{国际贸易}校园网出口解决方案

20XX年XX月

精心制作 您可以自由编辑

校园出口设计解决方案

项目小组：

小组成员：詹长贵、陈志洲、荣融

目录

1. 校园网出口设计的重要性 3
2 .当前校园网出口面临的挑战 3
    2.1 多出口支持挑战 3
    2.2NAT 性能挑战 3
    2.3 安全防御挑战 4
    2.4 流量控制挑战 4
    2.5 内容审计挑战 4
    2.6 高可靠挑战 4
    2.7 扩展挑战 5
3.选择的拓扑方案 5
4. 方案分析 5
    4.1 双出口设计 6
    4.2 RSR-16E 汇总出口数据 6
    4.3 ACE3000+NPE50 的完美组合 8
        4.3.1 RG-ACE30008
        4.3.2NPE5011
5. 实现的技术 15
    5 .1 NAT 技术 15
    5.2 PPTP VPN 技术 15
    5.3 策略路由技术 16
    5.4IPv6 over GRE 隧道技术 16
    5.5 访问控制技术 16
7. 产品的配件 17

附件：18

RSR-16E 技术参数 18

校园出口设计解决方案

第一章校园网出口设计的重要性

目前各高校对校园网的建设非常重视，大多数都建成了一个能满足数字、语音、图像等多媒体信息以及综合科研信息传输和处理需要的千兆以太综合数字网。校园网大都采用了千兆以太网技术，百兆到桌面，网络结构为核心层、汇聚层和接入层三大部分。随着各种网络教育实践活动的广泛开展，如网络办公、远程教学、科研工作、网上招生和在线培训考试等。同时，校园网内部用户也需要对外网资源的访问。出口，在世界数字化得今天，是我们通往世界的桥梁！

第二章当前校园网出口面临的挑战

2.1 多出口支持挑战

当前大部分国内高校校园网出口都采用多出口的架构,原因是:

(1) 提高访问不同网络资源的速度。和电信、网通等运营商互联仅在北京、上海、广州三地有交换中心,且带宽也不够高,这就给教育网访问公网,运营商网访问教育网带来瓶颈,需要采用多出口提高访问速度。

(2) 解决线路备份问题,避免出现单出口的单点故障。多出口的架构一般在实际应用中,需要出口设备支持多元素匹配的策略路由功能,而且实际应用的策略路由的规则数有几百条。早期或部分新的出口设备,启用海量策略路由后,性能下降较多影响出口。

2.2NAT 性能挑战

由于校园网大多采用私网地址,访问外网需要进行 NAT 网络地址换,即使有些高校拥有较多教育网只但通过网通、电信线路访问资源时仍然需要做,由于运营商分配的地址有限,因此校园网出口设备需要做海量的 NAT,出口设备 NAT 性能决定校园上网速度的重要因素。

NAT 性能主要取决几个因素:

(1) NAT 最大并发连接数；

(2) NAT 新建连接速率；

(3) NAT 吞吐能力。

2.3 安全防御挑战

校园网出口区域是校园网的“门户”,作为镇守校园网“门户”的出口设备自然也成为安全的第一关。由于近几年网络带宽的迅速增长,网络威胁也呈现快速增长态势,攻击、扫描、入侵、D0S 攻击、蠕虫病毒攻击、恶意软件、垃圾邮件、还有各种 P2P 应用。出口设备既要防范校外网络威胁进来,又要防范校内异常流量对出口设备造成破坏。校园网络带宽越大,网络威胁可能造成的危害也就越大,出口设备安全防御面临空前挑战。

2.4 流量控制挑战

近几年,各种 P2P 应用（BT、电骡、迅雷、网络电视等）非常丰富,这些应用占用了大量的网络资源,出口带宽的增长几乎永远无法满足这些应用的胃口,正常的应用带宽难以得到保障,所以非常有必要对一些影响正常应用的特定应用进行必要的流量控制。

