硬件防火墙新贵—FortiGate

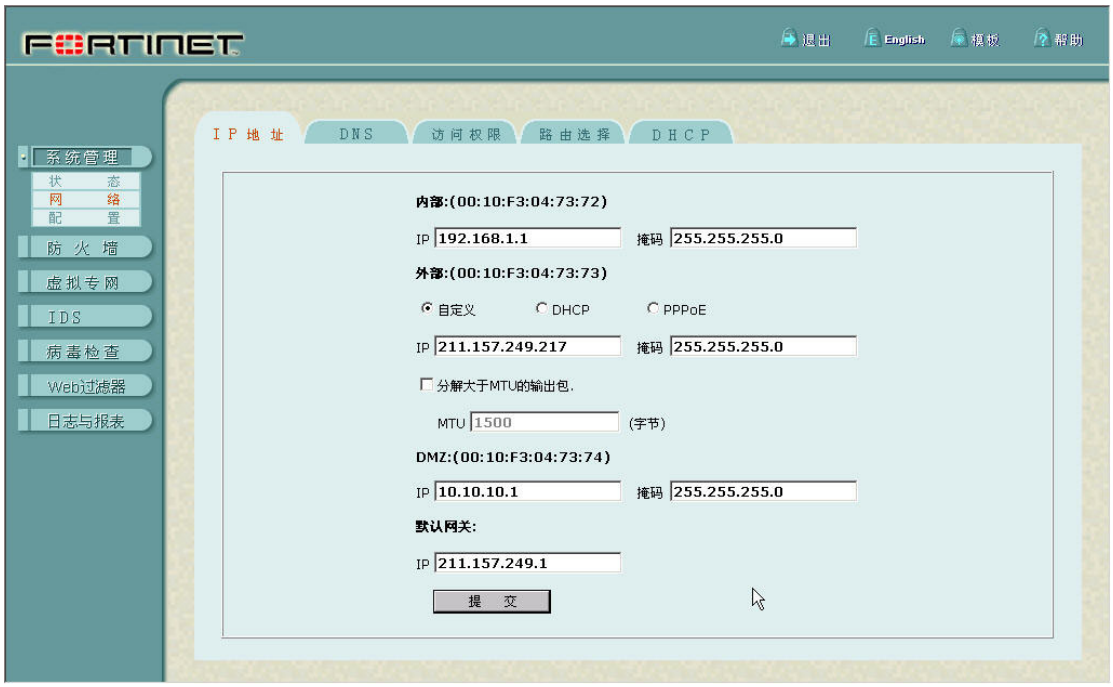
作者：SQL SQL@263.net
站点：www.isfocus.net

FortiGate™ 防火墙是最近刚刚进入市场的一款国外的硬件级别防火墙的产品，我知道国内很多公司都准备和它合作推出OEM级别的防火墙产品，由于目前在外面关于这款产品的介绍还不多，所以我就想写写关于它的东西。FortiGate 系列是以包括FortiNet的FortiASIC™内容处理器和FortiOS操作系统在内的革命性体系结构为基础的。专用硬件和软件强大的结合提供了线速处理深层次信息包检查、坚固的加密、复杂内容和行为扫描功能的优化。这也是FortiGate™ 防火墙最吸引人的地方它是一个纯硬件的设备里面有自己专用的OS和内容处理核心。

