



主要内容:

- 1 主要优势
- 2 实时流量策略构建器
- 2 现成的保护能力
- 2 高级执行能力
- 2 满足安全标准的要求
- 2 经济高效的应用安全
- 3 全面的应用安全与加速
- 3 集成的XML防火墙
- 3 DataGuard™ 和伪装
- 3 漏洞评估
- 4 攻击签名的实时更新
- 4 SMTP和FTP安全
- 4 集成的高级报告和数据库安全
- 5 架构
- 6 BIG-IP ASM平台
- 6 更多信息



利用下一代应用安全保障您的业务

随着更多的应用流量通过网络上传输，敏感数据面临着被盗、安全漏洞和攻击的威胁，尤其是在应用层。F5的BIG-IP®应用安全管理器™ (ASM) 是一个先进的Web应用防火墙，可显著减少和控制数据、知识产权和Web应用丢失或损坏的风险。BIG-IP ASM提供了端到端的应用保护、高级监控以及集中报告，并可以满足关键的法规要求。

BIG-IP ASM是业内最全面的Web应用安全与应用完整性解决方案。对于对业务至关重要的应用，屡获殊荣的BIG-IP ASM能够使其保持机密性、可用性和高性能，从而保护了您企业的安全，并维护了企业的声誉。

主要优势

确保应用的可用性

全面防护第7层DoS攻击、暴力攻击以及危险的FTP和SMTP命令等等。

更敏捷地应对威胁

注重利用自动安全策略来实现快速应用开发和部署。

降低成本，实现法规遵从

利用内置的应用安全防护功能，满足安全标准的要求。

获得现成的应用安全策略

利用预置的快速部署策略和最少量的配置提供保护。

增强应用安全和性能

提供先进的应用保护，同时在应用安全和加速方面，提升性能，保证经济高效。

据Web应用安全联盟称，96.85%的网站都存在漏洞，有遭受直接攻击的风险，而69.37%的漏洞都存在于客户端。随着越来越多的应用转移到网络上，Web应用的数据侵害成为值得关注的问题。一旦遭受数据侵害，Ponemon Institute估计：总体来看，平均每条记录因遭到破坏而造成的损失有202美元；如果是由心怀叵测的内部人员或前任员工所造成，损失则达225美元。²

实时流量策略构建器

BIG-IP ASM的核心是动态策略构建器引擎，它负责自动的自我学习并创建安全策略。它围绕新发现的漏洞自动构建和管理安全策略，部署快速、敏捷的业务流程，而无需手工干预。当流量通过BIG-IP ASM传输时，策略构建器解析请求和响应，提供独特的能力检验完整的客户端和应用流量的双向流程—包括数据和协议。通过利用先进的统计和启发式引擎，策略构建器可以过滤掉攻击和异常流量。策略构建器也可以在被告知站点更新的模式下运行。通过解析响应和请求，它可以探测站点的变化，并且相应地自动更新策略，而无需用户干预。

现成的保护能力

BIG-IP ASM配备了一套预置应用安全策略，可为Microsoft Outlook Web Access、Lotus Domino邮件服务器、Oracle E-Business Financials和Microsoft Office SharePoint等常用的应用提供现成的保护能力。此外，BIG-IP ASM包含快速部署策略，可立即为任何客户应用提供安全保障。这套经过验证的策略无需要花费任何时间进行配置，并且可以根据启发式学习和特定的客户应用安全需求，用作创建更先进的策略的起点。

高级执行能力

BIG-IP ASM可保护任何参数免遭客户端的篡改，并且通过验证登录参数和应用流来防御强制浏览和逻辑缺陷攻击。BIG-IP ASM还可以防护OWASP十大Web应用安全漏洞¹以及零日Web应用攻击。

满足安全标准的要求

先进的内置安全防护和远程审计功能可帮助您的企业以经济高效的方式满足行业安全标准的要求，包括PCI DSS、HIPAA、Basel II和SOX，您既不需要购置多个设备，也不需要对应应用进行更改或重写。BIG-IP ASM提供了针对新型威胁的高级报告能力，例如第7层拒绝服务攻击(DoS)和暴力攻击。此外，BIG-IP ASM与WhiteHat、Splunk和Secerno集成，可支持漏洞评估、审计和实时数据库报告功能，从而实现安全违规检查、攻击防护和法规遵从。

经济高效的应用安全与可用性

许多网站和应用都遭受过安全威胁，这些安全威胁会导致业务中断，并损害企业的品牌。BIG-IP ASM可以报告以前未知的威胁，例如暴力攻击，并且可减轻Web应用威胁，从而保护企业免遭数据侵害。BIG-IP ASM有助于预防棘手而且代价高昂的应用侵害，这些侵害可导致企业遭受数百万美元的损失，包括收入下降、监管机构处罚和品牌价值受损等。

¹ 欲了解BIG-IP ASM所防护的OWASP十大Web应用安全漏洞的更多信息，请联系您的F5业务代表。

² “在企业准备应对进一步损失的同时，数据侵害成本居高不下”，Robert Westervelt, SearchSecurity.com.

