道高一尺，牆高一丈：互聯網封鎖是如何升級的

新時代的防火牆像手術刀，精準迅速，直擊命門。而「翻牆」未來可能變成一門手藝，如何傳承，任重道遠。

特約撰稿人 VV　2015-09-04

1987年，中國第一封電子郵件由中國兵器工業計算機應用研究所發往德國，標誌中國成功接入互聯網。郵件內容是：“Across the Great Wall we can reach every corner in the world”——穿越「巨牆」（長城），我們無處不及。與這封郵件幾乎同齡的我，沒想到生活中竟總離不開「牆」。在物理世界和虛擬世界中多次穿牆，也去過世界各處，看「牆」越築越高，有時義憤填膺，有時啼笑皆非。僅以此文，記錄「牆」邊的一些見聞。

國家公共網絡監控系統

俗稱中國網絡防火牆（The Great Fire Wall of China，常用簡稱「GFW」或「牆」）。一般意義所說的GFW，主要指中國官方對境外涉及敏感內容的網站、IP地址、關鍵詞 、網址等的過濾。隨着使用的拓廣，中文「牆」和英文「GFW」有時也被用作動詞，網友所說的「被牆」即指被防火長城所屏蔽。

2008年校園網：「連坐」懲罰

2007年，我進入這所XX理工大學。它特別弔詭的設定是，大一不能帶電腦，大二考過國家英語四級的人才可以帶電腦。就這樣，2008年秋天，我終於正大光明地連上校園網。千兆比特級別以太網直入國家主幹網，中國電信、中國教育網雙通道。這個規格，算是極高的。網速之快，前所未見；可是，總有一些網站訪問不了。但這些小細節，終究不影響同學們DotA（一款基於Warcraft的對戰地圖）的熱情。

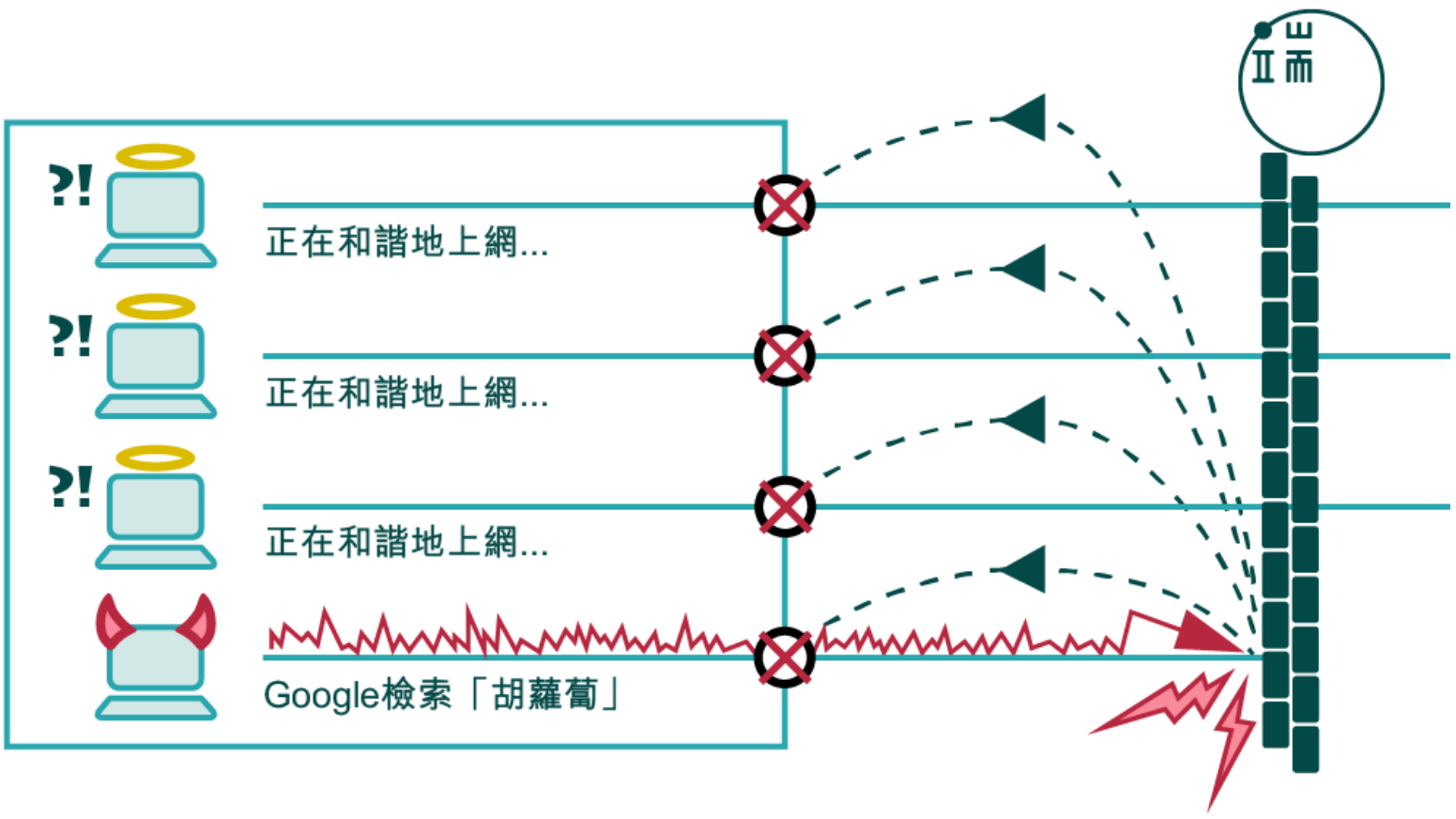
那個時候，我們愉快地上Google，查Wikipedia，學習西方先進科技。不時有好事者，會鍵入諸如「六四」、「胡蘿蔔」、「溫度計」（網民用來形容胡錦濤與溫家寶的指代用詞）這樣的神奇詞彙，於是全校與Google失聯十數分鐘。每當到這個時候，室友們相視一笑，「哦，誰又撞牆了！」但打壺開

水，泡一杯麵，還不等吃完，就又可以Google了。

那個時候的「牆」就好像霰彈槍，火力充足，但瞄不太準。一槍下去，打一大片，總是搞得「城門失火，殃及池魚」。

牆如何運作？

一台機器要與互聯網上的其他機器對話，需要一個IP地址，好比一個人需要身份證（ID），才能唯一標識一樣。否則，你喊一句話，對方不知應該回話給誰。而IP地址的總量是有限的，就好比一個大小固定的蛋糕。美國入場早，切走一大塊。接着列強瓜分。等到中國的時候，還剩下點面皮。而該理工大學在這輪「圈地運動」中，只得到2個IP地址，給全校數萬師生共用。這下好了，一個IP後面幾萬人，究竟誰在幹什麼，從校外是看不清的了。早期的防火牆，只能粗糙地在IP級別上執行封鎖，要管束，只能全盤封了整個學校的網絡。但畢竟一所國家重點高校，不可能用這種方式來管理，但不封鎖，又無法向監管部門交代。



