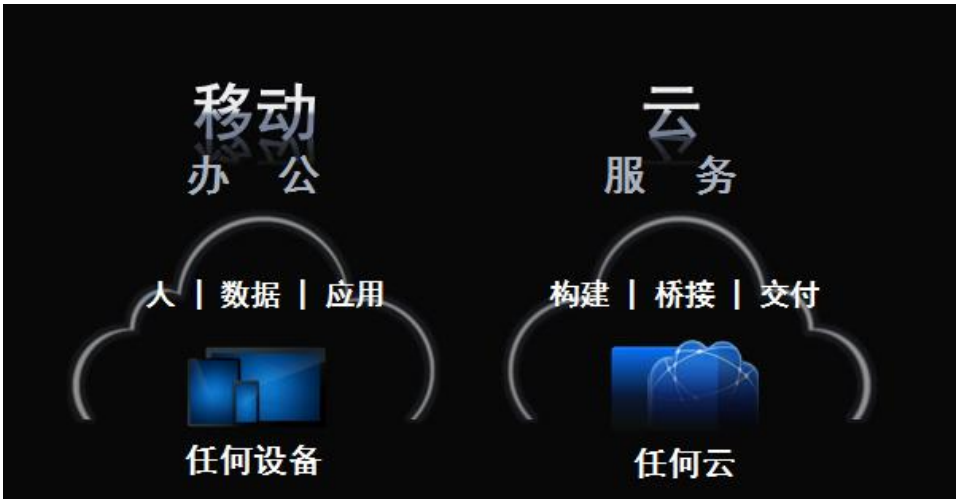
目 录

1 企业 IT 架构发展综述

随着后 PC 时代的来临，传统的以 PC 为主导的访问及其计算在近几年逐渐被各种智能终端所取代，通过智能终端作为应用的前端访问平台来访问后端数据中心上发布的各种应用变得越来越普遍和流行。市场调研分析报告指出用户 PC 的增长将会呈逐年下降趋势。PC 时代逐渐过渡到云时代，在此之际，Citrix 解决方案将企业 IT 架构划分为前端个人云，后端云计算中心，通过这两朵云来实现企业的灵活的 IT 架构发展，满足业务访问需求。

如下图所示



----关于云数据中心的那点事

古人云“天下大事，合久必分分久必合”。从 IT 发展至今，数据中心的发展总共经历的三个阶段，阶段一，早期大型机分时复用，用户通过共享机器的方式来使用数据中心部署的大型机，访问系统进行业务处理；阶段二，随着一家伟大公司 MicroSoft 的出现，桌面操作系统设计的人性化和简单易用，使得个人 PC 开始广泛普及并被使用，这使得人们可以通过自己的电脑进行办公娱乐；至此，我们可以看到用户在也不在需要依赖数据中心提供的机器来进行访问，这是数据中心分的演变。

另一方面，在 90 年代初中期，在当时美国总统克林顿的首肯和大力支持下，以美国为主导的互联网建设在全球得以快速发展，这其中包括跨国海底光缆的大量铺设，Internet 协议的研发。基础建设的大力发展为今后企业业务 Web 化提供了坚实的平台基础，使得人与人之间沟通变得更加快捷有效，正如托马

斯·弗里德曼所写的一样，“世界是平的”。Web 2.0 时代的到来，传统的个人 PC 上的独立应用已经无法满足人们的使用需求，人们需要一种新的应用模式来进行资源共享，协同办公和生活娱乐。B/S 架构的交互式应用被大量发布并使用。这其中典型的代表如国内的微信，微博，国外的 facebook, Instagram 等各种社交应用，这些在线应用无不都是大数据访问的代表。业务的 Web 化，数据的多样化，规模化，数据中心又重新走上了整合的道路，我们需要一种灵捷的，便于管理维护，可动态按需扩展的安全的数据中心架构来为用户提供服务，其实这就是我们今天所看到的企业建设的公有云，私有云，混合云。

----移动办公，让世界触手可及

21 世纪，一个伟大人物的出现，史蒂夫.乔布斯，如雷贯耳的名字，彻底颠覆了人们传统的使用 PC 的习惯。iPhone 的问世，iPad 的发布，颠覆了消费者们传统的使用习惯，为全世界的人们带来了全新的移动设备使用体验，人性化的操作系统，丰富的使用功能，使之瞬间风靡全球。大屏幕的出现让用户的使用体验得到很大的提升。App Store 的运营模式，使得针对 IOS 的原生应用被大量开发，从办公到娱乐全面覆盖。随后，谷歌安卓操作系统的发布，各种智能手机如雨后春笋般的出现，如 SangSung，HTC 等大家耳熟能详的智能手机。移动设备的智能化已经是大事所趋，这都极大的推动了移动办公的需求，企业员工希望使用自己喜爱和熟悉的设备来进行办公。BYOD 于是开始在企业中广泛流行起来。企业如何来满足员工移动办公的需求，或者说企业如何构建一个基于 BYO 的业务模式这都将极大的提高企业的生产率。

----Citrix 解决方案，沟通，联天下

Citrix 是首个提出个人云的厂商，通过 Citrix 个人云解决方案（其中 Citrix Receiver 是一款客户端，它可以安装到当前任何的智能终端上，支持各种移动 OS，实现 100%的兼容。通过它来访问 Citrix 部署在数据中心的虚拟化应用；GoTo 系列协同办公平台帮助企业员工轻松实现在线会议，在线协助；Sharefile 实现数据共享）来使用户随时随地的通过各种移动终端设备来实现协同办公，安全的访问企业应用和数据，通过个人云解决方案，将应用和数据随时跟员工移动变为可能；

与此同时，Citrix 在企业数据中心端通过部署各种虚拟化综合解决方案（服务器虚拟化，桌面/应用虚拟化，企业应用商店，云管理平台）来帮助企业架构适合企业发展的数据中心。

Citrix 提出的个人云及其云数据中心完全符合当前企业 IT 架构的发展模式。通过 Citrix 提供的丰富的产品，帮助企业在云中构建服务，并且交付到任何设备上。

2 Citrix Netscaler 企业解决方案

在上文中我们简要的介绍了 Citrix 的云架构解决方案，Citrix 提供了从前端到后端完整的解决方案来帮助我们的企业构建服务。其中 Netscaler 作为一个最为重要的组成部分可以帮助企业更好地发布和保护应用以及灵活的扩展数据中心规模。

2.1 统一应用接入点

Netscaler 部署在数据中心，作为后端应用的统一发布点，让用户在 Internet 上通过 Netscale 提供的一个**安全,高速,可用**的通道来访问数据中心中发布的任何业务，无论是 SaaS，还是企业搭建的应用（如中间件架构的应用），甚至是虚拟化应用。

2.2 数据中心动态扩展

随着企业规模的增长，单数据中心也许无法满足业务发展需求，无论是从性能扩展上还是高可用上。Netscaler 帮助企业将数据中心无缝扩展到更多的数据中心，又或是扩展到公有云中，如 Amazon。弹性的扩展数据中心的计算能力，降低企业的 TCO。

2.3 Netscaler 应用交付网络综述

传统的数据网络主要关注的是网络的互连互通，而各种新兴繁杂的网络应用，关注的则是业务逻辑和功能。如何将二者铆合在一起呢？目前在业界中，最为流行，也是最为关注网络和应用的新兴概念就是应用交付网络（Application Delivery Networking，ADN）的理念。

对于很多企业而言，当千辛万苦完成数据大集中后，另一个两难境地随之而来——应用系统不断增多，分支机构不断增加，需要维护的客户端也呈几何级数攀升，IT 架构变得分外复杂。于是，一方面急需快速高效部署各种新的应用系统，以保持业务优势；一方面又要确保 IT 架构的易管理性，以及降低 IT 投资的总体拥有成本。这时，就是建立应用交付网络的最佳时机。

安全：目前业界已经达成共识，网络安全对于网络应用的保障是至关重要的环节。而在应用交付网络中强调的是应用的安全，无论身居何处，应用交付网络可以预先提供全面的防护措施，以避免那些不正当的恶意访问和攻击。

快速及优化：应用交付网络可以优化用户的网络应用，使网络达到更快的速度并能减少资源消耗。无论是在全球的某个角落或者公司总部使用笔记本进行连接，应用交付网络都可以确保应用程序的高速运行。

企业规模的扩大和用户群体的全球化，都导致了关键业务访问远程化、窄带化。和最初的应用发布不同，越来越多的应用访问是通过上千公里的广域网访问而非最初的局域网访问。企业应用的大集中趋势，在带来管理、维护和总拥有成本降低的优势的同时，也造成了远程访问所带来的速度降低。应用内容的丰富性也进一步加剧了在广域网上的带宽消耗和资源占用。

因此，在一个完善的应用交付网络设计中，应当关注的一个重点就是如何提高广域网用户的访问速度，实现就近访问、更小的带宽占用和应用访问速度的提升。

高可用性和应用可视化：应用交付网络所提供的解决方案保证网络应用的持久性与可靠性，在基于安全、正常运行、高可靠基础上允许用户强有力并灵活地来设定各种应用的优先权，从而保证了各种网络应用的高可用性。

全球化经济正在逐步加强，用户的使用习惯和时区所带来的访问差异性，必然加大了应用系统的高可用性需求。大量的企业应用从最初的 5X8 的服务模式，已经提高到了 7X24 小时不间断业务模式。仅仅靠人员的增加已经完全不能满足应用的高可用性需求。

因此，在一个完善的应用交付网络设计中，应该充分考虑到应用的高可用性需求，通过自动、完善的切换手段，保证业务的不间断性和持续性。

同时应用的多样性和复杂性对于用户的管理者来说也是非常棘手的问题，当一套系统出现了性能问题，访问速度问题时，对于问题查找和排除都将变得非常困难。

从传统的四层负载均衡在向应用交付网络演进的过程中，共经历了 3 代的发展更迭来满足整个业务交付的需求变化。

2.3.1 第一代负载均衡产品

第一代产品特点是基于第 4 层（TCP）的负载平衡器。随着互联网的迅猛发展，受欢迎的网站仅靠一个 Web 服务器无法承载快速增加的流量负载。第一代第 4 层负载平衡器可在多个服务器上分配来自客户的连接负载。这些第一代产品能够将多个单独服务器作为一个虚拟的大型服务器有效呈现给外界。它们的方法是：创建一个虚拟互联网协议(IP)地址，这个地址向路由器和浏览器广告自己，然后将浏览器的数据包转发到带真实 IP 地址的多个真实服务器中。这些设备名为第 4 层 SLB，因为它们依赖数据包的 IP 地址和 TCP 端口等简单的 TCP/IP 信息做出负载平衡决策。

2.3.2 第二代负载均衡产品

第二代产品特点是简单的 L4－L7 服务器负载均衡。第二代负载平衡器一开始名为 Web 交换机。由于它们还提供第 4 层负载平衡功能，因此市场将其归为一类，统称第 4 层-第 7 层负载平衡器或流量管理设备。这些附加名称旨在说明这些设备不仅关注通过第 4 层信息来转发流量，而且还具有一定程度的应用层感知能力，但是智能度不高。第二代 SLB 通常提供精心定制的硬件或基于 ASIC 的独特架构，用于提供高速智能数据包处理性能。

这些设备也可基于 HTTP 报头中的一些信息，提供特殊的负载均衡决策。这是一个重要进步，使第 7 层 SLB 能够将单个最终用户与其使用的服务器“关联在一起”。第二代 SLB 还实现了对防火墙、网桥和不带 IP 地址的设备的负载平衡功能，从而添加了粒度更细的第 4 层控制能力。但第 4 层-第 7 层 SLB 的基础版本与第 4 层 SLB 的基础版本极其相似，其第 7 层功能也相对简单，而且真正让第 7 层功能有效展开，实际上它的数据处理也是非常困难的。往往 L7 层功能的启动会严重影响流量的处理能力。

由于 Web-Base 的应用在此时已成为主流的应用模式，而且绝大多数负载均衡设备上承载的 90％应用流量为 HTTP 应用，市场对负载均衡设备解决因“Web 化”所带来的新问题又基于厚望。因为此时传统的数据中心为保障 HTTP 应用安全、可用和高性能，在 Web 服务器前部署了众多繁杂的产品，如服务器负载均

