How to improve the security of Campus network
如何提高校园网的安全性

顾新征 黄文学 (南京 河海大学计算机学院 210098)

摘要: 随着网络的发展，网络入侵和网络攻击层出不穷，网络安全问题已经成为21世纪的世界性话题。本文结合工程实例，介绍了VLAN、防火墙和VPN在提高校园网安全性方面的应用。

关键词: VLAN 第三层交换 防火墙 VPN IPSec

1 校园网的安全状况与技术分析

正如校园网安全的需求分析所述，该校校园网在此前存在诸多安全问题：

(1) 内部网访问控制能力不足，难以有效保护众多的需保护资源；

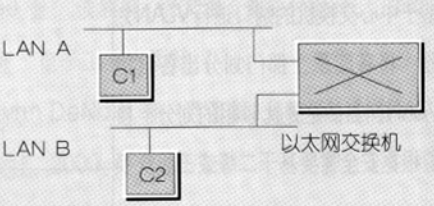
(2) 老的防火墙吞吐能力达不到要求，而一旦抛开它就等于门户大开，形成致命的安全漏洞；

(3) 两校区校园网的连接如果租用专线显然不经济，但直接通过CERNET连接又不安全。

问题(1)是传统交换式以太网的弊端所致。在传统交换式以太网中，交换机只负责把数据包送到目的端口，对数据流向是不加限制的。如图1所示，LAN A中的C1可以访问LAN B中的C2，即使C2中有受保护资源，交换机对此也"不闻不问"；同样，C2可以对C1进行网络攻击，甚至通过网络侦听窃取C1发出的保密信息，而交换机只是忠实地将攻击数据流发向C1或者将窃得数据送给C2。在这样的网络中，除非把LAN B转移到一台独立的交换机上，而且保证LAN B上的节点也不被盗用，否则难以保证C2不受非法访问。这样的物理隔离确实"防火防盗"，但毕竟不能划分太多的物理子网，而且不便于随需求把用户群重新组合，也不便于网络管理。因此，问题(1)的解决需要一种能灵活对用户群进行划分，并能对用户群间的互访问有效控制的方法，这就需要VLAN技术的支持。

问题(2)的产生是因为用作IOS防火墙的路由器和代理服务器的数据吞吐能力满足不了需求。IOS防火墙是基于包过滤的，它获取接收到的数据包中的目的地址、源地址或端口号进行判断，然后依据访问控制规则转发被认为是安全的包，而拒绝转发可能威胁内部网络安全的包。因此，路由器的吞吐能力直接限制了通过防火墙的网络带宽。另外包过滤防火墙在处理端点间的直接连接方面有明显的安全问题，一旦防火墙允许某一连接，就会允许

图1 传统交换式以太网



外部源直接连接到防火墙后的目标目的地，从而潜在的暴露了内部网络，使之容易遭到攻击。代理服务器实现了代理防火墙，当代理服务器得到一个用户的连接意图时，它们将核实用户请求，经过特定的安全化的Proxy应用程序处理连接请求，将处理后的请求传递到真实的服务器上，然后接受服务器应答，做进一步处理后，将答复交给发出请求的最终用户。代理服务器在外部网络向内部网络申请服务时发挥了中间转接的作用，使内外网络的计算机没有任何直接会话的机会，从而隐藏了内部网结构，避免了入侵者使用数据驱动类型的攻击方式入侵内部网，被公认为是最安全的防火墙。但是代理防火墙的处理速度较慢，服务器的数据吞吐能力往往成为网络的瓶颈。该校原代理服务器的最大吞吐能力是200Mbps，要适应千兆以太网环境，就有必要对其升级。

问题(3)的提出是出于安全和经济的网络连接需要。Internet在发展初期没有考虑完善的安全机制，公用网路上的数据可以被以多种手段侦听、伪造，所以Internet被认为是不可信任的。为保证信息传输的安全，就必须另外采取安全措施，如加密、认证(VPN就是其中一种解决方案)；或者保证独占物理线路，即专线连接，这在目前显然是不经济的。

2 网络安全方案

基于以上分析，我们可以采取以下方案。

VLAN的划分如图2所示。首先基于中心交换机的端口进行VLAN划分，将各院系、部门划分出各自的VLAN。当然这是比较粗的划分，接着根据安全需要基于二级或三级交换机的端口进行更细的划分。

