



F5 ARN应用就绪网络

为MICROSOFT WINDOWS SERVER 2008而定制

增强 Microsoft Windows Server 2008 部署的安全性、可用性和性能

综述

Microsoft® Windows® Server 2008 决不仅仅只是一个微软发布的新版本。从下一代 TCP/IP 协议栈到新版本的 Windows 终端服务和互联网信息服务，以及 Windows PowerShell 和安全套接字隧道协议等新技术，Windows Server 2008 可帮助信息技术专业人员最大程度地控制其基础架构，同时提供无与伦比的可用性和管理能力。在测试阶段和其它阶段中，F5 一直与微软合作，以保证与整个 Windows Server 2008 平台的高度互操作性和优化。F5 为 Windows Server 2008 定制的应用就绪网络不仅有助于优化 Windows Server 2008 部署的端到端性能、可用性和可扩展性，还可降低与部署、管理及运行相关的成本。

优点及 F5 价值所在

用户体验和应用性能

Microsoft Windows Server 2008 为各企业提供了一个强大的新平台，旨在为下一代网络、应用和 Web 服务提供强大的动力。Windows Server 2008 包含多个令人振奋的新组件，例如微软新型的 TCP/IP 协议栈、安全套接字隧道协议 (SSTP) 和新版本的行业标准应用，如 Windows 终端服务和互联网信息服务。F5 一直与微软密切合作，确保 F5 针对 Microsoft Windows Server 2008 的应用就绪网络提供最高的应用可用性、性能和最终用户满意度。

Microsoft Windows Server 2008 的一个亮点是完全重新从头设计的下一代 TCP/IP 协议栈。F5 解决方案包含多项兼容微软新协议栈的 TCP/IP 优化技术。这些优化与会话级应用感知、持久隧道、选择性确认、错误修正和优化的 TCP 窗口相结合，使 F5 设备和 Microsoft Server 2008 系统能够充分利用可用带宽。这使得 F5 设备能够实时地适应 WAN 链路的延迟、数据

包丢失和拥塞特征，并加快几乎所有应用流量。另外，F5 可隔离、控制和独立优化用户和服务器连接，使服务器和最终用户能够最大限度地提高工作效率。

随着互联网的迅速扩展和可用的 IPv4 地址的迅速减少，各企业都希望保证其网络基础架构能为未来的发展做好充分的准备。对互联网协议第 6 版本 (IPv6) 的支持已不再是一个奢侈的想法，而是一个必需的行为。作为互联网网络层的一套新的标准协议，IPv6 已被结合到 Windows Server 2008 和 F5 设备中，使您的网络和微软应用为这种不可避免的变革做好准备。由于 F5 对 IPv6 的支持，各企业随着 IPv6 流量的增长，对于在不进行大规模网络和应用升级的情况下分段进行网络移植都已制订了明确的战略。此外，F5 设备可进行 IPv6/IPv4 的转换，通过转换流量供 IPv4 或 IPv6 终端使用。这样，各企业可以随着对 IPv6 的需求不断增加而逐步移植。F5 使您能够随意将 IPv4 和 IPv6 服务结合

到 Windows Server 2008 上；例如，F5 可作为仅使用 IPv6 的 Windows Server 2008 Web 接入服务器的 IPv4 前端。有了 F5 设备，各企业将拥有一个满足当前及未来要求的强大解决方案。

Windows Server 2008 提供了极高的效率，表现在它为服务器工作负荷和应用要求提供了一个坚实的基础。F5 的一个核心强项是其在增强用户体验的同时提高应用和服务器性能的能力。F5 通过接管过去必须由服务器执行的多项职责而做到这一点。如果每台服务器必须执行处理器重负荷任务，例如压缩、缓存和 SSL 处理以及证书管理，则这些设备为执行核心任务而剩余的处理能力就会降低。通过将这类任务交给 F5 集中的高能力网络设备，F5 可大大提高 Windows Server 2008 服务器的效率，使企业减少所需的硬件数量。这适用于 Windows Server 2008 所有的主要组件，包括 Windows 终端服务、互联网信息服务器和 SSTP。