2.5 内容审计挑战

边界设备需要为海量的 NAT 记录日志以满足国家相关内容的审计要求。由于开启日志会严重影响性能,使得本来就难以承担海量 NAT 工作的边界设备性能进一步降低。

2.6 高可靠挑战

校园网出口区域由于其特殊的位置,因此校园网出口的不可用会导致整个校园网成为一个信息的孤岛,如何保证出口设备的高可靠,如何保证出口网络线路可靠,也都摆着校园网管理者的面前。

2.7 扩展挑战

校园网络迅速扩展,出口设备背后支持的用户数不断增长,虽然很多校园骨干网络已经是万兆网络,但出口设备与校园骨干网接入仍然采用千兆线路,网络带宽瓶颈依然存在二出口设备与骨干网采用万兆接口相连以解决带宽瓶颈的需求,会在未来一年扩展中逐渐浮现出。但若现有出口设备不支持万兆接口,恐怕就无法面对扩展的挑战,现有出口设备投资无法得到长期回报。

3.选择的拓扑方案

第四章方案分析

在出口部署了锐捷网络 NPE 网络出口引擎和流控设备；NPE 保证了出口的高性能。流控设备对各种应用进行识别和基于应用的带宽控制。从架构上，全网锥形架构；实现的效果是校内任何汇聚设备到出口只有 1 跳。

4.1 双出口设计



设置 Cernet（1G）,电信 ChinaNet（200M）。提高了访问不同网络资源的速度，解决线路备份问题,避免出现单出口的单点故障。

4.2RSR-16E 汇总出口数据

RSR-16E 是锐捷公司与 juniper 公司合作，针对电信、政府、电力、金融、教育、企业等用户网络需求现状定制的一款集高性能转发、高灵活性业务处理和高密度接入能力于一体的高端多业务路由器。

4.2.1 丰富的业务支持能力

全面的 VPN 业务可满足最多的客户需求,最大程度提高供应商收入；支持传统的 VPN 同时，同时支持基于 IP 的 2 层 VPLS 与 3 的 VPNRFC2547 ；IPSec 和 GRE 等；

支持 LLQ ，对话音、视频及其他实时敏感性应用提供高质量的保证；

按 DLCI、VP、VC、VLAN、信道(DS0)和端口 QoS ；

分类、速率限制、整形、加权循环调度、严格优先级调度、加权随机早期检测、随机早期检测和数据包标记；

第 2 层(802.1p、CLP、DE)映射到第 3 层 QoS(IPDSCP、MPLSEXP) ；

基于硬件的 IPv6 性能、MPLSIPv6、IPv6overIPv4GRE 隧道、IPv6/IPv4 双栈；

强大的组播支持包括 IGMPv1v3、PIM-SM、PIM-DM、MLD、SSM、RP、MSDP、BSR 以及 MPLS/BGPVPN 中的组播,以高效利用资源、传输高价值内容；

