Industry 锐捷网络解决方案 SOLUTIONS

锐捷网络

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								

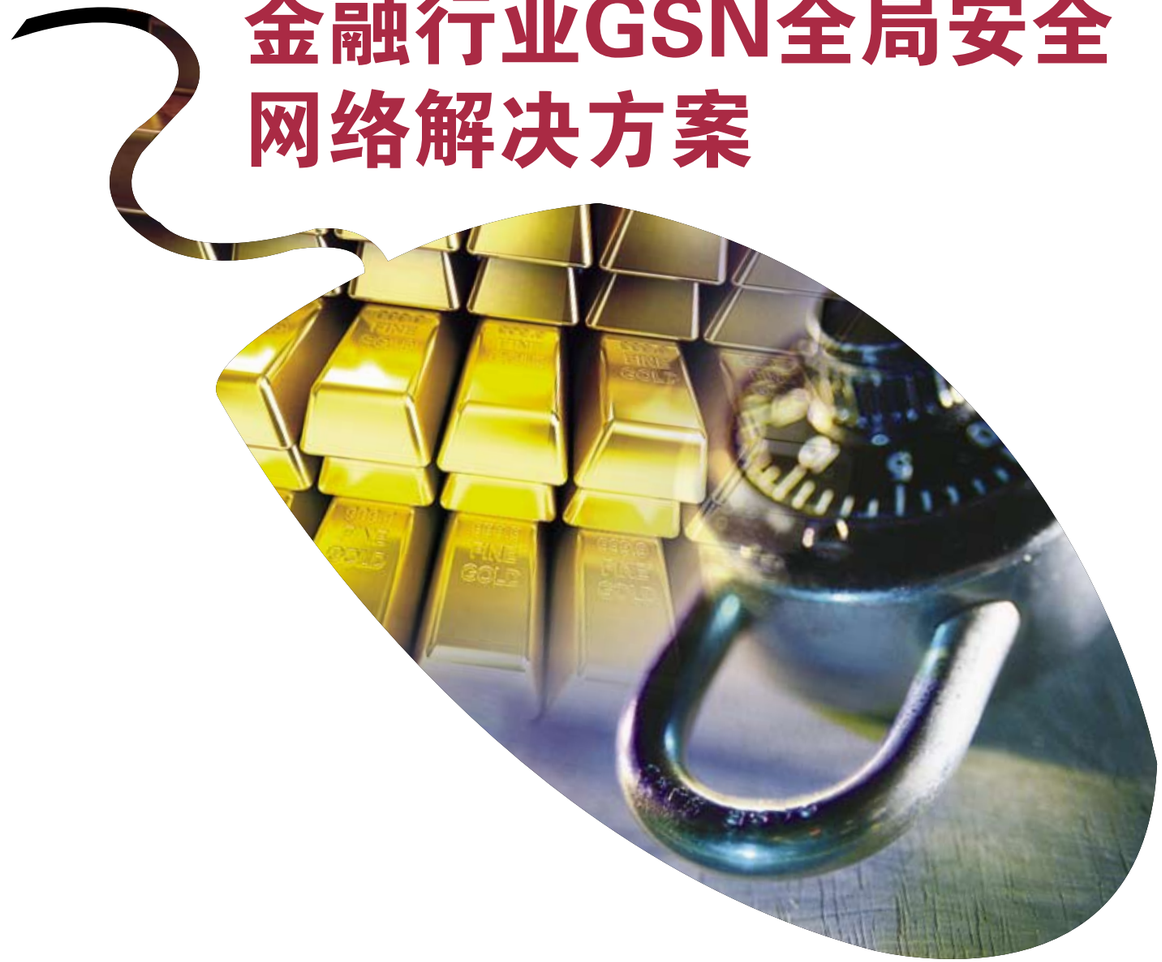
如需了解更多产品信息，请浏览 http://www.ruijie.com.cn

Industry 锐捷网络解决方案 SOLUTIONS

锐捷网络

解决方案

金融行业GSN全局安全网络解决方案



www.ruijie.com.cn

1. 背景分析

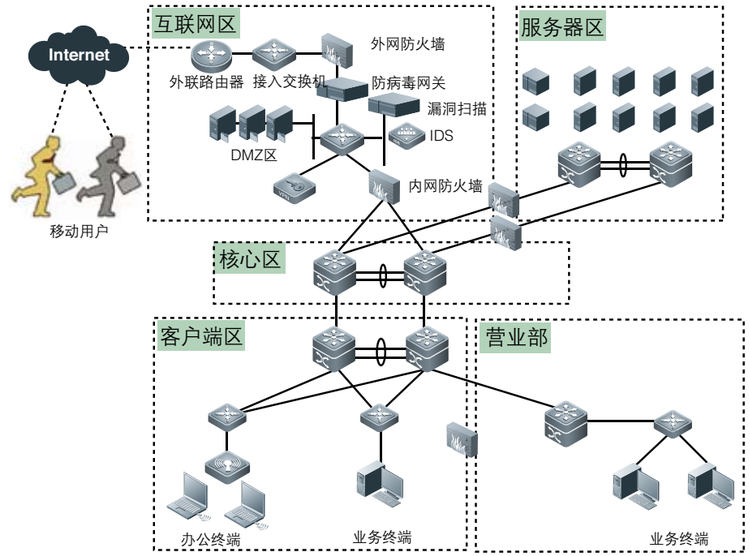
网络安全在金融企业的网络建设中，向来是设计方案中的一个最优先考虑的方面。无论是全国数据中心、广域网，还是一个分支机构局域网的建设，都需要依照网络安全规范进行。

近年来，随着业务量的不断增长和新兴业务的持续涌现，金融企业网络内部的应用行为愈加趋向复杂。同时，随着网络安全形式的日趋严峻，层出不穷、频频变种的病毒、木马、恶意攻击，让网络管理者们意识到了网络安全的重要性。根据业界主流防病毒厂商实验室的统计数据，过去的2008 年是有史以来安全事件最为严重的一年。根据IDC 提供的统计数据，超过70%的安全事件，起因都是来自于局域网的内部。如ARP 欺骗、熊猫烧香、机器狗、灰鸽子等我们或耳熟能详、或深受其害的病毒或木马，都是在局域网内部进行传播、扩散，给金融企业的正常运转带来极大的危害。

