

[首页](#)[探索掘金](#)[登录](#)**AhuntSun** Lv2

2020年02月22日 阅读 1397

[关注](#)

简单谈谈虚拟专用网VPN

虚拟专用网VPN

1.1.两类地址

本地地址——仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向因特网的管理机构申请。

全球地址——全球唯一的IP地址，必须向因特网的管理机构申请。

1.2.RFC 1918 指明的专用地址 (private address)

10.0.0.0 到 10.255.255.255

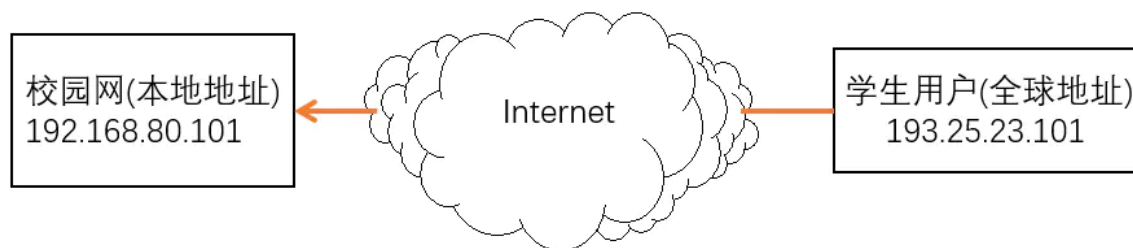
172.16.0.0 到 172.31.255.255

192.168.0.0 到 192.168.255.255

这些地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信。

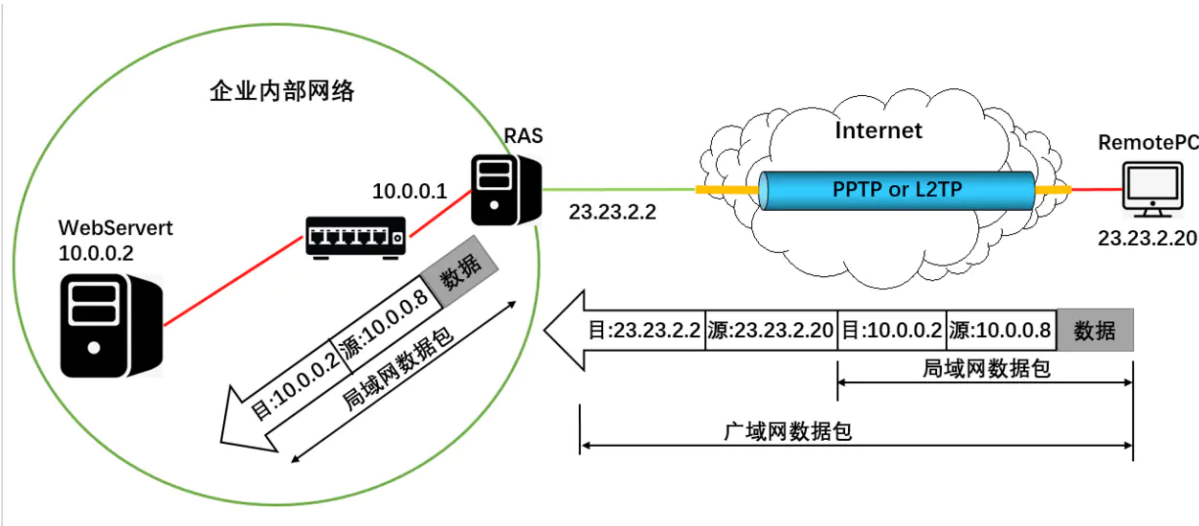
专用地址只能用作本地地址而不能用作全球地址。在因特网中的所有路由器对目的地址是专用地址的数据报一律不进行转发。

而虚拟专用网VPN技术实现的功能就是使全球地址也能访问本地地址。例如：



访问校园网。

1.3.远程访问VPN示意图



如图，一个用户出差在外，它的计算机公网地址为23.23.2.20。在企业内部有一个远程访问服务器(RAS)，上面有两个网卡，分别连接企业内网和外部因特网。企业内部有一台IP地址为10.0.0.2的WebServer。
(RAS表示远程访问服务器，即VPN服务器)

若远程用户想要访问WebServer，先要向公司内部配置好的远程访问服务器拨号，拨号拨通之后，远程访问服务器就会给远程用户一个私网地址：10.0.0.8。即远程用户获得了两个IP地址：一个公网地址23.23.2.20，拨号后获得的一个私网地址10.0.0.8。然后该用户就有能力访问企业内网的WebServer了。

