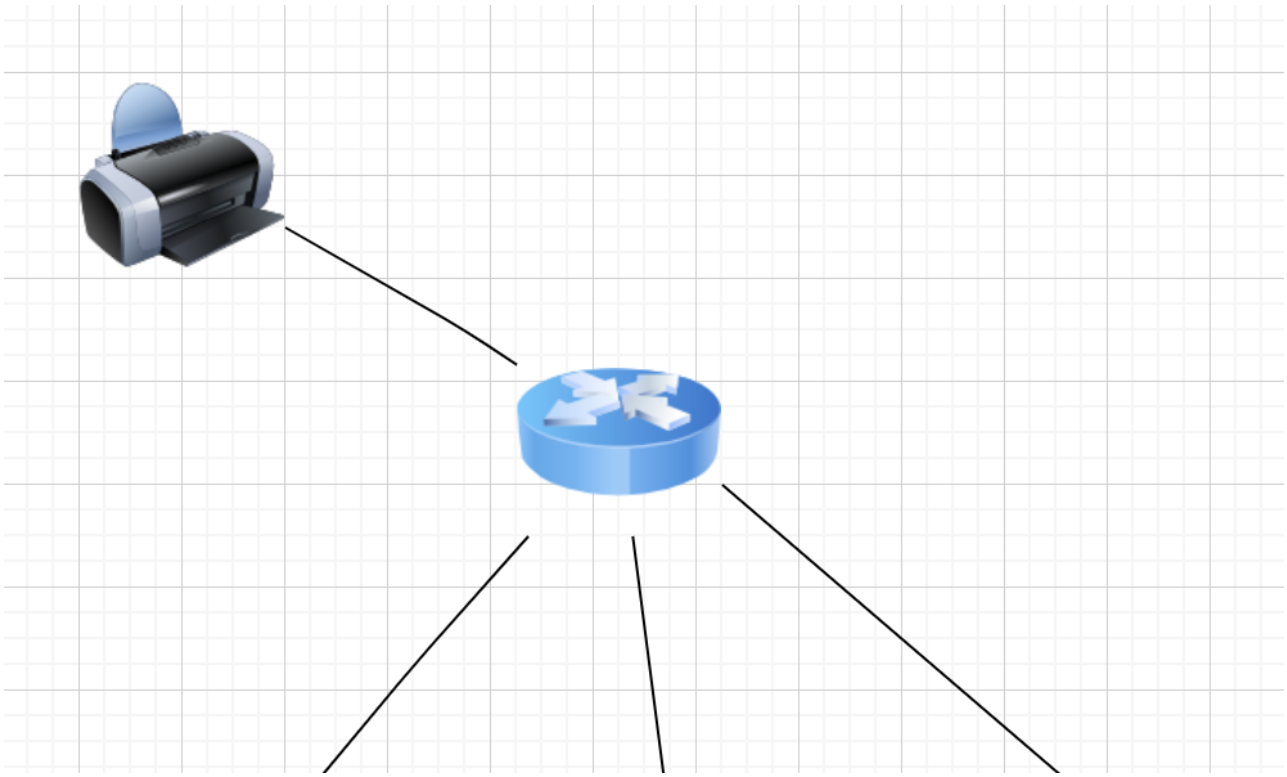
25 你就是看不见我 - VPN

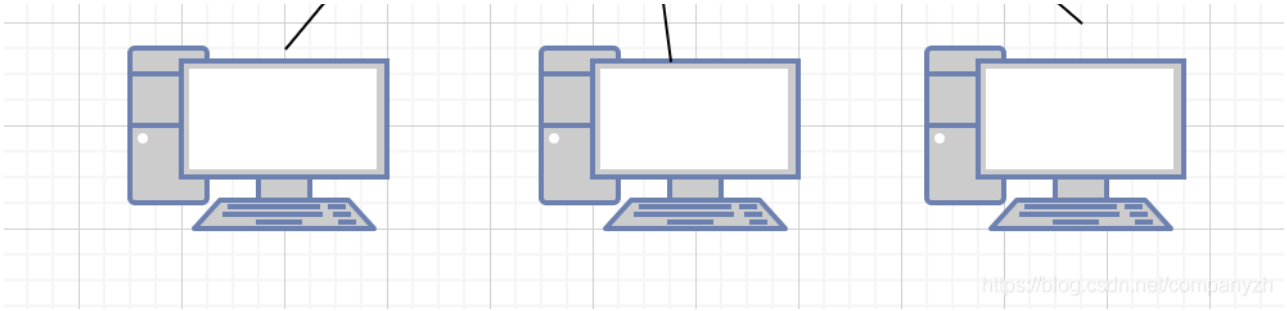
VPN也许对你很陌生，也可能你很熟悉，不知道你有没有翻过墙？不知道你有没有想要连接公司的网络？如果答案是Yes的话，那你已经对VPN有了第一印象了。

LAN 和 WAN

