

安全性

保护您的网络与应用，提高用户接入能力，优化性能，并降低管理复杂性。



特性

- >> 防止入侵，并保护敏感数据
- >> 简化接入控制、应用安全与**规范**监管管理
- >> 通过自动接入与更高性能提高工作效率
- >> 通过整合与简化安全管理而降低成本

F5安全解决方案： 灵活性、高效 性、经济性

保证您的网络安全性、快速和可用性对于业务的成功至关重要。安全违规可能导致您的企业的工作效率降低、失去机会和成本升高。这些有害的情况也会损害企业的信誉，并降低客户的信任度。

利用F5安全解决方案，您可以提供安全的远程接入，保护电子邮件，并简化Web接入控制，同时增强网络和应用性能。您的企业将拥有所需的定制安全性，而且您的用户将享受到他们需要的可靠而灵活的接入。

对驱动业务发展的基于网络的应用提供保护

挑战

许多网络级安全威胁与您的应用所使用的相同协议的不正当使用直接相关。为了保证应用的安全，您可以尝试追踪并修补明显的漏洞。您也可以部署单独的解决方案，专用于保护应用安全，但这些解决方案并不能增强性能或简化控制。

主要优势

- 控制恶意攻击，同时支持合法用户
- 防止敏感信息和通信受到安全威胁
- 利用高可用的应用提高工作效率

解决方案

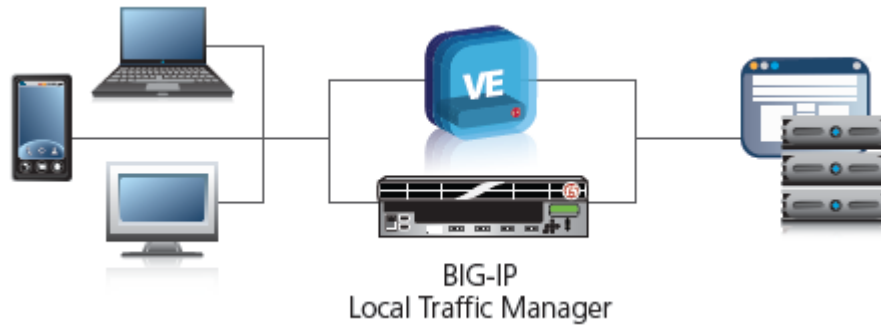


图1: BIG-IP本地流量管理器通过物理平台或虚拟版本而实现高可用性, 并防止基于网络的威胁。

F5® BIG-IP® 本地流量管理器™ (LTM) 应用交付控制器有助于您保证基于网络的应用与数据的安全, 同时提供一个战略控制点, 提高应用性能。从强大的网络级和协议级安全到应用攻击过滤, **BIG-IP LTM**为保护您的业务应用提供了一套安全服务。

BIG-IP LTM作为一个安全代理, 用于防止基于网络的SYN泛洪和其它网络拒绝服务 (DoS) 以及分布式拒绝服务 (DDoS) 攻击, 而且它提供了控制功能, 用于定义和执行基于L4的过滤规则, 以提高网络防护能力。

凭借行业领先的加密能力, **BIG-IP LTM**还使您能够有选择地加密数据, 以保护并优化您企业的通信。通过使用最强大的安全套接层 (SSL) 加密、位加密和4096密钥长度而支持先进的加密标准算法, **BIG-IP LTM**作为您的关键业务资源的**网关**。**BIG-IP LTM**可用在灵活的多解决方案设备平台上, 或者作为虚拟版本而运行。

提供网络与应用接入，同时保证安全

挑战

提供网络与应用接入对于提高员工的工作效率和提供有价值的客户服务至关重要。为了保证用户轻松地接入关键的Web应用，例如针对员工的时间跟踪软件或者针对宾馆客人的互联网浏览接入，许多企业创建了安全性最低的网络。尽管这些系统可以自动记录用户的IP地址，但无法安全地确定用户身份，而且绝对无法保障安全。

