卓尔 InfoGate内容过滤网关产品白皮书

版权声明

商标声明

信息更新

本产品最新版本信息、升级信息以及相关技术文档将在本公司 www.zrinfo.net 网站上及时推出，敬请留意。

信息反馈

招商卓尔公司欢迎您通过尽可能多的渠道向我们提供尽可能多的信息，您的意见和问题都会得到我们的重视和妥善处理，请将反馈信息投递到下述地址：

深圳总公司

地址：深圳市南山区科技园高新南一路创维大厦 A 座 3A 层

电话：（0755）33300878

传真：（0755）33300870

邮编：518057

邮箱：support@zrinfo.net

网站：http://www.zrinfo.net

1. 企业信息防护需求

面对日益复杂的企业信息应用以及日益增长的互联网，企业在信息防护方面已经从基本的网络层安全（通过防火墙、防黑客等产品来实现）上升到对应用层安全的要求。特别在企业连通 Internet 的网络通道上的应用信息安全，已经越来越成为企业的安全瓶颈。

对于企业互联网网关而言，信息防护的安全需求包括病毒防范、垃圾邮件过滤以及上网过滤等方面。卓尔 InfoGate 产品的功能正是针对这些需求的。

1.1. 网关防毒的需求

瞬息万变的信息化时代，病毒事件如走马灯般在新世纪的舞台上一出出上演。病毒、黑客在不经意中与企业不期而遇，随后便是与企业网络安全防护系统之间的一场殊死搏斗。针锋相对的较量之后，许多企业面对巨大的损失不得不承认自己成为了失败者。面对惨痛的代价，他们才开始充分地、真正地意识到网络安全的重要性。问题是，如何去建设网络安全防护系统？

纵观病毒的发展史，90 年代初，绝大多数病毒的传播途径是磁盘，因而这一时期的病毒破坏力大多局限于某个区域的范围，传播的速度也相对较慢。多数企业偏好使用本地防毒软件，因为它们获取病毒样本，寻找解决方案的速度会比国际大厂商来的迅速。然而，当今病毒传播的方式已经完全改变，根据 ICSA 统计报告，磁盘传播的病毒仅仅占 1%，93%来自 email，2%来自 Internet 的下载，另有 4%来自其它途径。一只源自美国的病毒可在 24 小时内散播至全球，若遇上类似 Nimda 之类的多重渠道感染的黑客型病毒，1-5 分钟就可遍及全球。因此，如何在最短时间内取得病毒样本、分析并找出解决方案，愈发显得刻不容缓。随着全球经济运行对互联网的依赖，企业同时也面对着日趋升温的病毒和黑客的侵扰，越来越多的企业考虑通过构建网络安全系统从整体上对企业的网络实行更为有效的多重防护。ICSA 2001 年的数据表明，99%的病毒都是通过 SMTP 或 HTTP 进入用户的计算机的，全球因此造成的经济损失达到了 129 亿美元。由此，采用

在 Internet 入口就封杀 毒源 的高效益的网关防毒产品已成为企业的网络管理员的迫切需求，同时这种需求也将成为防病毒软件市场新的增长点。

根据 IDC 的报告，从 2001 年起到 2005 年，世界网络安全市场将加速发展，营销额年增长率可达 23%，到 2005 年，收入预计将超过 140 亿美元。从 2002 年中国的网络安全市场来看，总的市场规模达到 50 多亿元，呈高速增长状态。在一项有关 2003 年安全开支准备的调查中，调查对象 79%的人表示，他们所在的机构将在防火墙硬件和软件上进行投资，网关防病毒产品被排在第二的位置。

那么，企业为什么对网关防病毒产品有如此大的需求呢？首先，传统的防病毒软件无法抵御类似于 SQLSlammer 的新型蠕虫的功击，如果工作站上的防病毒软件未及时更新或被禁用了，那么病毒仍然有机会感染工作站。网关防毒产品在企业网络的入口提供了简单的 即插即忘 式的保护，病毒在进入网络之前被直接了当地拦截，同时也避免了由于病毒入侵到服务器和工作站所引起的一系列的典型问题，为企业网络提供了一个额外保护层。

其次，在病毒传播事件中（就像以前 LoveLetter、Nimda、Klez 和 SQLSlammer 所引起的），邮件服务器可能会由于超负荷而当机或拒绝服务，或者是仅仅因为害怕被感染而关机。网关防毒是唯一的一种能够减小这种风险的解决方案，因为它可以避免由于病毒传播而对邮件服务器造成的额外负载（记住，90%的病毒通过 email 传播的）。

再次，另外，从采用与防火墙集成的防病毒软件和采用网关防毒两种方案的对比来看，硬件防毒墙能够拦截供给操作系统和应用软件安全漏洞的新型蠕虫（如 SQLSlammer），而传统的与防火墙集成的防病毒软件是无法检测和清除该类蠕虫的；在新病毒的传播事件中，一台集成了防病毒软件的防火墙将消耗其大部分的资源用于拦截病毒，而将它的主要任务——防止网络攻击放在了从属的地位；从效益来看，安装与防火墙集成的防病毒软件需要一笔重大的投资，并牵涉到改变防火墙的安全规则和改变边界网络的配置。

1.2. 反垃圾邮件需求

电子邮件作为人类有史以来最自由和便捷的交流方式，为互联网的普及起到了极为重要的作用。根据 IDC 2003 年 3 月份的调查报告，2002 年世界范围内平均每天发送 310 亿封电子邮件，其中近 18%，即约 56 亿封为垃圾邮件。而根据美国著名的反垃圾邮件厂商 Brightmail 的统计，如果去掉公司内部传递的邮件，垃圾邮件在外部邮件之中所占的比例为 36%。根据中国互联网络信息中心公布的第 11 次《中国互联网络发展状况统计报告》显示，我国网民平均每周收到 16 封电子邮件，其中垃圾邮件占据了 8.3 封，垃圾邮件数量已经和合法邮件数量相当。并大有超过合法邮件的趋势。

随着电子邮件的广泛应用，电子邮件不但被几乎所有的公司所采用，而且已经象日常消费品一样进入了千家万户。作为电子邮件的日常使用者，我们对垃圾邮件都有切身的认知和体验。我们常常在不知不觉中收到大量的包含广告、黄色内容、反动宣传言论等等的邮件，其中部分还带有各式各样的病毒，即使不看内容只是删除都要花上相当的气力和时间，而如果不慎打开了邮件内容，有时会造成灾难性的损失。与此同时，企业也不得不面对接踵而至的安全威胁，邮件服务器所遭受的攻击在各类攻击中占据很大的比例，在很多企业里，垃圾邮件消耗掉超过 1/3 的邮件服务器的资源，导致网络资源的浪费，给企业带来经济上的巨大损失。

