现代企业
IT架构规划建议

前言

随着信息技术几十年来的飞速发展，目前几乎所有的现代化企业都已经或正在把企业信息化作为企业发展的战略之一。企业信息化规划则是实施这一战略的蓝图。企业信息化规划以整个企业的发展目标，发展战略和企业各部门的目标与功能为基础，结合行业信息化方面的实践和对信息技术发展趋势的掌握，提出企业的信息化远景，目标和战略，全面系统地指导企业信息化的进程，协调发展地进行信息技术的应用，及时地满足企业发展的需要，以及有效充分地利用企业的资源。

不断提升并完善企业信息化的价值是一项复杂的系统工程，它既需要软件和硬件设备的大量投资，又需要人力、物力、智力的投入。近年来，很多企业都加快了信息化建设的步伐，通过互联网及企业内部网(专网)，宣传企业或开展电子商务；使用办公OA系统、ERP、CRM等信息管理系统；建立自己的门户网站等，以此提高企业核心竞争力。

因此，在网络信息技术高速发展的今天，企业信息网络是否高效、畅通、安全在很大程度上影响企业的生产、销售、管理等各个环节。对于现代企业来说，及时了解客户的需求和市场动态非常重要，建立一个高效、可靠、灵活的应用交付网络架构就显得尤为迫切。

本书由F5资深技术顾问陈亮主笔，结合了多年来协助众多企业规划IT架构的经验，并广泛征得了F5公司各位资深应用交付网络(ADN)专家的修改意见，几经易稿，终于与大家见面了。它必将成为广大企业在应用交付网络建网实践中不可多得的技术参考文书。

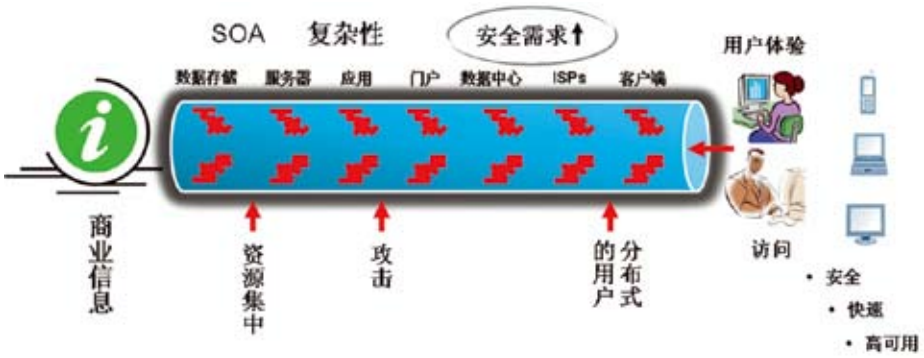
目录

当今的IT系统现状分析

传统大中型企业在信息化建设中，根据其自身的特点，在前期规划中均采用了以网络连通性为核心的规划理念。同时，为了能够实现“快速”，“安全”，“高可用”的用户访问体验，企业的IT建设步伐，一直没有停顿过。

然而，企业的关键商业信息(如WEB 、CRM、ERP、Mail、OA等)都是通过一个虚拟的访问管道将信息传递给企业内部或外部用户、分支机构、合作伙伴。如下图所示:

随着基于网络化应用规模不断的扩大，企业的经营运作对网络应用的依赖越来越强，在企业将商业信息通过这个虚拟的访问管道进行应用发布的过程中，必然会经过物理存在的服务器，应用，门户，ISPs等元素到达不同的类型的客户端最终到达用户，任何基于网络的应用故障，访问缓慢，服务器宕机，安全漏洞，攻击等问题的出现，都会使原本畅通的管道变窄，无法提供最佳的用户访问体验，最终严重影响企业的正常运作，从而降低企业生产力，丧失信誉度，影响企业形象等。如下图所示:



传统的企业IT架构面临的新挑战

在多年的企业信息化建设从无到有的过程中，企业的IT架构已经从以网络部署为核心向一切以保证应用发布为导向的目标发展。

“怎样才能不做任何改动就能让我的应用运行得更好，并且不会增加基础设施成本及管理上的显著开销呢？”“怎么样才能使我的网络及应用尽可能优化、尽可能简单、同时对资源的影响又最小？”

众多企业的CIO或CTO们，正在面临如何保证并提升应用发布管道的畅通，如何有效进行资源整合，如何保证关键应用的发布，如何整体提高网络及应用的安全等问题所带来的前所未有的挑战。

1. 如何保证应用的可用性

企业现有应用系统中常用的OA系统，Mail系统，KOA系统，财务系统，物流系统，WWW发布，网上定单系统，CRM、ERP等众多的应用已成为企业日常运作的重要组成部分，任何一个系统的访问失败都会影响企业运营的进行。

然而，用户在通过网络访问到企业所发布的应用所经过的处理环节中，造成应用访问失败的原因有很多，比如：单一的Internet或专线接入链路出现的单点故障，各网络设备或安全网关类设备的异常中断，后台服务器软硬件系统的失效或日常维护时的停机重启等操作，都无法有效保证企业关键应用系统可以7*24小时不间断运行。

2. 如何提升应用的访问速度

业务大集中后，所有关键应用都将以企业总部为中心，各分支机构、合作伙伴、通过Internet或专线访问的方式进行发布，然而：

- 总部Internet链路接入的带宽不断扩大，但访问速度仍然很慢

大量非关键应用的流量在网络进行传播，使得无限扩充的链路带宽始终无法得到有效利用。

企业内部用户访问Internet资源时，或外部用户访问企业发布的内部资源时，会受到ISP提供商网间互通的瓶颈，造成访问快慢不一的现像。例如：如果企业采用的ISP是通过网通接入的，在访问处于电信的资源时，会由于不同ISP之间互连互通的问题造成访问变慢，而访问网通资源时，就不会存在问题。

- 如何向遍布在全国范围的服务网络提供相同的快速访问途径

各分支机构或合作伙伴采用的网络接入方式，带宽的接入质量存在差异性，造成了访问企业总部应用时的快慢不一。大数量的应用数据传输时出现的延时或丢包等现像，严重影响了企业的关键信息数据发布或收集。

- 如何有效提升服务器的性能

当应用系统模块的增加，突发流量的产生，SSL业务对服务器压力，不均衡的服务器资源使用时，采用简单的服务器硬件升级方式，造成投入更多的服务器升级成本的同时，却无法真正实时智能的缓解服务器的性能压力。

- 如何加快WEB应用的访问速度

当前，许多企业在实施了数百万美元的WEB应用部署之后，却发现与原有的客户端服务器应用相比，新部署的性能不能让用户感到满意。同时，企业出于监管和数据安全性要求需要将服务器集中管理，而WEB应用的用户却作为远程分支办事处和移动用户而分布得更加分散。

与此同时，不幸的是，广域网延迟、错误和其它问题使得WEB应用无法快速交付。在门户应用、CRM应用、协作应用及其它企业

应用情形中，WEB应用架构师和管理员发现其交付性能难以满足用户的期望。

- 安全与性能如何才能兼得?

