端，并通过 OpenVPN 与腾讯云进行通信。

## 操作步骤

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页面。
3. 在 SSL 客户端管理页面，单击**新建**。
4. 在弹出的**新建 SSL 客户端**对话框中，配置如下参数。

| 参数名称 | 参数说明 |
| --- | --- |
| 名称 | 填写 SSL 服务端名称，不超过60个字符。 |
| 地域 | 展示 SSL 服务端所在地域。 |
| SSL 服务端 | 选择创建好的 SSL 服务端。 |

5. 完成 SSL 客户端参数设置后，单击**创建**启动 SSL 客户端创建，当**证书状态**为**可用**表示创建完成。

版权所有：腾讯云计算（北京）有限责任公司

# 查看 SSL 客户端

最近更新时间：2024-01-09 14:43:23

在 SSL 客户端创建完 SSL 客户端证书后，您可以在 SSL 客户端管理页查看 SSL 客户端证书详情。

## 前提条件

已 创建 SSL 客户端。

## 查看 SSL 客户端

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页。
该页面展示了 SSL 客户端 ID、名称、与客户端相连的 SSL 服务端、证书生效时间、证书到期时间、证书状态等信息。
3. 单击 SSL 服务端 ID 可以跳转至相连的 SSL 服务端，并查看服务端信息。

# 删除 SSL 客户端

最近更新时间：2024-01-09 14:43:23

在 SSL 客户端创建完 SSL 客户端证书后，您可以在 SSL 客户端管理页将其删除。

## 前提条件

已 创建 SSL 服务端。
已 创建 SSL 客户端。

## 删除 SSL 客户端证书

1. 登录 私有网络控制台。
2. 在左侧目录中单击**VPN 连接** > **SSL 客户端**，进入管理页。
单击 SSL 服务端 ID 可以跳转至相连的 SSL 服务端，并查看服务端信息。
3. 在需要删除的 SSL 客户端证书所在行单击**删除**。
**说明：**
该 SSL 客户端证书删除后，其关联的所有连接将立即中断，请务必确认后再进行操作。

# 下载 SSL 客户端配置

最近更新时间：2024-01-09 14:43:23

成功创建 SSL 客户端后，您可以在 SSL 客户端管理页下载客户端对应的配置，用于与 SSL 服务端连接。使用腾讯云下载的客户端配置，在 OpenVPN 或兼容 VPN 软件端与腾讯云 SSL 服务端连接时，将进行双向认证，通过后才允许该移动终端访问 SSL 服务端网关关联的云上资源（如 VPC 内的 CVM），确保您的通信安全。

## 租户管理员下载 SSL 客户端配置

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页。
3. 下载 SSL 客户端配置。

在具体 SSL 客户端证书实例所在行单击**下载配置**。

您需要将下载好的配置文件分发至需要通过 SSL VPN 连接腾讯云的用户（例如您的公司员工），该用户需使用此文件配置 OpenVPN 或兼容的 VPN 客户端，从而实现与腾讯云 VPC 互通。详细使用方法请参考 移动端配置。

**注意：**

请勿泄露配置文件给非相关人员，以避免您的资产受到损失。如果配置文件泄露，请及时停用SSL客户端，详情参考 停用 SSL 客户端证书。

## 用户通过自助 Portal 下载 SSL 客户端配置

如果您在创建 SSL 服务端时已开启身份认证，则移动终端的用户（例如您公司的员工）可以自助下载 OpenVPN 或兼容的 VPN 客户端所需的配置文件。同时，腾讯云通过身份认证确保整个下载过程的安全性。