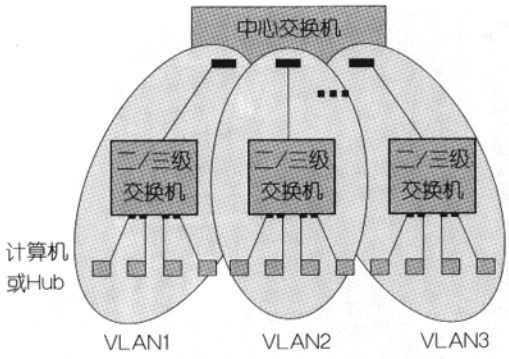


图2 VLAN划分

防火墙的部署如图3所示。在校园网与Internet的接口处部署高性能的硬件防火墙和代理防火墙。

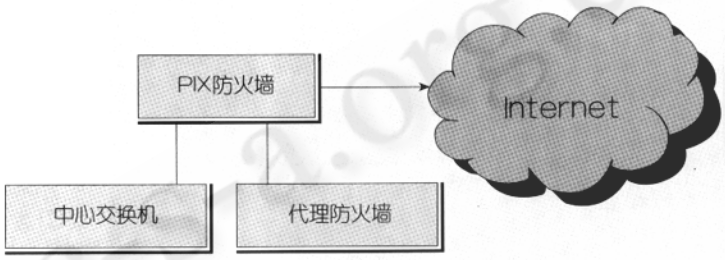


图3 防火墙部署

VPN的构建如图4所示。使用支持VPN技术的路由器在连接两校园网的Internet上构建一条双向加密隧道，从而构成VPN连接。

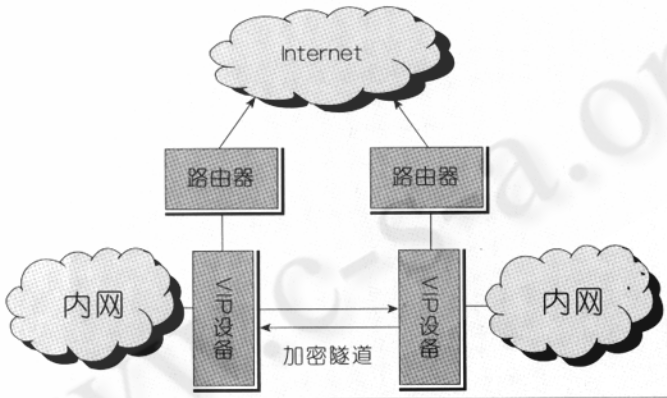


图4 VPN构建

3 技术实现

3.1 VLAN在校园网中的应用

该校利用Catalyst 6506进行第三层交换，分校校园网利用Catalyst 4003进行第三层交换，然后基于交换机的端口进行了VLAN划分。其中本部校园网部分VLAN的划分情况见表1。

表1中的VLAN划分将不同网段的节点划分在同一VLAN中，又将同一网段的节点划分到不同VLAN中，不同VLAN间通过第三层交换机路由层的路由设置进行通信。例如，核心网络设备(主要是二/三级交换机)的管理端口分布在不同网段、不同地点，把这些端口划分在同一VLAN中集中管理，不属于该VLAN的节点不能访问这些端口，这样既方便又安全；财务处等保密单位可以分在独立网段，有时也不得不和一些非保密单位处于同一网段，用VLAN把他们分离出来就可以灵活地保证他们不受其他节点的非法访问。

虚网ID	交换端口	光纤端口	子网IP	单 位
2	1–3	1–6,8	192.168.1.0	网管中心
3	4	9,10,11	192.168.2.0	校办
4	5	10,11,12	192.168.3.0	财务处
5	6	13,14,16	192.168.4.0	图书馆
6	7	7,13,17	192.168.5.0	研究生院
7	7	15,18,19	192.168.6.0	计算机系
8	8	18,19,20	192.168.7.0	数学系
9	8	14,16	192.168.8.0	工商学院
10	8	14,16	192.168.9.0	人文学院

表1 Catalyst 6506上的VLAN划分

通过划分VLAN，降低了通过网络侦听手段盗取诸如网络管理员等高级用户口令的风险，有效保障网络的正常运行和网络信息的安全；同时，还有效解决了IP地址盗用的问题：在路由器中用ARP命令将IP地址和MAC地址绑定起来，再把用户的MAC地址绑定在他所连接的交换机端口上。这样，即使盗用他人的IP地址，也只限于与

他连接同一端口的少数用户的IP地址，影响范围大大缩小了。

3.2 防火墙在校园网中的应用

考虑到性能和带宽的要求，选用Cisco 最新的PIX 535防火墙。PIX 535是一种硬件防火墙，其核心是基于自适应安全算法 (ASA) 的一种保护机制，可以提供面向静态连接的防火墙功能，并同时防止常见的拒绝服务 (DoS) 攻击。它将静态防火墙、IPSec 的虚拟专用网 (VPN) 功能与千兆位以太网吞吐量灵活地结合在一起，不仅具有非常好的安全特性，而且有最好的线速性能 (1Gbps吞吐能力，支持500,000个同时连接)。PIX 535采用专用的操作系统，减少了黑客利用操作系统BUG攻击的可能性。同时将代理服务器升级到Sun 4500，安装两块Intel Pro/1000F服务器网卡，使其满足千兆的网络连接。