网络管理员需要更好地了解并控制网络中日益增多的应用接入用户。然而，这一要求可导致您的IT基础设施的复杂性升高，扩展难度增大，而且费用昂贵。

主要优势

- 增强您的网络中的身份识别和动态接入控制能力
- 确保强大的终端安全
- 简化验证，整合基础设施，并降低成本
- 提供高性能、扩展性和灵活性

解决方案

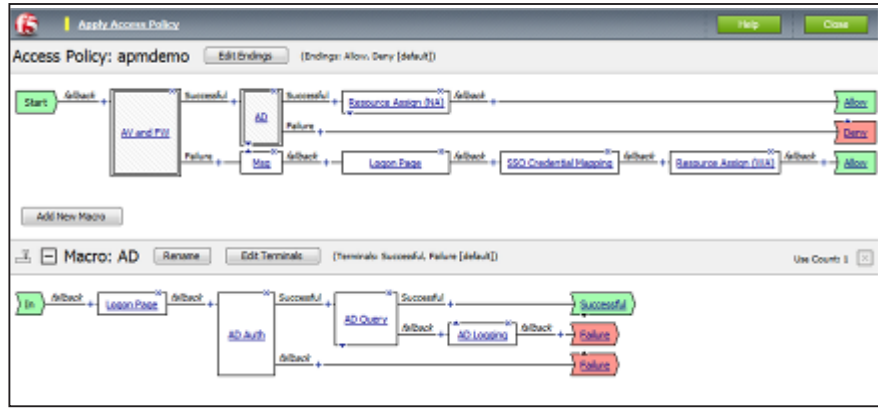


图2: BIG-IP可视策略编辑器有助于创建接入策略

BIG-IP® 接入策略管理器™ (APM) 是一个灵活的高性能接入与安全解决方案，提供了基于策略并具有上下文感知能力的用户接入，同时可以简化验证、授权和计费 (AAA) 管理。通过在BIG-IP上直接实现AAA控制，您可以整合接入基础设施，降低验证和授权成本，并同时支持数千个用户，同时保证每秒数百个用户登录。BIG-IP APM可作为灵活的多解决方案BIG-IP LTM和BIG-IP LTM虚拟版本平台上的一个产品模块。

高性能的安全规范监管

挑战

随着网络上的应用流量不断增加，敏感数据面临着遭受针对企业应用的漏洞攻击的风险。因此，恢复流程、法律费用以及知识产权数据丢失所带来的财务影响会非常严重。许多管理员认为他们的网络是安全的，因为他们部署了防火墙，但是，黑客很可能攻击应用层，因为该层存在更大的漏洞。

最近的研究表明：

- 75%的黑客攻击发生在应用层¹
- 96.85%的网站存在被攻击的漏洞²
- 一旦发生违规，数据违规的平均总成本将达到每条记录202美元，而内部恶意员工或者前任员工的违规成本则达到每条记录225美元³

主要优势

- 提高安全性，同时降低规范监管成本
- 以最少量的配置获得现成的应用安全策略
- 确保应用可用性，并提高性能
- 更灵活地处理不断变化的威胁

解决方案

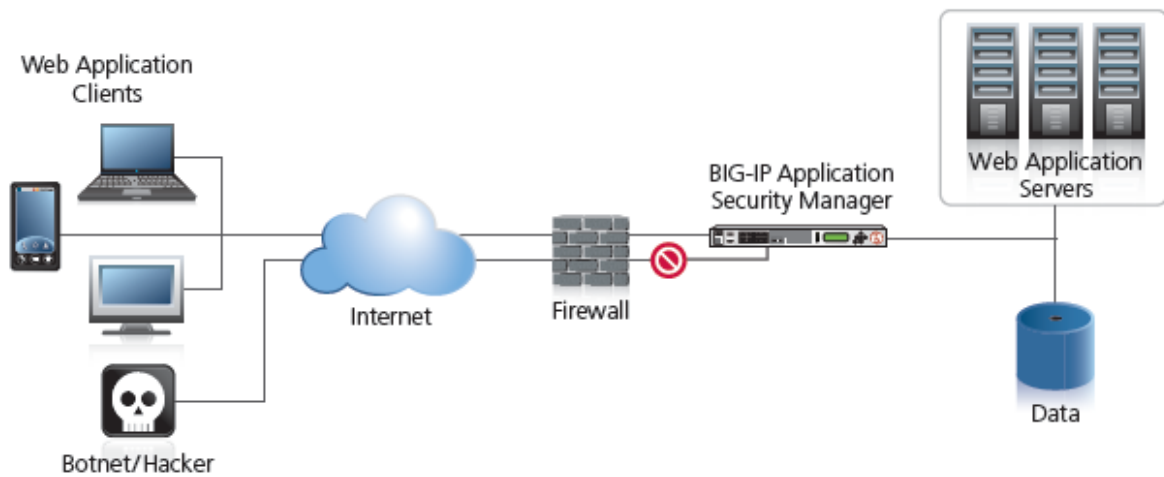


图3: BIG-IP ASM提供了全面的Web应用攻击防护

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提供了无与伦比的应用和网站防护，例如防止7层DDoS等最新的Web威胁。此外，BIG-IP ASM为您提供完整的攻击专家系统，并且可以满足关键的法规要求。