经典的金融企业网络采用安全级别划分和功能区域划分结合的方式。采用防火墙、交换机ACL 等方式进行安全隔离和访问控制。同时，结合如入侵检测系统、防毒墙等专有安全产品进行网络应用安全的监控。而针对终端管理，采用相应的终端/桌面管理软件实现。各个金融行业企业在网络安全建设方面，投入大量的精力和资金，在各级机构部署了大量相应的设备，采取了控制的措施。然而，从安全控制的力度、管理的统一和便捷、再到实施的效果，并不能让金融企业的网络管理者们满意，局域网内部的安全问题一直无法得到有效的控制。

2. 现状分析

金融行业企业网络中，各种新兴业务系统的上线，以及Internet 出口的设置，让金融企业的网络行为趋向复杂。近年来，病毒、木马和恶意软件通过包括网络在内的各种介质迅速扩散，涉及经济利益的网络犯罪行为的愈演愈烈，也让网络的安全压力加大。面临多重压力的网络中，亟待解决的主要是以下各类问题：



金融行业企业网络典型组成

2.1 缺乏有效的网络准入机制和访问授权

在办公区、测试区等存在客户端PC 接入的网络中，没有对入网的用户采取准入控制。任何PC 随时可以接入到网络中，使网络和业务面临重大风险。现有办公区的网络的业务日趋复杂，各类客户端PC 之间没有访问控制，如普通办公类客户端PC 在接入网络后也可以访问管理类、财务类服务器等。部分企业采用的Windows AD 的方式进行应用层面的准入管理，但在网络层面缺乏相应机制，用户即使不通过AD 认证，也可以接入内部网络，给网络安全带来了隐患。

2.2 主机安全的实现困难

为了保证信息安全，金融企业大多采购并要求员工在客户端PC 上安装防病毒软件和个人防火墙等安全工具，同时也搭建了Windows 更新服务器等用于操作系统升级。但由于缺乏相应的控制机制，所以经常会出现客户端PC 不按照要求进行必要软件安装或者操作系统升级的情况。同时，部分客户端PC 上安装企业命令禁止的软件如游戏软件，甚至私自设置与外网的拨号连接，严重威胁了金融企业的网络安全。

