敏锐把握应用趋势 • 快捷满足客户需求

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
技术支持电话：4008-111-000
客户投诉邮箱：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

解决方案

金融行业统一互联网出口解决方案

www.ruijie.com.cn

1. 方案概述

随着金融企业多渠道服务的拓展，越来越多的服务及业务应用需要通过互联网来进行。Internet技术的快速发展为广大用户获取广泛的资讯提供了很大的便利，同时网络中充斥的病毒、木马也使用户面临着更大的使用风险。如何在满足客户的服务需求、保证正常业务开展的同时，进行集中有效的风险控制与管理？ 这是广大金融企业目前考虑的重要问题。锐捷网络统一互联网出口方案或许能为您提供答案。

2. 互联网出口现状与挑战

2.1 互联网业务需求分析

2.1.1 银行业需求

网上银行服务渠道

网上银行是银行业基本的服务渠道之一，为了满足客户多样化的需求，目前银行通常的做法是在营业网点放置少量的PC，PC上安装Windows简化版，屏蔽大部分与网银使用无关的功能，租用运营商一根ADSL线路，供用户上网进行网上银行转账、行情查询、代缴费等操作。

办公业务的交互操作

银行内部员工进行个人网银操作的时候，使用办公IP网段通过内网上数据中心的网银服务器进行日常的个人业务办理，这样可以避免使用Internet，具有较高的安全性。但是带来的问题也比较明显，占用了内网的线路资源。

2.1.2 保险行业需求

保险行业在进行业务办理的时候，也有很多互联网业务的需求，一方面，保险公司和银行有业务交互操作。如省分公司的网银业务，目前有些保险企业的做法是，使用终端安全加密措施通过Internet和银行实现资金查询、划拨操作。另外为了提高客户满意度，在服务网点可以放置少量的PC供保险客户进行一些保单办理进度的查询操作。

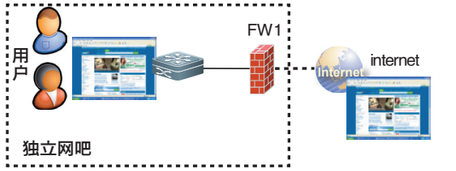
综上所述，由于有如上述的需求，因此金融行业的Internet需求必不可少。

2.2 互联网出口模式分析

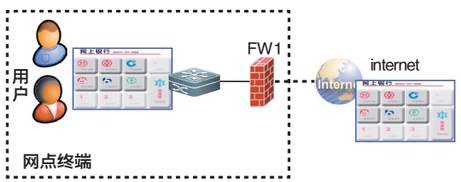
从目前来看，金融行业上互联网主要有独立网吧模式、混用模式及其他模式等几种。

2.2.1 独立网吧模式

这是一种相对比较安全的组网模式，完全独立，和内网生产、办公没有任何直接或间接地连接，也是银行业各级机构常用的组网方式，银行业各一级分行辖内存在众多分散的Internet出口。这些Internet出口有些是建设于一/二级分行、支行办公大楼内部，用于满足内部员工办理有关办公业务和日常上网浏览需求。

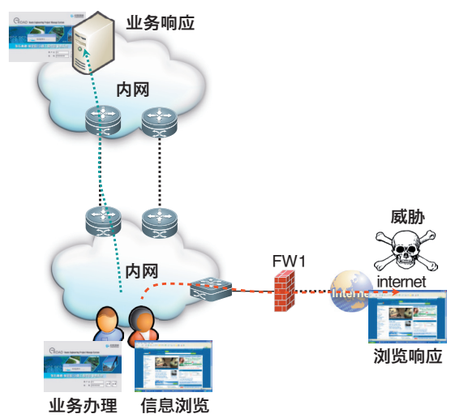


有些是建设于分行辖内各营业网点，用以满足网点为客户提供网银业务操作及演示的需求。这些环境大多是采用与银行网络系统物理独立的Internet网吧环境方式为用户提供服务。



2.2.2 混用模式

如右图所示，这是一种安全隐患比较大的组网模式，内网的机器既可以办理日常生产、OA业务，同时也可以上Internet进行信息的浏览与查询，这种组网模式通常存在信息安全建设起步较晚的保险企业，这也是与保险业的业务处理方式决定的，在处理业务的过程中，需要经常上Internet查询相关的数据。保险业各级机构存在众多分散的出口，出口通常用一台防火墙加一台路由器，添加一些简单的防护措施进行上网的安全控制。整体安全控制能力偏弱。



2.2.3 其他模式

由于统一控制机制的缺乏，可能有些金融用户还存在某些科室单独接入ADSL，采用一些小型的共享型网关，实现小范围进行上网操作的功能，这些方式都是分散的、不确定的，给统一的管理带来了很大的难度，同时也带来了很大的安全威胁。