利用BIG-IP ASM，您的企业将从完整的解决方案中获益，降低对多个设备的需求，降低维护和管理成本，并且提高关键业务应用和流程的机密性、可用性和完整性。BIG-IP ASM可用作灵活的多解决方案BIG-IP LTM平台上的一个产品模块，也可以用在独立设备。

¹Theresa Lanowitz, Gartner Inc., 应用层的安全, http://www.gartner.com/DisplayDocument?ref=g_search&id=487227 (2005年12月)

²Web应用安全联盟(Web Application Security Consortium), <http://www.webappsec.org/projects/statistics/> (2008)

³Robert Westervelt, Ponemon研究发现2009年的数据违规成本持续增加, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_qci1379486,00.html (2010年1月)

针对HTTP(s)、SMTP和FTP协议的安全检查服务

挑战

如果您的环境不仅需要3层和4层检查服务，则您在部署包含全部特性的Web应用防火墙时可能不具备所需的专业知识和管理能力。

作为一个替代方案，协议安全服务为HTTP(s)、SMTP和FTP协议提供了强大的防护能力，而且您只需最少的配置。

主要优势

- 全面防护HTTP攻击
- 集中的FTP安全管理
- 阻止垃圾消息的SMTP安全

解决方案

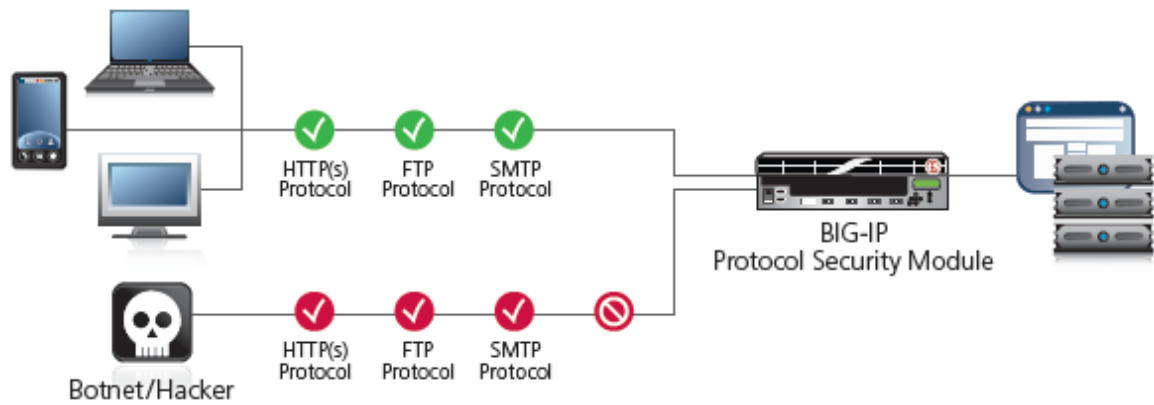


图4: BIG-IP 协议安全模块为HTTP(s)、SMTP和FTP协议提供了强大的安全服务

BIG-IP® 协议安全模块™ (PSM) 非常适合要求检查服务的环境，因为在该环境中，部署包含全面特性的Web应用服务器所需的管理费用不足，或者需要保证其它协议的安全。协议规范检查服务可以在每个虚拟服务器上实施，并且在几分钟内即可配置完成。通过对HTTP(s)、FTP和SMTP执行协议规范检查，该服务可以防止那些使用协议操纵技术的攻击。

提供安全且快速的远程应用接入

挑战

IT 部门必须支持不断增多的移动员工的要求。保证这些用户通过不同设备并在不同位置安全、无缝地接入应用和**数据**变得越来越具有挑战性。IT部门可以部署不同厂商的孤立解决方案，以促进接入、加速和优化。

但随着用户数量的增多，这种孤岛式方法不仅复杂、灵活性低，而且难以管理。随着新威胁不断出现，防止未授权的接入和攻击也变得日益困难。这种费用高昂且容易出错的环境限制了成功的远程接入，并阻碍了业务增长。