VPN技术的实现过程为：

当远程用户与企业内网WebServer通信时，数据包中的源地址和目标地址都为私网地址，但是互联网上的路由器不转私网数据包。解决方法为：

远程用户在公网上访问企业内部服务器RAS时，先使用RAS服务器分配的私网地址作为数据包的源地址，企业内部网的WebServer地址作为目标地址组成局域网数据包。然后远程用户再使用自己的公网地址作为源地址，RAS服务器的公网地址作为目标地址对局域网数据包进行封装，组成广域网数据包。由于广域网数据包的目标地址和源地址都为公网地址，所以数据包可以通过互联网顺利中转到企业内的RAS服务器上。

同样的，从WebServer发出的数据包，经过远程访问服务器RAS中转至公网前，先对数据包进行封装，加上一层公网的目标地址和源地址

即远程用户和企业内配置好的远程访问服务器RAS都拥有一个私网地址和一个公网地址，在公网上通信时使用广域网数据包，在私网内通信时使用局域网数据包。

VPN技术的实质就是在互联网上传输私有数据，但是使用Internet传输私有数据是不安全的。可以通过采取一定的安全措施使得这个传输过程变得安全，比如采用PPTP 或 L2TP等传输协议对数据进行加密和拨号前进行身份验证等。通过这些手段相当于建立了一段安全的专线，可以不安全的环境安全地传输私有数据，这就叫做**虚拟专用网络**。

1.4.创建VPN拨号连接

掌握VPN拨号技术可以帮助我们解决出差在外，远程连接公司内网VPN服务器，远程办公的需求。以Win10为例，创建VPN拨号连接的方法如下：

在桌面 "网络" 图标右键 "属性" 打开网络和共享中心，点击 "设置新的连接或网络"。



在打开的窗口中选择 "连接到工作区"。





选择一个连接选项



连接到 Internet
设置宽带或拨号连接，连接到 Internet。



设置新网络
设置新的路由器或接入点。



手动连接到无线网络
连接到隐藏网络或创建新无线配置文件。



连接到工作区
设置到你的工作区的拨号或 VPN 连接。

下一步(N)

取消

点击 "使用我的Internet连接(VPN)"。



[首页](#) ▼[探索掘金](#)[登录](#)

你希望如何连接?

→ 使用我的 Internet 连接(VPN)(I)
通过 Internet 使用虚拟专用网络(VPN)来连接



→ 直接拨号(D)
不通过Internet直接使用电话号码来连接。



取消

在打开的窗口中，红色框内输入VPN服务器的公网地址，蓝色框中输入VPN服务器的名称。输入完成后点击“创建”。



[首页](#) ▼[探索掘金](#)[登录](#)

键入要连接的 Internet 地址

网络管理员可提供此地址。

Internet 地址(I):

222.223.239.89

目标名称(E):

新建VPN拨号连接

☐ 使用智能卡(S)

☒ 记住我的凭据(R)



☐ 允许其他人使用此连接(A)

这个选项允许可以访问这台计算机的人使用此连接。

[创建\(C\)](#)[取消](#)

