SG-8000 深度安全网关

技术白皮书

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京安博通科技有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京安博通科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目 录

1 产品概述

安博通深度安全网关 SG-8000 系列（以下简称 SG-8000）采用先进的高性能多核架构，运行自主可控的操作系统，搭载接口丰富的硬件平台，结合智能路由等全面的网络层支撑以及双机热备，保障业务处理高效可靠，场景支撑灵活全面；配备 WAF 级别的入侵防御功能和独特实时病毒拦截技术的病毒防护功能，通过单路径并行处理的安全检测引擎和应用识别，实现对用户、应用和内容的深入分析，为用户提供安全智能的一体化防护体系。

2 产品价值

2.1 灵活高效全面，场景支持更丰富

SG-8000 搭载自主可控的 SPOS 防火墙系统，融合了丰富的网络特性，在满足 IPv4/IPv6 双协议栈的同时，配合智能路由和 DDNS 等，可在 802.1Q、RIP、OSPF 等各种复杂的网络环境中灵活组网；具备与第三方系统对接，数据共享，提升业务价值。SG-8000 产品具备优秀的适应性，适用各种复杂场景，更符合业务需要。

领先的多核架构及分布式搜索检测引擎，配合高性能的处理器，多业务并行处理，确保 SG-8000 在各种大流量、复杂应用的环境下，仍能具备快速高效的业务处理和防护能力。

SG-8000 产品集防火墙、负载均衡、入侵防御、病毒防护、应用过滤、行为控制、VPN 接入、业务可视、安全认证等功能于一体，为用户提供了一个灵活、高效、全面的网络解决方案。

2.2 病毒实时分析，立体防护更安全

随着互联网的普及，网络的资源共享进一步加强，信息安全问题日益突出。黑客们可以轻易地通过拒绝访问，攻击企业网络，使其瘫痪；木马、病毒等恶意软件也经常通过邮件、恶意的 Web 网页、文档下载等应用层途径使得病毒的危害范围和扩散速度加大。SG-8000 具备超过 3000 种预定义攻击特征的 WAF 级入侵防御功能和海量病毒特征独特实时病毒拦截技术以及高效引擎的病毒防护功能，实时的对流量进行分析，从数据链路层到应用层有效的阻断网络中的攻击和病毒行为。全方位的立体保护用户的关键数据，避免机密文件泄露和经济损失。

2.3 数据深度识别，行为管控更细致

员工上班时间进行业务无关的行为无疑会降低职工的办公效率，如果不慎发表不正当言论，将会给企业单位带来舆论风险，对形象声誉造成负面影响。SG-8000 产品采用 DPI/DFI 融合识别技术，通过对用户流量进行全面的分析，能够深入识别应用的内置动作，例如针对微信可识别控制多达 12 种行为动作。使用 SG-8000 产品能够避免员工上网娱乐的同时，帮助企业单位及时拦截不良言论。通过应用精细化管理让网络更有序。

2.4 带宽优化管理，用户体验更迅速

企业单位的出口带宽有限，带宽使用情况的不清晰不准确，造成了带宽未能有效的利用起来，带宽资源白白的被浪费掉。SG-8000 能帮助组织管理者透彻了解组织当前、历史带宽资源使用情况，并据此制定带宽管理策略，验证策略有效性。不但可以在工作时间保障核心用户、核心业务所需带宽，限制无关业务对资源的占用，亦可以在带宽空闲时实现动态分配，以实现资源的充分利用，提升用户使用网络的体验。基于不同时间段、不同对象、不同应用的管道式流控，能有效保障用户的上网体验，保障网络的稳定性。

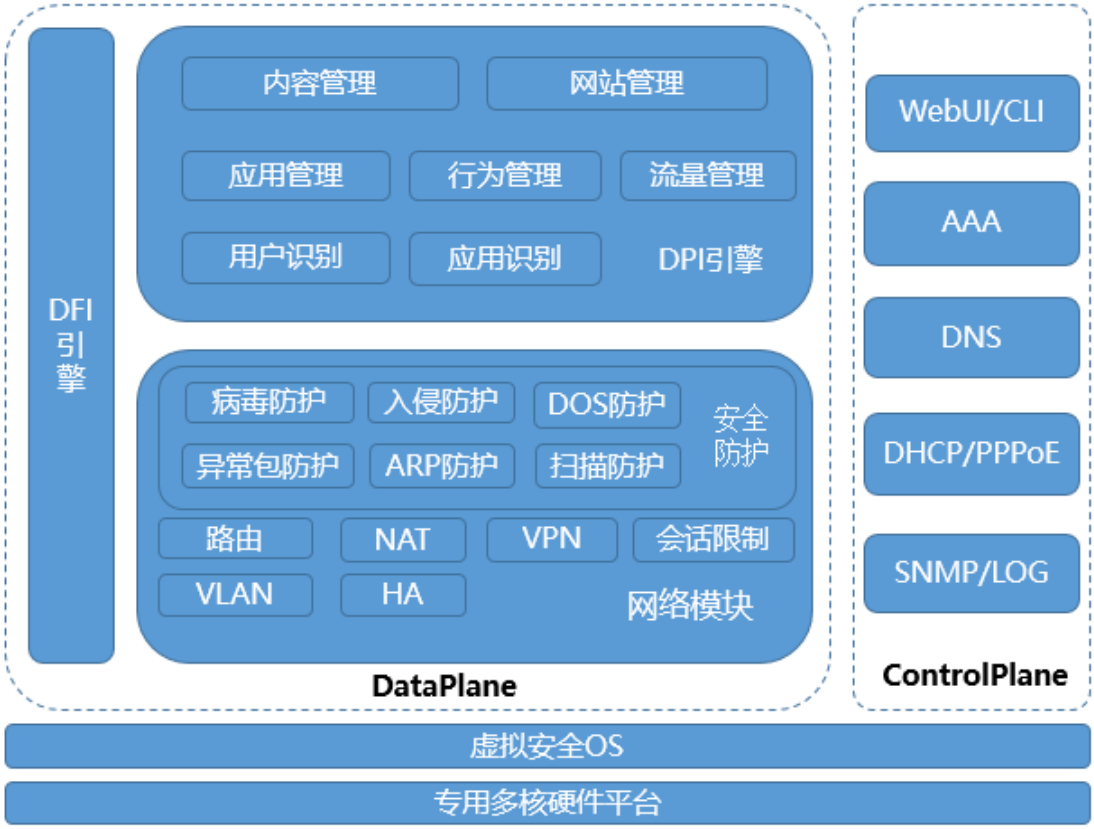
2.5 集中统一管控，网络运维更便捷

网络设备由于自身的专业性，非网络人员较难理解策略和日志的作用，日常管理和维护往往需要专业的网管人员；分支上线、分支业务变更，运维人员需要逐个分支进行配置，运维工作量大，周期较长。SG-8000 采用一体化安全策略，管理员只需要通过一条策略便可针对应用、URL、入侵防御、病毒查杀等内容进行统一管控，使用方便，维护简单。在大规模部署时，可配合安博通集中管理系统对分布部署的 SG-8000 进行零配置上线、统一策略管理、业务变更自学习、攻击事件监控、攻击事件分析、报表分析等。极大的降低了网络的更换难度，简化了运维的任务。

3 关键技术

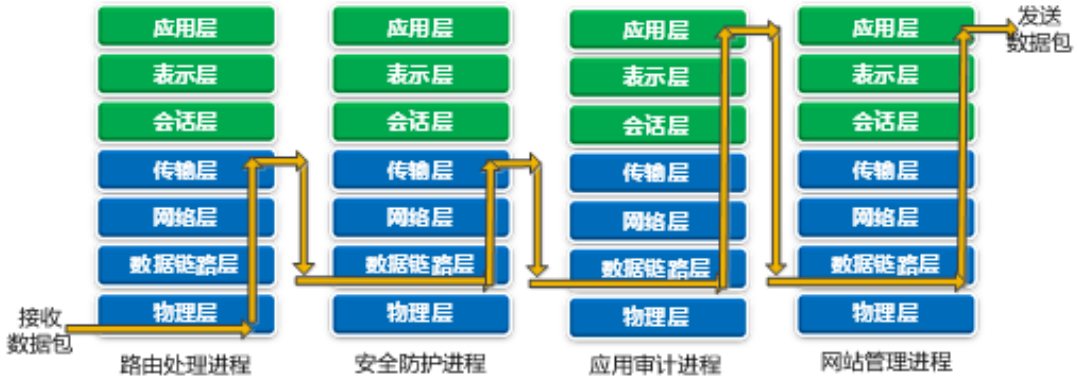
3.1 多业务并行架构

SG-8000 采用最新最先进的多核硬件架构，在硬件架构上运行自主知识产权的安全 OS，高效的并行调度算法和内存管理机制提高了流量转发报文的性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）6 和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统一部分 CPU 专职 CP 工作，大部分 CPU 专职 DP 工作。这样就避免了因系统调度，导致设备转发性能降级或者无法响应管理操作等现象。具体 DP 和 CP 的 CPU 分布根据用户场景定义。