主要优势

- 实现卓越的扩展能力，满意日益增加的移动员工的要求
- 通过支持在任何地方接入客户端而提高工作效率
- 提高管理能力并降低成本
- 通过强大的终端保护能力和精细的接入控制而确保安全
- 通过网络优化提高应用性能

解决方案

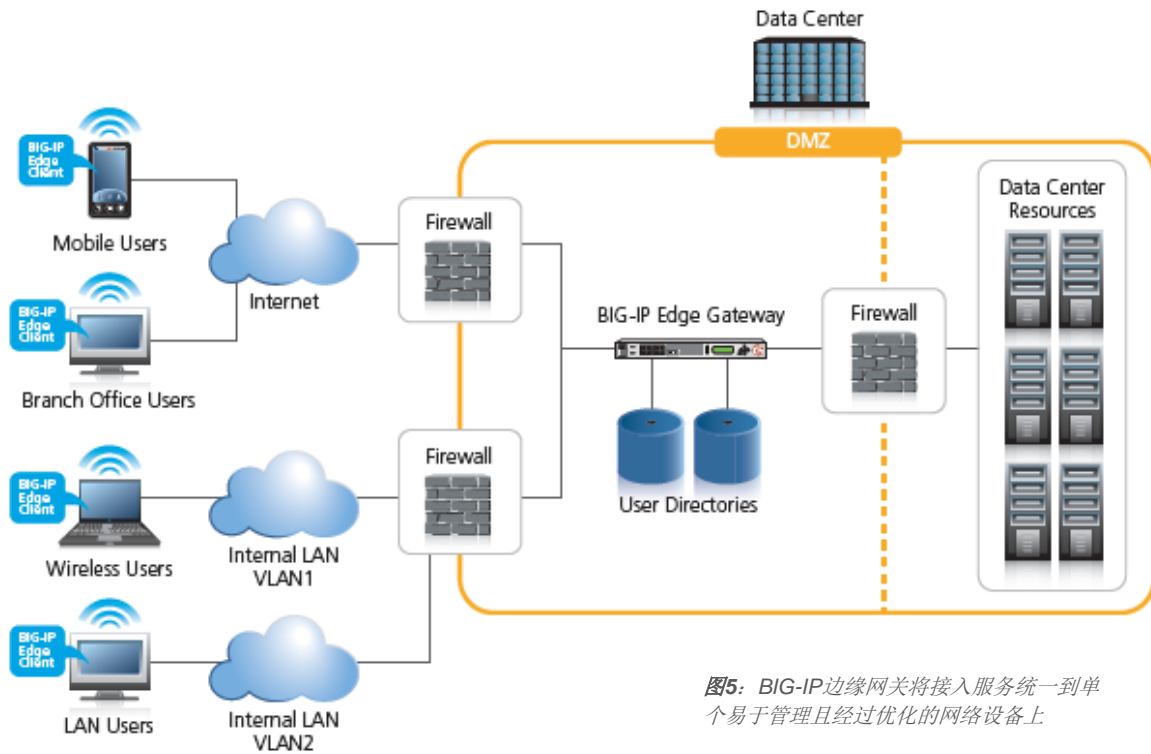


图5: BIG-IP边缘网关将接入服务统一到单个易于管理且经过优化的网络设备上

BIG-IP® 边缘网关™是一种企业接入解决方案，它将针对远程用户的SSL虚拟专网 (VPN) 远程接入、安全、应用加速和可用性服务结合在一起。BIG-IP边缘网关将身份管理融入网络中，以LAN的速度提供具有上下文感知的、基于策略的、安全的远程应用接入。

作为行业中最安全的加速接入解决方案，BIG-IP边缘网关可帮助接入关键业务应用和网络的用户实现最高的性能。借助BIG-IP边缘网关，客户可以轻松地使用户通过任何网络或移动设备（包括Apple iPhone、Apple iPad、Andriod、Windows Mobile和Windows Phone设备）更快地远程接入企业应用和数据。

简化 DNS 安全扩展 (DNSSEC) 技术，并确保全局分布的应用的高可用性

挑战

域名系统 (DNS) 在互联网上提供了最基础但又至关重要的一项功能。如果DNS不运行，则您的业务也可能无法运作。DNS缓存投毒和其它DNS攻击可威胁本地DNS服务器的安全，并使黑客能够劫持DNS响应，将客户重定向到恶意站点，并且接入私密信息。您可以利用域名系统安全 (DNSSEC) 保护业务和Web安全。