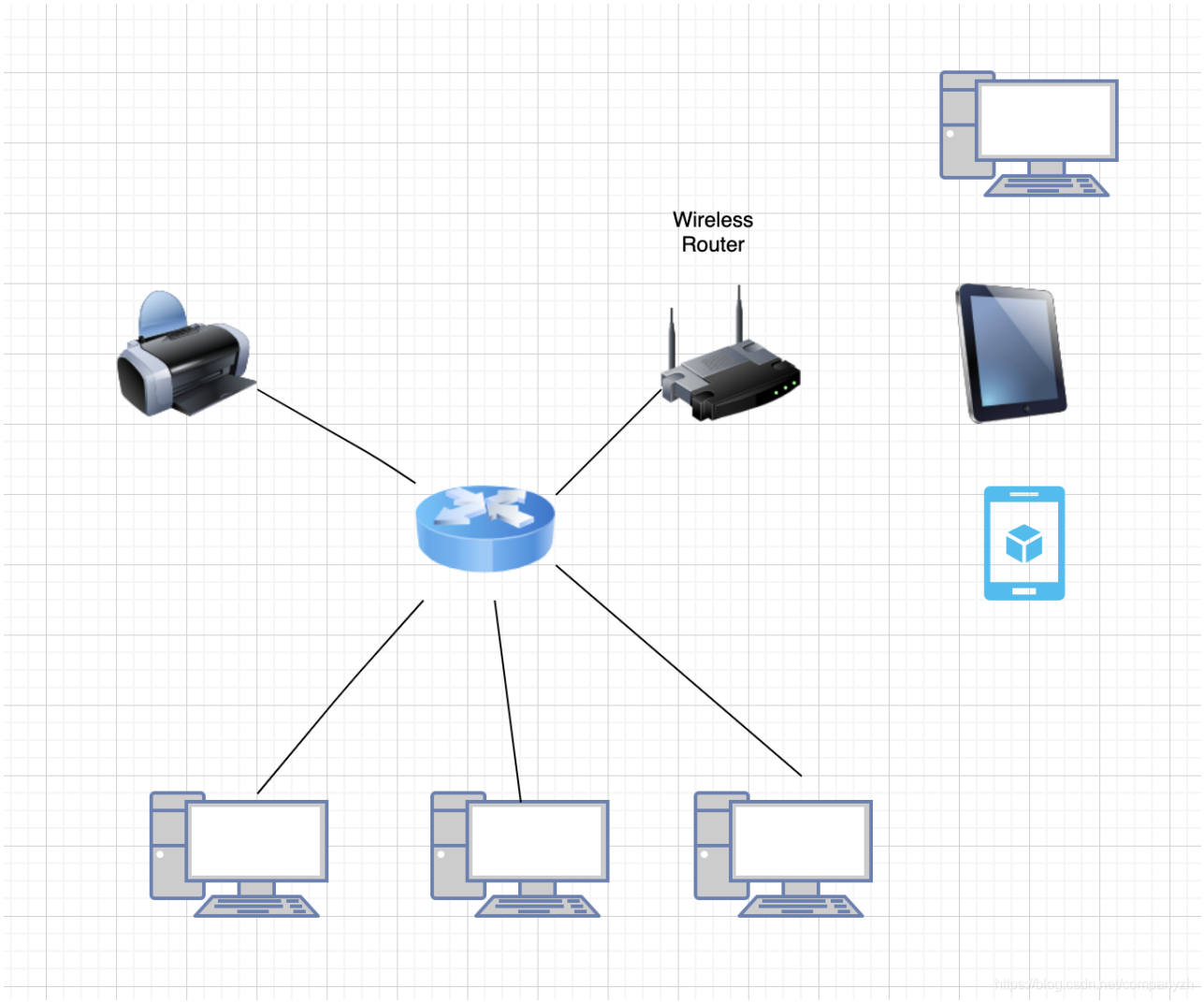
我如果和你说一个单词-网络，也许对于不同的人来说有不同的意义，就好像一百的人心中有一百个哈姆雷特。如果用户说网络故障了，通常意味着当前使用的应用程序无法正常工作，但是网络本身可能完全可以正常地工作。原因可能只是某些数据库或某些服务器处于脱机状态，导致用户现在无法使用其应用程序。