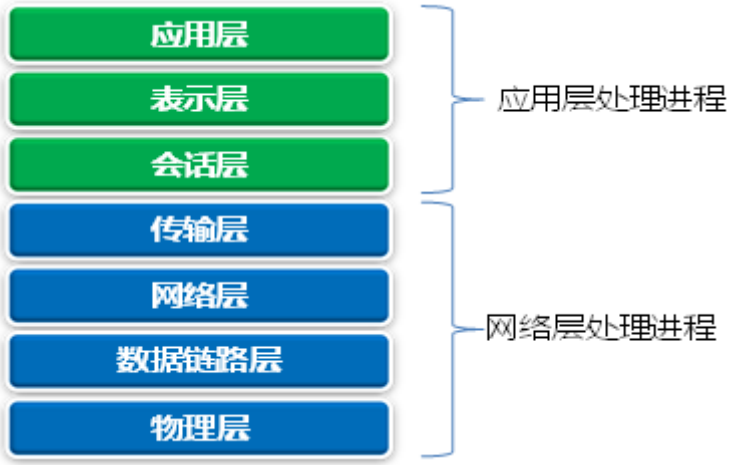


- 数据面

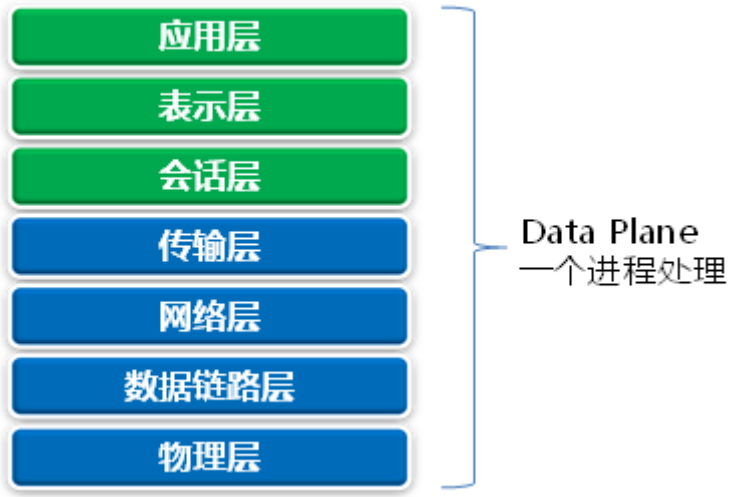
传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



有的设备则将网络层处理与应用处理分别在两个进程上实现，这样就出现了数据包多次拷贝的情况，增加了内存访问次数，降低了系统性能。



SG-8000 的 DP 主要处理转发相关的工作，通过对数据包一次解析，按层次由对应模块处理，可以节省不同模块间重启解析数据包所消耗的资源，从而降低网络延迟。



3.2 零拷贝技术

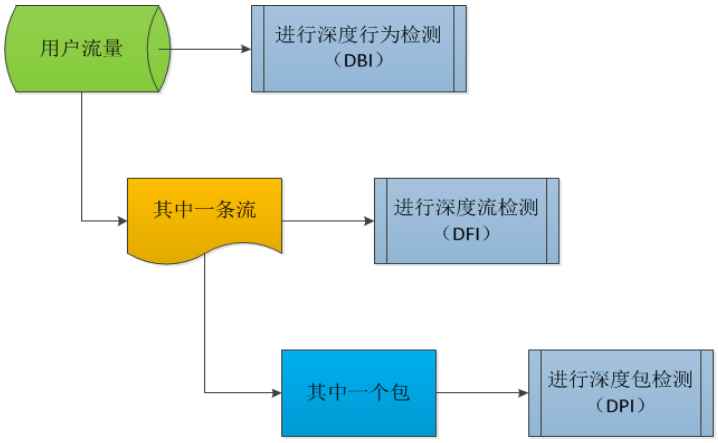
SG-8000 采用零拷贝技术，当数据包从网络设备到用户程序空间传递的过程中，减少数据拷贝次数，减少系统调用，提高 CPU 与内存的使用效率。实现零拷贝的最主要技术是 DMA

数据传输和内存区域映射技术。由于采用零拷贝抓包技术，极大减少了 CPU 的中断调用，显著提高了包处理效率，从而使整体性能有所提升。

3.3 应用识别

SG-8000 的应用识别具备传统的深度包检测（DPI）和深度流检测（DFI）两种技术，其中深度包检测（DPI）是基于特征库对数据包的 2~7 层数据内容进行指纹匹配，从而识别出流量对应的应用；深度流检测（DFI）则对同一数据流上多个数据包进行综合分析，通过该数据流的交互过程、报文关联特征、报文序列规则等分析识别流量对应的应用。

除此之外，SG-8000 还创造性地引入了深度行为检测（DBI）的新概念。通过对用户网络流量的统计分析，我们可以得出特定用户的流量模型，基于流量模型对用户行为进行匹配，真正做到万变不离其宗，有效识别未知应用，使得企业信息安全和网络资源得到最大限度的保障。



SG-8000 的应用识别引擎综合了以上三种深度检测技术，其技术特点包括以下几点：

- 用户流量模型：不同于以往的基于五元组的单流信息分析，真正基于用户的综合流量模型。
- 多维度流量统计：对每个用户的流量进行深度分析，及时发现高风险行为，保护企业信息安全；
- 应用协议自识别：通过对用户流量模型的分析，找出未知流量，根据其行为特征识别应用类型；
- 应用精细控制：在以往应用识别的基础上，更深入一步识别出应用的动作，允许管理员对用户行为进行精细化管控。

3.4 访问控制原理

SG-8000 在策略匹配方面采取了早发现早处理的机制。当数据包在匹配到策略后立刻处理，不会等到将全部流程跑完。同时，采用策略预匹配机制，策略不关注的数据流可以直接跳过处理流程。通过这些手段可以节约计算资源，减少数据包停留在设备内部的时间。降低网络延迟，提高网络吞吐能力。

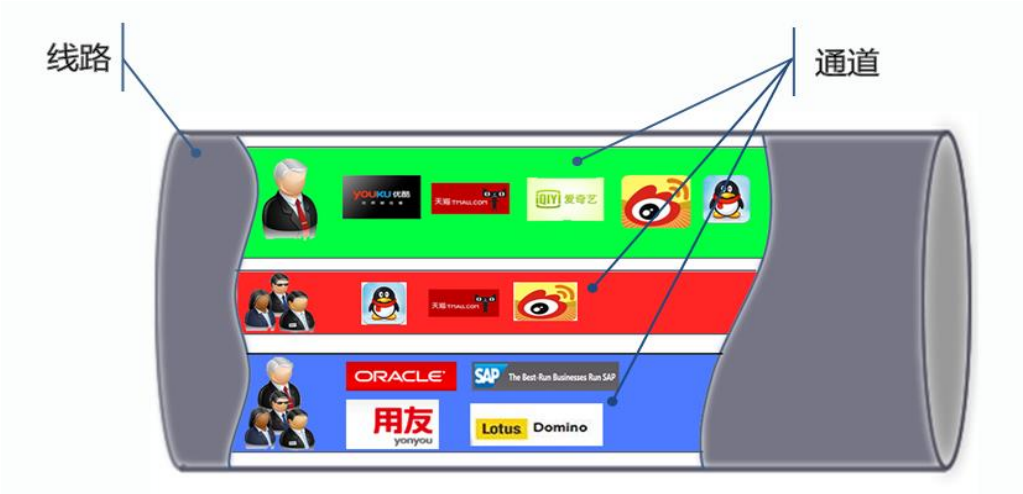
3.5 带宽管理特性

为了保障业务流转的通畅性、网络使用的正常性，SG-8000 在带宽管理方面较传统流控产品来说做了相应提高。

3.5.1 引入保障带宽和限制带宽，业务运行更通畅

保障带宽：从总带宽中划分出一部分带宽为某种指定流量独享。保障带宽可以保证即使在网络繁忙时，指定流量也能够独占保证带宽。当网络中没有指定流量时，保障带宽部分也能被其他网络流量使用。

下面是带宽管理示意图。绿色通道是 Boss 独享通道，使用应用不受限制；红色通道为员工通道使用非业务应用，该通道对带宽做了最大限制；蓝色通道为业务保障通道，公司的关键业务流量得到保障，其他的通道无法占用该通道的带宽。



3.5.2 引入弹性带宽管理，提供带宽利用率

弹性带宽管理，可以使空闲通道不占用大量带宽，减少带宽的浪费，减少因空闲通道占用带宽，流量达到极限出现丢包现象。弹性带宽就是为了解决带宽浪费的问题，空闲通道会自动让出部分带宽给繁忙的通道。一旦空闲通道带宽不足时，将自动抢占回借用出去的带宽。

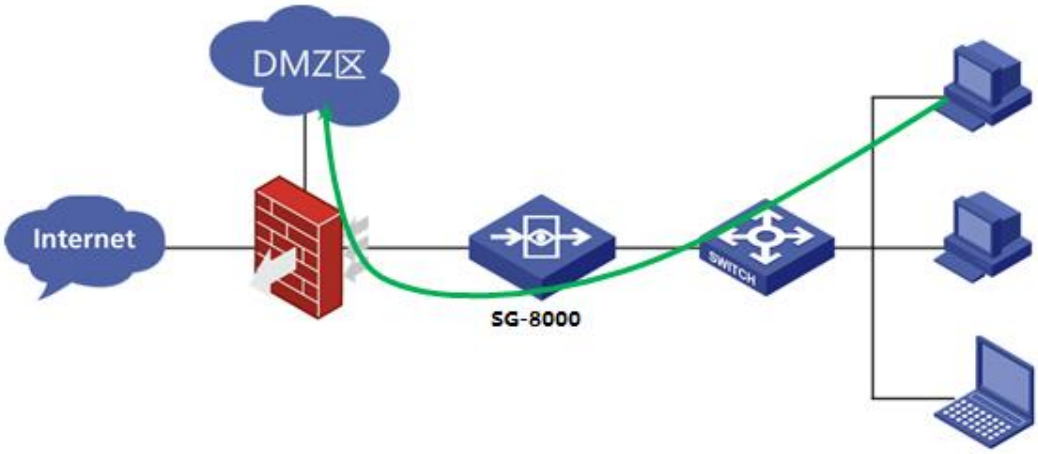
3.5.3 引入自动均分带宽，提升流量的可控性

SG-8000 采用了自动均分带宽，当在某个通道中只有一个用户使用时，该用户可以使用全部的带宽，如果有更多用户使用该通道时，带宽将按 IP 数量均分，提升用户上网体验。

