



# 瑞星防毒墙技术白皮书

——for RSW—1000P

This is an abstraction of RISING antivirus wall. It covers all functionalities and performance parameters briefly. If you need a detailed guide of RISING antivirus firewall, you should read the user manual instead.



# 目录

第一章	防毒墙系统简介.....	- 1 -
第二章	瑞星防毒墙产品功能.....	- 2 -
2.1	基本系统功能.....	- 2 -
2.1.1	灵活适用的工作模式.....	- 2 -
2.1.2	ADSL+PPPoE.....	- 3 -
2.1.3	强大的路由功能.....	- 3 -
2.1.4	管理员分级.....	- 3 -
2.1.5	远程管理.....	- 3 -
2.1.6	终端命令行管理.....	- 3 -
2.1.7	在线实时升级.....	- 4 -
2.2	防毒系统功能.....	- 4 -
2.2.1	强大的查杀病毒能力.....	- 4 -
2.2.2	快速过滤网络蠕虫.....	- 4 -
2.2.3	内容过滤.....	- 4 -
2.2.4	支持的文件格式.....	- 4 -
2.3	防火墙功能.....	- 5 -
2.3.1	状态包过滤.....	- 5 -
2.3.2	访问时间控制.....	- 5 -
2.3.3	MAC地址绑定.....	- 5 -
2.3.4	带宽管理.....	- 6 -
2.3.5	安全策略.....	- 6 -
2.3.6	策略分析.....	- 6 -
2.3.7	双向网络地址变换.....	- 6 -
2.3.8	实时连接查看.....	- 6 -
2.4	入侵防御系统.....	- 6 -
2.4.1	网络攻击防范.....	- 6 -
2.4.2	自身保护功能.....	- 7 -
2.5	安全审计系统.....	- 7 -
2.6	其他功能系统.....	- 7 -
2.6.1	流量管理.....	- 7 -
2.6.2	VLAN支持.....	- 7 -
2.6.3	协议支持.....	- 8 -
2.6.4	DHCP服务.....	- 8 -
2.6.5	DNS代理功能.....	- 8 -
第三章	典型应用案例.....	- 9 -
3.1	典型应用(一).....	- 9 -
3.2	典型应用(二).....	- 10 -
第四章	技术支持.....	- 11 -
附录 1	技术规范.....	- 12 -



## 第一章 防毒墙系统简介

据相关调查，危害网络安全的因素 80% 来自病毒，而硬件防火墙的主要功能并不在防病毒上。企业的 IT 管理者在制定、审查安全策略，防止通过网络后门或社会公共网络对系统的攻击时，对防火墙过度信任而导致网络被攻击的例子屡见不鲜。从企业角度而言，如果能将病毒在通过服务器或公司内部网关之前予以过滤，将是防病毒最有效的方法。瑞星防毒墙就满足了这一要求。

瑞星防毒墙是集成了强大的网络防杀病毒机制，网络层状态包过滤、敏感信息的加密传输和详尽灵活的日志审计等多种安全技术于一身的硬件平台。是符合工业级标准的网关产品。它采用的是瑞星最先进杀毒引擎技术——OOT 引擎，采用面向对象的高稳定性设计，构成了性能优异的真模块结构，是达到了国际领先水平的高应变型智能引擎。通过独有的行为模式分析（BMAT）和脚本判定（SVM）两项查杀病毒技术实现对未知病毒进行检测，该技术已经获得国家专利。

该产品适用于各种复杂的网络拓扑环境，可以根据用户的不同需要，具备针对 HTTP、FTP、SMTP 和 POP3 协议内容检查、清除病毒的能力，同时通过实施安全策略可以在网络环境中的内外网之间建立一道功能强大的防火墙体系，不但可以保护内部资源不受外部网络的侵犯，同时可以阻止内部用户对外部不良资源的滥用。瑞星防毒墙从完整意义上解决了企业网络防护和网络边缘杀毒的问题。