全面的应用安全与加速

BIG-IP ASM与BIG-IP® WebAccelerator™ 可同时在BIG-IP® 本地流量管理器™ 设备上运行，因此您可以确保应用的安全，同时提高应用性能。这个高效的多解决方案平台在不降低性能的情况下增加安全性。您可以立即过滤攻击，并对Web应用进行加速，从而改善用户体验。由于不需要向网络中增添新的设备，您可以获得一体化的解决方案，从而实现最高的成本效益。

集成的XML防火墙

BIG-IP ASM提供了特定应用的XML过滤和验证功能，保证Web应用的XML输入的结构正确。它提供了模式验证、常见攻击防御和XML解析器拒绝服务预防。

DataGuard™和伪装

BIG-IP ASM通过分离数据和隐藏信息而预防敏感数据的泄露（例如信用卡号码、社会安全号码等）。此外，BIG-IP ASM隐藏错误页面和应用错误信息，防止黑客发现底层架构并发起有针对性的攻击。

漏洞评估

与WhiteHat Sentinel Security的集成提供了一种独特的漏洞评估服务，该服务将自动化工具与专业的高技能应用安全专家联系在一起。通过与BIG-IP ASM集成，业界领先的WhiteHat Sentinel服务可以扫描Web应用，并创建专门处理应用中发现的漏洞的BIG-IP ASM规则。这样可以通过接近即时的漏洞控制响应而进行经过验证并且可行的漏洞评估，从而在开发人员纠正漏洞代码时保护应用的安全。

BIG-IP ASM提供了预置并且经过验证的应用安全策略，无需任何配置，并且为关键任务的应用提供了现成的保护。

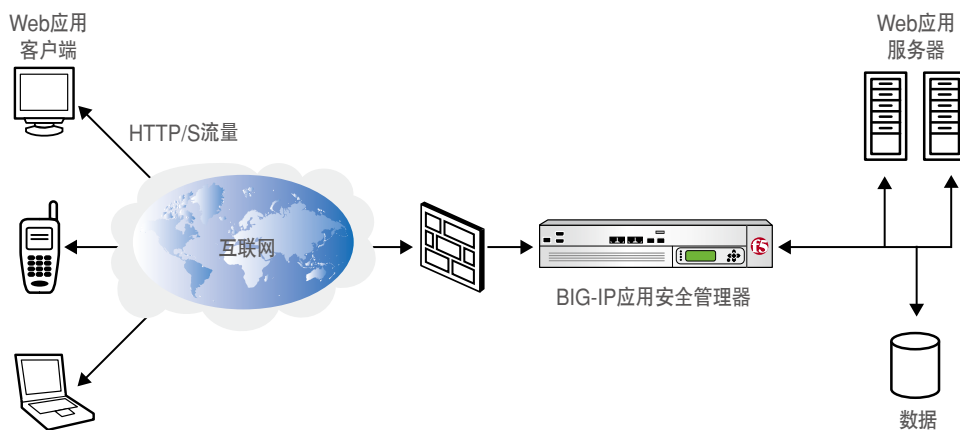


<input type="checkbox"/>	Name	Active Security Policy	Enforcement Mode	Logging Profile	State
<input type="checkbox"/>	OWA	OWA_default	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	Oracle_11i	Oracle_11i	Blocking	Log illegal requests	Enabled
<input type="checkbox"/>	PeopleSoft_Portal	PeopleSoft_Portal_default	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	SharePoint	SharePoint_Template	Transparent	Log illegal requests	Enabled
<input type="checkbox"/>	www.mycompany.com	www.mycompany.com_default	Blocking	Log all requests	VS1 Enabled

BIG-IP ASM提供了全面的Web应用防护。

攻击签名的实时更新

为了保证最新的防护能力，新攻击的新签名需要经常更新。BIG-IP ASM每天查询F5签名服务，并自动下载和应用新的签名。



SMTP和FTP安全

BIG-IP ASM使FTP服务器组的管理轻松易行。BIG-IP ASM验证FTP协议，控制暴力攻击，而且也可以对允许的FTP命令进行白名单控制。此外，BIG-IP ASM可以执行命令长度限制和主动/被动连接。对于SMTP，BIG-IP ASM提供了额外的全面安全检查。它还支持灰名单，目的是预防垃圾邮件，执行SMTP协议，将危险SMTP命令加入黑名单，并且控制目录获取攻击。BIG-IP ASM的速率限制能力有助于应对拒绝服务（DoS）攻击。

