美国FORTINET 公司

FortiGate

系列产品技术手册

V4.0版

2004年7月

北京办事处地址:

北京市海淀区中关村南大街2号数码大厦B座903室

邮编100086

电话：（010）8251 2622　　传真：（010）8251 2630

网站： www.fortinet.com

目　录

1． 公司介绍

1.1 公司背景

美国Fortinet(飞塔)公司是新一代的网络安全设备的技术引领厂家。Fortinet公司成立于2000年，总部位于美国加利福尼亚州的硅谷Sunnyvale市，在加拿大、法国、英国、德国、澳洲、日本、韩国、新加坡和中国大陆、台湾、香港均设有分支机构。Fortinet创始人Ken Xie谢青是网络与信息安全的杰出专家，美国加州硅谷著名的高科技创业家。技术总监Joe Wells为全球著名防毒专家，是著名的WildList国际组织创导人。该公司由于研制出世界上第一个内容处理器，在网络安全领域堪称走在硬件防病毒防火墙的前沿。

1.2 产品简介

Fortinet公司研制开发基于ASIC加速的实时硬件网络防护产品— FortiGate™病毒防火墙系列产品。产品检测并阻挡来自邮件的威胁，以及病毒／蠕虫入侵和不健康网页的Web流量。所有的检测都是在实时状态下进行，不会影响网络性能。FortiGate™系统采用独特的易于管理的平台，通过集中的管理平台和移动客户端软件，构筑完善的安全架构。

目前网络安全架构所面临的严峻挑战大多直接源自于传统网络系统的局限性。因为这些系统缺乏支持内容处理的专用硬件，所以难以突破所谓的“内容处理障碍（Content Processing Barrier）”。也就是说，无法在维持网络传输速度的同時，对应用层进行信息内容扫描，检测并排除各种有害的内容。Fortinet研制的FortiGate™ 产品系列则可以突破内容处理障碍，为业界在网络网关处提供应用层防护， 设立了一套高性能低成本的网络防御系统。该系列产品的每一款都具有管理灵活、性能全面的特性，可为企业提供多层次防护，包括应用层的病毒防护、内容过滤服务以及在网络层的防火墙、入侵检测、虚拟专用网（VPN）、流量管理等服务功能。

Fortinet公司现共有十六款产品。FortiGate病毒防火墙系列拥有十三款不同产品，包括满足小型或家庭办公环境（SOHO）的FortiGate-50A、60、100； 适合中小商务的FortiGate-200、 300; 适合中型企业的FortiGate-400、500、800、1000以及用于大型企业和运营服务商的FortiGate-3000、3600、4000、5000。FortiManager为网络安全管理平台，用于远程管理多台设备。FortiClient远程客户端软件， 支持VPN。 新产品还包括无线安全产品Forti60WiFi和集中式日志报告系统FortiLog。

1.3 关键技术

FortiGate™的病毒防火墙系列产品，是在网络边缘提供完整保护服务的专用硬件产品。基于Fortinet的ABACAS™技术和FortiASIC™内容处理器，FortiGate™系列突破了内容处理

障碍，提供实时的网络防御，阻挡基于内容的安全威胁(如病毒和蠕虫)，还具有防火墙、VPN、入侵检测、内容过滤和流量控制功能。

公司拥有11项审核的专利，FortiGate™病毒防火墙采用了先进的行为加速和内容分析系统技术（Accelerated Behavior and Content Analysis System-ABACAS™），包括FortiASIC™内容处理器和FortiOS™操作系统，突破了芯片设计、网络通信、安全防御及内容分析等诸多技术难点，解决了功能和性能上的矛盾。

公司所独有的基于ASIC的网络安全架构能实时地进行网络内容和状态分析。在网络网关处部署应用层防护措施，在维持网络传输速度的同时，有效地确保了企业网络安全。FortiOS™内容操作系统是一个专用的高可靠、高安全的操作系统，可以保证所有的FortiGate™产品高效率、无阻塞地运行。FortiGate™的体系结构设计核心处理技术利用了智能排队和独特的管道管理，极大地改善了传统的数据处理速度。

1.4 总裁介绍

谢青（Ken Xie），公司创办人，总裁兼CEO，是杰出的网络安全专家，拥有15年以上的丰富网络安全技术和管理经验，成功地创造了基于ASIC的硬件防火墙产品系列。谢先生创办并曾任总裁的NetScreen 公司（那斯达克：NSCN）现已成为防火墙设备的领先厂商之一。此前，谢先生还创办了Stanford Infosystems（斯坦福信息系统）并任总裁兼CEO。他还在Healtheon公司 （现为WebMD）和飞利浦公司担任过安全架构主管。谢先生获有清华大学计算机工程学士和硕士学位以及斯坦福大学电子工程硕士学位。

Joe Wells，抗毒技术总监，是现今世界计算机病毒业界权威人士。他创建的WildList Organization International(WLO)，为防毒业提供最全面和权威的病毒信息。他在1988年开发出第一个防毒软体—特洛伊木马病毒侦测器。此后，他不断为防毒技术业的研究发展作出重大贡献，同时和世界各地的防毒研究团体密切合作，包括Certus International, Symantec（赛门铁克）下属的 Peter Norton 集团, IBM的Thomas J. Watson 研究中心, Cybersoft（中软国际），并担任Warlab (Wells Antivirus Research Laboratory) 总裁兼董事长，该公司是从事抗病毒研究的一家著名公众利益公司，由Trend Micro支持建立。

1.5 业务范围

公司产品面向全球市场， 在世界各地建有十余个分支机构， 承担市场、销售和技术支持。 在中国现已建立起全国性总分销商、代理渠道，并与一些单位结成OEM和战略合作伙伴。北京办事处起到良好的市场推进、业务保障和技术支援作用。 我们的客户已经延伸到许多运用IP架构网络的大中型企业和电信运营商，为企业连接客户端、合作伙伴、远程员工提供了良好的产品和安全应用方案。

2. 产品系列介绍

产品功能列表

病毒检测 （ICSA实验室认证）
病毒和蠕虫防御：能够100%检测、消除感染现有网络的病毒和蠕虫，实时的扫描输入和输出邮件及其附件（SMTP，POP3，IMAP，FTP），在不损失Web性能情况下扫描所有Web内容和插件（HTTP）的病毒特征码。

VPN 反病毒： 消除 VPN 隧道的病毒和蠕虫，阻止远程用户及合作伙伴的病毒传播。

Web 内容过滤
处理所有的网页内容，阻挡不适当的内容和恶意的脚本。

Web 内容过滤： 根据 URL、关键词模式匹配阻止 Web 站点及页面。
免屏蔽列表：允许管理员设置专门的URL或关键字不被阻断。

脚本过滤：阻止网页的插件，例如ActiveX、Java Applets和Cookies。

防火墙(ICSA 实验室认证)
符合工业标准的状态检测防火墙， 很容易配置策略。

工作模式：网络地址转换，透明模式，端口地址转换，路由模式。

用户认证：内建用户认证数据库，支持RADIUS&LDAP认证数据库。

服务：支持近百种标准服务（例如：Netmeeting、GRE、HTTP,OSPF），支持用户自定义服务和服务组。

时间表：根据小时、日、周和月建立一次性或循环时间表，防火墙根据不同的时间表定义安全策略。

虚拟映射：通过把外部地址映射到内部或DMZ网络上的地址使得外部用户能够访问内部的服务器。

IP/MAC 绑定： 自动进行IP与MAC地址的绑定，阻止来自IP地址欺骗的攻击。

流量控制:
允许管理员定义带宽限制并且可以给特定的防火墙策略设置优先等级。

VLAN支持 ：利用虚拟域来支持VLAN子接口

反病毒控制：基于防火墙访问策略的细粒度病毒防御。

虚拟专用网 （ICSA 实验室认证）
在网络之间或网络与客户端之间进行安全通讯，支持工业标准的IPSec、PPTP、L2TP。

密钥交换算法： 支持自动IKE和手工密钥交换。

硬件加速加密： 支持DES，3DES和AES加密算法。

VPN客户端通过：支持IPSec 和 PPTP &L2TP 客户端通过。

Hub_and_Spoke:星型VPN网络

NAT_Traversal: 穿越NAT外部网络

入侵检测系统(ICSA 实验室认证)
实时的基于网络的入侵检测。

攻击数据库：用户可配置的超过1300种攻击特征库确保可靠的管理。

攻击检测： 检测已知的DOS、DDOS攻击，以及绝大多数操作系统和应用协议的漏洞。

邮件报警： 当监测到攻击时，防火墙会同时向3个邮件地址自动发出警报。

高可用性(HA)