## 第二章 瑞星防毒墙产品功能

### 2.1 基本系统功能

瑞星防毒墙的基本系统功能，如下图所示。

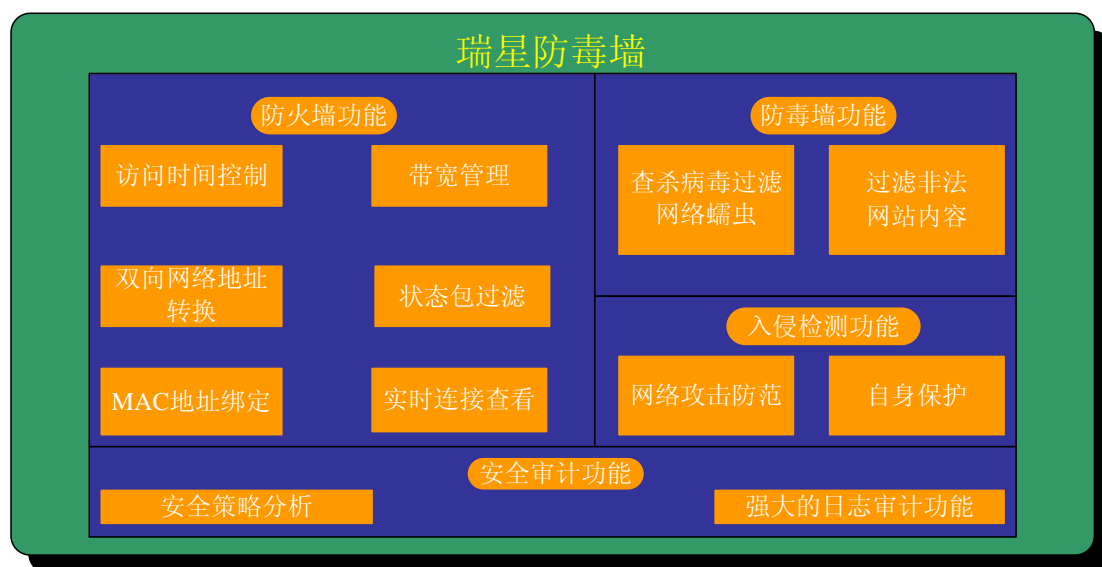


图 1 防毒墙功能图

#### 2.1.1 灵活适用的工作模式

瑞星防毒墙支持灵活的工作模式，采用了全新的接口配置理念，按拓扑设计的方式，每个物理接口的工作模式可以单独配置，能轻松简单的配置出复杂网络环境需求的防毒墙工作模式。瑞星防毒墙提供**透明模式(网桥)**、**路由模式**、**PPPoE 拨号模式**、**DHCP 模式**等。

- **透明模式**：对用户是透明的，即用户意识不到防毒墙的存在。要想实现透明模式，防毒墙必须在没有 IP 地址的情况下工作，不需要对其设置 IP 地址。当防毒墙工作在透明模式时，防毒墙此时工作类似于一个网桥，不需要用户对网络的拓扑做出任何调整。
- **路由模式**：当防毒墙工作在路由模式时，防毒墙此时工作类似于一个静态的路由器，可以提供静态路由功能。
- **PPPoE 模式**：利用 PPPoE 模式，防毒墙可以方便的接入拨号网络，提供安全的网关防护功能。大大的方便了用户的使用，保证了拨号接入网络的可用性。
- **DHCP 模式**：防毒墙的 DHCP 模式的好处在于省去了企业为单独设置 DHCP 服务器所消耗的成本，启用 DHCP 功能后，内网用户可以直接从瑞星防毒墙所提供的 DHCP 服务上获得相应的 IP 地址，这样会极大的节省用户投资，方便网络的统一管理。

另外，瑞星防毒墙最大限度的提供两个网桥的工作模式，通过这些模式的组合可以配



置出一个可以适应非常复杂的网络环境的防病毒网关。在配置接口 IP 时，可以指定 VLAN 属性，很方便的配置出带有 VLAN 特性的防毒墙系统。瑞星防毒墙不但可以架设在整个网络的出口，同时可以放置在某个部门的出口，也可以放置在特定服务器机群的前面，能够在所保护的對象之前设立一个安全屏障。防毒墙的工作模式界面具有强大的直观性，只要登录管理页面，就可以很容易了解每个物理接口工作模式，完全脱离了学习传统防毒墙需要一定网络安全知识的方式，更适合网络管理员的管理和减轻工作量。