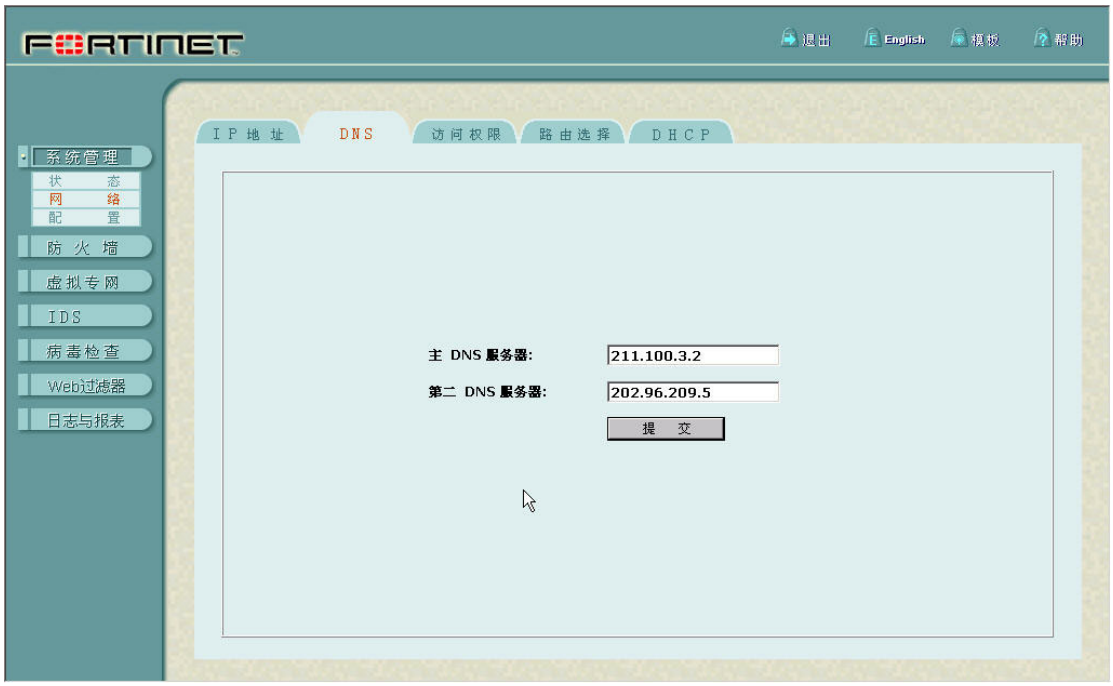
下面就简单的结合现在版本的FortiGate™ 防火墙300系列来介绍下它。

FortiGate™ 防火墙可以用 WEB 和专门的管理器登陆，我这次测试是用 WEB 方式登陆上去的，首先我们需要输入防火墙的用户名和管理密码。

同时我们可以在性能栏里查看防火墙当前的运行状况，包括 CPU 的占用率，持续工作的时间，以及当前通过防火墙所维持的连接状态。

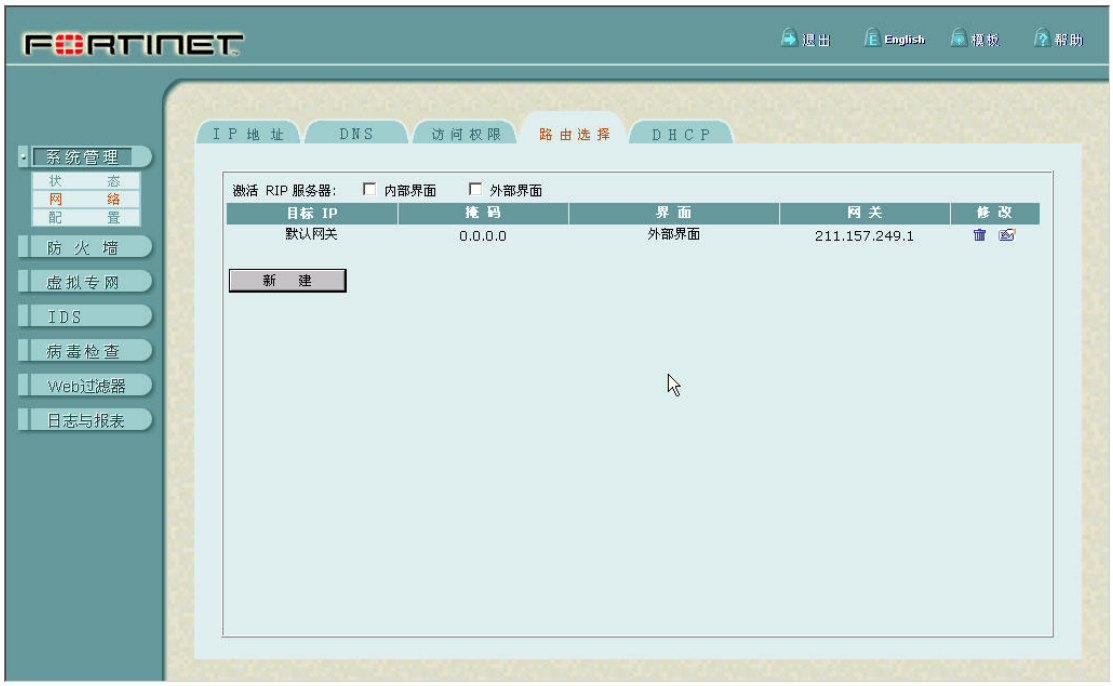


在配置栏目中主要是进行一些初始化的配置，如设置内网 外网 DMZ 区的 IP 地址范围。

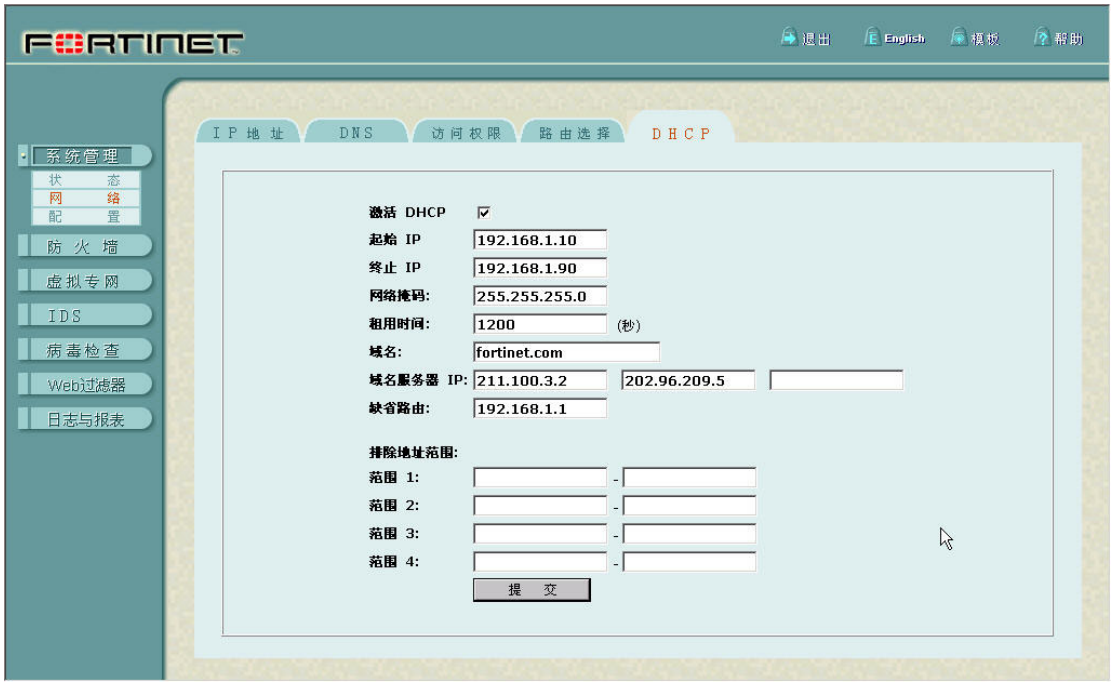


DNS 里面设置的是防火墙的 DNS 服务器，这里可以设置两个 IP 地址。

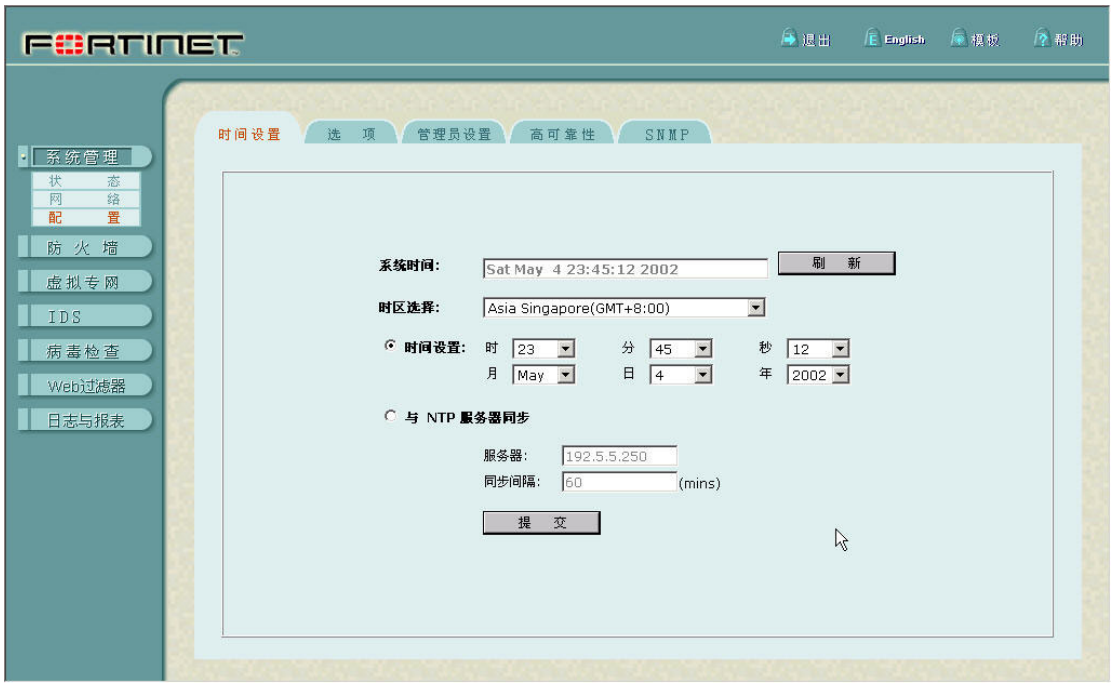
访问权限主要是针对内外网和 DMZ 区域对于防火墙的一些访问权限，这里简单的把它们分成了 HTTPS PING SSH 三种主要的管理方式。



路由设置很好理解不做解释了。

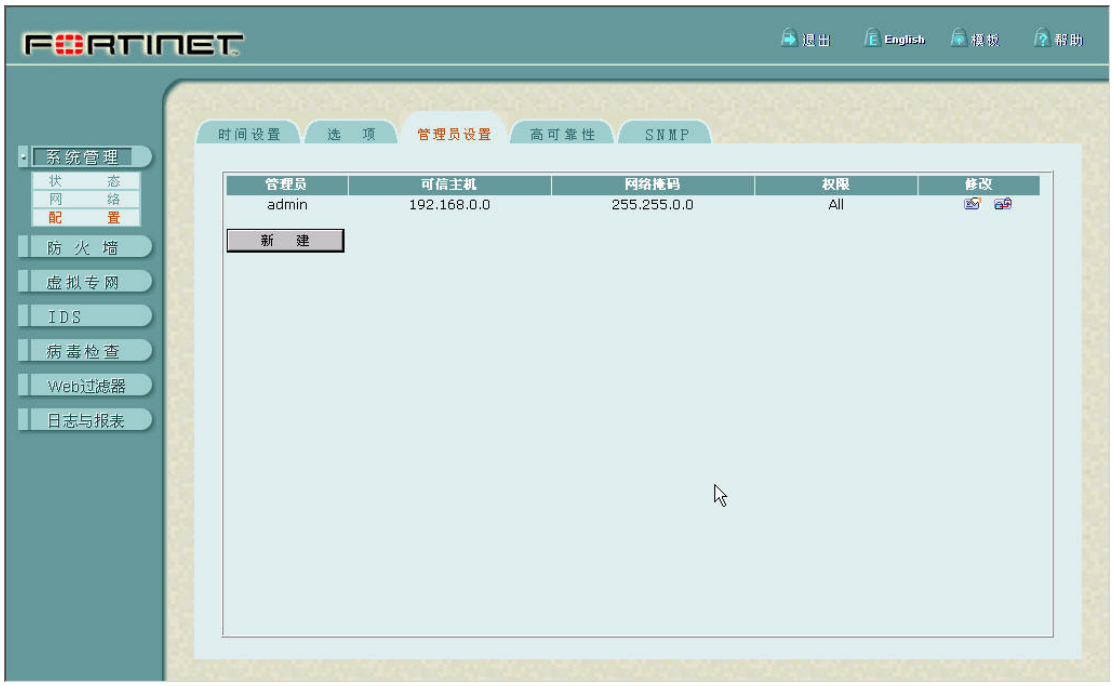


比较有特色的是 FortiGate™ 防火墙自己本身内置了一个 DHCP 服务器，这样在一些小型网络环境可以解决很多 IP 地址设置和管理的麻烦，是很实用的功能。



