DOI: 10.13657/j.cnki.gxkxyxb.2005.s1.022

NGN承载网的网络安全设计
Design of Network Security for NGN Load Bearing Network

何勇宁
He Yongning

(广西百色市无线电监测站,广西百色 533000)
(Baise Radio Monitoring Station of Guangxi, Baise, Guangxi, 533000, China)

摘要: 介绍了NGN(Next Generation Network)承载网安全模型的构建,讨论了NGN承载网的安全措施、信任区的安全部署、非信任区的安全保证措施。
关键词: NGN 承载网 安全区 信任区 非信任区
中图法分类号: TP393.08 文献标识码: A 文章编号: 1002-7378(2005)S0-0065-03

Abstract This article mainly introduced NGN load bearing network security model constructing, discussed the NGN load bearing network security measure, the trust area safe deployment, non-trust area safe guarantee measure.
Key words next generation network, load bearing network, security area, trust area, non-trust area

下一代网络(Next Generation Network简称NGN)主要由业务/应用、业务控制、核心交换和边缘接入等功能组成,在统一分组网络上集话音、数据、传真和视频业务于一体的全新的网络[1]。

目前NGN主要利用现有的数据网络作为业务的承载网,但语音、视频等实时性业务对NGN承载网提出了高安全要求,而且承载普通数据业务的宽带网、数据网在安全性和网络性能上均难以达到NGN业务开展与实施的要求[2]。采用IP物理专网方式组建NGN承载网,安全性虽好,但对现有网络资源来说是一种极大浪费,也不是大多数运行商的选择。本文介绍利用MPLS VPN技术实现NGN承载网业务隔离和安全域划分,并提出相应的安全措施,满足安全性要求。

1 NGN承载网安全区域的划分

通过MPLS-VPN的方式,承载网把NGN业务设备、NGN业务流以及NGN业务用户等划分到同一个VPN,把网管设备和网管业务流划分到一个VPN,把数据业务划分到一个独立的VPN,VPN之间的访问通过防火墙、信令/媒体代理等安全设备来进行控制。NGN业务网络跟其它网络逻辑上隔离,因而把其它网络上的一些威胁(比如蠕虫病毒、网络DOS攻击等)隔离在NGN业务VPN之外。

在NGN业务网络(NGN VPN)内部,为了提高NGN业务设备的安全性,确保NGN业务的持续可用,把NGN业务网络进行安全区域划分,分成3个安全区域:

(1)安全区域。一些重要的NGN业务设备,比如软交换设备,信令网管等,划分到这个域,这个区域是需要提供重点安全保证的区域。

(2)信任区域。由NGN媒体业务设备、网络汇聚层和骨干层设备(路由器、三层交换机等不直接接入用户的设备)组成,这个区域因为不直接接入业务用户,属于可控制的范围,因此可以作为信任区域。

(3)非信任区域。所有用户接入网络、用户接入设备、企业接入边界等,属于这个区域。在这个区域中,由于各种各样的接入方式的存在,以及大量的不同层次的业务用户的存在,是最不安全的一个区域,所有跟网络有关的安全事故的源头,往往就是这个区域,因此,这个区域跟其它区域需要重点隔离。

收稿日期: 2005-09-01
修回日期: 2005-09-24
作者简介: 何勇宁(1981-),男,广西藤县人,技术员,主要从事无线电监测和无线电设备检测、电磁环境测试工作。

2 安全区的安全措施

2.1 软交换设备端口备份

软交换一般有两个相互备份以太网端口,可以采用 VRRP技术将两个端口连到骨干网,实现对端口的备份和母局承载网的备份。目前的软交换的容量很大,为了实现容灾备份,可以将 2个软交换做负载分担和相互热备份,任一软交换的失效,另一个软交换将代替失效软交换的工作。软交换网关的安全措施原理也同样。

2.2 设置防火墙

由于NGN属于信任域,可以采用通常的防火墙部署方式,在 NGN核心区域与非信任区域之间部署防火墙。

2.3 IDS入侵检测设备

IDS可以及时的发现网络攻击,并作出告警,提示管理员可能发生的情况,或者自行采取一些措施,切断攻击源。IDS的部署提高了网络的抗攻击性。

2.4 有效网管部署

随着网络规模的扩大,网络承载业务的增多,网管的重要性越来越突出。对一个复杂的网络进行集中高效管理是反映一个网络好坏的重要指标[3]。

2.5 运行日志的收集处理

网络设备在运行的过程中,会针对各种各样的事件产生一些日志信息,对这些日志信息进行分析和收集是网络审计的关键。为了对这些日志信息进行统一的管理和分析,建议部署集中的日志收集系统。

2.6 病毒防护体系的部署

为了避免病毒给网络造成威胁,建立合适的病毒防护措施。一般情况下,病毒防护体系遵循客户服务器结构(C/S结构),病毒客户为安装在需要保护的客户 PC机或服务器上的病毒防护程序,服务器则是病毒防护程序的管理进程。

2.7 服务器安全定制

服务安全定制指针对服务器上运行的操作系统、数据库等系统软件,进行合适的配置更改、系统参数调整、安全策略实施等,提高这些系统参数的安全性和效率。操作系统和数据库自身的服务和组件会引入一些安全漏洞。通过对这些组件的分析,可以根据当时的业务需要停止某些组件或服务的运行,或者更改某些运行组件的参数,以达到提高系统性能和安全性的目的。