垃圾邮件可以说是因特网带给人类最具争议性的副产品，它的泛滥已经使整个因特网不堪重负。它给人类带来如下显著的问题：

1. 降低员工生产力：根据美国市场调查公司《Forrest Research》的调查，估计美国每年因为垃圾邮件而导致员工生产力降低而造成的经济损失为一千三百亿美金。
2. 对网络和服务器的影响：占用网络带宽，造成邮件服务器拥塞，进而降低整个网络的运行效率；
3. 侵犯收件人的隐私权，侵占收件人信箱空间，耗费收件人的时间、精力和金钱。有的垃圾邮件还盗用他人的电子邮件地址作发信地址，严重损害了

他人的信誉；

4. 造成法律风险：IDG 在 2001 年的一项调查中指出，10%的美国公司雇主因为员工的电子邮件问题而受到法院的传票。公司员工之间也常常因为垃圾邮件造成法律上的冲突。在美国，如果公司的员工传送垃圾邮件，接受人可以据此而控告该员工的雇主。
5. 带来安全风险：被黑客利用成助纣为虐的工具。如在 2000 年 2 月，黑客攻击雅虎等五大热门网站就是一个例子。黑客先是侵入并控制了一些高带宽的网站，集中众多服务器的带宽能力，然后用数以亿万计的垃圾邮件猛烈袭击目标，造成被攻击网站网路堵塞，最终瘫痪；
6. 严重影响 ***ISP*** 的服务形象：在国际上，频繁转发垃圾邮件的主机会被上级国际因特网服务提供商列入国际垃圾邮件数据库，从而导致该主机不能访问国外许多网络，而且收到垃圾邮件的用户会因为 ISP 没有建立完善的垃圾邮件过滤机制，而转向其它 ISP。一项调查表明：ISP 每争取一个用户要花费 75 美元，但是每年因垃圾邮件要失去 7.2%的用户；
7. 妖言惑众，骗人钱财，传播色情等内容的垃圾邮件，已经对现实社会造成了危害。

1.3. 过滤的需求

互联网时代的到来，使企业的经营、管理活动越来越依赖于网络，为在信息化社会生产中居于优先的地位，纷纷建立了企业内部局域网络，并与互联网相联。然而信息网络的使用，在给企业带来活力和商机的同时，也带来了巨大的负面影响，如果管理不当，甚至可能出现在资源重大浪费的同时，管理效率反而下降的恶果。请看以下的一些统计数据（由互联网统计中心做出）。

- 在单位有 30%-40%的上网访问活动与工作无关
- 用得最多的搜索关键字是和性有关
- 70%的有关性方面的访问都是发生在上午 9 点-下午 5 点的上班时间
- 有 37%的工作人员经常在上班时间上网
- 视频、音频等流媒体的使用从现在到 2005 年将增长一倍
- 32.6%的员工上网是没有目的的
- 大部分人在上班时间上网的时间比在家上网的时间多一倍

- 超过 36%的使用者在上班时间访问新闻、财经等网站，使用的时间占上网时间的 68%以上
- 在美国 82%的企业主管被调查时认为有必要对企业上网进行监管
- 56.5%的雇员认为在上班时间访问与工作无关的网站，会降低工作效率
- 31%的雇主已采取措施限制员工访问互联网

由此看到，互联网不受控制的使用带来的恶果主要体现在两个方面：

- 由于员工在上班时间访问了大量与工作甚至有害的网络信息，造成员工工作效率的下降和实际为企业工作时间的减少，得不偿失。企业甚至要为成为有害信息的传播渠道而付出社会的责任。
- 部分员工频繁地访问和下载与工作无关的信息，造成企业网络堵塞，使真正为了工作而上网的员工无法享用合理的网络带宽，造成资源浪费。

当然，由于访问过多不合法站造成病毒的泛滥等问题，也是属于比较大的危害。

另外，据中国互联网中心 CNNIC 统计，在上网用户中 23 岁以下的青少年用户占 53%，并以最快的速度增长，互联网对青少年产生了巨大的吸引力，人们可以通过互联网学习丰富的知识、查阅丰富的信息，提高生活的质量。但由于互联网的开放性及网上信息优劣参差不齐，使得网上各种不良信息也随之泛滥，特别是反动、色情、暴力等有害信息极大地危害着社会的稳定和青少年的身心健康，而法轮功邪教组织、民运分子、各种敌对势力也利用这一舞台，对我国进行各种宣传攻势和渗透演变。人们在欢迎网络技术的同时，也对网上不良信息对人们的负面影响产生了担忧。特别是在学校，由于上网学生年龄较小，好奇心强，容易受到不良信息的影响，所以加强网络管理，采取有效的技术手段防止学生访问有害网上信息是每一个上网学校的重要问题。

1.4. 机密信息防护的需求

谁最有可能盗取企业的数据？既不是政府机构，也不是来自竞争对手的商业间谍。最主要的嫌疑犯是时刻在企业内部的人　　企业的雇员。

2000年，软件主管 Jeffrey Chang 离开了当时工作的台湾芯片设计厂商 DLink公司，重返之前所在的 VIA 科技公司。但去年 12 月 Jeffrey Chang 却站在了台北的被告席上，他涉嫌将 D-Link公司的软件代码泄漏给 VIA 公司。一条强有力的证据可以证明这一点：他就职于 D-Link公司的同时，VIA 公司仍旧付给他薪金，这是来自 VIA一位高层管理者的可靠消息。

这些案件强调在最近几年公司内部信息泄漏给竞争对手的事情，多数被怀疑是自己公司的雇员所为。其实不难看出：间谍不再需要像 James Bond 那种拥有高超熟练技术的类型，现在的商业间谍很可能是在公司中地位低微的雇员，他们使用那些可以在任何亚洲计算机商业区都可以找到的廉价的小工具。

以完全数据显示，问题通常来源于企业的雇员，并非工业间谍。 Kroll 驻中国风险管理经理 Samuel Porteous说。无论怎样，雇员总能接触技术工具，并可以从中抽出大量有价值的信息，这将极大地损害雇主利益。

尽管损失是难以估量并且惨重的。但很少有公司愿意报告他们最终损失的情况以及在自身安全性上的疏忽。但根据 2002年 Price-Waterhouse-Coopers的一次较为全面的调查报告中显示：全世界 40%的公司由于此种原因导致其造成的平均经济损失在 350,000美元至 400,000 美元之间。而这 40%的公司之中有些是已经公布了公司内部的事件，而有些仅是被怀疑造成了损失但并没有得到证实。这些案件多数发生在北美洲，但是亚洲也占据了 13%的份额，成为了此类案件的第二高发区。