內網某個用戶登陸Google檢索「敏感信息」，這意味著一個端口「撞牆」，「牆」把接連着的四千多個端口都封掉，令無辜群眾也無法使用Google。

牆早期對用戶的「連坐」懲罰策略。圖：端傳媒設計部

說到底，監管當局不乏能工巧匠，他們很快想出一個辦法：封殺大約4千個連續的端口（Port）。如果我們把IP地址比作一棟房子，那麼端口就是出入這間房子的門。不同於真正的房子只有幾個門，一個IP地址的端口可以有65536（即2的16次方）個之多。端口在一

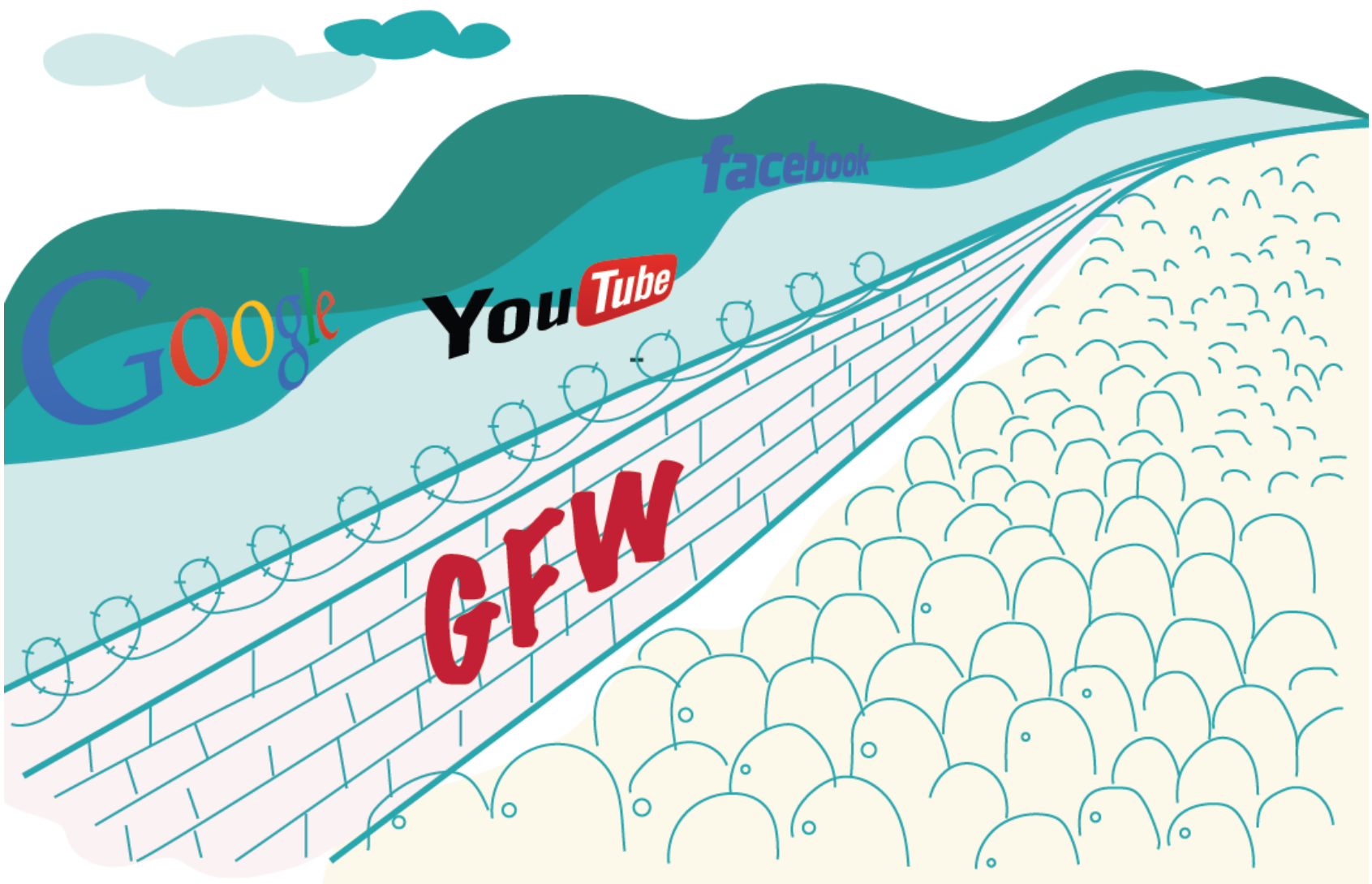
定時期內是被內網的一個用戶獨佔，於是數據包可以準確地回到始發地。不過，封一個端口不過癮，只是撞牆者自己倒霉而已。試想，你好不容易把野馬制服了，又會有一些原本安順的良馬變野，效果不佳。最好的辦法就是讓它成爲害群之馬，以做警示。所以，一旦內網某個用戶登陸Google檢索「敏感信息」，這意味着一個端口「撞牆」，「牆」就把接連着的約四千多個端口都封掉，令無辜群眾也無法上網。這種斷網的「連坐懲罰」短則幾分鐘，長則十幾分鐘，才能恢復服務。

2010年北京：合租服務器翻牆

3月，Google位於北京中關村的辦公室樓下堆滿了鮮花，網友以這種方式紀念因「遭受中國駭客攻擊」和「網絡審查」而決定退出中國市場的Google。

「牆」這個概念越來越清晰，也進入了更多人的視野。2009年，Facebook和Twitter相繼被封，昭示着中國政府通過防火牆阻隔國際互聯網，建立「局域網」的決心——「局域網」是中國網民對牆內狀況的戲稱。

「咱們合租一個VPS（Virtual Private Server）吧」，這是技術青年們見面經常談到的話題，僅次於買房和買車。VPS即虛擬主機，向服務商租取一段時間使用權即可。以前，大家合租VPS，多是爲了搭個博客，趕趕時髦。而現在，合租VPS，多是爲了翻牆。