在失败恢复期间提供“0”中断。

支持Active-Active负载共享

HA接口：可定义的“HA”高可用接口，连接两台防火墙状态失败恢复。

可靠性
冗余电源的支持确保发生电源故障时网络防御继续运行。
热交换能力：在电源发生故障时，冗余的电源能够在不中断供电的情况下快速安全的切换过来补给供电。
日志和报告
将日志记录到可选择的 20G 内部硬盘、远程 Syslog 主机或 NetIQ Webtrends 防火墙报表中心。
多种日志: 流量、事件和攻击日志。

搜索功能: 可以根据关键字,来源,目的,日期和时间搜索日志记录。

管 理
易于使用的、安全的图形化和命令行界面。

快速配置模版：根据配置模版，逐步配置。

图形配置界面：通过IE浏览器进行管理。

多语言支持 ：支持英文、中文、日文和韩语。

安全远程管理：通过浏览器界面，使用HTTPS ，HTTP远程登录管理；还可以通过命令行界面，使用SSH,Telnet远程管理。

LCD配置管理：使用前面板简单的按键和LCD对接口地址快速设置。

命令行界面 ：提供Console口或安全远程连接。

2.1 FortiGate-50A

FortiGate-50A病毒防火墙是一款紧凑小巧的、易于安装的、适合小型办公室或家庭办公(SOHO)网络安全的产品。体积虽小，但功能齐全。FortiGate-50A尤其适合在小型企业、分支机构，例如公司分部、呼叫代理或服务提供商等不同用户群的需求。

系统性能

防火墙性能：50Mbps
3DES(168-bit)：10Mbps
并发会话数：25,000
VPN通道数：20

接 口

2个10/100 BaseTX 端口（内部,外部）
1个RS232 Console 端口（9600）

2.2 FortiGate-60

FortiGate-60病毒防火墙是一款紧凑的、易于安装的适合小型办公室或家庭办公（SOHO）网络安全的产品。体积虽小，但功能齐全。FortiGate-60的功能能够满足从小型企业和分支机构到中型企业不同用户群的需求。FortiGate-60 的性能价格比很好。

系统性能

防火墙性能：70Mbps
3DES(168-bit)：20Mbps
并发会话数：50,000
VPN通道数：40

接 口

7个10/100 BaseTX 端口（4个内部接口,3个外部/DMZ接口）
2个USB端口
1个RS232 Console 端口（9600）

2.3 FortiGate-100

FortiGate-100病毒防火墙是适合需要性能 高的小型企业网络安全产品。它包含一个DMZ口用来提供本地Email和Web服务器的。并且容易安装，可通过方便的Web界面管理。FortiGate-100是FortiGate系列病毒防火墙产品的一款，该系列产品满足从小型企业到大型企业和服务提供商的安全需求，是一套全面的、有效的解决方案。

系统性能

防火墙性能：95Mbps
3DES(168-bit)：25Mbps
并发会话数：200,000
VPN**通道数：**80

接 口

3**个**10/100 BaseTX **端口（内部,外部和**DMZ）
1 **个**RS232 Console **端口（**9600）

2.4 FortiGate-200

FortiGate-200**病毒防火墙为中型企业或企业分支机构提供了最好的性价比,能够支持内部带硬盘，用来记录日志和做攻击分析。**FortiGate-200**病毒防火墙易于管理，与**FortiGate™ **其他产品完全兼容。**FortiGate-200**适合从小型企业到中型企业和运营提供商的安全需求。**

系统性能

防火墙性能：120Mbps
3DES(168-bit)：50Mbps
并发会话数：400,000
VPN**通道数：**100

接 口

3**个**10/100 BaseTX **端口（内部,外部和**DMZ)
1 **个**RS232 Console **端口（**9600）

2.5 FortiGate-300

FortiGate-300**病毒防火墙是满足中型企业或企业分支机构网络安全需求的产品，尤其适合大型的远程访问环境。**FortiGate-300**能够很容易的集成到现有的网络，和**FortiGate™ **其他产品完全兼容。该产品家族满足从小型企业到大型企业和服务提供商的安全需求，是FortiGat系列产品中使用最多、应用全面的的一款型号。**

系统性能

防火墙性能：200Mbps
DES(168-bit)：65Mbps
并发会话数：400,000
VPN**通道数：**1,500

接 口

3个10/100 BaseTX 端口（内部,外部和DMZ)
1 个RS232 Console 端口（115200）

2.6 FortiGate-400

FortiGate-400病毒防火墙是企业级的网络安全产品，它的四个端口能够配置成独立的安全区域，包括专用的高可用性端口， 适合于分区管理。它是重要应用的完美选择，并且能够很容易的集成到现有的网络，和FortiGate™其他产品完全兼容，适合从小型企业到大型企业和服务提供商的应用。

系统性能

防火墙性能：280Mbps
3DES(168-bit)：80Mbps
并发会话数：400,000
VPN**通道数：**2,000

接 口

4个10/100 BaseTX 端口（内部,外部,HA和DMZ）
1 个RS232 Console 端口（9600）

2.7 FortiGate-500

FortiGate-500 病毒防火墙为企业、部门层次级的细粒度安全和内容控制提供了空前的能力。 它具有12个可配置端口，能够使网络分段成不同的区，对不同的段配置不同的策略。FortiGate-500支持冗余配置，以保证最大的在线时间。它和FortiGate™其他产品完全兼容，应用范围广， 适合从SOHO到大型企业和服务提供商的应用。

系统性能

防火墙性能：280Mbps
3DES(168-bit)：90Mbps
并发会话数：400,000
VPN**通道数：**2,000

接 口

12个10/100 BaseTX 端口（内部,外部,HA和DMZ）(8个用户可定义端口)
1 个RS232 Console 端口（9600）

2.8 FortiGate-800

FortiGate-800病毒防火墙的特色是具有使网络可运行到千兆级的4个10／100／1000 三种速率以太网端口和4个用户可定义的10／100端口。 它能够通过网络分成不同区域，使用户实现网络细粒度分段安全管理， 并在区域之间配置不同的策略。FortiGate-800适合从SOHO到大型企业和服务提供商的应用，提供必要的性能、灵活性和安全性。尤其在要求高速率、灵活运用、和细粒度安全管理网络流量时，FortiGate-800是理想的解决方案

系统性能

防火墙性能：600Mbps

并发会话数：400,000

每秒建立： 10,000新会话

VPN通道数： 2,000

接 口

4 个 10/100/1000 三种速率以太网端口， 对网络升级到千兆级速率降低了成本

2.9 FortiGate-1000

FortiGate-1000病毒防火墙具有 1Gbps的系统性能，确立了更新层次的性价比。 产品提供了一套完整的包括防病毒、 防火墙、内容过滤、VPN、NIDS和流量控制功能。 它既可以在现有网络环境下很容易地安装以达到防病毒和内容过滤目的，也可以用作全面的网络安全解决方案。FortiGate-1000的可支持高可用性连接，增强可靠性，确保其不间断运 行。