2.3 安全事件处理效能低下

众多专业的安全设备，如防火墙、入侵检测系统、入侵防御系统、防毒墙等等，大多部署在核心或出口等部分，且均为独立发挥各自作用。检测到应用层的安全事件后，也只能从设备本身进行阻断等操作，很难快速定位或隔离存在问题的客户端PC。加上“高高在上”的部署位置，导致区域内部的网络安全形势依然十分严峻，部分病毒木马表现出的网络层面的行为，如ARP 欺骗或DDoS（ 分布式拒绝服务 ）攻击等，即使在安全设备采取了阻断措施，但由于其控制力度有限，仍然会对网络的稳定和信息安全造成重大威胁。同时管理员也要管理大量的异构的设备，直接影响了解决问题的效率。

3. 需求分析

综合金融行业网络现状，分析目前在金融行业企业中，存在的突出的需求有以下三点：

实现网络准入和访问授权 – 基于网络硬件的准入控制，能够采用多种的绑定方式，做到最为严格的入网身份管理。同时还需要实现对不同类别接入用户对网络访问权限的控制。

主机安全管理 – 按照企业规定，操作系统的补丁更新、防病毒软件的更新、软件黑白名单控制以及主机硬件接口的控制等，都需要进行相应的管理和控制。

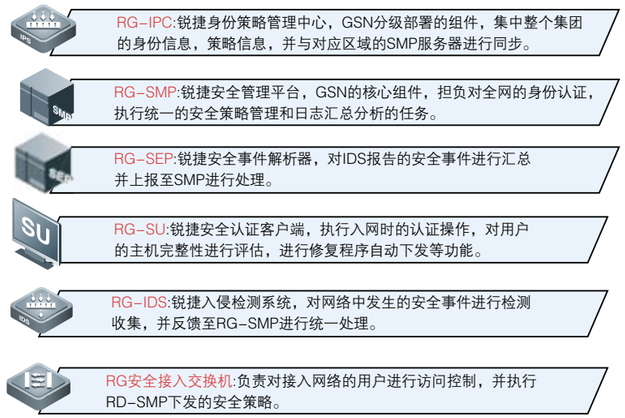
网络实时通信防护 – 解决安全事件发现、定位、处理效率低下的问题，将管理员的工作从繁冗的“亡羊补牢”改进为“未雨绸缪”。

4. 解决方案概述

网络访问控制（ NAC Network Access Control ）通过身份验证、主机健康性保障、网络安全性保障等多重角度，对内网用户进行有效的管理。通过这一系列措施，实现内网用户身份的合法化，上网主机安全状况的健康化，网络通信的安全化以及用户网络访问行为的规范化。即：让正确的人，使用健康的主机，访问安全的网络，做规范的事。

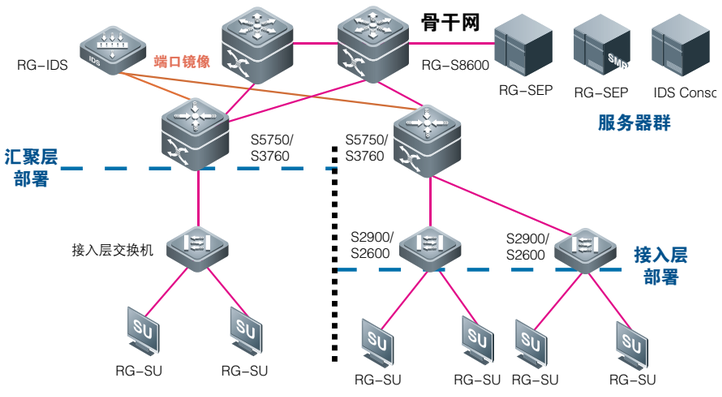
锐捷网络GSN（ Global Security Network ）全局安全网络解决方案是针对以上各个需求，定位于NAC 领域，旨在帮助用户建设全面安全的网络解决方案。

锐捷网络GSN 全局安全解决方案，融合软硬件于一体，通过软件与硬件的联动、计算机领域与网络领域的结合，帮助用户实现全局安全。GSN 是一套由软件和硬件联动的解决方案，它由后台的管理系统、网络接入设备、入侵检测设备以及安全客户端共同构成。