再举个例子，你也许会碰到过说这台打印机只能在本地网络上工作。这里的网络意义和上一个用户所说的上下文是不同。这里所说的网络其实是局域网也就是LAN。在这里的意思是如果你想使用这台打印机，那么你必须在此局域网上。局域网通常是指一组在Layer 2连接起来的设备。这意味着我们都已通过电线连接到交换机，因此任何通过电线连接到交换机的人都可以使用也在该层连接到网络的打印机。





我们还可以为此添加一个无线组件，以便无线网络或有线网络中的每个都位于同一层网络的设备，都可以使用局域网上的同一台打印机。



通常，大型公司由许多较小的局域网组成，并且它们全部包含在一个设施，或者都包含在多个设施中。当我们的公司进入某个设施时，很可能会使用某种第三层的设备（例如第三层交换机或路由器）将所有这些区域连接在一起，以便它们可以彼此通信。但是很有可能。如果你在一个足够大的公司，比如阿里巴巴。那么将有不只一个中心可供你连接和使用。也许在杭州有一个办公楼，上海有一个办公楼，数据中心可能在北京，但是不管在哪里，是不是都必须要让所有的员工仍然可以访问该设施。因此，我们要做的是必须在办公楼与数据中心之

间建立某种类型的连接，该连接称为我们的广域网也就是WAN。

通常，这些广域网是点对点连接，也就是说连接只有两个端点。一端是办公楼，另一端是数据中心。他们不一定总是要点对点，但通常是这样。在大多数情况下，广域网将成为仅使用两个设备（每个设施中一个设备）的点对点连接。我们的办公楼和我们的数据中心中都存在的路由器，因此我们可以使用三层连接和两台路由器将建筑物连接在一起，也可以使用第二层交换机将两座建筑物连接在一起并在我们两座建筑物之间建立一层连接，这有什么区别？一个是路由连接，一个通常是使用vlan的连接。

广域网允许使用这两种类型来进行连接，路由器或交换机都可以选择。我们可以使用光纤，也可以使用铜缆连接，当然使用Internet本身也可以。实际上我们可以使用Internet作为连接设施的机制，我们也可以使用无线。也许我们可以在每个设施上建立无线连接或两个无线接入点。如果这些建筑物足够近，并且没有障碍物，那么我们实际上可以使用无线方式进行连接。

