VPN Gate 综述

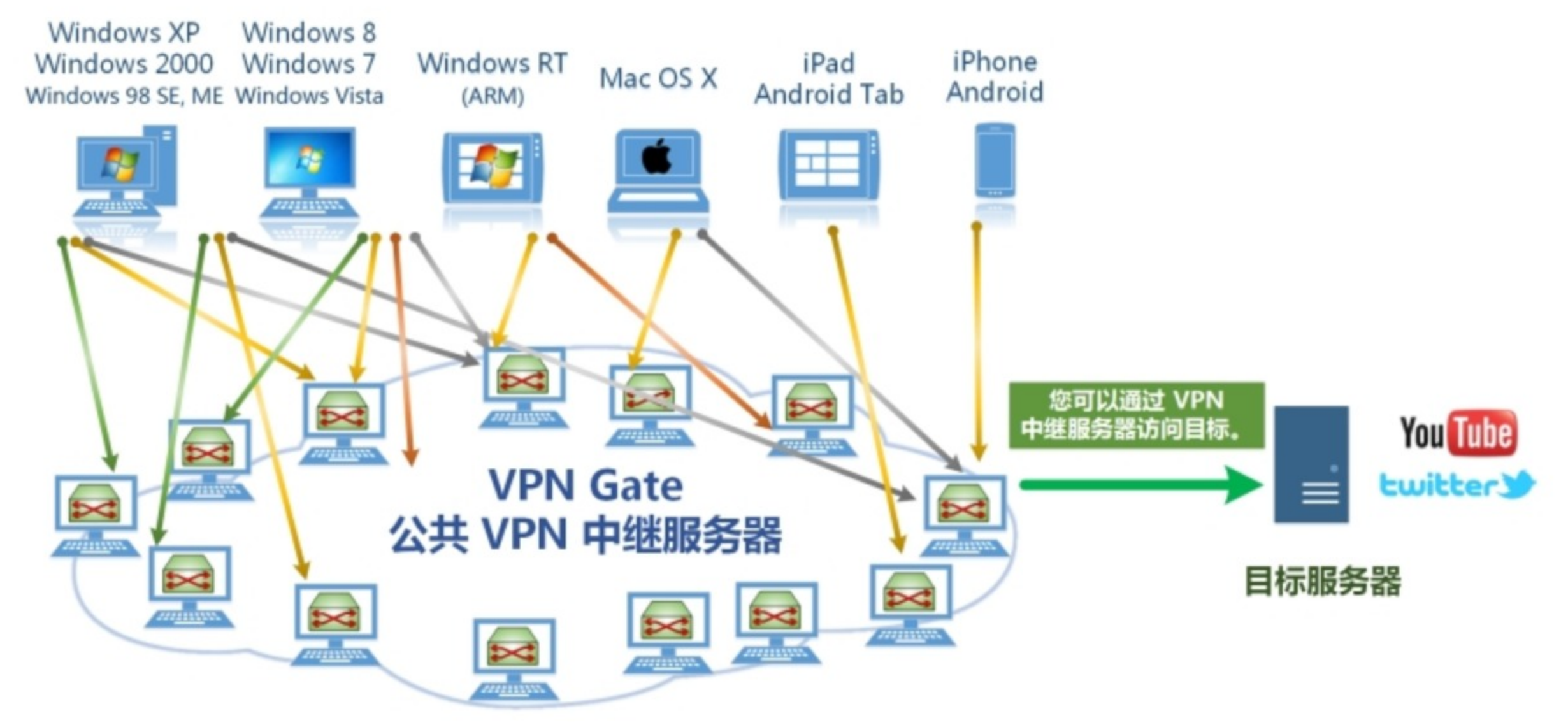
VPN Gate 学术实验项目是一个在线服务，由日本国立筑波大学研究生院为学术研究目的运营。本研究的目的是推广 "全球分布式公共 VPN 中继服务器" 的知识。