3.5.1 引入排除策略，避免内网业务被流控

在这个场景下， SG-8000 以透明的方式部署在防火墙和交换机之间开启流控功能。如果不启用排除策略，PC 终端在访问 DMZ 区的服务器流量会被控制，会影响 PC 终端的正常

业务访问带宽，因此需要将这部分流量排除在外，不做带宽控制。



3.6 集中管理和数据分析系统

安博通集中管理和数据分析系统是提供对 SG-8000 的集中监控、配置和升级，并且对上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用集中管理和数据分析系统，管理员可以高效地管理各 SG-8000 设备，全面掌握网络的整体安全状况。

3.6.1 采用高性能数据存储和查询

安博通集中管理和数据分析系统采用高性能数据仓库，此数据仓库是一款基于网格技术的列式数据库。简单易用，快速安装部署，使用中无需复杂操作，能大幅度减少管理工作；在应对 50TB 甚至更多数据量进行多并发复杂查询时，更能够显示出令人惊叹的速度。

3.6.2 深层次数据挖掘分析

安博通集中管理和数据分析系统采用了先进的数据挖掘分析技术，从收集到的大量数据当中进行深层的数据挖掘及分析，该子系统由日志代理、日志审计中心、日志数据库、审计系统管理器、日志分析中心五个部分组成。日志代理负责收集区域内各种操作系统、网络安全设备、应用程序的日志信息，过滤后发送给日志审计中心处理。日志审计中心负责接受区域内日志代理和各种安全设备、系统转发的日志信息，集中保存在日志数据库，日志分析中心负责对日志数据进行深度挖掘。

4 优势功能

4.1 安全防护

4.1.1 入侵防御

安博通经过多年网络安全领域的沉淀和积累，打造了一支资深的攻击特征库团队和安全服务团队，在蠕虫、后门、木马、间谍软件、Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计等防御手段，并随时关注业界最新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提供更新，实时完善攻击特征库，提供最及时、最全面的入侵防御。

- 超过 3000 种预定义攻击特征
- 实时在线更新
- 提供 WAF 级别的安全防护，有效的防御和预警 Web 服务器的攻击，包括网页防爬虫、网页防篡改、HTTPS 防护、DDoS 攻击防护、Web 攻击过滤、漏洞防护自学习等
- 处理网络类威胁，包括安全漏洞、木马后门、可以行为、CGI 访问、CGI 攻击、缓存溢出、拒绝服务、蠕虫病毒、网络数据库攻击、间谍软件、安全扫描、网络设备攻击、欺骗劫持
- 保证基础网络安全
- 分级事件及操作配置
- 虚拟补丁管理

4.1.2 病毒防护

SG-8000 拥有海量病毒特征库，配合先进的防病毒引擎，能够精准识别并清除流行木马和顽固病毒。病毒检测引擎针对非缓存流检测模式进行了全面结构调整和优化，使 SG-8000 的病毒检测率和处理性能获得质的突破：在保持高病毒检测率的同时，系统性能下降不超过 20%。

- 可以在 HTTP,SMTP,FTP,POP3,IMAP 等多种协议下病毒防御，支持非标准端口的 HTTP,SMTP,FTP,POP3,IMAP 协议中的病毒检测。
- 支持路由、透明、混合等各种工作模式下的网络病毒检测，支持无 IP 地址的透明桥下的网络病毒检测模式，支持 VPN 模式下的病毒扫描。
- 采用高效的病毒防御引擎和国内知名病毒厂商特征库，可检测不少于 300 万以上种病毒。
- 可以根据不同的源 IP 地址、目的 IP 地址、服务、时间、接口、用户等，采用不同的病毒防御策略。
- 可以过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒
- 特征库定时更新，支持病毒库本地升级，病毒库可实时在线升级。
- 支持基于病毒防护策略设置阻断、清除、记录日志，发送电子邮件报警。

4.1.3 异常流量管理

当受到攻击时，伴随而来的会出现网络异常情形发生，网络异常大概可分为以下三种：

4.1.3.1 通信协议异常

例如由外界网络流入大量过长的 IP 数据包、大量的 IP 碎片数据包、异常的 TCP 通信协议连机状态、被截断的 IP 数据包、无法重组的 IP 数据包等。

4.1.3.2 IP/Port 的扫描异常

通过 IP 扫瞄，黑客得以窥知目的端内网络结构和情形；通过 Port 扫描，黑客可以得知目标主机已开启的服务端口。

4.1.3.3 网络流量异常

例如突然产生大量的 TCP SYN、TCP、UDP、ICMP、IGMP 等数据包，占据正常网络使用带宽。

当上述攻击数据包发起时，经过改造的恶意数据包可能会造成企业内部网络系统死机无法对外提供正常的服务；IP/Port 扫瞄的行为将让企业内部的网络架构轻易被黑客得知；大量的异常流量数据包也可能造成企业核心路由器、交换机等因承载过重而死机。

SG-8000 内置异常包攻击防御模块，可以检测各项偏离预期的网络行为。依据 RFC 标准规范制作通信协议异常检测模块，可以阻止不符合标准通信协议规范的数据包。支持网络流量异常检测，不单只使用计数的方式，还使用专门的统计算法，可以准确地检测网络流量的异常情形。

4.2 虚拟化

4.2.1 虚拟防火墙

传统防火墙带有较为明显的缺陷，影响了传统防火墙的灵活性。传统防火墙应用的主要不足为：

- 较多的部分划分，导致企业需要部署多台独立防火墙，导致拥有和维护成本较高。
- 放置的多个独立防火墙将占用较多的机架空间。
- 增加了网络管理的复杂度，优秀出口特性功能。

传统防火墙的不足，推动了虚拟化技术的普遍发展。SG-8000 产品迎合网络时代潮流，自主开发了虚拟防火墙功能。SG-8000 可以逻辑的按照 N：M 的比例划分成多台虚拟的防火墙，每个虚拟防火墙之间独立控制和转发，互相隔离，可以被看成是一台完全独立的防火墙设备，可拥有独立的系统资源、管理员、安全策略、用户认证数据库。SG-8000 的虚拟防火墙功能适用于大规格云计算场景，能够为用户提供更为灵活的网络解决方案。

4.3 出口特性

4.3.1 动态路由协议

网络的迅猛发展，安全设备的静态路由已经无法满足企业网络实时自适应网络结构变化的需求。SG-8000 产品为用户提供 RIP、OSPF 等动态路由协议，针对网络规模大、网络拓扑复杂的网络，帮助企业网络快速收敛，已最佳的路径转发业务流量。

RIP 协议最初是为 Xerox 网络系统的 Xerox parc 通用协议而设计的，是 Internet 中常用的路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其它信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其它路由器。这样，正确的路由信息逐渐扩散到了全网。RIP 使用非常广泛，它简单、可靠，便于配置。但是 RIP 只适用于小型的同构网络，因为它允许的最大站点数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30s 一次的路由信息广播也是造成网络的广播风暴的重要原因之一。

- 支持 v1、v2
- 支持缺省路由发布和路由重发布
- 支持接口下发送版本和接收版本的设置
- 支持认证方式：字符、MD5、不需要认证
- 支持缺省路由发布、路由重发布
- 支持 OSPF 网络区域信息的增删改查
- 支持接口下相关配置

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其它路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其它一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其它区路由器的正常工作，这也给网络的管理、维护带来方便。

- 支持启用关闭，发布路由器 ID。
- 支持缺省路由发布、不发布、强制发布。
- 支持直连路由，静态路由，RIP 路由的重发布。支持 OSPF 网络设置。
- 支持 OSPF 接口、优先级、计时设置。

4.3.2 策略路由，ISP 路由

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。是一种比基于目标网络进行路由转发更加灵活的数据包转发机制。它转发分组到特定网络需要基于预先配置的策略，这个策略可能指定从一个特定的网络发送的通信应该被转发到一个指定的接口。通过策略路由配置实现对于满足所定义策略的报文，从指定的出接口或者下一跳转发的需求。

多出口路由器接入多条宽带线路可以实现带宽叠加、线路备份的作用，从而提高网络的稳定性。但是，如果接入的多条宽带线路不是同一运营商，则可能引起访问瓶颈，导致网络延迟大、丢包等现象。SG-8000 的 ISP 路由功能可以避免以上问题发生，实现访问对应 ISP 网络的数据走正确的出接口。

- 支持预置 ISP 信息，包括联通、电信、教育网、移动等运营商。
- 支持 ISP 路由信息自定义。
- 支持手工创建 ISP 路由条目。
- 支持通过入接口、源地址、目的地址、用户、服务、应用、时间等元组，触发策略路由。

4.3.3 负载均衡

随着带宽成本的下降及业务需求，企业通常存在两个或两个以上的网络出口，多出口提升了网络出口稳定性同时又带来了多链路带宽利用率低、多链路带宽差异大、各运营商网络质量差异、内网应用对带宽需求差异等问题；以上诸多问题只需通过 SG-8000 提供的链路负载均衡即可迎刃而解。具体实现主要基于以下几点：

✧ 实时多链路监测：

实时监测每条出口链路的逻辑连通性，即使端口处于 UP 状态，但可能由于远端故障导致的检测报文超时，SG-8000 同样会执行链路切换的动作，以保证网络连接的可用性，实现多条链路的冗余备份。