衡器（SLB），SSL 加速器，Web 缓存，应用防火墙以及更多的 Web 服务器来应对这些挑战。这又使得 Web 数据中心的架构变的更加复杂，设备互操作性存在隐患，而且投资不断增加，这都是目前用户所不愿意看到的，即便如此，可能性能方面依然不尽人意。因此如何彻底解决 Web-Based 应用的性能问题和安全问题成为一个热点话题。

近 2 年，第二代负载均衡的市场已经出现严重滑坡，并最终被提供更高级功能（包括 SLB 功能）的规模更大的新市场所取代。由此进入第三代负载均衡设备时期，业界将新一代具有安全、优化功能的负载均衡设备称为——应用交付控制器（ADC Application Deliver Controller），它们显著的特征真正降低服务器群集上的工作负载，最大限度的发挥 Web 和应用服务器的处理性能，而不只是简单的均衡负载和转发。

2.3.3 第三代负载均衡产品

最新一代负载均衡设备已经基本放弃负载均衡的称谓，而应用交付的概念日益增强，思杰的目标是通过新一代的技术平台产品为企业建立新兴的数据中心。思杰 NetScaler Web 应用交付平台能够在全面考虑用户、会话和业务内容上下文的情况下高效处理应用数据，同时提供对 Web 服务器的减负功能，提高服务器在 HTTP 处理上的效率。虽然经历这些复杂的数据处理过程，其性能及吞吐量仍达到网络设备线速高吞吐能力，而集成的第 4 层-第 7 层流量管理功能只是该平台的一个特性。

由此可见，思杰 NetScaler Web 应用交付平台是旨在适应新型数据中心的产品，它在简化数据中心整体架构的同时提供了全面有效的优化功能，并且这些产品的性能不会随功能的添加而降级。它避免了集成多个厂商或多种产品的复杂程度，同时也避免了设备之间相互功能对彼此性能方面的影响。而且思杰 NetScaler 产品采用真正的平台的方法允许对用户的 HTTP 请求进行优化整合，代替传统产品进行简单转发的功能，更有效的实现了负载均衡和对后台服务器的减负作用。除此之外管理员仅通过简单的操作就可以实现功能的启动和关闭，简化了管理和维护方面的复杂性。

2.4 应用交付网络在各个环节的作用

针对应用交付的各个环节中的薄弱点，应用交付网络提供了端到端的解决方案。

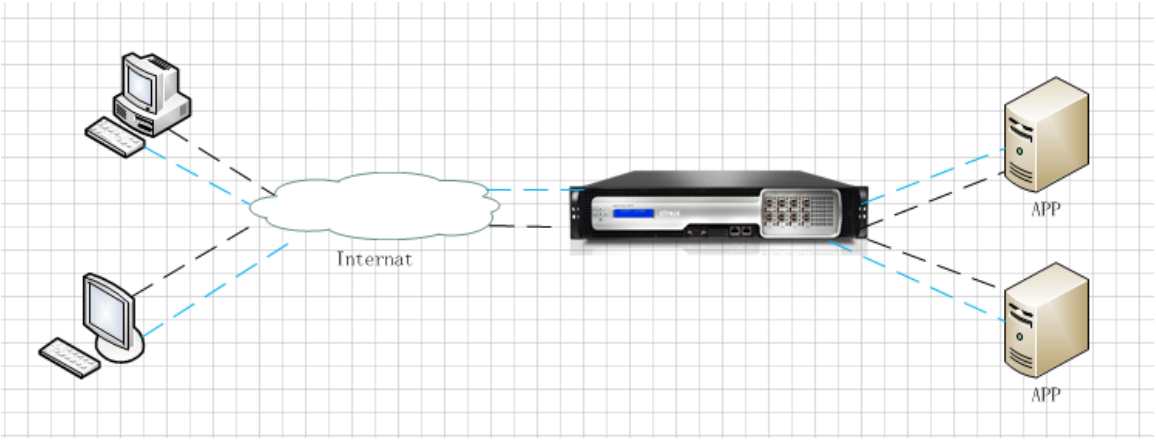
- 服务器整合：通过使用本地负载均衡、应用优化设备，实现服务器的高可用性、高安全性和可扩充性。
- 安全攻击：通过网络层安全防护、应用层安全防护和传输通道加密技术，提高系统的整体安全性。
- 用户分散加剧：通过广域网用户引导、多链路用户引导等技术，引导用户选择最佳的数据中心，通过最佳的链路到达应用服务器。
- SOA 建设：通过多协议、多平台的支持，对应用中的各种协议流量进行分析，实现精确引导和应用分布。
- 应用系统复杂性增大：通过对应用系统的深层次识别和各种应用加速技术，提高应用系统的访问效率和响应速度。
- 终端种类增加：应用交付网络通过对各种终端的识别，根据终端的类型对用户进行引导，并通过对各种终端接入设备的支持。增强系统的容错特性和安全性，优化各类终端的访问速度和效率。

3 思杰 NetScaler 产品优势

Citrix NetScaler 应用交付解决方案将传统数据中心产品的各项特性与功能整合至一个单独的网络设施中，其中包括负载均衡、缓存、SSL 加速、攻击防御和 SSL VPN 等。这一系列的精心设计旨在最大限度地提升应用性能。下文将分别阐述部分思杰 NetScaler 产品的技术优势。

3.1 先进的“请求交换”核心技术

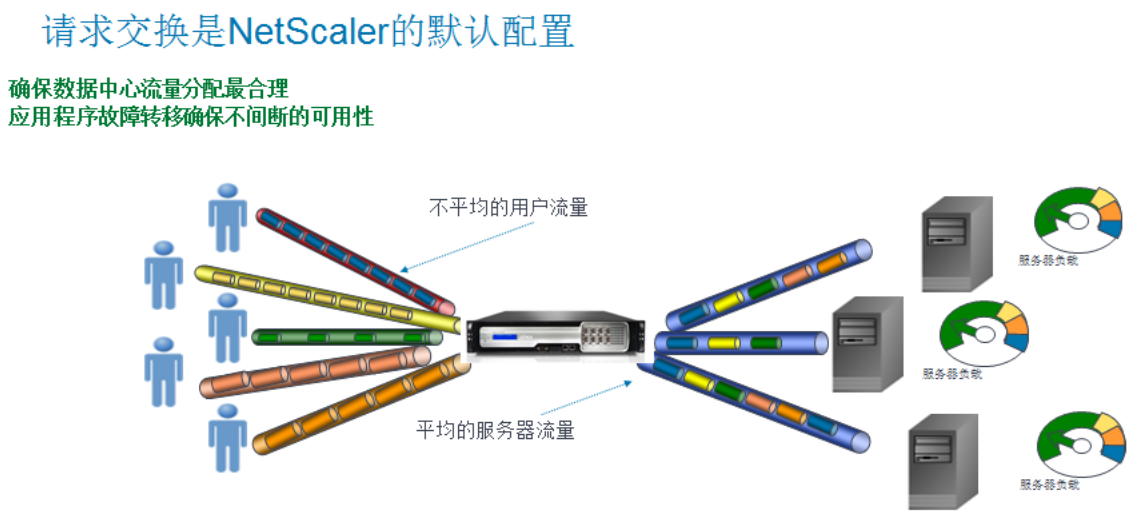
NetScaler 拥有专利的请求交换技术是得到业界广泛认同的，传统负载均衡技术向新一代流量管理技术演进的方向。NetScaler 打破了存在于连接和请求之间的关系，并在请求层检测所有的流量，请求交换提供了高性能的，安全的，可扩展的应用层服务。



请求交换技术的核心是一个新的运行范例，正是在这之上，NetScaler 系统分开管理每一客户端连接以及服务器端连接。因为 NetScaler 系统是每个客户端以及服务器端连接的终点，而不是简单的传输连接，所以它能提供以前其他流量管理系统所无法达到的许多加速和优化技术。因为请求交换引擎被专门设计来在请求层检测流量，所以负载均衡以及内容交换可以非常高效的完成。策略以及过滤可以在进入的请求上被应用并且丝毫不影响性能。成熟的负载均衡算法以及健康检查机制保证了服务的均衡性以及持续可靠性。先进的加速和优化技术在降低服务器负载的同时更快的把内容传送给了最终用户。

3.2 新一代的负载均衡技术

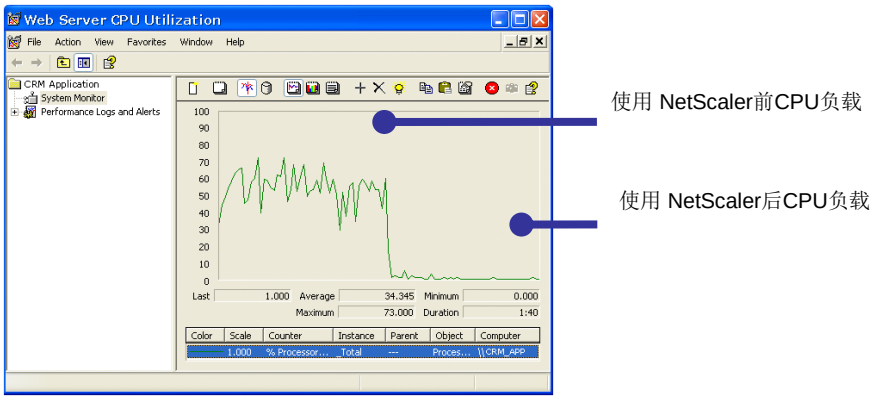
与传统负载均衡设备不同，NetScaler 基于应用请求而不是网络连接进行负载均衡，**最终达到的是服务器负载的均衡而不是服务器连接数量的平衡。**真正实现用户对负载均衡效果的预期。



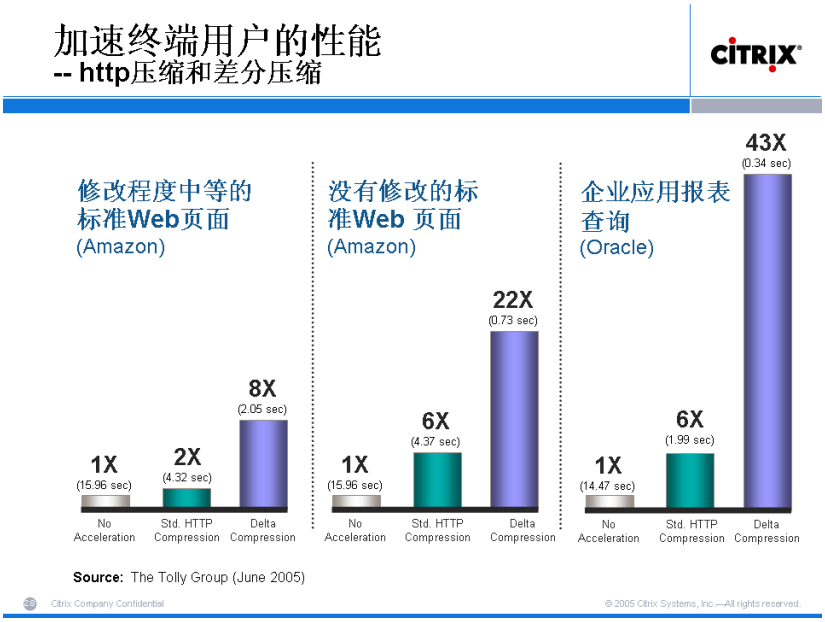
3.3 提高应用性能 2-15 倍

利用 Citrix 独有的请求交换技术，NetScaler 在提供负载均衡的同时，对应用进行优化与加速。

连接复用和 TCP 卸载：NetScaler 代替服务器终结客户端 TCP 连接，而且多个客户端请求被复用在少量服务器端连接内发送给应用系统。使用 NetScaler 进行负载均衡的服务器上的连接数比通过传统负载均衡设备均衡的服务器上的连接数降低几十至几百倍，服务器 CPU 和内存消耗大幅度降低，应用响应速度提高 1-5 倍。



AppCompress 压缩技术：利用 NetScaler 内置的压缩功能，可以将广域网传输数据量减少 3-50 倍，提高应用的响应速度。



此外，NetScaler 还提供 AppCache 高速内存缓存技术，TCPB 网络优化技术等多项优化功能，通过综合应用上述功能，如果用户使用 NetScaler 作为负载均衡设备，他们就可以在获得负载均衡功能的同时，获得 2-15 倍的应用速度提升。