2.3 互联网出口带来的挑战

2.3.1 挑战一　安全整合、统一管理

风险集中管理，统一的安全控制机制部署。有关上网用机的客户端安全管理、网络安全防护、网站访问权限范围控制、用户上网行为管理等措施都无法实施统一有效的管理，难以保证行内外用户安全有效地使用。

2.3.2 挑战二　企业内部风险控制，法规遵从

由于互联网资源具有复杂多变的特性，互联网的管理已与企业管理密不可分。2006年银监会发布《银行业金融机构信息系统风险管理指引》，明确指出“银行业金融机构应加强网络安全管理。生产网络与开发测试网络、业务网络与办公网络、内部网络与外部网络应实施隔离；加互联网接入边界控制；使用内容过滤、身份认证、数据加密等技术手段，有效降低外部攻击、信息泄漏等风险”。

对保险业而言，上级监管机构保监会也发布了《保险企业信息安全评估体系》对保险信息系统提出了完整的信息安全评估标准，从主机系统、数据库、网络及其他相关的信息资源提出了明确的风险控制要求。

3. 需求关注点

综合上述金融行业Internet使用现状及业务特点，总结起来在Internet的安全使用上需要重点关注如下的问题：

上网风险的集中控制与管理–需要统一规划，统一Internet出口；可以将互联网出口设置在总行（总公司）或省行（省公司），关闭下辖机构的所有互联网出口（现有的通过互联网办理的业务除外，如银行的网银）。将统一出口设置在总行（总公司）将给总部IT部门带来很大的管理压力，建议将互联网出口设置在省行（省公司）。实现风险集中、管理上收。

加强出口安全防护建设–Interent是最不可信任的区域，充斥着大量的病毒和木马，因此必须在互联网统一出口处，建立一套严密的安全防护措施，最大程度将安全威胁挡于门外。

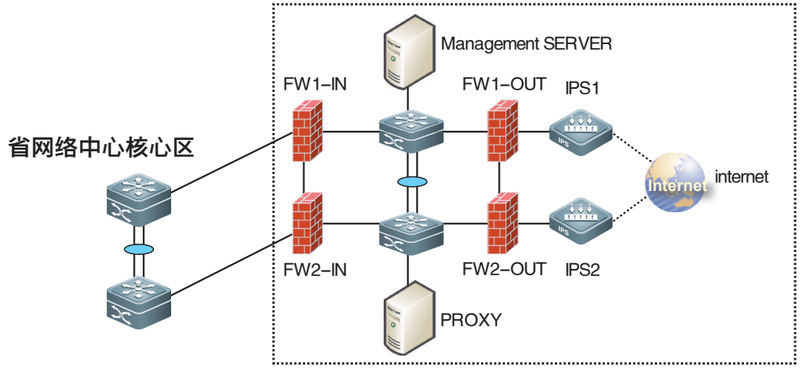
现有带宽资源的保护–互联网出口上收以后，网点、地市机构的Internet业务应用势必给二级骨干、三级网带来更大的传输压力，需要有合理的带宽管理机制减少对关键业务传输的影响。

上网用户的精细化管理–面对如此庞大的用户群，必须有严格的上网用户机分配策略、URL管理、上网日志管理等一系列的策略控制措施，保证整体网络的安全。

4. 锐捷网络解决方案

4.1 网络构架图

在省网络中心建立统一的互联网出口，如下图所示：



在省级网络中心建立独立的互联网接入安全区，Internet入口放置两台IPS入侵防护系统，对来自公网的各种攻击进行阻断、告警。

双层防火墙中间通过千兆交换机相连形成了一个安全缓冲区，缓冲区交换机可以接入上网代理服务器，上网行为统一安全管理软件等服务器。

在设备的选型上，建议采用锐捷的RG-S5750-48GT/4SFP全千兆线速交换机作为安全缓冲区接入设备。该交换机具有强大的抗攻击能力及防arp欺骗能力。防火墙选用锐捷的RG-WALL 1600。具体的产品特性请见后文描述。

4.2 方案要点

4.2.1 风险集中、统一出口

为了满足金融用户的上网需求，规范上网统一管理，增强网络的安全性，减少从Internet入口流入的病毒或木马的威胁。必须对金融各一级分支机构Internet出口进行整合，在各一级分支机构本部建设与企业内网逻辑隔离的集中的Internet出口。通过实施各种网络安全防护和客户端安全管理措施，满足银行各网点网银业务操作及演示、保险企业上网进行业务办理及各级办公用户互联访问需求。实现风险集中控制，管理上收。

4.2.2 多层防御、安全缓冲

入口第一道安全防护

处在网络最外层的是双IPS，同时具备检测和防御功能IPS 不仅能检测攻击还能阻止攻击，做到检测和防御兼顾，而且是在入口处就开始检测，而不是等到进入内部网络后再检测，这样，检测效率和内网的安全性都大大提高。