系统性能

防火墙性能：1Gbps

3DES(168-bit)：250Mbps

并发会话数：600,000

VPN通道数：3,000

接 口

4个10/100 BaseTX 端口

2个铜芯千兆端口

1个RS232 Console 端口（9600）

2.10 FortiGate-3000

FortiGate-3000病毒防火墙是适合多千兆网络的运营商级的安全产品，为企业和服务提供商提供高价值的、高可用的安全和内容控制服务。它支持实时的防病毒扫描，有2.25Gbps

吞吐量和VPN3DES加密530Mbps的性能。FortiGate-3000是提供不同管理服务的理想平台。多区域配置能够使端口分配到一个部门，并设置唯一的策略。它支持冗余电源，提高可靠性，高可用性端口则保证了在不间断运行状态下透明的进行灾难恢复。

系统性能

防火墙性能：2.25Gbps
3DES(168-bit)：530Mbps
并发会话数：975,000
VPN**通道数：**5,000

接 口

2**个光纤千兆端口**
1**个铜芯千兆端口**
3**个**10/100 BaseTX **端口**
1**个**RS232 Console **端口（**9600**）**

2.11 FortiGate-3600

FortiGate-3600是一款适合大型企业和服务提供商的高端产品，提供了2个铜缆千兆口和4个光纤接口，还有一个10/100兆以太网口。它的1,000,000并发连接数和4Gbps的吞吐量能够适应不同的网络环境， 达到用户所需的高性能。

系统性能

防火墙性能：4Gbps
3DES(168-bit)：600Mbps
并发会话数：1,000,000
VPN**通道数：**8,000

接 口

4**个光纤千兆端口**
2**个铜芯千兆端口**
1**个**10/100 BaseTX **端口**
1 **个**RS232 Console **端口（**9600**）**

2.12 FortiGate-4000

FortiGate-4000系统是由一个机箱和多个模块组成的。由于模块化结构，系统在吞吐量、冗余和端口需求量变化时能够相应地调整。FortiGate-4000机箱采用热插拔的电源和风扇模块，以保障供电和冷却的高可用性，并且配备了支持带内、带外管理的管理模块。FortiGate-4000机箱有十个插槽，可以插入十个FortiBlade-4010模块，满载时吞吐量达20Gbps。每个模块内置FortiASIC内容处理芯片，都具有防火墙、VPN、防病毒、入侵检测和阻挡、Web和email内容过滤和流量控制功能。

FortiGate系统的外部端口和集群选项使得它能支持多种应用，例如：

- 主机托管数据中心，每个FortiBlade-4010模块可以专供一个服务器群或一个客户
- 宽带接入服务中的病毒屏蔽
- 服务提供商接入点的内容屏蔽
- 企业总部和数据中心处的内容安全

FortiGate-4000系统可以采用以下两种FortiBlade-4010基本配置：

型号FortiGate-4000S是通过增加FortiBlade模块和采用Fortinet集群协议来扩展系统吞吐量的。它的基本配置主要包括以下几部分：

- 一个FortiGate-4000机箱
- 两个10×2接口的千兆交换模块
- 两个FortiBlade-4010模块
- 七个热插拔电源模块
- 四个热插拔风扇模块
- 一个10/100以太网模块(用于带外管理)
- 一个附加的管理模块(连接到FotiBlade-4010控制台接口)

FortiGate-4000S在基本配置基础上最多还可以再增加8个FortiBlade-4010模块，也就是说总共10个FortiBlade模块。多个FortiBlade模块通过集群方式，达到几千兆过滤病毒流量。

型号FortiGate-4000P系统是用于直接连接到每个FortiBlade-4010模块的应用环境。它的基本配置是由以下部分组成的：

- 一个FortiGate-4000机箱
- 两个10端口千兆吞吐量的接口模块
- 两个FortiBlade-4010模块
- 七个热插拔电源模块

- 四个热插拔风扇模块
- 一个10/100以太网模块(用于带外管理)
- 一个附加的管理模块(用于连接到FortiBlade-4010串口)

2.13 FortiGate-5000

FortiGate-5020系统病毒防火墙设计使用FortiGate-5020机箱，并装有1个或2个模块，以提供各种不同的吞吐量、冗余量和接口要求。FortiGate-5020机箱支持冗余热交换式电源模块，

以保证高可用性和不间断的运行。对于可扩展的吞吐量， FortiGate-5020机箱具有2个插槽，以适应FortiGate-5001母板式模块，每一个都装有FortiASIC™内容处理器芯片和提供高性能防火墙、VPN、，反病毒、入侵检测、Web和电子邮件内容过滤和流量控制功能和流量 控制功能。FortiGate-5001母板式模块具有4Gb小型规格尺寸插拔式(SFP)端口和4个三速Gb以太网端口。FortiGate-5020系统提供细粒化安全防护，能分别对每一组或部门予以设置唯一的策略，支持独立的安全区和映射到VLAN标签的策略。FortiGate-5020单元由Foritnet公司的FortiProtect™网络实时地自动更新攻击数据库。该网络提供持续的攻击库更新，以保护网络不受病毒、蠕虫、木马及其他攻击， 使网络随时随地的得到安全保护。

系统性能

防火墙性能：4Gbps， 8Gbps

3DES(168-bit)**:** 600Mbps， 1200 Mbps

并发会话数： 1,000K, 2000K

VPN**通道数：**5,000， 1,000

接 口

4**个，8个光纤千兆端口**

4**个，8个**10/100/1000 BaseTX **端口**

2.14 FortiManager系统

FortiManager网络管理产品集成在统一的硬件平台上。FortiManager系统包括控制台、服务器、和监视／日志三层体系结构， 其中服务器是集成在硬件上， 可支持数千台FortiGate 设备， 可以升级许可证等级。 通过集中管理器可以管理病毒防火墙所有的功能配置， 实时监控设备工作状态，并监控攻击时间和流量。

3. 产品功能和特点

3.1 病毒防火墙新理念

传统的防火墙和VPN设备不能阻止病毒和非法的网络内容进入网络内部，它们无法解决对进入内部的邮件、文件和Web页面进行应用层检测而花费巨大系统资源的问题，所以传统的网络设备无法阻止来自网络的病毒和不适合的内容。单一的防病毒产品（包括软件或硬件）无法做到网关级的病毒扫描，并且要配置适应不同的操作系统或软件系统才能做到防病毒，也不具备网络安全的其他功能，从安全整体性到对网络适应的灵活性都很难达到要求。

FortiGate病毒防火墙利用ASIC硬件技术进行数据包内容病毒扫描，保证了网络的性能。它能够对进出FortiGate设备的数据流做实时病毒扫描处理，并且100%覆盖业界著名的Wildlist组织的病毒库，提供了用户手动、自动升级病毒库，或服务器推送式病毒库更新功能。而且FortiGate还具有防火墙、VPN、NIDS和内容过滤等安全功能。所以FortiGate称之为病毒防火墙，也是世界上唯一基于ASIC芯片技术且获得ICSA认证的病毒防火墙。