专家认为在亚洲的商业间谍行为，范围很可能更广。因为像 PWC这样的调查经常不包括那些小型的软件公司或者客户数据库的被盗部分。而这部分恰好构成了亚洲地区最主要的损失。

同样，亚洲的公司更不可能及时向有关部门反映情况，台北私人咨询服务办公室负责人 Moray Taylor-Smith 说。在这个地区的公司更喜欢自己内部解决问题并且很要面子。例如，去年香港计算机应急行动小组报告存在超过 900 个安全漏洞，但是只有不到 2%的公司向权力机关报告这些安全漏洞。

导致问题的其他因素：在这方面亚洲缺乏一种强大的法律框架，以严惩那些数据偷窃行为；开展外包业务，实现更牢固的控制数据，以及树立相关的知识产权保护意识。在新加坡，很多公司都不将他们的产品申请专利，这便导致很难去保证知识产权，曾当过侦探如今开办技术调查公司的 Kelvin Low 说。

商业间谍的根基也在不断提高。过去，高水平高智能的偷窃案件大多数情况发生在北美洲，因为那里集中了大规模的研究与开发设备。但近年来随着亚洲特别是中国 R&D开支的大量增加，根据巴黎发达国家的经济合作与发展组织调查表明： 2001年中国的 R&D花费大约为 600 亿美元，这一数字使中国成为继美国和日本之后在 R&D 花费方面的第三大国。

根据美国反间谍活动办公室的调查显示：窃取工业机密的大多数人往往不是专业的计算机人士。他们一般采用的方法是使用最简单的电子邮件、传真或者电话。那些雇员通过晚归并趁机影印文件的日子已经一去不复返了。现在他们更大程度上仅需要短短的几分钟，使用简单的邮件软件即可完成这项工作。而使用日益广泛的即时通讯软件更是为这些雇员提供了帮助。

即使许多公司在与雇员鉴定的契约中包含禁止将公司内部信息泄漏给竞争者的条款，执行起来却毫无成效。不仅证据难收集，有关安全专业人士表示：目前亚洲涉及商业间谍行为的法律还十分不健全，一次成功检举的机会很低。台湾的 Taylor-Smith 说： 以我多年的经验，这种仅一次起诉就能成功的机会只有 50%。 而且，与美国关于间谍方面的法律相比，台湾这方面的法律还不是十分明朗及透明。Taylor-Smith 说：就台湾而言，你得到的赔偿远不能弥补你的损失。而在美国就市场份额而言，原告可以得到和损失同样多的补偿。

2. 产品简介

正是因为对企业信息安全威胁的了解，特别是在企业信息网络 Internet 网关连接处的安全需求，针对企业对网关病毒防范的需求，为了企业在 Internet 网关能够成功地进行病毒防范、垃圾邮件过滤、上网过滤以及机密信息防范，招商卓尔公司开发了国际领先的内容过滤网关 卓尔 InfoGate 整合式内容过滤安全网关，为企业提供了网关级的企业信息内容防护。

2.1. 设计思想

针对企业信息网络 Internet 网关信息内容防护要求而设计的卓尔 InfoGate 整合式安全网关，在设计阶段就充分考虑了企业网络环境和网关信息过滤的特殊需求。卓尔 InfoGate 产品的总体设计原则体现在：

- 实施简便，无须复杂的安装。
- 无缝地接入企业网络，能够在企业网的网关处和部门级网络连接处实施。
- 基本不影响网络使用速度
- 能够进行集成式的病毒防范、垃圾邮件过滤、上网过滤以及机密信息防范，并且能够进行模块化配置。
- 提供详细的过滤统计报告。
- 能够方便地远程管理和控制。

2.2. 实现原则

支持路由及网桥模式通用的结构设计

为了适合企业的各种网络环境，同时在实施安装上为客户提供最大的方便性，卓尔 InfoGate 内容过滤安全网关采用路由以及网桥模式通用的网络结构设计。采用网桥能够将卓尔 InfoGate 产品实施很多位置，如网关处在防火墙或路由器后面、或者在子网和主干网络的连接处等。网桥结构的卓尔 InfoGate 产品在实施时不需要改变任何的网络结构，也不需要改变任何桌面 PC 的网络设置。对于需要网关防护的企业，在实施卓尔 InfoGate 产品可以使用路由模式，采用路由模

式的卓尔 InfoGate 产品能够在 Internet 连接处建立起应用层的过滤网关。

模块式的内容过滤功能

卓尔 InfoGate 整合式内容过滤安全网关采用模块化功能结构。对于病毒防护、垃圾邮件过滤、上网 Web 过滤以及机密信息防范功能，卓尔 InfoGate 产品能够根据用户的需求来配置不同的功能模块，是卓尔 InfoGate 产品能够很好地适应用于的需求。

采用国际领先的防病毒引擎

卓尔 InfoGate 内容过滤安全网关采用世界第四大防毒厂家 Sophos 公司的防毒引擎。Sophos 公司。Sophos 公司是世界领先的防病毒厂家。从 80 年代末起，Sophos 公司致力于防病毒技术的开发，并成功地为超过两千万客户提供了病毒防范服务。2001-2002 年度，Sophos 防毒产品销售增长超过 50%，通过分支机构及合作伙伴服务 150 个国家的客户。

Web 管理模式

采用基于 Web 的管理界面设计，为用户提供了方便的管理手段。同时，卓尔 InfoGate 在产品设计时，充分考虑了统计报表对安全产品的重要性，保证了产品能够通过其 Web 界面提供详尽的统计数据。

3. 产品功能描述

卓尔 InfoGate 内容过滤网关围绕企业网络网关信息过滤的需求设计其功能，从而保障了企业网络在病毒防范、垃圾邮件以及 Web 过滤的需求。卓尔 InfoGate 内容过滤网关的主要功能包括：病毒过滤功能，垃圾邮件过滤功能、Web 过滤功能、泄密防范功能、防火墙功能、VPN 功能和日志统计功能。

卓尔InfoGate内容过滤安全网关产品

3.1. 病毒过滤功能

卓尔 InfoGate 内容过滤网关提供强大的病毒防范功能。卓尔 InfoGate 使用了世界领先的防毒厂家 Sophos 公司的防毒引擎，提供了强有力的病毒防范功能。

协议支持

卓尔 InfoGate 防毒功能支持对通用的 Internet 协议进行病毒扫描。目前，卓尔 InfoGate 支持的协议包括：HTTP、POP3、SMTP、IMAP、FTP、 ESMTP 和 NETBIOS。通过在网关处对这些协议的病毒扫描，卓尔 InfoGate 为企业内部提供了强有力的病毒保护。