创建完成后，回到 "网络和共享中心" 窗口，通过 "更改适配器设置" 选项打开 "网络连接" 窗口。

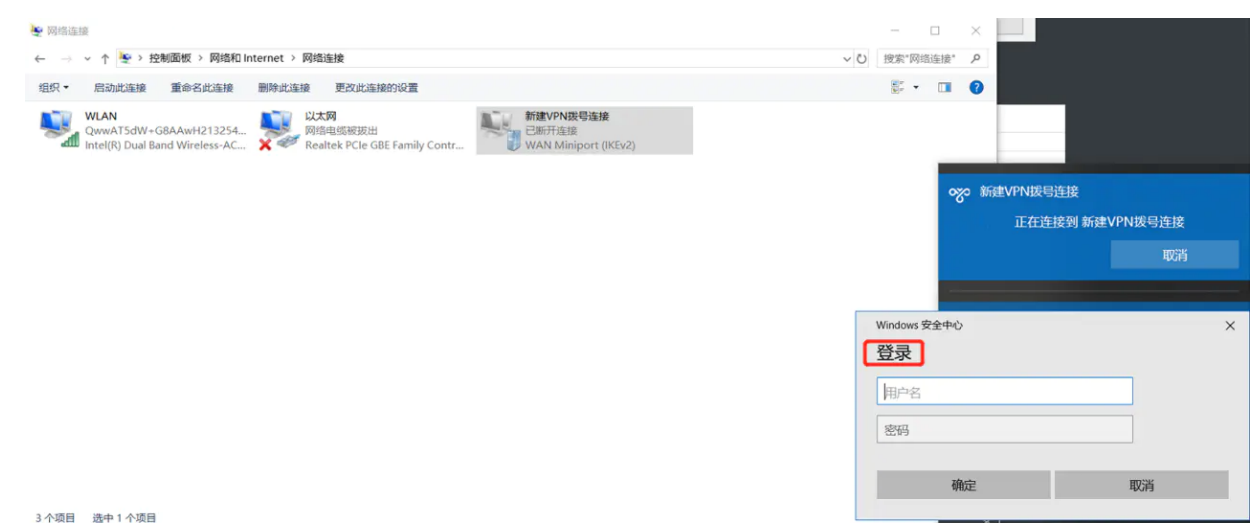


可以看到出现了刚才创建的VPN拨号连接。

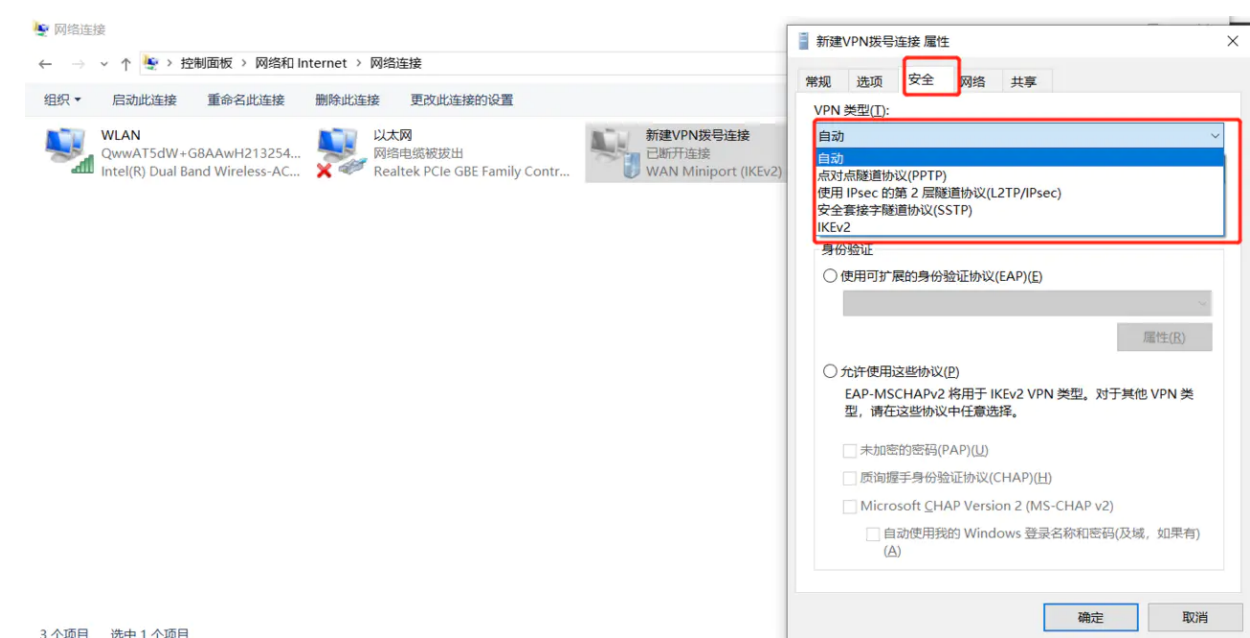




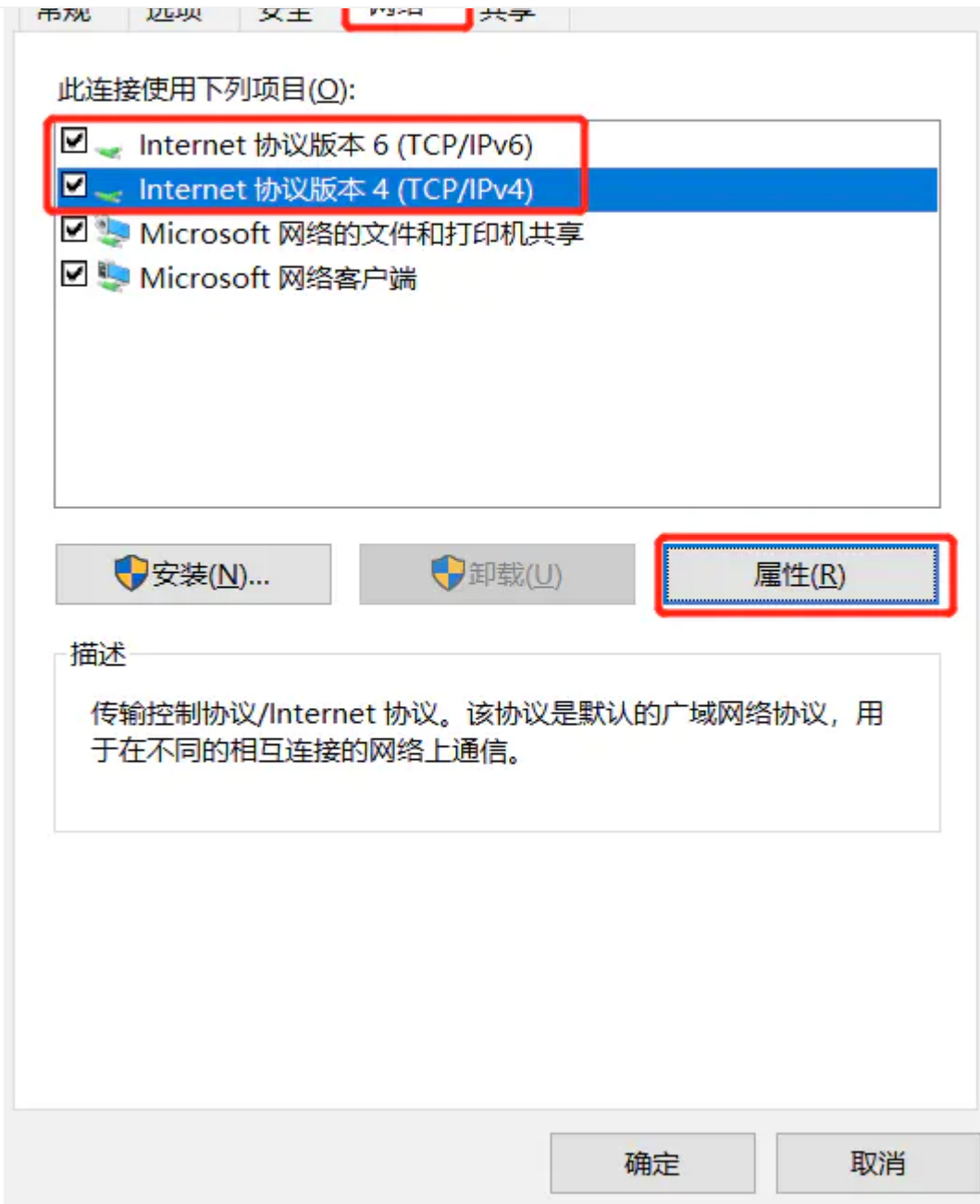
当连接该VPN服务器时，需要进行登录验证。



在新建的VPN连接处右键 "属性"，可以在 "安全" 选项卡下设置VPN类型，即选择在创建的VPN连接中传输数据时使用的协议。



在 "网络" 选项卡下选择IPv6或IPv4选项后，点击 "属性" 。

[首页](#) ▾[探索掘金](#)[登录](#)

在打开的IP协议属性窗口点击 "高级"。



[首页](#) ▾[探索掘金](#)[登录](#)

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

☒ 自动获得 IP 地址(O)

☐ 使用下面的 IP 地址(S):

IP 地址(I):

. . .

☒ 自动获得 DNS 服务器地址(B)

☐ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

. . .

备用 DNS 服务器(A):

. . .

高级(V)...