为保护企业网络及应用的安全，应对永不消失的黑客攻击、恶意入侵、垃圾邮件等等的侵扰，企业在网络中添加了更种IDS、IPS，防火墙，VPN之类的安全网关设备，对用户的身份进行认证，对访问请求进行层层过滤，虽然提高了企业网络的安全程度，但却严重影响了用户访问到应用的速度，造成生产力下降。例如防病毒设备的网络吞吐量通常只有3–10Mbps，因此网络中的安全设备成为了制约网络传输速度的新的瓶颈点。

3. 如何提升不同类型的访问终端的访问速度

基于CDMA、GPRS的拨号上网方式，具备上网功能的手持设备，如PDA，智能手机等被广泛应用，使用户可以随时随地的访问企业的内部信息，然而无论企业端的网络多么畅通，服务器处理性能如何强大，都无法解决由于客户端访问速率低所产生的问题。

4. 如何保证数据在基于WEB方式传输时的数据安全

银行帐号，电子定单，财务数据等关键的应用数据通过基于WEB应用的方式进行传输时，一旦非法人员获取，将使企业或合作伙伴造成重大的经济损失。

5. 如何提升安全防御能力

变化多样的网络攻击及蠕虫病毒在企业的网络中大量泛滥，促使企业不得不想尽一切办法来提升“木桶”的高度，以此来抵挡各种类型的攻击。

目前，企业更多是将精力投放在对网络层的入侵防护，但从近期的攻击来看，多数都是通过WEB应用进入的。

随着互联网资源的广泛利用，各大企业公司对网络流量管理及安全应用的需求也日益增长。现在，针对WEB应用的攻击方式层出不穷，例如cookies篡改、劫持WEB会话、还有就是利用脚本来实现攻击的phishers (网络钓鱼者) 。

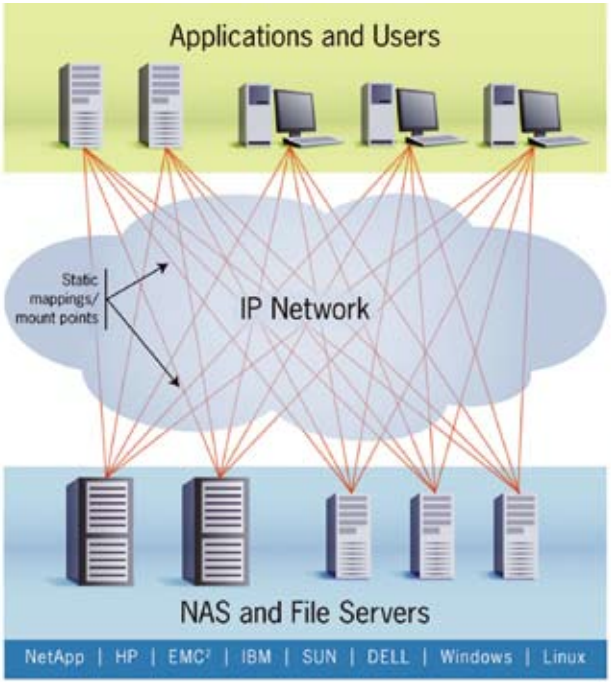
这些WEB应用攻击是网络防火墙等无法识别的攻击类别，这种请求在网络层的防护来说具有合法的格式，是一种有效的请求，既不是蠕虫、也不是其它什么病毒。它唯一出格的行为是: 想要访问未授权的信息。

6. 如何提供更便捷的移动办公方式

随着企业的业务发展，移动办公人员的增加，对于便捷安全的远程接入的需求越来越强，远程接入的使用者的需求就是可以使用任何上网设备，随时随地接入企业网络，访问数据。以往的IPSec VPN因为无法解决高可用性以及受网络接入条件的限制，无法满足随时随地接入的需求，具体表现在客户端使用不方便、某些网络条件下无法接入、无法满足7×24小时的高可用要求。

7. 如何摆脱传统文件存储基础架构的束缚

当前的文件存储基础架构存在一些与自身相关的问题:



※ 复杂性。今天，一般的企业存储基础架构由一系列存储平台、文件系统和操作系统组成，而这些设备可能来自不同供应商。遗憾的是，大多数设备并没有完美无缝地一起协同工作，而且每个设备不得不作为存储“孤岛”进行管理。

※ 缺乏灵活性。用户和应用程序静态映射到包含它们需要访问的数据的物理文件存储资源。在某些环境中，这有可能产生数百或数千个独立映射(或安装点) 。每当文件存储环境发生变化，例如，当提供新存储或移动文件时，这些静态映射都会被破坏。更新环境时，要求手动配置和系统停机。事实上，企业战略集团(ESG) 估计超过40%的企业每周或每月都要进行数据迁移，而大约58%的企业报告因为数据迁移而导致它们延长停机时间或遭遇突然停机。此外，这些停机与当今全天候的全球业务环境要求格格不入，意外停机已越来越不能被容忍。