3.4 为应用提供最佳的安全性

NetScaler 利用先进的请求交换技术，可以有效地抵御 L4 的 DoS/DDoS 攻击和各种已知与未来的 L7 攻击。NetScaler 基于请求交换技术的抗攻击能力是采用 Syn Cookie/Delay binding 防御方式的传统负载均衡交换机的 10 倍以

上。

3.5 业界最全面的解决方案

Citrix NetScaler 系统把传统数据中心的各种纷繁产品的功能，例如：负载均衡，缓存，压缩，SSL 加速，攻击保护，SSL VPN 等，融合进了单一的产品中，并利用其专利的“请求交换”技术，从底层整合各种功能，以极高的效率提升应用的性能、可靠性和安全性。

- 通过 L4-L7 层的 SLB 功能和智能的服务器健康检查特性，多数据中心和多链路的容灾保障 100%的应用可用性
- 通过动，静态缓存，压缩以及当前流行的 Speedy，MPTCP 等技术实现 5 倍以上的应用访问加速
- 通过 TCP 连接复用，SSL 卸载等功能来节省平均 60%的服务器资源，对于 Web2.0 这样非常消耗硬件资源的应用这是非常重要的一个特性
- 通过继承的 SSL VPN，Web 应用防火墙，L3-L7 层的安全防护功能保障端到端的访问安全，企业避免信息泄露。

Citrix Netscaler 的完整功能整合并不是简单的功能叠加，简单的功能叠加的产品在使用中很可能会造成系统性能的严重下降从而导致设备成为性能瓶颈。Netscaler 在 OS 层中进行整合优化，同时针对特定的功能芯片做了更好地驱动优化，大量的互联网用户的广泛使用证明了 NS 在面对大流量访问时的高

性能和高稳定性。

3.6 多核并行处理技术（nCore）提高产品性能

Citrix® NetScaler® nCore™技术作为一种高性能的并行处理架构， 可利用多核技术实现有效扩展，以满足要求最为严苛的 Web 应用的需求。要构建能有效利用多核处理器的系统必须考虑以下两个问题： （1）系统如何能够确保所有 CPU 核一直处于工作状态？（2）系统如何消除处理器间的同步损耗？

两者是相辅相成的，消除处理器间的同步损耗让每个处理器可尽可能地实现最佳性能。要了解 NetScaler 如何成功避免同步操作，首先必须掌握 NetScaler 数据包处理引擎的本质特性。

3.6.1 NetScaler 数据包处理引擎

Citrix NetScaler 数据包处理引擎的目的是将数据包从网络中分离出来，执行大量 TCP/IP 处理进程，加速和优化任务，以及执行安全策略。当数据包处理引擎处理完成一组数据包时，便会将回应返回到网络，然后继续处理新的数据包。

NetScaler 数据包处理引擎的高效率使其可在几微秒内完成数据包的处理。NetScaler 超低延迟数据包处理引擎优化了 Web 应用交付和用户体验。利用精心设计的分段数据包处理，数据包处理引擎即可消除数据同步需求。这样一来，单个 CPU 核上运行的单个数据包处理引擎可支持几千兆的吞吐量。

与基于 Linux 的传统产品相比， NetScaler 数据包处理引擎的高效率所带来的影响是非常值得赞赏的。传统的 Linux TCP 堆栈会让数据包在不同层之间传输时进行排队处理，而每一层在接收数据前都会产生大量的数据同步损耗。正因为如此，一些基于 Linux 并结合 ASIC 芯片处理数据交换的产品设计会将这种延迟放大。

值得注意的是，随着 NetScaler 平台的发展，不需要数据同步已变成一个差异化的特征，使得 NetScaler 能够以极高的效率将数据包处理引擎延伸到多个处理器核心。

3.6.2 零共享设计

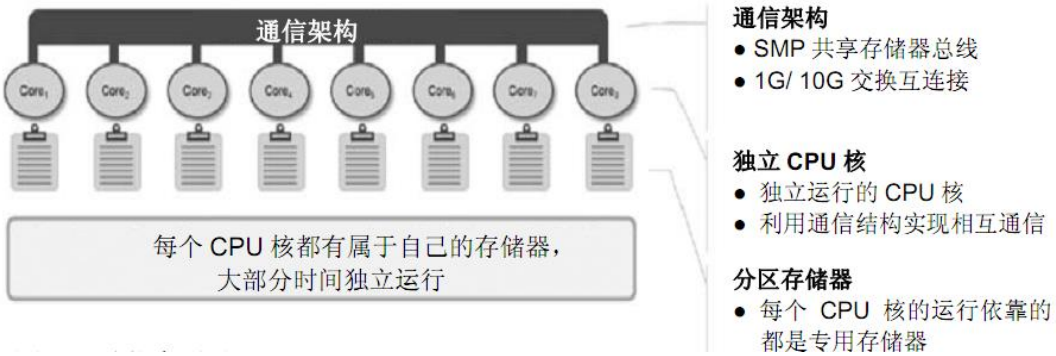
提升性能所面临的共同挑战就是共享。多个组件需要共享数据时，性能就成了问题。零共享有以下几大好处：

1、无同步化开销

2、大幅降低复杂性，从而提高稳定性

3、可更妥善地处理故障，因为组件之间不会互相影响

nCore 架构利用 NetScaler 数据包处理引擎的关键属性实现了零共享设计。



3.6.3 零共享的运作原理

nCore 零共享架构采用了一系列数据包处理引擎，每个引擎都具备完整的 NetScaler 功能，可通过专用存储空间实现应用优化和加速。由于每个数据包处理引擎都可执行所有的功能，因而可完整进行 Web 应用交易，无需借助其它数据包处理引擎的力量。

引擎之间的相互独立让同步不再成为一个问题。同时，资源争夺让数据包处理引擎再也不用相互等候。如此一来，NetScaler 可在极短的延迟时间内实现极高的吞吐量。

数据包处理引擎在每个 CPU 上运行时有两种不同的状态：1）搜寻需要处理的数据包；2）正在处理数据包。每个数据包处理引擎搜寻的是基于硬件的数据包队列中的数据包。为了支持零共享理念，每个数据包处理引擎都有自己的队列，不和其它 CPU 核共享。因为硬件部署是完全对称的，因此，出站数据包也将通过每个处理器的专用队列发送出去。

由于每个数据包处理引擎可利用整个 CPU 核，因此每个 CPU 核与数据包处理引擎之间进行 1 对 1 映射，确保硬件提供的每个可用周期都可得到充分利用。随着系统新增 CPU 核，可大幅提高线性性能，提高平台在将来的可扩展性。

3.6.4 数据包队列中的流量分配方法

在多核 CPU 系统设计中，CPU 核之间分配网络流量有多种方法，常用的三种方法如下：

1、功能并行性

2、将网络接口映射到处理器

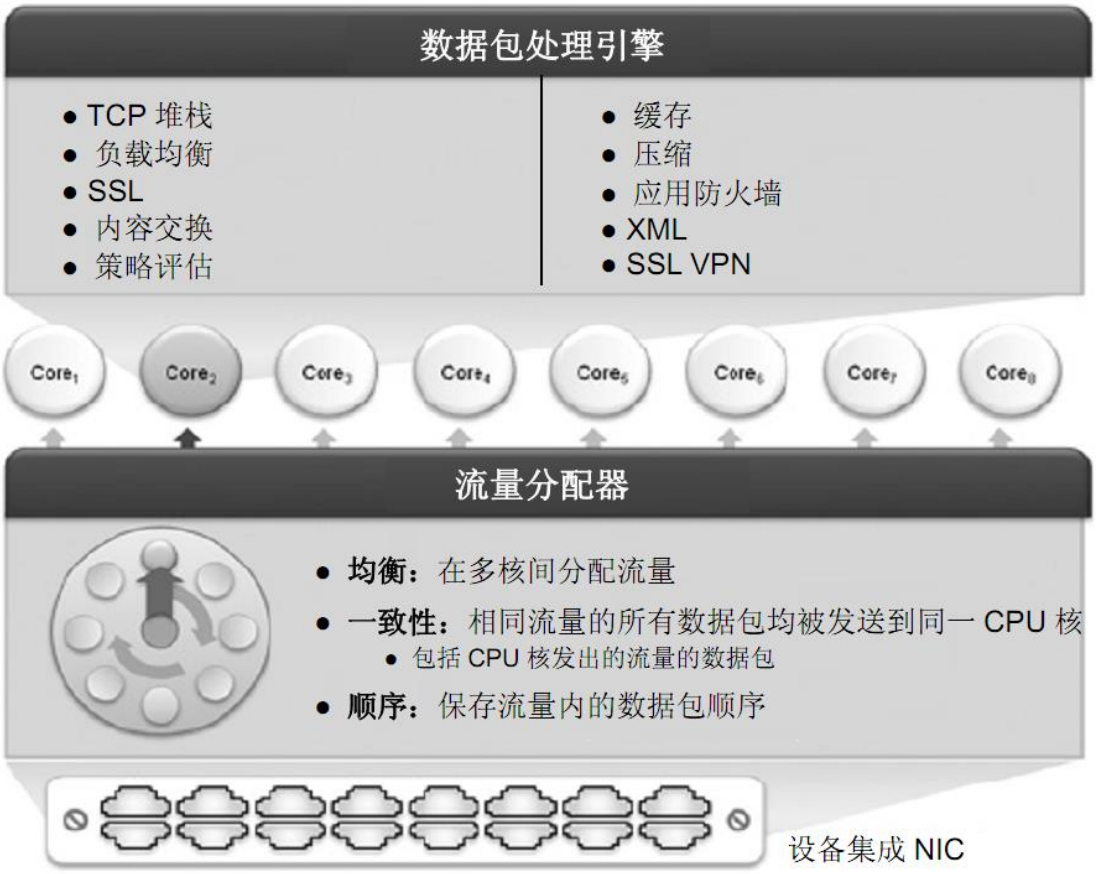
3、单独流量分配

在应用交付领域，功能并行性的典型实现方法是通过分离多核 CPU 之间的任务来实现的。结果，指定 CPU 核只承担相应功能。例如，核 1 专门用于管理网络流量， 核 2 用于处理 TCP/IP， 核 3 用于 7 层 （如 HTTP）处理等等。这在表面上似乎也很合理，因为它将一种功能的峰值从另一种中分离了出来。然而，在现实情况下，这种架构通常会大幅降低 CPU 多核的利用率。例如，如果一个应用要求进行更多的 7 层处理，而不是 SSL 处理，它也不会将未使用的 CPU 资源从 SSL 转移到 7 层处理上。

将网络接口映射到处理器是传统的网络领域方法，这种方法是将物理口连接到指定 CPU 核上。 更新一些方法则是将 IP 地址映射到指定 CPU 核。然而，与功能并行性类似，这也依然无法实现均衡多核 CPU 之间的负载，单个应用就有可能用尽单一 CUP 核的容量，而不能利用其它空闲 CPU 的容量。

经过对功能平行性以及将网络接口映射到处理器这两种方法的评估后 NetScaler nCore 技术决定选择单独流量分配的方法。其实，这种方就是最细粒度的负载共享机制，充分利用了单个数据包处理引擎可执产品的每项功能这一能力，最终实现均衡多核 CPU 之间的负载，确保单个应用或功能不会受制于单个 CPU 核的容量，仍可以使用其它空闲 CPU 的能力。

为了以最高速度实现单独流量分配，必须使用对称的流量分配器。这种特殊的硬件可捕获发送到每个网络接口的数据包，并快速确定由哪个数据包处理引擎入站队列来接收指定的网络流量。由于决策的根据是 TCP/IP 报头信息，因此，分配器必须确保指定流量的数据包会发送到相同的数据包处理引擎。