F5 提供了用于保障网络最高效率的技术。因为 F5 独特的 TMOS™ 操作系统是一个全代理架构，它可以优化系统中连接的任何终端。作为通信的全面代理，系统可优化其中每个终端设备的通信。这种优化可在从传输层到协议和应用层的整个协议栈中实现，这些功能是 Windows Server 2008 所不能企及的。这样可以减轻 Windows Server 2008 设备的工作负荷，从而提高服务器的效率。通过减少网络中不必要的协议通信，F5 加快了 Windows Server 2008 部署和网络中其它应用的响应时间，并提高了利用率。

在 WAN 环境中，即使是高性能、高效的应用和服务（例如 Windows Server 2008）以及局域网中的其它设备也往往会显得无可奈何，无法发挥其高性能和高效率。WAN 中的网络延迟是全球各地的 IT 部门遇到的最大挑战，也是各企业在部署 Windows 终端服务此类可供用户从任何地方接入的应用时考虑的一个主要问题。简单地增加带宽并不能解决问题。F5 可帮助以多种方式显著降低延迟的影响。除了可以从 TMOS 中获益之外，F5 还通过多种能力解决延迟问题，包括避免重复浏览下载相同数据，并通过控制浏览器的行为保证带宽得到最充分的利用。通过减少额外的有条件请求和浏览器与 Web 应用之间（重复）发送的过量数据，F5 减轻了 WAN 延迟、网络错误和数据包丢失的影响。

“Windows Server 是我们的企业客户最常用的应用平台之一。因此，F5 投入了大量资源，在 beta 版产品测试的每个阶段测试其应用交付产品对 Windows Server 平台技术的兼容性，以保证高度互操作性。”

Jim Ritchings, F5 业务开发副总裁

F5 应用就绪网络的一个优点是大量的资料可以使用，从而减轻配置和优化设备的精力负担，并将宝贵的 IT 人力资源用于开展其它项目。在为 Microsoft Windows 2008 而定制的应用就绪网络中，F5 针对 Windows Server 2008 的主要组件进行配置、测试并且调试了我们的设备，并且在“部署指南”中仔细地对程序进行了归档。F5 还提供了配置设置和策略，使设备的配置简单易行，而又具有强大功能和灵活性，其中一些策略包括如 Microsoft 互联网信息服务和 Windows 终端服务组件的预置下拉菜单。现在，利用我们的管理设备，部署指南配置文件可用作模板，并轻松地上传和应用到 F5 设备中。凭借 Microsoft PowerShell 的强大功能，利用 Windows Server 2008 中包含的命令和脚本语言，以及 F5 的 iControl PowerShell Cmdlets 和脚本，开发人员就可以通过独特的方式在一个地点控制和管理 F5 设备¹。

应用安全

性能和最终用户体验对于 Windows Server 2008 的成功部署至关重要，但是，确保应用的安全性可能更为关键。由于应用和数据库中存储的数据的敏感性，加上遵从新的要求和关于数据保护的政府法规的需要，保证您应用的安全比以前更加重要。F5 安全解决方案为 Windows Server 2008 提供了全面的防护，保证您的数据和应用处于安全状态。

多年前，仅仅在 LAN 前部架设网络防火墙被认为足以保证安全。接下来出现的入侵防护/检测系统，进一步增强了安全性，尽管这是一种被动安全模式。

然而，IPS/IDS 系统仅可以防止已知的攻击和签名。F5 实时检测并减少无模式漏洞入侵，对不能有效应对 HTTP 和 HTTPS 承载的威胁的现有防火墙和 IDS 设备增加准确的补充保护。