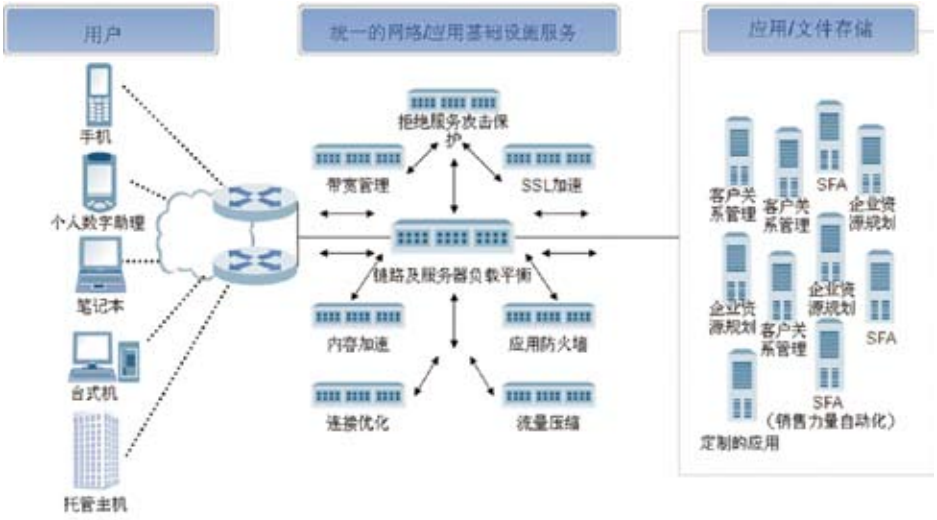
※ 低效率。虽然可能有一些特定的文件服务器或网络连接存储(NAS)设备得到高度利用，但总的看来，文件存储设备并没有被充分利用，在大多数企业环境中容量利用率平均起来仅达到40-50%。这通常不是设备利用率不足的结果，而是设备供应过多的结果，因为一直没有一种简单但又不具破坏性的方法在不会造成停机的情况下平衡文件系统的需求或增加容量。

※ 大规模增长。容量需求正在快速增长，而文件数据占到了该增长的70%以上。这进一步加剧了这个问题：随着存储需求的增长，需要不断补充存储设备，这又会使环境变得更加复杂、更不灵活和效率更低。

对更大存储容量永不满足的需求，再加上管理存储所需的更大成本，导致了存储费用螺旋式上升。因此，必须要有一个更好的方法来管理这种快速增长的文件存储基础架构，而且不会相应地增加管理费用。

传统的企业IT架构存在的弊端

传统的企业IT架构由于以前更关注网络连通性的架构设计，因此在企业面临上述挑战时，通常都是采用“打补丁”式的解决方案将负载均衡设备，安全网关，带宽管理，SSL加速，应用防火墙等产品添加到网络中，如下图所示:



这种“打补丁”式的方案虽然可以有效解决性能压力，访问延迟，安全漏洞等问题，但在实际使用中，其结果却是管理费用浩大、繁杂，导致显著的应用延迟。企业仅仅是在“拆东墙补西墙”，并未真正解决问题。这些问题主要体现在以下几个方面:

1. 复杂的部署方式

在添加这些产品时，将涉及各厂商设备之间兼容性问题，互协调性等问题。而为避免点单故障问题，也将采用冗余的方式，对原有网络进行大的改动。

2. 网络延时增加

每添加一台设备都将加大网络的延时，都有可能成为新的性能瓶颈点。

3. 增加运维成本

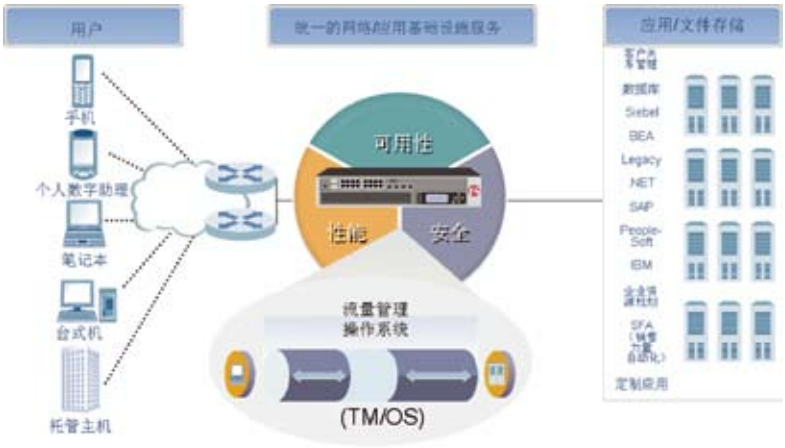
方案中使用了大量新兴的如负载均衡，流量控制，连接优化等多种多样的复杂技术，这样就必需要求企业的技术人员需要掌握更多的新兴技术，才能对各厂商的产品进行管理。

同时，企业需要与越来越多的产品提供商，服务提供商进行沟通，大大增加了企业的运维投入成本。

ADN-实现现代企业IT架构目标的源动力

基于现代企业IT架构目标的广泛需求，F5公司率先推出了确保网络/应用可用性，提升处理速度，促进安全等三大技术为一体的统一网络/应用基础IT架构，即ADN (应用交付网络) 解决方案。

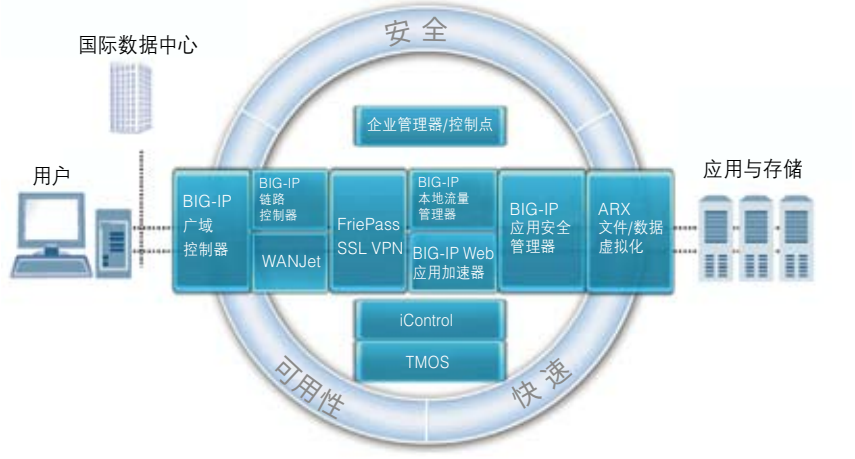
F5公司的ADN解决方案以确保应用交付为核心，其产品及技术涉及到了负载均衡，应用健康状况监控，带宽管理，应用加速，数据压缩，SSL加速，SSL VPN安全远程接入，防止拒绝服务攻击等世界领先的技术。