基于网络的安全业务包括 NAT 和状态防火墙、以及按 VRF 的 NAT 和状态防火墙；

用于汇聚链路的 MLPPP、MLFR.15 和 MLFR.16,802.3ad ；

利用 Flow 记帐、源级使用以及目的级使用特性,可按应用和 CoS 资源使用灵活计费,以及基于距离的计费；

通过合作伙伴关系实现多厂商网络管理解决方案；

基于 XML 的 ScriptAPI 便于第三方和内部 OSS 开发。

4.2.2 广泛地提供业务

特性丰富的 RGNOS 软件在平台上运行,确保一致的业务,并使供应商可独立于连接或服务地区密度向所有用户推出所有业务；

可通过任何接入技术,包括 ATM、FR、以太网和 TDM 连接；

支持不同类型的接口：DS0 到 OC-192/STM-64 ；

降低运营成本；

可无缝迁移到更大的平台,以适应网络的增长。

4.2.3 低投入高产出的基础设施

业务构建可完全隔离控制层面、转发层面和业务层面,可在单一平台支持多种业务；

在尽可能降低资本开支和运营开支的同时,最大限度提高收入；

将以前由 NAT、状态型防火墙、IPSec 和 QoS 等不同设备执行的功能整合到锐捷 RSR-16E 平台中；

在单一平台上提供多种业务使客户可以不必进行资本投资即可尝试许多不同的业务,从而扩展业务,进一步拓展用户数量；

逻辑路由器支持供应商将一个路由器分割成多个管理域和路由域,以便使两个完全不同的机构共享一个基础设施。

4.2.4 高可靠性

用于 RE 切换的无中断切换,具有无中断转发特性；

联机软件升级可实现无中断的较小升级；

MPLSFRR 确保流量能够迅速地绕过故障；

MPLSTE 路径控制用于路径优化,结合了可预测的性能,可用于话音和视频等延迟敏感型业务；

LSPping 等高级 OA&M 特性可用来排除 MPLS 的故障；

支持 GR（完美重启）,可实现业务无中断重启 IS-IS、BGP、OSPF、OSPFv3、LDP、RSVP、第 2 层 VPN 和第 3 层 VPN ；

模块化 RGNOS 软件可确保某一个模块发生故障时不会对整个操作系统产生影响；

4.2.5 安全网络

高性能 NAT、状态型防火墙、攻击检测和通过多业务 PIC 实现的 IPSec ；

隔离路由层面和控制层面,可利用状态型防火墙保护控制层面；

Flow 状态型数据包流监控带有标准的 flowdv5 和 v8 记录,可全面监控网络；

扩展性高的过滤、单点发送 RPF 和速率限制可防止 IP 欺骗和 DOS 攻击；

高性能 IPSec 和 MPLSIPSec 具有数字证书支持特性,可进一步加强安全性；

其他无处不在的安全特性,如端口镜像、加密管理会话业务、安全隧道功能、安全远程登录和可配置的权限级别及用户账户。

。

4.3RG-ACE3000——流控专家

RG-ACE 应用控制引擎以 DPI（DeepPacketInspect ，深度包检测）技术为核心，支持软/硬件 Bypass ，提供了基于七层应用的带宽管理和应用优化功能；在带宽管理方面，配合用户自定义的带宽策略以及 RG-ACE 的核心带宽自动分配算法，可以为网络链路划分多个虚拟带宽通道，能够实现最大带宽限制、保证带宽、带宽租借、带宽配额、应用优先级、随机公平队列等一系列带宽管理功能，为客户提供了带宽管理、分析和优化的一体化解决方案，能够有效的检测和防止不正常应用对网络带宽资源的非正常消耗，保证关键应用带宽，限制非业务应用带宽，改善和保障了整体网络应用的服务质量。

4.3.1 网络实时流量监控与分析

□网络流量的实时采集、监控和精细分析使得网络运行状况、应用情况、带宽使用情况等状况完全可视化

□基于协议和基于 IP 地址（用户）两种类型的实时流量分析器，提供访问的源/目的 IP 地址、服务端口、应用协议、Session 数以及流量大小等详细信息。

4.3.2 应用层自动识别和分类

□P2P 应用：Bittorrent、eMule、KAZAA、KURO、NAPSTER、EDONKEY、AUDIOGALAXY、EZPEER、KUGOO、GNUTELLA、VAGAA、SOULSEEK、POCO、PIGO 等 30 多种 P2P 软件。

□IM 应用：MSN、Yahoo、ICQ、AOL、QQ、YAHOO、WEBIM、IRC、XMPP 等 10 多种主流的 IM 软件。

□视频/Streaming 应用：新浪直播、搜狐直播、RTSP、SIP、PPSTREAM、PPLIVE、APPLEQTC、CCIPTV、QUICKTIME、REALPLAYER、MMS、QQlive、H.323 等主流的视频和流媒体应用。

