



解决方案

# 金融行业外联网 解决方案



## 星网锐捷网络有限公司

### 福州总部

福州市金山大道618号橘园洲星网锐捷科技园  
邮编: 350002  
电话: 0591-83057888 0591-83057000

### 北京市场中心

北京市海淀区复兴路33号翠微大厦东楼9层  
邮编: 100036  
电话: 010-51715999/68156699 传真: 010-51715896

技术支持网站: <http://support.ruijie.com.cn>  
技术支持信箱: [service@ruijie.com.cn](mailto:service@ruijie.com.cn)  
技术支持电话: 4008-111-000  
客户投诉邮箱: [claim@ruijie.com.cn](mailto:claim@ruijie.com.cn)

### 分销中心

北京 010-51715999	长春 0431-88996643	长沙 0731-4428255	成都 028-85400328	大连 0411-84687815	福州 0591-83057382
广州 020-37600792	贵阳 0851-5870013	哈尔滨 0451-87532700	杭州 0571-88259262	合肥 0551-5528521	深圳 0755-83043874
济南 0531-86161486	昆明 0871-3161087	兰州 0931-8457776	内蒙古 0471-3382678	南昌 0791-8177610	南京 025-83247911
南宁 0771-2844846	上海 021-64325691	沈阳 024-31321335	石家庄 0311-89617960	苏州 0512-62511139	太原 0351-7924993
天津 022-27422925	武汉 027-87854855	西安 029-87285471	厦门 0592-2295501	新疆 0991-2338406	郑州 0371-65350175
重庆 023-68889979	青岛 0532-88029575				

如需了解更多产品信息, 请浏览 <http://www.ruijie.com.cn>

内容解释: 本资料内容制作时间为2009年8月, 其产品图片及技术数据仅供参考, 如有更新恕不另行通知, 具体内容解释权归锐捷网络所有。

[www.ruijie.com.cn](http://www.ruijie.com.cn)

011001010100101010101

敏锐把握应用趋势 · 快捷满足客户需求

## 1. 背景

随着加入WTO 进程越过5 年期限,我国银行业将进一步开放,国际竞争的加剧,迫使中国银行业从重视资本负债业务转向重视中间业务的发展。为了最大限度的提升金融服务能力、挖掘客户资源、开拓赢利渠道,金融行业不断创新业务品种和服务手段,应运而生了大量的中间业务品种,例如:跨行支付、银联卡、各类代收代付业务、银证代理业务、银保代理业务、银税代理业务等。金融企业通过与渠道伙伴的联网,拓展了服务渠道、丰富了业务品种。

专家预测,未来几年,中国经济将高速发展和进一步开放,银行中间业务市场将进一步快速增长。由于中间业务的发展潜力是一个逐步释放的过程,银行业的支付结算、代理业务、银行卡、电子商务等各大类中间业务均将保持一定的发展速度,从而带动中间业务市场的整体性增长。在相对保守的假设下,专家预测未来五年,我国商业银行中间业务收入将保持年均30%以上的增长速度。而作为中间业务处理的IT 网络支撑系统,是拓展业务渠道的基础,金融行业已在其各级机构中建设了大量的外联接入,而且随着业务品种的创新,数量越来越多,目前业务品种已达数百种,大型金融企业仅一个一级分行辖内与合作伙伴的网络连接就可达上百个。

这将对保障中间业务稳步增长的银行外联网络提出更高的要求。

### 1.1 目前金融行业外联网存在一些不足

#### 1.1.1 接入方式多样性, 不易维护和部署

- 接入线路类型和外联接入平台设备多种多样,如PSTN、ISDN、DDN、E1转以太网等等。
- 接入点分布在多层分支机构,较分散,有些在二级、三级机构都部署有外联出口。
- IP地址规划和地址转换缺乏统一规范性。