如上图所示: F5公司所推荐基于ADN的IT架构设计中，极大减少了企业的投入成本，并可以利用F5公司所提供的产品及技术提升企业原有网络/应用的可用性，性能及安全性。

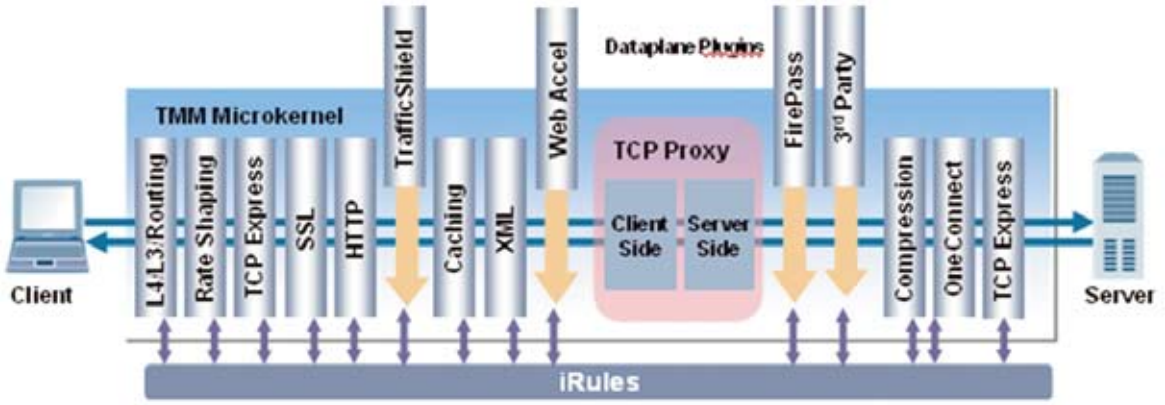
1. ADN体系架构各关键元素介绍

F5公司的ADN体系统架构依托于传统的网络架构基础之上，并以确保应用发布为核心。因此，在ADN架构中，各组成部分将主要围绕可用性，高效，安全等三大方面。



ADN各元素包括:

- TMOS-ADN的核心元素



ADN的核心是一款创新体系结构，称为TMOS (流量管理操作系统)，它为企业提供了一套统一系统来帮助其实现最佳应用交付。TMOS针对BIG-IP上的每项功能都做了改进，在支持BIG-IP智能地适应应用与网络日新月异的需求同时，提供了面向所有服务的完全可见性、灵活性和控制能力。

TMOS使BIG-IP能够高效地将客户机与服务器端数据流隔离开来、独立维持每个连接设备的最佳性能，并承担起系统间的通信工作，以改进应用性能。

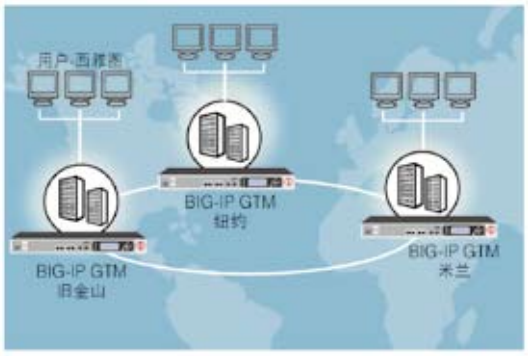
F5产品家族中所有运行在TMOS体系架构中的产品(除WANJET, FirePass及Enterprise Management——企业管理器外)，即可以单独运行在一台设备上，又可以以软件模块的形式共同运行在同一台设备中，减少硬件设备数量。

如今，任何与BIG-IP相连的系统或IP应用都将可以更高效地工作。

- BIG-IP Global Traffic Manager——广域流量管理器

BIG-IP广域流量管理 (以前称为3-DNS) 可以为运行于多个全球(或全国)散布的数据中心的应用提供极高的可用性、最出色的性能和集中式管理。

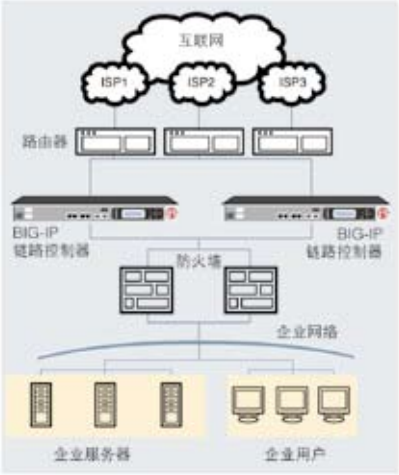
基于F5模块化和可扩展的TMOS构架，BIG-IP广域流量管理器可根据业务策略、数据中心和网络条件来分配最终用户应用请求，以确保最高的可用性。



- BIG-IP Link Controller——链路控制器

随着企业开始更多地使用互联网来交付其应用，只有一条到公共网络的链路意味着较高的单点故障和网络安全性风险。BIG-IP链路控制器可以无缝地监控多条WAN ISP连接的可用性和性能，以智能地管理到某一站点的双向流量，从而提供出色的容错性和优化的互联网访问。

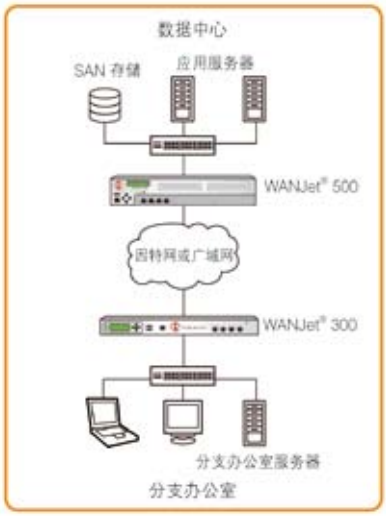
凭借F5的TMOS体系结构，BIG-IP链路控制器提供了改善的链路性能和较高的可用性，以及灵活、强大的状态检测、全面的安全性和改进的可用性等附加优势。



- WANJet

WANJet是一款硬件解决方案，能够在广域网中实现局域网一样的应用性能。WANJet可对文件传输、电子邮件、客户端——服务器应用、数据复制及其它应用进行加速，改善所有广域网用户的服务性能和可靠性。