系统配置项目里，第一个是时间设置主要是设置防火墙的时间的。

第二个选项中比较有意思的是界面的语言版本，FortiGate™ 防火墙支持中文在内的 5 种语言你可以轻松的把界面在这五种语言中来回切换。

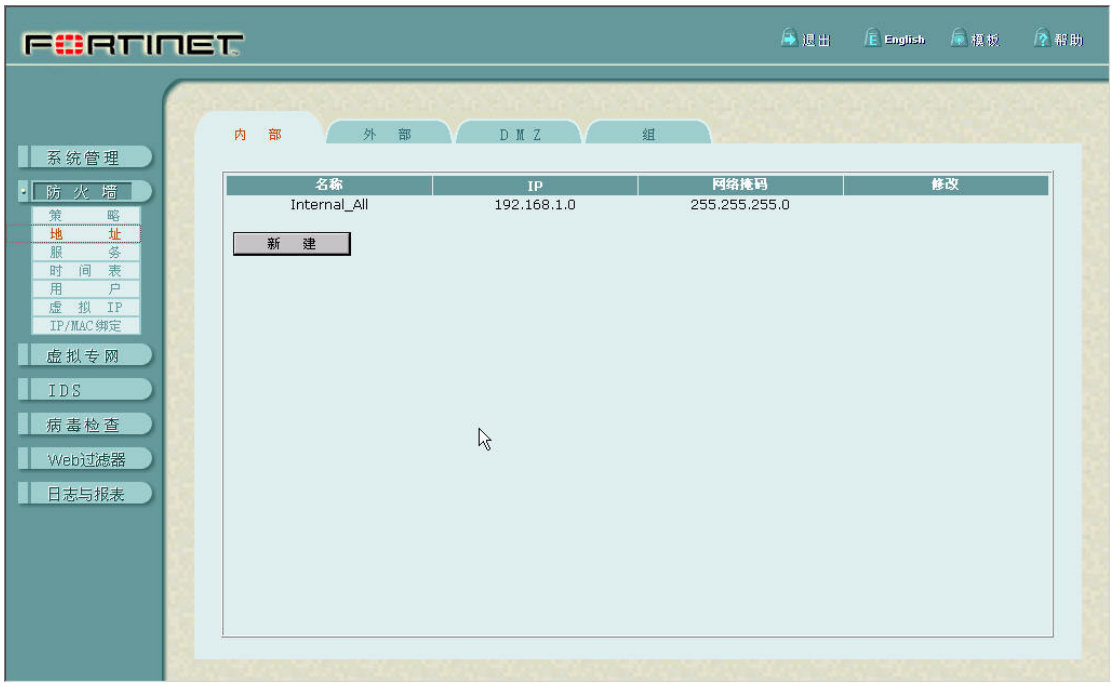


管理员设置中，主要是针对管理员允许登陆的 IP 地址进行限制。

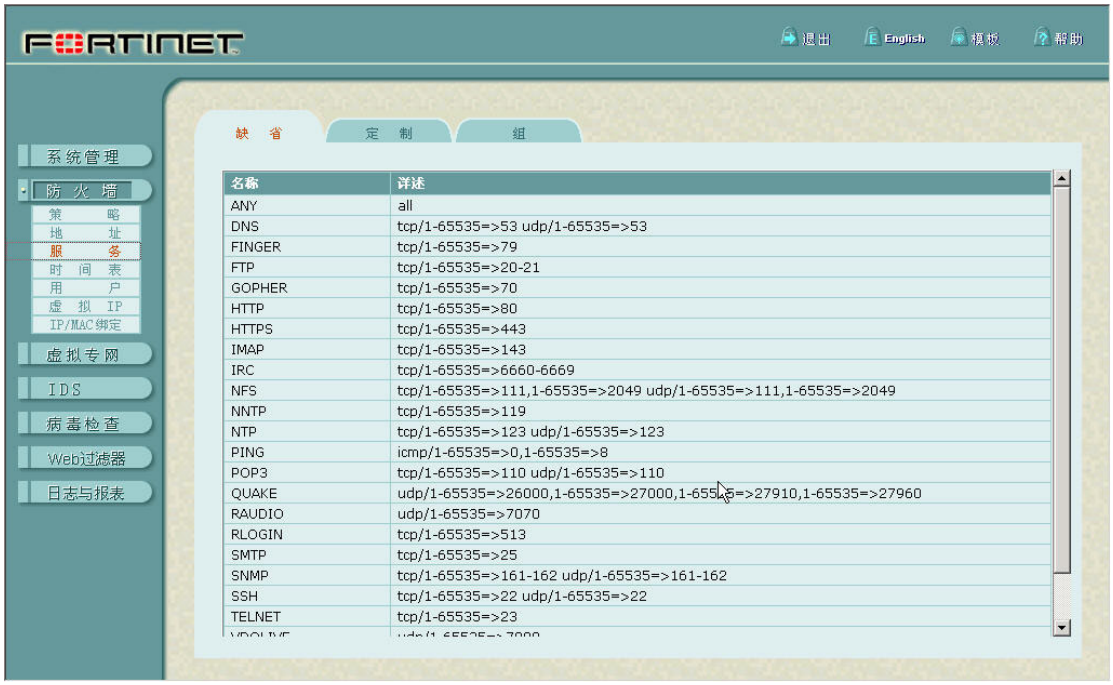
高可靠性就是双机热备的接口设置了，FortiGate™ 防火墙高端产品还支持自己的专用双机热备接口。