### 前提条件

租户管理员已经在数字身份管控平台已创建用户组、添加了相应的用户并为用户组配置应用授权。

在 VPN 控制台已 创建 SSL 服务端，且 SSL 服务端支持身份认证。

租户管理员已经将开启身份认证的 SSL 服务端 ID 分发给您（作为用户）。如果没有，请联系您的管理员获取。

### 操作步骤

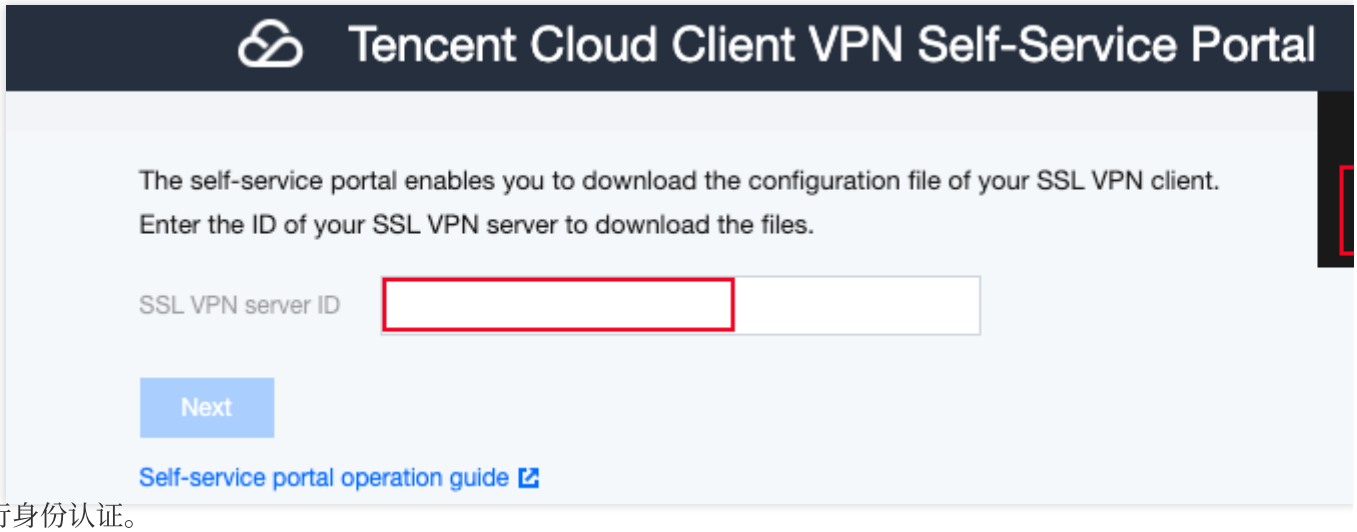
以下步骤由移动终端的用户（例如您公司的员工）自助进行。

1. 登录 腾讯云 Clinet VPN 自主服务门户。

**说明：**

建议使用 Chrome 浏览器最新版本。

