

FORTIGATE™ 400A

为企业提供实时网络

保护



FortiGate 病毒防火墙是专用的基于 ASIC 的硬件产品，在网络边界处提供了实时的保护。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。系统还集成了防火墙、VPN、入侵检测与防御、内容过滤和流量控制功能，提供了高性价比、方便和强大的解决方案。



FortiGate-400A病毒防火墙为日益增长的企业网络的安全，提供了其所需要的性能、灵活性和安全。FortiGate-400A有两个 10/100/1000M自适应以太网接口，可以升级到千兆网络。它有四个用户定义的 10/10M接口，可以提供冗余的WAN连接，高可靠性和多区域的特性，允许管理员在划分其网络的区域时有更高的灵活性和在不同区域之间设置策略。FortiGate-400A病毒防火墙可以作为高性能病毒防火墙和内容过滤网关，或者作为防火墙、入侵检测与防护和VPN的综合网络防护解决方案。FortiGate-400A对于企业来说是非常理想的产品，功能、速度和性价比各个方面都是无可匹敌的。FortiGate-400A通过FortiProtect™可以自动实现攻击数据库的更新。FortiProtect™提供了 24 小时的、全球的最新的病毒、蠕虫、木马和其它攻击持续升级服务。

产品优势

通过基于网络的病毒防御，Web 和 Email 的内容过滤、防火墙、VPN、动态入侵检测和防御、流量控制和反垃圾邮件提供完整的网络保护

保持网络性能的基础下，从邮件和文件传送和实时 Web 流量中消除病毒、蠕虫和灰色软件/间谍软件的威胁

使用简便和易于实施——快速的图形化配置指南,引导管理员完成初始化系统配置

通过对包括 DoS 和 DDoS 攻击在内的 1400 多种入侵进行检测和防御

自定义的端口提供了实施的灵活性

高可用性对于关键应用提供了透明的失败恢复功能

基于专用的 ASIC 硬件加速体系结构，提供了高性能和高可靠性

可以从 FortiProtect 服务网络中获得最新的病毒和攻击库，还支持即时“推动”方式更新

通过 FortiManager 集中管理工具可以对数以千计的 FortiGate 防火墙进行管理

采用FortiOS™操作系统得到了反病毒、防火墙、IPSec VPN和IDS的ICSA认证

基于 WEB (GUI) 的配置界面和内容过滤都提供了多语言支持

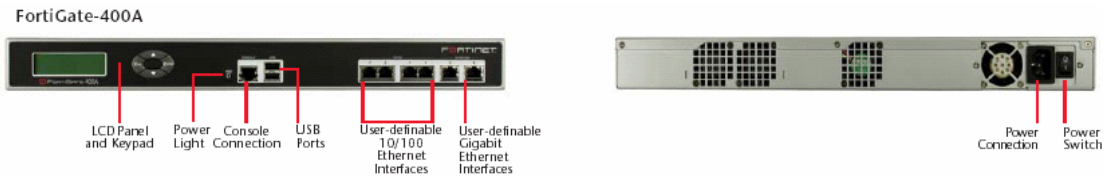


主要的特性和益处

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 Email 附件 (SMTP、POP3、IMAP) 和所有 FTP 和 HTTP 流量，包括基于 Web 的 Email，不会影响 Web 性能	在网络的边界处消除了危险病毒和蠕虫的入侵
动态 IPS 入侵检测 / 阻挡 (ICSA 认证)	可以根据用户自定义攻击的阈值，对 1400 多种入侵和攻击进行检测。可以从 FortiProtect 服务网络自动更新 IPS 特征值	对快速扩散的威胁实时响应，阻止可以穿越常规防火墙的攻击
防火墙 (ICSA 认证)	强大的状态检测防火墙	经过认证的防护体系，良好的性能和可扩展性
WEB 内容过滤	处理所有的 WEB 内容，以阻挡不当的内容和恶意脚本	提高企业的生产力，对实施 CIPA 规范的教育机构提供有力的保障
VPN (ICSA 认证)	支持工业标准的 PPTP, L2TP 和 IPSEC 的 VPN	在企业网络和客户之间建立安全的会话通道
远程访问	提供了 FortiClient 主机安全软件，来支持远程用户的加密访问	提供了廉价的无处不在的网络服务和安全控制
用户自定义的接口	六个用户自定义的接口(2 个 10/100/1000M 和 4 个 10/100M 以太网接口)，可以提供灵活的部署方式	提供冗余的 HA 选项，可以将网络划分成区域，在不同区域之间建立策略

