

FORTIGATE™ 5020

高性能内容安全实时网络保护

FortiGate 病毒防火墙是专用的基于 ASIC 的硬件产品,在网络网关处提供实时的保护。基于 Fortinet 的 FortiASIC™ 内容处理器, FortiGate 是业界唯一能够在不影响网络性能情况下检测有害的病毒、蠕虫及其他基于内容的安全威胁的产品。 FortiGate 系统还集成了防火墙、VPN、入侵检测、内容过滤和流量控制功能,提供的是一个高性价比、使用方便的而强有力的解决方案。



所有 FortiGate-5020 系统病毒防火墙设计都是使用 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。每一个 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 Fortinet 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。

产品优势

为大型企业和受管理的安全服务商 (MSSP) 提供完美的网络保护解决方案

VLAN 和安全区细粒化安全分区管理,支持独立的安全区和接入控制政策

在保证网络性能的基础上,从电子邮件、文件转发和实时(web)流量以及邮件流量中消除病毒和蠕虫的威胁

实时系统状态监视降低了业主的总成本,提供图形界面,可方便地监视 CPU 和内存使用情况、网络和会话状态,病毒和入侵检测,由于采用硬件加速、基于 ASIC 的体系结构,和冗余热交换式供电电源,提供了优秀的性能和可靠性

提供完整的网络保护功能:

基于网络的防病毒、web 和电子邮件内容过滤、防火墙和 VPN,基于网络的入侵检测/阻挡和流量控制

“透明”模式工作支持高可用的体系结构和安装配置,对现已有的防火墙、VPN 入侵检测/防止或其他系统连接时,可又用作防病毒网关和进行内容过滤

自动下载最新的病毒攻击库,能接受 FortiProtect 网络的即时“下推”式更新

通过检测和防范 1300 多个不同的攻击，包括 DoS 和 DDoS 攻击，减少网络受威胁。专用的 FortiOS™ 系统获得 ICSA 的四项论证，即防病毒、防火墙、IPSec VPN 和入侵检测