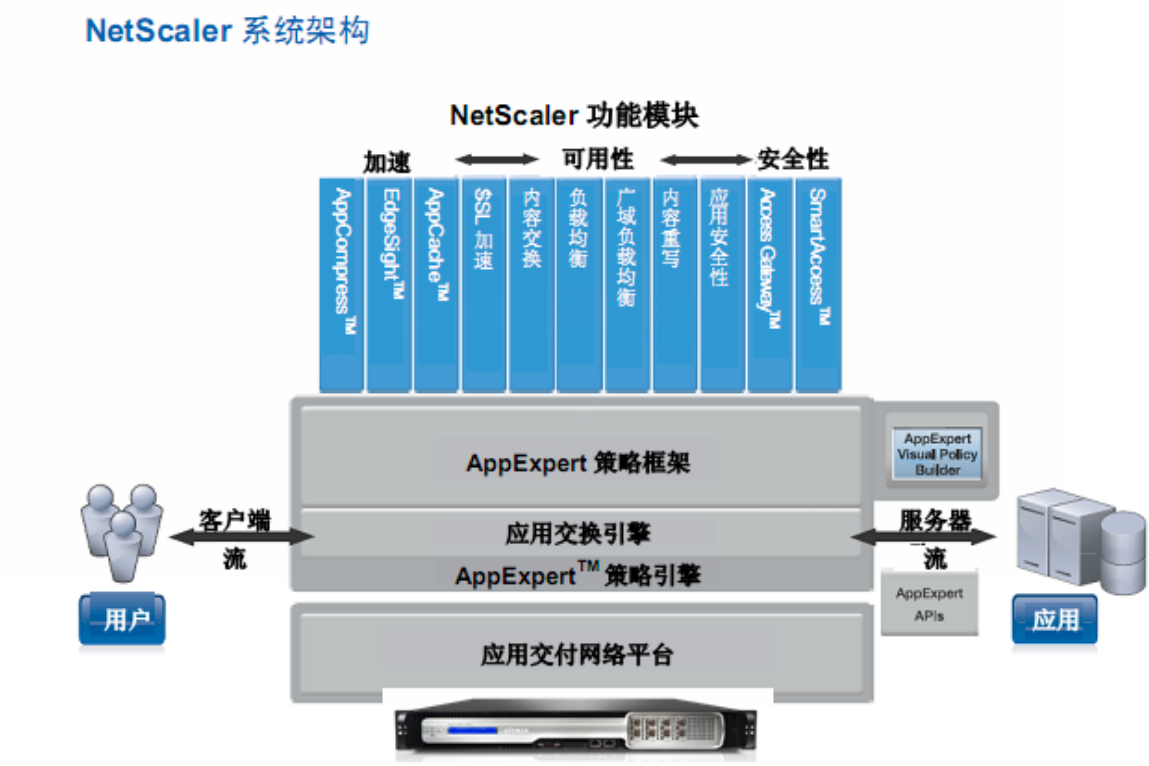


流量分配器使用的算法均衡了所有数据包处理引擎之间的流量分配，从而确保所有数据包处理引擎能支持系统的全部工作负载。在 nCore 架构中，宝贵的处理器资源决不会用于数据同步损耗，也会均衡地分配网络流量。

4 NetScaler 产品体系架构

Citrix NetScaler 是一款智能地分配、优化和保护 Web 应用的 4 层 - 7 层 (L4-L7) 网络流量的应用交换机。除了可以提供多种应用优化，应用安全以及应用高可靠设计等多种上层功能模块外，在产品底层架构上，NetScaler 也有具有非常独特的专利架构。NetScaler 在底层架构上有两个非常智能，且协调工作的模块－应用交换引擎与 AppExpert 策略框架。

应用交换引擎将 HTTP 应用层的数据提取出来，根据这些应用的特性，使用者可在 AppExpert 策略框架上灵活编写策略调用上层的功能模块（例如压缩，缓存等）。



4.1 应用交换引擎

NetScaler 拥有专利的应用交换引擎展示了下一代的流量管理技术。NetScaler 打破了存在于连接和请求之间的关系，并在请求层检测所有的流量，应用交换提供了高性能的，安全的，可扩展的应用层服务。

基于该引擎， NetScaler 系统分开管理每一客户端连接以及服务器端连接。因为 NetScaler 系统是每个客户端以及服务器端连接的终点，而不是简单的传输连接，所以它能提供以前其他流量管理系统所无法达到的许多加速和优

化技术。应用交换引擎被专门设计来在请求层检测流量，所以负载均衡以及内容交换可以非常高效的完成。策略以及过滤可以在进入的请求上被应用并且丝毫不影响性能。 成熟的负载均衡算法以及健康检查机制保证了服务的均衡性以及持续可靠性。 先进的加速和优化技术在降低服务器负载的同时更快的把内容传送给了最终用户。

应用交换引擎是 NetScaler 应用交付系统的技术核心。基于在请求层管理流量的原理，应用交换引擎可以在最终用户的地理位置和连接速度各不相同的情况下高效的加速和优化内容传输。由于 NetScaler 系统是一个在客户/服务器端通信代理，因此 NetScaler 可以最大限度的利用 HTTP 1.1 对于连接保持的优越特性。多个请求可以在一个客户连接上被复用，这样消除了连接建立的时间以及客户端的延迟。与服务器保持的常连接，可以复用多个客户端来的请求，甚至可以是从不同客户端来的，或者甚至客户端不支持连接保持。 这将减少 TCP 连接在服务器上的消耗，使得服务器可以更有效的专注于内容的服务。

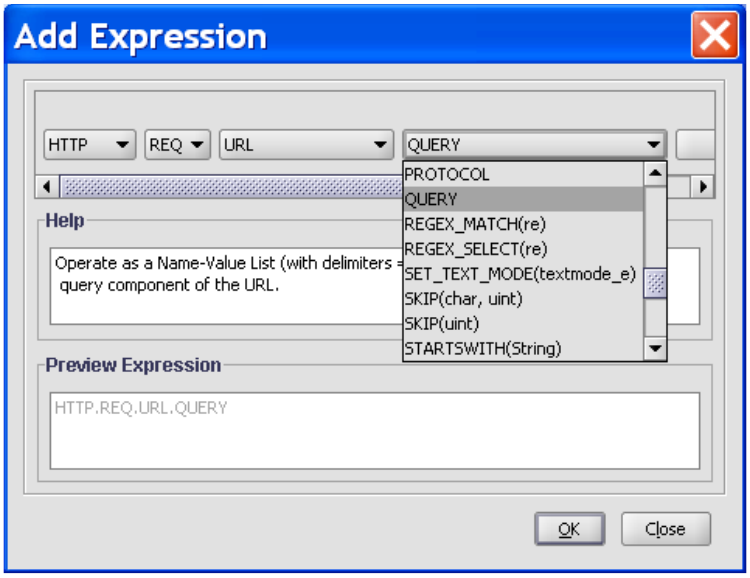
此外，应用交换引擎具有优化过的 TCP/IP 堆栈，确保 NetScaler 系统消除服务器对于客户端连接速度的依赖性。一旦一个向服务器的请求建立，响应可以线速传递到 NetScaler 系统。NetScaler 系统会缓冲该响应并以客户端连接速度来把内容传递给客户端，这样使得服务器可以持续服务接下来的其他请求。

4.2 AppExpert 策略框架

AppExpert 策略框架是整个 NetScaler 功能调用的核心，可提供 Web 应用流量以及所有 NetScaler 功能模块如何发挥作用的控制者。

AppExpert 策略框架定义 NetScaler 上的流量过滤和管理的特定详细信息。它由两部分组成：表达式和操作。表达式定义策略匹配的请求类型。操作告诉 NetScaler 当请求匹配表达式时做什么。例如，表达式可能要使特定的 URL 请求与某种类型的安全攻击相匹配，操作为断开或重置连接。

每个策略都有优先级，优先级确定评估策略的顺序。当 NetScaler 收到流向或来自它管理的任何服务器的流量时，相应的策略列表将确定如何处理流量。


Add Expression
HTTP
REQ
URL
QUERY
PROTOCOL
QUERY
REGEX_MATCH(re)
REGEX_SELECT(re)
SET_TEXT_MODE(textmode_e)
SKIP(char, uint)
SKIP(uint)
STARTSWITH(String)
Help
Operate as a Name-Value List (with delimiters =
query component of the URL.
Preview Expression
HTTP.REQ.URL.QUERY
OK
Close

5 产品功能描述

5.1 保障应用可靠性功能

NetScaler 的对应用的多种高可靠性保障机制可在不影响应用或用户的情况下自动重新分配资源，并根据流量大小增加或减少容量，从而实现了服务器资源的最佳使用。保障可用性的设计允许用户只会访问到正确的应用资源，因此可确保应用处于 100%的可用状态，消除了停机和灾难期间常见的故障时间。

5.1.1 本地服务器负载均衡

用户可根据系统的实际情况，在 NetScaler 中定义若干个虚拟服务器（也称为 vserver 或者 VIP)， 其上包括了一个 IP 地址和端口。这个虚拟服务器被设置成与一组运行在真实服务器群上的真实服务所绑定。真实服务包含了后台真实服务器的 IP 地址以及端口。在这样的情况下，一个客户发送一个请求到虚拟服务器，然后虚拟服务器在真实服务器群中选择一个并将请求转发到该真实服务器。不同的虚拟服务器可以设置成与不同的真实服务绑定，例如 TCP 以及 UDP 服务。虚拟服务器支持的协议和应用包括： HTTP, FTP, SSL , SSL BRIDGE, SSL TCP ,NNTP 以及 DNS 等等。

同时对于某些特定的服务，我们在虚拟服务器上配置“会话保持” ： 一旦一个服务器被选择了，后续的从该用户发出的请求都被转发到同一服务器上。“会话保持”对于那些状态需要保存在服务器上的应用，例如：购物系统等是非常重要的。NetScaler 主要支持的“会话保持”算法包括：

- 源 IP
- Cookie
- SSL 会话 ID
- URL
- 客户化服务器 ID
- 策略（可以选择任何 HTTP Header 中的对象）
- 源和目的 IP
- 目的 IP

NetScaler 系统也负责检查服务器群的服务的健康状况。一旦发现服务有问题， NetScaler 系统仍将继续依照负载均衡算法把服务转向到其他正常的服务上去。NetScaler 主要支持的健康检查算法包括：

- PING
- TCP
- HTTP
- TCP-ECV
- HTTP-ECV
- UDP-ECV
- DNS
- FTP
- RADIUS
- USER
- HTTP-INLINE
- SIP-UDP
- LOAD
- FTP-EXTENDED
- SMTP
- SNMP
- NNTP
- MYSQL
- LDAP
- POP3
- CITRIX-XML-SERVICE
- CITRIX-WEBINTERFACE

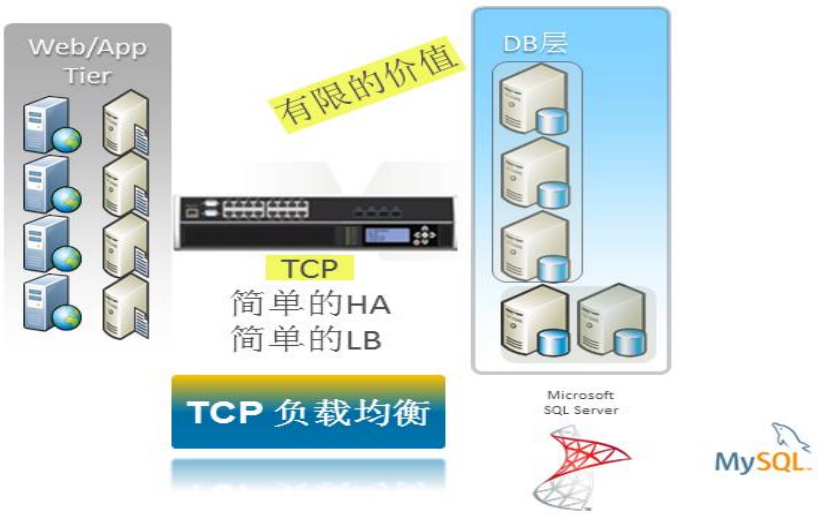
负载均衡算法指定了负载均衡的标准，也就是说，负载均衡算法选择了一台真实服务器来传递用户的请求。如果这个被算法选定的最合适的服务器达到或者超过了其最大用户连接数（使用-maxClients 在 CLI 命令行中队服务进行设定），那么另外一个连接数比较合适的服务器将被代替。这个方法可以通过在