✧ 基于权重流量分担：

SG-8000 提供了基于优先级和权重的多链路流量分担算法以满足不同应用场景的需求，从而达到高效的利用出口链路带宽的目的。

✧ 运营商智能选路：

内置电信、联通、移动和教育网地址库，可以智能的依据目的 IP 运营商属性来决定流量走向，将属于该运营商的访问自动的指向该运营商的链路，实现“南北互通”。

✧ 智能应用路由：

SG-8000 内置超过 1400 种以上的应用识别能力，将网络中各种应用进行准确分类和精细识别，让不同的应用分别使用不同的出口线路，保证重要业务不中断。

✧ DNS 透明代理：

通过透明代理技术，完成对客户 dns 流量的无感知代理，从而保证客户的 dns 请求得到最快，最稳定的响应，大幅度提升客户的上网感受。

SG-8000 支持全面的负载均衡功能如下：

- 支持负载均衡出接口及下一跳。
- 支持出接口链路健康状态的检查。
- 支持免负载均衡地址
- 支持负载均衡的策略配置
- 支持基于出接口权重、优先级的选路
- 支持负载均衡状态监控

其设计原理如下：

负载均衡出接口可同时被多条负载均衡策略引用，作为匹配了负载均衡策略流量的出接口，可以支持三层物理口、三层 VLAN 子接口、三层聚合口、tunnel 口。

负载均衡的策略，负载均衡策略的匹配项包含：源接口、源地址、目的地址、服务、应用、用户、时间。各匹配项的配置个数与普通安全策略相同。需要默认提供四大运营商中国

联通、中国电信、中国移动、中国教育网的地址对象。

负载均衡策略的匹配点，在策略路由匹配之后、系统路由匹配之前，流量应从上向下依次匹配负载均衡策略。

负载均衡策略的优先级可以修改，与普通安全策略的修改方式相同。

配置变更无需自动触发流量重新匹配策略。

最多支持配置 32 条负载均衡策略，每条策略的出接口最多可以配置 32 个。

基于出接口权重、优先级的选路，基于权重选路是将流量的会话按照可用出接口间的权重比进行分配；基于优先级选路是在可用出接口中选取优先级最高的接口转发。

因为有些特殊应用场景，需权重、优先级同时生效，所以引入接口组的概念，接口组内可以配置权重或优先级，接口组和组外接口也可配置权重或优先级。可以实现组内多个出接口按权重负载，组外有低优先级出接口进行链路备份。

选路时采用 HASH 算法，可使用获取随机 hash 值，应确保同一链接的所有流量使用相同出接口。对于父子链接的应用：sip、h323、pptp、ftp、tftp 等要求主从链接必须使用同一个接口完成转发。可以采用只根据源 IP hash 的方法，或者直接使用会话 master 的下一跳。

负载均衡状态监控，负载均衡状态的统计，需要可以基于策略显示每个出接口的实际流量，可以基于策略显示每个出接口在一定时间内的流量比例饼图。

可以仿照接口流量统计的机制，定时将策略出接口的流量进行记录，以供查看。

4.3.4 DDNS

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

目前 ISP 大多提供动态 IP（如拨号上网），若想在网际网络上以自己的网域公布，DDNS 提供了解决方案，它可以自动更新用户每次变化的浮动 IP，然后将其与网域相对应，这样其他上网用户就可以透过网域来交流了

DDNS 可以让用户在自己的或家里架设 WEB\MAIL\FTP 等服务器，而不用花钱去付虚拟主机租金。主机是自己的，空间可根据自己的需求来扩充，维护也比较方便。有了网域与空间架设网站，FTP 服务器、EMAIL 服务器都不成问题。

如果用户有对 VPN 的需求，有了 DDNS 就可以用普通上网方式方便地建立 Tunnel。透过网域的方式连结，实现远端管理、远端存取、远端打印等功能。

4.3.5 DNS-DNAT

为了规避运营商出口故障带来的网络可用性风险，和解决网络带宽不足带来的网络访问问题，企业往往会租用两个或多个运营商出口（如：电信、网通等）。内网用户访问外网的情况下，如果我们通过主机上配置的 dns 服务器来进行查找，此时返回来的 ip 地址并不一定是对应的运营商的 ip 地址，此时的访问网络的效果并不能达到理想的效果。SG-8000 系列支持 DNS-DNAT 功能，能让我们对应的链路能够返回对应的服务商提供的服务的 ip 地址，解决上网速度慢的问题。

该功能基于负载均衡策略实现，在解决上网速度的问题的同时，也能够解决链路负载不均衡的问题。

该功能的实现流程为：在用户的 DNS 流量配置到策略的时候，根据策略选择好了出接口，此时负载均衡策略出接口上配置了 NDS 服务器，我们需要将原来的 DNS 流量的目的地址替换为配置的 NDS 服务器地址，即做 DNAT。

4.4 灵活、安全、自动的 VPN

4.4.1 IPsec VPN

SG-8000 支持标准的 IPsecVPN，支持点对网和网对网的接入方式，提供高安全的加密隧道方案。通过简单配置用户就能轻松搭建安全的 VPN 隧道连接；满足各种总分型企业用户对数据传输的便捷性、安全性以及高性价比的要求。

对金融、能源、交通等行业一些分散型的营业网点，对于业务连续性以及内网数据安全要求非常高。在租用运营商的固网光纤专线作为主链路的同时，还需一条安全稳定的备份链路以应对突发状况，专线成本高、灵活性差的缺点暴露无遗；SG-8000 支持 4G 网络并支持 4G IPsecVPN 加密连接，4G 连接提供按需拨号，无需改变原有网络架构，在主线路故障时主动承接和中心端的网络加密通信，具备数据完整性、数据传输安全、高性价比、网络无改变等特性。

4.4.2 SSL VPN

企业级用户业务系统中的高价值信息资产越来越多，外出办公人员接入重要的业务系统时需要保障端到端的安全性。SG-8000 具备 SSL VPN 功能，该功能主要是由两部分组成，一部分是 SSL 记录协议，它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。另一部分是握手协议，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。它们共同为应用访问连接提供认证、加密和防篡改功能，为各种应用协议提供基本的安全服务，保障用户数据的私密性、完整性和安全性。

SG-8000 提供使用多平台、多终端的 VPN 客户端，帮助用户在访问 Web 服务的同时，可以访问其他形式的资源，例如 FTP、文件共享等。支撑移动办公人员多业务、多应用的需求，为其提供舒适化移动办公的环境。

4.5 精准细致的行为管控

4.5.1 应用、URL 控制

SG-8000 产品采用流检测和包检测技术对各类应用进行深入分析，可以对 802.1Q、MPLS、QinQ 等特殊封装报文解析，搭建应用协议识别框架，准确识别主流应用协议。内置 1520 多种应用特征，60 种 URL 分类，千万级别的 URL 条目，单种应用多达 12 种行为控制动作，特征库每周更新，保障识别应用的特征。管理员可以基于用户、接口、域、源地址、目的地址、时间、端口等维度，针对应用、URL 和自定义地址，通过关键字和行为动作的控制进行细粒度行为管理，在工作时间允许微信“发消息”动作，不允许“摇一摇”、“朋友圈”等动作，限

制员工发表不良言论和外发企业机密文件。管理员通过策略的控制，达到用户上网精细化管理的效果，最大程度的提高员工的工作效率，减少舆论风险给组织形象声誉带来影响。

4.5.2 加密网站、邮件审计

互联网时代，越来越多的网站启用 HTTPS，而随之而来的是员工利用这种加密方式泄露企业敏感信息的可能性也越来越大；并且由于 HTTPS 网页经过了加密，采用普通的流量分析方式是无法审计到访问行为的，那么就意味着员工使用 HTTPS 的方式进行娱乐，企业是无法清晰准确的了解员工的工作状态和网络的运行状态。为了保障企业有清晰的事后审计，保护企业机密，SG-8000 产品提供了 HTTPS 审计功能，SG-8000 采用特有的加密流量识别技术，能够对主流的加密网站、加密网站搜索记录、加密邮件等进行行为识别。管理员可以采用自定义的方式，定向审计用户和加密网站，让网络运行情况更加清晰明了，做到管理规划有据可循、有的放矢。

解析 DNS 报文，设备获取 DNS 回应报文，匹配解密策略的源地址组，解析出域名对应的 IP，往当前策略上添加 IP 域名信息。

转发报文流经设备，判断 TCP 443、995、993、465 端口进入解密策略匹配流程。依次匹配入接口、源地址对象、目的地址对象、若为 443 端口判断目的 IP 是否存在于 DNS 解析的 IP 中，若均匹配上报文送入 linux 内核，通过内核的 iptables redirect 功能重定向到本机代理进程。

代理进程建立双向 SSL 连接，并对数据进行加解密，解密后的数据封装 SKB 后送入审计流程。

4.6 用户管理

4.6.1 全面身份认证方式

使用 SG-8000 产品，管理员能依据组织架构灵活的建立用户身份认证体系，有效的区分用户，防止身份冒充、权限滥用等情况。

SG-8000 支持丰富的身份认证方式；

- 本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定；
- 第三方认证： LDAP、RADIUS、AD 域等；
- 短信认证：通过接收短信获取验证码，快速认证；
- 微信认证：通过扫描二维码，关注微信公众号进行快速认证；
- APP 认证：通过下载安装运行 APP，强制认证
- 免认证：无需认证，快速上网