对于数据中心，WANJet具有较高的容错性和可扩展性，可支持高达20,000 条优化连接。对于分支办事处，WANJet 200具有较高的容错性、静音性和性能，可支持高达1,000条优化连接。WANJet解决方案可在所有广域网中无缝运行，包括专用链路、IP VPN、帧中继和卫星连接。



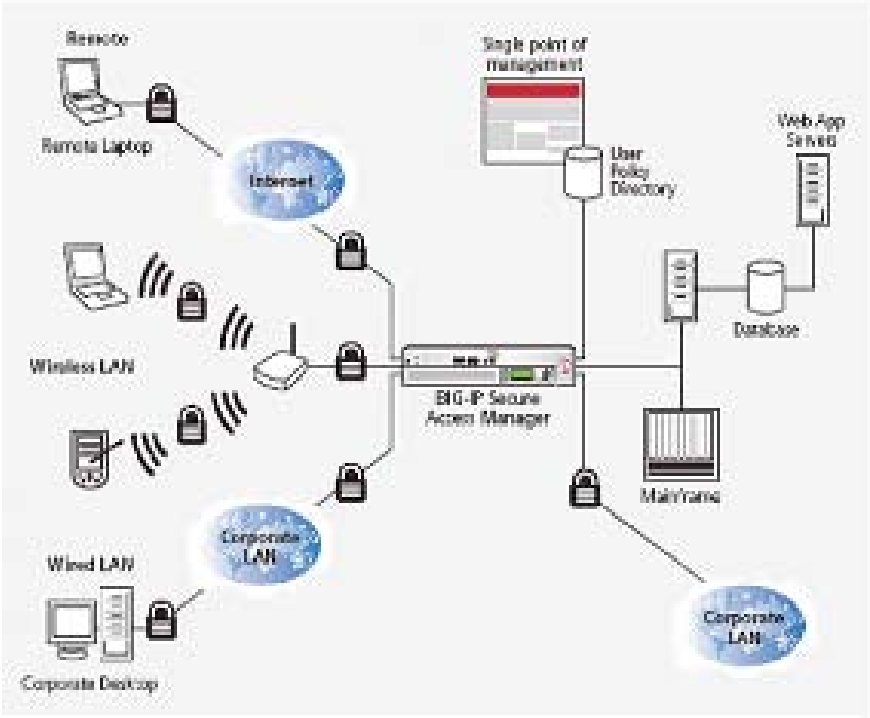
- FirePass——SSL VPN

借助FirePass，企业将能够支持在家办公或在路上移动办公的员工，使用任何支持Web的设备，通过任意接入网络随时随地安全地远程访问网络资源。通过FirePass平台，企业将可以获得卓越的性能和出色的可扩展性、以及易于管理的特性和先进的应用安全性，进而受益匪浅。此外，该产品还提供了业界唯一的开放式应用编程接口 (API) 、"Visual Policy Editor (可视化策略编辑器) " 和软件开发商套件包 (SDK) ，并带有众多同类产品所没有的一系列独特性能与功能。

- BIG-IP SAM (Secure Access Management) ——安全接入管理器

BIG-IP® 安全接入管理器™ (SAM)是一个高性能、灵活的安全平台，它通过单一设备提供了统一的安全接入解决方案。BIG-IP安全接入管理器采用SSL隧道技术对流量进行加密，为任何客户端用户提供了对企业应用的基于策略的安全接入，包括员工、承包商、合作伙伴和供应商到任何企业资源。BIG-IP安全接入管理器为安全的web应用客户端与企业应用的连接提供了端到端的数据保护。

BIG-IP安全接入管理器基于F5独特的TMOS™ 架构，这个专用的、高伸缩性操作系统是专为精细地控制网络流量而设计的。BIG-IP安全接入管理器与TMOS的密切集成提供了在单一设备上支持多达25,000个并行用户的能力，凭借其较高的扩展能力和吞吐量性能而支持统一的网络接入管理系统。



- BIG-IP Local Traffic Manager——本地流量管理器

BIG-IP本地流量管理器对进出应用的流量了若指掌，可帮助实现最大的应用可用性与性能加速。

主要提供:

可靠性——提供业界最成熟、最先进的系统，以确保应用的可靠性。

应用加速——提供无可比拟的控制能力以实现高达三倍的应用性能加速，确保高优先级应用可最先得到服务，并卸载极耗资源的服务器循环。

降低服务器与带宽成本——通过一整套丰富的基础设施优化特性而实现三倍的服务器容量提升；通过智能 HTTP 压缩、带宽管理及其它特性减少 80% 的带宽成本。

更高的网络与应用安全性——从DoS保护到隐蔽(cloaking)再到应用攻击过滤，BIG-IP提供了网络中其它设备所无法提供的关键安全特性。

无可比拟的应用智能与控制能力——业界唯一一款可实现完整应用流畅性的解决方案，支持网络速的全负载检测和程式基于事件的流量管理，以对应用流进行分析和做出响应。

所有IP应用的总集成——提供一款全面的解决方案，可集成所有应用，不只是基于Web的协议。为企业提供一款支持所有IP应用的集中式解决方案，包括原有和新出应用(如VOIP)，全在单个统一的系统内。

业内领先的性能——提供业内最快速的流量管理解决方案，以满足企业在安全性、内容交付和性能优化方面的需求。提供目前市面上最佳的SSL TPS、批量加密以及最高数量的并发SSL连接。

BIG-IP VIPRION-按需扩展应用交付控制器

从日益增多的用户数量到数据中心整合以及部署更多功能丰富的应用，企业不断扩展的基础架构对网络施加更大的压力。扩展应用交付网络(ADN)来满足这些演进需求意味着将提高运营成本和复杂性。由此导致的资源紧张可能限制企业快速响应发展需求的能力。

VIPRION(威普龙)是一种单一而功能强大的应用交付控制器(ADC)，它采用模块化高性能插卡，插拔模块不会中断应用运行。无需向网络中添加更多设备和分割应用，您可以随着需求的增长轻松地提高现有基础架构的处理能力。威普龙为您提供必要的可扩展性，帮助您制定可靠、可持续的ADN增长战略。