均衡算法中将连接数作为权重设置来实现。NetScaler 系统可以设置按照以下这些算法来实现服务器负载均衡：

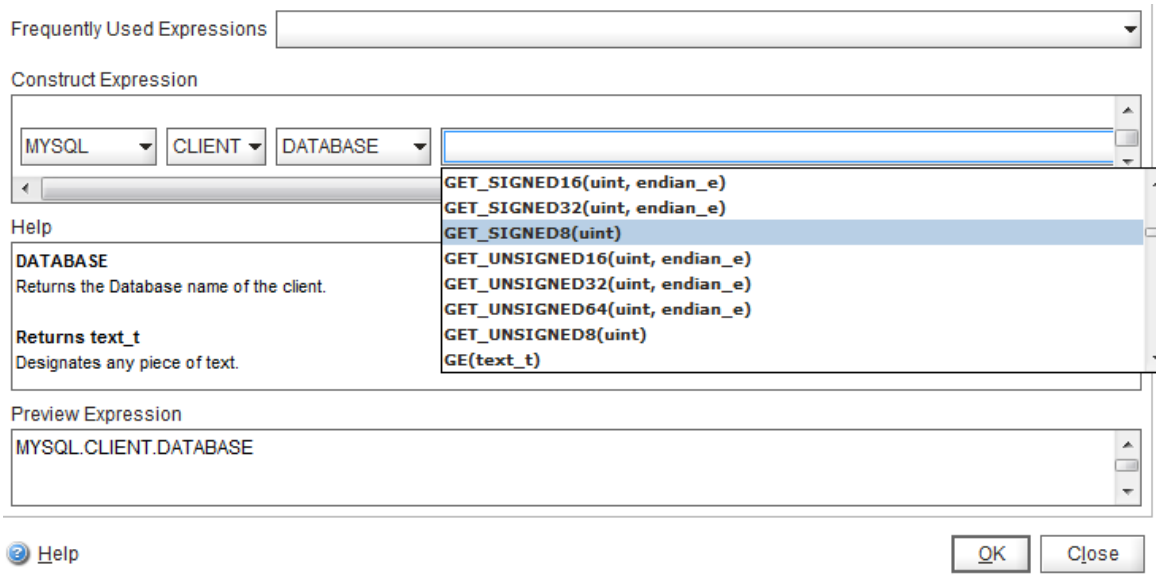
- 最少连接数
- 轮询（可加权或比率）
- 最少响应时间
- 最低带宽
- 最少包
- 令牌
- URL 散列法
- 域名称散列法
- 源 IP 地址散列法
- 目的 IP 地址散列法
- 源 IP-目的 IP 散列法
- 自定义的基于 SNMP 的判断

5.1.1.1数据库服务器负载均衡

数据库的查询是非常消耗服务器的 CPU 资源的，传统的 SLB 设备仅能基于 TCP 连接做数据库的负载均衡，不能做到真正意义上的基于 7 层应用实现负载均衡，同时对于服务器的健康检查方式也非常单一，仅能检查数据库端口是否正常，无法判断数据库处理是否正常。



Netscaler 独有的 DataStream 功能，可以帮助企业实现基于 MySQL 和 SQL Server 数据库的负载均衡。可以实现基于数据库的操作内容来进行读写分离，负载均衡，同时通过前述的 TCP 连接复用等功能显著提成服务器性能。Netscaler 特有的数据库健康检查可以更准确的判断数据库是否正常。



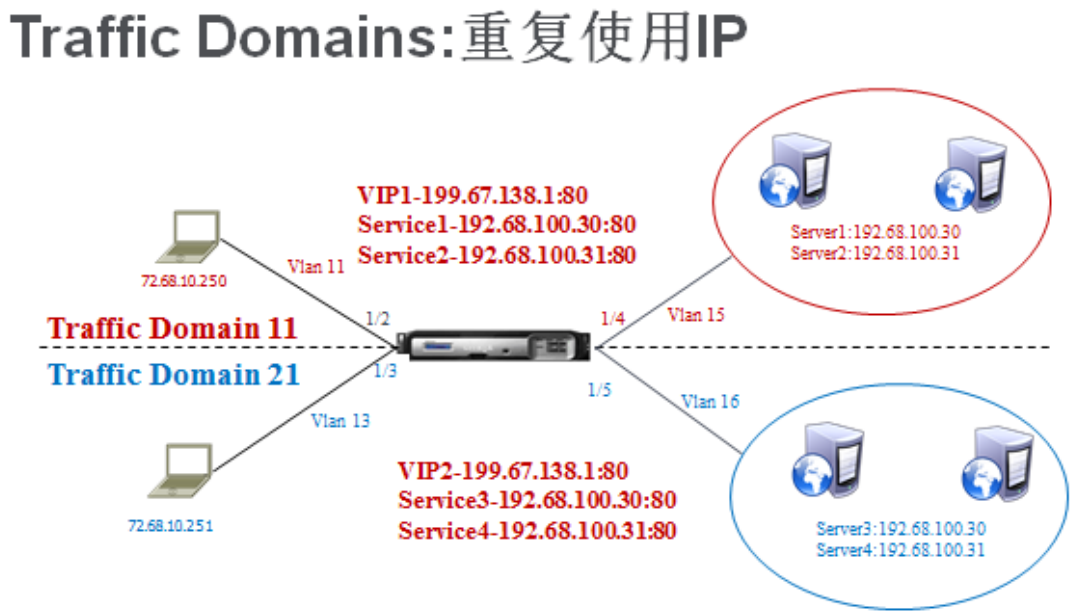
5.1.2 Traffic Domain 实现设备虚拟分区

在传统的解决方案中，单一设备是不能实现多租户的功能，即一台设备可以给多个不同用户使用，复用相同的 IP，路由等。

Traffic Domain 帮助企业在单一的 ADC 设备中实现多租户功能，同时其重点是允许路由和 IP 重用。

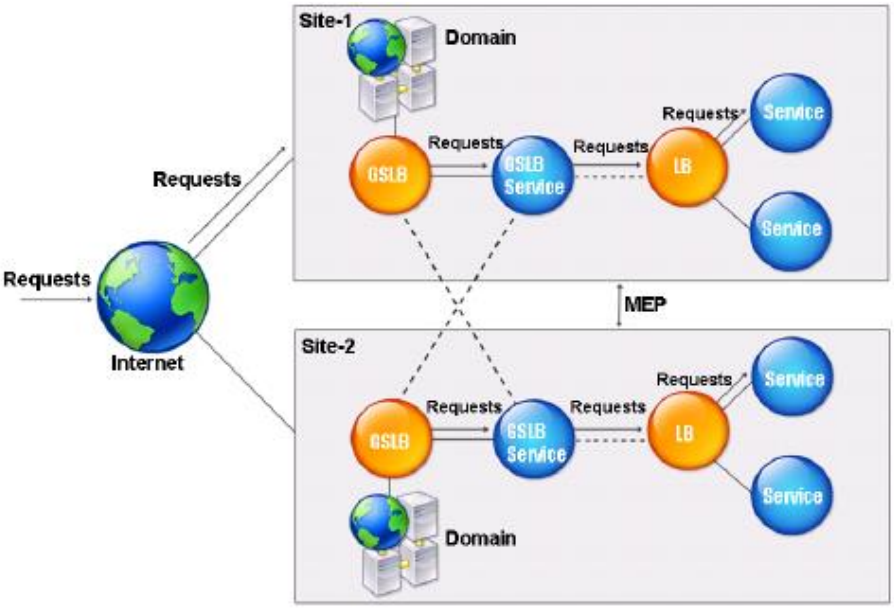
Traffic Domain 使我们的用户可以创建多个逻辑分离租户，所有租户并存同时相互之间不可操作，不可见。在每一个 Traffic Domain 中，Netscaler 的功能模块均可以得以实现。

需要说明的是，Traffic Domain 并不是真正意义上的做租户设备，所有 Domain 共享硬件资源，在下文 Triscale 中，将着重介绍 Netscaler SDX 多租户解决方案。



5.1.3 全局负载均衡

NetScaler 为数据中心应用交付提供多种优化和提高可用性的功能，但针对全局多站点间负载均衡需求，主要用到了 NetScaler 的全局负载均衡功能。NetScaler 的全局负载均衡功能可以把客户对一个网站的访问请求引导到分布在 Internet 上多个站点中性能最佳的一个站点。从而实现用户的就近访问，站点之间的负载均衡和远程容灾。下图为典型的全局负载均衡部署



NetScaler 支持的全局负载均衡算法（量度方法）如下：

- 轮询
- 源 IP 地址散列
- 站点服务器连接数最少
- 站点服务器响应最快
- 站点带宽最低
- 站点数据包最少
- 自定义的基于 SNMP 的判断
- 静态的就近性
- 动态的就近性

上述算法中的第 1、2 种算法的作用主要是将客户端的访问均匀的分散到各个站点，实现站点之间的负载均衡和远程容灾；第 3-7 种算法可以将用户端的请求引导到服务器性能最好或服务器最空闲的站点，主要用在服务器运算密集型的应用场景；第 8-9 种算法可以将用户端的请求引导到距离用户最近的站点，实现用户的就近访问。

在全局负载均衡中，NetScaler 可以根据用户所在的地理位置和用户使用的 ISP 链路，选择用户访问 Web 站点接入的 ISP 链路， NetScaler 的全局负载

均衡功能是基于 DNS 实现的，并由 NetScaler 系统自动智能判断。因此常用的全局负载均衡配置方法如下：

部署多台 NetScaler，分别用来解析 DNS 查询请求。当 NetScaler 收到一个 DNS 请求后，

1. 如果该请求是来自网通或电信的 IP 地址段，则根据静态就近性算法，判断此用户是网通还是电信用户，并返回响应的解析结果给用户，即网通用户使访问网通站点，电信用户访问电信站点。其中，静态就近性算法是指 NetScaler 依靠一个预先手工配置好的“IP 地址与地理位置的映射列表”选择就近的站点，例如，我们可以在 NetScaler 中配置以下信息

100.100.100.0/24　　中国.网通.北京
100.100.101.0/24　　中国.网通.河北.石家庄
100.100.102.0/24　　中国.网通.河北.保定
100.100.103.0/24　　中国.网通.河北.唐山
100.100.111.0/24　　中国.网通.山东.济南
100.100.112.0/24　　中国.网通.山东.青岛
200.100.100.0/24　　中国.电信.北京
200.100.100.0/24　　中国.电信.上海
… …

当一个用户访问 NetScaler 时，NetScaler 根据用户端的源 IP 地址在列表中查询出其所处的地理位置或运营商信息，并与各个站点的地址位置和运营商信息进行匹配，匹配长度最长的站点一定是距离客户端最近的站点或相同的运营商，NetScaler 就使用该站点或运营商的 IP 地址响应 DNS 请求。

2. 如果用户请求是来自非列表中的 IP 地址段，我们不确定该用户访问哪个站点效果更好，则可以让两台 NetScaler 分别通过动态的就近性算法探测用户的本地 DNS 服务器，测量由客户端网络到达各站的速度，并依据这个量度，选择访问速度最快的站点，解析域名到该站点对应的 IP 地址，从而将用户访问引导到该站点。

3. 如果通过动态就近性算法探测发现用户访问各站点的速度相同，NetScaler 则采用轮询算法（ROUND ROBIN）将用户访问平均分配到各站点上，确保入站流量的负载均衡。

