第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)20—0277—02 文献标识码：A 中图分类号：TP393.08

基于GAP的校园网安全系统的研究与实现

黄 文，文春生，欧红星
（湖南科技学院网络中心，永州 425006）

摘 要：实时交换型GAP技术是一种新型的网络隔离技术，正获得越来越多的重视与应用。针对校园网安全问题的多层次与分布性特点，该文提出了一个基于GAP的“安全区域”解决方案。阐述了方案的关键技术，给出了其实现方法。

关键词：数据交换；网络隔离；GAP；PC104PLUS

Research and Implementation of School Network's Security System Based on GAP

HUANG Wen, WEN Chun-sheng, OU Hong-xin
（Network Center, Hunan University of Science and Engineering, Yongzhou 425006）

【Abstract】The real time exchange GAP is a new technology of network isolation, which is attracting more and more attention in network security. Aiming at the multi levels and distributing characteristic of school network's security, this paper presents a "region security" settle project base on GAP. It explains the key technology of this project, and presents a method to realize this project.

【Key words】data exchange; network isolation; GAP; PC104PLUS

高校的校园网是Internet的一个缩影， Internet所有的安全问题也几乎都存在于校园网中。安全问题是校园网直面的一个难题，而且其解决方案比一般机构更复杂，实现也更困难。

本文提出了校园网安全问题的特点及相关需求，讨论了GAP技术的框架，在此基础上提出了基于该框架的校园网安全系统的设计及实现，最后作出了系统的评估和总结。

1 校园网安全问题的特点

校园网用户是极其复杂和活跃的一个群体，对网络安全的要求也各不相同，总体上校园网安全问题的特点可以概括为：多层次与分布性。这里不妨对校园网从安全层次上做如下区域划分：

(1)涉密区。如重点实验室等，这类机构在高校很典型，需要最高的安全性，若满足不了要求则宁可不联网。这一层次除了收发邮件外，可以浏览信任网，信息只进不出，成为单向连接。

(2)核心区。学校的计算中心、办公网等，这是一个可信网，这一层次需要对外信息服务，但其数据绝对不能被破坏，对其访问必须经过安全性检测。

(3)可管区。电子阅览室、学生机房等，这一层次需要保证其系统稳定工作，系统稳定性和易恢复性是最主要的需求。

(4)不可管区。学生宿舍网络等，这一层次安全性要求最低，只要能高概率地保证其系统不遭破坏即可，但也可能被要求采用访问控制策略。

这4个安全层次的需求基本覆盖了Internet的全部安全层次，而且在校园网中是分布式的，这给解决网络安全问题带来了非常大的困难。

2 基于GAP的校园网安全系统模型

2.1 GAP技术概述

GAP技术最早由以色列和美国军方提出，是目前网络隔离新技术。GAP技术可分成3类[1]：实时交换类型，单向连接类型和网络切换类型。后两种类型因为适合使用的场合有限，不适合校园网的多层次与分布性。实时交换类型GAP技术在两个网络中加入一个转发数据的GAP设备(GAP设备是一个在任一时刻只能物理地连接网络一端的硬件设备)，使两个网络物理隔离；同时采用GAP控制技术通过GAP设备实现两个网络间的安全数据传输和资源共享，原理如图1所示。

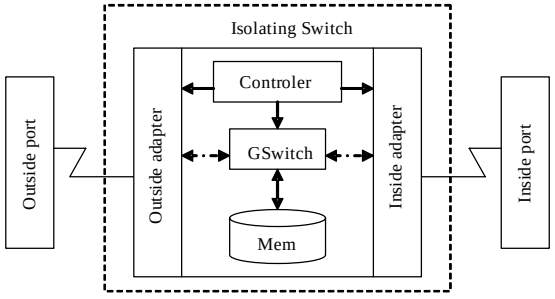

图1 实时交换型GAP结构

在图1中，Outside Port, Inside Port与Isolating Switch构成一个GAP系统，外部网络通过Outside port与Outside adapter连接，内部网络通过Inside port与Inside adapter连接。在Controler的控制下，Outside adapter或Inside adapter通过GAP Switch唯一地与Mem连接，以完成内外网的数据访问。

2.2 基于Gap的校园网安全系统架构

利用GAP技术可以设计出较好的网络安全体系，能充分满足校园网络多层次和分布性特点的需求。基于GAP的校园

作者简介：黄 文(1967－)，男，副教授、硕士，主研方向：网络信息安全，多媒体技术；文春生，副教授、硕士；欧红星，讲师、硕士研究生

收稿日期：2006-11-19 **E-mail：**hw_0802@sina.com

网安全系统架构如图 2 所示。防火墙部署在外网与校园网之间，构成校园网的第 1 道安全屏障。在校园网的 4 个安全区同时部署 IDS，作为校园网的第 2 道安全措施。除不可管区外，在其它 3 个区部署网络 Antivirus 系统，构筑校园网的第 3 道安全防线。以上措施均可采用第三方的产品和手段，能较高概率地保证校园网络的安全，但不具备强安全性保证。能给校园网带来强安全保证的是 GAP1~GAP3 3 个隔离系统。GAP1~GAP3 隔离了 4 个不同安全层次的 VLAN，高、低级的安全区的数据传输必须经过 GAP 设备。

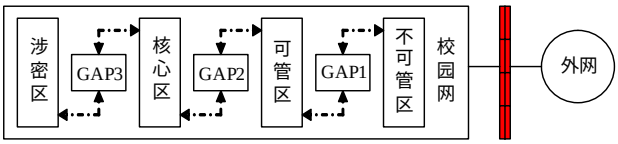

图 2　基于 Gap 的校园网安全系统架构

这里 GAP1~GAP3 的设计相同，但在各级安全区的代理服务中必须设计不同的安全检测规则以满足多安全层次特性的需要。同时对各区 VLAN 的 IP 和 MAC 绑定，使之满足分布式访问控制规则并能嵌入第三方检测规则，以满足校园网的分布特性的需要。