GSN 的组成

锐捷网络GSN 的部署，可以采用“接入层部署”和“汇聚层部署”两种方式，同时还可以支持分级部署。



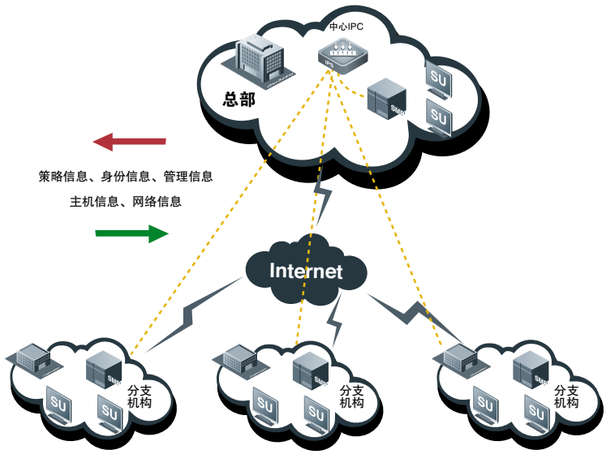
GSN 的两种部署模式

接入层部署方式，将GSN 组件之一的安全接入交换机部署在网络的最接近PC 终端的边缘，即在接入层的安全智能交换机(如锐捷S2600/S2900)上进行身份认证，将安全管理控制到网络边缘，这种部署模式的好处在于，认证设备处于网络边缘，能够控制的粒度最细，对用户端的管理权限最强。还可以采用汇聚层部署方式，将安全接入交换机或汇聚交换机部署于汇聚层，这种部署方式对网络改造要求低。

对拥有众多分支机构、具有垂直管理结构的金融企业需要统一管理的单位，其分支机构众多，且分布于不同的地理位置，与上一级机构之间的物理线路也大多采用运营商专线实现。

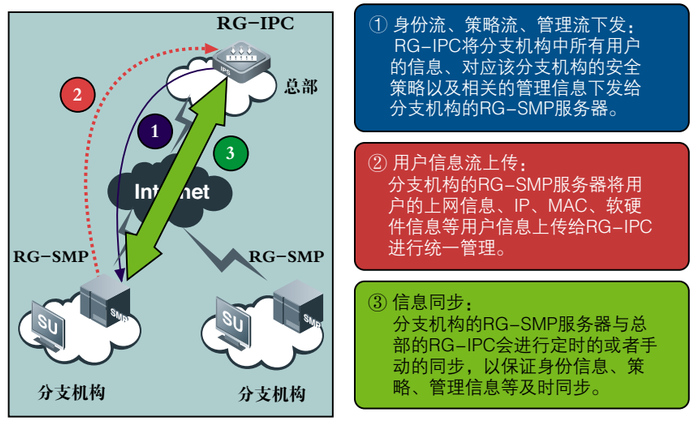
GSN 的分布式部署、集中管理的部署模式，就是顺应这种需求而推出的。通过在总部部署RG-IPC 身份策略管理中心，在分支机构部署RG-SMP 安全管理平台，实现了整个企业统一策略、集中管理、分布式部署的整体安全架构。

针对金融企业分级的机构组成方式，如银行“总行 – 分行 – 支行/网点”，以及保险的“总公司 – 省分公司 – 市/县分公司”的情况，可采用分布式部署模式，进行统一的身份认证和策略部署。拓扑如下图所示：



GSN 的分布式部署方式

在管理中心，管理员可以通过RG-IPC 方便的为整个企业或者辖内网络制定统一的或者个性化的安全策略，然后将这些信息发送到对应的分支机构的RG-SMP 服务器中以执行，同时将整个企业/辖内的用户信息、主机信息加以收集、整理，从而在管理中心形成一个完整的用户信息、主机信息以及对应安全策略的数据库。



分布式部署的模式

在分支机构，RG-SMP 安全管理平台将RG-IPC 下发的安全策略在本地执行，负责用户的身份、主机、网络等多层面的安全管理，同时将本地的用户信息和更新与总部的RG-IPC进行同步，以保证RG-IPC 服务器中的数据的准确性。

同时，为了减轻总部管理人员的管理工作量，可以通过RG-IPC 给分支机构的RG-SMP下放管理权限，让分支机构的管理员实现本地管理，同时将分支机构自己制定的安全策略与总部同步。

通过分布式部署，GSN 解决方案实现了总部对不在同一地理位置的分支机构的统一管理，由于优质算法的采用，使得分支机构RG-SMP 与总部RG-IPC 服务器之间的同步数据量非常小，并有多种机制保障数据的完整性，所以GSN 的分布式部署对总部到分支机构之间的线路要求很低，即使是ADSL 也能达到要求。这种部署方式，能够很好的适应金融行业企业现有网络管理对带宽经济性的需要。