3.2 FortiGate 系列

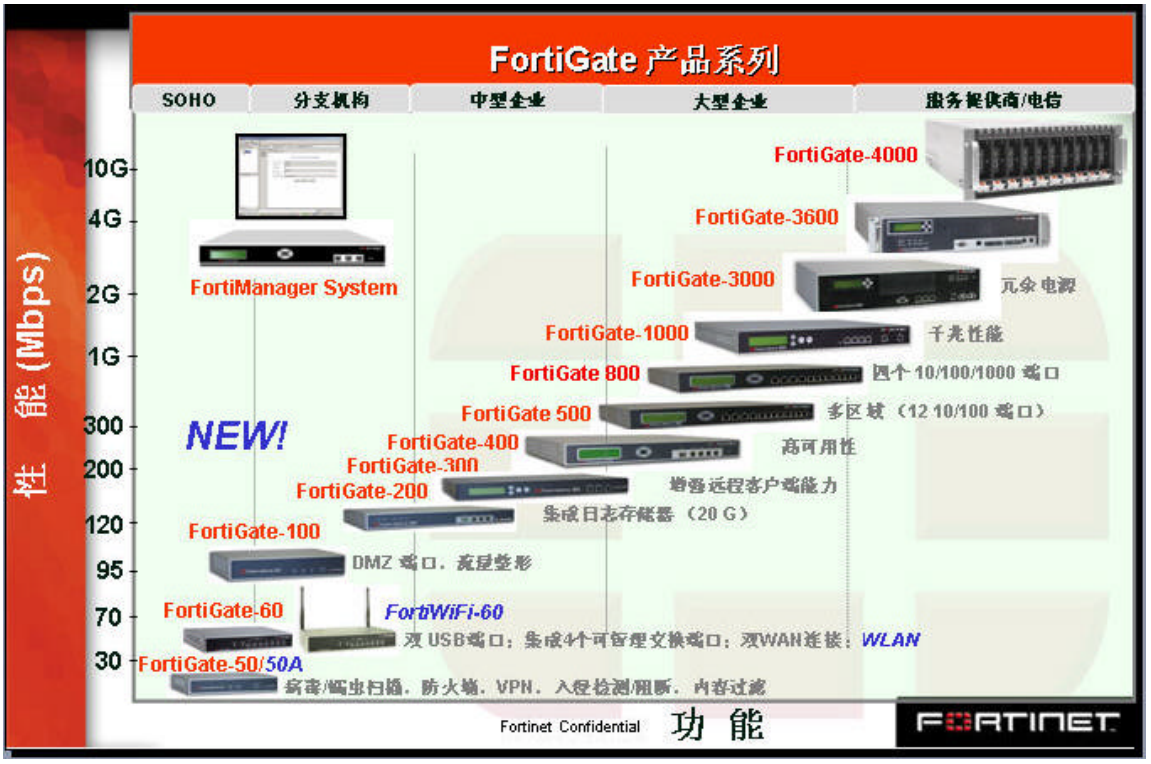


图 一 FortiGate产品系列功能/性能图

3.3 基于网络的防病毒

互联网是一个连接全球丰富资源的大网络。随着互联网应用的飞速发展，用户对网络信息的依赖性也倍速增长，但是网络病毒也伴随着网络的发展而迅速增长，互联网的技术支持需求随之成为企业IT部门最主要的业务负担。为网络全方位安全而设计的基于网络的病毒防火墙FortiGate系列， 着眼点是为了保障互联网的畅通和安全。

FortiGate病毒防火墙是网关级安全设备，它不同于单纯的基于主机的防病毒产品。FortiGate在网关上做HTTP、SMTP、POP3、FTP和IMAP的病毒扫描，并且可以通过策略控制流经不同网络方向的病毒扫描或阻断，充分体现应用的灵活性和安全性。

3.4 分区域安全管理的特色

安全域是在同一个平等的安全层次上传送流量的一组接口，域间的流量不在同一个平等的安全层次上，必须有安全策略来控制，同一安全区域内的接口可以屏蔽通信或开启通信。FortiGate安全域包含系统域定义的和用户自定义的安全域，策略引擎控制域间流量，明确列出来源和目的域的策略控制。各安全域之间不但可以自由设置工作模式 NAT/ROUTE，而且可以自由设置安全级别。

3.5 VPN功能

FortiGate产品系列工业标准的VPN在两个FortiGate保护的网络或FortiGate与支持IPSec、PPTP或L2TP的第三方VPN保护的网络之间， 建立加密流量传输隧道。

VPN隧道终止后，FortiGate自动地加密VPN流量，并发送内容穿过反病毒引擎。

FortiGate VPN的特性包括以下几点：

- 支持IPSec安全隧道模式
- 支持基于策略的VPN通信
- 硬件加速加密IPSec,DES,3DES
- HMAC MD5 或 HMAC SHA认证和数据完整性
- 自动IKE和手工密钥交换
- SSH IPSEC客户端软件，支持动态地址访问，支持IKE
- 通过第三方操作系统支持的PPTP建立VPN连接
- 通过第三方操作系统支持的L2TP建立VPN连接
- IPSec和PPTP
  VPN穿越使你的内部网络的计算机或子网能够连接到互联网上的VPN网关
- IPSec NAT在途径NAT设备阻断的情况下建立IPSec隧道

- 支持HUB-and-Spoke星型VPN，该功能允许在在分支机构与总部之间容易地建立VPN隧道，这样减轻了管理员在许多分支机构与总部之间维护需要安全通讯的VPN隧道。

3.6 防火墙功能

FortiGate系列产品防火墙都是基于状态检测技术的，保护你的计算机网络免遭来自Internet的攻击。防火墙通过仔细地设置接口，提供了安全控制策略，甚至在复杂的情况下仍可做详细的控制。

FortiGate 安全策略完全包括了以下所有选项：

- 基于策略的反病毒和Web内容过滤
- 通过网络分段和细粒度的策略到达多个区域
- 控制输入、输出流量
- 对所有策略选项支持阻止、允许、加密、认证访问
- 基于时间的策略控制
- 接收或拒绝单个地址到达或发送的流量
- 控制个别组标准的和用户自定义的网络服务
- 对用户授权认证，支持基于用户的策略控制
- 对每个策略可以进行基本带宽、保障带宽以及优先级设置的流量控制
- 支持动态IP地址池，允许配置使用地址池的NAT灵活策略
- 基于策略的日志记录

3.7 独特的内容过滤

FortiGate的内容过滤不同于传统的基于主机系统结构内容处理产品，FortiGate设备是网关级的内容过滤，是基于ASIC芯片硬件技术实现的。FortiASIC™内容处理器包括功能强大的特征扫描引擎，能使很大范围类型的内容与成千上万种关键词或其它模式的“特征”相匹配。具有根据关键字、URL或脚本语言等不同类型内容的过滤，还提供了免屏蔽列表和组合关键词过滤的功能。

3.8 基于网络的IDS/IDP功能

FortiGate网络入侵侦测/阻断系统(NIDS/IDP)是一种实时网络入侵检测传感器， 它能对外界各种可疑的网络活动进行识别及采取行动。NIDS使用攻击特征库来识别超过1300多种的攻击。为通知系统管理员有攻击，NIDS将此攻击及一切可疑流量记录到攻击日志中，并根据设置发送报警邮件。

Fortinet可定期更新攻击数据库。您可下载并手动安装攻击数据库。也可设置FortiGate自动查询和下载更新的IDS数据库。

Fortinet NIDS/IDP可以检测并阻断多种类型攻击，例如拒绝服务攻击（包括Smurf flood，TCP SYN flood,UDP flood和ICMP flood，Ping of Death，Tear drop等）。

3.9 VPN远程客户端软件

Fortinet Remote VPN Client是远程VPN客户端软件，使用了工业标准的IPSec加密和认证和因特网密钥交换（IKE）管理技术。IPSec客户端软件，安装在Windows主机（桌面或笔记本电脑）或工作站上，目的在于保护基于IP的通信，简化对网络、设备、公共或非信任网络中其它主机的安全远程接入。通过采用IPSec协议和第二层通道协议（L2TP）实现安全性。