自动更新

卓尔 InfoGate 防毒功能每天自动更新病毒特征库，及时获取最新的病毒信息，从而能够在最快的时间内为企业提供第一时间的病毒防范。同时，卓尔 InfoGate 防毒功能定期更新 Sophos 防病毒引擎，使卓尔 InfoGate 防毒功能具有扫描最新病毒品种的能力，并不断提高病毒扫描的效率。

病毒扫描

为了提高病毒扫描效率，卓尔 InfoGate 防毒功能提供给客户进行扫描配置的选项，允许产品对相关的文件类型不进行扫描，同时对某些文件类型自动清除，这样提高了病毒扫描的速度。

在线杀毒

在提供网关级病毒防范的同时，卓尔 InfoGate 产品还提供先进的在线杀毒功能，帮助最终用户对其桌面 PC 或者服务器进行进行全面的病毒查杀，从而将从其他途径进入到网络内部的病毒进行清除，确保了内部网络的安全性。

3.2. 垃圾邮件过滤

3.2.1. 高度准确性

卓尔 InfoGate 产品的反垃圾邮件引擎采用评级系统通过一系列测试对电子邮件进行评估。 它可以高度准确地识别出垃圾邮件，并且可以捕获所有垃圾邮件中高达 75%的垃圾邮件，垃圾邮件未被识别出来的错误肯定率小于 0.1%其默认规则由卓尔公司维护，无需设置规则就可以高效检测出垃圾邮件。

3.2.2. 等级评定和识别

卓尔 InfoGate产品使用一种基于全面的规则集的等级评定系统来判断某个电子邮件是否为垃圾邮件。 针对每个电子邮件运行数百个规则，每个规则都有一个负的或正的分数。得负分数的规则表示邮件为合法邮件，得正分数的规则表示邮件为未经请求的非法邮件。 将所有分数相加，就能够得出每一封邮件的 总

体垃圾邮件级别 。 采用一种遗传算法 (genetic algorithm) 对分数进行优化处理，并使用数百万个垃圾邮件和非垃圾邮件存档消息来评估每一个规则的分数。由于电子邮件是企业体系结构中的关键组成部分，因此对于每一个进行垃圾邮件防护的供应商来讲，防止错误地识别垃圾邮件至关重要。在当今反垃圾邮件的斗争中，评级系统起着基石的作用，它们比传统的匹配技术更为准确，在检测要识别的垃圾邮件时它可以检测到邮件里很多细节的部分，从而保证邮件识别的准确率。

3.2.3. 扫描邮件系统

卓尔 InfoGate 产品通过扫描进出企业信息网络的电子邮件（通过 SMTP, POP3协议等）减少了企业在垃圾邮件的成本，从而极大降低网络资源的损耗。在 Internet 网关处检测垃圾邮件可以防止其进入网络并浪费宝贵的网络资源，同时，通过减轻员工阅读无用邮件的负担可以提高员工的生产效率。 此外，InfoGate 还可防止接收非法邮件内容。

3.2.4. 垃圾邮件的处理方式

卓尔 InfoGate产品提供灵活方便的垃圾邮件处理方式。企业的管理人员可以根据企业内容垃圾邮件的情况来采用不同的垃圾邮件处理方式。对于 SMTP, 管理人员可以设置将垃圾邮件拦截，并且只作日志纪录或者定时发送报告邮件。其他的处理方式包括将垃圾邮件的信息发送给最终用户，同时在邮件标题上进行提示。这样最终用户就可以在邮件客户端软件（如 Outlook, Foxmail等）里创建 收件箱 规则，自动对潜在的垃圾邮件进行过滤。

3.2.5. 多种检测方法

利用基本的默认规则集过程，卓尔 InfoGate产品通过不同的检测方法对用户收到的每一封电子邮件进行检查。

- 完整性分析 卓尔 InfoGate对每一封邮件的邮件头、版面和组织进行检查，以识别垃圾邮件的一般特征。 在单次传递过程中，高级模式匹配

引擎同时应用数百个算法，然后确定其可能得分以判断该邮件是否为垃圾邮件。 这种用于检测垃圾邮件的方法非常准确。

- 前瞻性检测 - 前瞻性检测通过一系列内部测试来判断某个邮件是垃圾邮件的可能性，每一个测试都有相应的分值，以便降低错误率。 强大的前瞻性检测功能确保 卓尔 InfoGate能够前瞻性地工作，以保护您的环境免受垃圾邮件的威胁。
- 内容过滤 - 该功能可以用来识别电子邮件中的关键字或关键短语，从而判断其是否为垃圾邮件。 管理员可以输入字或短语来创建被禁止内容的列表。
- 黑名单和优先名单支持 - 管理员定义的黑名单会拦截住管理员认为是垃圾邮件发件人所发送的电子邮件，而管理员定义的优先名单允许管理员指定域中的电子邮件的通过。 同时，卓尔 InfoGate支持对 SMTP连接的 RBL检测。
- 反垃圾邮件攻击 卓尔 InfoGate 产品提供完整的反垃圾邮件攻击功能。通过对邮件连接建立数量和并发数量、邮件连接收件人数量和邮件发送数量的限制，能够充分地保护邮件服务器。卓尔 InfoGate支持对 SMTP连接的反向 DNS检测。这样可以防止来自无域名的 IP地址的攻击（大多垃圾邮件发送是使用这样的 IP地址）。

3.3. Web 过滤功能

卓尔 InfoGate产品提供强大的上网监控功能。卓尔 InfoGate产品遵循了 多重过滤，多重保护 的原则，通过对内容和网址的监控，对内容不良的网站实行过滤，从而实现对企业内部员工以及校园内学生的上网进行监控的功能。同时，卓尔 InfoGate提供了对网页嵌入应用和下载文件的拦截功能。

3.3.1. 内容过滤

关键字过滤

管理员可以设置敏感关键字或敏感关键字组合，对于出现相关关键字或关键字组合的网页进行封堵，不允许访问这些网站。同时，管理员也可以设置关键字

及组合的白名单，对于出现相关关键字的网页予以通过。

关键字权重过滤

管理员可以设置关键字权重，也可以使用系统预配置的不同类别的关键字权重。同时，管理员设置权重阀值。当网页内容里出现的关键字权重相加或相减得出的权重大于阀值，网页将被封堵。系统提供三个级别的缺省阀值：少儿级别（50分），青少年级别（100分），青年级别（160分）。管理员可以根据自己网络的特点，设定相关的阀值。

贝叶斯统计模型

贝叶斯统计模型是统计归纳的数学模型，依赖对经验的学习，到达对未知事物进行判断的能力。卓尔 InfoGate产品应用贝叶斯统计模型，通过对不良网站词汇统计信息的学习，能够准确地辨别不在黑名单上的不良网站，防止对新出现不良网站的访问。