2. 在 SSL 服务端 ID 所在行的输入框中输入前述管理员分发的 SSL 服务端实例 ID，然后单击**下一步**，进入登录界面。




3. 进行身份认证。

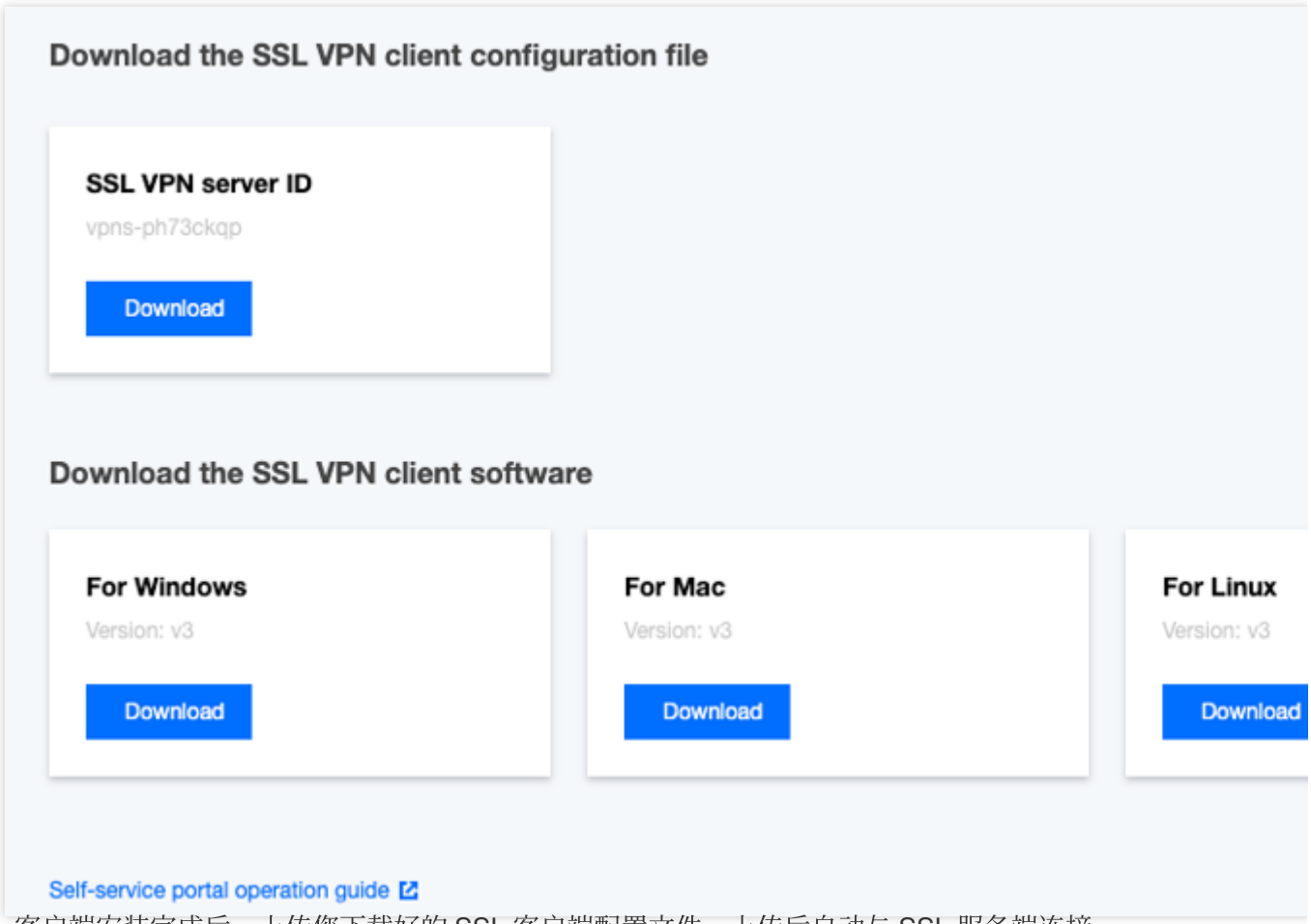
单击

进行 SAML 认证，然后单击**跳转进行认证（SAML）**进行登录。您需要使用您的租户管理员指定的身份认证方式通过认证。例如，租户管理员在 EIAM 指定与您的企业账号系统对接认证，则您将在浏览器上看到您归属企业的域账号登录页面，请输入您的域账号通过认证。如果管理员指定了其他的身份认证方式，如企业微信，则您需要通过对应的账号进行认证。