### 2.1.2 ADSL+PPPoE

为了满足用户对实际网络环境的要求，瑞星防毒墙支持 **PPPoE 功能**支持灵活多变的接入方式。

### 2.1.3 强大的路由功能

瑞星防毒墙支持普通环境下的静态路由配置功能，同时也提供复杂的策略路由配置功能，能够很方便的实现用户网络环境内的多种复杂的路由策略需求。

### 2.1.4 管理员分级

瑞星防毒墙采用管理员分级原则，共分为超级管理员、配置管理员和审计管理员三种。

- **超级管理员**：对防毒墙拥有最大权限的用户，可以阅读全部防毒墙设置，同时可以修改全部设置。
- **配置管理员**：可以阅读全部防毒墙设置，可以进行部分修改。
- **审计管理员**：拥有的权限最低，只可以阅读防毒墙设置，但不可以修改。

不同的管理员拥有不同的管理权限，可以一定程度上进行相互制约，从而起到安全管理网络的实际意义。

### 2.1.5 远程管理

瑞星防毒墙采用远程 **Web 界面管理**和远程 **ssh 命令行管理**，管理员必须通过用户认证才能登录到防毒墙，对防毒墙上的配置文件进行修改。管理主机（可以放置在内外网任何地方，包括拨号网络）与防毒墙之间的通信采用加密传输，以防止黑客利用网络嗅探器对数据的窃取。利用这种机制，可以杜绝黑客假冒管理员对防毒墙文件进行篡改和获取敏感信息。同时严格限制了管理员能够登录系统的途径，除允许的接口或 IP 外其他任何企图登录防毒墙都将遭到拒绝，并且采用了锁定多次失败登录的用户和 IP 地址的方式，确保登录系统的用户是可信的。

### 2.1.6 终端命令行管理

瑞星防毒墙提供的终端命令行管理基本上可以实现 Web 管理的所有命令，且所有的命令字段能够自动补全，所有的配置效果与 Web 配置的结果一样，为网络访问不方便的情况



下提供了最完美的配置解决方案。简洁明快的配置管理界面也可使熟悉命令行的管理员迅速管理防毒墙的配置。

### 2.1.7 在线实时升级

瑞星防毒墙支持在线实时升级功能，能够实时升级病毒特征库及病毒引擎等相关的内容，从而不断提高防毒墙的防病毒能力和查杀能力。

## 2.2 防毒系统功能

### 2.2.1 强大的查杀病毒能力

瑞星防毒墙内集成了瑞星最新的杀毒引擎，能够查杀各种类型的病毒，查杀效率更高，运行更稳定。瑞星防毒墙支持 HTTP、SMTP、POP3、FTP 协议四种常用协议的病毒查杀。当这几种协议的数据通过防毒墙的时候，防毒墙截获其中的数据，根据用户的配置实现只查毒、杀毒、隔离病毒等方式。对于 HTTP 协议，当用户通过 IE 来下载的时候，防毒墙一边传送数据，一边检查数据中是否存在病毒，如果发现病毒，那么防毒墙就主动断开与客户的连接，此时用户就无法得到完整的数据，已经下载的数据同时会自动删除。对于 SMTP 和 POP3 邮件协议不但提供强大的病毒查杀处理，并且提供病毒告警功能，使得用户在接收到邮件的时候明确的知道邮件中有什么病毒，防毒墙又做了什么工作。同时防毒墙针对协议数据中出现的病毒做详细的日志记录，以便管理员和用户查询。在 HTTP、SMTP、POP3、FTP 协议中可以灵活定制查杀数据的大小、文件类型、查杀方式等多种策略保证在不影响处理功能的前提下提高处理的性能。

### 2.2.2 快速过滤网络蠕虫

瑞星防毒墙支持快速有效的阻断蠕虫王、冲击波、麦托、尼姆达、震荡波和高波等网络蠕虫病毒的渗透，在保证网络不被蠕虫感染的同时，也充分保证了网络带宽的正常使用。

### 2.2.3 内容过滤

瑞星防毒墙支持查杀病毒过程中，对部分关键内容进行过滤。包括网站过滤、URL 过滤及文件类型过滤等，过滤支持源和时间策略，即支持针对指定的源在指定的时间范围内进行过滤。