提高智能及性能，而不会增加运营成本

由于不断扩展的基础架构需要更强的处理能力以进行7层处理、SSL、压缩等，您只需向威普龙机柜中添加插卡，它将开始自动处理流量。不论您是在使用一个插卡还是四个，威普龙都仍是一个设备，其管理成本保持不变。威普龙通过卸载服务器和整合设备，可帮助您简化网络，从而节约数据中心的管理成本及电力、空间和冷却成本。

威普龙的极高性能和可扩展性有助于减少应用交付控制器的数量，甚至是交付最高要求的应用所需的应用交付控制器的数量。通过卸载计算密集的处理，威普龙可大幅度减少所需的应用服务器的数量。

- BIG-IP WebAccelerator-Web应用加速器

F5的WebAccelerator是一款高级Web应用交付解决方案产品，可提供一系列智能技术，以解决影响用户性能的浏览器、Web应用平台和广域网延迟相关问题。

凭借F5的智能浏览器参考(IBR)特性，WebAccelerator可将许多Web应用、门户应用、CRM应用及协作应用的用户端性能提升高达10倍，这些应用包括MS Sharepoint、Oracle Portal、MS Outlook Web Access、Siebel、Hyperion、Peoplesoft、Plumtree、SAP，以及其它定制Web应用。

- BIG-IP ASM(Application Security Manager)-Web应用防火墙

ASM是一款Web应用防火墙，提供了完善的前瞻性应用层安全保护，能够有效抵御传统防火墙和其它类型安全设备不能检测或预防的安全隐患。

ASM与其它入侵检测和防护设备的区别在于，它采用了一种积极的安全模型，能够筛选出潜在的安全威胁。消极的安全模型通常根据已知的威胁列表，对进入的流量进行筛选。与此不同，ASM采用了“crawler”技术来搜索应用并创建一个允许进入规则集或策略列表。这些策略用于筛选所有直接到此应用的流量，并拒收任何与策略不符的流量。

这一方法的优势在于，它能够识别并阻止一些“零时差(zero day)”攻击。此类新病毒一般不存在现有的配置文件，但经证明会给企业带来重大损失。

- F5 Acopia ARX智能文件虚拟化

F5 Acopia ARX设备是具有高性能、高可用性的智能文件虚拟化系统，能够大幅度地简化文件存储管理。

使用F5 Acopia ARX设备，您可以将智能文件虚拟化引入到文件存储基础架构中，消除与存储管理有关的所有障碍并自动完成许多存储管理任务，从而突破这些限制和约束。这将大幅度地帮您降低成本、提高企业灵活性和业务效率。

- Enterprise Manager——企业管理器

F5硬件型企业管理器使您可以集中管理网络中的所有F5设备。借助企业管理器，您可以:

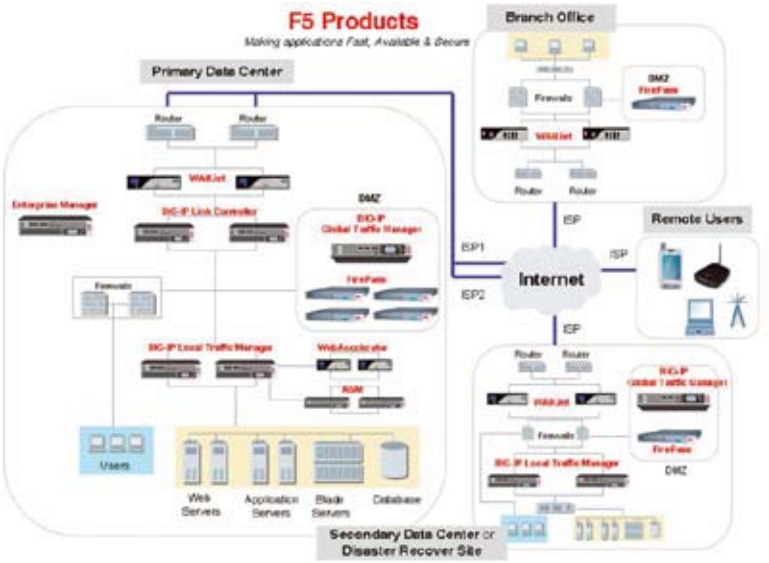
- 针对应急计划存档设备配置
- 对新设备作集中、远程配置，无需到现场
- 降低设备管理的人工成本
- 轻松、快速地部署软件升级与安全补丁

企业管理器产品支持所有F5 TMOS设备。这使用户在单个界面即可完成所有关键设备管理功能，从而减少单台设备管理所需的时间。

- iControl——免费的应用开发接口

F5产品包括一个称为iControl的开放式API、以及一种基于标准的语言，从而使得F5产品能够在相互之间、以及与其它网络设备和应用进行通信。iControl允许用户创建一种“可识别应用”的网络。在这一网络中，应用能够自动预测不断变化的网络条件，并相应地做出响应和调整。通过进行这一通信，它能够消除应用和流量管理设备之间的手动干预。从而企业将无需耗费技术人员大量的宝贵时间来进行服务器维护等日常工作，并能够自动完成诸多当前仍需要手动干预的工作。

2. ADN各元素在企业网络中的部署建议



- 链路接入部分

※ 部署BIG-IP LinkCtroller

选择两个或两个以上的不同ISP运营商，作为企业对Internet的出口，并在Internet出口处部署BIG-IP LinkCtroller，由链路控制器提供智能选路功能。即可避免因单条Internet链路故障等问题造成的Internet故障，又可以解决各ISP运营商之间因为网间路由产生的访问瓶颈所造成的应用访问缓慢。

※ 部署WANJet

如果企业的分支机构或合作伙伴在远程访问总部的应用数据时出现大量延迟，可以在访问端及总部同时部署WANJet广域加速产品。WANJet可对文件传输、电子邮件、客户端－服务器应用、数据复制及其它应用进行加速，在广域网中实现局域网一样的应用性能。

※ 部署FirePass

借助FirePass强大的SSL VPN功能，企业将能够支持在家办公或在路上移动办公的员工，使用任何支持Web的设备(如PDA，手机等)，通过任意接入网络随时随地安全地远程访问网络资源。

※ 部署SAM安全接入管理器

BIG-IP安全接入管理器提供了从所有接入网络对企业应用的安全连接，包括远程LAN、内部LAN以及公共网和内部无线网。这个灵活、易于管理、高性能的平台采用SSL隧道技术提供从任何位置和任何客户端设备对任何用户的安全接入。