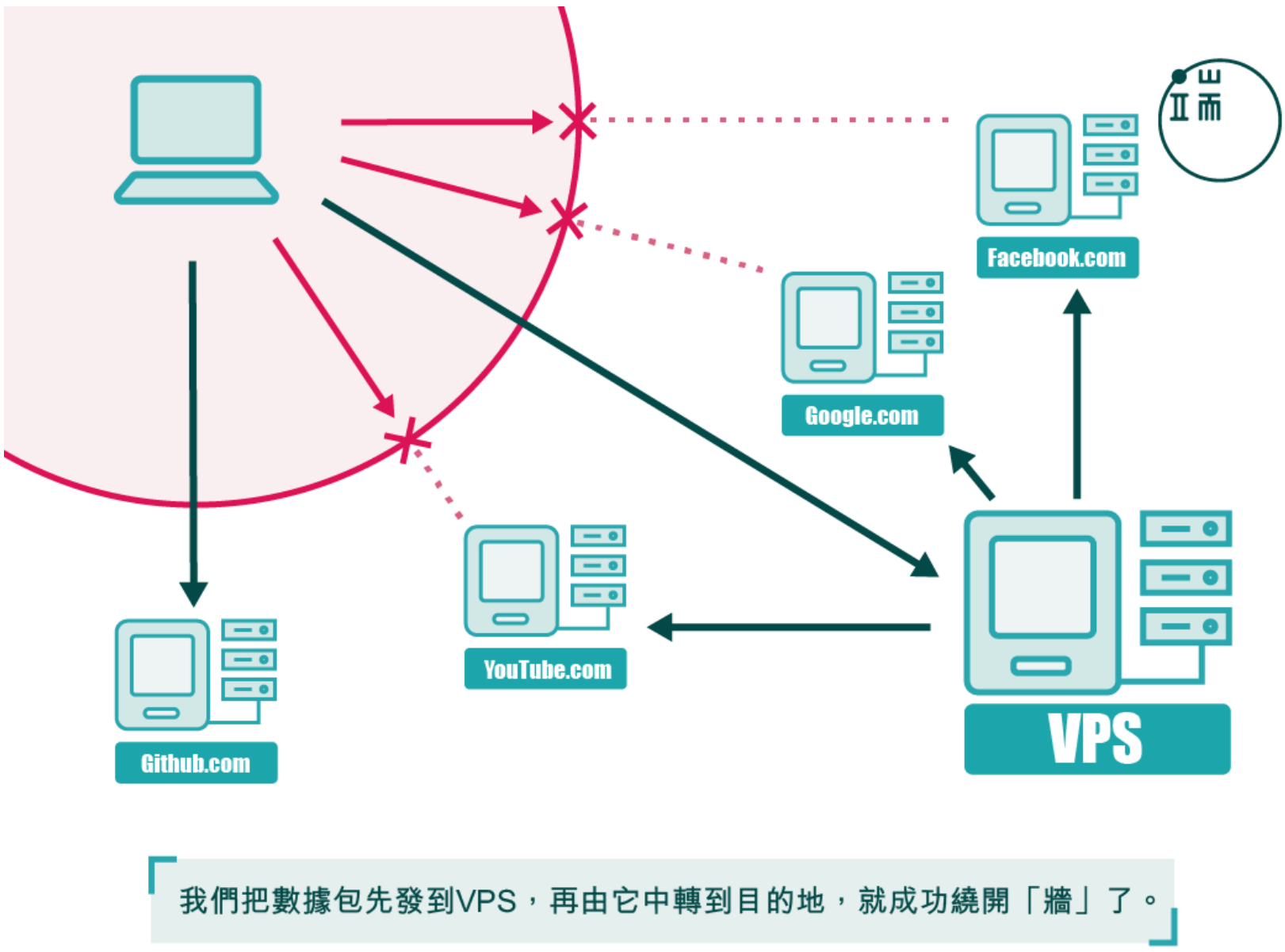


牆外豐富多彩的世界吸引着年輕人。圖：端傳媒設計部

對這些年輕人來說，「翻牆」用Google檢索最新資訊，使用垃圾郵件最少的Gmail，隨時查詢在線百科全書Wikipedia，通過Facebook、Twitter與同行保持密切的技術資訊溝通，就像呼吸一樣自然。也有更多人翻牆是要選擇不同服務器進行聯網遊戲，或下載最新的影視內容，「翻牆」就像玩貓和老鼠的遊戲。

VPS如何幫你翻牆？

當你發一個數據包到Google或者Facebook時，防火牆可以直接識別目的IP地址而自動攔截。而前面提到的VPS，是虛擬主機，自己也有IP地址，但無公開記錄其歸屬，難以確認是否是敵軍。既然如此，我們把數據包先發到VPS，再由它中轉到目的地，就成功繞開「牆」了。由於VPS的這種特性，它也被稱作「跳板」。