4. 当一个站点发生故障，无法正常工作时，NetScaler 会自动发现，并把用户访问全部集中到正常工作的另一站点，从而确保站点的高可用性。

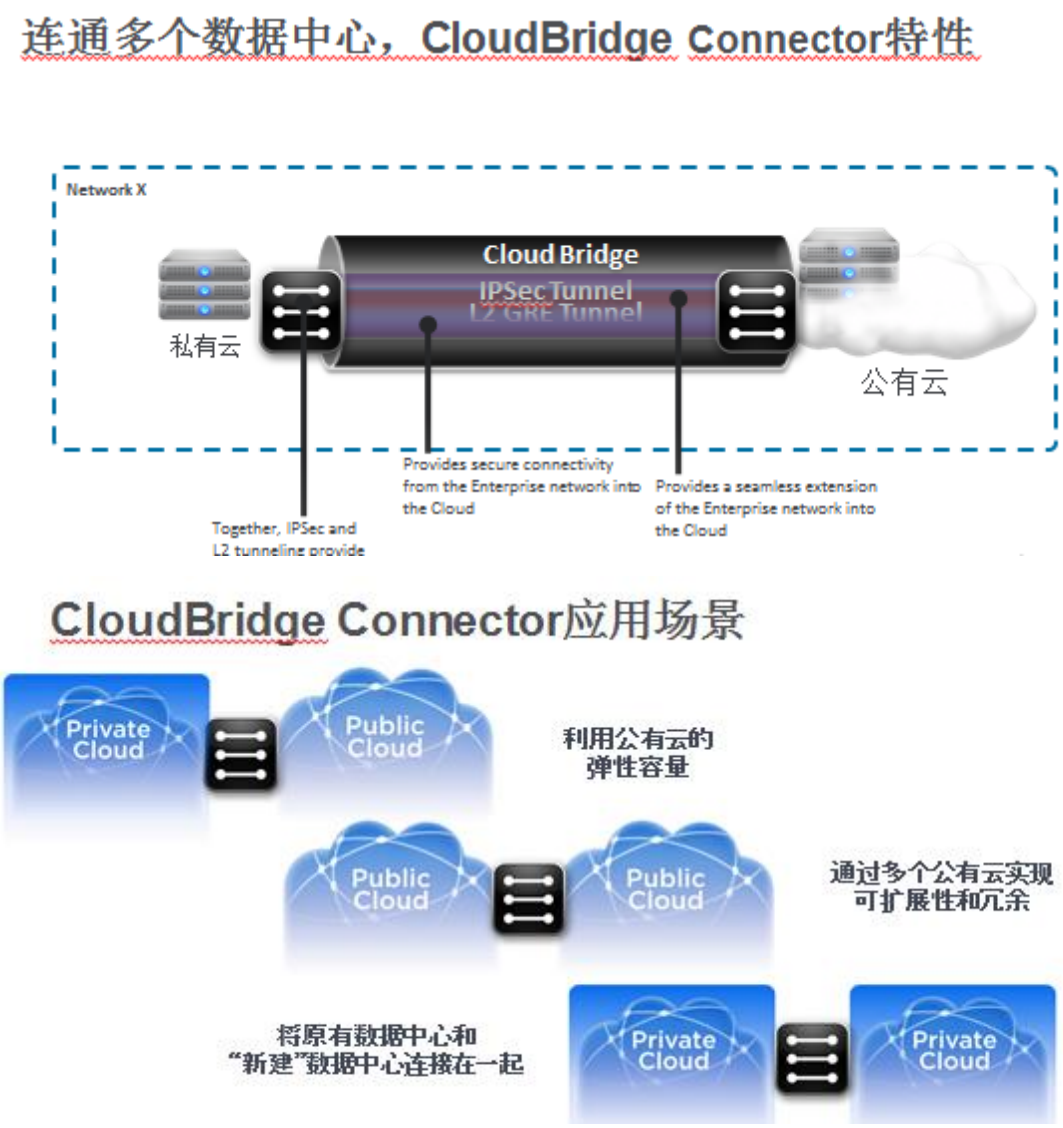
5.1.4 链路负载均衡

NetScaler 也可以对相同站点内多个 WAN 链路实行负载均衡并提供故障转移，从而进一步优化网络性能并确保业务持续性。

NetScaler 的应用智能流量控制和健康状况检查可以在上联路由器之间有效地分配流量，从而确保网络连接保持高度可用。确定最佳 WAN 链路以根据策略和网络条件路由入站和出站流量，并通过提供快速的故障检测和故障转移使各项应用免受 WAN 或 Internet 链路失效影响。

5.1.5 多数据中心扩展

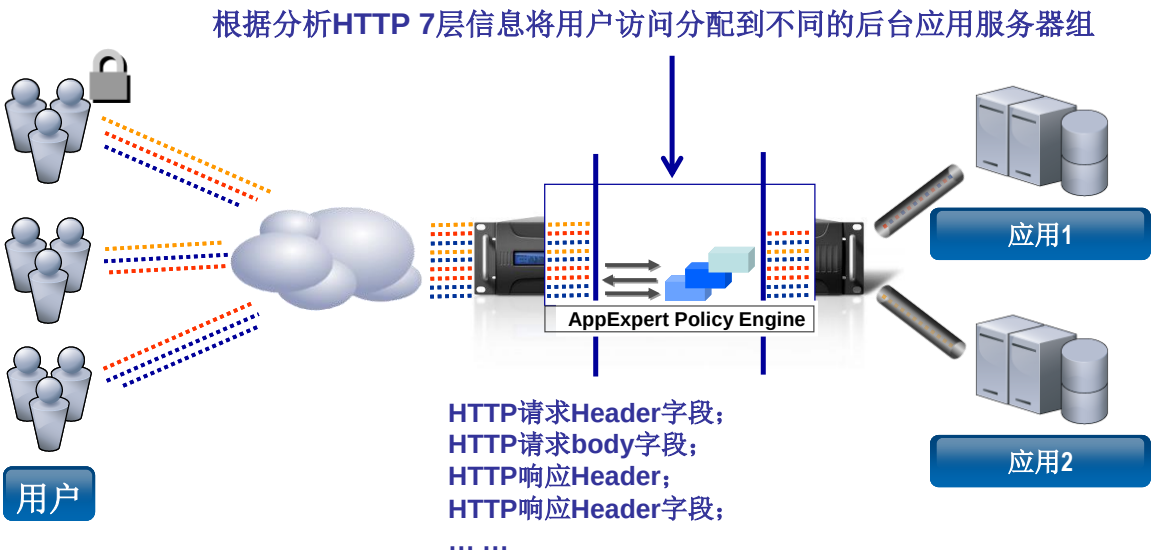
Netscaler 可以将企业多个数据中心实现二层打通，帮助企业构建一个透明的扩展的数据中心。使用 Netscaler 的 CloudBridge Connector 功能在两个数据中心之间建立一个（IPsec+GRE 封包）安全二层隧道。通过这样的方式，企业无需在重新规划 IP，修改应用网络设置，只需用现有的架构进行扩展即可。



5.1.6 7 层请求交换

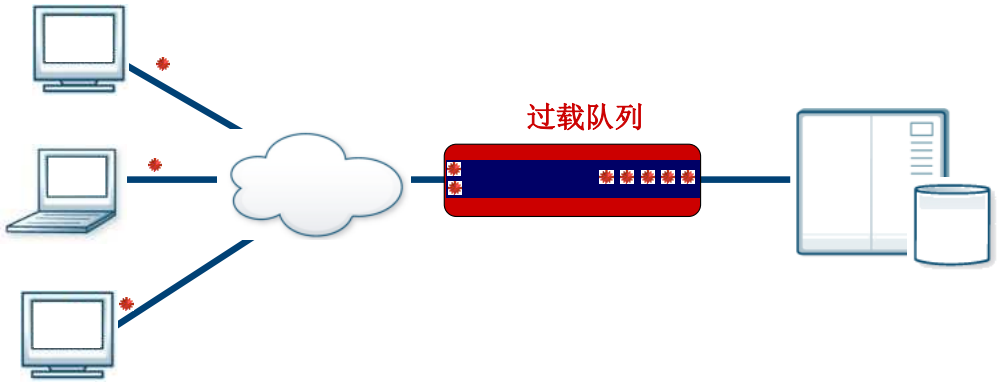
NetScaler 提供的 7 层请求交换是 Web 应用系统的基础，它是拥有最佳的性价比，能保证持续，安全的 Web 应用。基于在网络优化方面的领先研究，请求交换技术以最有效的方法处理 Web 应用流量：

在应用请求层进行分析，然后加入安全性，重定向进入流量，使得优化流向，保护以及控制流量变为可能。基于这些技术，NetScaler 打破了应用请求对于传输层的依赖性，从而实现了每个最终用户的请求。这一独特的处理特定应用请求以及响应的能力，使得应用层得到保护，网络基础得到全面优化，而这是其他技术以及方案所不能提供的。下图为一个请求交换的示例：



5.1.7 浪涌保护

由于 NetScaler 架构工作在应用层面，因此 NetScaler 能够实施监控服务器的处理能力。通过比较收到请求的速率和服务器响应的速率，能够了解服务器目前的处理能力，如果一组 Web 服务器已经不能处理更多的请求，NetScaler 会拿出自己的内存缓存数据，根据 Web 服务器的响应速度，适量发送请求给后端的 Web 服务器。NetScaler 的浪涌保护能确保服务器不会在连续高流量作用下出现“雪崩式瘫痪”。



5.1.8 4 - 7 层带宽控制

5.1.8.1优先级队列

当用户的 Web 站点在由于攻击出现浪涌流量的时候，所有客户端对服务器资源的访问出现争抢的现象。NetScaler 通过优化流量队列确保重要的流量分配高优先级，同时用户可以通过 NetScaler 策略引擎定义对重要流量的定义，无论从网络层还是应用层。优先级队列特性区分流量的高优先级和低优先级，确保重要流量对 Web 服务器资源的访问。

5.1.8.2最大连接与带宽控制

用户可以选择采用基于最大连接数或者基于带宽的流量控制，可根据服务器组的处理能力为每个 VServer 或服务器配置最大连接数或这带宽，当连接数或带宽到达设定的的阈值后，可根据 用户自定义的策略重定向流量到备份 VServer 或者限制用户访问。

5.1.8.3HTTP/TCP/DNS 请求速率控制

NetScaler 不仅可以为应用分配优先级，限定最大连接数和带宽，而且可以控制用户访问应用的速率。以 HTTP 请求为例，当一个客户端的访问速率超过 50 个请求/秒，NetScaler 可以识别访问速率，并根据预先配置好的策略处理超过此速率的请求，例如重定向或阻止，从而确保后台服务器或应用的可靠性。对 TCP 新建连接速率，以及 DNS 查询速率同样可以进行控制。

5.2 提高应用性能功能

NetScaler 提供加速 Web 应用性能的多种功能，为企业带来了直接的效益，提高员工生产效率，增强网络通信，并提高用户满意度。下文将介绍 NetScaler 提供的多种加速 Web 应用交付技术。

5.2.1 TCP 连接复用

对于 HTTP 流量， NetScaler 系统通过利用保持自己与用户端的连接以及保持自己与服务器的常连接的技术来保证了快速的页面下载时间。

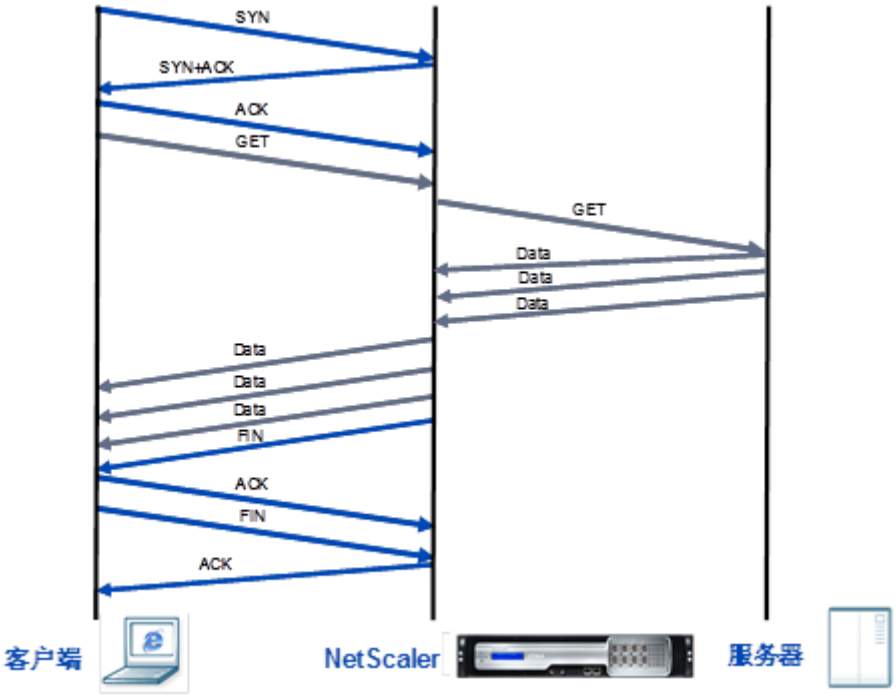
这个是通过在客户端以及服务器上的 HTTP “连接保持” 技术来实现的。

对于服务器来讲，它永远只感觉到自己在和一个一直保持连接的用户（就算实际上该用户不是一直保持连接的）进行交互。而对于客户端来讲，它永远感觉到自己在和一个保持连接的服务器在进行交互（就算实际上该服务器被设置成例如一个请求一个连接这样的非 keep-alive 方式).