※ 部署BIP-IP Global traffic management

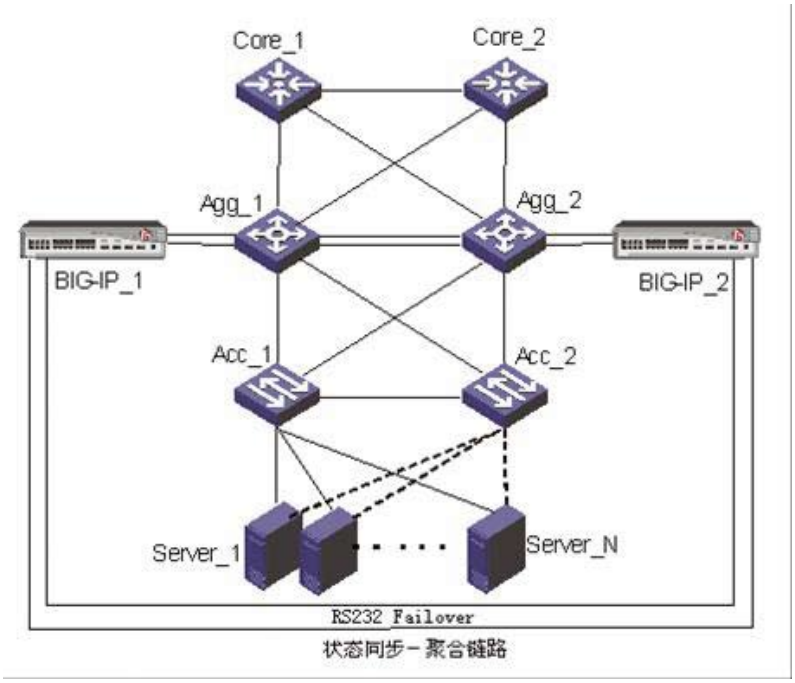
一旦企业建立灾备中心并部署了BIP-IP Global traffic management后，当主中心的IDC出现站点级别的重大事故时，

BIG-IP广域流量管理器可以智能将用户的请求导向备份中心，及时恢复业务。

BIG-IP广域流量管理器可以为运行于多个散布的数据中心的应用提供极高的可用性、最出色的性能和集中式管理。

- 应用前端

※ 部署BIG-IP Local traffic management



在企业原有应用服务器前端的核心交换机位置旁路接入两台BIG-IP本地流量控制器(工作在冗余状态下)，并建议与交换机配合采用Tag vlan的方式将不同的应用系统划分在不同的vlan区间内，确保灵活的扩展性且便于管理。

在部署BIG-IP本地流量控制器之后，可通过BIG-IP强大的性能优化，负载均衡，应用状态监控，应用安全过滤等功能，确保应用的安全交付。

※ 部署WebAccelerator-Web应用加速器

F5的WebAccelerator是一款高级Web应用交付解决方案产品，可提供一系列智能技术，以解决影响用户性能的浏览器、Web应用平台和广域网延迟相关问题。

凭借F5的智能浏览器参考(IBR)特性，WebAccelerator可将许多Web应用、门户应用、CRM应用及协作应用的用户端性能提升高达10倍，这些应用包括MS Sharepoint、Oracle Portal、MS Outlook Web Access、Siebel、Hyperion、Peoplesoft、Plumtree、SAP，以及其它定制Web应用。

注: WebAccelerator可以作为BIG-IP本地流量控制器中一个软件模块使用。

※ ASM-Web应用防火墙

ASM是一款应用防火墙，提供了完善的前瞻性应用层安全保护，能够有效抵御传统防火墙和其它类型安全设备不能检测或预防的安全隐患。

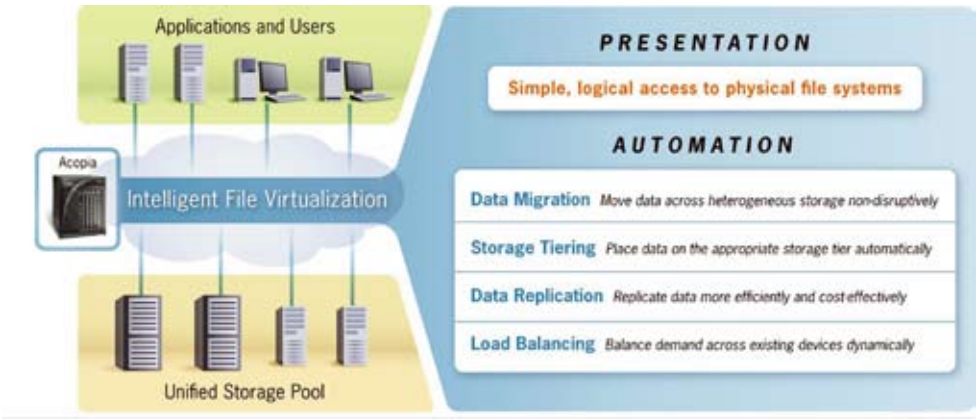
ASM与其它入侵检测和防护设备的区别在于，它采用了一种积极的安全模型，能够筛选出潜在的安全威胁。消极的安全模型通常根据已知的威胁列表，对进入的流量进行筛选。与此不同，ASM采用了“crawler”技术来搜索应用并创建一个允许进入规则集或策略列表。这些策略用于筛选所有直接到此应用的流量，并拒收任何与策略不符的流量。

这一方法的优势在于，它能够识别并阻止一些“零时差 (zero day) ”攻击。此类新病毒一般不存在现有的配置文件，但经证明会给企业带来重大损失。

注: ASM可以作为BIG-IP本地流量控制器中一个软件模块使用。

- 文件存储服务器前端

※ 部署F5 Acopia ARX智能文件虚拟化设备



摆脱传统文件存储基础架构限制的关键在于是否能够消除客户端与存储资源之间的静态映射，允许改变存储资源的构成以及数据在资源之间自由移动，但不影响客户端访问数据。智能文件虚拟化完全做到了这一点。它为网络提供了一个智能层，能够将逻辑访问文件从那些文件的物理位置中分离出来。有了这一智能层，数据便可以自由迁移，存储资源也可以自由更改，而且也不会像先前那样因这些操作而发生中断。