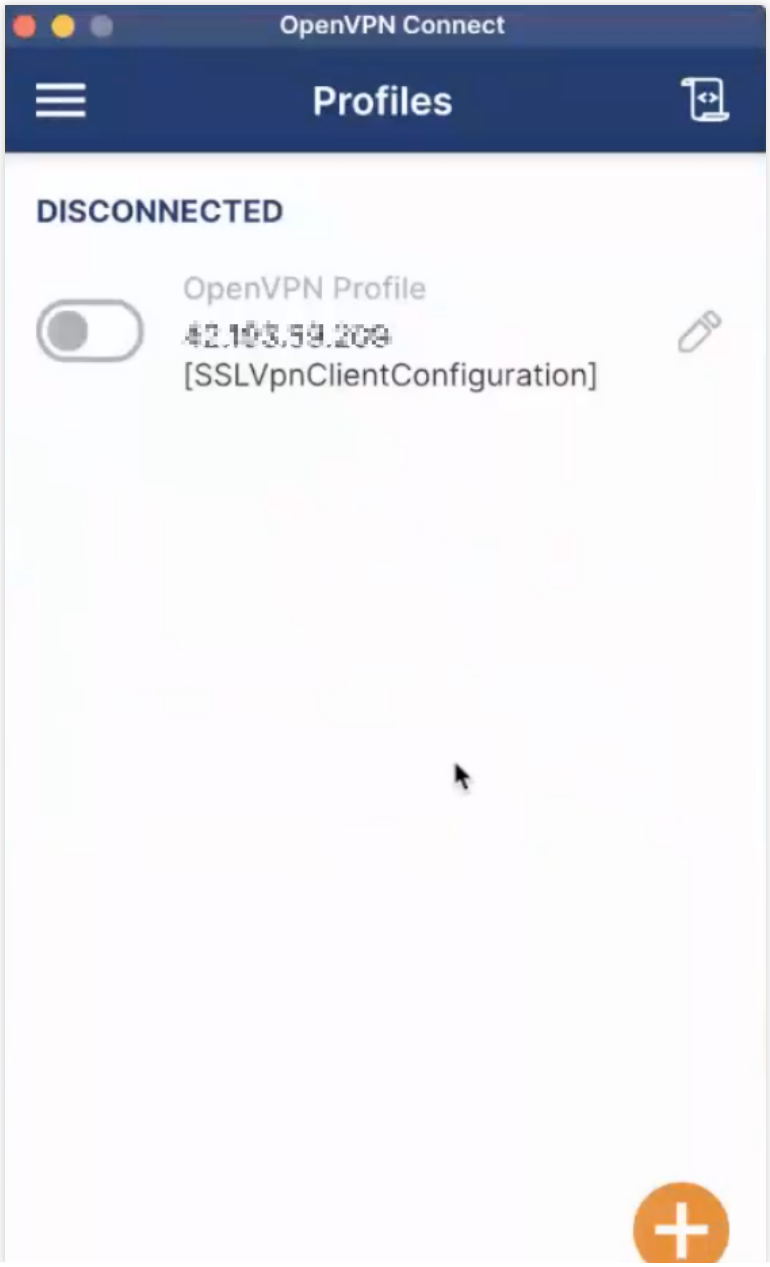
**说明：**

1. 目前仅支持通过 SAML 认证登录，请确保您在 EIAM 的用户组中，并在 SSL 访问控制策略中。如果提示“未授权访问该应用，请联系管理员”，可联系管理官将您添加到 EIAM 用户组即可。
2. 如果您有修改 EIAM 应用需求，请确保原 EIAM 应用中的用户已经迁移至新的 EIAM 应用，避免原应用中用户无法访问。
3. 切换 EIAM 应用后，已连接的 SSL VPN 连接不会中断。
4. 下载 SSL 客户端配置文件和 SSL 客户端。
5. 在**下载 SSL 客户端配置文件**区域找到您需要下载的客户端配置文件，单击**下载**。
6. 在**下载 SSL 客户端**区域找到适合您的 SSL 客户端软件，下载后请安装该客户端。

版权所有：腾讯云计算（北京）有限责任公司




7. SSL 客户端安装完成后，上传您下载好的 SSL 客户端配置文件，上传后自动与 SSL 服务端连接。


OpenVPN Connect
Profiles
DISCONNECTED
OpenVPN Profile
[SSLVpnClientConfiguration]

# 启用和停止 SSL 客户端证书

最近更新时间：2024-01-09 14:43:23

在 SSL 客户端创建的 SSL 客户端证书默认是开启的，需要关闭在启动证书列操作。

## 启用 SSL 客户端证书

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页。
3. 在待开启的证书所在行打开启用开关。

## 停用 SSL 客户端证书

1. 登录 私有网络控制台。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页。
3. 在已开启的证书所在行关闭启用开关。

版权所有：腾讯云计算（北京）有限责任公司

# 绑定 DDos 高防包

最近更新时间：2024-01-09 14:43:23

1. 登录 DDoS 防护（大禹）管理控制台，选择 **DDoS 高防包** > **资产列表**，选择地域。
若您的 DDoS 高防包实例是独享包，则选择**独享包**页签。
若您的 DDoS 高防包实例是共享包，则选择**共享包**页签。
2. 在列表中找到您需要绑定的 DDoS 高防包实例，单击该实例操作栏中的**更换设备**。
3. 在弹出框中选择关联设备类型和关联机器，设备类型选择 “VPN 网关”，在列表中选择您需要关联的 VPN 网关。
4. 选择完毕后，单击**确认**即可。