SG-8000 产品的微信认证按照微信标准的 3.0 接口开发完成，为用户上网摆脱了繁琐用户名、密码验证，提升上网体验；为企业公众账号迅速增粉，打造一个会营销的无线网络。微信认证自适应各种终端，用户连接 wifi 后，自动弹出“一键打开微信连 WiFi”页面，点击按钮，页面跳转到微信中，点击“立即连接”，成功上网，跳转到自定义 URL，进行推广。同时，商家不需要在微信服务器部署代码，节省实施成本。为了简化用户的认证过程，SG-8000 产品内置超长无感知时间，用户二次到店，用户无需再次认证；有多分支门店的客户，门店间

可以漫游认证，即在一个门店微信认证过后去其他门店可以免认证，给用户超预期的用户体验，提高企业品牌认可度。

SG-8000 可拓展 APP 认证。零售企业网点和商户，推出了自己的 APP，该 APP 可以帮助用户在线购物，服务预定；帮助商户提升品牌影响力。用户连接商户 WiFi 后，自动弹出 APP 的下载页面，用户下载安装运行后，打开 APP 后即可上网。为了缓解商户带宽压力，提升 APP 下载速度，APP 和对应的下载链接可以预先缓存在 SG-8000 产品中，用户下载 APP 时，SG-8000 产品本地下发 APP，用户下载速度媲美 4G。 APP 认证有效的复用了现有商户网络资源，帮助商户节省营销成本，取得较好的营销推广效果。

SG-8000 产品具有丰富的认证方式，能够帮助管理员灵活的针对用户分组进行认证划分，管控身份权限，实现职位匹配权限。

4.6.2 用户数据同步

SG-8000 集合了多系统、多平台的主流用户系统对接方式，包括 Radius、LDAP、AD 域、SAM、AAS、IMC、深澜、城市热点等，SG-8000 产品能够实时的和第三方用户系统同步上下线用户信息，保障上网实名制； SG-8000 产品能够根据 OU 或 Group 读取 AD 域控服务器上用户组织结构，并保持与 AD 的自动同步，方便管理员管理。

4.6.3 灵活用户管理

SG-8000 产品可以完全按照组织的行政结构建立树形用户分组，实现父组、子组等多层嵌套的要求。在完成用户组的创建后，将用户分配到指定的用户组中，以实现网络访问权限的授予与继承。

SG-8000 产品的用户管理模块，管理员能够自定义的移动单个或者多个用户和用户组的位置，实现网络访问权限的自定义变更。此外 SG-8000 支持用户以及用户组跨页模糊查找。SG-8000 将用户/用户组信息与需要查找的用户名字信息进行匹配过滤（利用 strstr 函数进行匹配匹配），将符合条件的用户/用户组信息返回。

灵活的用户管理模块，能够帮助管理更清晰的了解当前组织的行政结构，更迅速更便捷的管理内网用户的上网权限。

4.7 VPN 级 HA 高可靠

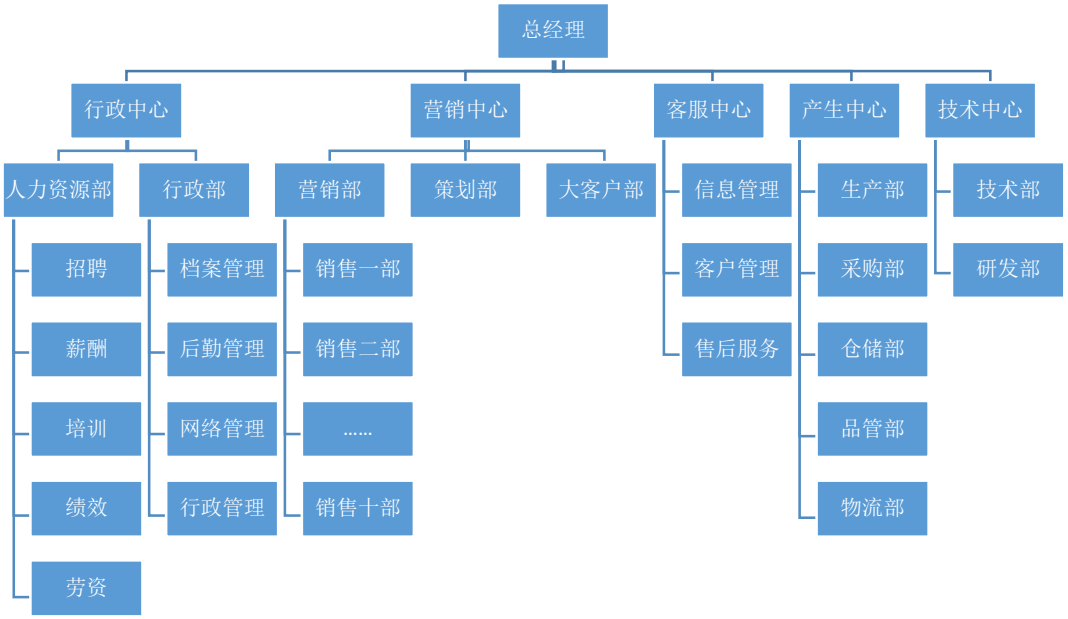
随着 IP 技术的飞速发展，各种增值业务在互联网上得到了广泛的应用。新兴的 NGN/3G、IPTV 流媒体、大客户专线和 VPN 互联等重要的电信级业务，对网络的可靠性提出了很高的要求。

SG-8000 配备 VPN 级别的 HA 功能。SG-8000 除了市面上支持主主、主备模式功能，同步配置、运行状态、会话、用户上线状态、特征库等内容之外，SG-8000 能够同步 IPsec VPN 状态。VPN 对于电信级业务来说是命脉，如果普通设备的 VPN 断开重连，按照协议标准，算上 DPD 超时和 IKE 建立的时间，估计在 100 秒到 120 秒，其中的时间成本是企业无法承担的。SG-8000 产品完美的解决了这个问题，主备设备同步 VPN 的状态，主备切换时，零丢包零中断，保障用户的关键业务不中断，极大的避免了企业的损失。

4.8 带宽管理

4.8.1 流量管理

SG-8000 使用了卓越的应用识别技术，由于该识别技术有效的融合了 DPI 和 DFI 两种识别方法的优点，大幅度提升了应用识别的准确度。但是随着企业规模不断扩大，网络带宽管理需要更精细的管理。对于大多数企业组织架构通常由中心、部门、子部门组成，如下图：



由上图可知，3 级流控只能满足到基层部门的流控制，对于部门下的应用控制已经明显力不从心，为此 SG-8000 提出了 4 级流控，可以满足大中型企业普遍带宽管理需求，策略主要支持基于用户/组、应用/组、服务、源地址等七元组的方式实现带宽管理细化，满足用户各种带宽管理的需求。如下图：

	线路名称	匹配条件					上行(出)			下行(入)			优先级	操作
		源地址	用户	服务	应用	时间	保障带宽	最大带宽	每IP	保障带宽	最大带宽	每IP		
1	某企业	-	-	-	-	-	↑100M	↑100M	-	↓100M	↓100M	-		-
2	营销中心	-	营销中心	-	所有应用	always	↑10M	↑50M	-	↓10M	↓50M	-	高	
3	大客户部	-	大客户部	-	所有应用	always	↑5M	↑20M	-	↓5M	↓20M	-	高	
4	策划部	-	策划部	-	所有应用	always	↑2M	↑20M	-	↓2M	↓20M	-	高	
5	营销部	-	营销部	-	所有应用	always	↑5M	↑40M	-	↓5M	↓40M	-	高	
6	销售一部	-	销售一部	-	所有应用	always	↑2M	↑10M	-	↓2M	↓5M	-	高	
7	P2P限制	-	所有用户	-	迅雷, 迅	always	↑50kb	↑1M	-	↓50kb	↓1M	-	高	
8	邮件保障	-	所有用户	-	广东省教	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
9	默认通道(名	-	-	-	-	always	↑400kb	↑10M	-	↓400kb	↓5M	-	低	
10	销售二部	-	销售二部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
11	销售三部	-	销售三部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	

4.8.2 流量可视化

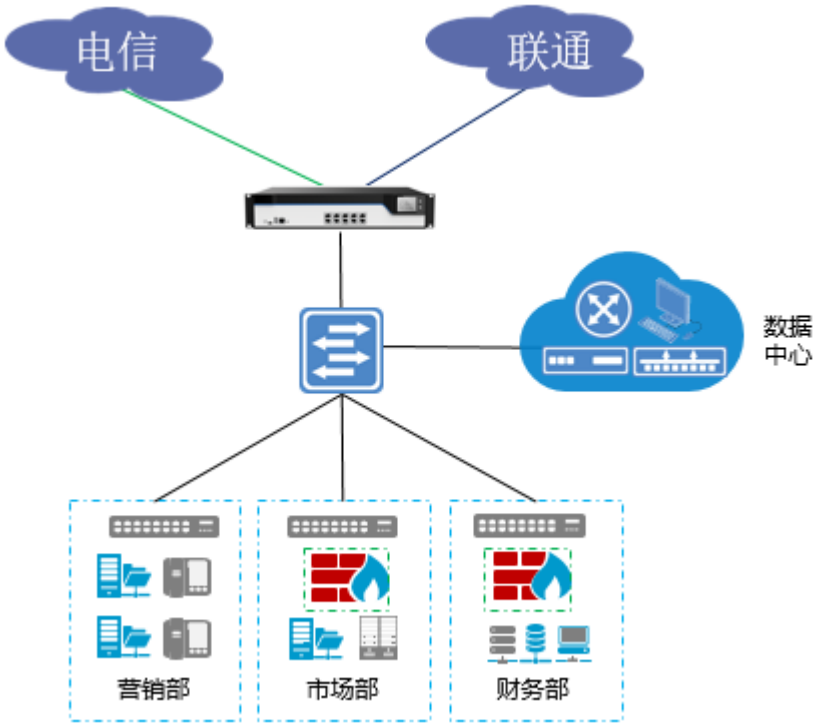
SG-8000 为管理员提供了清晰直观的流量查看功能。管理员可以查看出口流量曲线图、应用流量统计、用户流量统计、设备流量统计、设备健康统计、会话监控、攻击监控等信息，直观了解当前网络运行状况，让管理员轻松掌控用户网络行为分布和带宽资源使用等情况，