这个智能文件虚拟化层为企业环境带来了一些好处:

※ 简化访问。可以将数百或数千个客户端到资源的映射整合缩小到一个更易于管理的数字。更为重要的是，这些逻辑映射无需更改 – 它们是永久不变的。可以在不要求客户端重新配置的情况下执行供应、整合和迁移等存储管理任务。

※ 增加灵活性。数据不再受物理存储资源的约束，它们可以随意移动，并且不会影响客户端访问该数据。

※ 优化利用率。可以在现有系统间透明地共享富余的容量，而不会影响客户端，最大限度利用现有的资源。

※ 自由选择。文件虚拟化提供“选择自由”，使得多供应商设备组成的异构文件存储基础架构协作。可以灵活地利用和更换文件存储供应商，以满足长期的业务和IT要求。消除许多影响基础架构改变的内在障碍，有助于减少供应商限制。

智能文件虚拟化使企业能够更加有效地访问、管理和优化文件存储资源。

一旦企业建立灾备中心并部署了BIP-IP Global traffic management后，当主中心的IDC出现站点级别的重大事故时，BIG-IP广域流量管理器可以智能将用户的请求导向备份中心，及时恢复业务。

BIG-IP广域流量管理器可以为运行于多个散布的数据中心的应用提供极高的可用性、最出色的性能和集中式管理。

3. ADN架构让企业应用发布高枕无忧

- 保证应用的可用性

基于TMOS的实时健康检查功能提供了复杂的监视器来检查Internet链路、各类安全网关应，应用和内容的可用性，其中包括支持许多应用的专用监视器 (包括各种应用服务器、SQL、SIP、LDAP和XML/SOAP等) 以及用以检查内容和模拟应用呼叫的监视器。同时，它还能前瞻性地检查并对任何服务器或应用错误即时作出响应，从而帮助企业在降低系统负载的同时，获得出色的可靠性。

- 提升应用的访问速度

基于TMOS的应用加速功能，可以通过数据压缩，HTTP压缩，静态/动态内容Cache，连接复用，IE多并发访问，SSL加速等混合技术的使用，缓解服务器的压力，改善所有广域网用户的服务性能和可靠性，提升用户的访问速度。

- 保证数据在基于WEB方式传送时的数据安全

基于TMOS的SSL加解密技术，使得银行帐号，电子定单，财务数据等关键的应用数据都将通过密文在基于WEB的网络上进行传递。

作为领先的SSL加速解决方案，BIG-IP提供了惊人的SSL处理扩充性，持续SSL吞吐率可达6Gbs。通过加速批量加密和设置加密，企业可使用更安全的加密方法将其全部通信移植到SSL上，同时不会对应用性能带来任何影响。

- 显著提升安全防御能力

基于TMOS的安全防范攻能，不仅可以阻止攻击，同时还可以为合法用户提供即时服务。从这两方面来看，BIG-IP均提供了一整套安全服务，在提高网络和应用的安全性方面扮演了日益重要的角色。从增强网络和协议级安全性到过滤应用攻击，BIG-IP都可以部署在关键网关上，来出色的保护您的珍贵资源：运行业务的应用。

灵活的安全网关负载均衡功能，可以使各安全网关设备工作在集群模式下，可以在不损失安全的前提下提高各安全网前的处理性能。

- 提供便捷的应用访问方式

FirePass SSL VPN设备提供了一种通过标准网络浏览器，到公司应用和数据的安全访问能力。无论在家中或是在路上，FirePass出色的性能、可扩展性、易用性以及安全性都可帮助您提高工作效率和确保公司数据的安全性。

BIGIP SAM安全接入管理器为用户提供了一个更具有针对性的安全接入解决方案，通过基于SSL技术建立VPN网络通道，实现端到端的远程安全接入。

- 建立容灾中心，避免站点故障

凭借BIG-IP广域流量控制器为多个数据中心和分布式站点提供智能流量导向的技术，为企业带来最大投资回报、最高可用性和最佳客户端体验。

- 统一管理，应用维护的真正体现

作为以面向应用发布为设计核心的ADN架构中，TMOS可以弥补企业在应用层监控的不足，利用TMOS的实时应用统计功能，管理员可以实时了解各关键应用系统的工作状态及性能情况，使管理员对各应用的运行情况了如指掌。

- 灵活的扩展架构

ADN的使用为企业提供了最为灵活的扩展架构，网络/应用需要扩展时，在ADN的架构下，企业可以方便将服务器、安全网关等加入到网络中，以此提升性能，同时由于负载均衡功能的存在，新旧设备可以同时工作，快速回收企业的投资成本。

- 简化的部署方式

F5提供了ADN架构中几乎所有的关键技术，所有企业需要的应用优化、可用性以及安全性，都被集成在一个统一的架构之下。并且各关键产品均可以同时运行在一台统一的基于强大硬件支持的应用交换机平台之上，减化了设备数量。

灵活的产品添加方式，无论是新的网络架构还是在原有网络中进行改造，都将避免较大的网络改动。

- 节省运维成本

方案中使用的大量新兴的如负载均衡，流量控制，连接优化等多种多样的复杂技术，网管人员可以通过统一的管理界面进行配置，详细的培训课程，可以使企业的技术人员尽快掌握这些技术。大大节省了企业的运维投入成本。同时，F5公司建立的完善技术服务支持体系，可以7×24小时为用户提供技术支持，及时解决突发问题，将企业的损失降到最低。

总结

F5的ADN解决方案，可以确保用户获得:

- 确保数据中心和应用系统达到99.999%的高可用性
- 服务器资源消耗降低80%
- 互联网络带宽节省75%
- 客户响应速度提高3-7倍
- 数据传输速度提升10倍
- 网络层到应用层的全方位安全保障
- 简化文件存储管理方式，减低成本，增加生产力

THE WORLD RUNS BETTER WITH F5

F5北京代表处
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
Tel: 010–59234000
Fax: 010–59234100

F5 上海代表处
上海市虹桥路3号港汇中心2座27 10室
邮编：200030
Tel: 021– 61132588
Fax: 021–61132599

F5广州代表处
广州市环市东路368号,花园酒店花园大厦1035室
邮编：510064
Tel: 020–83884169
Fax: 020–83883897