主要优势

- 强大的DNS安全
- 遵从政府DNSSEC法规
- 可选的FIPS密钥安全
- 通过网络优化而优化实施，并降低管理成本
- 高可用性和高性能

解决方案

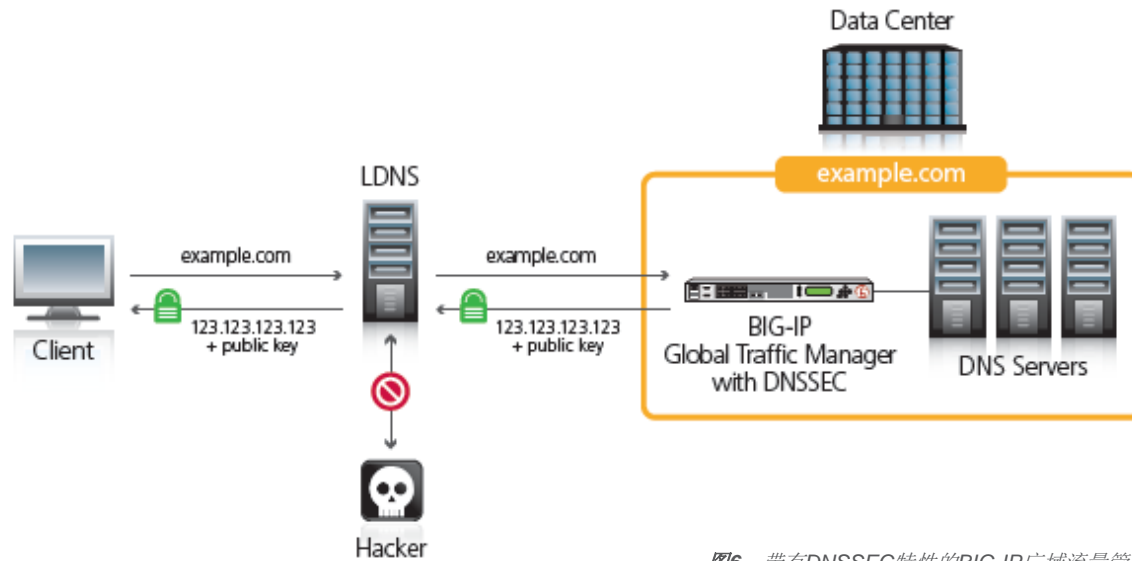


图6: 带有DNSSEC特性的BIG-IP广域流量管理器实现安全、动态的DNS响应

带有DNSSEC特性的BIG-IP® 广域流量管理器™ (GTM) 提供了以下能力:

- **DNS数据来源验证。** 解析器可以验证数据来自权威来源。
- **数据完整性。** 解析器可以验证响应在传送过程中没有修改。
- **证实域名不存在。** 在没有数据可供查询时, 权威服务器可以提供一个响应, 证明没有数据存在。

F5 DNSSEC保证了您的客户在要求名称解析时收到的答案来自可信的域名服务器。实施BIG-IP GTM DNSSEC特性可以显著提高您的DNS安全。BIG-IP GTM有助于您遵从**全球**DNSSEC要求, 并保护您宝贵的域名和Web财产不被恶意服务器用于发送无效的响应。

F5采用的DNS安全方法, 使企业能够快速且轻松地将DNSSEC部署到现有的全球服务器负载均衡环境中。带有DNSSEC特性的BIG-IP GTM提供了可扩展、易于管理且安全的DNS基础设施, 能够应对DNS攻击。

将企业电子邮件的保护能力扩展到企业网络边缘

挑战

在您的企业网关中，每一封不需要的电子邮件消息都会消耗昂贵的带宽和服务器资源，并且可能对安全产生潜在威胁。在系统容量有限，而且安全威胁不断增加的情况下，IT部门更难保证业务连续性。企业通常的应对方式是在基础设施中增加更多的邮件安全网关、防火墙和邮件服务器，并且购买更多的带宽满足电子邮件流量的要求。鉴于这些原因，保证消息处理成本不超出预算是一项具有挑战性的任务。

