厂商名称	梭子鱼	思科	思杰	安恒信息	飞塔	绿盟
产品名称	梭子鱼WEB应用防火墙	Cisco ACE Web 应用防火墙	Citrix NetScaler	DBAPPSecurity	FORTIWEB Web应用防火墙	绿盟WEB应用防火墙
安全性	HTTP/HTTPS/FTP协议扫描	完全反向代理	缓冲区溢出	SQL注入	自学习安全分析	二维防护体系：网页挂马
	表单参数扫描	监控器模式部署	CGI-BIN参数处理	命令注入	数据泄漏防护	网页篡改
	动态学习功能	缓存溢出控制	表格/隐藏字段处理	Cookie 注入	网页防篡改	恶意扫描
	Web站点隐藏	HTTP参数操作，协议遵从性	强制浏览保护	跨站脚本(XSS)	HTTP RFC 规范验证	HTTP Flood
	强制浏览防护	零字节阻拦	信息块或会话中毒	敏感信息泄露	漏洞评估	传统攻击
	会话跟踪	输入编码规范化	跨站点脚本编写（XSS）	恶意代码	XML 防火墙	“0 ”day攻击
	速率控制	响应过滤和重写	命令注入	错误配置	应用层漏洞保护	网络层抗DDos
	上传文件病毒扫描	灵活的防火墙活动	SQL注入	隐藏字段	PCI DSS 合规	ARP欺骗防护
	全面的响应控制	Cookie和进程窜改	引发敏感信息泄露的错误	会话劫持	防御OWASP TOP 10 攻击	双向在线清洗
	外发数据窃取防护：信用卡卡号、	跨站点编程（XSS）	不可靠的密码系统应用	参数篡改	可防御的攻击类型：跨站脚本	智能应用层DDoS攻击防护
	外发数据窃取防护：社保卡卡号	命令注入、SQL注入	服务器错误配置	缓冲区溢出	SQL 注入	结合了静态规则与基于用户行为识别的动态防御机制防御的攻击类型：网络钓鱼
	XML防火墙	防止信息泄漏，保护私密性	后门和调试选项	应用层拒绝服务	会话劫持	隐私侵犯
	信任主机	实施加密功能	基于速率的策略实施	其他变形的应用攻击	Cookie 篡改/中毒	身份窃取
	阻断常见攻击：SQL 注入攻击	应用和服务器错误消息防御	已知的平台漏洞	网页防篡改	跨站请求伪造	经济损失
	阻断常见攻击：跨站脚本（XSS)攻击	Referrer实施	零时差攻击	策略配置	命令注入	名誉损失
	阻断常见攻击：OS 命令注入攻击	主动和被动安全模式	内容改写和响应控制	专利级WEB入侵异常检测引擎	远程文件包含	
	阻断常见攻击：Cookie 篡改及劫持攻击	定制规则和签名	内容过滤	支持多保护对象	表单篡改	
		PCI遵从性简况	L4-7 DoS攻击防护	支持用户自定义规则库	隐藏区域控制	
		全面的SSL v2/3支持，带可配置的密码套件	深度流量检测；双向分析		外出数据信息泄漏	
		FIPS 140-2 Level 3平台	HTTP和HTML报头和攻击行为检测		HTTP 请求走私	
			HTML深层分析；语义提取		编码攻击	
			会话层及状态分析		失效访问控制	
			协议中立性		强制浏览	
			HTML表格字段保护		目录穿越	
			Cookie中毒防御确保Cookie不会被修改		站点侦察	
			合法URL强制实施 - Web应用内容完整性		搜索引擎黑客攻击	
			XML数据保护		强制登录	
			URL转换			
认证及授权	客户端证书验证		身份验证、授权和审计		支持本地、LDAP 和NTLM多种认证方式，可以“卸载 ”Web 服务器上的认证功能，通过FortiWeb 实现认证	
	基本验证					
	表单验证					
	网站访问控制					
	支持LDAP/RADIUS或本地的用户数据库					
流量优化	负载均衡		全面的SSL卸载	高速缓存	负载均衡	SSL加速与卸载
	内容路由			负载均衡	硬件加速SSL 卸载	Web缓存
	缓存				高可用性	Web压缩
	压缩					高可用性
	SSL 卸载					软/硬Bypass
	高可用性					
统计功能	丰富的报表功能	系统日志、消息和事件记录	PCI-DSS合规性报告工具	访问日志审计	提供数以百计的内置报表类型，使管理员、审计人员可以针对合规需求，分析攻击、事件和流量	安全事件监控
	攻击日志，访问日志，审计日志	流量和服务水平协议(SLA)监控和报告		实时告警，支持邮件、短信等多种方式告警		访问情况监控
		用于监控、各种告警和触发的统计数据		支持自定义统计，报表支持各类导出格式（WORD、EXCEL、PDF、HTML等）		设备负载监控
		管理操作的审计跟踪		统一日志平台接口		安全缓存监控
加密支持		加密算法包括：AES		全面支持HTTPS/SSL加密协议		
		DES				
		3DES				
		Blowfish				
		RSA				
		Diffie-Hellman				
		DSA				
		SHA-1和 MD5				
管理		Web用户界面	基于Web的安全GUI		Web用户界面	
		命令行界面	基于SSH的CLI接入网络管理			
		SSH	SNMP			
		SNMP	基于Syslog的日志			
		RBAC				
		委派管理				
		集中策略管理和分布式实施				
		配置、统计数据和记录的输入和输出				
部署方式	桥（透明）模式			支持全透明直连部署	透明检测	
	路由模式			支持监控、阻断、软硬件物理直通等多种应用模式	和透明代理	
	旁路（单臂）模式			直连透明部署	反向代理	
				旁路牵引防护部署	旁路	
				HA部署模式		