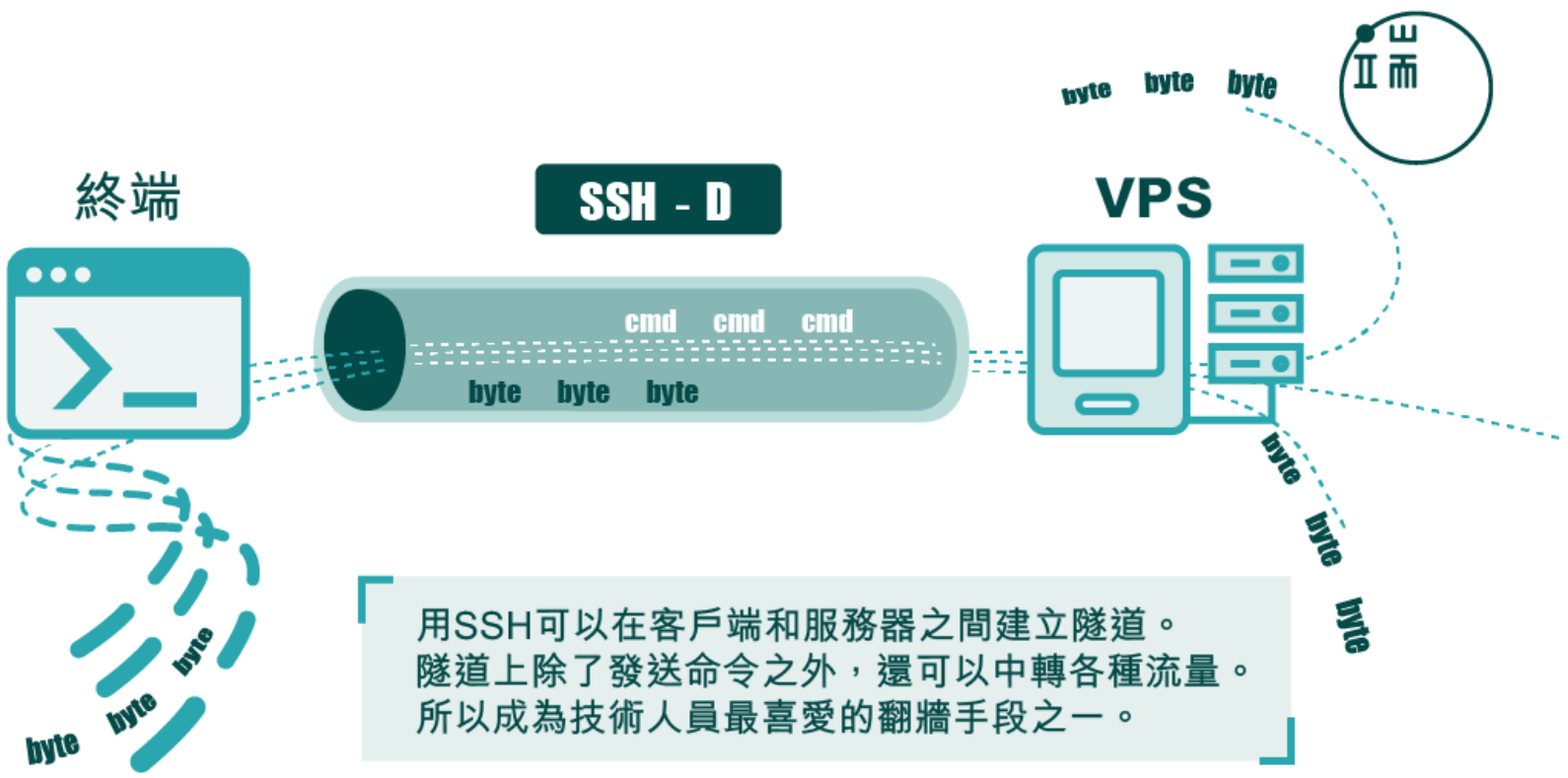


「跳板」是所有「翻牆」技術的共通原理。圖：端傳媒設計部

利用一個「跳板」繞過「牆」，正是許多翻牆軟件的基本原理。曾經繁榮的翻牆軟件「無界」、「自由門」，還有眾多的「代理服務器」，包括後來更廣泛應用的VPN（Virtual

Private Network），都是借用跳板原理。VPN最早是用來幫助一個企業多地的辦公室間互聯，也可以讓員工在異地進入公司內網，方便執行一些高權限的作業。這樣一來，跨國公司天然就擁有了穿牆的隧道：數據包先發到海外辦公室，再去向世界各地。所以，VPN也成了跨國公司員工翻牆的主流手段。

這年，我第一次用“ssh -D”（一行命令）翻牆。SSH可以讓系統管理員連接上主機，進行遠程操作。同時它相當於在客戶端與服務器之間建立了一個隧道，所以也能傳輸其他的數據，包括「翻牆」流量。只要這台機器的IP不在牆的「黑名單」中，也就可以成功繞過牆的封鎖了。對技術人員來說，買VPS是最簡單且低成本的翻牆方法。即便一台VPS被牆，再買一台即可。一年幾十美元的價格，合租下來非常便宜。



SSH協議可以建立「隧道」，成爲技術人員「翻牆」的最愛。圖：端傳媒設計部

2011-14年香港：「牆」成為一門顯學

在Google、Wikipedia中文、Facebook、Twitter等全球流行網絡應用被阻隔在防火牆之外後，中國大興土木建設的「局域網」，這幾年也初現雛形。

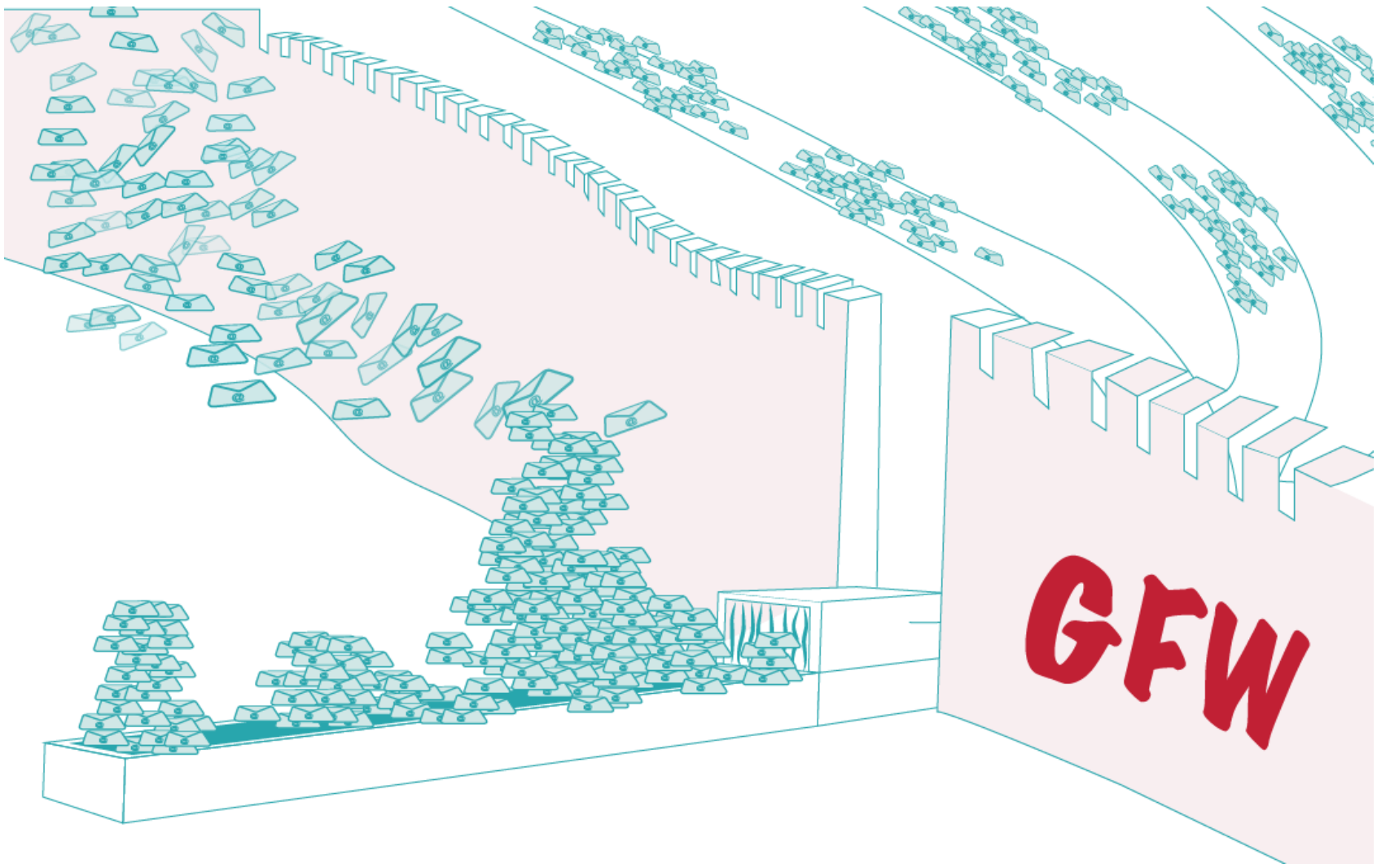
搜索用百度，郵箱有163/QQ，社交有微博/人人，購物用淘寶/京東，即時聊天用微信——各種互聯網服務，牆內應有盡有。對大部分網民來說，翻牆成了越來越不必要的需求。而剩下的一小撥執着於翻牆的用戶，以及全世界