5. 功能简介

针对金融行业网络里面存在的三大类问题，GSN 全局安全网络解决方案可以帮助客户实现从用户身份管理、主机管理到网络通信管理等多方面的功能，解决这些问题。

5.1 身份管理体系

GSN采用了基于802.1X协议和Radius协议的身份验证体系，通过与安全智能交换机的联动，实现对用户访问网络的身份的控制。通过严格的多元素(IP、MAC、硬盘ID、认证交换机IP、认证交换机端口、用户名、密码、数字证书)绑定措施，确保接入用户身份的合法性。通过对用户计算机ID(硬盘序列号)的绑定功能，灵活的实现用户、主机、网络位置三个元素的自由绑定，GSN采用了基于802.1X协议和Radius协议的身份验证体系，通过与安全智能交换机的联动，实现对用户访问网络的身份的控制。通过严格的多元素(IP、MAC、硬盘ID、认证交换机IP、认证交换机端口、用户名、密码、数字证书)绑定措施，确保接入用户身份的合法性。通过对用户计算机ID(硬盘序列号)的绑定功能，灵活的实现用户、主机、网络位置三个元素的自由绑定。例如在金融企业办公区或测试区存在固定主机(网络位置固定，多用户使用)、个人流动主机(单用户，网络位置变化)、个人固定主机(网络位置固定，单用户)等多种PC管理模式，多种绑定措施方便针对不同的功能分区的不同终端PC实施定制化的准入策略。而通过数字证书的认证，将进一步提高账号管理的便捷性和入网的安全性。

在办公区存在不同的业务终端PC，需要区分其访问权限的情况下，GSN 可以依照用户身份，限制不同用户的访问权限，让用户在接入网络后，只能访问自己权限之内的服务器，网络区域等。

GSN 的访问权限限制

5.2 防非法外联

非法外联将会严重影响金融企业网络的完整性，给信息安全造成重大隐患。

GSN 通过锐捷安全认证客户端与SMP 系统的Syslog 组件联动，实现对内网主机连接互联网行为的日志记录，将用户的用户名、IP 地址、MAC 地址，用户主机的硬盘序列号等多项内容全部记录下来，可以精确的定位到是哪个用户、哪个主机在进行互联网的访问，让用户对于非法外连行为无法抵赖。

5-20-2009	16:33:05	User,Critical	172.16.8.128	May 20 16:32:53 172.16.8.128 SuService:IP=172.16.8.128;Mac=00:16:d3:20:a1:c2;HDSerial=WD-WXNY08N50232;UserName=zhangsan;Time=20 16:32:53
5-20-2009	16:33:00	User,Critical	172.16.8.128	May 20 16:32:48 172.16.8.128 SuService:IP=172.16.8.128;Mac=00:16:d3:20:a1:c2;HDSerial=WD-WXNY08N50232;UserName=zhangsan;Time=20 16:32:48
5-20-2009	16:32:54	User,Critical	172.16.8.128	May 20 16:32:43 172.16.8.128

GSN 的用户非法外联Syslog 记录

针对常见的采用Modem 进行拨号外联上网的方式，GSN 解决方案提供了相应的监控和处理功能。用户在进行拨号操作时，GSN 会将其内网连接断开，并向用户提出警告，同时也会干预用户的拨号过程，使拨号失败。

安装双网卡也是一种常见的外联上网实现方式，如有用户采用有线网络接入办公网，又采用无线网络连接到互联网，这样就打通了内网和外网。GSN 提供对双网卡用户的限制功能，一旦两块网卡都产生网络流量，则会对用户进行警告，并切断内网连接，保护内网安全。

运行代理服务器方式较为隐蔽，不容易被发现和定位。GSN 通过客户端对客户端PC运行进程的检查，能够立即定位代理服务器进程，对用户进行警告并采取断网等相关措施。

5.3 软件黑白名单控制

企业要求必备的软件如防病毒软件，以及不允许安装的软件如游戏软件等，其管理措施可以通过GSN 的软件黑白名单控制功能实现。GSN 的黑白名单功能可提供基于多个层面的检测和控制。