SNMP 的协议设置可以激活 SNMP 的响应，并且可以自定义几个最常见的 SNMP 的属性。

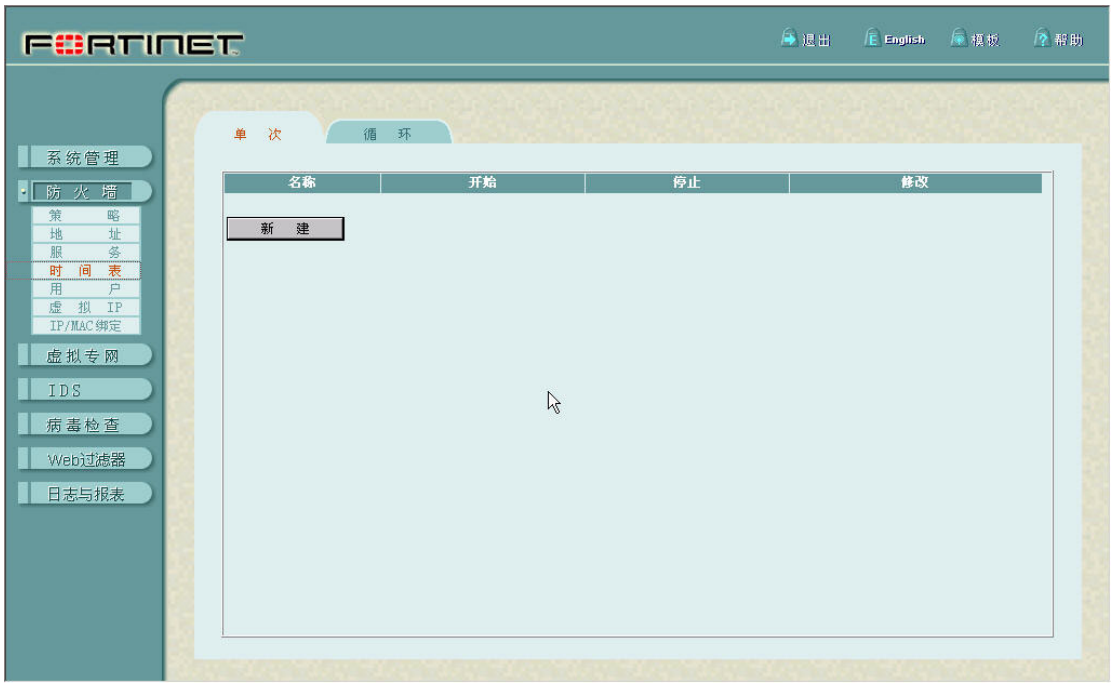
策略栏目中定义各个区域之间的访问策略



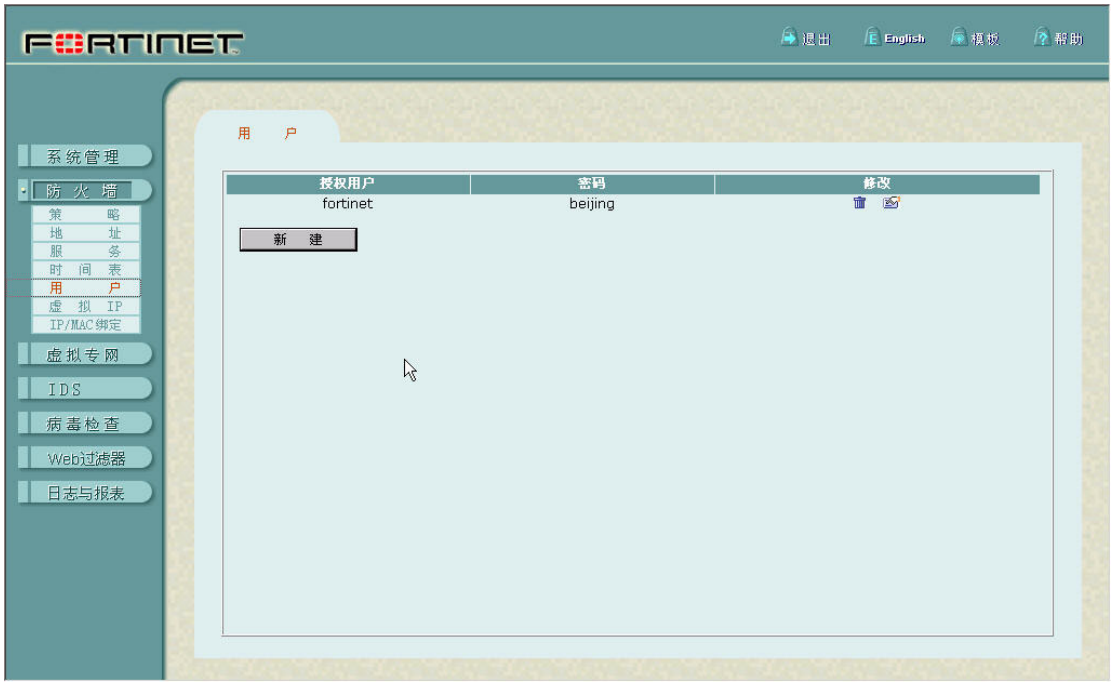
地址栏目中定义不同区域的网络范围地址



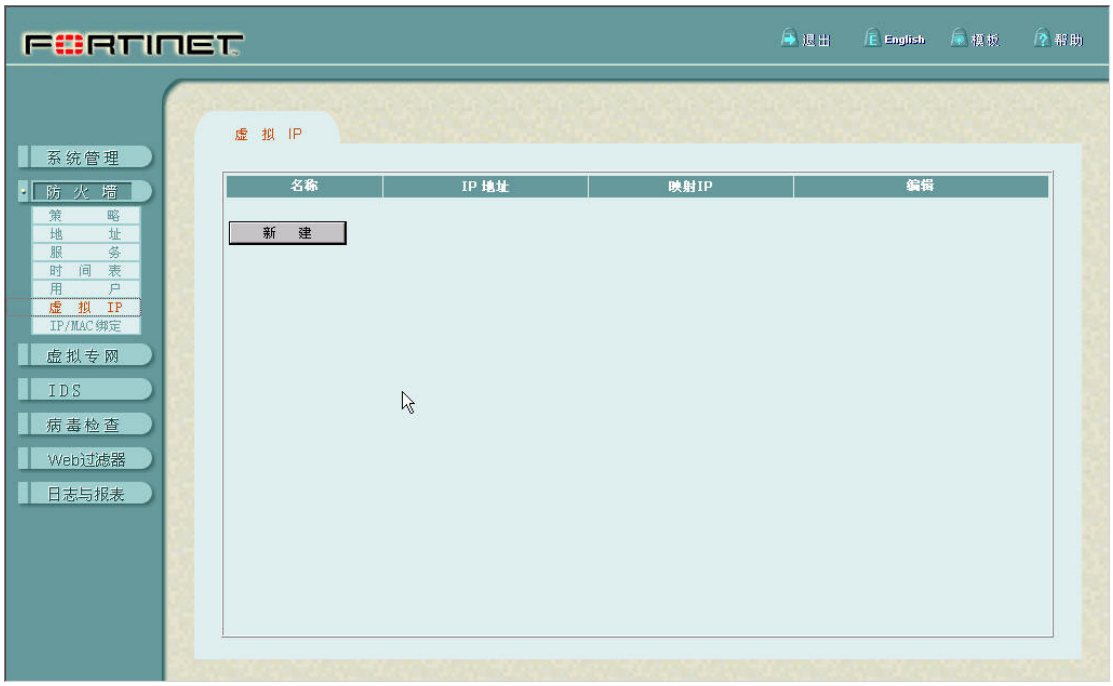
服务中有事先定义好的一些服务，也可以自己定义新的服务。



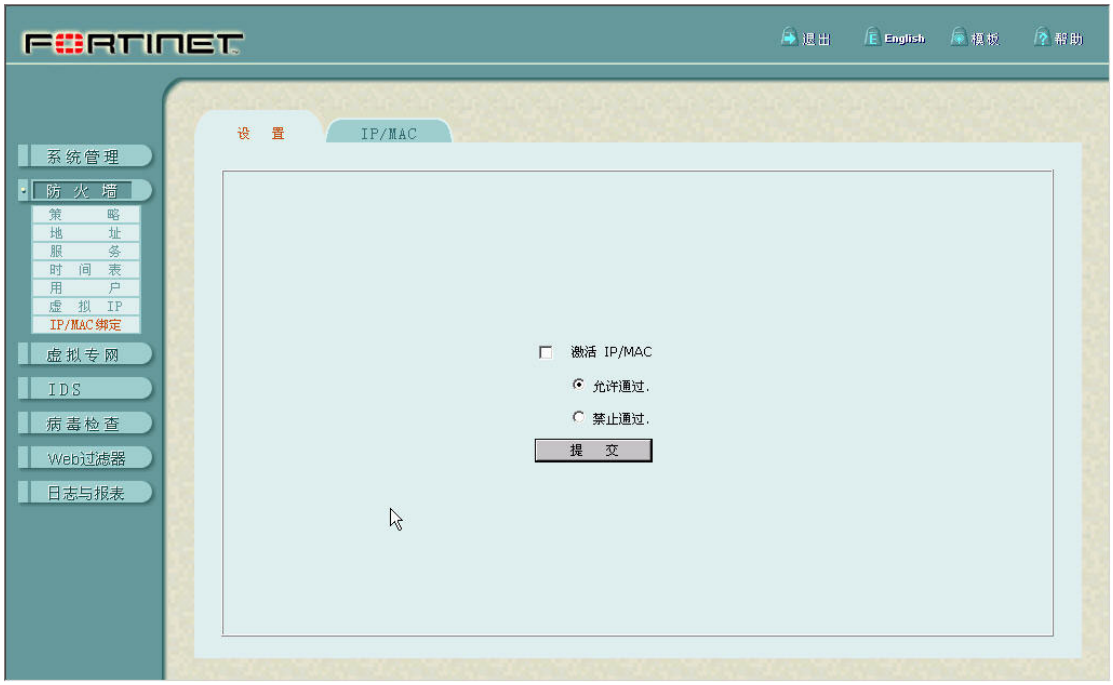
可以根据时间来做访问策略，但需要事前把时间段定义出来。



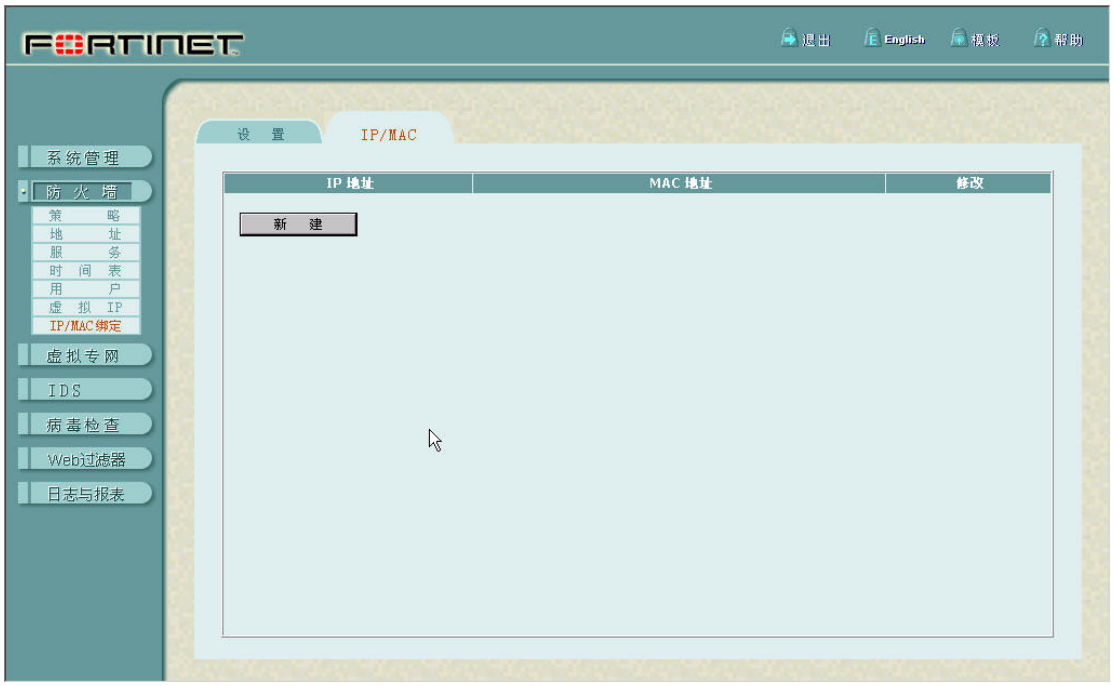
基于用户的访问规则，在这里定义用户。



虚拟 IP 地址设置其实就是做 NAT 的地方。

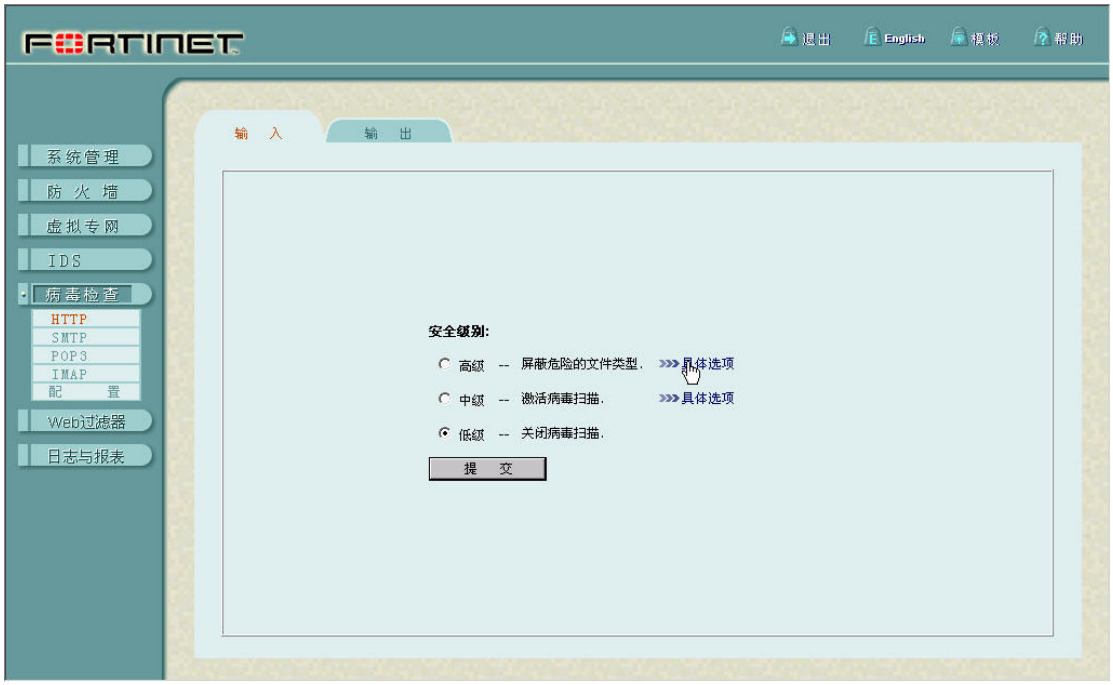