致力於研究「牆」的學者，他們見證了「牆」的升級，與之鬥智鬥勇，也從一些滑稽的表象，捕捉到「牆」發展的各種蛛絲馬跡。

因「牆」不同的工作原理，越來越多的翻牆工具被開發出來。對「翻牆」這個行當來說，這是個百花齊放的時代。

解析郵件

2011年初，Gmail大規模延遲，這可能是生活在中國的很多「良民」第一次看到牆的影子。他們並不是Twitter、Facebook的忠實用戶，對自由世界的「危險信息」也並不感興趣，只是日常收發郵件，竟也撞牆。實測顯示，Gmail與大陸服務商之間的郵件有不同程度的延遲，少則幾個小時，多則幾個星期。人們紛紛猜測，「牆」已經進化到開始解析郵件。

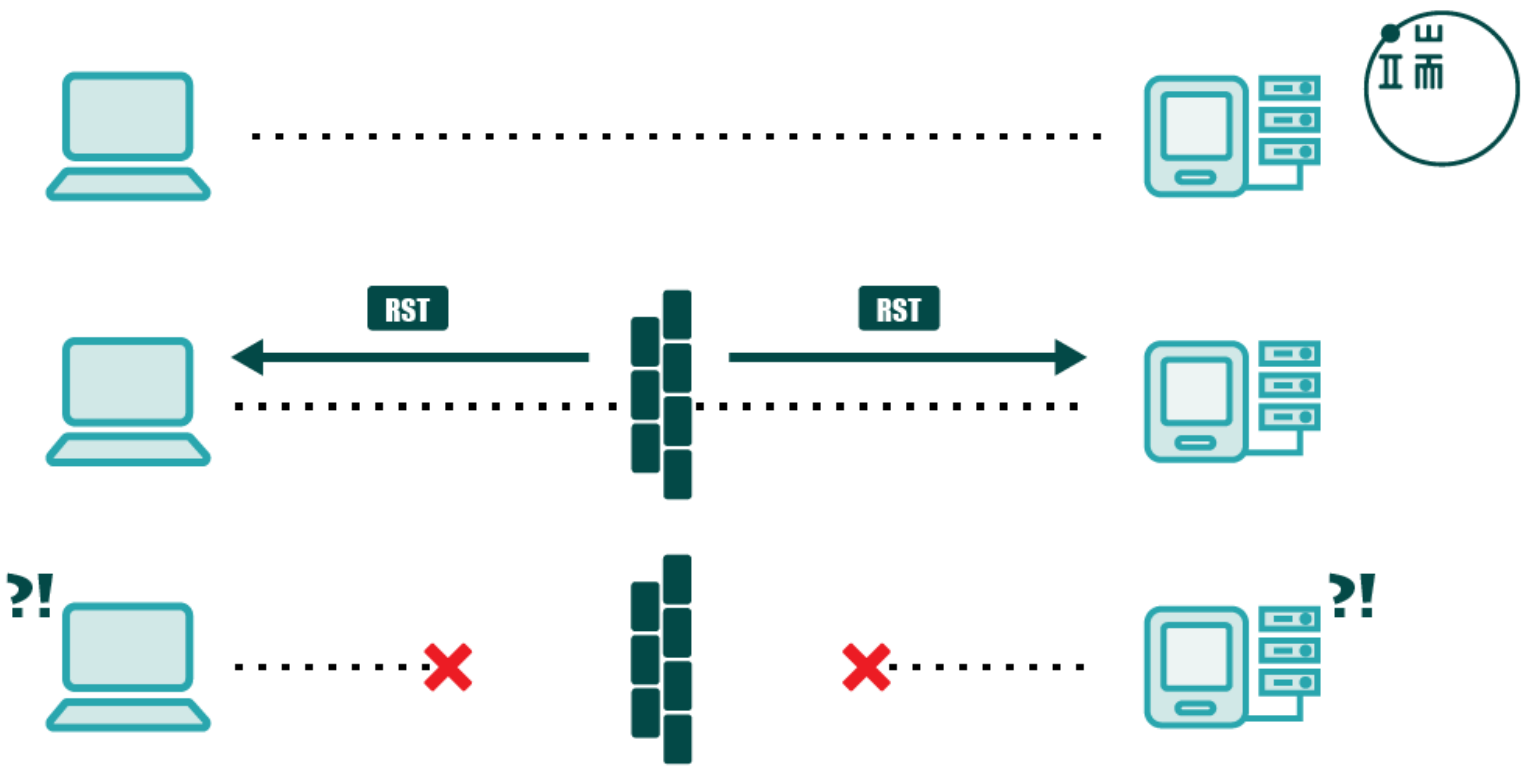


「牆」開始嘗試解析牆內外郵件，終因負載太高，造成大規模延遲。圖：端傳媒設計部

敏感詞觸發RST，偶爾需要「向內翻牆」

這幾年，我在香港求學，當時因為研究需要，我要下載大陸某公司的中文詞庫，奇怪的是，無論使用何種工具，進度條總是停在70%的地方。後來分析發現，每次下載到這個位置的時候，系統就會收到一個“RST”包——“RST”是“Reset”（重置）的意思。這是一種特殊的數據包，當計算機收

到這種包的時候，會重置一條網絡鏈接。這個特點被「牆」廣泛用來掐掉「不和諧」的網絡鏈接。好比A和B正在打電話，「牆」想要掐斷電話，和以前粗暴地摔電話機不同，「牆」對A說：「B掛你電話了」，同時又對B說，「A掛你電話了」，不明真相的兩人就真的自己把電話掛掉了。敏感詞觸發RST，這種「牆」的工作機制，如今已是衆所周知。而這種監控與阻斷是雙向的，出入都可能撞牆。有時候在牆內需要翻出來，有時候在牆外需要翻進去。