VPN

我们现在来想一下现在的情况，当病毒横行的时候，可能你去不了办公室办公，就好像我从2020年3月就开始在家工作了。当然平时正常的时候，如果懒了，你也可以在家工作。相信现在基本上每家都有Internet连接。我们可以做的是利用互联网连接，建立从你家里的计算机到网络在到你公司网络的VPN隧道。但是这样隔着万水千山，数据来回传送，会安全吗？

Remote Access VPN （远程VPN）

想法是，我们对隧道中的数据进行加密，这样的话，Internet上的其他人都无法解密并理解和收听正在发送的数据是什么？这就是Remote Access VPN也就是为远程访问VPN。远程访问VPN真正的好处是，不管你连的是哪个网络都没有关系。通常来说的因为某些国家，政府和某些组织实际上会阻止你创建VPN隧道。例如，很可能如果你位于银行网络内部，那么他们很可能不会让你建立VPN隧道，因为他们不希望你窃取信息并通过加密的通道发送信息。但是他们会授权给为该组织工作的用户具有通过VPN发送流量的能力（比如银行自己的员工，所以出事第一调查的就是内部人员，内鬼往往作案的比例很大很大）。

所以，我们可以从外向内构建VPN，无法从内而外进行。不考虑特殊和复杂的环境，我们可以构建VPN隧道，这种远程VPN，可以让用户安全的发送数据，这一点是几乎可以在地球上的任何地方都工作的。也许当你去美国旅游的时候，你负责的项目发生问题了，这个时候只有你能解决，你就必须要远程工程，对不对。这个时候，你需要连接到你在中国公司的网络，你使用的肯定还是美国的Internet，然后在这个Internet之上建立了你的VPN隧道。远程访问VPN只是VPN的一种。

Site to Site VPN （站点对站点VPN）

现在你旅游回来了，回到了北京的当地网络，也许你的公司收购了另一家公司，比如csdn收购了Gitchat。GitChat和csdn在一个完全不同的服务区域中，我们并没有一个很好的机制来建立到从csdn到Gitchat的WAN。我们可以做的就是在该位置定一个高速Internet连接也许是光纤，就像为家庭用户所做的一样（也许你家里就是光纤了，我家就是）。现在csdn的办公室和GitChat的办公室都有光纤的网络了，我们可以做的是在两个位置使用路由器或防火墙建立两端的VPN，这被称为站点对站点VPN。站点到站点VPN的目的是将一个机构的整个局域网连接到另一机构的局域网。这个概念就和上面所讲的有点不同，对吧？因为这里我们不仅有像笔记本电脑之类的计算机来建立VPN连接，我们还建立了某种类型的网络设备来建立VPN连接，而VPN另一端的设备可能都不知道自己连接到了这个VPN。无需使用VPN连接Gitchat就可以像访问常规WAN一样来访问CSDN公司内部的网络了。因此，此处的站点到站点VPN旨在占用整个局域网或多个局域网，并提供回到公司主网络的广域网连接。

VPN加密

我们前面提到了VPN是加密的，所以选择加密和安全协议是规划和部署VPN不能缺失的一部分。这个当然会因为产品的厂家不同和有所差异。在某些情况下，还取决于你选择的是client-to-site还是site-to-site VPN. 这里会涉及一些加密的内容，感觉听不懂或者不感兴趣的同学可以跳过。

对称加密 Symmetric

我们对称密码学开始聊起，在对称密码学中，相同的密钥用于加密和解密，所以叫做对称密码。我们可以在两个不同的VPN端点上以相同的方式手动配置同一密钥，当然你也可以使用非对称的公钥和私钥。在手动配置中，密码短语（passphrase）是经常用于配置的密码（passphrase是满足了一定规则约束的password, 安全性要高一些），当然你必须在VPN的两端以相同的方式进行配置。