VPN Gate 公共 VPN 中继服务器

在 VPN Gate 学术项目网站上有一个公共 VPN 中继服务器列表。互联网上的任何人都可以建立 VPN 连接至任一列表上的 VPN 服务器。无需用户注册。

VPN Gate 公共 VPN 中继服务器的特点

- VPN Gate 包括许多由世界各地的志愿者所提供的 VPN 服务器。
  您可以提供自己的电脑作为一个 VPN 服务器加入到这个实验中。
- Windows, Mac, iPhone, iPad 和安卓都可以连接到 VPN Gate 服务器。
- 支持 SSL-VPN (SoftEther VPN) 协议， L2TP/IPsec 协议， OpenVPN 协议和 Microsoft SSTP 协议。
- 接受匿名连接。无需用户注册。
- 每个 VPN 服务器的 IP 地址是不固定的。 IP 地址可能会不定期改变。
- 每天 VPN 服务器会有增加和减少。因此，所有 VPN 服务器不处于特定 IP 地址范围。
- 当一个 VPN 客户端连接到 VPN 服务器时， VPN 客户端可以通过那台 VPN 服务器访问互联网。您可以隐藏你的客户端的 IP 地址。
- 当您使用一个在物理上位于海外国家的 VPN 服务器，您的任何通信都被认为，好像是从该国发起的。然后你就可以通过使用 VPN Gate 访问网站了，这通常是无法从您所在的国家访问的。