软件安装监控 – GSN 可对系统已安装的软件情况进行监控，获取系统已安装的软件列表，然后根据软件列表检测用户是否已经安装了违禁的软件，即可进行相应的处理。

系统进程监控 – 有些软件如“绿色版本”的软件在安装之后，在“添加或删除程序”项中并不会出现，GSN 采用系统进程监控的方式对其进行监控，当其运行时，相关进程就会出现在进程管理器中，如果监控到对应的进程，则说明违禁软件正在运行，可进行处理。

注册表监控 – 软件运行或者安装，都会向Windows 的注册表中写入键值，病毒也如此(病毒、木马本身也是一种软件)，GSN 通过检测注册表中对应的键值，可以对软件进行监控和处理。

后台服务监控 – 一些软件是以Windows 的后台服务的方式运行的，在进程管理器中也找不到它，但事实上它是在运行的，诸如一些病毒或木马，还有大部分的杀毒软件也是以这种方式运行的，那么通过对系统服务的监控，也能对软件的使用进行限制。

通过对软件安装情况、进程运行情况、注册表修改情况以及后台服务运行情况的监控，可以对软件的安装和使用情况有一个详细的了解。同时，可依照企业的相关规定进行处理。例如禁止运行聊天软件，就可以对聊天软件进行检测，如果检测到聊天软件，则对用户进行提醒或者处理如禁止其上网，直到客户端PC 卸载或关闭聊天软件等。

5.4 操作系统补丁/软件强制更新

不安装补丁的操作系统很可能成为网络安全的漏洞，而未及时安装补丁的软件也可能成为别有用心的人发动攻击的一个平台。

防病毒软件作为客户端PC 的重要的安全保障，对网络安全和主机信息安全起到重要的保护作用。而某些重要的应用软件，如Microsoft Office，SQL-Server 等软件，也是日常业务中的重要组件。

由于安全问题的不断涌现，防病毒软件的杀毒引擎和病毒库的及时更新就显得十分重要。不定期发布的重要应用软件的补丁，也会对业务系统乃至整个网络的正常运行起到关键的作用。如SQL Server 软件不安装Service-Pack 的情况下，很可能招致严重的蠕虫病毒攻击。

针对防病毒软件和其它重要业务软件的更新，GSN 系统采用基于软件黑白名单机制和客户端PC 修复、隔离机制共同实现。目前GSN 针对业界主流的十多种防病毒软件进行联动检测，支持对防病毒软件的安装/运行状态、病毒库版本和引擎版本信息进行检测。

杀毒软件名称	联动方式	检查项		检查限制		启用	操作
江民2008及其以后的版本	强联动	杀毒引擎	不检查			☑	修改
		病毒库	检查	自适应顺延天数	7		
江民杀毒软件KV2007	弱联动	杀毒引擎	不检查			☑	修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基反病毒软件6.0	弱联动	杀毒引擎	不支持			☑	修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基互联网安全套装6.0个人版	弱联动	杀毒引擎	不支持			☑	修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基反病毒7.0个人版	弱联动	杀毒引擎	不支持			☐	修改
		病毒库	检查	自适应顺延天数	7		
卡巴斯基反病毒7.0网络安全版	弱联动	杀毒引擎	不支持			☐	修改
		病毒库	检查	自适应顺延天数	7		
Symantec AntiVirus企业版 8	弱联动	杀毒引擎	不检查			☐	修改

防病毒软件联动配置界面

GSN 已经支持与以下厂商的防病毒系统进行联动。进行病毒库和杀毒引擎的检查和自动更新。

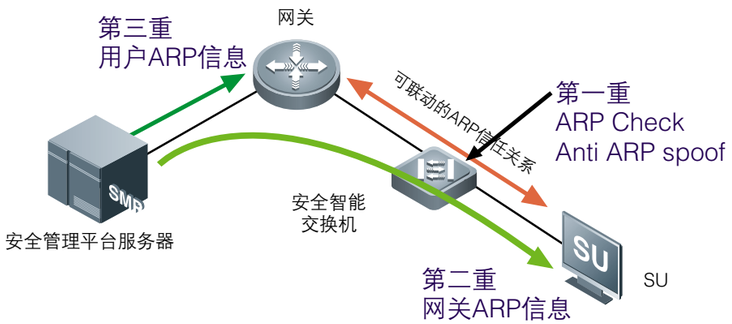
GSN 的合作防病毒软件厂商

针对统一的重要软件更新包下发，可采用GSN 的服务器主动推送的方式进行。此措施可针对所有或某一组、某一个在线的客户端PC 进行，统一下发更新包。而离线的客户端PC 将在上线之后收到更新包。可要求客户端PC 必须打上指定补丁后才能够入网。