3.3.2. 网址过滤

管理员通过配置网站服务器、网址 URL和 IP地址的黑白名单，达到对不良网站过滤的功能。同时，卓尔 InfoGate提供预定义的不同类型黑名单，并定期更新相关的黑名单。在黑白名单里配置网站服务器，卓尔 InfoGate会对整个网站（包括其下属网页）进行监控。

3.3.3. 文件及应用过滤

管理员可以对通过 HTTP协议下载的文件类型，以及嵌入网页的应用类型进行过滤，从而防止恶意程序的破坏，减少终端和网络的安全风险。支持对 BT、电驴、QQ, UC, 网易泡泡、Skype、网络游戏等应用的拦截，支持针对用户分组的应用控制，支持分时间段的应用控制，支持对 BT、电驴、QQ, UC, 网易泡泡、Skype、网络游戏等应用的流量控制。

3.3.4. 上网策略设置

对于不同用户不同的上网管理需求，卓尔 InfoGate 产品允许网络管理员将不同用户进行分组管理。针对不同的用户组，管理员可以制定不同的上网管理策略，其中包括不同的关键字黑白名单、权重关键字、站点以及网址的黑白名单等等。这样就能够根据企业内部不同用户的具体情况，对用户进行全面的上网管理。

3.4. 泄密防范功能

卓尔 InfoGate 产品提供了全面的机密信息防范功能，能够帮助企业、政府等单位对内部的机密信息进行保护。卓尔 InfoGate 泄密防范功能包括对邮件、Web 信息发送、MSN 以及 QQ 的信息过滤、监控或拦截功能。

3.4.1. 邮件信息防护

针对通过 SMTP 协议向外发送的电子邮件，卓尔 InfoGate 采用了特定的邮件内容过滤技术，从最大程度上确保了企业电子邮件的正常和合法的使用。

发送限制

卓尔 InfoGate 提供了邮件发送限制的功能。由于企业信息网络上邮件发送主要依赖于 SMTP协议，因此针对 SMTP协议，卓尔 InfoGate采用了逐层限制的方法为企业内部的管理员提供了限制内部邮件发送的功能。通过逐层限制技术，卓尔 InfoGate能够在每一个 SMTP 的发送过程对邮件发送每一步的内容进行管理。这其中包括邮件的发件人、发件人 IP、收件人、收件人域名等方面进行管理，从而保证邮件的发送符合企业的管理规范。

邮件内容搜索

对于企业向外发送的邮件，如何了解其内容并及时拦截不符合企业信息安全管理规范的邮件是企业机密信息过滤中的关键点。卓尔 InfoGate 采用了全面的邮件内容搜索技术，能够对邮件的正文、附件进行全面的关键字搜索。对于邮件的

附件，卓尔 InfoGate 能够对 Word、Excel、 Powerpoint、PDF、HTML、Txt 等文件格式进行识别。卓尔 InfoGate 是通过对上述文件格式结构的深入解析来识别文件格式的，而不是简单地通过文件的扩展名来识别。同时，卓尔 InfoGate 能够将 Word、Excel、Powerpoint、PDF、HTML 等文件格式中的文本提取出来，然后进行关键字过滤。在后面的版本中，卓尔 InfoGate 将支持更多文件格式的关键字过滤。

多种处理方式

卓尔 InfoGate 提供了对被过滤邮件的多种处理方式。对于限制发送的邮件，卓尔 InfoGate 会拦截邮件的发送，并回复错误信息给 SMTP 邮件客户端。对于被内容过滤的邮件，被过滤掉的邮件将被警告信所代替。管理员可以设置将警告信发送给发件人、收件人或者企业的管理者（需要设置邮件地址）。

3.4.2. Web 发送过滤

卓尔 InfoGate 提供了专门针对 Web 信息发送（也就是 Web POST 方法）的内容过滤技术。通过对特定网站的访问限制功能，卓尔 InfoGate 提供了限制终端用户随意通过 Web 发送邮件或者其它言论的行为。同时，卓尔 InfoGate 提供对终端用户发送信息的内容过滤，即关键字过滤。能够帮助企业管理者阻止终端用户将企业机密信息发送到企业的外部。另外，卓尔 InfoGate 还提供通过 Web 上传文件的限制。这样就能够控制终端用户通过 Web 发送邮件附件。

3.4.3. MSN 过滤

针对 MSN 可能带来的信息泄漏隐患，卓尔 InfoGate 提供了基于 MSN 的过滤功能。采用 MSN 透明代理的方式，卓尔 InfoGate 能够在保证内部终端用户正常使用 MSN 的同时，对通过 MSN 发送的信息进行监控和过滤。同时能够阻止用户通过 MSN 发送文件。对于 MSN 通讯，管理员可以设置基于 IP 地址的黑白名单。对于在黑名单上的用户，使用 MSN 将被禁止，所有来自于这个用户的 MSN 通讯将被拦截。对于在白名单上的用户，MSN 通讯将不会被过滤和记录。

3.4.4. QQ 拦截

卓尔 InfoGate 提供对 QQ 进行拦截的功能。卓尔 InfoGate 采用独创的基于特征的访问控制技术，对 QQ 应用实现全面的拦截。对于 QQ 通讯，管理员可以设置基于 IP 地址的黑白名单。同时，管理员需要设置是启用黑名单还是白名单。如果启用黑名单，那么在黑名单上的用户使用 QQ 将被禁止，其余用户可以使用 QQ。如果启用白名单，那么在白名单上的用户允许使用 QQ，其余用户被禁止使用 QQ。

3.5. 应用控制功能

卓尔 InfoGate产品针对目前 Internet网络的应用。研发出有效控制 BT、电驴、QQ、UC、网易泡泡、Skype、网络游戏。通过对它们的协议分析，获取不同应用协议的特征码，进行管理。

卓尔 InfoGate产品针对应用的控制，可以基于对象的管理、可以对单一用户进行管理、也可以基于网络段、网络范围、用户组等多种形式进行管理。

卓尔 InfoGate产品针对应用的控制，可以根据对象使用的不同时间范围进行管理，用以高效有限的网络资源。

卓尔 InfoGate产品针对应用的控制，可以网络用户身份的不同，灵活分配使用网络应用的带宽，对于过大的占用带宽进行监控、管理。

3.6. 防火墙功能

卓尔 InfoGate 产品提供基本的网关防护功能，能够帮助企业、政府以及学校在其网络连接 Internet 处设置基本的安全保护措施。

3.6.1. 接入管理

卓尔 InfoGate 防火墙支持多个 LAN、多个 WAN、DMZ、VPN 接口的定义，可以根据企业的实现需要，定义出支持双 WAN 线路的接口。

卓尔 InfoGate 防火墙支持基于 ADSL、VDSL、DHCP Server/Client、静态路由、NAT、透明网桥的接入。

3.6.2. 访问控制技术

通过卓尔 InfoGate 防火墙，能够将网络分成外网、内网和非军事区（DMZ）三个部分。管理用户可以在每个区域设置不同的用户和用户组。同时，管理用户还可以设置不同的网络服务。然后，根据内部网络应用以及企业网络的安全需求，企业的管理用户可以配置不同的访问控制策略，来限制用户/用户组对网络服务的访问。