### 2.2.4 支持的文件格式

**可执行格式：**对通过的后缀为 EXE、SRC、PIF、BAT、COM 格式的文件进行查杀。

**库格式：**对通过的后缀为 DLL、SYS、VXD、DRV、BIN、OVL、386、SHS、MAI、SCR、LNK 格式的库文件进行查杀。

**邮件格式：**对通过的后缀为 MSG、DBX、IDX、IND、SNM、EML、NWS、MHT 格式的邮件文件进行查杀。



**脚本格式:** 对通过的后缀为FON、DOC、DOT、XLS、XLT、VBS、VBE、JS、JSE、WSH、SCT、HTA、HTT、CHM格式的脚本文件进行查杀。

**压缩格式:** 对通过的后缀为ZIP、ARJ、CAB、RAR、ZOO、ARC、LZH、PKZIP、GZ、TGZ、PKPAK格式的压缩文件进行查杀。

**网页格式:** 对通过的后缀为HTM、HTML、ASP、CSS、PHP、ASPX、DHTML、JHTML、CGI、JSP、XML格式的网页文件进行查杀。

**图片格式:** 对通过的后缀为JPG、BMP、GIF、PNG、PCX、TGA、TIFF格式的图片文件进行查杀。

**自定义文件类型:** 用户还可以根据需要定义其他格式文件的病毒查杀。

瑞星公司未知病毒查杀技术拥有专利权, 将该技术应用到防毒墙系统上, 无疑为系统增加了一道有力的安全屏障。

## 2.3 防火墙功能

瑞星防毒墙同时也是一个功能强大的防火墙系统, 能够建立高效安全的防火墙策略, 以保证可信网络的安全。

### 2.3.1 状态包过滤

瑞星防毒墙采用了最先进的状态包过滤技术, 根据状态包过滤的思路, 在核心中维护一个连接链表, 记录着相应连接的状态, 对请求建立连接的数据包进行更细粒度的检查, 检查通过后记录到状态链表中, 从而对后续的或是关联的数据包只需检查其是否属于已建立的连接, 不需全部进行规则匹配, 经过这样的状态处理机制后不仅使安全性得到加强, 同时也大大提高了包过滤的效率。

### 2.3.2 访问时间控制

瑞星防毒墙在网络层过滤技术中引入了时间表的概念。对每一条过滤规则, 允许管理员定义一个时间范围, 使该条规则只在这一时间范围内起作用。通过这种控制机制, 可以为企业提供更加灵活的策略配置。

### 2.3.3 MAC 地址绑定

瑞星防毒墙支持 MAC 地址绑定, 支持将内网每台主机的 IP 地址与该主机网卡的物理地址进行一对一的绑定, 不但具有手工绑定功能, 也具有自动绑定功能, 同时还提供 MAC 地址的分组管理等功能, 这样不但有效阻止用户通过修改 IP 地址所进行的非授权访问, 而且降低管理的复杂程度。在使用 DHCP 服务的网络中, 各主机的 IP 地址是变化的, 这时可以在设置安全策略时使用源 MAC 地址来进行访问控制, 系统内核进行包过滤时就只匹配数据包的源 MAC 地址, 从而在设置安全策略时可以忽略主机的动态 IP 地址, 大大提高了管理的灵活性。



### 2.3.4 带宽管理

瑞星防毒墙支持带宽管理。带宽管理用于针对性的对某些特定的服务进行限制带宽使用或是保证带宽使用。管理员可以事先为带宽分组，然后在添加安全策略时，将相关的策略使用同一个带宽分组，系统进行带宽管理时，就能根据要求来保证某个服务可以至少使用多少带宽或是至多使用某个带宽，从而保证了内部网络能够合理的利用公司已有的网络带宽。

### 2.3.5 安全策略

瑞星防毒墙提供的安全策略配置功能，简单明了，通过预先定义的地址组对象、服务对象和时间对象后，只需要进行合理的选择就可以生成一条复杂的安全策略，安全策略的位置可以随意移动，即时生效。