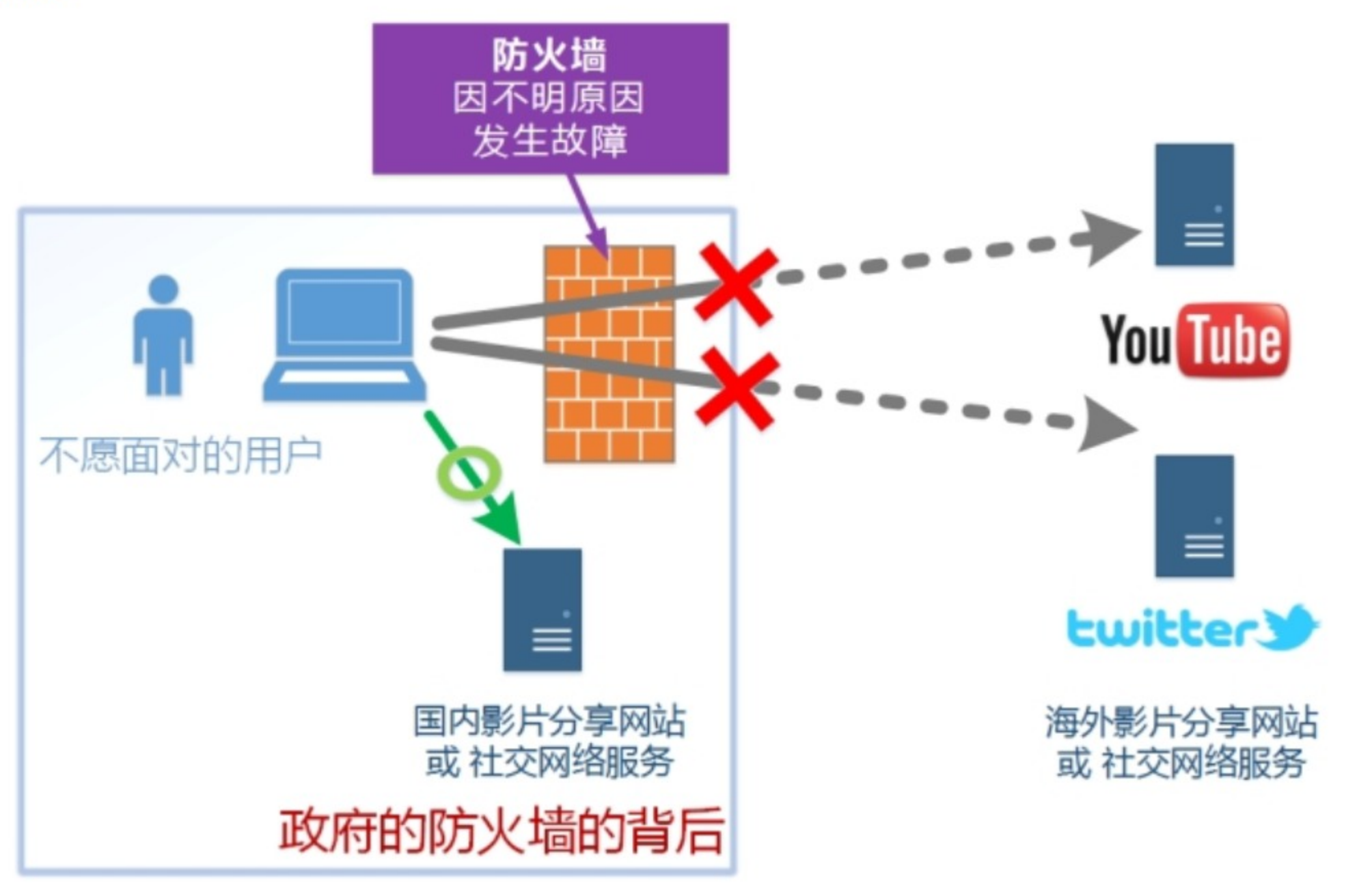


本研究想要解决的问题

开始 VPN Gate 实验的动力是解决以下现存问题。

存在的问题 1: 政府的防火墙有时未通过，一些海外网站变得遥不可及。

某些国家的防火墙由于 "未知故障" 导致通信失败。例如，你在某一国家旅行，并尝试访问 YouTube， Twitter， Facebook 等网站，但却失败了。然而，你却可以访问到其他的海外网站，如雅虎等。



存在的问题 2: 通过跟踪一个服务器访问日志的 IP 地址，可以确定一个人的隐私信息。

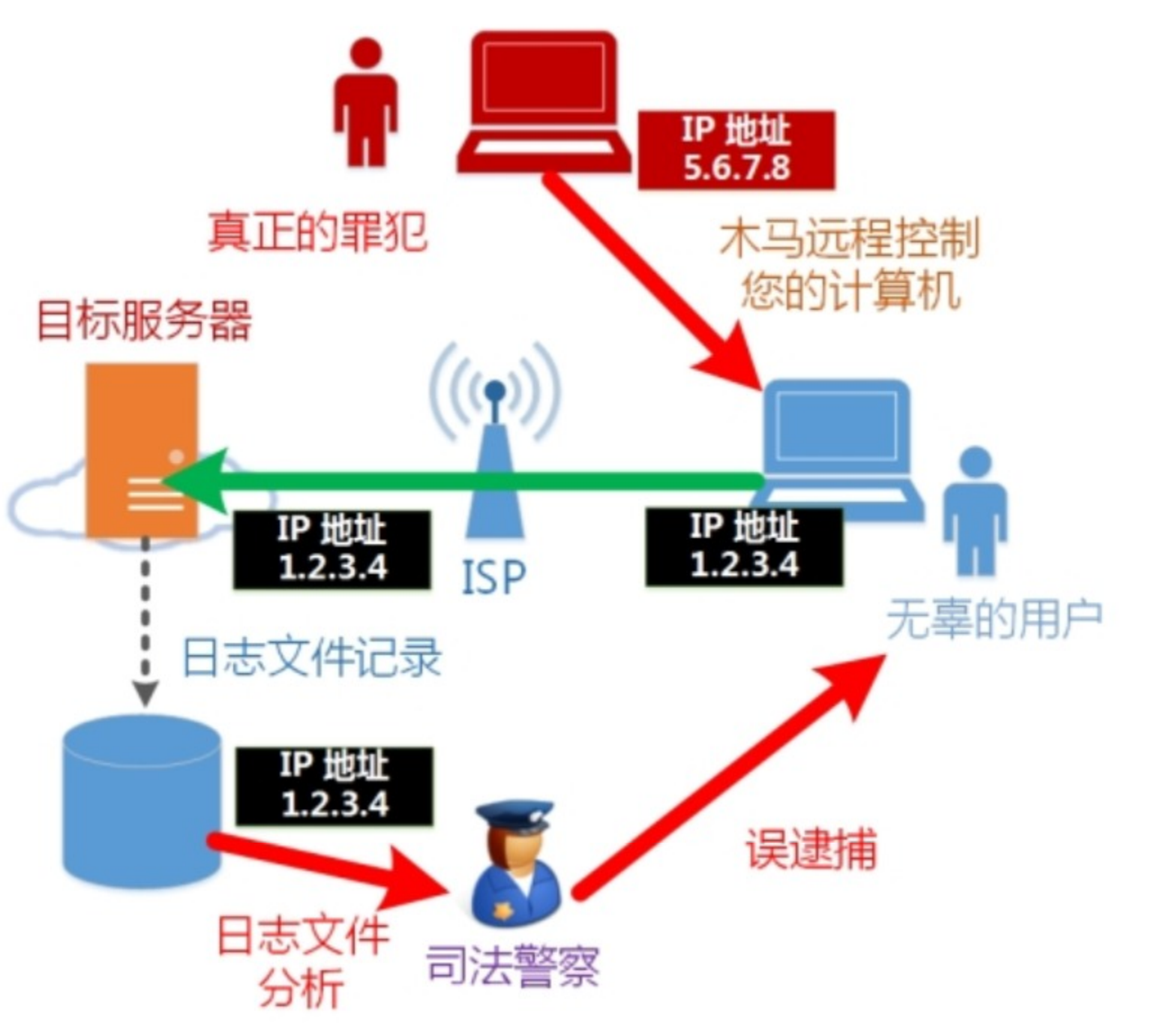
如果您访问网站或发送电子邮件，你的源 IP 地址将被记录在目标 Web 服务器上，或在包含有电子邮件内容的包头里。