一般而言，对称密钥的安全性不如使用非对称密钥。通常将非对称和对称密钥同时使用以提供安全的解决方案。在非对称密码学中，你可以发现解密和加密使用的是不同的密钥（虽然在数学上相关，万事万物都有关联，只是你能不能发现和破解而已）。这是通过公钥基础结构PKI（即数字安全证书的层次结构）完成的，每个证书都包含该证书唯一的数学上相关的公钥和私钥对。这意味着使用公钥进行加密，用私钥进行解密。顾名思义，公钥可以与任何人自由共享，但是私钥必须保密，并且只能由颁发证书的一方使用。在VPN的配置中，需要在每个VPN设备上配置一个PKI证书，尤其是站点到站点VPN的配置。根据解决方案的不同，客户端到站点VPN，你很可能不需要在客户端安装PKI证书。当我们确实使用这些PKI证书时，所有设备都必须信任证书颁发者，这一点非常重要。

IPsec或IP安全不是保护VPN隧道的唯一方法，但它是最常用的，例如L2TP或VPN的第2层隧道协议类型。 IKE代表Internet Key Exchange。其目的是在两个通信方之间建立安全联盟或SA。因此，我们需要在连接的两端都生成相同的对称密钥，而无需通过网络发送，通常使用Diffie-Hellman协议（当然还有其他方法可以完成）。

象我前面提到的，密码学或者安全性是一个特别大和专业的领域，甚至是一个比网络协议要大的多的话题，如果这里你不能理解的话，不要纠结，明白公钥和私钥就可以了。

VPN安全

确保VPN安全适用于VPN的计划，实施，以及客户端如何使用VPN阶段。在VPN客户端，我们应该考虑的配置是禁止保存VPN的Credential（证书）。现在已经21世纪了，移动设备基本上是人手必备。当我们讨论丢失，被偷或损坏的移动设备时，如果这个设备记住了你的VPN证书，则可以从移动设备上获得访问权。如果由恶意用户获得设备，则可以进入VPN并接触许多其他隐秘的内容。

当然还有离线的密码破解工具可以用在保存了VPN证书的设备上。所以取决于VPN客户端以及否保存了密码讲确定潜在问题的严重程度（也就是通常所说的潜在安全问题）。我们还需要考虑公司VPN的使用政策，以及有关如何使用VPN的任何文档。这通常是新员工入职的第一课，用来确保你是否知道在什么地方以及什么时候可以使用VPN。我们还应该考虑VPN甚至是Web浏览器的指纹识别或其他识别方式。例如，可以通过检查传输的IP地址来间接检测是否正在使用VPN。所以，当我们通过VPN时，传输内容会通过VPN隧道进行加密或保护，但随后会在VPN隧道的另一端被解密，因此这个内容或者流量可能来自该VPN设备。