针对特定软件的版本检测和补丁检测，可通过软件黑白名单控制中的注册表检测实现。可针对不同软件制定不同的检测策略或检测策略组。如针对Microsoft Office 软件，可建立针对Office 软件的更新检测策略组，里面包括针对Word/Excel 等组件的分别的检测策略。在遇到客户端PC 出现不符合策略组要求的情况，可根据策略组要求对客户端PC 进行修复或隔离。

5.5 ARP 欺骗的防护

面对在金融等行业的局域网络中时常出现的ARP 欺骗，GSN 能够通过三层网关设备、安全智能交换机以及客户端Su 软件的联动，实现了对ARP 欺骗的三重立体防御。



GSN 的三重防护体系彻底防止ARP 欺骗

采用锐捷网络的可信任ARP(Trusted ARP)专利技术，实现三层网关设备和客户端PC 之间的联动的可信任的ARP 关系，从而保证了用户与网关通信的正常。

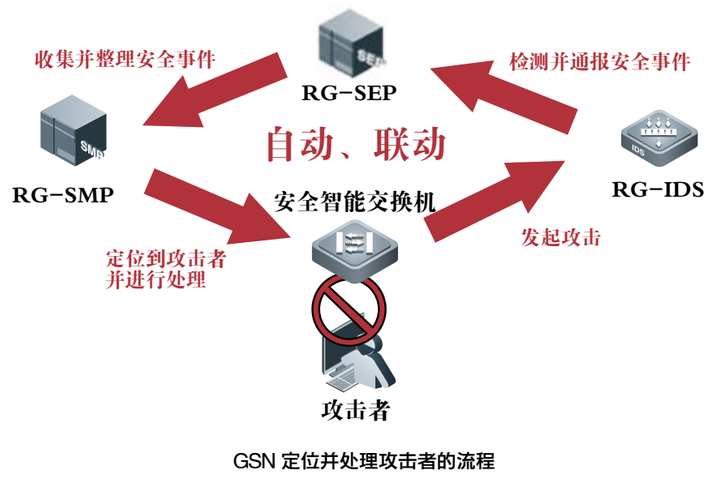
在安全智能交换机上结合用户认证信息，则能够实现基于端口的ARP 报文合法性检查，基于深度检测的硬件访问控制列表，将所有ARP 欺骗报文全部过滤，从而彻底阻止了ARP 欺骗的发生。

5.6 联动的网络安全事件处理

入侵检测系统IDS 可以监控网络中流量的情况，并针对异常的流量发起预警。IDS 汇报上来的信息包含源、目的IP，但这些信息对网络管理人员处理安全事件来说，并没有太大的意义。因为处理网络安全事件一定要追根溯源，定位到机器甚至定位到人，才能彻底解决，仅仅提供IP 地址这是不够的。GSN 体系中的安全事件联动解决了这个问题。IDS 作为网络通信的探针，对网络的流量进行旁路兼听，并随时向安全策略平台SMP 上报发生的安全事件通过对IDS 上报的安全事件的解析，并通过GSN 体系中每个用户的信息来将安全事件定位到人，并根据IDS 与GSN 共享的事件库，对安全事件给出建议的处理方法，或者可以通过预先定制好的策略来对

安全事件进行自动的处理，这就解决了在IDS 检测到安全事件后，处理难的问题。

通过RG-SMP 安全管理平台、RG-IDS 入侵检测设备、安全智能交换机和Su 客户端的联动，实现了对网络安全事件的检测、分析、处理一条龙服务。基于严格的身份验证，可以方便的将网络安全事件定位到人，并自动通知和处理。