通过设置访问控制功能，企业能够对内部网络的 Internet 访问进行很好地控制。同时，企业能够很好地防范来自外部不安全网络的不安全访问。另外，通过设置非军事区，能够帮助企业安全地放置其 Web 服务器、邮件服务器等 Internet 应用服务。

通过卓尔 InfoGate 防火墙，能够基于客户的 IP 和 MAC 地址的绑定，有效控制基于对外部网络的访问。

通过卓尔 InfoGate 防火墙，能够对用户和对象，进行分组管理、基于时间段的管理、基于流量的管理。

3.6.3. 攻击防范技术

支持强大的攻击防御功能，提供 DoS/Ddos、Land、Franggle、WinNuke 、Ping of Death 、IP Spoofing 、SYS Flood、ICMP Flood 、UDP Flood、ARP 欺骗等恶性攻击，确保内部网络安全。

3.6.4. 入侵检测技术

卓尔 InfoGate 防火墙内置基于状态的特征检测技术根据攻击的特征模式对网络报文进行匹配。通过与定义的入侵检测规则库进行匹配，发现潜在的攻击，对其进行拦截。

卓尔 InfoGate 防火墙内置基于协议异常分析检测技术，针对网络协议自身的缺陷，利用网络协议的有序性，发现异常的序列。大大提入侵检测的准确度。

卓尔 InfoGate 防火墙内置基于流量异常分析检测技术，通过网络流量分类统计的方法对被保护网络的流量进行检测，超过定义阀值的流量将被认为是非法流

量。

3.6.5. 网络地址转换

对于采用路由模式的卓尔 InfoGate 防火墙，能够提供管理用户设置网络地址转化功能。通过网络地址转换功能，企业能够隐藏其内部网络的结构和设置。

3.7. VPN

卓尔 InfoGate 支持基本的 VPN 功能。提供基于 IPSEC 通用协议的 VPN 功能，卓尔 InfoGate 提供了通过 Internet 连接两个局域网的功能。通过完善的加密协议，两个局域网之间的通讯将被完全加密，从而保证了通讯的保密性。

3.8. 日志统计功能

卓尔 InfoGate 提供详细的信息过滤日志。对于每一种协议，卓尔 InfoGate 提供访问纪录，让用户能够了解网关处 Internet 访问的具体情况。同时，卓尔 InfoGate 还提供详尽的过滤统计信息（如病毒、垃圾邮件等），对于每种协议的过滤行为进行全面的统计，并提供过滤后的相关邮件、文件等信息，从而为用户对过滤的情况进行分析提供了帮助。

4. 产品型号

卓尔 InfoGate 产品是一款硬件的内容过滤网关。针对不同企业、政府以及学校的网络规模以及网络应用特点，卓尔 InfoGate 产品提供以下各种型号的卓尔 InfoGate 硬件设备：

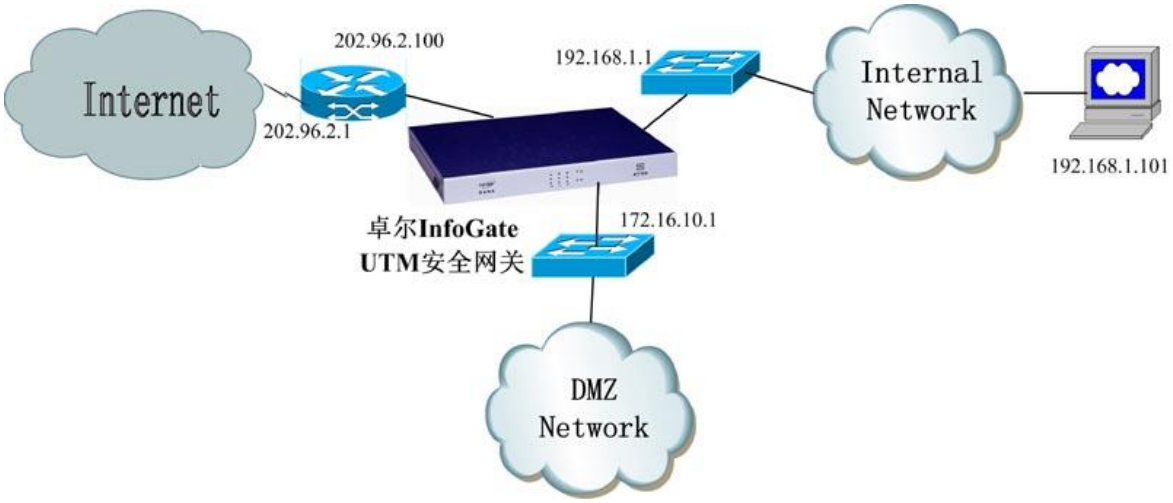
- ZR-IG-50/50A：路由或网桥模式，50 用户数，1U 机型。该产品是一款紧凑的、易于安装管理、适合小型用户或分支机构信息安全需求的产品，可取代代理服务器或上网共享器用于网关连接。
- ZR-IG-100/100A：路由或网桥模式，100 用户数，1U 机型。该产品是一款紧凑的、易于安装管理、适合中小型用户或分支机构信息安全需求的产品，可取代代理服务器用于网关连接。
- ZR-IG-200/200A：路由或网桥模式，200 用户数，1U 机型。该产品是一款紧凑的、易于安装管理、适合中型企业信息安全需求的产品。多采用网桥型，安装于企业 Internet 连接处。
- ZR-IG-300/300A：路由或网桥模式，300 用户数，1U 机型。该产品是一款紧凑的、易于安装管理、适合中型企业信息安全需求的产品。多采用网桥型，安装于企业 Internet 连接处或保护内部邮件/Web 服务器。
- ZR-IG-500/500A：路由或网桥模式，500 用户数，1U 机型。该产品是一款紧凑的、易于安装管理、适合中型企业信息安全需求的产品。多采用网桥型，安装于企业 Internet 连接处、部门子网连接处或保护内部邮件/Web 服务器。
- ZR-IG-1000/1000A：路由或网桥模式，1000 用户数，2U 机型。该产品是一款紧凑的、易于安装管理、适合大型企业信息安全需求的产品。多采用网桥型，安装于企业 Internet 连接处、部门子网连接处或保护内部邮件/Web 服务器。
- ZR-IG-2000/2000A：路由或网桥模式，2000 用户数，2U 机型。该产品是一款紧凑的、易于安装管理、适合大型企业信息安全需求的产品。多采用网桥型，安装于企业 Internet 连接处、部门子网连接处或保护内部邮件/Web 服务器。