Fortinet的远程VPN客户端软件的独特之处是带有个人防火墙，保护远程客户免受攻击和恶意流量，防范网络后门攻击，有条件地过滤进出流量，并提供IPSec数据加密前和IPSec数据加密后过滤。借助防火墙的功能， 网络确保只有经过选择的流量和应用才能允许进入和离开VPN。同时，网络地址转换技术保证了远程VPN客户端与已有的防火墙和网络地址转换系统可以容易地集成。VPN集中管理使管理员能从中心控制和改变安全策略。

3.10 FortiASIC技术和FortiOS 操作系统

FortiGate操作系统（OS）是专用的、实时的强化安全的操作系统，它在安全平台上支持病毒扫描，内容过滤，状态检测防火墙，IP安全（IPSec）VPN，基于网络的IDS和流量管理应用。以下介绍其设计特点、应用级和网络级功能。

3.10.1 高性能并行处理

FortiGate采用新一代ASIC设计体系，利用OS有效地分解和协调系统的处理任务。在任一特定时间，每个数据流都得到最佳的处理水平。由于利用了独特的算法，任务切分和协调过程中的消耗减到了最小程度。

3.10.2 实时体系结构

与非实时OS（例如许多防火墙和设备采用的不同风格的Linux）相比，OS是使数据流程处理达到优化的实时操作系统。在非实时OS中，核心并不总是对输入的数据包触发的中断作出及时反应；这不仅使数据包排队时间增长，而且造成系统资源（例如内存）不能有效地利用，因而增加了丢包率。OS的设计集成了智能排队和管道管理，与包的到达/处理相关的系统中断得到立刻的重视。同时，基于内容处理加速模块的硬件加速（见下一段）使各种类型流量的处理时间达到最小，加上最短的排队时间，从而给用户提供了最好的实时系统。

3.10.3 实时内容级智能

FortiGate系统设计为综合基于网络的和基于代理的两种网关的优点，具有基于流的检测引擎和多应用级代理（HTTP, SMTP, POP3, IMAP）引擎。独特的系统专利设计在包检测和

代理之间给出最佳的协调，由ASIC和在FortiGate中的内容加速单元提供了基于代理系统的智能，而在性能上达到很高的水平。

3.10.4 提供分区间安全的虚拟系统支撑

用户能够建立一个单个的FortiGate单元行为，就好象它包含大量的独立的“虚拟系统”，它们提供专门的服务，对各个部门或用户分别具有自己独特的策略。FortiGate体系结构中设计了虚拟系统支持。符合802.1Q标准的一个或多个VLAN能被映射到一个虚拟系统，带有VLAN中继支持的交换机/路由器与FortiGate的物理接口相连接。FortiGate-3000千兆产品能提供多达500个虚拟系统。基于不同的管理员可以管理不同的虚拟系统，使它们建立和维护它们自己的一套安全策略、地址和地址组，以及监视系统状态。

3.10.5 高可用性(HA)

FortiGate通常用于关键任务环境，例如运营服务商基础设施或大型企业，不能容忍由于任何一点故障而丢失业务。用户使用备份的一对FortiGate单元，并利用Fortinet Redundancy Protocol（FGRP）协议，来确保万一有故障发生时的故障恢复实现零中断，通过专用的HA链路传输设备的监控（心跳）信息：

- 通过心跳监控，来检测每一个设备的运行状态，当有一个设备发生故障（包括网络故障、设备故障、电源故障等），业务会马上转接到另一个系统中。
- 链接状态监视
  FortiGate监视上行和下行交换机/路由器的流量状态，可以为维持连接而从备份状态转到使用状态。
  FortiGate能利用FGRP的能力，配置为完全的备份环境，使得没有单个点的故障。能配置为支持热备份模式（Active-Passive）或负载共享模式（Active-Active）。

3.11 FortiGate提供整体解决方案

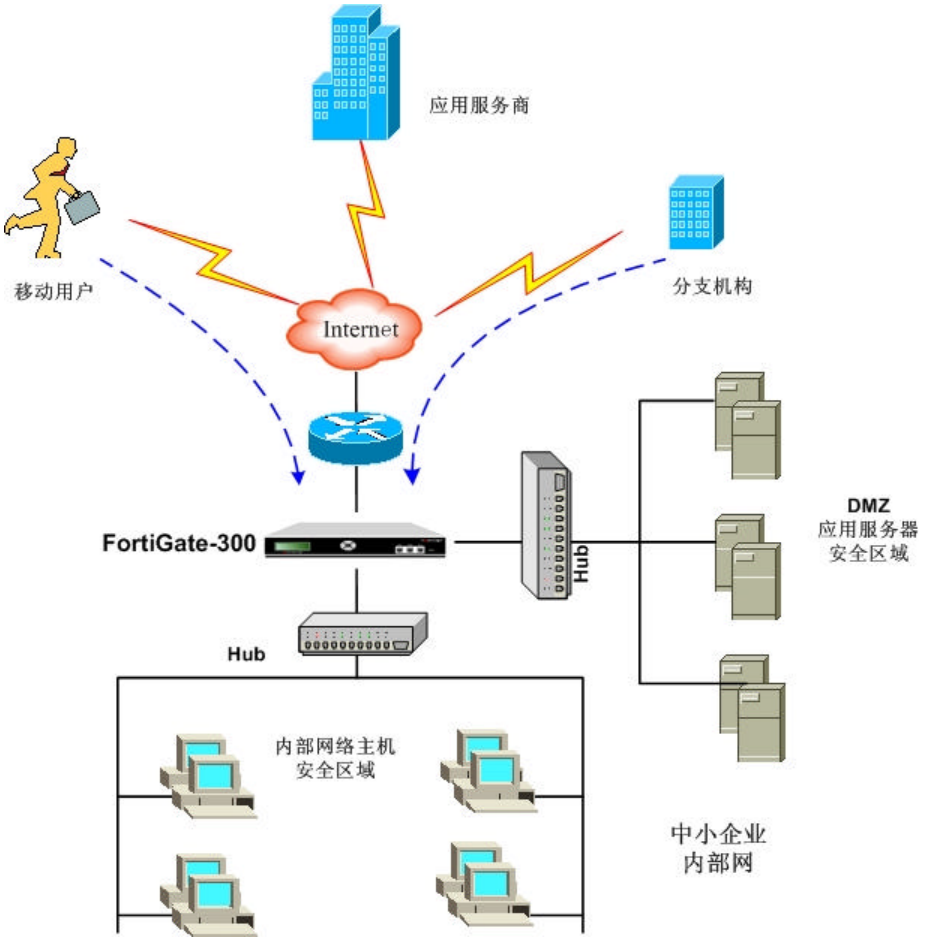
FortiGate在网络边界部署应用层内容过滤服务，具备防火墙、虚拟专用网VPN、网络入侵检测、防病毒/蠕虫、Web内容过滤等功能，在维持网络传输速度的同时，确保网络安全的实时性、有效性，提供完整的全方位网络与信息安全解决方案。

FortiGate系列产品众多，产品线丰富，无论是个人办公、SOHO一族，还是中小型企业，或是大型企业和运营服务商，FortiGate都能提供最佳选择。同时FortiManager™ 软件支持远程管理多端设备的大型集群安装,并拥有多区域安全管理解决方案。

4. FORTIGATE防火墙典型应用方案

4.1 中小型企业防火墙应用

- 策略控制
- 病毒防御
- 网络攻击防御
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 远程VPN安全访问