双层防火墙构建安全缓冲区

内外层防火墙建议采用两家不同厂商的设备，异构防火墙设备大大增强了网络的安全稳固程度。当第一层防火墙意外被攻破时，增加了攻破第二层防火墙的难度。由于是省内机构上Internet唯一的出口，这就要求防火墙必须具备先进的数据包状态检测功能及强大的数据处理能力，这样可以保证防火墙不会成为瓶颈；而且海量日志分析、压缩、储存也至关重要。这样便于日常的维护与管理。

从职责分工上来看，IPS主要偏重于攻击检测与防护，而防火墙则偏重于访问控制，两者可以很好地互为补充。大大提高Internet入口的安全防护能力。

缓冲区接入交换机的安全

接入交换机一方面连接了内外双层防火墙，另一方面连接了上网代理服务器和上网行为管理等重要的策略服务器，因此缓冲区交换机自身的安全控制能力也显得至关重要，自身的安全防护、安全接入控制能力等的安全辅助设置可以使Internet接入区的安全能力得到进一步的提升。

锐捷交换机具有如下的特性优势：

- 独立的安全协议栈

RG-WALL1600防火墙采用独立的安全协议栈，可以自由处理通过协议栈的网络数据，基于网络行为检测的多流关联分析技术，支持对网络数据的深度状态检测。

- 采用先进的硬件平台

通过多内核系统实现对不同数据流量的调度，极大提高设备的处理性能，满足用户对高性能安全设备处理能力的需求。

● 深度状态检测

RG-WALL1600防火墙支持对网络数据的病毒过滤、支持入侵检测(IPS),支持对P2P和即时通讯软件的限制、支持URL以及WEB内容过滤、支持邮件内容过滤,支持FTP内容过滤,还可以和多种IDS产品联动,为细粒度的网络安全管理提供了有利的技术保障。支持按照时间段进行过滤,支持对每一个连接状态信息的维护监测并动态地过滤数据包,支持对FTP、HTTP、SMTP、RTSP、H.323等应用层协议的状态监控。

● 强大的处理能力

RG-WALL1600防火墙采用快速流检测(FFD,Fast Flow Detect)引擎,对网络报文处理流程进行了革命性的改造和优化,将关键处理过程下移,在硬件中断里实现流分类、流交换;产品采用分段直接寻址安全规则搜索算法(MSDAL,Multi-Stage Direct Addressing Lookup Algorithm),减少因系统内部任务间切换、内存缓存管理以及安全规则匹配对性能的消耗,从而提升了整个系统的处理性能。支持一对一、多对一、多对多、静态网段、双向转换等多种形式的NAT,提供源的和基于目的策略路由支持,高速的处理性能基本不受策略条目和并发连接数目的影响。

● 支持全面的网络攻击防护

支持CC、SYN flood、DNS Query Flood等DoS/DDoS攻击防护,支持MAC和IP绑定功能,支持智能防范蠕虫病毒技术、TCP报文标志位不合法攻击防范、超大ICMP报文攻击防范等等网络攻击防护;

● 完善的日志管理与审计

提供各种日志功能、流量统计和分析功能、各种事件监控和统计功能、邮件告警功能,配合日志管理系统可以完成日志的记录、查询和分析。

● 支持高可靠性

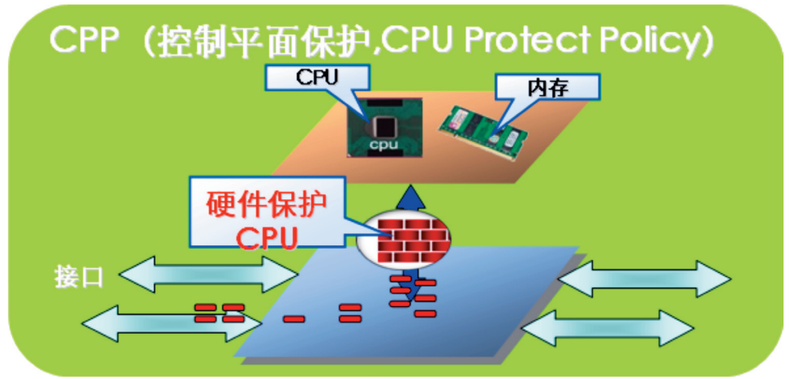
支持双机状态热备功能,支持Active/Active和Active/Passive两种工作模式,实现负载分担和业务备份。设备关键部件均采用冗余设计。

锐捷防火墙具有如下的特性优势:

● 自身的抗攻击能力

缓冲区交换机利用自身的安全控制能力,可以使internet接入区的安全能力大大提高。

CPP安全保护技术,CPU保护策略(CPU Protect Policy,CPP)用于避免网络设备的CPU收到网络上不必要和具有恶意攻击目的的数据流,提高网络设备自身安全性能,还可以通过设置QoS过滤机制来保护网络设备的控制平台(Control Plane ,简称CP)在遭受攻击和高负载的情况下仍能保持数据转发和协议状态的稳定。



● 防ARP欺骗

锐捷交换机提供DAI和ARP-Check两种防ARP欺骗的功能。

动态分配IP:该模式下,用户会和DHCP 服务器交互DHCP 报文,从而获取IP 地址。于是交换机通过会探测用户的DHCP 报文,记录用户的IP 和MAC,形成IP+MAC 的绑定表,然后对接收到的ARP 报文进行安全性检查(ARP-Check),对不符合绑定表的ARP 报文采取丢弃措施,从而解决ARP 欺骗问题。

静态分配IP:要防ARP 欺骗,需要首先绑定用户的IP 和MAC。那在该模式下,交换机如何才能知道正确的IP 和MAC 呢? 需要第三方告诉交换机正确的IP 和MAC,之后再形成IP+MAC 的绑定表,然后对接收到的ARP 报文进行安全性检查(ARP-Check),对不符合绑定表的ARP 报文采取丢弃措施,从而解决ARP 欺骗问题。

4.2.3 资源有限、精细管理

由于金融网点的互联网访问数据需通过三级网和二级骨干网访问位于一级分支机构的代理服务器，因此网点到二级分支机构的三级网、二级分支机构到省网络中心的二级骨干网流量将增大，因此需要对带宽进行必要的扩充和控制，有两种方法，第一：可以考虑增加专业的流量管理工具来对上网行为进行严格的带宽控制；第二、可以通过上网代理服务器，关闭相应的服务端口，然后借助网络设备的QOS能力，保证有限的线路资源下最大的业务应用。对具体实施方法如下文所述。

三级接入网带宽考虑

对银行用户来说，考虑到网点网银自助服务机访问网站有限，且IE浏览器本身存在缓存机制，每个终端考虑提供60K的访问带宽，每个网点设计4台终端，需要增加240K的实际流量。

对保险用户来说，统一核保核赔业务集中上收省公司，增加了大量的图片信息的传输，鉴于网点的PC数量也相对较少，除生产、OA业务以外，仅浏览网页信息而言，每终端60K的流量也基本能满足需求。

综合上述，初步预计，金融网点使用2M线路基本能满足要求。

增加二级骨干网的带宽

由于下级机构需要访问位于省一级网络中心的代理服务器，这个数据流和内网其他业务数据流带宽占用方向一致，因此需要进一步确定每个用户数和访问特性，对二级骨干网线路进行一定的扩容。建议给每个二级机构至少增加2M的带宽。

Qos设计

相比内网核心业务来言，访问互联网的应用需求应为最低，即可将访问数据流配置到最低优先级的default的队列中，以避免在网络发生拥塞情况下对其他高优先级业务的影响。

4.2.4 统一规划、严格控制

信任站点管理

设置非信任站点列表，根据企业内部的管理规定，定义禁止访问的站点域名或IP地址，尤其是色情网站。

设置信任站点列表，根据企业内部的管理规定，对OA用户需通过Internet进行业务处理需要访问的站点列表。各科室、部门用户的需求不一样，可能有多个信任站点列表。

上网用户规划管理

上网代理服务器通过配置防火墙策略实现对内部用户访问外网的控制。部分企业采用的Windows AD的方式进行应用层面的准入管理，这样可以根据客户端的IP地址和用户认证来作为策略匹配条件，将用户进行分组，指定组成员，并最终确定这些用户都有什么样的上网权限。

上网机器规划管理

坚决避免上和Internet有连接的机器同时上内网生产网络。

- 银行网点的网上银行自助终端。可以访问相应的信任站点。
- 专用Internet机器，为了降低安全风险，建议主要采用此模式。可以访问除非信任站点的所有站点。
- 需要通过Internet进行业务操作的OA机器。可以访问相应的信任站点。

上网行为管理

上网行为控制管理至少要满足如下的要求：

- 屏蔽网络中存在着大量的P2P软件(如BT、迅雷等)，保障互联网访问业务的顺利进行；
- 控制网络中充斥的大量病毒，屏蔽病毒在网络大量传播、发包，造成网络的中断，有效阻止互联网的病毒带入内网；
- 保障业务数据的保密性，通过内部网外发信息进行审计(包括POST审计和邮件审计)，保证企业内部信息外发的安全；
- 屏蔽网络娱乐功能：通过对网络游戏和网络电视等带宽控制和屏蔽，一方面保护二、三级网络的带宽，另外一方面提高可以员工的工作效率。