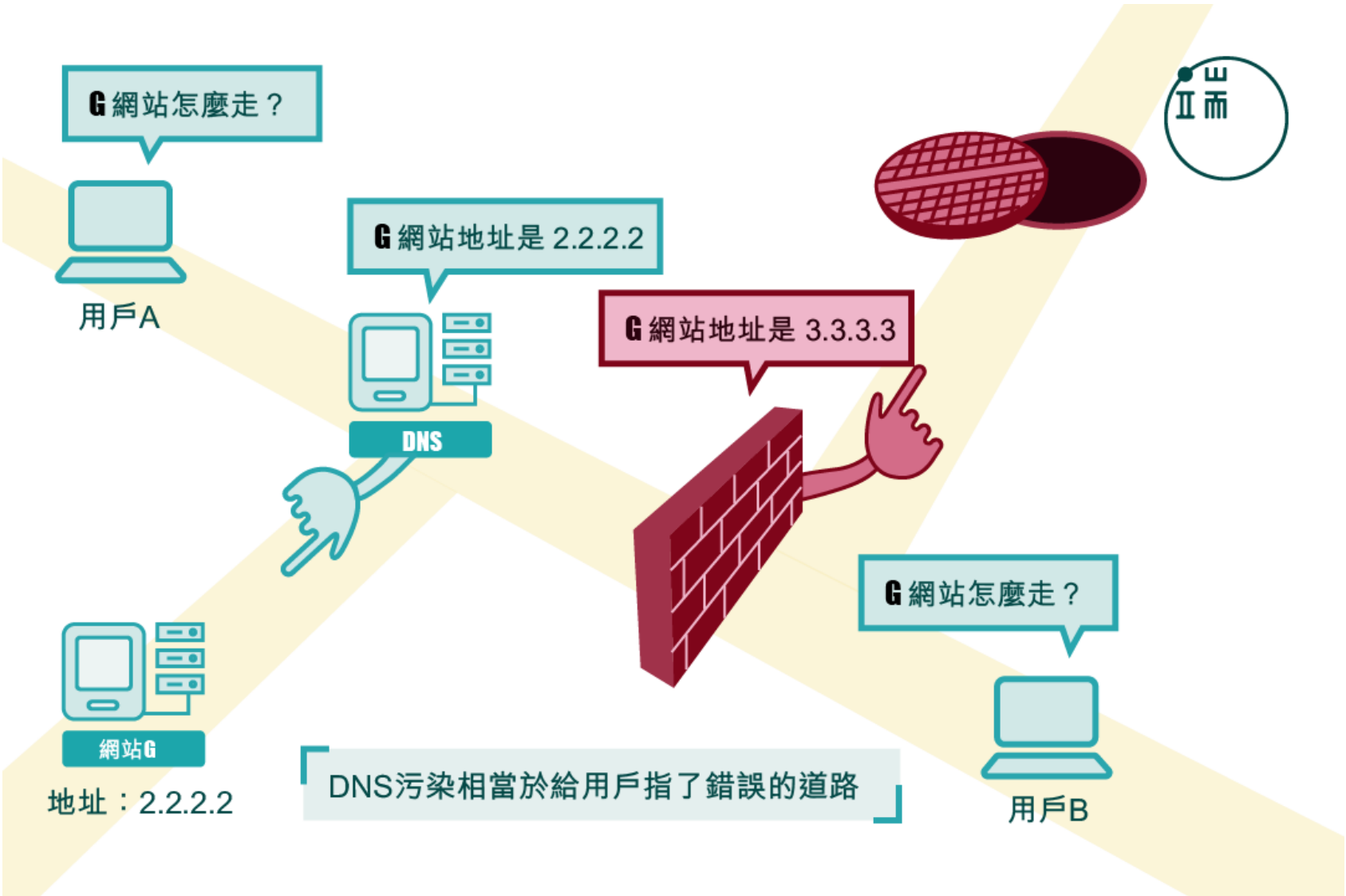
> 好比A和B正在打電話，「牆」想要掐斷電話，它對A說：「B掛你電話了」，同時又對B說，「A掛你電話了」，不明真相的兩人就真把電話掛掉了。

通過"RST"欺騙通信雙方，以阻斷鏈接。圖：端傳媒設計部

走出國門的DNS污染

DNS（Domain Name Service）即「域名解析服務」，功能好比是互聯網上的電話簿。早期，僅通過IP來封鎖服務的話，「牆」需要查看每個數據包，判斷是否放行。但使用「DNS污染」技術，相當於直接給用戶一個錯誤的「電話號碼」，從源頭就遏制了「不良通信」。值得注意的是，「DNS污染」這種強力武器，不僅能有效封鎖國內網民對敏感內容的訪問，還會連帶影響其他國家。2012年，世界頂級網絡通訊會議SigComm上，出現一篇匿名論文。論文發現，中國發動的「DNS污染」已經超越了國界。在測試了全球4萬多個域名解析服務器後，他們發現其中26.41%的服務器受到了這種污染