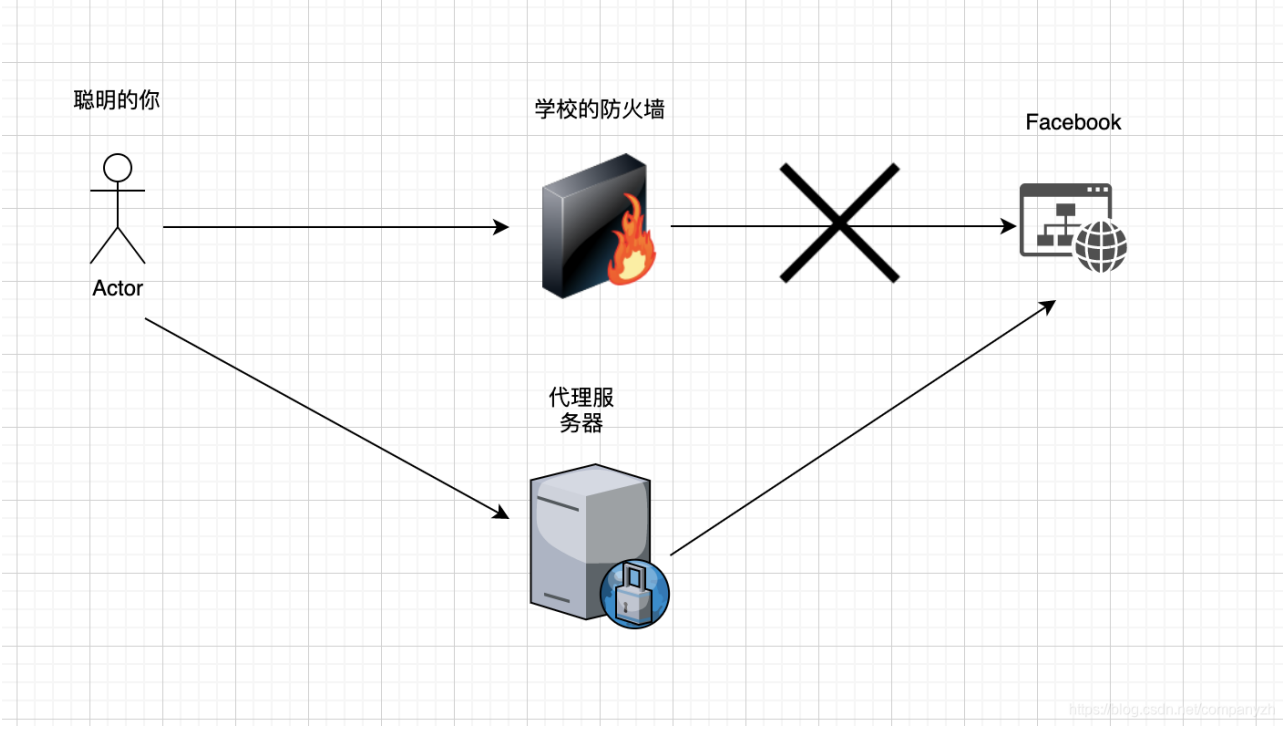
另一个注意事项是登录VPN服务器或VPN设备。在企业中，我们通常会保留日志用来日后的审核。还有VPN的一些最佳配置做法包括修改VPN身份验证超时。我不是建议你去增加或减少超时时间，你应该根据特定的解决方案和平均网络速度来配置，因此你要确保身份验证超时不会太长，以便用户知道如果他们是不是要尝试从设备（例如密钥卡）中重新输入密码。

理想情况下，应在每一个IT解决方案中使用Multifactor（多身份验证），而不仅仅是VPN（比如AWS，就会因为没有Multifactor的设置，是有安全隐患的，还有Github等等，我相信阿里云，腾讯云等会有相应的设置）。Multifactor之所以在VPN中尤其重要，是因为VPN可能允许外部设备访问内部受保护的网络和信息，所以我们要最大程度地去保护它，使用多因素身份验证需要使用多个安全类别来识别你就是你。

除了用户名和密码这种传统的单因素身份验证，我们的VPN还要求使用密钥卡，该密钥卡具有与VPN同步的数字更改代码设备（比如有一个App叫做Authenticator）。下一个需要配置的应该是启用帐户锁定，以便在多次错误登录尝试之后，将该帐户锁定，并且这些特定值

需要根据环境来确定，因为它需要与你公司的安全策略保持一致。对于任何类型的配置，无论是Windows，Linux主机，移动设备，网站，还是我们现在讨论的VPN，理论上都不应该使用默认设置。我们应该始终更改默认设置，以使其更难以受到侵害，减少潜在的危险。

互联网上的许多人都使用个人VPN匿名服务器App。比如，学校的孩子可能会在智能手机上使用VPN应用程序，这样即使学校的防火墙可能阻止了某类网站的连接，他们仍然可以连接到Facebook（美国孩子不好管呀）。通过使用个人VPN匿名服务器App，真正发生的是流量被隧道传输到其他地方的服务器，并且从那个位置开始在连接到其他地方。



上一页 下一页