大型IP城域网系统安全案例的经典解析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E5_A4_A7_E5_9E_8BIP_E5_9F_c101_142900.htm 某联通公司目前已经开通的业务有GS M130/131和CDMA133移动通讯、193长途通讯、165数据通讯及17911 VoIP电话等。并在各地市建设城域网，为客户提供相应的网络互联业务，并提供电信增值服务。城域网同样需要安全系统建设。 需求分析 a、需要对地市城域网与省公司骨干传输网进行访问控制，防止来自外部互联网对城域网的攻击。城域网连接着中国联通的骨干传输网络，并与Internet连接。对于某省联通城域网来说，所有连接到联通骨干网的外部网络都是不可信任的，需要防火墙系统的保护。 b、需要对城域网的服务器进行保护。 每个地市城域网都有自己的内部网络和重要服务器。服务器都存在着安全隐患，如果不采取网络安全措施，服务器就可能来自各个互联网络的攻击，因此需要防火墙系统的保护。 c、需要对城域网的客户进行有效管理。 城域网的客户比较复杂，不乏存在着不规范的上网行为甚至是恶意入侵行为，因此对城域网的客户进行管理非常重要。比如，通过防火墙的NAT地址转换、IP/MAC地址绑定、访问日志的记录、审计等等功能，可对城域网的客户进行有效的管理。 解决方案 1 综述 东软股份通过在某省联通地市城域网上配置防火墙系统并设置有效的安全策略将达到以下目标： a、保护基于某省联通的城域网业务不间断的正常运作，包括构成城域网网络的所有设施、系统、以及系统所处理的数据（信息）。 b、某省联通地市城域网系统中的重要信息在可控的范围内传播，即有效的控制信

息传播的范围，防止重要信息泄露给外部的组织或人员，特别是一些有目的的竞争对手组织。 信息系统的安全是一个复杂的系统工程，涉及到技术和管理等多个层面。为达成以上目标，东软股份将在充分调研和分析比较的基础上采用合理的技术手段和产品以构建一个完整的安全技术体系，同时通过与某省联通工作人员的共同工作，协助某省联通建立完善的城域网络安全管理体系。 2 防火墙产品选型推荐 通过对某省联通城域网网络的应用情况及实际拓扑结构的了解，我们注意到，城域网未来将提供越来越多的增值服务，如视频服务、在线游戏等等。这些服务器资源使用非常集中，对时效性要求非常强，会对网络的传输带宽要求很高，因此推荐的防火墙产品不能对网络的性能有较大的影响。 目前黑客（甚至某些计算机病毒）对网络的攻击往往利用服务器应用层协议的漏洞来进行。比如黑客可以通过HTTP对WEB服务器中IIS程序发动攻击，一旦攻击成功后，可进一步在Web服务器上安装特殊的木马程序建立秘密的HTTP通道，整个内部网络就都暴露在黑客的面前。因此推荐的防火墙产品不仅仅具有包过滤的性能，同时更应具有防范应用层攻击的能力，即具有代理防火墙的安全性。 根据前面的分析，推荐使用东软集团完全国产研制开发的具有国际先进水平的NetEye防火墙系统。该系统是一套软硬件结合型防火墙，采用“ 流过滤 ”技术，同时具有状态检测包过滤与应用代理防火墙的优势，能够在交换模式与路由模式下工作，其性能、稳定性、安全性完全可以满足某省联通城域网网络的安全及未来发展的需求。 3 某省联通地市城域网防火墙具体配置建议 a、放置在整个城域网与联通互联网的接口处，防范来自外部的攻击 ； b

、保证网络的性能不受较大影响；c、将城域网业务服务器系统放置在防火墙的DMZ区中，只开放指定端口，这样可以更好的保证城域网服务器的安全。 建议在某省联通各地市城域网与互联网之间分别放置东软NetEye 防火墙系统，将城域网服务器单独放置在防火墙的一个区域。考虑到某省联通城域网业务的迅猛发展，视频、在线游戏等增值业务是未来的发展方向，对网络带宽的要求会越来越高，因此我公司建议配置千兆防火墙，以满足近两年地市城域网的发展需求，具体型号为NetEye 4200G.。并配置为双机热备方式。 项目效果 东软在NetEye防火墙中以状态检测包过滤为基础实现了一种我们称之为“ 流过滤 ”的结构，其基本的原理是在防火墙外部仍然是包过滤的形态，工作在链路层或IP层，在规则允许下，两端可以直接的访问，但是对于任何一个被规则允许的访问在防火墙内部都存在两个完全独立的TCP会话，数据是以“ 流 ”的方式从一个会话流向另一个会话，由于防火墙的应用层策略位于流的中间，因此可以在任何时候代替服务器或客户端参与应用层的会话，从而起到了与应用代理防火墙相同的控制能力。比如在NetEye防火墙对SMTP协议的处理中，系统可以在透明网桥的模式下实现完全的对邮件的存储转发，并实现丰富的对SMTP协议的各种攻击的防范功能。 东软NetEye防火墙凭借先进的“ 流过滤 ”技术优势，丰富的功能，稳定的性能，充分满足某省联通城域网网络的安全及未来发展的需求，在多次大规模爆发的蠕虫事件中，为用户有效的保护了网络资产，赢得了某省联通的信赖！ 