确定

取消

在打开的窗口中，去掉默认勾选的 "在远程网络上使用默认网关" 的选项。





IP 设置 DNS WINS

此复选框只应用于你同时连接到局域网和拨号网络上。如果选中，不能发送到局域网上的数据将被转发到拨号网络上。

☐ 在远程网络上使用默认网关(U)

☐ 禁用基于类的路由添加

☒ 自动跃点(A)

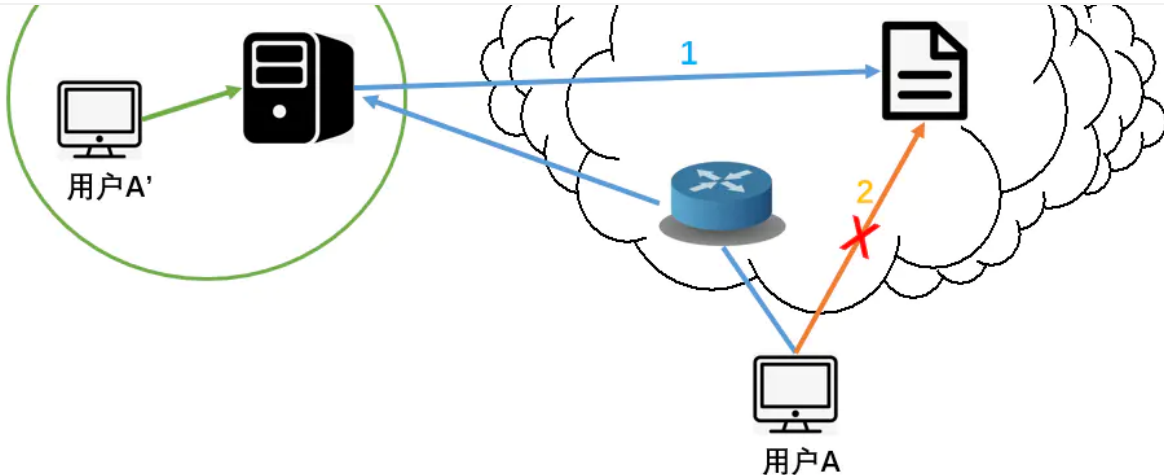
接口跃点数(N):

确定

取消

该选项的作用为:



[首页](#)[探索掘金](#)[登录](#)

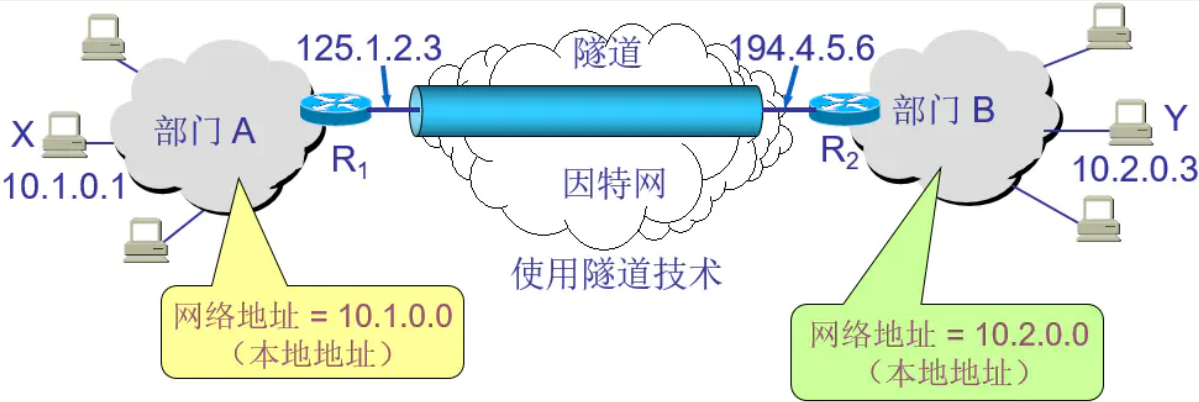
如图，远程用户A使用VPN技术，通过Internet访问企业内网相当于直接把电脑搬到企业里直接访问，如用户A'所示。但是当用户A想要访问Internet上的网站时，不能走线路2直接访问Internet，而是走的线路1，先访问企业内网，再在企业内网里访问Internet。相当于用户A在企业里访问Internet，绕了远路。

取消了上述选项的作用可以理解为：告诉远程用户A不用先把所有数据流量传输到企业内网，再让企业内网的服务器决定如何中转这些流量来访问Internet。而是使用用户A的公网地址，采用线路2直接访问Internet。即用户A到企业内网网段的流量走线路1，到其他网段的直接走线路2。