除了分析和阻止已知攻击签名外，F5 还可以从报头中剥离出识别操作系统

和 Web 服务器的信息（例如版本字符串、签名和指纹），向用户隐藏所有 HTTP 错误消息，并且从发送给用户的页面中消除应用错误消息，同时通过检查保证不会有服务器错误或私密 HTML 注释泄露到公共网页上。

F5 设备还预防那些采用 Cookies 以及透明分发到其他标记的攻击。F5 设备可以通过轻松配置对 Windows Server 2008 使用的 Cookies 进行加密，从而防止 Cookie 篡改和其它基于 Cookie 的攻击。这为企业运行中的应用及更高的用户身份信任度提供了卓越的安全性。

对于连接到网络和 Windows Server 2008 服务器及应用的远程用户，F5 提供了极为严格的终端安全。在远程用户登录到 F5 设备访问网络之前，除了登录前的其它多项检查之外，F5 可确定用户 PC 上是否运行了防病毒软件或个人防火墙，或者强制要求升级到特定的操作系统补丁。

F5 不仅为您提供全面的应用安全解决方案，还可以提供安全性极高的设备。我们保证您的 Windows Server 2008 部署及其中包含的信息处于绝对的安全状态。

统一的安全管制和接入控制

对于一个完整的安全平台来说，另一个不可分割的要素是安全管制和接入控制。要求从外网接入企业资源的员工数量每年都在增加。随着企业与企业间的交易日益增多，不仅员工需要接入网络，合作伙伴、承包商和供应商都要求接入不同的内部应用，各企业都面临着接入控制和强化管理问题。无论是什么样的最终用户、客户端类型、什么样的应用、无论是接入网络还是网络资源，F5 都提供了一套完整的安全执行方法，为 Windows Server 2008 提供接入控制。

利用 F5 设备，对 Windows Server 2008 资源的接入可以轻松进行极为严格的控制。例如，员工可以被授权全面接入内部资源，可信的合作伙伴群体只能接入特定的一组应用，承包

¹ 关于 iControl 和 Microsoft PowerShell 集成的更多信息，请访问 <http://devcentral.f5.com/Default.aspx?tabid=71>。

² SANS@RISK, “The Consensus Security Vulnerability Report”

商群体只能接入一个特定的应用或端口。F5 集中实施这种接入控制，并且使接入控制的配置和执行简单易行。

业务连续性和灾难恢复

灾难恢复和业务连续性对于一个企业的成功至关重要。断电、整个数据中心的数据被清除，这些产生大量麻烦的未知事件和灾难，并不是仅仅是一个牢固的安全平台所能够预防的。这些破坏性事件不仅会使企业花费数千甚至数百万美元的代价，还可能因行业和政府有关数据保护和灾难恢复规则而导致承担法律后果。由于网络和 Windows Server 2008 这样的应用中存储大量不可替代的、对业务至关重要的信息，因此，拥有高效的灾难恢复计划是基本的要求。

F5 产品的独特之处在于它们能帮助企业减少灾难和其它破坏性事件。F5

是唯一以集成化方式实现数据中心、VPN 接入、优化和流量虚拟化以保证 Windows Server 2008 设备和应用始终可用的厂商。

当甚至是像遭遇到暴风雪天气、大部分员工无法到达办公室这样的破坏性事件发生时，F5 提供的高度安全的远程接入网络和 Windows Server 2008 设施的方式，确保只要有一个数据中心还能运行，即使员工无法到达办公室，业务仍能够继续开展。