### 2.3.6 策略分析

瑞星防毒墙还提供了策略分析功能，包括安全策略分析了带宽控制策略分析，策略分析时，可以列出已经生成的策略详细列表，也可以查询某个 IP 或是某个时间段有什么样的安全策略或是带宽控制策略。通过进行策略分析，可以让管理员很放心自己实施的安全策略。

### 2.3.7 双向网络地址变换

瑞星防毒墙支持源地址转换和目的地址转换。通过地址变换，不但可以对外屏蔽内部网络拓扑结构，而且可以节省 IP 地址资源，从而有效的防止外部网络的威胁。

### 2.3.8 实时连接查看

瑞星防毒墙提供当前系统的连接信息查看，查看的信息包括协议、源地址、目的地址、源端口、目的端口、上传字节数、下载字节数、上传包数、下载包数、连接、时间。相同的源地址到同一目的地址的同一端口只列出一条，并统计出这样的连接数量，信息简洁完整。还可以按指定的条件来查询相关的连接信息，同时可以指定显示的连接其空闲时间，即防毒墙可以只显示在指定的空闲时间内的连接信息。

## 2.4 入侵防御系统

瑞星防毒墙也是功能强大的入侵防御系统，对系统资源的非授权使用能够做出及时的判断、记录和防范，从而保护自身系统资源。

### 2.4.1 网络攻击防范

瑞星防毒墙缺省设置了一些基本规则，不需要用户参与，可以有效防范 IP 地址欺骗、Ping of death 以及 Syn flood 等基本网络攻击，保护内网和防毒墙免遭多种形式的拒绝服务攻击和非法访问，保证服务器能够正常的提供服务。



## 2.4.2 自身保护功能

瑞星防毒墙是建立在安全操作系统的基础上，取消所有已知存在安全漏洞的程序和不必要的服务，只运行必要的防毒墙守护进程。除了需要的必须的服务外，其他的任何端口都是关闭着的，从根本上防止访问防毒墙的可能。

## 2.5 安全审计系统

瑞星防毒墙提供了强大的日志审计功能，并可提供详细的日志分析统计报告。系统管理员可以在管理主机上实时查看防毒墙的运行状态和浏览各类报告。为避免系统硬盘空间耗尽，防毒墙保存的日志文件定时滚动，最长保存时间可由用户设置。同时，可选的日志实时备份模块，能够实现日志异地存储。仔细阅读日志，可以帮助管理员发现被入侵的痕迹，以便及时采取弥补措施，或追踪入侵者。

防毒墙日志支持本地 syslog、本地 mysql 和远程 syslog、远程 mysql 等多种记录方式。瑞星防毒墙安全审计日志功能分成事件日志、管理日志、系统日志和日志保存设置。

- **事件日志：**记录包括 HTTP、FTP、SMTP、POP3 协议不同时间段病毒的查询，以及病毒日志的详细信息。
- **管理日志：**支持查询任何时间所有用户登录的具体信息。
- **系统日志：**记录用户对系统的修改。
- **日志保存设置：**配置防毒墙日志如何进行保存。

## 2.6 其他功能系统

### 2.6.1 流量管理

瑞星防毒墙支持流量管理功能，可以针对指定的网络段或主机进行统计，经过统计的主机也可以有选择的决定是否要进行流量控制，控制周期也很灵活，可以有针对性的分别设置。控制周期分为每小时、每天、每周、每月和每年。在流量管理中，可以实时的查看当前周期下，各被统计的主机使用的网络流量，也可以浏览或是打印当前统计周期内的详细流量记录。支持对指定控制的主机进行锁定或解除锁定的功能，从而控制其在超过额定流量情况下的使用网络的方式：拒绝或是允许。提供的流量分析功能可以分析网际 IP 数据流动状况，了解需要了解的数据流动状况，方便网络管理员的使用。能够直观、全面的一致性管理网络设备、主机、服务器周边运维环境，深入的数据流分析。