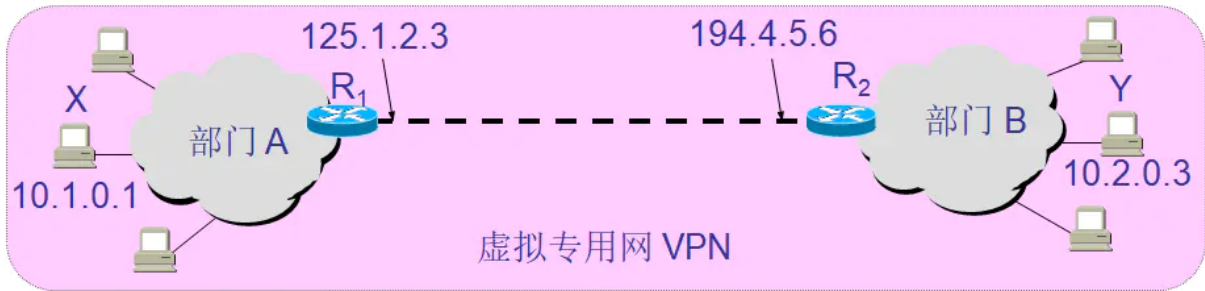
全部设置完成后，通过登录认证连接VPN服务器，连接成功后，会发现所连接的VPN服务器给本地计算机分配了一个私网地址。

1.5.用隧道技术实现虚拟专用网

隧道技术是基于上述地VPN原理，实现数据在互联网上的安全传输的技术。



1.6.内联网 intranet 和外联网 extranet



由部门 A 和 B 的内部网络所构成的虚拟专用网 VPN 又称为**内联网**(intranet)，表示部门 A 和 B 都是在**同一个机构**的内部。

一个机构和某些**外部机构**共同建立的虚拟专用网 VPN 又称为**外联网**(extranet)。

两种网络的实现都是基于 TCP/IP 协议。

1.7.VPN技术的实际应用

内网互联：

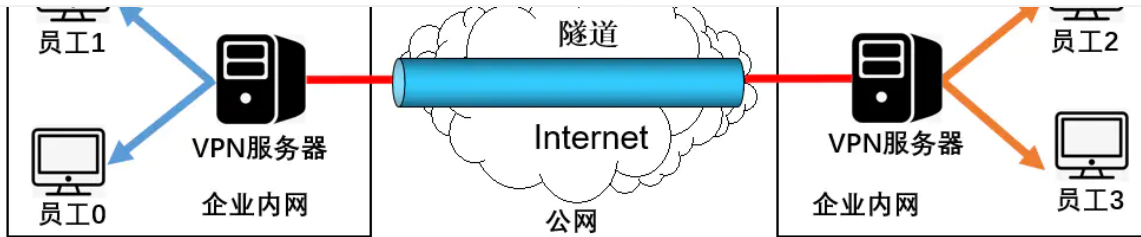
情况一：



首页 ▾

探索掘金

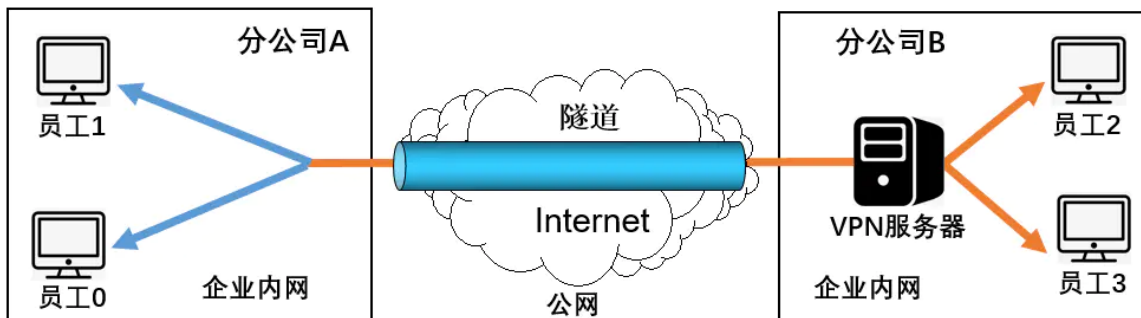
登录



如图，分公司A与分公司B两个企业内网通过Internet连接在一起，两个分公司只要配置好各自的VPN(远程访问)服务器，就可以通过VPN隧道技术实现两企业内网间的无障碍访问，且企业内网用户无需拨号申请公网地址，相当于两个分公司的员工同在一个局域网下，只不过速度慢了点。