的影響，覆蓋109個國家。



DNS污染。圖：端傳媒設計部

近500個實體「哨所」

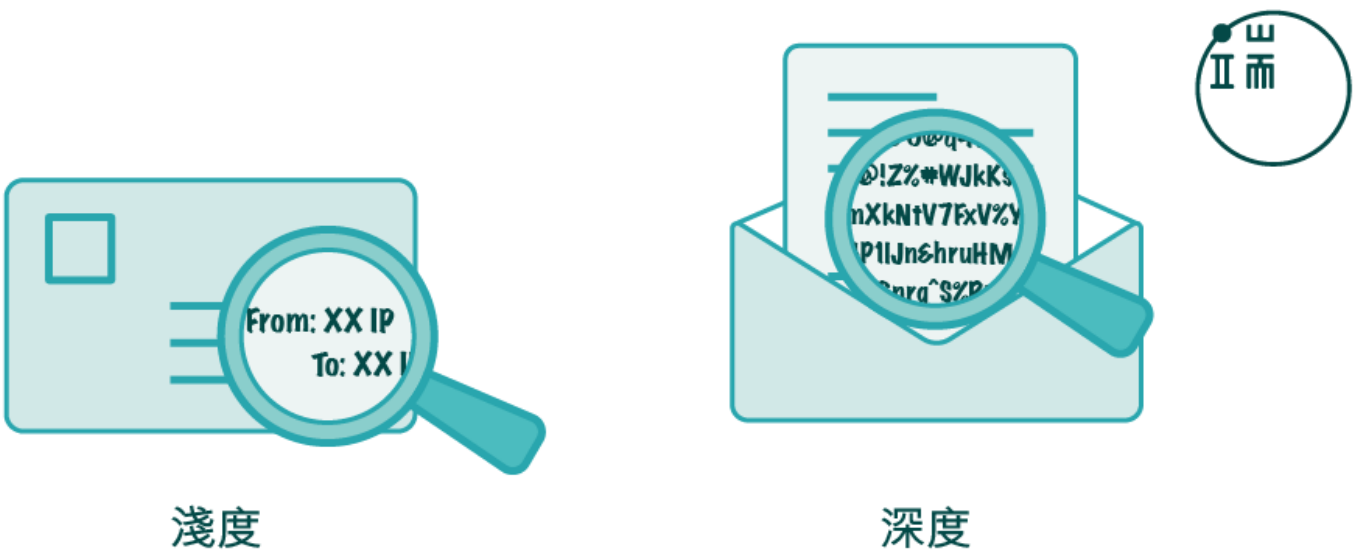
2012年，一組來自Michigan大學的研究者，對「牆」的位置進行了探測。他們發現，就像真實的長城並非連綿不斷的，防火牆也並不是密不透風地「堵」在我們的「網絡」上，而是一組散落各處的「哨所」，只有當發現威脅的時候，它們才用「RST」或「DNS污染」這樣的方式進行干擾。截止2012年底，研究者總共探測到了近500個這樣的「哨所」，在中國南方，部署數量頭三位的省份爲：廣東（84個）、福建（29個）、湖南（28個）。

小插曲是，研究者把探測「哨所」的工具在GitHub（世界最大的開源代碼託管服務）上開源發布後，引起了激烈的爭論。一些人認爲，此舉會激怒「牆」的管理者，導致GitHub被封鎖，影響牆內程序員學習交流，所以應該刪除這樣的代碼倉庫，「保持技術社區的純粹」。另一些人，則認爲翻牆是程序員的基本技能，表示不受影響，所以力挺該項目，並極力反對技術社區加入「自我審查」的行列。

深度數據包檢測

2012年底，「牆」的總設計師、北京郵電大學時任校長方濱興的研究團隊曾發表論文「網絡流量分類，研究進展與展望」，文章提到了多種使用機器學習進行「深度數據包檢測」（Deep Packet Inspection，DPI）的技術。隨後幾年，這些先進的技術逐漸在「牆」上部署開來。

要理解「深度數據包檢測」的威力，我們可以把數據包想像成一封信。「淺度」的數據包檢測，就好像是看看信封上的發件人和收件人，即決定是否放行。這給「跳板法」留下可乘之機：我們先將信送到中間站（如虛擬主機VPS），再轉發到目的地，就繞過檢查了。「深度」的數據包檢測，可以理解成對信件內容的探查——相比起暴力打開信封，這種基於機器學習的技術更具有藝術性。它並不實際解讀數據包的內容，而是搜集周邊信息，對數據流進行「肖像刻劃」（Profiling）。舉個例子，你用Google搜索時，網絡上只會有文本和少量圖片經過，數據量很小，並且是突發的；但用YouTube看視頻時，就會有持續一段時間的大量數據流過。「牆」的監控也是基於這樣的抽象指標，比如它監控到到間歇而細小的流量，便推斷你不太可能是在用YouTube。將諸如此類的可參考指標放在一起，就組成當前數據流的一副「肖像」。把這個「肖像」與數據庫裏面已經存放的巨量「翻牆流量肖像」和「非翻牆流量肖像」做個比對，就可以相應歸類了。如所有的機器學習算法一樣，這種歸類會誤殺一些非翻牆流量，也會錯放一些翻牆流量。但日積月累，「牆」觀察的樣本越多，準確率也就越高。



「淺度」的數據包檢測，像是看信封上的發件人和收件人，即決定是否放行。
「深度」的數據包檢測，可以理解成對信件內容的探查。

淺度與深度數據包檢測。圖：端傳媒設計部

2015年深圳：「牆」的瘋狂進化

新時代的牆，像是手術刀，精準迅速，直擊命門。

在深圳小住半年，我深刻感受到「數字圍剿」的壓力。隨着2014年底，Gmail全面被封禁，牆進化迅速、部署增強，還配合行政措施打擊翻牆勢力。深度包檢測的大規模部署、DNS污染的擴大、轉守爲攻的國家防火牆策略、ISP的深度合作——「牆」儼然是正規軍，而翻牆的社區只能打一場場的游擊戰，越打越疲憊。

首先，是香港的學校專用VPN開始不好使了。據傳，幾種主流的VPN協議已經被「牆」破解，手段十分細膩：有時候連上VPN，可以使用Google搜索和Google Drive辦公，但一旦鏈接YouTube或者Facebook，網絡鏈接就立馬被掐掉了。

緊接着，一系列政策出台：境外VPN需要備案。像Astrill等常用的商業VPN服務，迅速被封。

同時，「DNS污染」的範圍與頻度都擴大了。爲了抵禦「DNS污染」，我曾一度使用「DNSCrypt」——這個開源項目會加密客戶端和服務器之間的通信內容，不被牆查探到。然而好景不常在，很快，「牆」將已知的DNSCrypt的服務器IP計入黑名單，這樣連訪問DNSCrypt的服務器也是需要「翻牆」了……有段時間，我依賴SSH+DNSCrypt翻牆。但這套組合拳，最終打在牆上只是手疼，而牆還是泰然自若。

更有甚者，一些二級ISP（不自建主幹網，但提供社區寬帶接入到主幹網服務的ISP）參與了合作，封禁「非常用」的DNS地址。家庭寬帶用戶，只能選擇ISP默認分配的DNS，或者一些「廣爲人知」的DNS服務器，如Google多年前提供的8.8.8.8（該服務器的IP地址）就是其中之一。「4個8」曾經是大陸網民用來抵禦「DNS污染」的緩衝劑，但它使用普通DNS協議，很容易被攻擊。社區很快發現，「牆」會選擇性地污染8.8.8.8返回的結果。

「DNS污染」、「RST攻擊」、「深度數據包檢測」——「防火長城」的一套立體防禦體系已經建成。從左到右，精準度逐漸加大，防禦成本也逐漸加大。這個時候，不管使用什麼VPN，最常見的現象是，翻牆幾分鐘後，網絡延遲加大，進而鏈接被阻斷，導致日常工作都不能正常進行。