### 2.6.2 VLAN 支持

瑞星防毒墙具备虚拟局域网 (VLAN) 分组数据交换功能。用户可以通过配置接口 IP 时指定 VLAN 的 ID 功能对接口进行 VLAN 分组，支持 IEEE802.1Q 协议，提供符合国际标准的 VLAN 接口和配置管理，方便用户防毒墙的部署。



### 2.6.3 协议支持

瑞星防毒墙支持常用的 TCP/IP 协议，同时支持 802.1q、SNMP、IGMP、H.323、OSPF、RIP 网络协议，能够很好的解决各接口间的视频数据的转发。

### 2.6.4 DHCP 服务

瑞星防毒墙提供 DHCP 服务。防毒墙的 DHCP 服务可以有选择的启用指定接口的 DHCP 功能，多台计算机可直接由防毒墙分配网络地址及相关网络设置。启用 DHCP 服务能极大地降低企业的网络在实际应用环境中的维护工作，真正做到即插即用。

### 2.6.5 DNS 代理功能

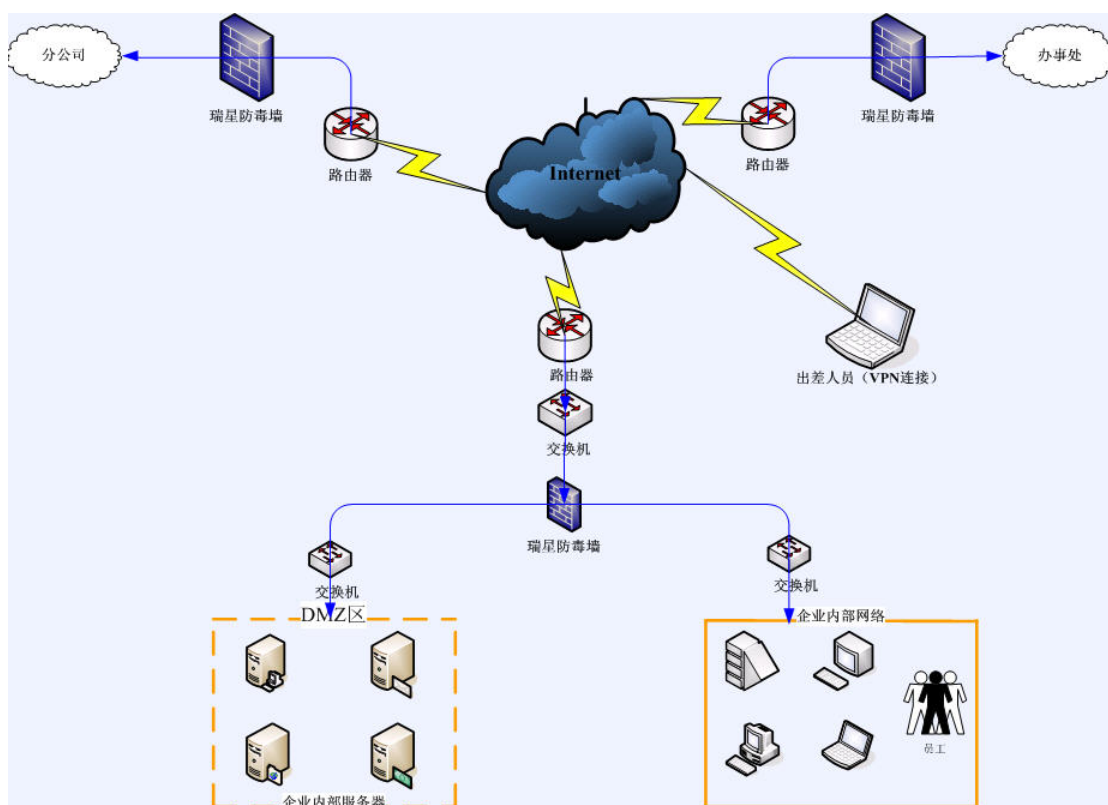
瑞星防毒墙提供 DNS 代理功能，通过使用 DNS 代理功能，用户可以方便的为一个外部域名使用内部主机 IP 进行访问。



### 第三章 典型应用案例

瑞星防毒墙可以针对不同的应用环境灵活地满足不同的安全需要,最常见的应用如下:

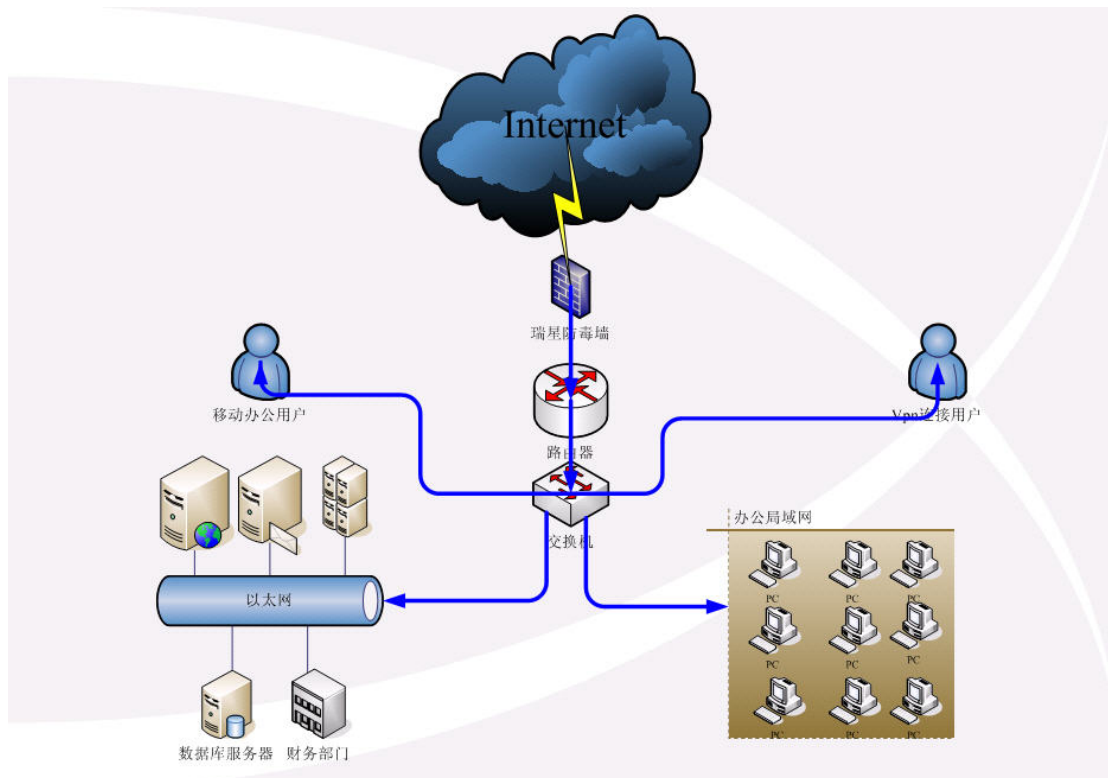
- 应用在企业内网与 Internet 或其他非安全网络的唯一出入口。
- 应用在企业内部网络, 保护敏感部门的子网。
- 对内部网的不同域进行隔离, 实施不同的安全策略。
- 限制内网用户对不良网络资源的滥用。