了解流控策略效果，为带宽管理的决策提供准确依据；为保障系统持续稳定运行打下基础，为网络扩容提供依据。

5 组网应用

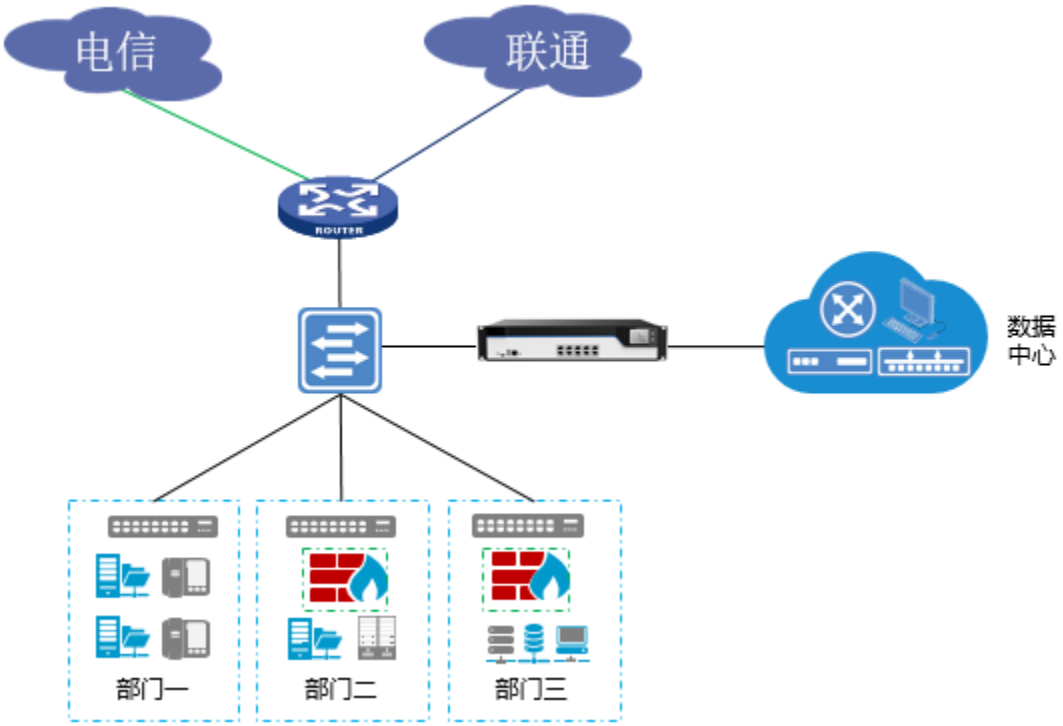
5.1 企业边界网关部署

- 适用于大中型企业用户，以网关方式在线部署于网络出口
- 抵御内外网的入侵防御，对网络中的病毒进行过滤查杀。
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽
- 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理



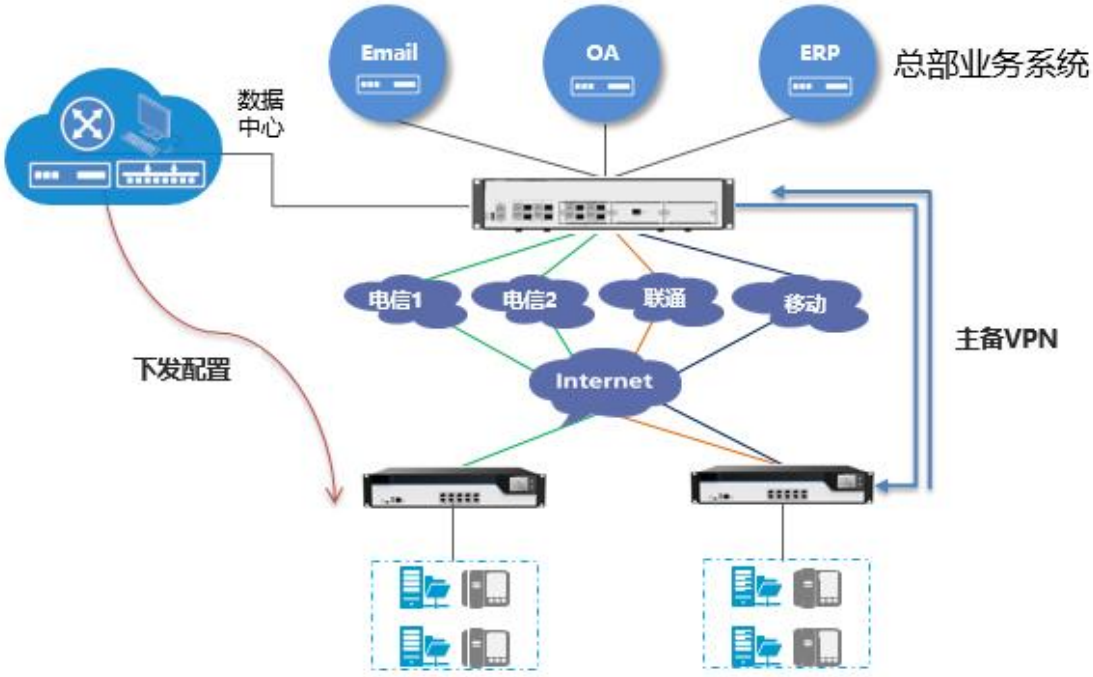
5.2 关键业务串行防护

- 适用于数据中心机房，可灵活的以串行路由或者透明方式部署于数据中心机房出口，根据实际网络环境署简单；
- 通过 SG-8000 的 AV 和 IPS 功能的保护，除了对外网针对数据中心的暴力攻击能有效阻挡之外，还可对所有进出的封包均进行详细的七层分析，让黑客利用合法方式进行非法存取的攻击将无所遁形；
- 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，并可进行数据分析。



5.3 总分型网络集中部署

- 适用于大型总分型网络，以边界设备方式部署在总部和分支网络的出口；
- SG-8000 可以为总部和分支提供 AV 和 IPS 保护，有效的抵御各种网络威胁；
- IPsec VPN 配置简单易用，零配置上线，全自动收敛，几乎零配置，自适应多线路，完美地解决分支运维能力弱的问题；
- 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，可多台分布式部署统一管理，并可进行大数据分析。



6 功能列表

分类	功能	详细指标
部署模式	旁路	单接口监听交换机镜像流量
	串行	支持透明、路由、混合（透明+路由）、多组桥、多口桥
	混合	支持旁路和串行混合部署
接口配置	物理接口	启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		DHCP 下发 DNS
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		协商模式：自动、强制（可设置双工和速率）
		工作模式：路由模式、桥模式
		MTU，修改范围 1280-1500
	子接口	子接口管理（增删改查）
		子接口 ID：1-4094
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	桥接口	桥接口管理（增删改查）
		桥接口 ID：0-255
		启用/关闭
		IPv4 地址类型 :静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	聚合接口	聚合接口管理（增删改查）
		聚合接口 ID：0-255
		启用/关闭
		IPv4 地址类型 :静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500

	loopback 接口	支持生成、配置 loopback 接口。（命令行支持）
		支持基于 loopback（或指定 IP）接口地址的管理（设备管理等）（命令行支持）
	隧道接口（显示）	隧道模式：IPv6 隧道、Ipsec 隧道
		显示项目：接口名称、隧道模式、连接状态、启用状态
	4G 接口	支持联通 4G 上网卡（推荐：华为 E3372）
	TCP MSS 调整	支持根据业务类型智能调整
		命令行支持接口 TCP MSS 手工调整, 支持全局设置和 VPN 单独配置
端口镜像	镜像接口	物理接口支持作为镜像接口和被镜像接口
	镜像功能	支持将多个物理接口的流量镜像到一个接口
		支持基于接口全部流量，上行流量，下行流量的镜像
DHCP	DHCP 服务类型	DHCP 服务器
		DHCP 中继代理
	服务器属性	网络配置：网关、子网、开始结束 IP 地址
		租约：无限、有限时长
		高级属性：DNS 支持 2 个，Wins 支持 2 个，域
		支持排除地址
		支持 IP-MAC 绑定
	DHCP 监视器	显示 IP 地址和 MAC 地址及开始时间、结束时间
		清除条目
IPv4 路由	路由表	显示设备路由信息
	高级路由属性	支持非对称路由
		命令行下支持强制源进源出
	静态路由	增删改查
		支持基于路由权重的多链路负载均衡
		支持路由优先级
		支持 VRF 配置
	策略路由	增删改查、移动
		5 元组策略路由+时间
		基于用户的策略路由
		基于应用的策略路由
		支持基于路由权重的多链路负载均衡
	ISP 路由	内置电信、联通 ISP 信息
		支持自定义 ISP 信息
		增删改查
	RIP	支持 v1、v2
		支持缺省路由发布和路由重发布
		支持接口下发送版本和接收版本的设置
		支持认证方式：字符、MD5、不需要认证
	OSPF	支持缺省路由发布、路由重发布