□网络游戏：COUNTERSTRIKE、QUAKE1、DOOM3、QQGAME、CGA、SUBSPACE、XBOXLIVE、QUAKE-HALFLIFE、BATTLEFIELD1942、WOW、联众等网络游戏。

□炒股软件：大智慧证券信息平台、天一证券网上交易系统、华泰网上交易分析系统、证券之星等炒股软件。

□企业办公、数据库与中间件：HTTP、SMTP、POP3、IMAP、文件共享、FTP、SQLServer、Oracle、DB2、WebSphereMQ 等企业的关键应用。

□为用户关键应用提供量身定做的自定义特征码。

4.3.3 网络流量控制管理

□支持基于用户（源 IP 地址）、目标 IP 地址、时间、协议和应用等为参数进行灵活的阻断

与允许功能；

□支持基于用户（源 IP 地址）、 目标 IP 地址、时间、协议和应用等为参数进行上行与下行带宽控制；

□支持基于用户（源 IP 地址）、 目标 IP 地址、时间、协议和应用等为参数进行 Session 数量控制；

□支持组对象的配置，如定义用户组（IP 组）、协议组（如 P2P 协议组、游戏组）对同一类型的应用、相同级别的用户进行带宽管理策略的控制。

4.3.4 流量整型与应用优化

□支持自定义虚拟带宽通道、最大带宽限制、保证带宽、带宽租借、应用优先级以及随机公平队列等一系列的应用优化和带宽管理控制功能。

4.3.5 提供丰富的图表报告分析和统计

□提供一年内的应用或协议流量纪录，并可生成天、周、月、季度、年时间段内的应用及协议的带宽使用统计报告。包括：总带宽分析报表、应用带宽分析报表、基于协议的带宽分析报表、基于协议和流量方向（进入/出去）的带宽分析报表、基于应用和流量方向（进入/出去）的带宽分析报表、基于 IP 地址的带宽分析报表、用户自定义报表等等

4.3.6 应用层防火墙

□应用层防火墙能够识别并阻断黑客的端口扫描以及 DoS 攻击行为，支持通过 Session 数控制、带宽控制来提高网络可用性和安全性；

4.3.7 集中化的图形化管理平台

□提供中英文的图形化管理平台，可以用一台管理服务器集中的管理网络上的多台 ACE 设备。图形化管理平台采用 JAVA 架构，能够适应于各种操作系统和服务器，用户只需利用浏览器即可远程访问管理服务器进行设备管理。

4.4NPE50——NAT 转换高手



NPE50 产品是锐捷网络公司针对网络出口实际需要开发的专用设备，采用全新 NP 架构设计，主控板固化提供了 3 个光电复用的 101000M 以太网口，带两个支持热拔插的 NMX 模块插槽；NPE 具备转发高性能，在启用 NAT、ACL、PBR（策略路由）的情况下，在通常情况的报

文流情况下（平均报文长度为 500byte 左右的混合报文）,双向可以达到 8Gbps 的线速转发，每秒可以创建 30 万条以上的 NAT 会话，在 2Gbps 的 NAT 线速转发情况下，每秒仍然可以达到新建 7 万条的 NAT 会话，达到 200 万条的并发 NAT 会话，内嵌防火墙功能，具有强大的设备自身抗攻击功能。

4.4.1 先进的硬件体系架构

采用双核 NP 硬件体系架构，NP 内双核并行处理，性能倍增。

在主控板上固化提供了 3 个 GE 口，直接和 NP 连接，不占用背板带宽，达到线速转发。

GE 口都支持光电复用，不需要额外单独购买价格昂贵的 GE 模块，节省投资，应用灵活方便。

模块化设计，NPE50-20 支持 2 个 NMX 模块插槽，通过扩展可以支持达到 7 个光电复用的 GE 口。NPE50-40 则支持 4 个 NMX 模块插槽，通过扩展可以支持到 11 个光电复用的 GE 口

支持 1+1 的冗余电源，保证系统的可靠性。

支持 USB 的应用，提供了 2 个标准 USB 插槽，采用 USB2.0 的标准，兼容 USB1.1 标准。支持 USBFLASHMemory（U盘），可存储配置文件及日志文件，因其具有良好的可移动性，可减少许多重复的配置工作，大大减少系统维护的工作量。