图 4 VPN构建在校园网中应用防火墙的拓扑图如图5所示。

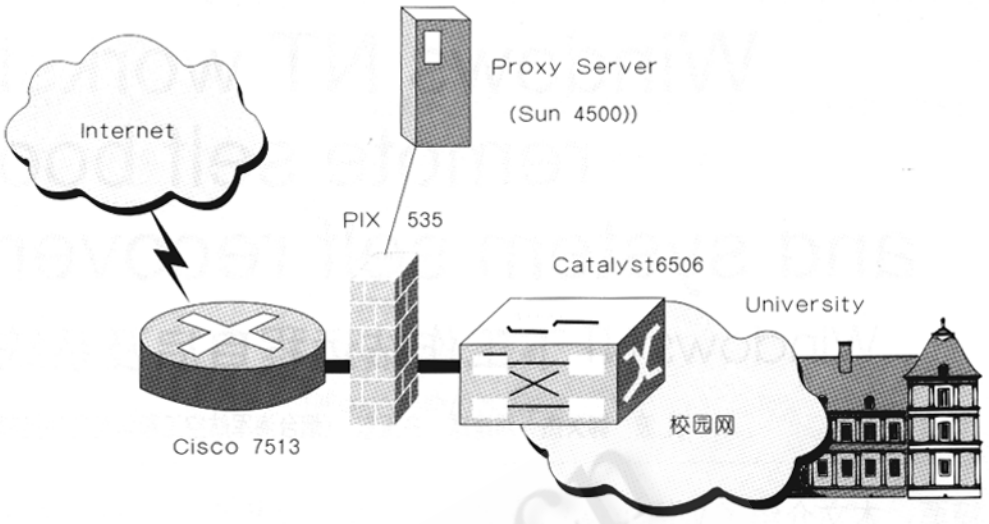


图5 防火墙在校园网中的应用

3.3 VPN在校园网中的应用

VPN既可以在两台主机之间实现，也可以在路由器之间实现。该校校园网的VPN连接利用Cisco 7513路由器的VPN连网功能来实现，拓扑如图6所示。

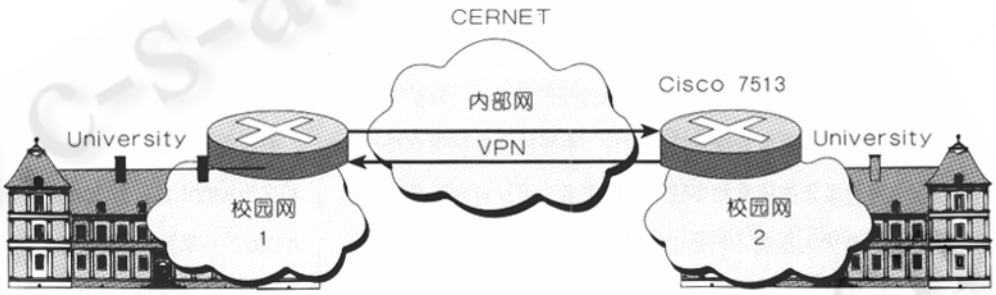


图6 VPN连接拓扑图

图6中两个Cisco 7513路由器在两个校园网之间构建了一个100Mbps的内部网 (Intranet)VPN，这个VPN连接实际就是一对或多对加密隧道，路由器为两个网络之间的通信量提供IPSec服务 (加密、认证等)。IPSec是IP层提供的功能，因此不需要对因特网作任何修改 (只负责传递IP包)，也不需要在两端的PC机和服务器上安装IPSec服务。每个网络内部的局域网是可信网络，对在它上面传递的通信量不作保护；但对于通过因特网在各网络之间交换的数据要进行加密保护。通过在每个路由器上进行策略配置，可以使发送方到对方网络之外的通信量 (如发送到因特网公共网站上的通信量) 正常传送，即不进行任何IPSec处理。

4 结束语

本文结合工程实例介绍了三种网络安全技术在校园网中的应用，由目前校园网的运行状况和安全状况可以证明这些应用是很成功的。目前，全校网络按安全和管理需要初步划分成了20多个VLAN，各VLAN间进行了合理的访问控制，非法访问保护资源、网络侦听和IP地址盗用等现象大大减少了；PIX 535防火墙和代理防火墙运行正常，有效保护了内部网络，同时没有对网络速度造成明显影响；两校区可以方便地通过VPN进行安全的互访问，该校校园网的安全问题得到了很好的解决。当前网络在我国的发展非常迅速，各个大学都建立了自己的校园网，而且越来越多地使用和依赖网络。这些校园网一般都与Internet连接，难免受到来自外部的攻击和内部的非法访问。因此网络安全是在校园网建设中不容忽视的问题，必须投入一定的资金和人力加以解决。同时，在参与工程实施中，作者也感到硬件设备只是保障网络安全的一方面，而对网络软硬件的有效管理也是同样重要的。只有这两方面都做好了，才能最大限度地保障网络的安全。

参 考 文 献

1 RFC2764, A Framework for IP Based Virtual Private Networks [S] February 2000。

2 [美] Donald C. Lee 著，谈利群、张文海、谢能付等译，[M] Cisco网络增强型IP服务，电子工业出版社。

3 [美] Jim Metzler, Lynn DeNoia 著，卢泽新、周榕译，[M] 第三层交换，机械工业出版社，2000。