		支持 OSPF 网络区域信息的增删改查
		支持接口下相关配置
		支持认证方式：字符、MD5、不需要认证
NAT	通用功能	支持日志发送
		地址池
	源 NAT	支持配置的增删改查、移动
		源地址转换类型：出接口、地址池、 不转换
	目的 NAT	支持配置的增删改查、移动
		目的地址转换类型：地址池、转换端口、不转换
	静态 NAT	支持配置的增删改查、移动
	ALG	动态端口支持协议 ALG：H.323、SIP、FTP、TFTP、PPTP
		FTP、TFTP、SIP 支持非标准端口设置
会话限制	规则管理	增删改查
	功能	支持基于地址对象的限制
		支持基于 IP 的会话数、每秒新建的限制（如引用地址对象，则对地址对象中的每个 IP 地址进行限制）
	限制阻断	显示限制信息
		IP 会话限制内容 :IP 地址、连接数、会话限制、每秒新建、每秒新建限制、限制阻断统计、引用地址对象名
		支持查询过滤和全部显示
	会话统计	显示当前 IP 地址的连接数
		支持 session 状态监控
地址探测	接口探测	支持 ping 地址监控条目
		支持 tcpsyn 地址监控条目
		支持 dns 地址监控条目
		支持接口类型：物理接口，子接口，桥接口，聚合接口，隧道接口
	地址探测组	支持多个地址探测从属组关系
		分为严格模式和非严格模式（严格模式即所有探测条目均成功组状态才成功，非严格模式探测条目间为独立状态）
		支持对探测组描述
	路由探测	支持探测路由以确保路由有效性
	支持场景及部署方式	支持静态路由或 ISP 路由联动
		支持与接口状态联动
		支持与 HA 联动
	日志说明	可对地址探测失效、恢复有日志记录
链路负载均衡	链路负载均衡	基于七元组的链路负载均衡策略
		基于域名的负载均衡策略
		基于接口，接口组的负载均衡策略
		基于直连网段和特定网段的负载均衡排除
		负载均衡接口支持 pppoe，dhcp，聚合链路，物理接口，

		等三层接口
		基于 ICMP 的接口探测机制
		支持基于源地址 hash 的链路负载均衡
		支持基于优先级的链路负载均衡
二层支持	VLAN	vlan 子接口
		子接口都支持 IEEE 802.1Q，能进行封装和解封。
		支持对报文进行二次基于 802.1Q 封装的 VLAN-VPN 应用。(QinQ)
	生成树协议	支持 802.1d 的 STP 生成树协议。
	报文透传	支持二层解封装和再封装，对上层透明
IPv6	基础功能	IPv6 路由通告
		IPv6 静态路由、OSPFv3
		支持用户和应用均为任意的 7 元组策略
		扩展报文头的逐跳报文的处理、分片报文等的处理
		隧道支持：手工隧道，6to4 隧道，ISATAP
		Nat64
		防畸形报文攻击
应用缓存	应用缓存	支持文件缓存
服务质量管理	服务质量管理	支持 PING、TCP、DNS 探测
		支持接口探测
		支持自定义间隔时间探测
VRF	接口虚拟化	接口默认属于 root，创建 VRF 后可把接口添加到 VRF 内，一个接口只能属于一个 VRF；
	IP 地址重叠	不同 vrf 下的接口可以配置相同的 ip 地址
	静态路由	支持静态路由
通用功能	黑名单	支持手动配置
		支持触发防攻击规则和 IPS 阻断源地址规则自动进入黑名单
		支持生存时间配置
	分析模块	扫描攻击分析
		异常包攻击分析
		Flood 攻击分析
扫描防护	通用	基于接口的配置
		支持自动加入黑名单
		扫描阈值设置
	扫描方式	端口扫描、IP 地址扫描
异常包防护	异常包类型	Ping of Death ;Land-Base ;Tear Drop ;TCP flag ;Winnuke ; Smurf ; IP 选项 ; IP Spoof ; Jolt2
ARP 防护	防 ARP 攻击	启用与关闭
		支持 ARP 学习与主动保护

		可设置 IP-MAC 绑定
		防 ARP Flood 攻击
		支持 ARP 表查看、绑定、清除、接口信息
	ARP 学习控制	基于接口的 ARP 学习控制
Flood 防护	通用	一体化配置
		基于目的 IP、IP 范围
		支持接口防御
		阈值设置
	支持类型	SYNFlood、UDPFlood、ICMPFlood、DNSFlood
通用功能	配置管理	增删改查
流量控制	线路管理	绑定接口
		支持基于接口的上下行带宽管理
	通道管理	支持高、中、低优先级通道设置
		支持应用、用户、源地址、服务、时间的通道匹配
		保障带宽
		限制带宽
		每 IP 限速
		自动支持流量整形
排除策略	排除策略	支持用户、地址排除
IPv4 安全策略	配置管理	支持策略增删改查、启用/禁用、移动
		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
	策略	七元组策略匹配条件：用户、应用、源地址、源接口、目的地址、目的接口、服务
		支持基于时间表的策略配置
		支持应用选择过滤
		支持基于应用的应用类型组选择
		支持策略动作为：允许、拒绝、IPSec
		基于策略的长连接（老化时间）
		支持动作为拒绝的策略进行日志记录
IPv6 安全策略	配置管理	支持策略增删改查、启用/禁用、移动
		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
	策略	支持用户和应用均为任意的 7 元组策略
		支持基于时间表的策略配置
		支持策略动作为：允许、拒绝
		支持动作为拒绝的策略进行日志记录
应用过滤策略	配置管理	增删改查
		启用禁用
		描述

	策略	支持根据应用/应用类来区分不同的应用行为
		支持根据应用行为来区分不同应用的审计内容
		根据应用行为确定审计内容
		支持基于关键字或者数字的内容审计
		支持允许/阻断的策略动作
		审计日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息
URL 过滤策略	配置管理	增删改查
		启用禁用
		描述
	策略	支持恶意 URL 过滤
		支持预定义和自定义 URL 分类过滤
		支持 URL 阻断和审计（动作：允许 、拒绝）
		URL 日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息
应用控制及审计	通用审计内容	审计用户名、所在组名
		审计应用名、所在应用类
		审计操作系统、平台、终端、供应商
		审计源 IP 地址、目的 IP 地址、目的端口
	即时通讯	基于帐号的登录控制、黑/白名单
		支持非加密收发消息时的关键字内容审计
	P2P 类	识别迅雷
	股票软件	基于行为（登录、交易、行情）的控制和审计
	网络游戏	基于行为的控制和审计
	搜索引擎	关键字过滤
	Webmail	支持邮件内容审计，不支持附件审计。
		支持普通版 webmail 审计（QQ、163、126、新浪、139 邮箱）
	社区类	支持论坛（BBS、博客）主题过滤（如果有）
		论坛（BBS、博客、微博）内容过滤
	联系人	支持以发件人过滤
	非加密邮件	支持邮件客户端的主题、内容、附件名过滤
		支持记录邮件内容，需要带本地硬盘
	命令类	支持基于命令和操作的审计
		论坛上传下载文件名过滤
https 解密	https 网页解密	支持预定义 https 页面解密
		支持自定义 https 页面解密
	ssl 加密邮箱解密	支持 ssl 加密网页版邮箱解密
		支持 ssl 加密客户端邮箱解密
	解密策略	支持解密策略的启用禁用
		支持基于入接口，源地址，目的地址多维度的解密策略

		支持解密策略排除特定的站点
入侵防御	入侵防御	支持基于源、目的、规则集的入侵检测。
		支持 5 种自定义动作
		支持软件 bypass（CPU and 内存高于 70%）
	DDOS 防护	可记录攻击日志和报警。
	特征库	支持系统规则库手动、自动升级。
		系统定义超过 3000 条规则，包含 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game。
防病毒	病毒防护	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
		查杀邮件正文/附件、网页及下载文件中包含的病毒
		支持 300 万余种病毒的查杀，病毒库定期与及时更新
		支持启发式扫描查杀未知病毒
		支持 ZIP/RAR 等压缩文件的病毒查杀
		压缩：默认 5 层，最大 20 层
		支持 TAR 等多种打包文件的病毒查杀
PKI	证书格式	支持 X.509 V3 数字证书，支持 DER/PEM/PKCS12 多种证书编码。
	本地 CA	支持内置 CA，为其他设备或移动用户签发证书。
		支持本地 CA 根证书、根私钥的更新。
		支持在线 CRL 列表。
IPSec VPN	IKE 第一阶段协商模式	支持 IKEv1
		支持主模式和野蛮模式
	IKE 身份认证	预共享密钥
		RSA 证书认证
	加密/HASH 算法	国际标准算法(DES/3DES/AES;MD5/SHA-1)
	IPSec 封装模式和协议	支持隧道模式
		支持 ESP 和 AH 封装
	部署模式	网关到网关
		远端地址为动态
		对端地址为 DNS
		Hub Spoke 组网，spoke 之间通过 IPSec 通信
		VPN track（可以探测到 VPN peer 地址不可达并将隧道删除）
		客户端远程接入，支持扩展认证和模式配置
		隧道 VPN
	配置方式	基于安全策略配置/基于路由（隧道口）配置
	其他特性	DPD
		NAT 穿越