4.4.2 高性能 NAT

由于 IPv4 地址的匮乏，NAT 作为网络出口设备必备功能，随着网络规模和出口带宽的扩大，需要更高速的 NAT ，锐捷 NPE 设备，采用 NAT 与 REF（锐捷快速转发）高效配合，并充分利用流交换技术，实现高速 NAT ，NPE 作为网络出口设备性能上不会成为瓶颈：

在启用 NAT、ACL、PBR（策略路由）的情况下，在通常情况报文流情况下（平均报文长度为 500byte 左右的混合报文），双向可以达到 8Gbps 的线速转发。

每秒高达 30 万条的 NAT 新建连接会话。在 2Gbps 的 NAT 线速转发下，每秒达到新建 7 万条 NAT 会话。

并发达到 200 万条的 NAT 会话数。如果按照每个网络节点 300 条 NAT 会话，则可以同时支持将近 7000 台的网络节点同时在线。

4.4.3 多功能 NAT

支持 NAPT、NAT 以及路由的混合使用，满足各种复杂的网络地址规划；

支持 NAT 静态映射，向外提供 WWW、Telnet、FTP 等服务；

支持 NATRe-routing 和反向 NAT ；

提供 NATALG 功能，支持 FTP、RTSP、MMS、H.323、SIP 等特殊应用协议。

4.4.4 快速 ACL 包过滤技术

NPE 提供性能卓越的 ACL 包过滤功能，支持标准和扩展的 ACL 访问控制列表。NPE 采用先进的流表处理技术，利用源 IP、 目的 IP、源端口、 目的端口、协议号等 5 个元素来定义一条流。每秒可以处理和创建的流数量达到 10 万条。

每个 ACL 包涵多个控制列表表项（ACE），NPE 将 ACL 和流交换高效整合，实现 ACL 和 ACE 数目多少对于数据转发接近零影响，有效的提高网络出口设备的数据包转发能力。

4.4.5 高性能策略路由

根据用户制订的策略路由，基于源接口更加灵活的数据包路由转发机制。与功能强大的 ACL 配合使用，可以根据报文的源地址，目的地址,应用协议进行有效组合，实现策略路由。

NPE 设备上，将策略路由与流交换高效整合，实现 PBR 规则数目多少对于数据转发接近零影响，有效的提高网络出口设备的数据包转发能力。

4.4.5 灵活的流量控制

流量限制是防止某些用户或者应用（如 BT 等 P2P 应用）占用过多的网络资源，使用流量管理用户能够公平使用带宽。对于一些常见的 DOS/DDOS 攻击，在其他防御手段都无效的情况下，流量限制是一个简单直接的方式。NPE 具有丰富的流量控制功能：

带宽限制：可以提供从基于接口的带宽限速，到基于策略的每用户的带宽限制；
并发会话数限制：基于策略的或者每用户的并发会话数限制；

新建会话速率限制：基于策略的或者每用户的新建会话速率限制；

4.4.6 完备的日志管理

日志对于网络安全的分析和安全设备的管理非常重要。NPE 针对各种网络攻击和安全威胁进行日志记录，采用统一的格式，支持本地查看的同时，还能够通过统一的输出接口将日志发送到日志服务器，为用户事后分析、审计提供重要信息，NPE 日志包括：

设备日志：设备状态，系统事件日志
上网记录日志：上网记录日志

攻击日志：设备网络受到攻击的日志信息

4.4.7NPE 内嵌防火墙功能

NPE 设备作为网络出口设备集成防火墙功能：

报文过滤：报文过滤是防火墙最基本的功能，根据安全策略对数据流进行检查，让合法的流量通过，将非法的流量阻止，从而达到访问控制的目的。

状态检测：对基于六元组来识别网络流量，并针对每条网络流量建立从二层至七层的状态信息。并基于这些状态信息进行各种丰富的安全控制和更深粒度的报文过滤。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/046203205132011000