这一常连接保持技术利用在客户系统上，可以显著提高用户客户端的页面下载时间。其原因在于用户不需要再建立新的连接，而一般来讲这些新建连接过程在 WAN 上通常会带来 50 到 500ms 的延迟。

服务器端的常连接保持带来的服务器服务卸载。NetScaler 保持与服务器的连接，并且所有来自客户端的连接被 NetScaler 终结。这样的情况下，服务器可以将更多的资源用在对于用户请求的响应上而不是去浪费在 TCP 连接的建立和拆除的管理上。

常连接保持使得服务器上只存在有较少的连接，服务器 CPU/内存 使用率被显著降低，其原因是服务器现在处理的连接建立和拆除进程减少很多了。NetScaler 连接复用工作原理示意图如下：



5.2.2 优化 TCP 协议栈

NetScaler 设备除了具有 TCP 连接复用优化技术之外，它还依据 IETF 的最新研究成果，按照 RFC 相关标准，提供优化 TCP 协议栈的一些功能。在基于标准的 TCP/IP 协议上，创新性地实现了 SACK 选择性确认（RFC2018）和 Windows

Size 缩放（RFC1323）等功能。这些技术的支持，极大的提高了 TCP/IP 协议栈的效率，确保 NetScaler 在那些广域网链路环境下具有更佳出色的吞吐能力和传输效率。为那些通过广域网访问应用系统的最终用户带来高达 5 倍的性能提升，并提高广域网链路的使用效率。

5.2.2.1 SNAK

TCP 通信时，如果发送序列中间某个数据包丢失，TCP 会通过重传最后确认的包开始的后续包，这样原先已经正确传输的包也可能重复发送，急剧降低了 TCP 性能。为改善这种情况，发展出 SACK(Selective Acknowledgment, 选择性确认)技术，SACK 信息是通过 TCP Header 的选项(option)部分提供的，该选项参数告诉对方已经接收到的不连续的数据块，这种机制的好处是接收方能通知发送方哪些数据丢失，哪些数据重发了，哪些数据已经提前收到等。发送方可根据此信息检查究竟是哪个块丢失，从而发送相应的数据块。这样 TCP 发送方就只重新发送丢失的包，不用发送后续所有的包，显著的提高了有损网络中的数据传输效率。

5.2.2.2 Windows Scaling

Windows Scale 窗口缩放因子参数也是通过 TCP Header 的选项(option)部分提供，窗口扩大选项使 TCP 的窗口定义从 16 位增加为 32 位。

典型的 TCP 数据包头信息中通过 16 个 bit 描述 Windows Size 的大小，也就确定了数据发送和接收的容量，按照 16 bit 位计算，最大的 Windows Size 是 65525 字节（2^16 = 64K Bytes）。假设每次 Windows Size 都能协商成为最大值（网络条件非常理想的情况），这意味着，数据传输在确认完成 64KB 后，再发送下一个 64KB 数据，否则必须等待，在链路延迟较大的情况下，等待 Ack 的行为会降低传输效率，表现为数据吞吐较低。而 RFC 1323 扩展了这一限制，通过 TCP 数据包头 Option 部分定义一个 Windows Scaling（窗口缩放因子）参数，将 TCP Windows Size（窗口大小）维持为 32 个 bit 的值，达到 2^32 = 4G Bytes。

NetScaler 设备启动 Windows Scaling 功能后缺省 TCP 窗口大小扩展为 1M Bytes，Windows Scale 的 factor 设置最大为 14，即支持最大 TCP 传输窗口尺寸为 2^30 = 1G Bytes，这种技术的采用，有效减少了协议交互的次数，使得在广域网上的数据传输吞吐大大提高。

5.2.2.3 TCP Westwood

TCP Westwood 为移动应用提供更好的拥塞控制。无线应用数据传输中 Packet loss 是一个大麻烦，如 Wifi 用户在不同的接入点间切换丢包，3G 用户在不同的基站间切换丢包。

现有解决方法：检测到 packet loss，把拥塞窗口大小减半。

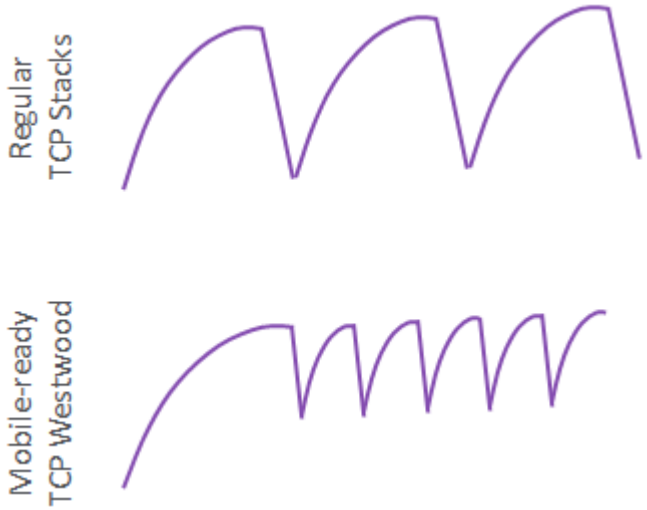
好处：为宽带用户提供良好服务，更快适应到新的传输速率。

坏处：如果丢包频率稍高，如移动用户，将会较大降低传输速度。

TCP Westwood：检测到 packet loss，将拥塞窗口减少到一个适应的估计值。

如何实现：使用 “灵敏探针” 来跟踪估计带宽

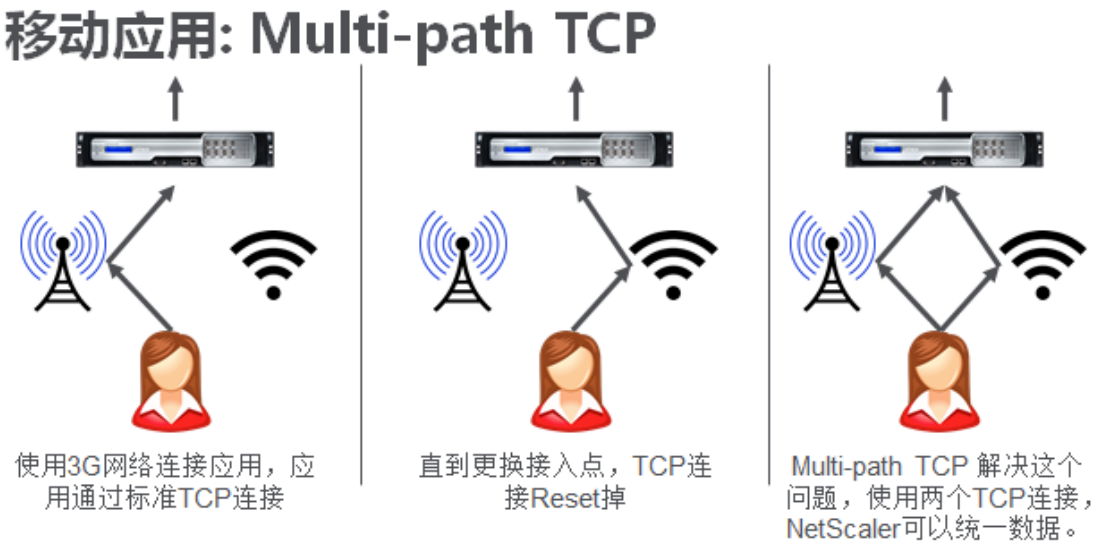
估计带宽 = (amount of data acknowledged in an interval) / time



可以看到，使用 TCP Westwood 后，数据传输变得更为平滑稳定。

5.2.2.4 Multi-path TCP 协议支持

TCP 传输失败导致最终用户体验变差，并造成重大传输延迟。今天，我们可以看到移动设备可以有多个路径连接到资源，但是，没有什么好办法可以有效地利用多条路径。多路径 TCP 专注于给最终用户带来最好的多条路径，同时减少延迟和提高最终用户体验。



5.2.3 SSL 卸载

SSL 卸载可以将 CPU 密集型的 SSL 加密或解密任务从本地 Web 服务器转至 NetScaler，从而释放 Web 服务器资源来处理请求。 SSL 卸载可以确保 Web 应用的安全交付，并且不降低性能。在将 SSL 流量解密之后，所有标准服务都可以对其进行处理。

处理安全 SSL 事务会消耗 Web 服务器的 CPU 能力的很大部分，降低性能并提高最终用户的响应时间。SSL 加速会透明地改善进行 SSL 事务的 Web 站点性能。SSL 协议可以无缝运用于各种类型的 HTTP 和 TCP 数据，为使用此类数据的事务提供了安全通道。

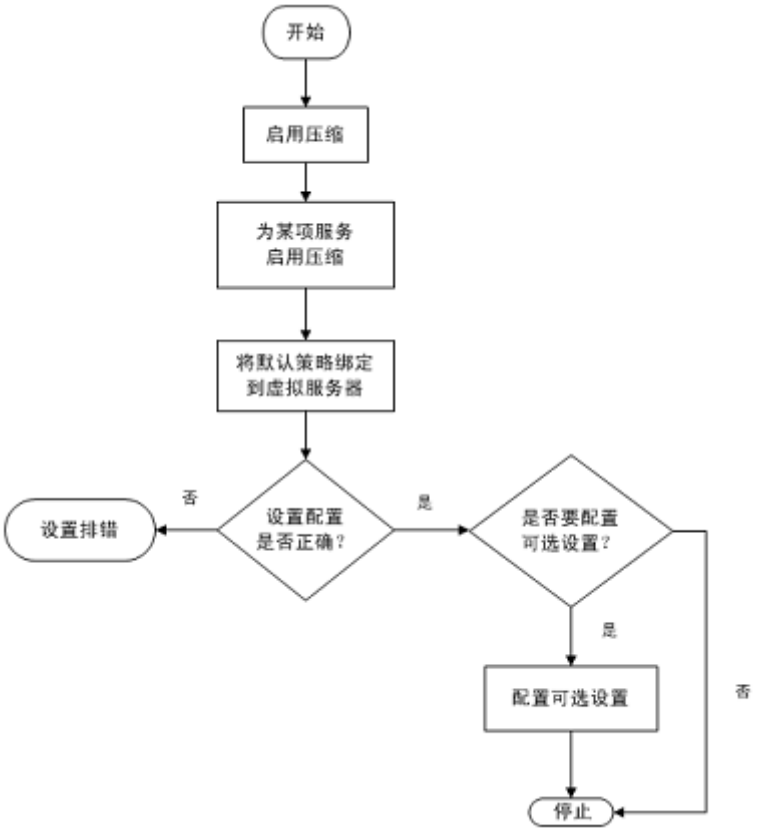
配置了 SSL 加速的 NetScaler 位于 Web 服务器的前面，它在此代表服务器拦截 SSL 事务、处理 SSL 事务、应用负载均衡和内容交换策略，然后将事务传送给服务器。SSL 功能的实现如下图：

5.2.4 HTTP 压缩

NetScaler 提供 HTTP 压缩功能，压缩功能通过减少下载时间和带宽使用来改善性能。

压缩功能在具有 HTML 或其它可压缩内容（静态或动态生成）的原始站点实施。NetScaler 会压 MIME 类型的内容，例如 text/html、text/plain、text/xml 、 text/css 、 text/rtf 、 application/msword 、 application/vnd.ms-excel 、 application/vnd.ms-powerpoint 、 Internet Explorer、Firefox 和 Netscape 等浏览器会拦截 HTTP 压缩。NetScaler 不压缩属于 application/octet-stream、二进制或字节类型的内容，也不压缩 GIF 或 JPEG 格式的图像。