		FQDN
		DH 组配置
		PFS
	维护手段	隧道监视器
	流量统计	支持隧道持续时间统计等
	用户功能	支持用户强制下线
	VPN 功能优化	提供 VPN 接口和 VPN 路由
		VPN 展示优化
		同设备对接和第三方对接
通用功能	导入导出	用户、组的导入导出
	新建、删除	用户、组的新建、删除
	用户组	支持用户组
	用户种类的改变	可以在认证用户、固定 IP 用户、匿名用户之间自由变换
	批量移动	支持一个或者多个用户的批量移动功能
	模糊查询	支持用户，用户组的模糊查找功能
	一键删除	支持一键删除所有的用户，用户组
	超时检查	对认证用户、移动用户、第三方认证用户支持超时时间检查
认证用户	账号管理	增删改查
	认证服务器	支持 HTTP 登录
	认证方式	本地认证、认证服务器、静态绑定
	认证设定	锁定时间
		认证用户保活
		支持唯一性检查
		登录后重定向页面
		绑定多个认证地址
	基本功能	用户登录和注销界面
		支持移动设备登录页面自适应
IPv6 支持	IPv6 用户	用户可绑定 IPv6 地址
移动用户	用户	自动添加用户
	移动用户组	内置移动用户组
第三方认证	支持 portal 联动	支持 portal 服务器联动
	radius 携带 nas-id	开发实现 NAS-Identifier(32)在无线场景携带 AC 名字
LDAP 用户管理	LDAP 用户同步	支持定时自动，手动的 LDAP 用户同步功能
		支持标准 AD 服务器和 OPEN LDAP 服务器的用户导入
	LDAP 用户	导入的用户支持策略引用

	策略	
识别相关	识别范围	设置识别的 IP 地址范围
重定向	重定向页面	默认重定向页面
策略	认证策略	匹配项：源接口、源地址、目的接口、目的地址、时间
		重定向页面选项（相关行为）
		支持微信、短信、本地、免认证、portal 认证
用户认证	微信认证	限制微信流量放通（pc 和移动端，认证通过放通）
		支持基于 http 获取 access_token
		支持微信内部浏览器 http 弹 portal
		强制关注功能（定时检查用户是否关注公众号）
	混合认证	支持本地、短信、微信、免认证四种认证方式的混合认证
	认证白名单	支持基于源地址的用户认证白名单
系统管理员	账号管理	管理员账号的增删改查
		只读管理员查看配置权限（审计员）
		登录认证方式支持本地认证、Radius 服务器认证、LDAP 服务器认证
		密码复杂度：必须包括数字，英文和字符，6-63 个字符
		每帐号可绑定 3 个 IPv4 地址或子网
	管理设定	支持三权分立
		支持账号唯一性检查
		最大登录重试次数 1-60 次，默认为 5 次
		登录失败阻断间隔 1-3600 秒，默认为 1 分钟
		页面超时时间 1-480 分，默认为 10 分钟
		在线管理员 1-20 个，默认为 20 个
	在线用户管理	支持管理员在线监控和强制下线
	阻断用户	支持管理员黑名单，阻断用户可监控，可解锁
认证服务器	Radius	支持用户信息在远端 Radius 服务器存储
		支持多用户第三方存储远端请求认证
		单服务器认证
	LDAP	支持用户信息在远端 LDAP 服务器存储
		支持多用户第三方存储远端请求认证
		不支持 LDAP 组同步认证
		支持 LDAP 用户、用户组同步
		单服务器认证
	服务器组	Radius/LDAP 服务器组，支持主备和集群
	短信认证	支持短信验证码验证身份实现 wifi 认证上网
		短信网关认证页面自定义

	微信认证	支持微信关注公众账号实现 wifi 认证上网
		支持二维码扫描认证
	免认证	免认证
	无感知认证	无感知认证（非跨门店）
系统维护设定	系统时间	手工设置时间
		NTP 同步
		设备间同步时间（通过 NTP 保持一致）
	系统重启	恢复出厂配置
		系统重启
	部署方式	旁路部署
	授权	许可证
	配置文件	配置文件导入导出
		双备份配置
	系统升级	系统升级手动、自动、升级历史
		支持断点续传
		动态库升级（应用、URL、IPS、AV）
	诊断工具	ping 探测
		traceroute 探测
		TCP SYN 探测
	抓包工具	支持按照过滤条件抓取数据报文
		支持将报文下载到本地保存查看
	信息收集	设置方式：手动搜集和自动收集
		收集内容操作：下载、查看、删除
可靠性	硬件 bypass	电口断电 bypass
		电口启动过程 bypass
	软件 bypass	IPS 模块软件 bypass :瞬时 cpu 使用率超过 70%按 10:1 进入检测流程，命令行可调比例
双机热备 HA	主备模式	支持配置同步
		支持流同步
		支持特征库同步
		支持接口状态监控
		支持抢占模式
		支持备机可管理
		支持 AGG 口作为心跳口，提高心跳口可靠性
		支持 HA 状态监控
	主主模式	支持认证用户同步
		支持流同步
		支持接口状态监控
		支持地址代理

		支持非对称路由
		支持 AGG 口作为心跳口，提高心跳口可靠性
接口状态同步组	物理状态同步	支持两个或者多个接口状态绑定
SNMP	SNMP 配置	SNMP 代理
		版本：v1、v2、v3
	trap	trap 版本：v1、v2 Notification、v2Inform
		trap 地址
	私有 mib	CPU、内存
	SNMP 用户	增删改查
		认证方式：None、MD5、SHA
	支持跨三层 IP MAC 绑定	支持跨三层 IP MAC 绑定
域名相关	DNSserver	支持 4 个 DNS 服务器
		静态域名（256 个）
	DNS 透明代理	代理接口支持三层接口
		实现基于优先级的 dns 代理算法
		实现基于权重的 dns 代理算法
		支持静态域名配置
		支持特定域名特定 dns 服务器解析
		静态域名和特定域名支持模糊匹配
		支持 dns 透明代理缓存管理
日志设定	syslog 日志配置	日志服务器：地址和端口（3 组）
	日志过滤	本地认日志记录开关、日志服务器日志级别开关
	设备映射表	设备映射表流量、上网行为、系统管理
Debug	命令行	各模块 Debug 支持
管理端口漂移	cli 端口：telnet ssh	支持命令行管理端口的漂移
	WEB 端口：80；443	支持界面管理端口的漂移
首页	系统信息	设备序列号、主机名称、产品型号、系统版本、URL 版本、APP 版本、IPS 版本、AV 版本
		系统时间、日志汇总（访问网站、收发邮件、论坛与微博、IM 聊天）、当前会话数、运行时间
	实时流量（设备）	基于物理口的上下行流量统计 bps（1 小时 60 个点）
		整机总流量统计 Kbps/Mbps/Gbps
	接口信息状态	接口状态
		接口详细信息

	用户、应用流量排名	Top 20
	系统资源	CPU、内存
在线用户	全部用户	显示所有用户
	移动用户	显示移动用户
	查询	按网段查询
	管理	冻结、解冻
		离线
防私接防共享	防私接防共享	支持基于 IP 及 IP 段配置白名单
		支持 基于用户、MAC、终端数量的监控
		支持状态监控、解锁操作
统计集	应用流量统计	应用统计总览可视
		应用比例图呈现
		应用统计趋势图总览
		应用统计详细信息展现
		应用与用户维度耦合
		应用 TOP20 统计
	用户流量统计	用户统计总览
		支持用户统计柱状呈现
		用户统计详细信息总览与应用维度耦合
		支持查看单个用户的应用趋势及应用 TOP 列表
		用户 TOP15 统计
流量监控	接口流量统计	支持接口上下行统计，包含每小时、每天、每周
		支持设备转发数据历史的可视化
		支持每个接口收发数据历史的可视化
	用户信息中心	支持时间轴方式记录账号网络访问过程
		支持将客户多种审计条件统一管理查看
	健康统计	支持对设备转发流量统计，cpu 使用率，内存、会话、转发流量 4 项统计趋势图
		支持时间选项查阅历史使用情况
地址	IPv4 地址对象	增删改查，支持批量删除
		支持子网、地址范围、主机的地址添加方式
		支持排除地址
	IPv6 地址对象	增删改查，支持批量删除
		支持子网、地址范围、主机的地址添加方式
	地址组对象	增删改查，支持批量删除
		支持组嵌套
服务	预定义服务	支持 89 种预定义服务

	自定义服务	增删改查，支持批量删除
		支持协议类型：TCP、UDP、ICMP、其他协议号
	服务组	增删改查，支持批量删除
		支持预定义自定义服务添加
		支持组嵌套
	非标准端口配置	非标准端口 ALG（FTP、TFTP、SIP）
应用	预定义应用	显示预定义分类，支持 18 个分类
		显示分类下应用的属性：中英文名称、平台、风险级别、流行度、描述
	应用组	增删改查
	识别模式	支持修改识别模式以达到对应识别目的
		智能模式：应用引擎将尽可能多的方法识别应用流量
		快速模式：应用引擎关闭部分智能分析以提高性能
		关闭模式：应用引擎关闭
时间表	通用	增删改查，支持批量删除
		内置任何时间条目：any
	时间类型	日计划、周计划、月计划
		计时器
URL	恶意URL白名单	支持对恶意 URL 手工排除
		支持 URL 过滤黑白名单简单配置
	预定义	查看预定义 URL 分类
	自定义	增删改查，支持批量删除
关键字	自定义	增删改查，支持批量删除
数据库	嵌入式数据库	分类记录
		日志存储空间耗尽后，可滚动覆盖
日志记录	事件日志	系统关键事件日志
	管理日志	管理员操作日志
	安全日志	攻击防护日志
	IPS 日志	IPS 日志
	AV 日志	AV 日志
网站日志	访问网站日志	支持记录 html 编码格式为 UTF-8 和 GBK2312 的网页 title
		支持超链接直达客户所访问网页
		不记录无意义 URL 日志（如内嵌广告）
		查询，可自定义查询条件
	恶意URL日志	查询，可自定义查询条件