5. 产品应用方案

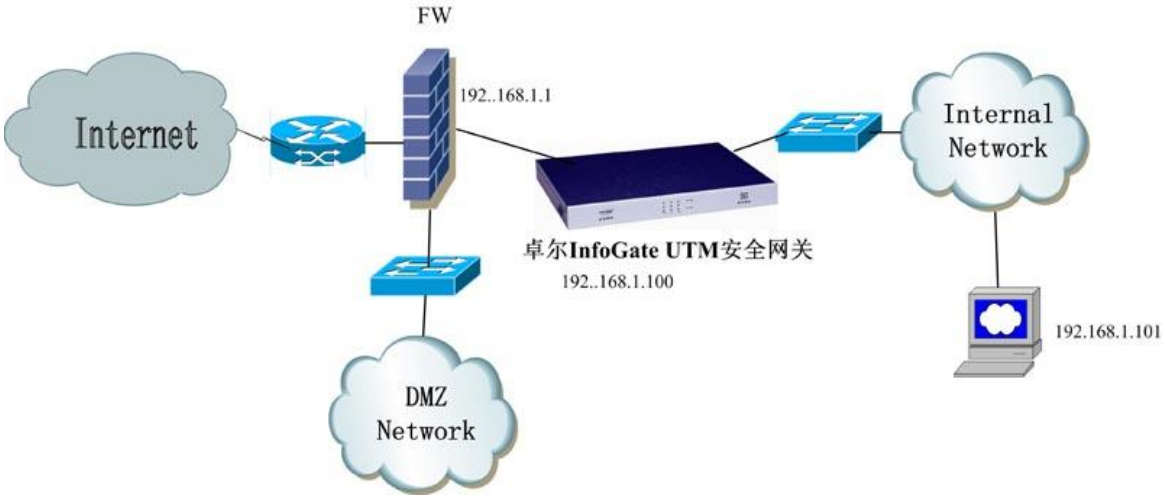
卓尔 InfoGate 内容过滤网关是针对企业网关信息过滤需求设计开发的产品。针对企业网络的特点，卓尔 InfoGate 产品在应用时有三种方案：

l 全网级应用防护方案：对于需要对整个内部网络提供安全保护的企业，建议将卓尔 InfoGate部署在网关或网关的后面（网桥方式）。部署只需非常简单的配置，就可以对进出网关的网络访问进行内容过滤与监控。

Ø 路由模式：在路由模式中，卓尔 InfoGate的三个网口连接着不同的子网，卓尔 InfoGate承担着连接这三个子网的任务。管理用户需要配置内网、外网以及 DMZ区的借口。通常而言，如果用户使用卓尔 InfoGate做为连接互联网的网关，卓尔 InfoGate采用的一般是路由模式。

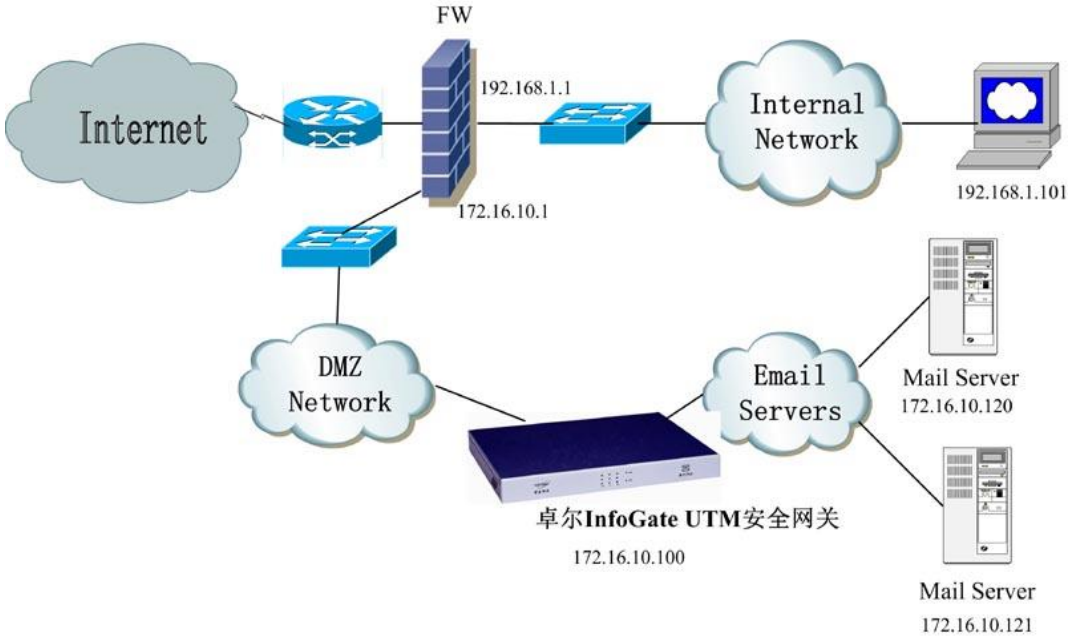


Ø 网桥模式：如果采用网桥模式，卓尔 InfoGate的两个网口（内网口和外网口）连接的是同一网段的两个部分。管理用户需要为卓尔 InfoGate配置一个网桥 IP。这个 IP也是属于卓尔 InfoGate连接的这个网段的。通常情况下，作为网桥的卓尔 InfoGate产品被部署在防火墙或者路由器的内部。