FORTIGATE™ 400A

系统规格



系统规格

规格说明	FortiGate-400A	FortiGate-400A	FortiGate-400A
接口		日志和监控	
10/100/1000M以太网接口	2	内置硬盘	可选
10/100M以太网接口	4	支持远程Syslog/WELF服务器	√
USB接口	2	图形化实时监视和历史记录	√
		SNMP	√
系统性能		E-mail通知病毒/攻击	√
并发会话	400,000	VPN通道监控	√
新会话/秒	10,000		
防火墙性能 (Mbps)	450	网络功能	
168bit3DES加密 (Mbps)	135	支持多个WAN链接	√
无用户数限制	√	支持多个区域	√
策略数	5000	不同区域之间路由	√
调度	256	支持基于策略的路由	√
		系统管理	
反病毒，蠕虫检测&清除		控制台接口	√
通过FortiProtect自动更新		WebUI (HTTPS)	√
病毒库	√	多语言支持	√
扫描SMTP,FTP,IMAP,POP3,		命令行接口	√
HTTP和VPN数据流	√	安全命令行 (SSH)	√
根据文件大小阻挡	√	FortiManager系统	√
防火墙模式和特性		管理	
NAT, PAT 透明 (桥模式)	√	基于角色的管理	√
路由模式 (支持RIP v1, v2)	√	多个管理员和用户级别	√
支持OSPF	√	TFTP & WebUI方式的软件升级	√
支持基于策略的NAT	√	系统软件回退	√
虚拟域(NAT/透明模式)	2/10		
支持VLAN标记(802.1q)	√	用户认证	

用户组认证	√	内部数据库	√
H.323NAT穿越	√	外部LDAP/Radius数据库	√
支持WINS	√	RSA SecurID	√
		IPSec VPN的Xauth Radius认证	√
VPN		IP/MAC 地址绑定	√
PPTP,L2TP和IPSec	√		
专用通道	2000	流量管理	
加密方式(DES, 3DES, AES)	√	DiffServ 设置	√
SHA-1/MD5认证	√	基于策略的流量控制	√
PPTP, L2TP, VPN客户端穿越	√	支持保证/最大/优先带宽	√
支持VPN的Hub and Spoke	√		
IKE认证	√	尺寸	
IPSec NAT穿越	√	高度	1.75英寸
对端状态检测	√	宽度	17英寸
		长度	12.6英寸
		重量	5.4公斤
内容过滤		电源	
URL/关键字/词组屏蔽	√	交流输入电压	100-240VAC
URL免屏蔽列表	√	交流输入电流	1.6A
保护内容表	32	频率	50- 60Hz
阻塞Java 小程序, Cookie和		功率	最大50W
Activex	√		
支持FortiGuard™ Web过滤	√		
动态入侵检测 / 阻挡		环境	
入侵检测 / 阻挡1400多种攻击	√	操作温度	0 – 40 °C
从FortiProtect网络自动实时升级数据库	√	存储温度	-25-70 °C
用户化攻击列表	√	湿度	5 – 95% 非凝结
反垃圾邮件		安全标准	
实时黑名单 / 开放中继库服务器	√	FCC Class A Part 15,CE, UL, CUL, C-Tick, VCCI, CB	√
MIME头检测	√	ICSA Antivirus, Firewall,	
关键词/词组检测	√	NIDS, IPSec认证	√
IP地址黑名单/免屏蔽名单	√		