3 信任区的安全措施

信任区包括 NGN承载网的骨干层设备以及汇聚层设备,由于这些设备不直接接入最终业务用户,因此,该区域面临的威胁相对较小。

3.1 骨干层的安全保证措施

核心的 IP网建议采用全网状/半网状互连组网,要求其具有路由备份能力;边缘路由器和网关设备通过双归属的方式跟核心骨干网互连;链路层尽量采用 SDH/MSTP/RPR等技术,可以在 50ms内完成故障倒换[4]。

一般情况下,在基础网络构架当中,网络设备是被攻击的对象,因此,除适当的部署防火墙、IDS等手段外,通过实施网络设备本身的一些安全特性,比如 ACL,路由认证等手段,提高整个网络的安全性。

3.2 汇聚层的安全保证措施

边缘汇聚层必须有宽带用户管理能力的设备存在,汇聚层设备应具有 BAS功能,保证 IP城域网安全,对汇聚层设备安全特性主要考虑几点:

(1)汇聚 BAS设备能够保证接入侧用户相互隔离,保证接入的安全性,能够防止 IP地址盗用、仿冒等行为,能够防止用户之间的相互攻击;

(2)支持访问控制列表(ACL),包括支持在虚拟路由器中创建 ACL列表,可根据 IP/ICMP/UDP进行过滤,多种过滤规则可提供多种层次的对目标网络的保护,禁止部分用户的访问或有选择地屏蔽网络服务。

(3)与防火墙、IDS实现联动考虑,若流量异常时,自动将流量镜像到 IDS,由 IDS进行攻击检测,检测结果反馈到原始设备,进行封堵源 IP或者封端口。

由于汇聚层设备的关键地位,因此需要重点考虑。另外,从长远看,用户安全防护也需要考虑,以提供用户安全防护。提供用户防毒和集中安全管理以及升级将是提高通讯网络安全的关键。

4 非信任区的安全措施

接入层是 NGN核心网的延伸,可以利用各种的接入技术延伸 NGN业务覆盖的范围,要求接入网在链路层实现用户隔离。接入设备如 BAS设备、二层交换机等,它们需要支持用户间的隔离,能够将隔离用户的物理信息传递,这是 IP城域接入网络的基本需要。对于 XDSL接入,由于用户是物理隔离,相对比较安全,LAN方式需要考虑对每一个用户划一个

VLAN隔离,保证用户数据的安全。另外,需要考虑用户带宽限制。WLAN接入方式的安全性本身比较弱,必须考虑认证措施和数据加密。常用方法如下:

(1)完善用户标识机制。用户标识指的是能唯一确定一个用户的数字表示。比如,可以采用MAC地址+ VLAN ID+ VPI/VCI+ IP地址+ 用户名绑定的方式来区分用户,这样一个用户就可以被精确的区分,即使存在用户名盗用的情况,也因为该用户名的其它部分不匹配而不能正常接入网络[5]。

(2)采取用户接入流量监控,反向转发路径检查,接入访问列表控制等措施。

(3)要从根本上解决城域网的安全问题,必须对用户接入网络的终端主机进行安全的管理,将安全延伸到用户终端,或者说对用户终端发出的、进入网络的流量进行规范。即运营商为保护公共的承载网络——宽带IP城域网,而对终端的一个规范要求,类似于终端的入网检测以及接入规范。

5 结束语

因为MPLS固有的许多优点,在MPLS上实现VPN的网络配置简单,可提供用户与网络的安全性,而且具有良好的可扩展性,且其在速度和QoS支持上有很大的优势。MPLS是目前唯一能够实现IP网中的QoS与流量工程的网络技术[4],流量工程也是解决网络安全的重要措施之一。通过MPLS VPN组建多业务网络、宽带数据业务和NGN业务共用物理承载网,需要在接入边界对宽带业务流进行优先级强制标识,以防止流量攻击。本文引入MPLS VPN技术,通过网络结构优化,解决了改造前NGN承载网中存在的QoS、安全性和稳定性的问题,取得了良好的效果。NGN承载网需要全网的规划,实现难度比较大,而且需要有支持MPLS协议的设备如三层交换机和路由器等。如果应用发展,网络难以承载高速发展的NGN业务时,必须采用IP物理专网方式组建NGN承载网,或考虑部分NGN业务独占一条物理网络。

参考文献:

[1] 杨红梅. NGN与下一代通信业务[EB/OL]. http://www.trs.cttl.com.cn, 2005-02-11.

[2] 陈如明. NGN问题理解及其发展策略思考[EB/OL]. http://www.telecom.com.cn, 2004-03-12.

[3] 胡道元. 网络设计师教程[M]. 北京: 清华大学出版社, 2001.

[4] 沈金龙. 现代电信交换与网络[M]. 北京: 人民邮电出版社, 2001.

[5] 叶 华, 谢 玮. IP电话/传真技术[M]. 北京: 人民邮电出版社, 2000.

[6] 沈金龙. 计算机通信网[M]. 西安: 西安电子科技大学出版社, 2003. 321-365.

(责任编辑: 黎贞崇)