这种VPN技术在许多连锁店铺中经常用到，因为全国的连锁店每日的账目都需要通过网络来传输汇总。

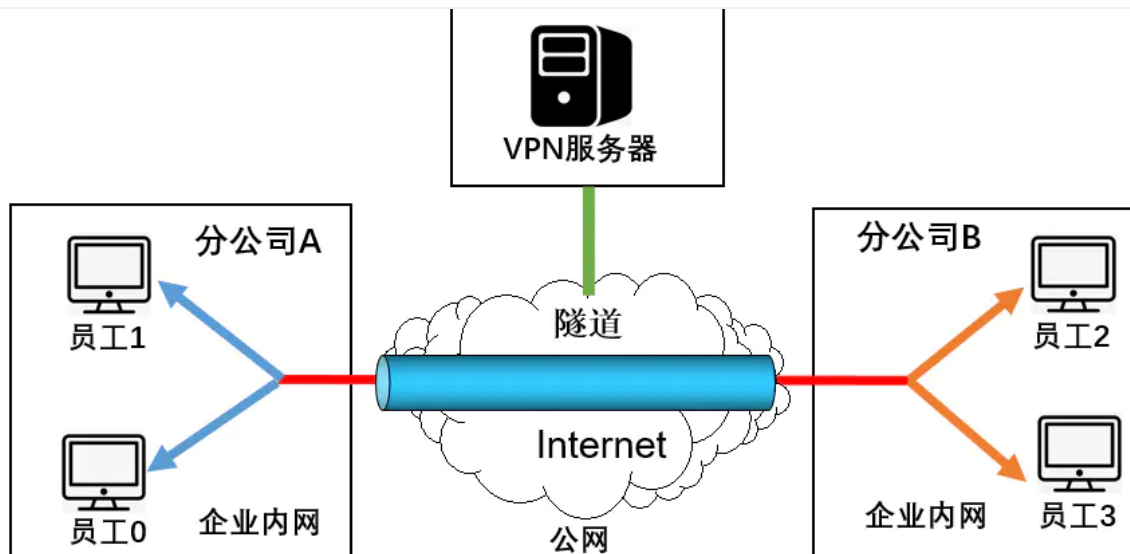
情况二：



只要分公司A或B中的一方有配置VPN服务器，另一方就可以通过VPN服务器访问该分公司的内网。比如在上图中，分公司B配置了VPN服务器，那么分公司A的员工1就能通过该VPN服务器远程连接分公司B内网中的员工2。