现在的防火墙都是支持 IP 地址和 MAC 地址绑定来防止内部网络用户盗用 IP 地址上网，这里可以做这个设置，当然我们知道这种功能实现的时候限制很多比如不能防止内部网络用户修改 MAC 地址而且不能跨交换机或者路由器。

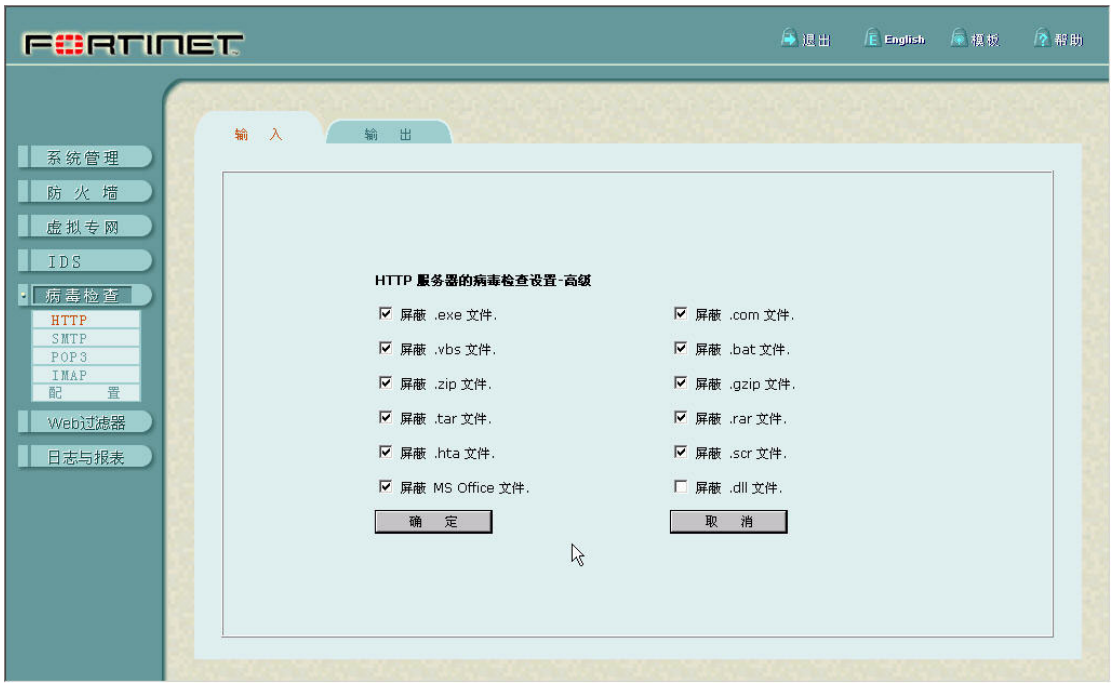


IDS 的设置栏目是我比较感兴趣的地方，本来以为可以看到些对于应用层的入侵检测内容，但发现其实还是传统防火墙的基于网络层的一些攻击模式的检测

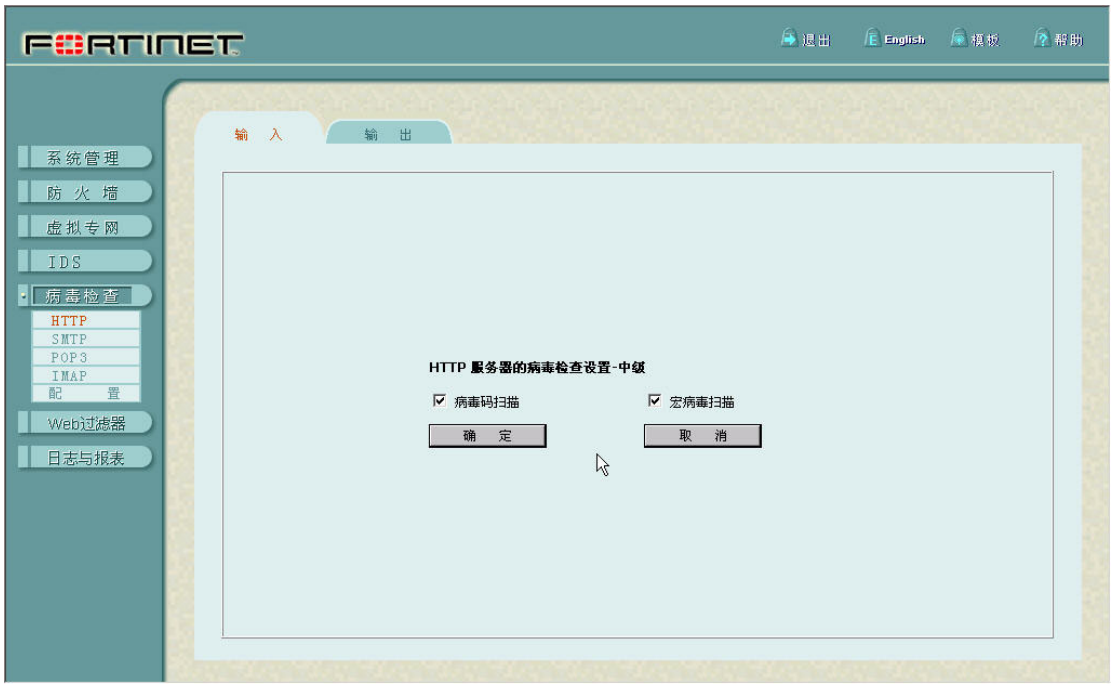
当发现攻击后，防火墙会自动给远程的一个邮箱发送警告邮件。



对于病毒检测是个防火墙最最重要的一个卖点了，所以这块也是非常吸引我的，我们可以看到目前 FortiGate™ 防火墙可以对 HTTP SMTP POP3 IMAP 四种协议传输的文件进行病毒检测，每种协议还分成输入输出两个方向，这个很好理解主要就是内外网之间的关系。我们先来看看高级设置中的内容了。