版权所有：腾讯云计算（北京）有限责任公司

# 告警与监控

# 设置告警

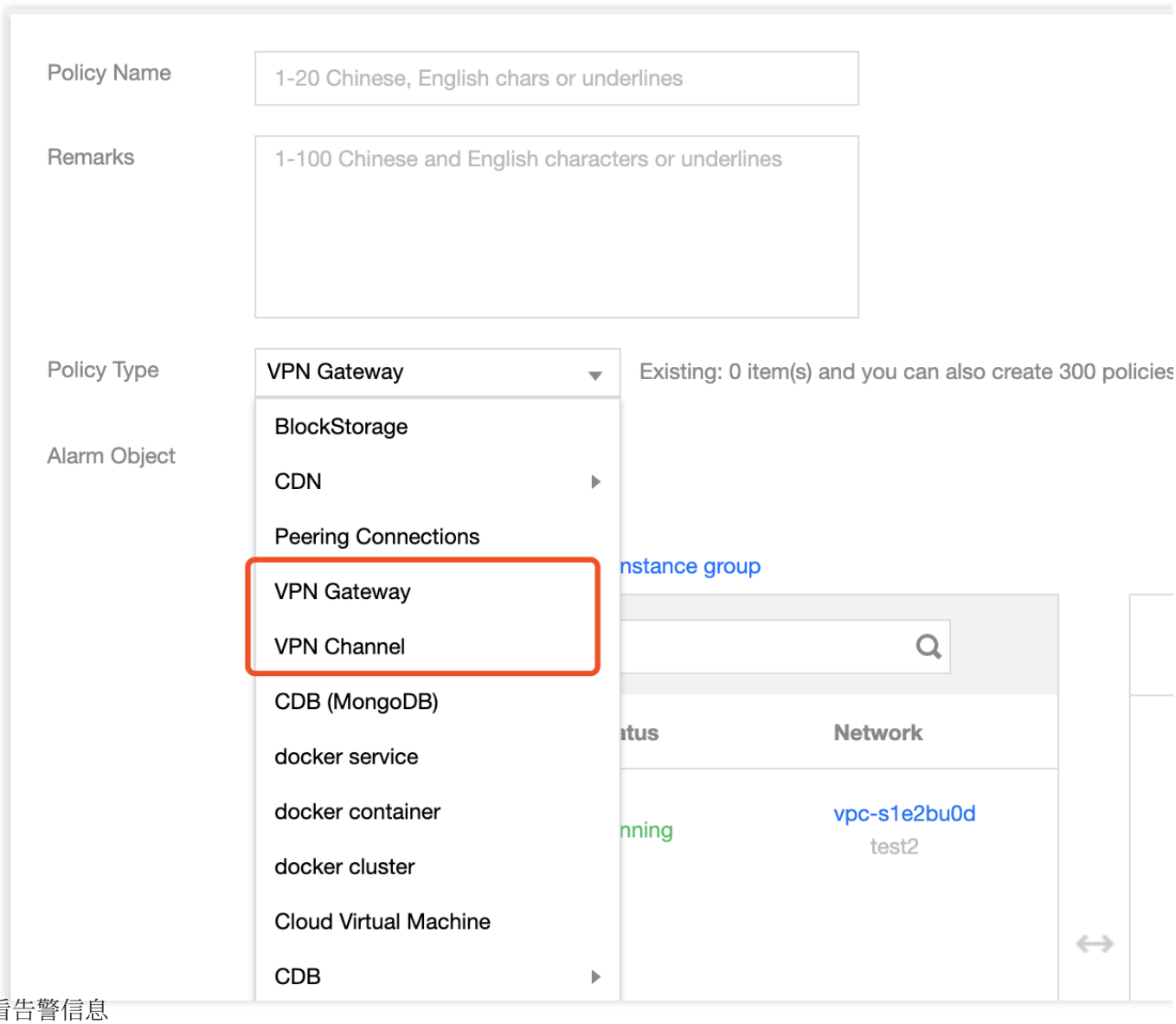
最近更新时间：2024-01-09 14:43:23

您可以为 VPN 连接设置自定义流量告警，当指标超过一定阈值时自动告警，告警消息会通过电子邮件和短信发出，帮助您提前预警风险。告警服务无需额外收费，同时当故障发生时，能帮助您快速定位问题。