情况三：

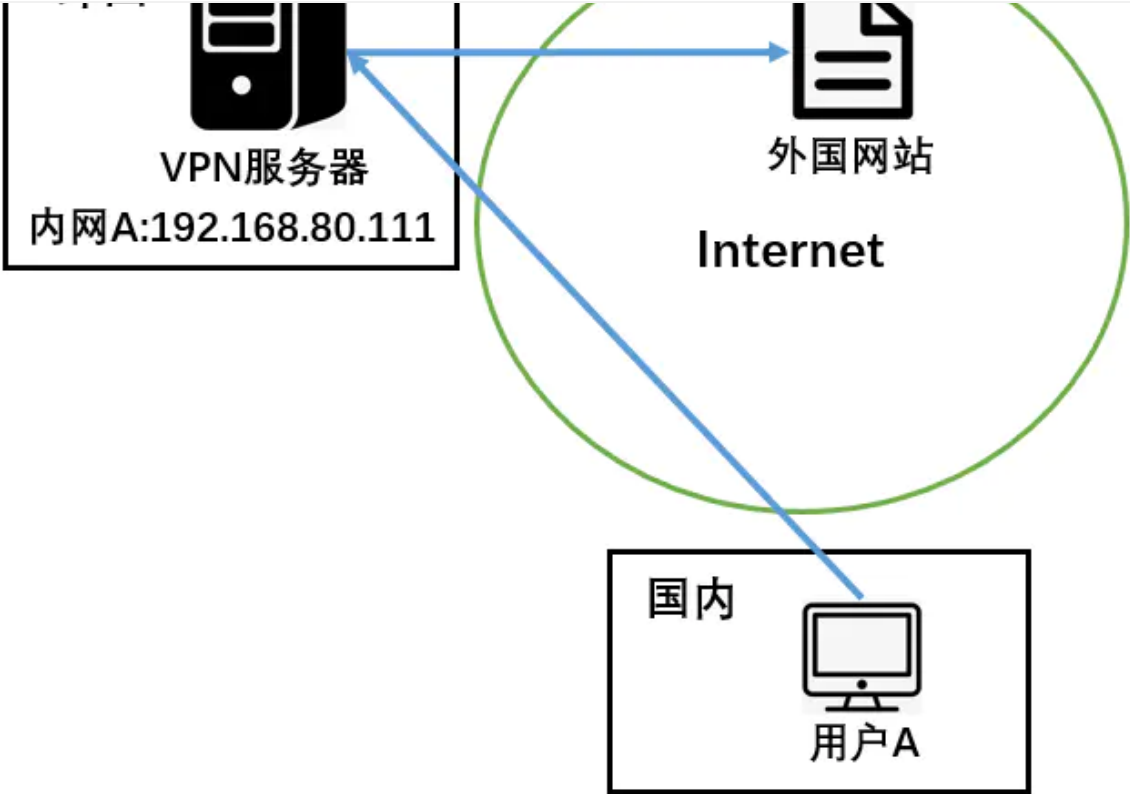


[首页](#) ▾[探索掘金](#)[登录](#)

分公司A和B双方都没有配置VPN服务器，分公司C配置了VPN服务器，那么分公司A和B都可以通过该VPN服务器访问其他分公司的内网用户。

访问外网：

访问外网，即所谓的翻墙，由于防火墙的限制，国内用户无法访问大多数的国外网站，而使用VPN技术可以实现无障碍访问外网。




大多数外国网站都会拦截来自国内网段的数据包，国内的用户A想要访问Internet上的外国网站，可以通过向布置在外国某内网里的VPN服务器拨号，以此来获得外国网段的公网地址，相当于把用户A搬到了外国的内网A里面。由此实现了对外国网站的访问。

我们平常使用的VPN软件，其原理就是向位于世界各地的VPN服务器拨号，以此获得外国网段的公网地址，实现外网访问。

关注下面的标签，发现更多相似文章

设计



AhuntSun

前端开发工程师

获得点赞 37 · 获得阅读 7,000

关注

安装掘金浏览器插件





输入评论...

相关推荐

秦国首席剑术教师的学生 · 8天前 · 架构 / 设计

技术需求文档，应当这么写！

👍 9



伴鱼技术团队 · 24天前 · 后端 / 设计

调用链追踪系统在伴鱼：理论篇

👍 16



Isvih · 25天前 · 设计 / 掘金翻译计划

构建设计系统和组件库

👍 9



阿里山小火车 · 22天前 · 设计

Activiti 工作流与业务整合实战

👍 1



夏天是个胖子 · 1月前 · 设计

SSO 前端设计与思路

👍 9



慕客 · 1月前 · 设计

UI & UX 小提示合集 -- 第一集

👍



慕客 · 1月前 · 设计

超全面的 UI 工作流程指南（三）：设计规范

👍 4





首页 ▾

探索掘金

登录

图用有哪三优势：为什么我们使用图用：如何使用：

👍 8

💬 1

摹客 · 6月前 · 设计

提升用户体验？指示性设计元素不可或缺

👍 2

💬 1

蚂蚁RichLab前端团队 · 2月前 · 支付宝 / 设计

SEE Conf 2021 如期而至，体验科技极致美

👍 4

💬 3

奔跑的毛球 · 29天前 · 设计

高可用系统设计原则

👍 1

💬

doodlewind · 3年前 · 编程语言 / 前端 / 设计模式 / 设计

如何无痛降低 if else 面条代码复杂度

👍 1182

💬 104

J_Knight_ · 2年前 · iOS / API / 设计 / UML

面向对象设计的六大设计原则（附 Demo & UML类图）

👍 384

💬 64

吴德宝AllenWu · 3年前 · Go / API / 设计 / 后端

Golang的反射reflect深入理解和示例

👍 143

💬 10

凹凸实验室 · 6月前 · 设计 / 前端

design tokens —— 设计和开发碰撞的火花

👍 27

💬 2

众成翻译 · 24天前 · 设计

构建视觉语言/ Airbnb设计

👍 1

💬



从0到1搭建企业级后台

👍 3

💬

摹客 · 1月前 · 设计

摹客：无需登录快速访问全貌画板

👍 2

💬 2

owlling · 21天前 · 设计

从多维度考量设计等待

👍 1

💬

大愚Talk · 8月前 · Go / 设计

Golang技巧之默认值设置的高阶玩法

👍 17

💬 11