GSN 定位并处理攻击者的流程

1. 攻击者发起攻击；

2. IDS 设备通过对网络流量的监控捕获到攻击流量，并根据内置事件库分析攻击的类型，通过RG-SEP上报给RG-SMP；

3. RG-SMP 服务器收到上报的信息后，与内置的用户数据库进行比对，得到攻击者和被攻击者的相关信息，如IP、MAC、用户名、所在交换机及对应端口等信息。

4. RG-SMP 服务器根据攻击对应的自动处理策略或者手动处理，对攻击者和被攻击者进行处理策略下发到交换机，如隔离、警告、下发修复程序等。

5. 交换机根据RG-SMP 服务器发出的指令，对用户进行网络层面的处理，如将用户隔离至安全区域，或者完全中断用户的网络访问。

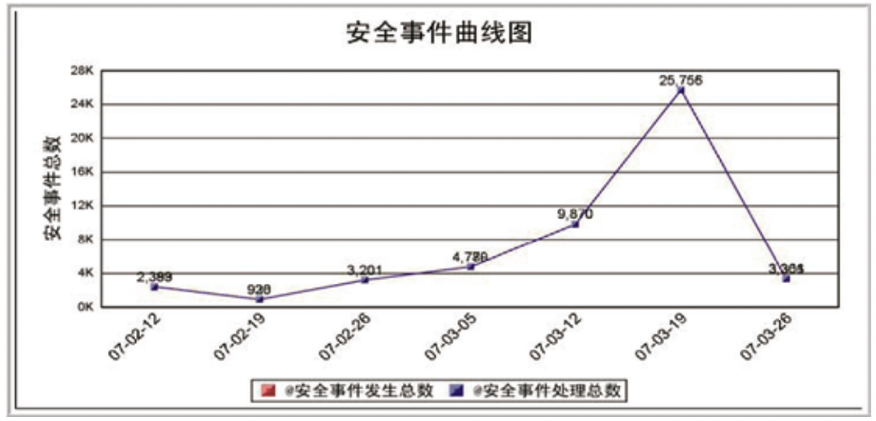
6. SMP 服务器可同时将警告消息、修复程序等直接下发给用户，指导用户对非法行为进行改正、或补全漏洞避免被攻击。

7. 用户在进行修复等处理后，重新检测安全状态，符合要求后重新正常上网。

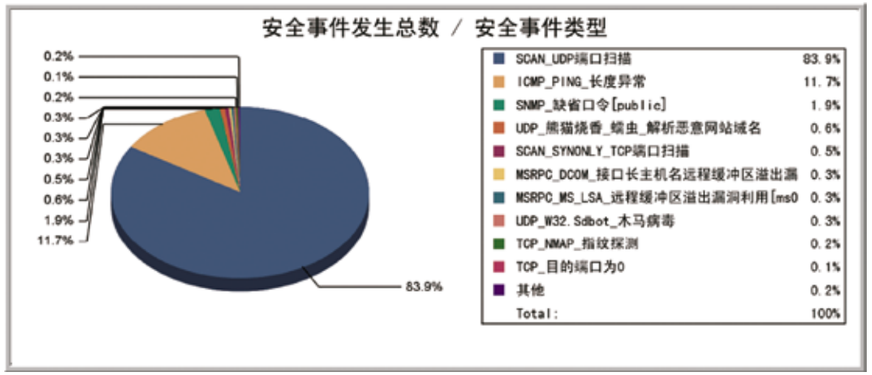
锐捷IDS 将会以星期为单位，进行安全事件库的更新，能够跟踪定位最新的网络安全事件。针对不同行业的定制事件策略库的做法，也极大的降低了IDS 误报的可能。

GSN 针对安全事件的处理方式可以定制，管理员可在综合评估网内安全形势的情况下，对不同等级的安全事件做出不同程度的处理。如普通的ICMP 扫描采用向客户端PC 下发警告信息，而蠕虫病毒攻击则采用警告消息、下发修复软件和隔离的综合手段。

在防御的同时，还能够对安全事件进行统计分析，为日后的安全报表做好准备。



安全事件曲线图



安全事件统计图

锐捷网络GSN 全局安全解决方案中，通过传统的入侵检测设备IDS 与后台服务系统、客户端、交换机等软硬件的联动，有效的实现了网络通信系统主动、自动、联动的保护。整个检测、分析、处理过程由软硬件联动实现，无需网络管理人员的过多干预，有效帮助用户实现“无人值守”全局安全网络。

5.7 方案总结

针对金融行业网络关注的三个焦点问题，GSN 全局安全解决方案通过软硬件的联动、计算机层面与网络层面的结合，从身份、主机、网络等多个角度对网络安全进行监控、检测、防御和处理，帮助用户共同构建身份合法、主机健康、网络安全、行为规范的全局安全网络。同时通过分布式部署、集中管理的部署模式，帮助拥有众多分支机构的金融行业企业方便的进行分级别的统一管理。