## 操作步骤

1. 登录 云监控控制台。
2. 在左侧目录选择**告警配置** > **告警策略**，进入告警策略配置页面，单击**新增**。
3. 填写告警策略名称，策略类型选择私有网络> VPN 通道，选择告警对象，设置告警策略，选择告警接收组和告警渠道，单击**完成**，即可在告警策略列表中查看已设置的告警策略。

版权所有：腾讯云计算（北京）有限责任公司




4. 查看告警信息

告警条件被触发后，您将通过已选择的告警渠道接收到告警通知（短信 / 邮件 / 微信等），也可以单击左侧目录**告警历史**查看。更多告警相关信息，请参考告警配置。

# 查看监控数据

最近更新时间：2024-01-09 14:43:23

VPN 通道和 VPN 网关提供监控数据查看功能，监控服务无需额外收费，同时当故障发生时，能帮助您快速定位问题。

## VPN网关

1. 登录 私有网络控制台。
2. 单击左导航栏中 **VPN 连接** > **VPN 网关**。
3. 选择地域和私有网络，单击列表中需要查看的 VPN 网关监控图标，即可查看监控数据。
 也可单击网关ID进入详情页，在**监控**页签查看。
4. 单击左导航栏中 **VPN 连接** > **VPN 通道**。

## VPN通道

1. 登录 私有网络控制台。
2. 单击左导航栏中 **VPN 连接** > **VPN 通**道。
3. 选择地域和私有网络，单击列表中需要查看的 VPN 通道监控图标，即可查看监控数据。

