如何穿透防火墙进行网络攻击思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_A6_82_E4_BD_95_E7_A9_BF_E9_c101_644218.htm 作为一个网络或是系统管理员，你常常需要限制进出你的网络的服务，实现的方法很多，目前为止最常见的就是使用防火墙，然而，无论如何通常大多数的防火墙和网络至少需要放开一种服务-比如打开用户网上冲浪的功能，HTTP是一种十分简单而常用的协议（如较ftp而言），几乎任何网络中的任何一台普通工作站都是允许发送HTTP请求的，通常服务器也同样。 HTTP行为是可以走代理的实现的，然而，这仅仅指明文的HTTP，通过SSL加密的HTTP（HTTPS）通常不可能通过代理实现，这些系统可以和网上的服务器直接通讯而不用担心被窃听，HTTP（S）在某种意义上还是一种交互的协议。你给服务器发送一个请求，服务器给你一个回应，两者之间的交互以及大量的数据传送行为都很普遍，这就决定了通常会被防火墙或其他类似设备屏蔽的数据传输可以轻松的通过HTTP（S）通道到达目的地。来源：www.100test.com 有很多合法的这一技术的使用者，比如，微软，它现在使用HTTP来处理系统之间的RPC请求，通常微软的 RPC（端口135）进入数据包都会被大多数防火墙屏蔽。现在，通过把（这种服务）定向到HTTP（S），你可以大摇大摆的使用RPC服务而无须任何担心。这也就使使用RPC开发的人员工作起来非常容易，无需为了它去做大量的甚至对系统基础的修改。 两个非常典型的例子就是HTTP-Tunnel（window的一个商用方案）和GNU的httptunnle（linux和其他平台所使用开放源码的解决方案）

。HTTP-Tunnel使你很方便的通过任何防火墙。你可以利用它使用大多数的即时通讯软件（ATM，ICQ，Yahoo等，同时，它支持TCP，SOCKS5，Napster等。 这些技术对在有限制的防火墙后面的用户都是很有帮助。如果允许通过HTTP proxy进行WWW访问，那么就有可能使用httptunnel，而且，通过telnet 或是PPP对防火墙以外的访问也就同样有可能了。 很明显可以看出： 用户可以连接那些假定被防火墙所应该屏蔽的外界服务 用户可以使用那些通常被防火墙屏蔽的软件（ICQ，Napster） 攻击者可以使用这种技术来实现远程控制（比如，通过email发送恶意代码） 有一些后门程序同样使用HTTP（S）连接被攻击者控制的外部机器，由攻击者发送指令，实现攻击者与外部机器的交互，相当于使用telnet（通常防火墙会屏蔽这种服务）。 更加糟糕的是，当前使用SSL加密的HTTP变得日益普遍，很多站点都使用这种技术，攻击者（或是内部的人员）因此可以避免任何形式的监控，这是因为任何入侵检测系统都不能解密或是检查HTTPS的数据包。这可就等于任何依赖入侵检测系统检测出去的HTTP-tunnel都形同虚设。 那么为了阻止或是察觉这种行为你有什么可以做的？ 首先你可能需要做的是更改你的安全策略，使它达到如下效果，禁止安装通过HTTP来通道的软件如AIM或是ICQ. 如果你不能确定所使用的软件是否符合这一规范，联系相关的网络管理员。 你还可以列出一些（禁止使用）软件（如windows下的HTTP-Tunnel）。一般而言，如果一个合法用户需要一些访问外界的一些服务，他们应该联系相关的安全管理员而非试图去绕过被保护的系统。 下面一步该做的工作是强化出去的WWW数据控制（如果你还没有这么做的话）

，实现的最好方法是安装一个代理服务器同时过滤出去的HTTP访问包，这样用户将被强迫使用代理。如果对HTTPS这样做的话要困难的多，同时会造成一些安全隐患。但是由于大多数的HTTP tunnel软件还不怎么支持HTTPS，你目前还不用过于担心这个。 一种可以提供这种服务的例子就是微软的Proxy server.你可以实现最基本的限制每个用户或是每个组的使用协议。从机器的角度来进行限制也是一个好的办法，但是要注意用户可能登录到一个“ 可信 ”的系统然后利用它对外界进行访问。 如果可能的话，你应该对出去的请求进行记录。这使你可以查看过长的HTTP请求，或是“ 过 ”快的连续的系列HTTP请求等等奇怪的行为。你还可以审核看起来奇怪的使用方式。除非有人在机器面前，大多数的工作站都不应该产生出去的HTTP流量。HTTP proxy产生的用户进出使用日志使你可以把注意力集中到可能被入侵的机器上。此外，要求用户使用proxy的同时记录那些直接向外的访问，你就可以发现那些没有使用proxy的设备，快速的定位可疑的主机。客户端可以用POST方式取代GET方式，这样的话也就意味着记录出去的数据变得困难起来（我还没有听说过可以支持记录POST数据的东东，这是因为这种数据可能是可执行的，图象，文本之类的）对真正劲头十足的家伙而言，记录所有出去的HTTP数据也是个可考虑的方案，虽然在一个大的网络环境下这样做可能需要充足的空间来存储这些信息。而且如果站点使用SSL，那么就不可能记录了。 总结 计算机安全就像一个快速进化的野兽，新的威胁不断出现老的威胁变得过时（但看起来永远不会“ 死亡 ”）。在早期你可以依靠相应的端口屏蔽相应的服务。然而，由于这种方式被大量采用，需

要用到这些东东的软件提供商（如微软）开始寻找其它的解决方案。不幸的是，把数据放到流行的协议如HTTP，尤其是很容易采用加密的服务上，软件商让公司的企图控制数据进出他所管理网络的网络管理员日子难过了许多。作为一个网络管理员（或是公司安全人士等），你需要维护一个更新的安全策略从而对付这些新的威胁，同时维护一个多层面的安全方案。要知道看起来软件公司（或是个人）可是不象会停止那种想尽办法绕过你的安全手段的呀。