

FORTIGATE™ 800

适合大型企业的

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、蠕虫及其它基于内容的安全威胁的产品，它甚至可以实时对网站浏览予以防护。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，并且提供了高性价比、方便的和强有力的解决方案，来检测、阻止攻击，防止不正常使用和改善关键网络应用的服务。



FortiGate-800 病毒防火墙能够满足保护多数大型企业网络安全所要求的性能、灵活性、安全等指标。FortiGate-800 不仅可以作为高性能病毒和内容过滤的网关，还提供了一套包括防病毒、防火墙、内容过滤、VPN 和 IDP 的完整解决方案。FortiGate-800 病毒防火墙提供了可以运行于千兆网络的四个 10/100/1000 自适应以太网接口，还提供了四个用户可以自行定义的 10/100 接口。这四个接口可以用作多个安全区域来提供细粒度的安全，管理员可以用它把网络划分成不同的安全区域，并且在这些区域之间设计不同的安全策略。两个以上的 FortiGate-800 病毒防火墙可以通过一个高可用的端口相连，以实现冗余集群，来提高可用性和无故障运行时间。Fortinet 公司的实时响应服务提供了持续的攻击库更新，以保护网络不受最新病毒、蠕虫、木马及其他攻击，使网络随时随地的得到安全保护。所有的 FortiGate-800 病毒防火墙都会连接到该实时响应服务器自动升级，以获取最新的数据。

产品优势

融合了基于网络的防病毒、网页内容过滤、防火墙、VPN、入侵检测和防护，以及流量控制的综合安全解决方案

在保证网络性能的基础上，实时消除病毒和蠕虫对邮件、文件传输和实时数据传输 (WEB) 威胁

通过独立的安全区域和与 Vlan 标记相关的策略实现了细粒度的安全

可以检测和防御 6000 多种不同的入侵行为，包括 DoS 和 DDoS 攻击

高可用性对重要应用支持透明的失败恢复

硬件加速的、基于 ASIC 芯片技术的体系架构提供了较高的性能和可靠性

自动下载最新的病毒和攻击数据库，支持从 FortiResponse 网络接受推送式更新

专用的 FortiOS™ 系统获得 ICSA 认证的病毒网关、防火墙、IPSec VPN 和入侵检测

操作简便易于实施：

简单快捷的向导帮助管理员完成基于图形界面的初始化过程

通过病毒隔离区可以方便地将攻击样本提交给 Fortinet 的攻击响应组织

高性能确保了企业网络的高效运行

10/100/千兆三速率自适应接口可以降低用户升级到千兆网络的成本

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)、所有 FTP 和包括 web email 的 HTTP 流量, 而不影响网络的性能	通过阻止病毒和蠕虫进入网络的方式, 消除了危险
入侵检测 (ICSA 认证)	可选择的攻击数据库 (>1300 攻击特征)	识别和分析外部的攻击, 并实时报警和记录数据
入侵防护	根据用户定义的阈值, 对 30 多种入侵和攻击进行主动防护	在网络的边缘处阻挡了绝大多数的攻击
防火墙 (ICSA 认证)	功能强大的状态检测防火墙	经过认证的系统防御, 良好的性能和可扩展性
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	提高企业的生产力, 确保 CIPA 规定的教育组织的条例的实施
VPN (ICSA 认证)	业界标准的 PPTP, L2TP 和 ICSA 认证的 IPSEC 支持	在局域网和客户端之间构建安全通道
透明模式	提供网桥模式下的病毒防御, WEB 内容过滤, 和其它内容相关的控制, 可以部署在现有防火墙和其他设备之间	比较容易和已有网络结合起来, 保护已有投入
远程访问	支持远程用户的加密访问, 提供了 IPSEC 客户端软件	为外地员工、移动办公提供了廉价的无处不在的网络服务

系统规格

FortiGate-800



规格说明	FortiGate 800	FortiGate 800
接口		
10/100M以太网接口	4	
10/100/1000以太网接口	4	
系统性能		HA (高可用)
并发会话	400K	主动对主动的HA √
新会话/秒	10K	主动对被动的HA √
防火墙性能	1 Gbps	状态故障恢复(防火墙和VPN) √
168bit3DES加密 (Mbps)	200	设备失败检测/通知 √
无用户数限制	√	链路监控 √
策略数	20k	网络功能
调度	256	多个广域网口支持 √
病毒、蠕虫清除		支持多个区域 √
扫描smtp,imap,pop3,http和VPN数据流隔离被感染信息	√	各区域间路由 √
隔离感染信息	√	基于策略的路由 √
基于文件大小控制	√	系统管理
防火墙模式和特性		控制接口 (RS232) √
NAT, PAT 透明(桥模式)	√	WebUI (https) √
路由模式(支持RIPv1 v2)	√	多语言支持 √
基于策略的NAT	√	命令行接口 √
虚拟域 (NAT/透明模式)	2/10	安全命令行 (SSH) √
VLAN(802.1q)	√	FortiManager系统 √
访问控制列表(源地址, 目标地址, TCP和UDP端口)	√	管理
基于用户组认证的策略	√	多管理员和用户级别 √
H.323NAT穿越	√	Web&TFTP方式的软件升级 √
支持Wins	√	管理软件版本回退 √
VPN		用户认证
PPTP、L2TP、IPSEC	√	内部数据库 √
通道数	3000	支持LDAP √
加密 (DES、3DES、AES)	√	Radius数据库 √
SHA-1/MD5认证	√	IP/MAC绑定 √
支持PPTP、L2TP、VPN	√	流量管理
客户端穿过		基于策略的流量控制 √
VPN支持Hub-and-Spoke	√	保证带宽 √
IKE认证方式	√	最大带宽 √
		优先带宽 √

IPSEC NAT穿越	√	尺寸	
停滞点的检测	√	高度/宽度/长度	3.5/16.75/13.5英寸
兼容主要的VPN产品	√	重量	4.5公斤
		可上机架	√
内容过滤			
URL屏蔽基于策略控制	√	电源	
关键字/词组屏蔽	√	交流电源	110-240V
URL免屏蔽列表	√	输入电流	4A
内容摘要	32	频率	50 – 60Hz
阻塞Java 小程序, Cookie 和Activex	√	功率	300W max
Email过滤(关键词、黑名单、样品表)	√	环境	
		操作温度	0 – 40 °C
		存储温度	-20– 80 °C
入侵检测		湿度	10 – 90% 非凝结
超过1300种攻击列表	√	安全标准	
超过30种防御列表	√	FCC Class A Part 15	√
用户化攻击列表	√	CE	√
		UL	√
日志和监控		ICSA Antivirus	√
内部日志记录、硬盘可插拔	40G	ICSA Firewall	√
支持远程Syslog/WELF服务器	√	ICSA IPsec	√
图形化实时化和对记录的监控	√	ICSA Intrusion Detection	√
SNMP	√		
病毒和攻击的email报警	√		
VPN通道的监控	√		