## 相关文档

VPN 网关监控指标
VPN 通道监控指标

版权所有：腾讯云计算（北京）有限责任公司

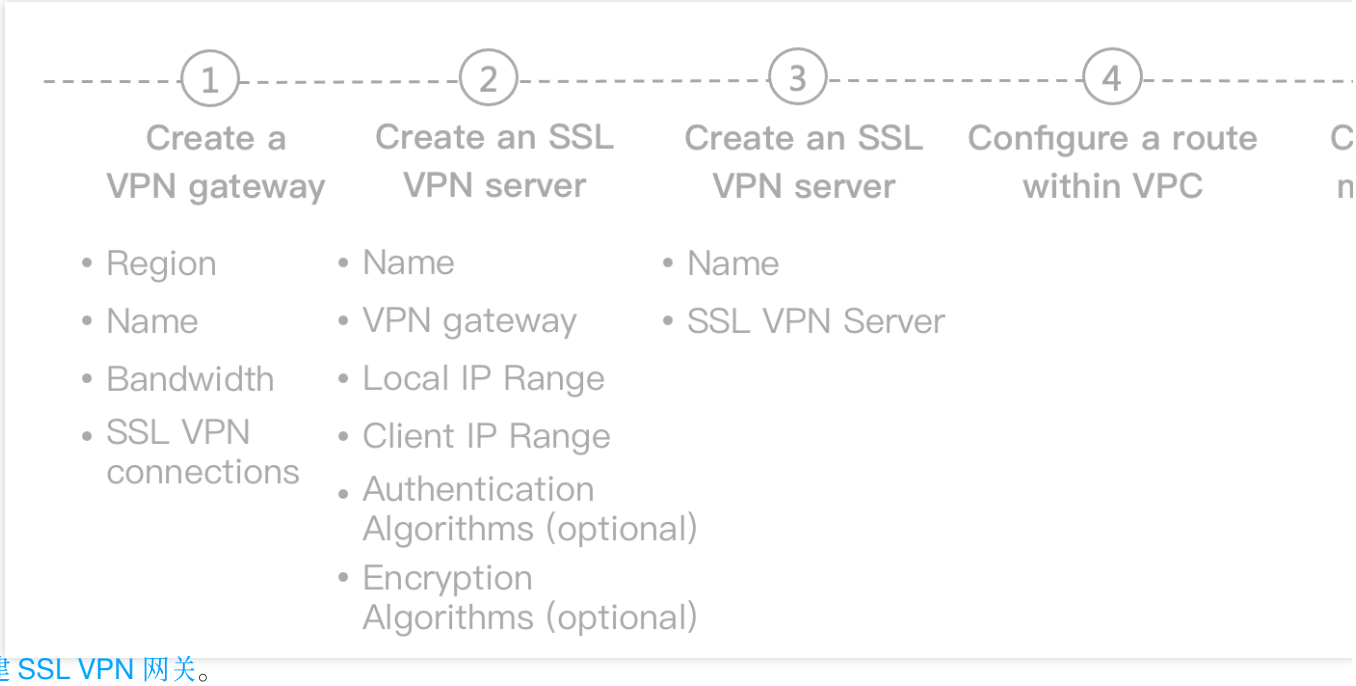
# SSL VPN 配置指南
# SSL VPN 配置指引

最近更新时间：2024-01-09 14:43:23

## 前提条件

本地设备和腾讯云侧 VPC 内私有网段不能相同，避免出现 IP 冲突。
客户端已连接公网。

## 配置流程




1. 创建 SSL VPN 网关。
创建 SSL 协议类型的 VPN 网关。
2. 创建 SSL 服务端。
在 SSL 服务端中指定要连接的腾讯云侧网段和客户端网段。
3. 创建 SSL 客户端。
用户使用证书和密钥与 VPN 网关建连，用户侧验证服务端证书，服务端验证用户端证书，校验通过后，服务端从客户端 IP 地址池中分配一个 IP 给用户，该 IP 用于和 VPC 内 CVM 通信时使用。
4. 配置 VPC 内路由。
在 VPC 内配置流量从用户移动端到腾讯云 VPC 内的路由转发策略，目的地址为客户端网段，下一跳类型为 VPN 网关，下一跳为 SSL VPN 网关。

版权所有：腾讯云计算（北京）有限责任公司

5. 配置用户移动端。

在用户移动端完成 SSL 证书配置。

6. 测试连通性。

腾讯云侧和用户移动端配置完成后，使用 Ping 验证 SSL VPN 连接的连通性。

# IPSec VPN 配置指南
# IPSec VPN 配置指引

最近更新时间：2024-01-09 14:43:23

## 前提条件

本地设备和腾讯云侧 VPC 内私有网段不能相同，避免出现 IP 冲突。

## 配置流程

1. 创建 IPSec VPN 网关。
 创建 IPSec 协议类型的 VPN 网关。
2. 创建对端网关。
在 SSL 服务端中指定要连接的腾讯云侧网段和客户端网段。
3. 创建 VPN 通道。
 用户使用证书和密钥与 VPN 网关建连，用户侧验证服务端证书，服务端验证用户端证书，校验通过后，服务端从客户端 IP 地址池中分配一个 IP 给用户，该 IP 用于和 VPC 内 CVM 通信时使用。
4. 用户本地网关配置。
 在用户侧完成网关配置。
**注意：**
 腾讯 IPSec VPN 支持业界主流的用户端网关（防火墙），具体配置请参考 本地网关配置 。
5. 配置 VPC 内路由。
 在 VPC 内配置流量从 IDC 到腾讯云 VPC 内的路由转发策略，目的地址为对端网络的网段，下一跳类型为 VPN 通道/云联网。
如果**下一跳类型**为**VPN 通道**，则选择已创建的 VPN 通道。
如果**下一跳类型**为**云联网**，则系统自动展示该 VPN 网关关联的云联网实例。
6. 测试连通性。
 腾讯云侧和用户侧完成配置后，使用 Ping 验证 IPSec VPN 连接的连通性。

# 操作总览

最近更新时间：2024-01-09 14:43:23

VPN 连接通过公网加密通道实现用户 IDC、内部办公网络与腾讯云 VPC 的安全通信。VPN 网关提供 IPsec VPN 连接。您可以通过 VPN 控制台完成 VPN 连接的配置及管理。例如查看监控数据、修改 VPN 通道配置、绑定高防包等。本文将介绍使用 VPN 连接的控制台操作指南。

版权所有：腾讯云计算（北京）有限责任公司