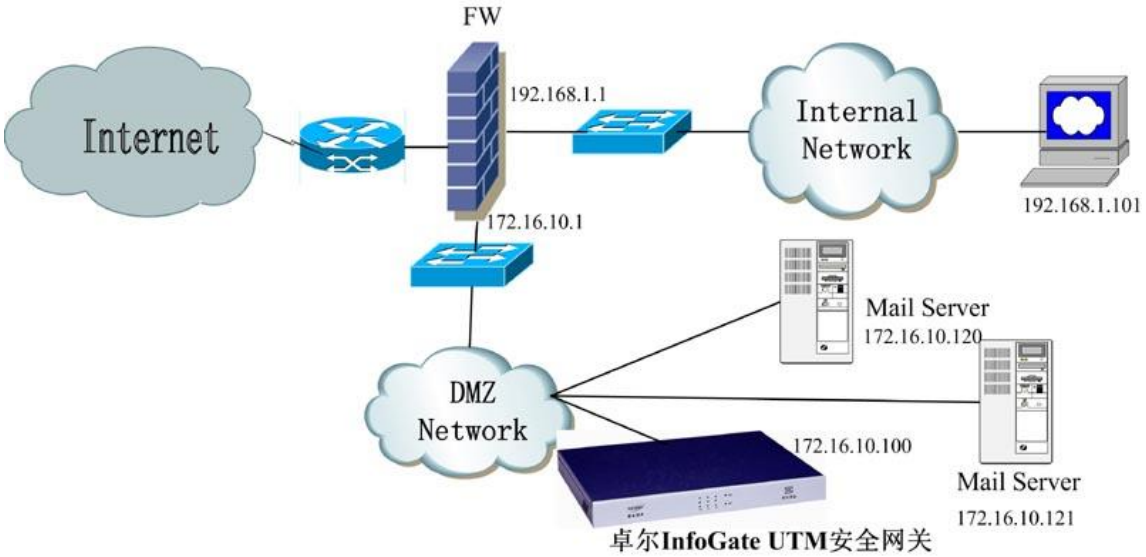
邮件网关

- 物理网桥模式：在物理网桥模式下，卓尔 InfoGate 被部署在邮件服务器（或者邮件服务器群）前，通过物理的网络连接为邮件服务器提供保护。管理用户需要为卓尔 InfoGate 配置一个 IP 地址。卓尔 InfoGate 通常和邮件服务器在同一个网段内。



- 逻辑 **MTA** 模式：采用逻辑 MTA 模式，卓尔 InfoGate 可以作为企业邮件服务器的 MTA。进入企业的邮件首先进入卓尔 InfoGate，经过过滤之后，再转发到企业内真正的邮件服务器。管理用户需要在企业的 DNS 服务器里设置相关的 MX 纪录，然后在卓尔 InfoGate 里设置需要保护的邮件域。这样就能够让卓尔 InfoGate 保护企业的邮件服务器。被保护的邮件服务器可以在不同的网段，只要能够通过网络访问就可以了。管理用户需要为卓尔 InfoGate 配置一个内网口的 IP 地址。卓尔

InfoGate 通过内网口连接到企业网络上。



6. 产品优势阐述

卓尔 InfoGate 整合式内容过滤安全网关是国内领先的网关级信息过滤产品。产品设计借鉴了国际相关领先产品的功能，使用了国际防毒著名厂家 Sophos 公司的病毒引擎，同时结合招商卓尔公司特有的协议过滤平台，为企业提供了优秀的病毒防范、垃圾邮件过滤、上网过滤以及机密信息过滤功能。与其他相关产品比较，卓尔 InfoGate 的产品优势明显。

模块化内容过滤

卓尔 InfoGate 产品提供了病毒防范、垃圾邮件过滤、上网过滤以及机密信息过滤等内容过滤功能。采用灵活的模块化设计，卓尔 InfoGate 产品能够根据用户的安全需要，方便地配置不同过滤功能的组合，最大化地满足用户的需求。

病毒扫描效果优异

卓尔 InfoGate 内容过滤网关在病毒防范方面采用了世界领先的 Sophos 防毒引擎，为企业网关提供了卓越的病毒扫描能力。同时，卓尔 InfoGate 及时更新病毒特征库和病毒引擎，能够将最新的病毒阻止在企业的内部网之外。卓尔 InfoGate 目前提供对 HTTP、POP3、SMTP、IMAP、FTP 和 NETBIOS 协议的扫描，并会在以后的版本里提供更多的协议扫描，从而在 Internet 网关处提供了全面的病毒防范能力。

多重过滤的反垃圾邮件

卓尔 InfoGate 内容过滤网关在针对日益复杂的垃圾邮件问题时，采用了多重过滤的反垃圾邮件措施，是卓尔 InfoGate 产品能够具有过滤率高、误判率小的特点。同时，对于不断变化的垃圾邮件，能够调整相对应的过滤策略，以确保卓尔 InfoGate 产品能够不断地适应垃圾邮件的变化。

灵活的上网策略设置

针对企业内部复杂的上网管理需求，卓尔 InfoGate 产品提供了灵活的上网策

略设置，帮助管理用户对企业内部的用户进行分组的策略管理。卓尔 InfoGate 产品能够针对不同的用户组，采用不同的上网管理策略，使企业能够全面地管理内部的上网行为。

独特的机密信息防范

卓尔 InfoGate 前瞻性地提供了机密信息防范功能，为企业、政府等行业提供了保护信息安全的有力手段。通过特有的文件文本检索技术，卓尔 InfoGate 提供了对邮件内容的全面过滤。同时，卓尔 InfoGate 提供的 Web 信息发送过滤技术全面地防范了 Web 邮件的使用。MSN 过滤和 QQ 拦截功能提供了国内领先的即时通讯管理功能。

实施维护简单

因为卓尔 InfoGate 内容过滤网关采用透明网桥的硬件网络设备形式，在实施上十分简单。用户在实施卓尔 InfoGate 时，只要将产品安装相应的应用方案接入网络结构中就可以了，不需要改变网络原有的网络结构，也不需要在用户终端上做任何的配置修改，使卓尔 InfoGate 在使用上对最终用户是完全透明的。另外，卓尔 InfoGate 采用基于 Web 的远程管理模式，在管理很简明方便，不会增加管理员的维护工作量。

产品性能稳定

卓尔 InfoGate 产品采用硬件设备的形式，与安装在性能不稳定的 Windows 操作系统上的软件产品相比，产品性能非常稳定，保证了网络用户的上网稳定。使用了性能稳定的硬件安全设备，减少了产品当机、死机的情况，也减少了企业网络管理员的维护工作。

上网影响小

卓尔 InfoGate 产品采用了成熟的过滤平台技术，充分利用各种协议提供的功能，对扫描的内容进行了优化，提高了终端用户的网络访问速度，从而在一定程度上抵消了因为扫描而带来的上网访问速度延缓。

7. 技术支持与服务

7.1. 服务宗旨

为客户提供优质、高效、快速的技术支持服务，保证我们的产品在您的网络环境中连续、稳定、高效地运行，以客户满意为导向，是招商卓尔公司技术支持服务的宗旨。

7.2. 服务体制

招商卓尔公司拥有经验丰富的售后支持工程师，他们将按照 售后服务流程通过服务热线电话及传真等通讯设施为客户提供多方式、多渠道的技术支持服务，必要时，还可以提供现场服务。此外，招商卓尔公司还提供内容丰富的资料供用户参考。完善的组织结构、经验丰富的工程师及先进的通信手段，为我们的服务提供了保障。

注：由于产品升级而与上述介绍不符的，以当前产品为准，恕厂家不另行通知。