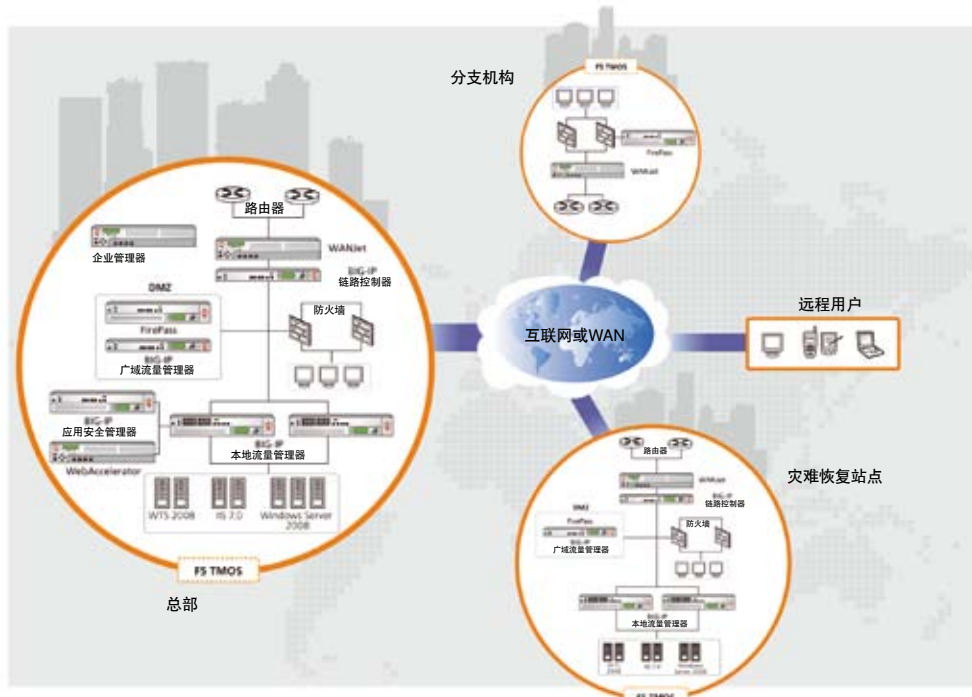
F5 远程接入设备支持 Microsoft Vista 以及 Windows Server 2008 设备的接入，甚至提供了从 Windows Mobile® 5/6 PocketPC 和 Smartphones 的安全应用接入。

在灾难恢复计划中经常被忽略的一种情况是：灾难事件没有在您的企业中发生，而是在您的 ISP 发生。尽管许多企业有多条链路，但必须进行复

杂的 BGP 配置。F5 简化了多宿主部署，这样，您不再需要 ISP 的协作，也不需要定义 IP 地址段、ASN，或者依靠复杂的 BGP 配置来保护您的网络不受 ISP 网络中断的影响。利用 F5 的技术，企业还可以选择将多个小链接汇总到一起，而不必投资建立一个高带宽连接。这样可使企业能够随着业务的增长而扩展服务范围。F5 无缝地监控多个 WAN ISP 连接的可用性和性能，从而智能地管理站点的双向流量，实现灾难恢复和优化的互联网接入。F5 设备检测整个链路中的错误，以提供端到端的可靠 WAN 连通性。F5 监控每个连接的健康状态和可用性，检测链路或 ISP 的连接中断。在出现故障的情况下，流量被动态地路由到其它可用的链路上，使用户始终保持连接。

广域网中部署F5与Windows Server 2008

以下为采用 F5 系列产品在广域网及局域网中优化、保护和交付 Windows Server 2008 应用的配置图。



其他相关信息

部署指南

部署F5和Windows Server 2008

介绍部署 Windows Server 2008(包括 Windows 终端服务和互联网信息服务 7.0) 时, 如何配置 BIG-IP® 本地流量管理器™ (LTM) 和 WebAccelerator™ 的详细步骤。

欲了解更多微软部署指南, 请参考 F5 解决方案中心的部署指南专栏。

欲了解 F5 和微软合作的更多信息, 请参考 F5 解决方案中心的 Microsoft Partner Showcase。

F5 产品系列

BIG-IP 系列产品

BIG-IP 产品提供了高可用性、更高的性能、应用安全性和接入控制, 所有这些都单个设备中实现。单个 BIG-IP 设备可执行十多个专用产品的工作。更重要的是, 它能以高效、统一的方式做到这一点, 而且随着业务和技术需求的变化, 它更容易管理和适应变化。