一个 IP 地址不仅仅是个人信息。然而， IP 地址可以被用来跟踪在各个网站产生活动的个人。这种跟踪技术常被用于垃圾邮件或强制广告中。

此外，通过法律的强制执行程序，一个 IP 地址可以被用来确定谁是发起相关通信的人。警察、检察官或律师可以使用其特权要求互联网服务供应商主持的 IP 地址分配的日志文件。在平常的时候，这样的 IP 地址分配日志通常由互联网服务供应商附上。然而，一旦有人获得日志，他可以调查谁发送了电子邮件、或谁发布到网站上一条消息。

此外，在互联网上，一个人在特定时间被分配了一个特定 IP 地址的人将被视为与在同一时间从此 IP 地址发起的任何非法通信有责任。最近在日本，执法者的可耻事件做为严重的问题被批评，执法人员错误地逮捕了从来没有在他的电脑上进行非法事情的无辜互联网用户，而是电脑感染了木马，被真正的犯人远程控制。真正的犯人让无辜的互联网用户的计算机发送敲诈邮件给一些公司，无辜的人被执法人员不公正地逮捕。无辜的人最终被释放，但这是在日本近代历史上最糟糕的诬告事件之一。

因此，当你访问互联网时，最好有一个方法来暂时隐藏你的真实 IP 地址。如果你的真实 IP 地址被隐藏，没有广告目的的 IP 地址的追踪将是不成功的。IP 地址可追溯性的风险将会降低。如果隐藏你的真实 IP 地址连接到互联网时，即使你的电脑感染了木马或恶意软件，错误逮捕的风险将永远不会给你。