#### 1.1.2 网络可靠性低

- 有大量低端路由器在使用,无电源、引擎等可靠性配置,设备的可靠性较差。
- 外联网络设备没有考虑冗余性,存在单点故障,如防火墙、汇聚交换机、接入路由器等还采用单机结构等。

- 没有采用冗余网络结构和冗余路由设计,网络不具有可靠性。

### 1.1.3 多接入点和规范不一致,导致安全性风险

- 由于外联出口分散在多个分支机构的情况存在,大量分散的外联接入边界导致攻击风险点分布广泛,导致安全风险增加。
- 安全防护措施单一,很多机构在边界都采用了防火墙,但策略部署简单,只用来进行简单的访问控制,没有从多点和多层面来设计和部署安全防护体系。
- 外联网更容易被攻击,由于直接连接外联单位,更具有不可控性,现在基于网络的攻击手段和各类病毒越来越多,如木马、蠕虫、DDoS等等,使威胁更难以抵御,甚至导致网络瘫痪。

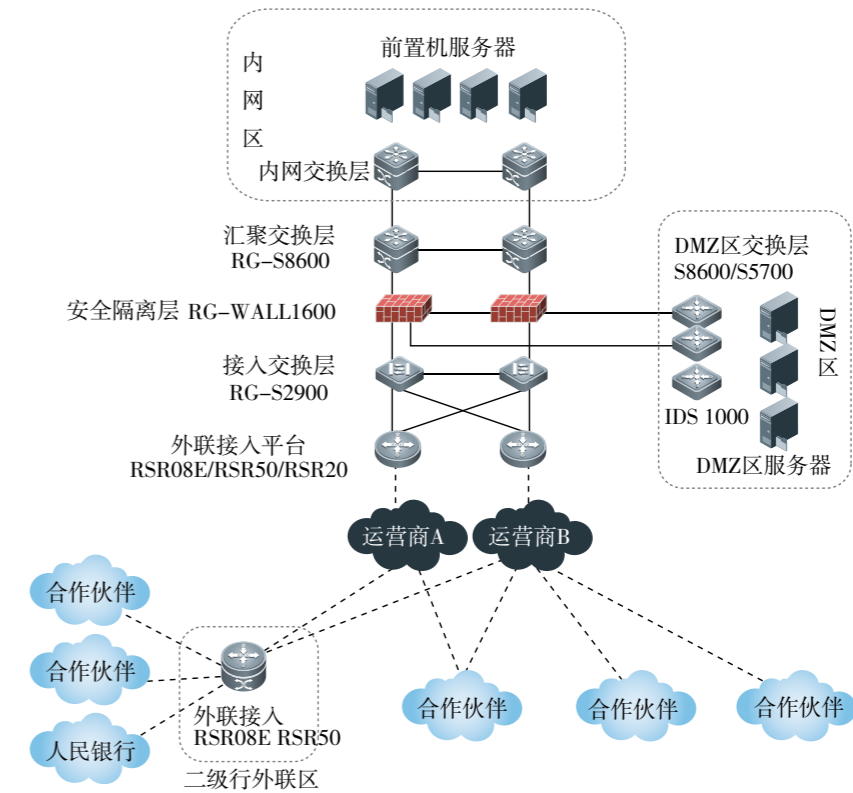
### 1.1.4 可扩展性差

- 有些金融机构的外联网没有模块化和规范化设计,不利于随着新外联业务的快速发展而灵活扩展,导致新的应用开展时,不容易部署和应用,以及难于管理。

## 2. 锐捷金融行业标准化外联网解决方案

方案采用上下分层、左右分区设计,将不同功能的应用分区部署,物理上每一层都采用冗余设备布署,冗余互联模式,采用高可靠性的设备。纵向上采用RG-S8600高端交换机作为外联区汇聚层;采用RG-WALL 1600防火墙形成安全隔离层;采用千兆二层交换机RG-S2900形成交换接入层;采用锐捷RSR08E、RSR50系列和RSR30、RSR20系列作为外联接入层。外联网区又将DMZ单独成区,采用RG-S8600系列或RG-S5700系列作为DMZ区接入交换机;采用IDS1000形成入侵检测层。