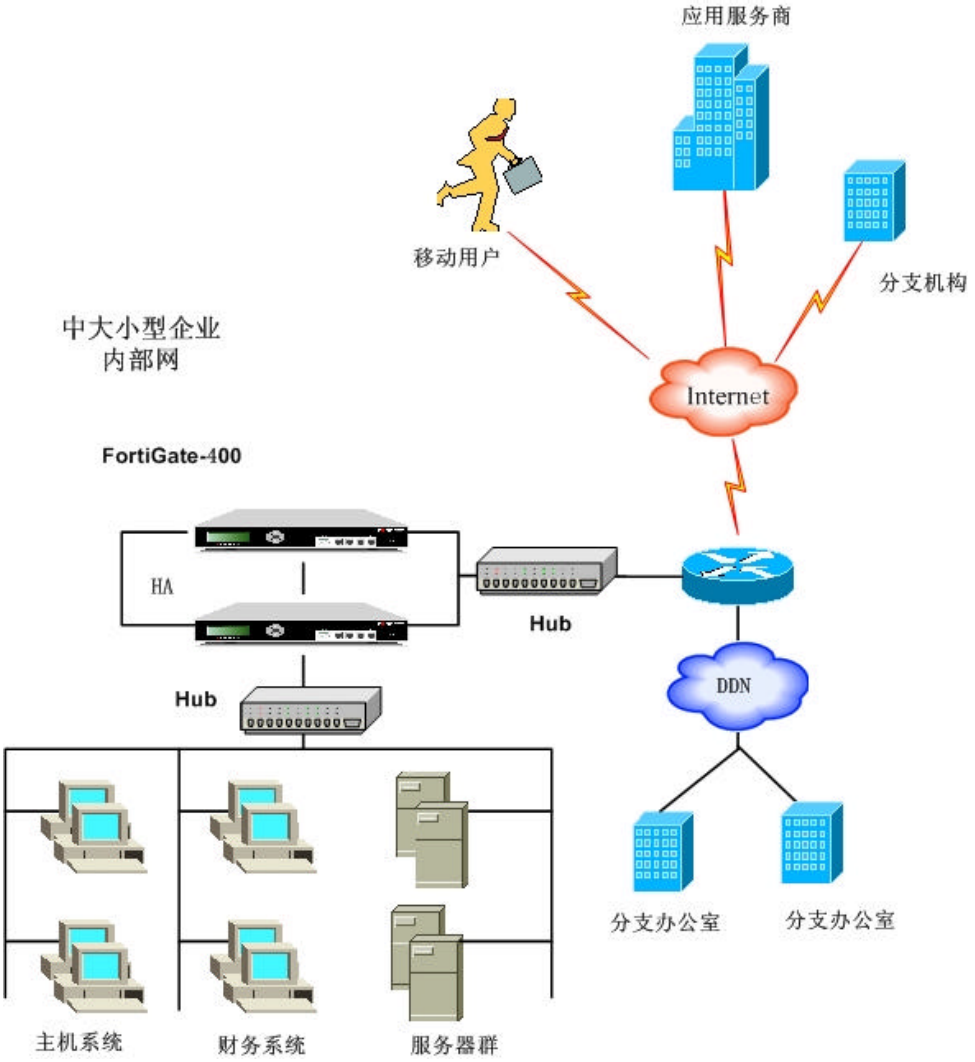


图二 中小型企业防火墙应用

在本应用中，企业内部网络被划分成两个物理网段，对外发布信息的服务器放置在DMZ（非军事区），通过策略控制来限制外部用户的合法访问。内部主机放置在内部网中，通过防火墙NAT地址翻译访问Internet公网资源，同时可以根据用户的不同部门通过防火墙屏蔽有害的邮件（如红色代码、求职信、尼姆达等病毒入侵），对于放置在DMZ区的邮件服务器和Web服务器来说可以通过FortiGate-300提供内容层保护，屏蔽有害邮件和恶意攻击。

4.2 中大型企业防火墙应用

- 策略控制
- WEB内容和有害网页控制
- 网络攻击防御
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 远程VPN安全访问
- HA双冗余配置



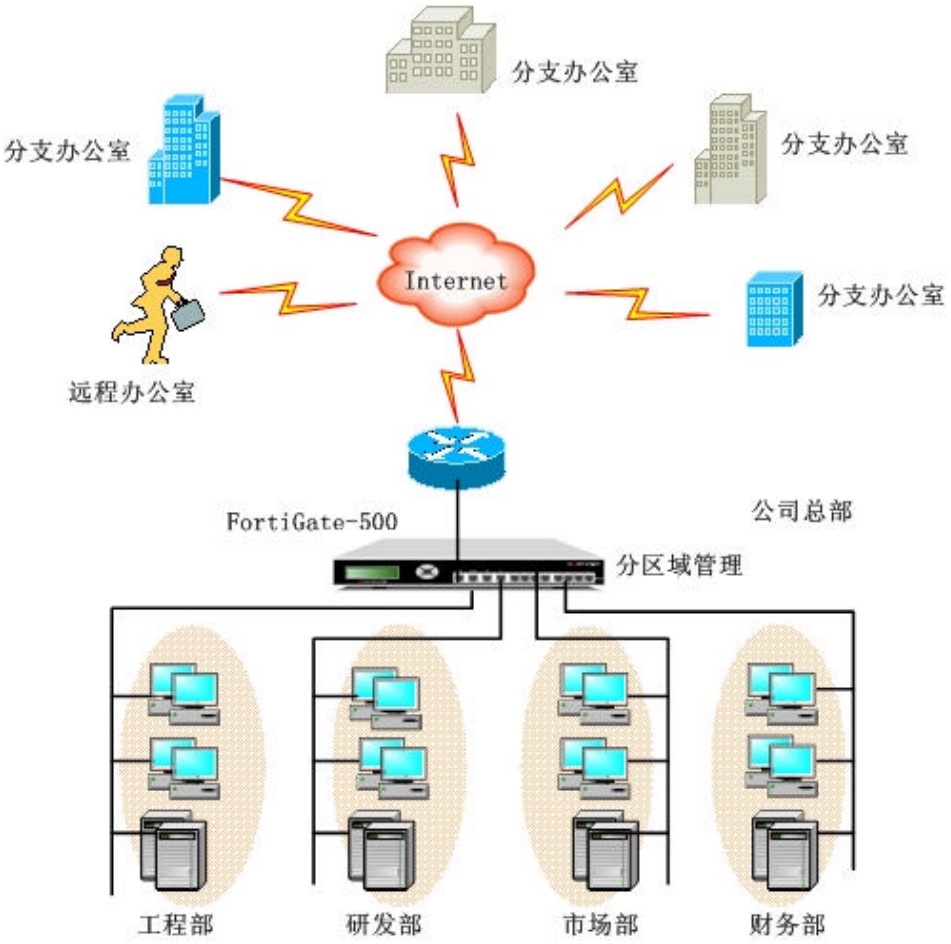
图三 中大型企业防火墙应用

在本应用中，企业内部网络在Internet出口配置两台FortiGate防火墙，采用了双机冗余配置，避免单点故障发生。对外发布信息的服务器和内部主机都放置在内部网，通过VIP地址影射和端口影射发布服务，同时通过策略控制来限制外部用户的合法访问。内部主机通过防

火墙NAT地址翻译访问公网资源，可根据用户的不同限制所访问的WEB内容和地址，可建立基于时间的访问策略控制对一些聊天游戏等与工作无关内容的访问，避免占用有效的带宽。

4.3 分布型企业防火墙应用

- 策略控制
- WEB内容和有害网页控制
- 网络攻击防御
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 分支企业和总部的VPN安全访问



图四 分布型企业防火墙应用

在本应用中，企业总部网络在Internet出口配置FortiGate-500防火墙。FortiGate-500防火墙可以提供12个接口，充分解决了企业总部不同部门之间的安全控制。如图所示，企业总部有四个主要的应用部门，分别是工程部、研发部、市场部和财务部。通过FortiGate-500的多接口和安全控制功能，物理隔离了四个部门，使部门之间的访问通过集中的管理进行限制，对外发布信息的服务器和内部主机分布在不同的部门之间或集中到一个网络，通过VIP地址影射和端口影射服务开放服务，同时通过策略控制来限制外部用户及分支企业的合法访问。