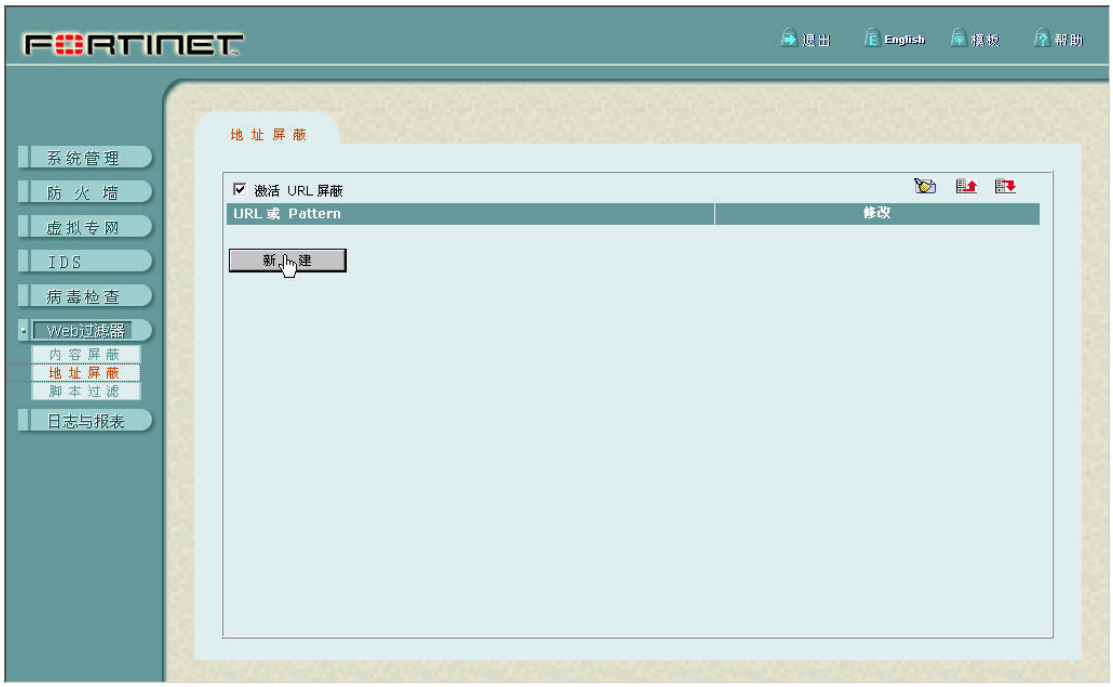


高级设置是采用屏蔽策略，简单的说就是发现网络上有些文件需要穿过防火墙的时候，直接在这里就把文件丢弃掉了，并不做杀毒的处理。具体有一些文件属性我们可以根据后缀名来选择。