产品模块(这些模块也可作为独立的设备运行)

LTM: BIG-IP LTM 使企业能够保证服务质量和可管理性, 将业务策略和规则应用到内容交付上, 支持日益增多的业务量, 安全地提供应用, 提高运作效率和成本控制能力, 并且灵活地应对未来的应用和基础架构变化, 以保护投资。

GTM: BIG-IP 广域流量管理器 (GTM) 模块为多个全球分散的数据中心内运行的应用提供高可用性、最高的性能和全局管理, 无缝地实现 FirePass VPN 的虚拟化, 以自动提供不间断的接入控制。

ASM: 应用安全管理器™ 使应用层免遭有针对性的和普遍性的应用攻击, 以保证应用的始终可用和最佳的运行性能。

WA: F5 WebAccelerator™ 是一个先进的 Web 应用交付解决方案, 它提供的一系列智能技术旨在克服浏览器、Web 应用平台的问题以及影响用户性能的 WAN 延迟问题。

LC: BIG-IP 链路控制器模块无缝地监控多个 WAN 连接的可用性和性能, 从而智能地管理站点的双向话务流量——提供故障容错、优化的互联网接入。

特性模块: 这些是单独的特性包, 可以添加到 BIG-IP 流量管理平台中。特性模块包括信息安全、智能压缩、L7 速率修整、IPv6 网关、高级客户机验证、SSL 加速、高速缓存和高级路由模块。

FirePass

F5 的 FirePass SSL VPN设备提供了使用标准 Web 浏览器安全接入企业应用和数据的方法。FirePass 具有卓越的性能、扩展性、易用性和终端安全性, 有助于提高在家中或移动办公人员的工作效率, 同时保证企业数据的安全。

WANJet

WANJet® 是一个基于设备的解决方案, 通过 WAN 提供类似 LAN 的应用性能。WANJet 加速的应用包括: 文件传输、电子邮件、客户机/服务器应用、数据复制等, 从而为所有的广域网用户提供可预测的高性能。

企业管理器

F5 基于设备的企业管理器™ 使您能够集中发现并维护网络中的 F5 设备。利用企业管理器, 您可以对设备配置进行存档和安全防护(用于制订应急计划), 从一个集中位置配置新设备, 无需手工处理每个设备, 轻松而且快速地发布软件升级和安全补丁等。

F5 Acopia ARX

F5 Acopia™ 屡获殊荣的智能文件虚拟化解决方案将文件访问与文件实际位置分隔开。我们的 ARX® 产品无缝集成到现有的网络存储 (NAS)、Windows®、UNIX® 和 Linux 环境中。ARX 设备提供了业界领先的扩展性、性能和可靠性, 并且专门为了满足企业存储环境的需求而设计。

iControl API

iControl® 是 F5 的 SOAP API, 它用于每个 BIG-IP LTM 系统上。iControl 实现应用和网络之间的自动化, 并且使企业能够灵活地保证应用和网络协同工作, 以获得更高的可靠性、安全性和性能。F5 的开发人员社区 DevCentral 有 iControl 应用和代码的样例。请访问 DevCentral 上的微软页面进入 Microsoft 专区论坛, 并了解关于 F5 与微软应用集成的其它信息。



<http://www.f5.com.cn>

F5公司北京代表处

地址: 北京市朝阳区建国路79号
华贸中心1号写字楼1707-09室
邮编: 100025
电话: 010-59234000
传真: 010-59234100

F5公司上海代表处

地址: 上海市虹桥路3号
港汇中心2座27110室
邮编: 200030
电话: 021-61132588
传真: 021-61132599

F5公司广州代表处

地址: 广州市环市东路368号
花园酒店花园大厦1035室
邮编: 510064
电话: 020-83884169
传真: 020-83883897