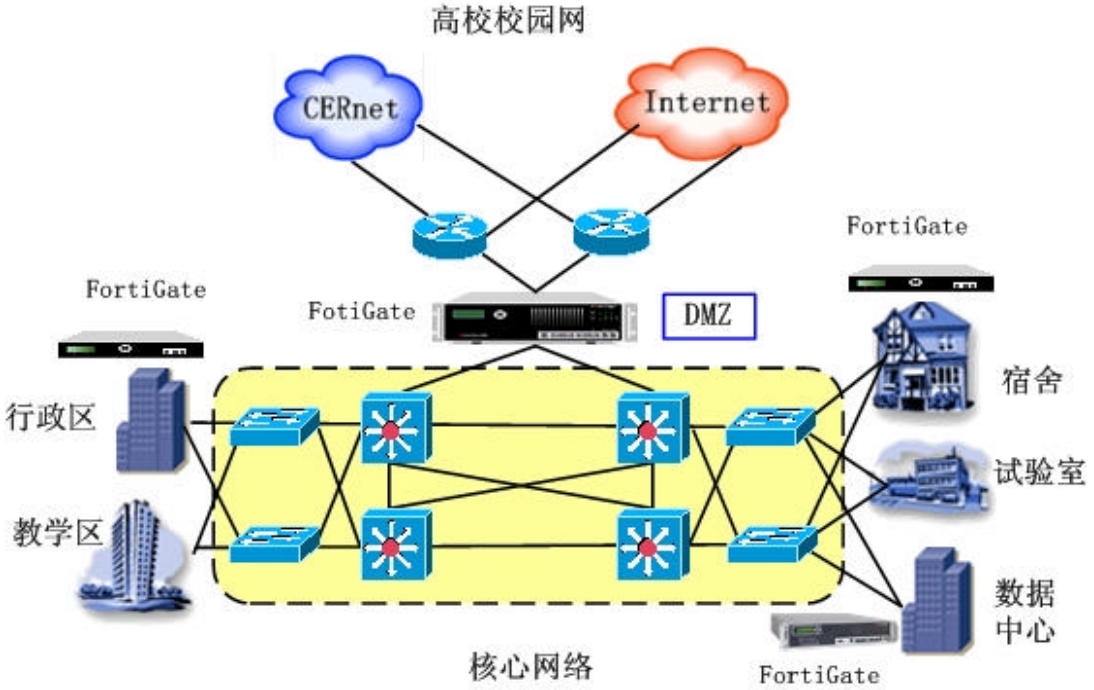
内部不同部门通过防火墙NAT地址翻译访问Internet公网资源，同时可以根据用户的不同部门限制其所访问的WEB内容和地址，还可以建立基于时间的访问策略来控制对一些聊天、游戏、电影等与工作无关内容的访问，避免占用有效的网络带宽。

各企业分支机构可以和总部建立VPN的隧道连接，利用3DES168位最高加密算法提供了高强度的数据安全。VPN系统使分布在不同地方的专用网络在不可信任的公共网络上安全的通信。它采用复杂的算法来加密传输的信息，使得敏感的数据不会被窃听。

一般网络系统中，如果网络系统总部和各分支机构之间采用公网网络进行连接，其最大的弱点在于缺乏足够的安全性。总部企业网络接入到公网中，会暴露出两个主要危险：一是来自公网的未经授权的对企业内部网的存取，二是当网络系统通过公网进行通讯时，信息可能受到窃听和非法修改。利用FortiGate完整的集成化的企业范围的VPN安全解决方案，提供了在公网上安全的双向通讯，以及透明的加密方案以保证数据的完整性和保密性。

4.4 校园网安全部署应用

在该应用中，网络出口处和数据中心都部署千兆级防火墙FortiGate，下面分成几级，可安装FortiGate-200 或FortiGate-300。对外发布信息的服务器 放置在DMZ，通过策略控制来限制外部用户的合 法访问。把学校分成几个安全区， 例如图中有5个区域， 分别为数据中心、教学区、行政区、实验室、宿舍区。一旦网络出现问题时，易于定位分析。FortiReporter的图形报告可以搜索显示网上状况，例如谁在上QQ，可列出全部名单。

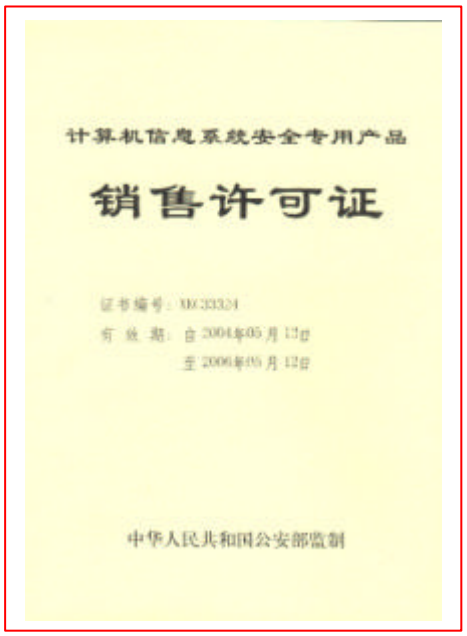


图五　高校校园网安全部署拓扑图

5. 销售许可证和认证证书

5.1 公安部硬件防火墙销售许可证

公安部销售许可证号：XKC33324


计算机信息系统安全专用产品

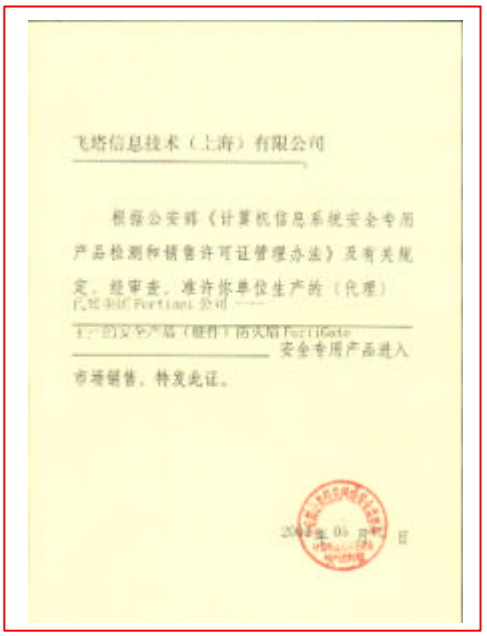
销售许可证

证书编号：XKC33324

有 效 期：自 2004年05月12日

至 2006年05月12日

中华人民共和国公安部监制


飞塔信息技术（上海）有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）代理美国 Fortinet 公司 ——

下产的 FortiGate（硬件）防火墙 FortiGate

安全专用产品进入市场销售，特发此证。

2004 年 05 月 12 日

5.2 公安部病毒防火墙销售许可证

公安部销售许可证号：XKA10248 通过中国计算机病毒防治产品检验中心测试


计算机信息系统安全专用产品

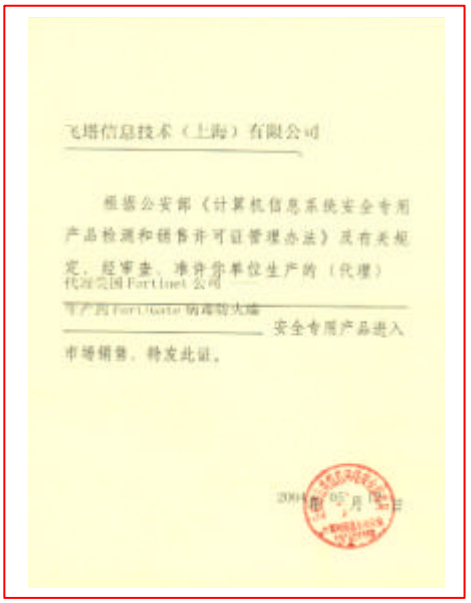
销售许可证

证书编号：XKA10248

有 效 期：自 2004年05月12日

至 2006年05月12日

中华人民共和国公安部监制


飞塔信息技术（上海）有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）代理美国 Fortinet 公司