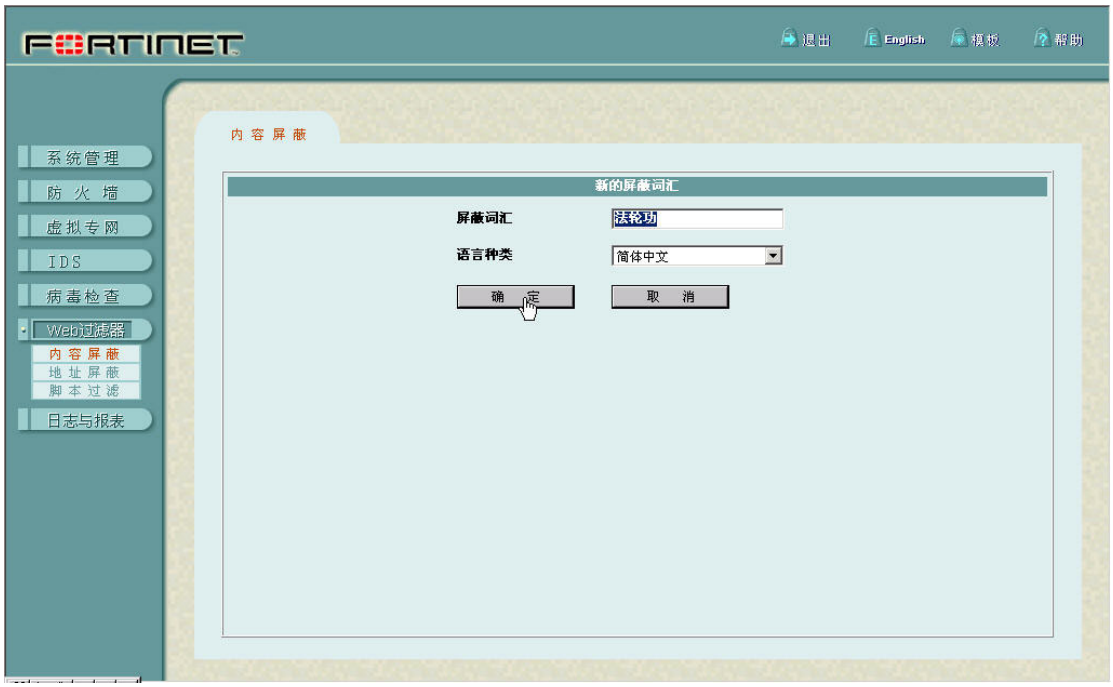


中级的设置就是直接比较正规的杀毒过程了。

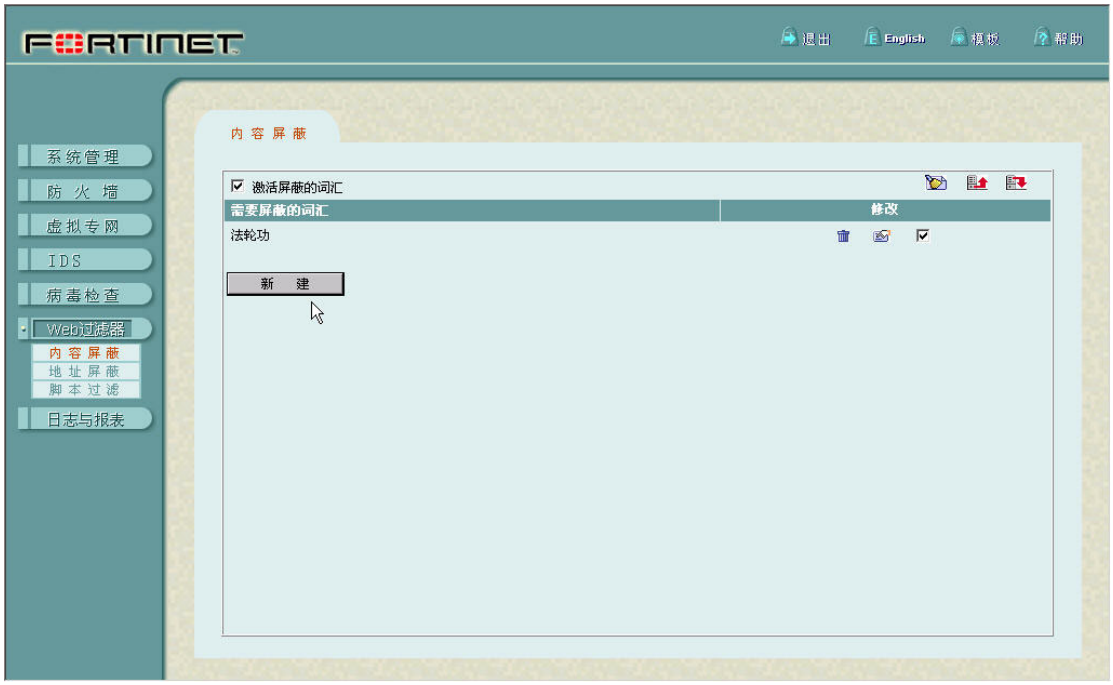
做为防火墙端的杀毒软件功还同时支持自动到指定的更新服务器上自动更新病毒库文件。



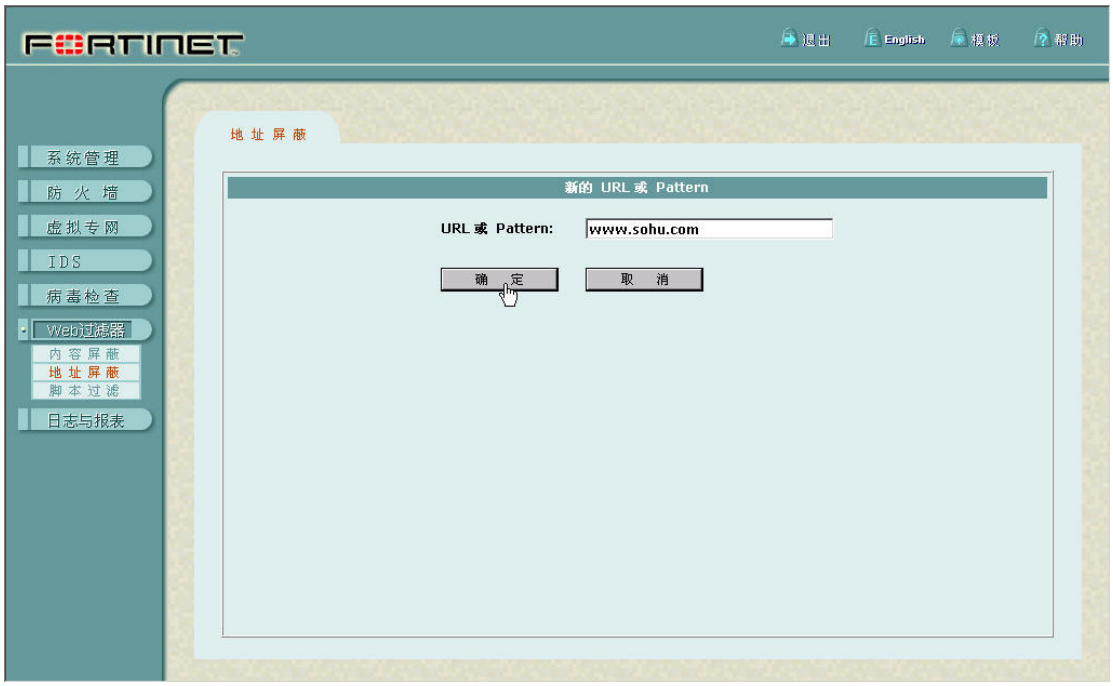
WEB 过滤器的功能也是号称可以做到内容过滤的地方，我们也需要仔细看看。我们可以选择填加一个需要过滤的关键字。



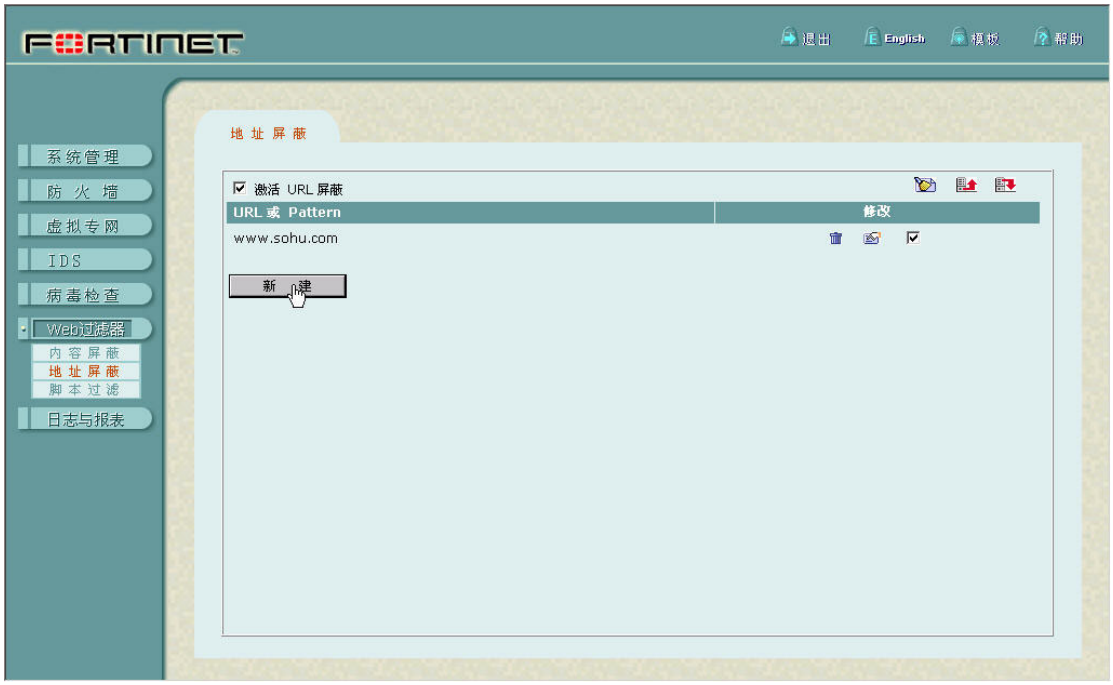
比较好的地方是 FortiGate™ 防火墙对于 WEN 页面过滤的文件考虑到了不同文字编码的区别，设置了不同语言的选择给我们。



填加好了以后，我们需要激活防火墙上的过滤设置，我估计此时的防火墙就把工作模式转变为了透明代理的模式。

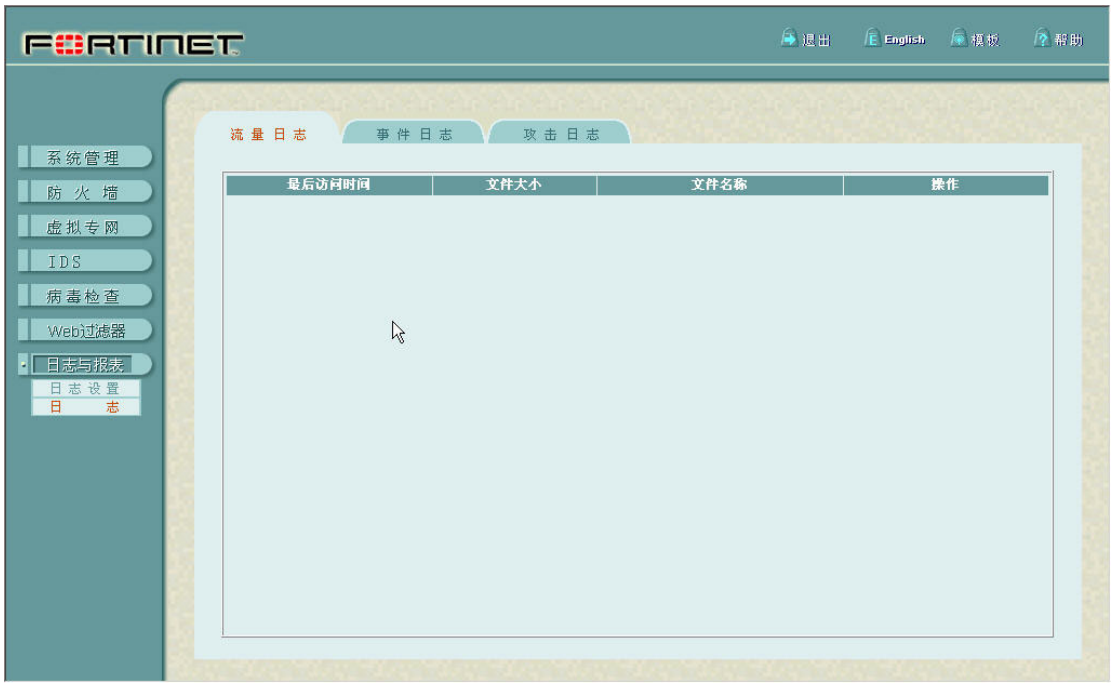


对于地址的屏蔽很简单就是禁止什么网站不能上，这样比较直接不用去设置 IP 策略，很多站点好象 SOHU 其实都不只一个 IP 地址，在这里设置一个域名就全解决了。



脚本过滤也很好理解，简单说一句就是很多客户追问防火墙能不能在这里自己分辨出恶意的脚本而解决，自动也许正常的脚本通过，目前来说我还没有看到谁家的产品可以实现这个功能。

最后一个就是防火墙的日志处理了，简单的可以用 SYSLOG 的格式重定向到另外一个 SYSLOG 的服务器上处理，也可以保存在本地的 FLASH 盘上处理。



我们在最后这里查看防火墙的时时报警显示，有流量日志，事件日志，攻击日志三种不同的日志查看。

最后就是简单介绍下这款防火墙的产品型号的区别和具体的应用环境。

FortiGate™系列介绍

FortiGate™ 安全和内容控制系列产品，是利用一种新的体系结构方法研发的，具有无与伦比的价格/性能比；是完全的、所有层网络安全和内容控制的产品。经过一些安全行业深受尊重的安全专家多年的研究开发，FortiGate解决方案突破了网络的“内容处理障碍”。提供了在网络边界所有安全威胁类型（包括病毒和其它基于内容的攻击）的广泛保护。并且具备空前的消除误用和滥用文字的能力，管理带宽和减少设备与管理的费用。