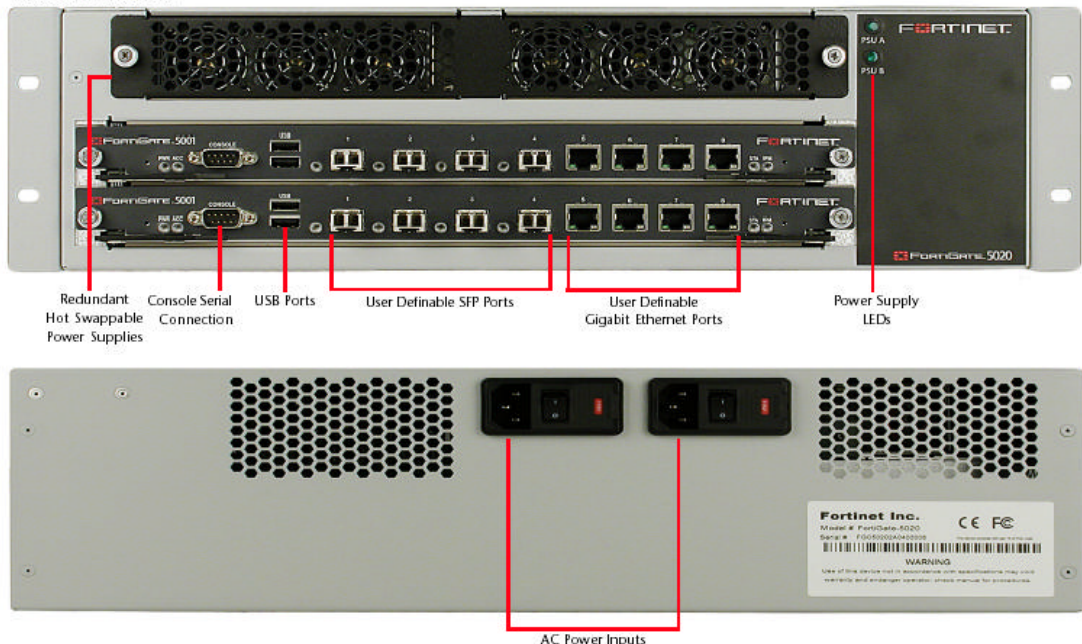
主要的特性和益处

特性	描述	益处
基于网络的病毒防御 (ICSA 认证)	实时检测和清除病毒和蠕虫。扫描进出的 E-mail 附件 (SMTP,POP3,IMAP) , HTTP 和 PTP 流量，包括基于 Web 的 E-mail 和加密 VPN 通道	关闭脆弱窗口，在网络的边界处阻挡病毒蠕虫入侵网络
入侵检测和防护系统 (ICSA 认证)	基于用户可设置的门限值 ,可检测和防护 1300 种以上入侵攻击。自动更新来自 FortiProtect 网络的 IPS 特征	阻挡攻击，监控外部的攻击，对快速传播的威胁作出实时反应
WEB 内容过滤	处理所有的 WEB 内容，可以屏蔽有害的 WEB 页面和代码，支持 URL 和关键词拦截	提高企业的生产力和效率，并且符合与 CIPA 兼容的教育机构规范
防火墙 (ICSA 认证)	业界标准的状态检测防火墙	安全可靠的系统防御 ,良好的性能和稳定性
VPN (ICSA 认证)	支持业界标准 PPTP, L2TP, IPSecVPN	低成本使用公网构筑自己的点对点私有网和远程接入通信
透明模式	可与企业原已在使用的防火墙和其他设备结合，提供网桥模式下的病毒防御，WEB 内容过滤，策略控制等应用	在老设备上增加新功能，方便老系统的集成和投资保护
远程访问	支持远程用户的加密访问 ,提供了 IPSec 客户端软件	提供了廉价的无处不在的网络服务和安全控制

FORTIGATE™ 5020

系统规格

FortiGate-5020



规格说明	FortiGate -5001	FortiGate -5020系统		FortiGate -5001	FortiGate -5020系统
接口			病毒和攻击邮件报警	v	v
SFP 端口	4	8			
10/100/1000BT口	4	8	VPN通道监控	v	v
系统性能			HA (高可用)		
并发会话	1000K	2000K	状态恢复 (FW/VPN)	v	v
新会话/秒	25K	50K	主动-主动/主动-被动HA	v	v
防火墙性能 (Gbps)	4	8	设备失败检测/通知	v	v
168bit3DES加密 (Mbps)	600	1200	链路状态监控	v	v
无用户数限制	v	v	链路失败恢复	v	v
策略数	50k	100K	网络功能		
调度	256	512	多个广域网口支持	v	v
病毒、蠕虫清除扫描	v	v	各区域间路由	v	v
SMPT,IMAP,POP3,HTTP和加密			各区域之间路由	v	v

VPN数据流					
隔离感染的信息	v	v	策略路由	v	v
根据文件大小隔离文件	v	v	系统管理		
防火墙模式和特性			控制接口 (RS232)	v	v
NAT , PAT 透明 (桥模式)	v	v	WebUI (https)	v	v
路由模式 (支持 RIP v1, v2)	v	v	多语言支持	v	v
基于策略的NAT	v	v	命令行接口	v	v
支持VLAN标记 (802.1q)	v	v	安全命令行 (SSH)	v	v
策略路由	v	v	FortiManager系统管理	v	v
基于用户认证的策略	v	v			
H.323NAT穿越	v	v	多管理员和用户级别	v	v
支持WINS	v	v	Web&TFTP方式的软件升级	v	v
VPN			IP和管理员绑定	v	v
PPTP、L2TP、IPSec	v	v	基于角色的管理	v	v
通道数	5000	10,000	系统版本恢复	v	v
加密 (DES , 3DES , AES)	v	v	用户认证		
支持PPTP, L2TP, VPN客户端穿越	v	v	内部数据库	v	v
Hub-and-Spoke VPN 体系结构	v	v	外部LDAP/Radius数据库	v	v
支持IKE认证方式(X.509)	v	v	IP/MAC绑定	v	v
死节点的检测	v	v	RSA SecurID	v	v
手工密钥/自动密钥支持	v	v	IPSec VPN基础上的Radius的Xauth认证	v	v
IPSec NAT穿越野蛮模式 (Aggressive)	v	v	流量管理		
重演检测	v	v	基于策略的流量控制	v	v
兼容主要的VPN产品	v	v	保证带宽/最大带宽/优先带宽	v	v
SHA-1/MD5认证	v	v	尺寸		

内容过滤			高度/宽度/长度	5.25英寸/17英寸/15.5英寸
URL/关键字/词组屏蔽	v	v		
URL免屏蔽列表	v	v	重量	16.1公斤
内容表	v	v	可上机架	v
支持FortiGuard	v	v	电源	
网页过滤				
支持Cerberian网页过滤	v	v	交流电源	100-240V
阻塞Java 小程序, Cookie 和Activex	v	v	输入电流	6A
入侵检测与防御			频率	50 – 60Hz
1300多种攻击的入侵防御	v	v	功率	最高800W
用户化攻击列表	v	v	环境	
自动更新攻击数据库	v	v	操作温度	0 – 40
反垃圾邮件			存贮温度	-25 – 70
黑名单/开放中继服务器	v	v	湿度	5 – 95%非凝结
MIME头检测	v	v	安全标准	
关键字/词过滤	v	v	FCC Class A Part 15	待
IP地址黑名单/免屏蔽列表	v	v	CSA/CUS	待
日志和监控			CE	待
内部日志记录(可插拔的硬盘)	20G	40G	UL	待
支持远程 Syslog/WELF服务器	v	v	ICSA Antivirus	v
图形化实时监控	v	v	ICSA Firewall	v
SNMP	v	v	ICSA IPsec	v
			ICSA IDS	v

2004年6月。