2.3　系统功能描述

不可管区部署校园网外围代理服务器 Web PROXY，众多的初级用户通过 Web PROXY 与外网连接。Web PROXY 其实也就是一般意义上的 Web SERVER，这一安全区不必用 GAP 隔离。首先，这一层次安全需求决定不必使用 GAP；其次，这一区域用户群体庞大，数据流量极大，GAP 切换造成的延迟，对用户带宽会带来不必要的损失。

可管区部署 Web PROXY1，不可管区的 Web PROXY(可管区的 Web PROXY1)根据配置将应用层数据处理后交 GAP1 的 Outside adapter(Inside adapter)，经 Controler 控制对 Mem1 进行存取访问。经 GAP1 到 Web PROXY1 的数据，在 Web PROXY1 中经过可管区的安全检测，连接可管区真正的 Web SERVER1，完成从不可管区到可管区的逻辑通道。若经 GAP1 到 Web PROXY1 的数据在 Web PROXY1 中不能通过安全检测，则链路被安全隔离。

与前面所述相似，核心区部署 Web PROXY2，可管区与核心区通过 Web PROXY1、GAP2 和 Web PROXY2 进行数据传输。涉密区部署 Web PROXY3，核心区与涉密区通过 Web PROXY2、GAP3 和 Web PROXY3 进行数据传输。但是 Web PROXY1~3 的安全检测规则是不同的，必须满足各自的安全需求，并且 VLAN 段的 IP 和 MAC 是不相交的。

这里的描述仅对 WWW 服务，对于其它服务需要相应的代理，基本原理是一致的。

3　GAP 模块的设计

实时交换型GAP技术目前还是网络隔离的前沿技术，国内面市的产品不多，且报价高得惊人，若按本文方案部署，耗资巨大。这里提出了一个基于PC104PLUS[2]高速SCSI通信模块的解决方案[3]，方案以成熟的PC104PLUS模块为硬件，配以自主开发的软件模块能够较好地满足系统的设计要求。

3.1　硬件系统设计

本文采用 MSMS PC104PLUS 通信模块，该模块最高存取速度为 40Mb/s，支持多操作系统，PCI 接口，32KB BIOS，256KB DDR，是理想的 SCSI 通信模块。本方案用两个 PC104PLUS 模块分别作为 GAP 的 outside adapter 和 inside adapter，配以电子开关构成如图 3 所示的 GAP。

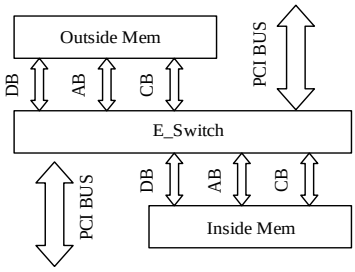

图 3　基于 PC104+的 GAP 结构

图 3 的核心是电子开关 E_Switch，E_Switch 可以通过对两个 PC104PLUS 模块编程来约定实现。outside adapter 的 PCI BUS 工作时，E_Switch 连接 inside Mem，做只读操作，将 Inside Port 的数据读取到 OUTSIDE port。inside Mem 数据读空时，E_Switch 切换到 outside Mem，做只写操作，Outside Mem 满或 outside port 发送队列空则 outside adapter 挂机，同时启动 Inside adapter。inside adapter 的工作机制与 outside adapter 相似，只是 outside Mem 与 inside Mem 的作用正好相反。

不管是 outside adapter 还是 inside adapter，其工作状态由另一方的挂机信号驱动，本方无自启动权限，这样就保证了在任一时刻只有一方在对 Mem 进行读写操作，实现了对两个网络的物理隔离。

3.2　软件系统设计

软件系统主要有[4]：(1)控制E_Switch和adapter的驱动引擎，因为本方案采用SCSI通信模块，所以不妨称为G_SCSI。(2)代理服务系统PROXY，负责真正服务器的数据转发，并且进行对接收数据的安全检测。

(1)G_SCSI 的设计

G_SCSI 采用标准 SCSI-II 协议与通信模块进行实时通信，实现对图 3 所示硬件的 I/O 操作，包括 E_Switch 的切换、检测己方 adapter 是否启动、对 Mem 的读写、将己方 adapter 关闭同时启动对方 adapter 以及对读写数据按 SCSI-II 协议封装解封等。其流程描述如下：

1)检测己方 adapter 是否启动，是则转 2)，否则等待。

2)E_Switch 打到对方 Mem，有待读数据则读取数据，解封，交 PROXY。

3)E_Switch 打到己方 Mem，有待写数据则封装，写数据。

4)待写数据队列空或 Mem 满，关闭己方 adapter 同时启动对方 adapter。

(2)PROXY 的设计

PROXY 与 G_SCSI 接口，将应用层的数据请求转发给另一个同类代理，以连接远端服务器。同时，也将接收到的数据做安全性检测，将通过检测的应用服务请求连接到本地服务器。其流程如下：

1)检测 G_SCSI 接口有无数据发送，否则等待。

2)对接收数据进行安全性检测，通过则交本地服务器处理。否则丢弃。

3)检测本地服务器有无数据发送至 G_SCSI，否则转 1)；是则发送，直到 G_SCSI 写队列满。

3.3　性能评估

按照上面的软硬件设计，在嵌入式Linux系统[5]下实现了GAP系统。系统采用两块PC104PLUS通信模块，内核选择Linux2.4，利用Linux的SCSI Generic Interface[6]实现G_SCS对GAP设备的I/O操作。利用HTTP、SMTP和POP3

(下转第 282 页)