内容处理障碍

常规的安全系统，像防火墙和 VPN 网关在防止称为网络层攻击是有效的，它通过检查包头信息来保证来自信任源合法请求的安全。但在现今，绝大多数破坏性的攻击包括网络层和应用层或基于内容的攻击进行联合攻击，例如病毒和蠕虫。在这些更多诡辩的攻击中，有害的内容常常深入到包内容，通过许多表面上“友好的”很容易穿过传统防火墙的数据包传播。同样的，有效的网络保护依靠辨认复杂和狡猾的若干信息包模式样本，并且需要除了网络层实时信息，还有分解和分析应用层内容（例如文件和指令）的能力。然而，在现今的网络速度下，完成高效率的内容处理所必需的处理能力要超过最强大网络设备的性能。结果，使用常规解决方案的机构面临着“内容处理障碍”，这就迫使他们在桌面和服务器上加强内容服务的配置。无论如何，当我们变得更依赖网络通讯的时候，这样是无法接受的：增加安

全的同时维持原来的性能和降低成本是最基本的，为了这些，一种新的方法是必需的。

FortiNet 突破内容处理障碍

FortiGate 产品线设计了从低端到支持广泛的安全和内容控制，提供千兆及以上线速性能的同时，为电信、小型办公室、企业和服务提供商节省有效的成本。

FortiGate 系列是以包括 FortiNet 的 FortiASIC™内容处理器和 FortiOS 操作系统在内的革命性体系结构为基础的。专用硬件和软件强大的结合提供了线速处理深层次信息包检查、坚固的加密、复杂内容和行为扫描功能的优化。FortiGate 的体系结构使 FortiGate 系列产品能够提供一套完整的服务，包括以下几点：

-防火墙（地址转换、端口转换和状态检测）
-病毒/蠕虫检测和消除
-入侵检测
-根据 URL、关键词或词组过滤内容
-拒绝服务检测和防止
-虚拟专用网
-流量控制

通过将这些基本功能合并在紧凑的、可靠的、容易管理的 FortiGate 产品里，FortiNet 已经打破了内容处理的障碍。

完全的、线速安全和内容控制:

FortiGate 系列产品按照可选择的解决方案提供了功能和受益无与伦比的结合：

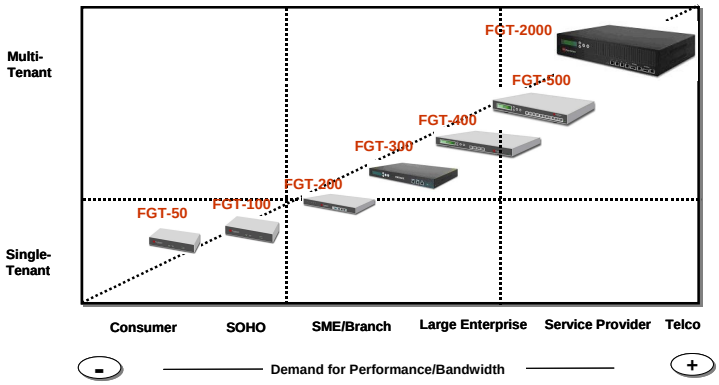
- FortiNet 加速的行为和内容监测系统（**ABACIS**）是第一个结合防火墙、防病毒和内容过滤、VPN、入侵检测和流量控制功能在一起的产品。ABACIS 技术消除了由若干单个功能设备引起的低效率和资源浪费，这样减少了设备费用、更容易的网络集成、简单的管理和较低的更换费用。
- FortiNet 独特的**内容扫描**技术使用专门设计的 ASIC 芯片和软件，提供了无比的能力和适应性。**FortiASIC™内容处理器**完成深层次包检查，并且能够分类和分解数据包，还可以在没有危及网络性能的情况下根据攻击的数百、数千个“特征码”进行内容匹配，比如病毒和蠕虫。内容扫描技术也能够使 Web 内容过滤基于用户自定义的关键字或短语，支持多种语言，另外还可以阻止挑选过的 URL。内容过滤这种方法比单一的 URL 阻止提供了更好的选择性和控制，保护了来自任何地方的不必要的内容。
- FortiASIC 芯片集成的加密引擎为安全和高性能的 VPN 提供了线速加密和认证性能，支持点到点和远程访问通讯。FortiGate 的 VPN 功能是与工业标准（IPsec, L2TP, PPTP）完全兼容的，可与第三方 VPN 网关、微软和其他提供商的客户端共同使用。
- FortiGate 入侵检测系统辨认和阻止攻击的范围，包括端口扫描、IP 欺骗、IP 源路由攻击和其他的攻击方式。在一个企图入侵者被检测和阻止时，系统会自动发出一个报警和日志记录以便管理员分析。
- FortiGate 流量控制系统使网络管理员能够保证指定用户特殊服务的质量。例如，挑选单独的一个组，给它支持一个特殊服务带宽使用的优先权，比如视频流，一会儿另一个不是基本服务（比如游戏）所使用的带宽就被禁止掉。
- FortiNet 的 **FortiGuard™保护服务**提供了关于 FortiGate 新攻击的自动更新。当发现新的攻击类型，它们的特征码就会很容易自动的加载到 FortiGate。
- **FortiGate 管理系统**提供了一套完整的管理工具 ，支持安装从单个点到多个点的企业网络，管理来自包括数百或数千个本地和用户主要服务提供者提供的服务。提供有权使用

所有的管理功能，基于浏览器界面，功能强大而简单，能够管理所有的 FortiGate 产品，多个管理员可以定义不同的权限。对于巨大的安装用户，**FortiManager™控制中心**是一个基于硬件的管理系统，能够自动策略定义和交叉地配置搜集到的大量 FortiGate 设备。FortiManager 中心提供了集中的、可靠的设置和策略存储，也为系统事件提供了集中记录日志和报告。基于浏览器的 FortiManager 管理控制台提供了使以前定义的策略容易的在多个设备间交叉复制，这个为大的企业和服务提供商安装减少了管理时间和成本。

FortiGate 系列产品，突破了功能、性能和成本效率的结合，第一次使网络安全和内容控制没有界限。

全面的产品系列:

FortiGate 安全和内容控制单元（SCCU）(每一款产品称为一个单元) 适合于从 SOHO 环境到服务提供商环境各个层次的需求。所有的 FortiGate 单元支持全部的安全和内容控制服务，为每一个应用很容易的选择恰当的设备。



FortiGate 个人办公环境/小型商务系列

FortiGate 个人办公环境/小型商务系列(SOHO/SB 系列) 包括 FortiGate-50, FortiGate-100 和 FortiGate-200。提供了配置简单，管理灵活的安全网关解决方案，为小型办公室和个人办公室也为分支机构提供了最高价值。通过我们的专利保护的所有层次深度扫描技术，该系列作为高效防火墙（从 **30Mbps** 到 **120Mbps**）加强了内部网络与外部网络之间安全控制之外，还保护您免于病毒、蠕虫和基于内容的攻击。VPN 功能使得你的员工能够通过安全通道与办公室相连。

FortiGate 企业系列

FortiGate 企业系列(Enterprise 系列) 包括 FortiGate- 300, FortiGate-400, and FortiGate-500。独一无二的设计能够满足对效率、可用性和可靠性企业级的需求。企业系列提供吞吐量从 **200Mbps** 到 **500 Mbps**，并且具有诸如高可用性性能在没有会话数丢失的情况下进行灾难恢复。独特的 FortiGate-500 具有 8 个可配置端口，实现贯穿企业的全部安全和内容控制，有效的将网络分段成不同的区，使各个组、部门或其他之间的内容流控制能够基于策略实现。

FortiGate 电信/ISP 系列

FortiGate-2000 是根据电信/服务提供商对性能和可靠性的需求而专门设计的安全网关。FortiGate™-2000 利用多个 CPU 和 FortiASIC 芯片提供两个 2Gbps 以太端口、两个千兆光纤接口和四个运行于 200 Mbps 的

10/100 端口，具有双电源保护，支持负载均衡。FortiGate™-2000 高性能、可靠性和管理简单的特点是管理服务提供商自然而然的选择。

FortiGate 产品应用配置图

FortiGate CCSU 能够安装在许多环境下，并且可以集成到任何实际的网络拓扑中。下图提供了针对从家庭办公，到企业、服务提供商以及电信不同客户的配置选项概览。