金融二级分行也存在非常广泛的外联业务,对于二级分行外联,一个简单、安全、规范的方式是通过独立的线路接入一级分行外联平台,本方案也是采用这种方式实现二级行外联的整合接入,二级行外联区域采用锐捷RSR系列路由器作为外联平台,实现大量合作伙伴的灵活、安全、高效接入。



### 2.1 实现外联网络的规范统一

分散在一级、二级分行、甚至三级机构的外连接入方式,接入点多、分散,虽然接入较灵活,但导致了更大的安全风险,不利于管理和维护。所以,尽量减少外联边界,整合外联出口,规范外联接入方式和线路类型,外联网络向一级分行集中甚至向总行集中是大势所趋。集中的外联出口有利于安全风险的控制,采用更高带宽、更高速、更高可靠性的汇接外网链路,将使外联网的部署容易、快捷,适应中间业务的高速发展和渠道的更快拓展。

锐捷网络RSR08/16E系列、RSR50系列路由器,是基于可编程ASIC架构高性能多业务路由器,具有CPOS、ATM、T3/E3、CE1、LAN等丰富的接口类型,能保证外联网统一整合接入,大容量的转发性能和最高16槽扩展能力确保了对外联业务的承载能力。

### 2.2 实现外联服务的可持续性

外联网络采用上下分层、左右分区设计,将不同功能的应用分区部署,物理上每一层都采用冗余设备布

署,冗余互联模式,采用高可靠性的设备,如接入平台和防火墙都采用VRRP、防火墙还采用双Active模式的HA技术等等,这些高可靠性技术确保了网络任何一个环节的问题都能得到迅速恢复,保证外联业务的持续性。

## 2.3 实现外联服务坚不可摧的安全性

面对外联网络存在的巨大安全风险,必须采用全方位的立体安全防护体系进行风险防范。如:采用分区设计的网络架构,将应用服务器进行分类,分为对外(对合作伙伴)和对内(不直接对合作伙伴)服务两类,对外提供服务的服务器集中放置到DMZ区,对内的服务器集中到内网服务器区,使对外和对内分离,从应用系统部署和网络结构设计都能确保整个外联网络的高安全性。

作为外联接入平台的路由器,是外联网的第一道关口,首先自身必须具备足够的抗攻击能力,特别是应该具备强大的防火墙功能,而不仅仅是单一的访问控制过滤功能。锐捷网络的RSR系列路由器除具备基本的安全访问控制能力外,还具备强大的防火墙功能,能基于状态识别和控制每一个流,同基于状态的防火墙功能一致。

作为隔离层部署的防火墙,在外联网络中起最关键的安全隔离作用,起到将内网跟外网隔离关键作用,同时基于状态防火墙的精确控制,确保了外联网络的安全可信。锐捷网络RGWALL1800、RGWALL1600系列防火墙,是新一代基于硬件高速状态检测防火墙,具有强大的数据处理能力、丰富的安全特性、DOS/DDOS防护等功能,同时采用多种高可靠性技术,完全支持双机状态热备功能,支持Active/Active和Active/Standby两种工作模式,实现负载分担和业务备份。

## 2.4 实现金融行业IP 信息安全和有效管理

保证金融行业的IP信息安全,对保护金融网络的安全至关重要。所以,采用完善的NAT技术,不但可以保护IP信息的安全,而且实现IP地址的有效管理使用。方案中采用的锐捷公司防火墙和RSR系列路由器所具备的基于硬件流表技术的高性能NAT功能,在接入平台上对合作伙伴网络地址进入内网后进行精确的IP地址转换,而在锐捷防火墙上实现将内网IP地址转换后才发布到对方,既有效防范了内部地址信息的泄漏,又避免网络地址的变更给双方带来实施和部署上的困难。

11011001010100101010101

敏锐把握应用趋势 · 快捷满足客户需求