「進攻是最好的防守」——2015年3月，國家防火牆突然轉守爲攻。這是一種與「防火長城」（Great Fire Wall，GFW）部署在一起的設備，網友戲稱其爲「大加農砲」（Great Cannon，GC）。經過3月初的一系列測試，「大砲」從3月中旬開始發動瘋狂攻擊，其首輪攻擊的重點目標之一是GitHub上“greatfire”這個代碼倉庫。“greatfire”上集結了大量的翻牆工具與資訊，儼然一個巨大的「翻牆軍火庫」。「大砲」攻擊目標的原理簡單而有效：它會劫持跨越中國邊境的流量，注入惡意腳本，向指定目標發動「DDoS攻擊」。

DDoS

DDoS（Distributed Denial of Service，分布式拒絕服務），是一種通過巨大流量導致目標服務器不堪重負而下線的攻擊手法。DDoS是一系列方法的統稱，他們使用不同的技術，「大砲」所使用的流量劫持並注入惡意腳本的技術是一種比較新的形式。衡量一場DDoS攻擊的能量，可以使用「峯值速率」。如2014年6月，香港的公民投票網站“PopVote”受到超過“300Gbps”的攻擊，連提供網絡支持服務的Google和Amazon都抵擋不住，宣布退出，最終服務商靠着全球網絡服務業者聯手，才維持「佔中」公民投票持續進行。2015年7月，支持加密功能的即時通信軟件Telegram受到超過“200Gbps”的攻擊，受影響區域很快從東南亞蔓延到全球，導致大量用戶無法通信。要知道100Gbps的流量有多大，可以想像同時在線點播兩萬部高清（720p）視頻。也可以參考的一個數據，据CNNIC報告顯示，截至2014年底，中國大陸的所有國際出口帶寬總和爲4100Gbps。

「牆」轉守爲攻的這一異常舉動，是一個明顯的信號，希望GitHub刪除「有威脅」的代碼倉庫。最終，在巨大的輿論壓力下，「大砲」停止了攻擊。在牆的攻防體系中，「大砲」雖然不直接設防，但它對牆外的「反動勢力」是一種威懾的的存在——必要的時候，隨時可以出擊。

招式	防禦力	攻擊力	精確度	成本
客户端IP/Port封禁	💧💧💧💧💧	✕	💧	$$$
DNS污染	💧💧💧💧	✕	💧💧💧	$
RST攻擊	💧💧💧💧💧	✕	💧💧💧	$$$
深度包檢測	💧💧💧💧💧	✕	💧💧💧💧💧	$$$$$
大砲	✕	💧💧💧💧💧	💧💧💧💧💧	$$$

牆的招式列表。大砲作爲一種威懾的存在，以攻爲守。圖：端傳媒設計部

在「牆」的拼命圍剿之下，傳統翻牆手段逐一失效。原因很簡單：主流方法都有特定的模式，逃不過基於機器學習的「深度包檢測」技術。機器學習的準確性是隨着樣本增加而提升的，所以要逃離「牆」的圍剿，就得把自己的流量僞裝得不一樣。海外專業VPN服務Astrill，以及國內的「曲徑」、「紅杏」等後起之秀，都是通過打造私有協議，來繞過檢測。

在這種形勢下，開源翻牆利器ShadowSocks被更多的人注意到，基於SS搭建的翻牆服務如雨後春筍一樣出現。它的中文名爲「影梭」，社區昵稱爲“SS”——這是一個由中國程序員發起的開源項目，主要開發者在牆內。

2012年4月，SS第一份代碼提交；

2013年，SS完成主要開發；

2014年夏開始，由於牆的升級，SS受到社區更多的關注，進入高頻升級的階段；

……

ShadowSocks開發記錄。

ShadowSocks提供的其實是一套框架，支持多種加密方式，可以監聽不同的端口，只需要很簡單的配置，就可以在客戶端和跳板機之間建立一條隧道。這些特點，讓SS成爲「游擊隊員」們最喜愛的工具。作爲一款「非主流」的工具，SS曾經是非常有效的翻牆手段。但從15年初開始，深圳的部分ISP已經部署針對SS的阻斷系統——推測是基於同一套「深度包檢測」技術。好在SS的參數衆多，隨便調整一下，即可生成不同的「肖像」，令「牆」在觀測不足的情況下，無法迅速動手。但隨着時間推移，「牆」總會搜集到足夠的樣本。剛開始的時候，選一套SS的參數可以堅持幾個星期，到後來，就只有幾個小時了。但牆一天不倒，游擊戰就一天不停。換密碼、換加密協議、換端口，如每天吃飯一樣，逐漸變得規律。實在不行，就只有換IP了，即再買一個VPS。SS的高級玩家，會加入自己定製的加密模塊，使得流量更隱蔽。總之，SS是一個開源項目，玩法多種多樣，打遊擊的優勢巨大。

2015年香港：遙看牆內圍剿「造梯人」

還有太多重要的事情要做，不能將時間浪費在與「牆」無休止的游擊戰中——我決定搬回香港。

而牆內，一場密謀已久的圍剿，終於顯露。

8月20日，ShadowSocks作者在GitHub上關閉了相關項目的Issue面板並清空所有幫助信息，同時GitHub上「shadowsocks」組織的成員信息被隱藏。

8月21日，GoAgent（一款曾經主流的翻牆軟件，託管在Google Code）的論壇上傳出SS作者「被喝茶」的消息。

8月22日，ShadowSocks作者現身GitHub，證實「喝茶」，並刪除了代碼庫。

8月25日，Google Code轉爲只讀狀態，GoAgent論壇散落。

8月25日，GoAgent託管在GitHub上的倉庫被刪。

8月25日，GitHub受到超過兩個小時的DDoS攻擊，攻擊源目前不明。

8月26日，多處消息源顯示，曲徑、紅杏等大陸多家VPN服務商受到直接或間接的壓力，停止服務。

……

以前幹掉的是製造和售賣梯子的人，現在連設計梯子的人也要幹掉。

未來會如何呢？可以想像，大規模的VPN服務會消失；一些小規模的地下服務，繼續運行。另一方面，翻牆工具鏈，勢必會持續升級。公開的成熟項目被封後，社區會衍生出不同變種，以適應「牆」的改變。特別是像SS這樣的開放框架，稍作修改，又是一種玩法，無窮無盡。但沒了牽頭的人，沒了集中的論壇，知識傳遞的形式將會反古。原本，互聯網讓知識可以扁平傳遞，現在「屠梯」行動恐將人們逼回「口耳相傳」的模式。未來，「翻牆」可能是一種手藝，如何傳承，任重道遠。