#### 3.1 典型应用(一)

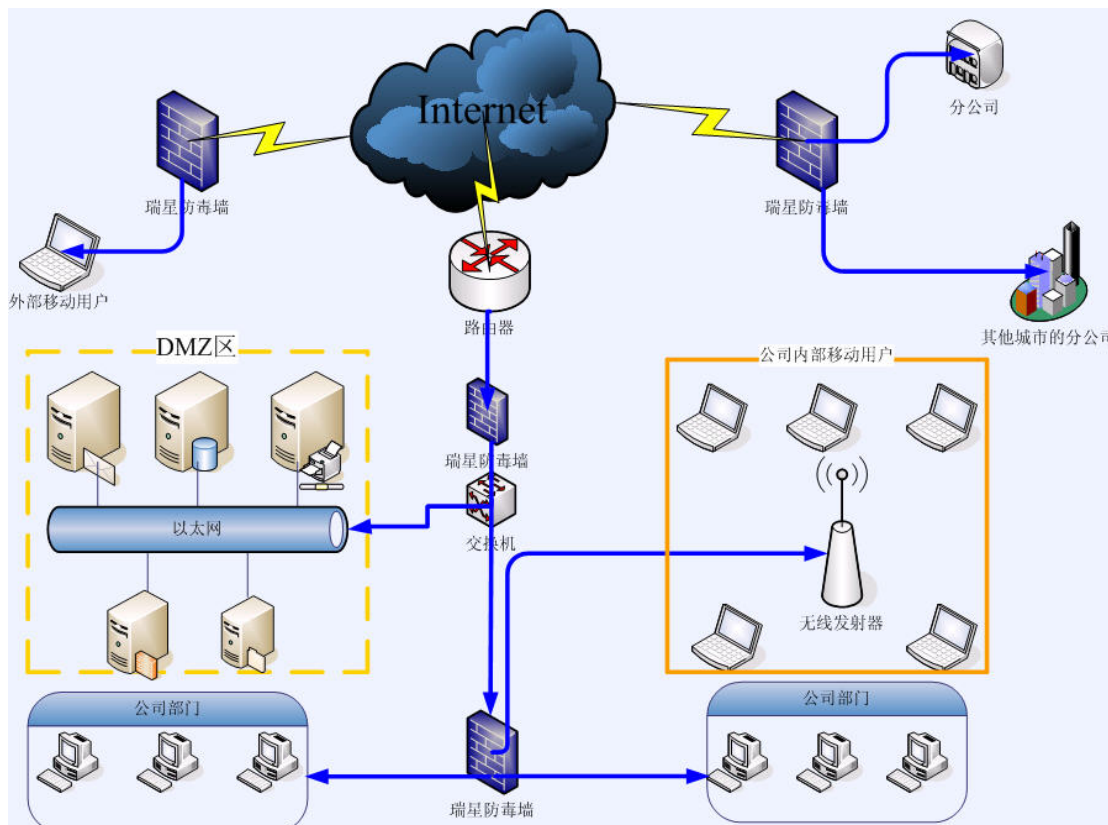
防毒墙放在内外网边界, 隔离企业内部网和外部非安全网络, 如下图。





### 3.2 典型应用(二)

防毒墙放在各个分公司或部门边界，对企业内部各部门的敏感数据进行保护，如下图



## 第四章 技术支持

地址：北京市中关村大街 22 号· 中科大厦 1305 室

邮编：100080

总机：(010)82678866

传真：(010)62564934

客户服务：(010) 82616666

邮件支持：<http://csc.rising.com.cn>

公司网站：<http://www.rising.com.cn>



## 附录 1 技术规范

瑞星防毒墙 RSW-1000P			
性能		系统主要功能	
吞吐量 (Mbps)	100	防火墙功能	支持
最大连接数 (个)	128000	入侵防御功能	支持
HTTP 新增连接数 (个/秒)	100	实时升级功能	支持
HTTP 杀毒吞吐 (Mbps)	10	支持查杀的协议	HTTP、 FTP、 SMTP、 POP3
HTTP 最大并发连接数 (个/秒)	1000		
HTTP 延迟 (ms)	小于 2000		
FTP 最大吞吐 (Mbps)	10	内容过滤	支持
FTP 最大并发连接数 (个/秒)	300	流量控制	支持
邮件数 (封/每秒)	30	带宽管理	支持
SMTP/POP3 最大并发连接数 (个/秒)	300	即插即用和透明模式	支持
物理属性		DHCP 服务器	有
电源	220V/50Hz 250W(最大)	DNS 代理服务器	有
机型	标准 1u 机架式机箱	地址转换	支持
长度/宽度/高度 (cm)	30.5 x 43.8 x 4.5	VLAN	支持
重量 (Kg)	6.12	PPPoE 模式	支持
相对湿度	10-90%@40 摄氏度, 非冷凝	路由模式	支持
工作温度	0-45 摄氏度	WEB 界面和串口管理	支持
非工作温度	-20-65 摄氏度	强大的日志系统	支持
网络接口		管理帐号分级	支持
3 个 100/10M 自适应		自定义服务	支持