下产的 FortiGate 病毒防火墙

安全专用产品进入市场销售，特发此证。

2004 年 05 月 12 日

5.3 中国信息安全产品测评认证中心

2004年获得中国信息安全产品测评认证中心认证证书. 注册号： CNITSEC2004TYP23

5.4 计算机世界推荐产品奖

2004年3月FortiGate-3000获得计算机世界企业级千兆防火墙推荐产品奖。

Fortinet 是唯一一家获此殊荣的公司。

5.5 中国计算机学会奖项

美国Fortinet公司2004年5月日获得中国计算机学会计算机安全专业委员会、中国计算机报颁发的以下奖项：

2004年中国信息安全值得信赖的防火墙产品

2004年中国信息安全电信领域值得信赖的品牌

5.6 ICSA认证证书

在美国著名的ICSA Lab**先后获得** AntiVirus, IPSec, Firewall，IDS **四项认证证书。**

5.7 在美国获奖

Fortinet 荣获《计算机世界》2002年度新技术评比最佳网络产品奖

Fortinet 荣获《网络通信》杂志2002年度产品奖

Fortinet 病毒防护防火墙产品获得“ SC杂志 ”的SC Awards 2003最佳产品提名

Fortinet 网络安全网关入选InfoWorld十强产品

Fortinet 赢得“ 个人电脑 ”杂志评测的极高评价

2003年6月，FortiGate 400获得享有声誉的美国“ Miercom ”网络推荐认证

2004年1月，FortiGate-3600病毒防火墙荣获《搜索网络》的“ 年度产品金奖 ”

2004年2月，FortiGate-3600病毒防火墙荣获CRN测试中心推荐产品

6. 技术支持方式

6.1 北京办事处技术支持

Fortinet北京办事处为所有用户提供技术支持。用户在使用产品时遇到任何问题，均可及时与办事处联系，技术支持热线号码为：010-8251 2622。电子邮箱：support@fortinet.com

6.1.1 技术支持、售后服务及人员培训

北京办事处有独立的技术支持服务部门。目前，已经建立了一套完整的技术支持和售后服务体系，在人员、技术和服务等多方面完全有实力满足用户的需要。可通过电话和邮件方式， 为全国范围内用户提供远程支持。针对重点客户，可组织专门的客户服务小组，及时提供优质的技术咨询、技术培训、技术实施、技术支持、故障排除、维护支持等综合服务。

6.1.2 服务组织结构

北京办事处建立了以北京办事处为中心，以Fortinet在中国的一级分销商为二级服务中心，辐射全国的客户服务技术咨询和技术支持中心。北京办事处为各一级分销商提供咨询、培训和监督，以及响应服务。各分销商直接参与技术实施、用户咨询培训和产品维护服务。

6.1.3 技术咨询和培训

为各分销商和合作伙伴的技术人员提供定期的技术咨询服务和培训，包括网络安全常识问题的解答，产品介绍，系统配置说明，安全策略的制定，日常维护常见疑难问题解答。为了使用户能够独立完成安全系统的日常维护和管理工作，包括FortiGate病毒防火墙的安装、配置和使用等，Fortinet对分销商、代理和用户进行系统的技术培训，并推出两种技术支持工程师的认证资格，即FCSE（售前系统工程师）和FCTSE（售后系统支持工程师）。

6.2 FortiProtect防护服务中心

FortiProtect防护服务中心网站为 http://www.fortinet.com/FortiProtectCenter/，每天提供当前网络威胁完整的概况、关于特殊病毒和漏洞和FortiGate病毒库与入侵检测库最近更新的网络威胁的详细说明，以及网络安全防护的有关信息和资源。FortiProtect中心信息数据每天被更新，非常易读和容易理解，所反映的都是最新的安全威胁，保证了时效性，体现了Fortinet的对客户的忠实承诺。具体内容如下：

- **状态摘要**

  状态摘要页面列举最新的病毒威胁和网络安全漏洞，并针对每一项提供了简短解释。状态摘要页面还显示最新近的Fortinet AV和NIDS特征代码数据库的版本号。

- **病毒百科全书**

百科全书包含病毒、蠕虫、特洛伊木马程序，和其它目前非常活跃的威胁。病毒信息摘要包括该威胁的等级和发现的日期，以及适用于该威胁等级的FortiGate特征代码数据库版本。症状列表中，会具体描述受影响的系统，该威胁的详细分析和已知的一些变种。百科全书可简单地以全名或部分名字来查找一种特别的病毒。

- **漏洞列表**
  漏洞列表提供到对当前安全漏洞和攻击的安全警告的连接。
- **有关信息资源**
  防病毒和安全资源页面提供综合网络安全信息，包括Fortinet白皮书和访问大多数可信任的和有价值的网站的链接。这些网站发布了关于各种网络安全专题的信息。

6.3 FortProtect安全防护小组

FortiProte安全防护小组(FSRT)是FUI(FortProtect更新体系)的关键组成部分。FSRT研究和综合信息，并将之提供给FortiProtect分布式服务中心，同时24小时不停的监控随时出现的新的安全威胁。这个小组收集和分析病毒样品，并深入研究病毒特征码，不断更新当前的Fortinet AV病毒特征代码库。这个小组也研究网络安全漏洞的特征码，不断更新Fortinet NIDS入侵检测特征代码库。FSRT由WildList组织创始人、防病毒专家Joe Wells领导。FSRT对全球的Fortinet用户的受威胁和受攻击做调查报告。FSRT对新出现的安全威胁做出迅速响应，并通过FortiProtect分布式中心(FDC)，更新分散FortiGate病毒防火墙的AV和NIDS的特征代码库。

6.4 FortiProtect推进式网络

FortiProtect分布式网络(FDN)利用FSRT开发的病毒和入侵特征代码库，提供自动、及时可靠的升级更新，确保全世界的FortiGate病毒防火墙有最新的AV和NIDS特征代码库。FDN是一个分等级、多层次的服务器体系结构，为全世界的FortiGate防病毒防火墙提供快速可靠的AV和NIDS数据库更新。FDN由一个最高级的FortiProtect分布式中心(FDC)和多个第二层的FDC组成。每个FDC维护一个或多个FortiProtect分布式服务器(FDS)。FDS给在分布式网络内的FortiGate病毒防火墙分配AV和NIDS的更新数据库。

在正常的情形下，FortiGate病毒防火墙根据用户的配置按计划定期的从FDSs上下载新的特征代码数据库。在紧急情况下，例如Nimda爆发，Fortinet提醒FortiGate用户保持警觉并促使他们马上更新数据库。FDS也可以通过“推进式”更新方式，主动为FortiGate病毒防火墙更新，在紧急情况下提供尽可能迅速的响应。通过“推进式”的紧急更新，替代了单一的计划式更新，FDN降低了甚至是关闭了网络的漏洞隐患。

7. 说明

7.1 附件：公司与产品介绍资料

公司与产品介绍资料（8页彩色）。

7.2 联系我们

Fortinet公司美国总部地址：

920 Stewart Dr.

Sunnyvale, CA 94054, USA

电话： （408）235 7700

传真： （408）235 7737

中国北京办事处地址：

北京市海淀区中关村南大街2号数码大厦B座903室

邮编100086

电话： （010）8251 2622／3／5／9

传真： （010）8251 2630

网站： www.fortinet.com

E-mail: fei@fortinet.com