存在的问题 3: 公共 Wi-Fi 存在数据包被窃听的风险

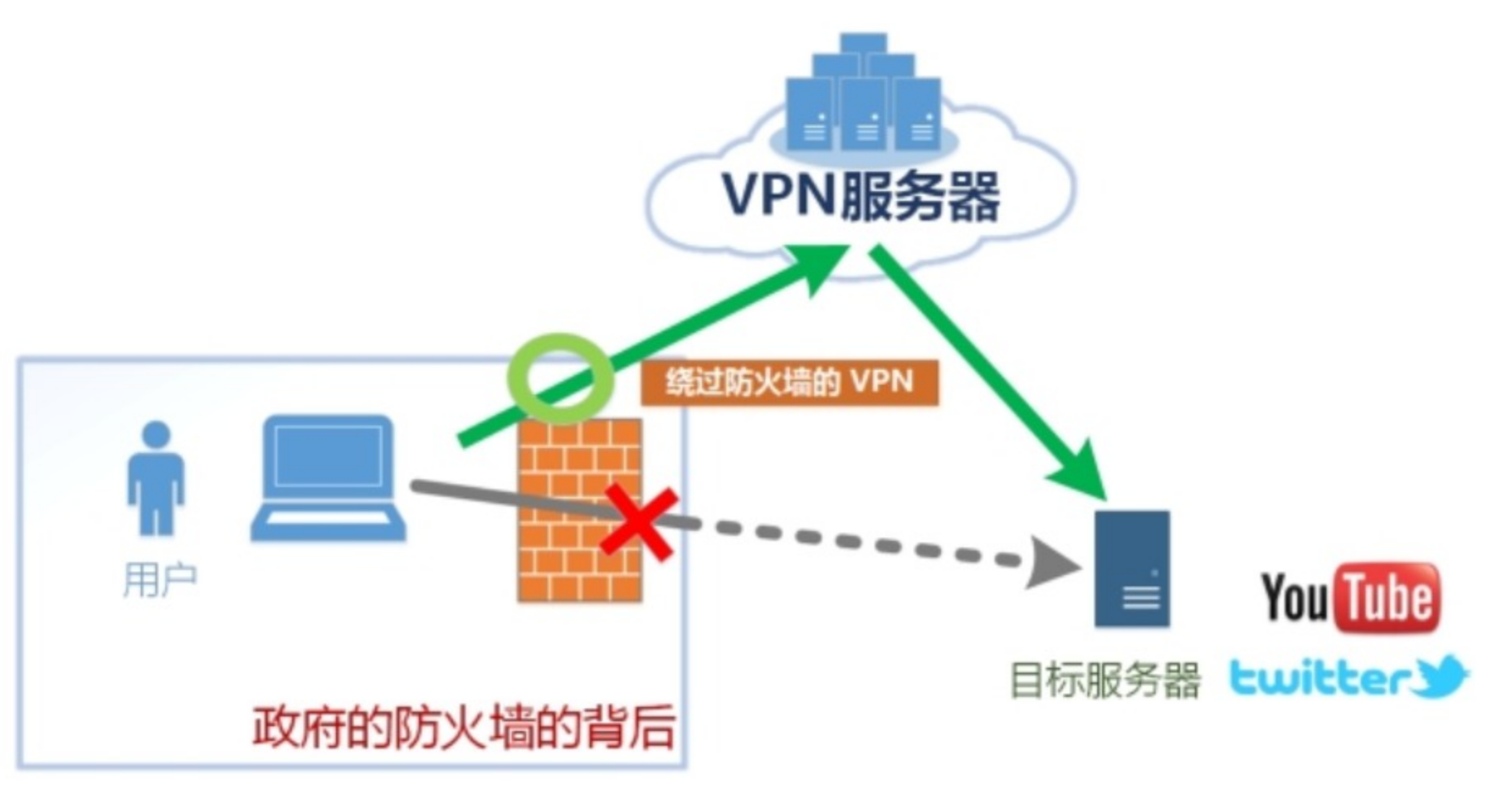
大多数公共 Wi-Fi 可以被人窃听。您的明文通信是不安全的。有线网络也有被窃听的风险。ARP 电子欺骗攻击者可以获取你的数据包。此外，网络管理员或提供公共 Wi-Fi 的咖啡馆或机场的设施业主可以随时窃听您的通信。即使你在家使用互联网，也有风险，您的 ISP 或电信公司的雇员可能窃听，在线路上偷看您的明文数据包。(事实上，有一个犯罪事件，日本电报电话公司的雇员，在电信大楼进行了窃听。所以，我们永远不能信任 ISP 或电信公司的员工)。

当在互联网上使用 HTTP、POP3 或 IMAP 纯文本通信时，你无法避免窃听。SSL (HTTPS) 对窃听是安全的，但是大多数网站使用的是 HTTP。HTTP 数据包传输的是纯文本格式。

最好的是存在这样的方法，对所有到互联网服务器的通信进行自动加密。在这种情况下，没有人可以在本地网络或本地电信大楼偷看你的数据包的内容。

VPN 可以加密和转播你的通信

如果你在使用互联网时使用 VPN ， 可以解决上述这三个问题。



解决方案 1: VPN 可以绕过防火墙。

由于某些政府防火墙发生的 "未知故障" ， 一些海外网站从防火墙后面无法访问，你可以通过海外的 VPN 服务器访问这些网站。海外 VPN 服务器将会把你的通信转到目标 Web 服务器。

解决方案 2: VPN 可以隐藏你的真实 IP 地址。

当 VPN 连接建立时，所有的通信的源 IP 地址将被替换为中继 VPN 服务器的 IP 地址。这将对你非常有帮助，因为在那一刻没有人再可以轻松地分析和跟踪你的真实 IP 地址了。目标 Web 服务器或 E-mail 的邮件头列表上的 IP 地址日志将被记录，好像通信是通过中继 VPN 服务器发起的。您可以安全地隐藏你的 IP 地址，并且可以发送匿名帖子或电子邮件到网站或邮件服务器。此外，如果您的计算机感染了由 "真正的罪犯" 发送的木马，真正的罪犯发送一个远程操作，让您的电脑发送非法敲诈邮件给某人，你不再处于被执法者错误逮捕的风险中。

解决方案 3: VPN 可以防止在本地网络上的窃听

如果你总是使用 VPN ， 所有通信都将被自动加密。即使你的邻居在本地网络上是个搭线窃听者，你的数据包也不能被他偷看到。

VPN Gate 和现有 VPN 服务之间有什么不同 ?