主要优势

- 将不需要的电子邮件和垃圾消息显著减少70%
- 基于实时查询发件人信誉而采取策略
- 降低总体基础设施成本

解决方案

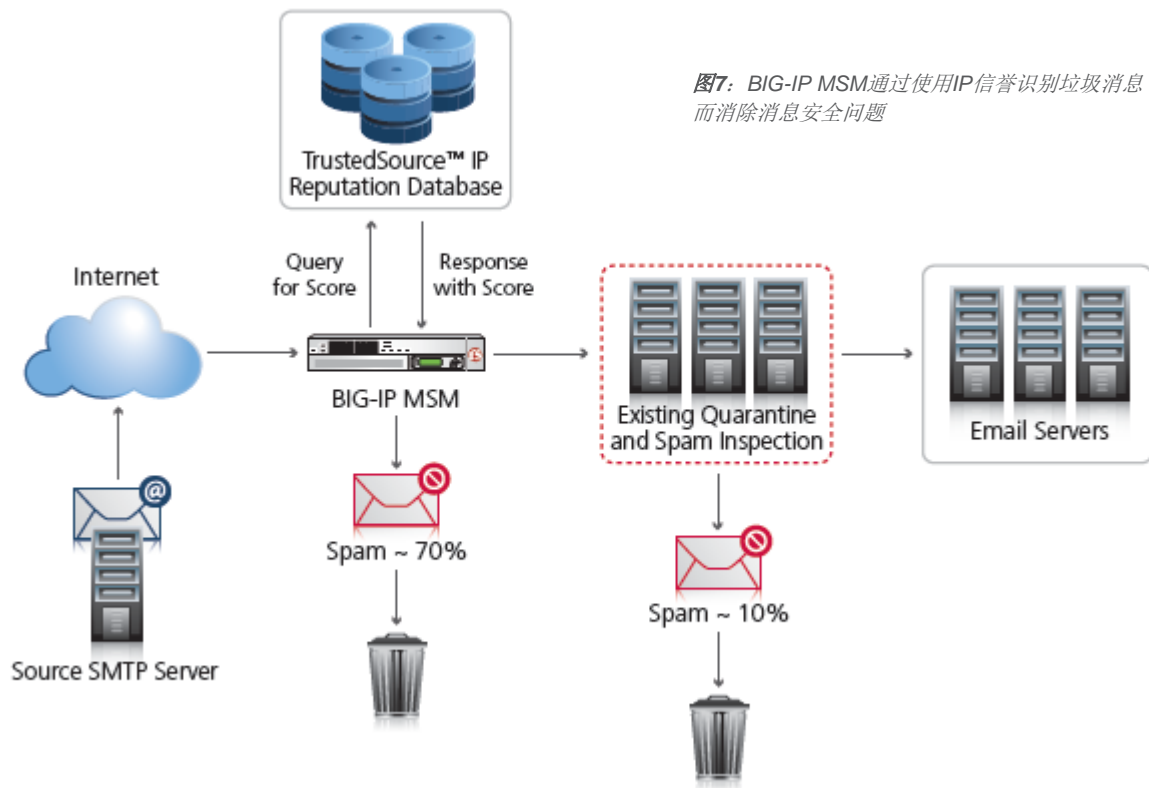


图7: BIG-IP MSM通过使用IP信誉识别垃圾消息而消除消息安全问题

BIG-IP® 消息安全模块™ (MSM) 是一个网络边缘解决方案，它增加了安全智能化，通过在做出流量管理决策时考虑发件人的信誉而管理并过滤收到的电子邮件流量。BIG-IP MSM是业内第一个基于信誉的网络边缘安全模块。

BIG-IP MSM利用来自Secure Computing的TrustedSource多身份信誉引擎的数据，将企业电子邮件的防护能力扩展到企业网络边缘。该解决方案为企业应对日益增多的不需要的电子邮件流量提供了极为强大且高效的工具。

更多信息

欲了解F5安全解决方案的更多信息，请访问 [f5.com](https://www.f5.com)，搜索以下产品和解决方案页面。

BIG-IP本地流量管理器

BIG-IP接入策略管理器

BIG-IP应用安全管理器

BIG-IP协议安全模块

BIG-IP边缘网关

BIG-IP广域流量管理器DNS安全

(DNSSEC)解决方案

BIG-IP消息安全模块

“简言之，我们现在能够为
客户提供一个高度可靠且安
全的**Web**平台，这是我们未
来成功的重要因素。”

– Steven Opstaele, 领先的人力资源软件和服务供应商NorthgateArinso首席基础设施架构师

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

本文中的其它所有产品和公司名称可能是各自所有者的商标，不作任何明示或暗示的认可或从属关系声明。

© 2010 F5 Networks公司。保留所有权利。F5、F5 Networks、F5标识、BIG-IP、FirePass、iControl、TMOS和VIPRION是F5 Networks公司在美国和其它国家的商标或注册商标 CS18-00007 0211