集中的高级报告和数据库安全

Splunk是一个大型的高速索引和搜索解决方案，提供了15种不同的BIG-IP ASM特定报告。这些报告提供了攻击和流量趋势的深入信息、用于讨论的长期数据汇总、故障响应的加速以及风险发生之前无法预期的威胁的识别。

对Web访问敏感数据、破坏数据库或者执行DoS攻击，SecernoDataWall和BIG-IP ASM共享相同的报告。恶意用户可以被隔离，同时报告和告警对这些攻击的类型和威胁提供了及时的侦测和信息。

BIG-IP ASM架构

BIG-IP ASM运行于F5独特、专用的TMOS®架构上。TMOS是一个智能的、模块化、高性能平台，可增强BIG-IP ASM的每项功能。TMOS提供了洞察力、灵活性和控制力，旨在帮您智能地保护Web应用。

TMOS提供了：

- SSL负荷卸载
- 缓存
- 压缩
- 即时处理任何应用内容的能力（无论是入站还是出站流量）
- TCP/IP优化
- 先进的速率整形和服务质量
- IPv6网关™
- IP/端口过滤
- 通过内置交换机支持VLAN
- 资源配置
- 路由域（虚拟化）
- 远程认证
- 安全
 - 显示定制的合法通知和安全登录横幅
 - 执行管理会话超时
 - 安全地登出BIG-IP系统
 - 遵循增强的审计和日志记录要求
 - 全面隔离和保护SSL证书不被读取或修改

- 强制浏览
- 隐藏字段操作
- 请求走私
- XML炸弹/DoS

额外的网络安全服务包括：

- SSL加速器
- 带状态的3-4层防火墙
- 透明和非透明的反向代理
- 密钥管理和故障切换处理
- SSL终止和重新加密到Web服务器
- VLAN分段
- DoS保护
- 客户端证书支持
- 通过LDAP/RADIUS进行客户机验证
- 专用管理端口
- URI监控
- 采用Splunk提供集中的高级报告
- 采用Secerno的DataWall保证数据库安全

BIG-IP-ASM防护多种应用攻击，包括：

- 第7层DoS
- 暴力攻击
- 跨站脚本
- SQL注入
- 参数篡改
- 敏感数据泄露
- 会话劫持
- 缓存溢流
- Cookie篡改
- 多种编码攻击
- 断开的接入控制

预置的应用安全策略包括：

- Lotus Domino 6.5
- OWA Exchange 2003
- OWA Exchange 2007
- Oracle 10g Portal
- Oracle Application 11i
- PeopleSoft Portal 9
- 快速部署安全策略
- SAP NetWeaver 7
- SharePoint 2003
- SharePoint 2007

BIG-IP ASM平台

欲了解详细的物理规格，请参阅BIG-IP®系统硬件产品资料。

BIG-IP ASM可在11050、8900、6900、3900和3600平台上用作BIG-IP本地流量管理器的附加模块，并可在11050、8900、6900、3900和3600上作为单独解决方案。



11050系列



8900系列



6900系列



3900系列



3600系列

专业服务与支持

F5致力于帮助您从F5产品中获得最大的价值。欲了解F5支持服务如何帮您提高投资回报(ROI)，缩短管理时间，降低管理费用，并且优化IT基础架构的性能和可靠性，请联系：consulting@f5.com。

更多信息

欲了解有关BIG-IP ASM以下资源或更多信息，请浏览F5.com。

产品概述

BIG-IP应用安全管理器

白皮书

遵从PCI DSS要求6.6

案例研究

Crédit Coopératif保护其在线银行业务的安全

F5中国免费咨询热线：800 990 1330

F5在线联系：chinainfo@f5.com

F5中国技术支持中心直拨电话：

4008-155-595（免费），010-5923-4123（北京）



F5公司北京代表处

地址：北京市朝阳区建国路81号
华贸中心1号写字楼1708室
邮编：100025
电话：(+86) 10 5923 4000
传真：(+86) 10 5923 4100
www.f5.com.cn

F5公司上海代表处

地址：上海市卢湾区湖滨路222号
企业天地1号写字楼1119室
邮编：200040
电话：(+86) 21 6113 2588
传真：(+86) 21 6113 2599
www.f5.com.cn

F5公司广州代表处

地址：广州市天河区珠江新城华夏路
10号富力中心写字楼1108室
邮编：510623
电话：(+86) 20 3892 7557
传真：(+86) 20 3892 7547
www.f5.com.cn

F5公司成都代表处

地址：成都市滨江东路9号
香格里拉中心办公楼18层
邮编：610021
电话：(+86) 28 6606 5210
传真：(+86) 28 6606 5211
www.f5.com.cn