如上所述， VPN 可以解决使用互联网中的几个问题。但是，通常你在远程地点 (海外) 至少需要一台物理的 VPN 服务器，实际利用上述 VPN 的功能。

大多数互联网用户都无法在海外拥有自己的 VPN 服务器。对于这样的用户，一些互联网公司提供了现有的、付费的、共享的 VPN 服务。这样的服务需要用户注册，用信用卡付款，将可以为用户创建一个帐户。用户将获得根据合同的具体条款使用共享 VPN 服务器的权利。

所以，什么是 VPN Gate 和现有的支付 VPN 服务之间的不同呢 ? 以用户的观点出发，两个似乎是相似的。但是， VPN Gate 与现有的 VPN 服务的差异描述如下。

现有共享 VPN 服务的问题

现有的 VPN 服务的实施，是供应商公司在数据中心托管的一些 VPN 服务器。在数据中心提供一些共享的 VPN 服务器的这种传统方法有一个问题，即每个 VPN 服务器的 IP 地址都在相同或相似的 IP 地址分配块。因为 IP 地址通常由相同的 ISP 分配。每个 VPN 服务器的 IP 地址是固定的，所以他们很少改变。

这种共享的 VPN 服务不容忍对 "政府防火墙的未知故障" 。 "政府防火墙的未知故障" ， 通常会出现一系列 IP 地址块变成完全无法从该国境内访问的情况。如果 "未知故障" 发生在包含共享的 VPN 服务器群集的 IP 地址块分配的 IP 地址范围，没有群集的 VPN 服务器将无法从该国访问。事实上，最近有报道说，某天一个现有的共享 VPN 服务器的、特定的群集，从一个特定国家的政府防火墙突然无法访问。

现有共享 VPN 服务的另一个问题是: 带宽占用。现有的共享 VPN 服务器物理放置在特定的数据中心。每个用户的所有通信将集中在数据中心的上行线路的互联网传输线上。所有处理的工作量将集中在数据中心托管的一些共享 VPN 物理服务器上。服务提供商认为在集群中增加 VPN 服务器的数量，或增加互联网传输线路的带宽，但这种扩张需要成本。如果成本增加，这种共享的 VPN 服务的费用将会增加。如果节省成本，这种共享的 VPN 服务的速度将下降。大多数共享的 VPN 服务不能向用户提供优等质量。

VPN Gate 学术实验的优点

正如你可以看到 VPN Gate 公共 VPN 中继服务器的列表，有很多运行在 VPN Gate 公共 VPN 中继服务器。这些 VPN 服务器没有物理地放置在一个特定的数据中心，也没有一个特定的 IP 地址分配块，他们都是由不同 ISP、在物理地点托管的。

每个 VPN Gate 公共 VPN 中继服务器是分布式的，并由许多志愿者托管。一名志愿者是拥有一台计算机、保持带宽连接到互联网的人。他是一个同意提供 CPU 时间和带宽、支持 VPN Gate 学术实验的人。你可以成为一名志愿者。

志愿者在地理上是分布式的。志愿者的 ISP 也是分布式的。所以每一个 VPN 服务器的 IP 地址是分布式的。分配的 IP 地址没有特点。每天志愿者的数量增加或减少，每个 IP 地址每次都改变。如果政府的防火墙出现 "故障" ， 整个 VPN Gate 中继服务器不受影响。如果一些 VPN 服务器无法从你的国家访问，你仍然可以访问其他 VPN 服务器。

因为 VPN Gate 服务器由志愿者托管，每个志愿者花费极少量的带宽成本和 CPU 时间在他的 VPN 服务器上， VPN Gate 服务可以被大家免费使用。免费的意思为任何想要使用 VPN Gate 服务的用户无需注册。

因此，不同于现有的共享 VPN 服务， VPN Gate 学术实验服务可以无需付费地使用。

VPN Gate 网站的镜像服务器

一旦一个用户连接 VPN 会话到 VPN Gate 公共 VPN 中继服务器之一，他可以从任何国家获得自由访问互联网。

然而，如果 www.vpngate.net 网站 (本网站) 无法从他的国家访问，他不能首先获得 VPN Gate 公共 VPN 中继服务器列表。

所以，我们提供了许多镜像站点的 URL ， 以帮助在这些国家的用户。如果一个用户能获得访问至少一个镜像网站，他可以浏览 VPN Gate 公共 VPN 中继服务器列表页。

如果你是一个国家的公民由于政府防火墙的未知错误，防止从国内互联网访问 www.vpngate.net ， 请访问镜像站点列表页面，复制 URL 列表，并将其粘贴到你们国家的 SNS、博客或社区论坛，以帮助你们国家的 VPN 用户。