配置了压缩策略的 NetScaler 会拦截来自启用压缩的客户端的请求，并应用压缩策略以确定客户端是否可以接受可压缩内容。在收到来自服务器的 HTTP 响应后，NetScaler 检查内容以确定是否可以压缩。如果内容可压缩，NetScaler 将对其进行压缩，修改响应标头以指明所执行压缩的类型，并将压缩的内容转发给客户端。NetScaler 中压缩功能处理流程如下所示：



5.2.5 Web 缓存

利用 NetScaler 的 Web 缓存功能，将服务器上最常被访问的 Web 对象缓存在 NetScaler 设备的内存中，以极高的效率响应用户的请求。

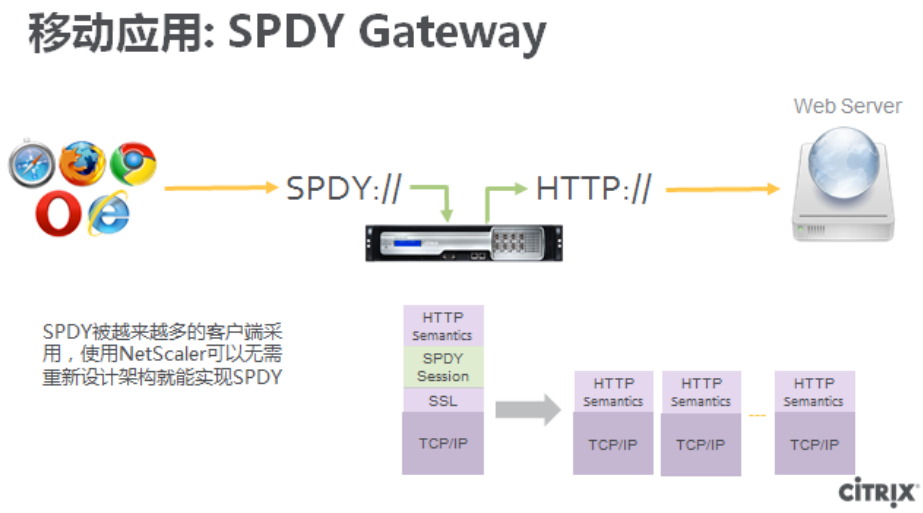
同时，针对这些 Web 对象的访问将不再发往服务器处理，大幅度降低了服务器的访问次数，降低了服务器负载。进而提高了服务器的处理速度，减少了所需服务器的数量。

此外，NetScaler 还提供了创新的参数化动态内容缓存功能，可缓存数据库查询等动态的内容，例如对基金证券净值的查询是一个典型的动态应用，传统缓存设备和负载均衡器根本无法缓存此类内容。而 NetScaler 使用其参数化动态内容缓存功能，将动态内容转换为可缓存内容，减少了数据库 99%的动态运算，大大降低了数据库负载。

5.2.6 SPDY 协议支持

一种新的网络协议“SPDY”(发音同“speedy”)由谷歌开发，以最小化网络延迟，提升网络速度，优化用户的网络使用体验。SPDY 并不是一种用于替代 HTTP 的协议，而是对 HTTP 协议的增强。新协议的功能包括数据流的多路复用、请求优先级，以及 HTTP 包头压缩。谷歌表示，引入 SPDY 协议后，在实验室测试中页面加载速度比原先快 64%。这一数据基于对全球 25 大网站的下载测试。目前 SPDY 团队已经开发了一个可使用的原型产品，谷歌决定开放这一项目，希望“网络社区能积极参与、提供反馈及帮助”。

要使用 SPDY，浏览器和应用程序都需要支持，目前，主流的浏览器均支持 SPDY，后端应用程序需要对 SPDY 进行支持方才可以工作。但是，现阶段，企业的很多应用已经开发完毕并且在线使用，很难在为了 SPDY 在对现有应用进行二次开发。Netscaler 目前已经支持 SPDY 协议，可以作为 SPDY 网关将企业的应用通过 SPDY 协议让客户端进行访问。



5.3 增强应用安全性功能

NetScaler 应用交付系统具备全面的攻击防御系统，可确保系统不受 DoS、DDoS、网络蠕虫/病毒和应用专用漏洞的攻击。底层应用交换技术支持 NetScaler 应用交付系统对应用请求进行检查，辨别恶意内容并阻止其进入应

用服务器。下文将介绍 NetScaler 提供的多种安全防护机制。

5.3.1 L4 层 DOS 攻击防护

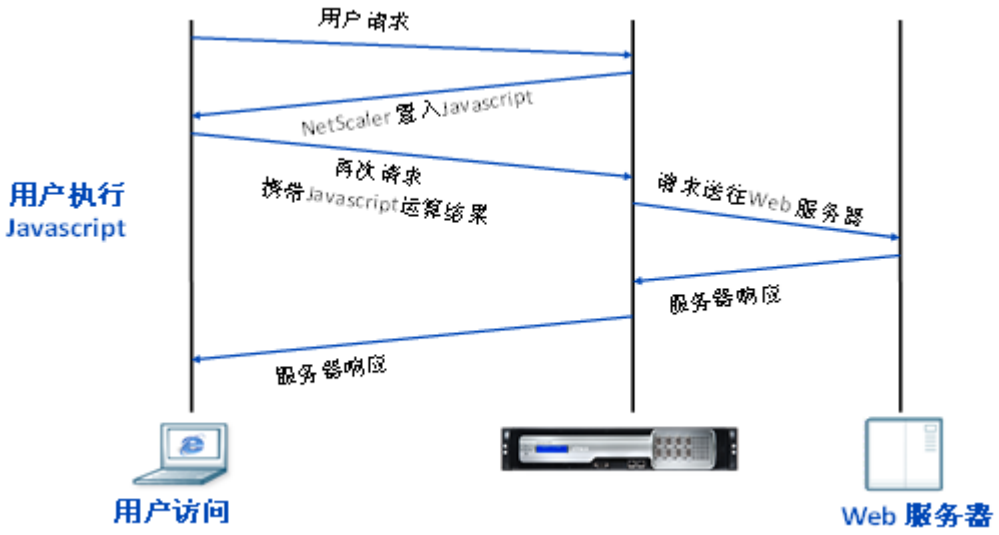
NetScaler 系统使用 SYN cookies 原理来防范 SYN Flood 等 DoS/DDoS 攻击。Cookies 被发送到发送请求的用户端，该初始会话状态没有被保留在 NetScaler 系统上。正因如此，NetScaler 没有为该会话分配内存，正常的由合法的用户发出的 TCP 连接并不会被打断。NetScaler 系统的 SYN-Cookie 概念一直是起用的，并不需要其他额外配置。NetScaler 系统在收到非 HTTP 流量的最终 ACK 包或者收到 HTTP 流量的 HTTP 请求包时才为连接分配内存。 正因如此，NetScaler 系统可以达到非常高的 SYN 处理能力。NetScaler 系统的 SYN cookie 机制确保了以下几点：

1. NetScaler 系统的内存不会浪费在非法的 SYN 包上，实际上，内存只被用来向合法用户提供服务。
2. 合法用户的普通的 TCP 对话可以不间断的得到服务，就算系统在 SYN Flood 攻击下也是如此。
3. 正由于内存只在收到 HTTP 请求后才予以分配给连接， NetScaler 系统使得 Web 站点避免受到 “空闲连接” 攻击。

5.3.2 L7 层 DOS 攻击防护

一般来讲，有两种类型的 7 层 HTTP DoS 攻击： Get 攻击以及 IDLE 攻击。 对于 Get 攻击,黑客在一个连接建立后发出非常多的 Get 请求。 对于 IDLE 攻击，攻击者在连接建立后恶意停止一切活动而空闲等待。

NetScaler 系统在处理时，当连入的 Session 速率达到一个预先设定的门限值时，DOS 防卫功能就自动触发。 NetScaler 系统会抽样对一部分客户端请求发送带有 SET-COOKIE 的响应。 恶意攻击主机通常不会响应 Set-Cookie，所以这些攻击包就会被丢弃。 而普通正常的 HTTP 请求不会受到影响。 这个触发的门限值以及发送 Set-Cookie 的比例值可以针对每个服务来精细微调。 并且，由上所述，连接不会在第一个 GET 请求到达前建立。所以 NetScaler 系统也可以有效的防止 IDLE 攻击。

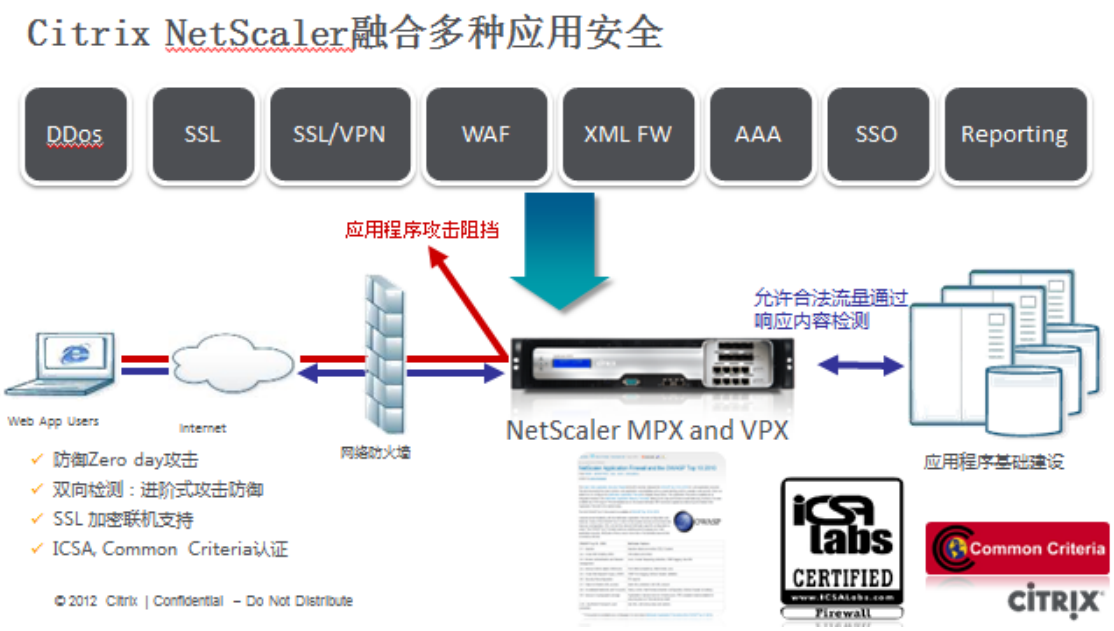


5.3.3 内容过滤

NetScaler 不但支持基于源/目的地址、源/目的端口、协议类型等三、四层基本的过滤功能，而且 NetScaler 通过分析 IP 地址等网络层信息和 HTTP Get 和 Post 等应用层请求信息，来过滤客户端对 Web 应用的访问，即七层内容过滤。当出现已知攻击的情况下，NetScaler 可以根据其策略引擎灵活定制过滤策略。例如类似 Nimda 和红色代码等攻击，我们都可以通过定制针对 HTTP 请求的 URL 的过滤策略，防止攻击的产生。

5.3.4 Web 应用防火墙

Citrix 应用防火墙（Application Firewall）作为 NetScaler 中的一个安全模块，用来防御已知和未知的 Web 和 Web Services 应用攻击的高性能且强大的安全设备。Citrix 应用防火墙 （Application Firewall）实施了只允许正确 Web 应用行为的积极安全模型，而无需依赖攻击签名。应用防火墙（Application Firewall）分析所有的双向流量，包括 SSL 加密通信，防御 16 个层面的 Web 应用漏洞而无需对应用进行任何修改，可作为能够满足各种部署需求的特制设备，而且它具有两种软件版本以便在威胁、应用和防御变得越来越复杂时能够提供升级功能。



5.3.4.1阻止 16 大类 Web 漏洞攻击

- 缓冲区溢出
- CGI-BIN 参数处理
- 表单/隐藏字段处理
- 强制浏览
- 消息或会话攻击
- 被破坏的访问控制表或弱口令
- 跨站点脚本攻击（XSS）
- 命令注入
- SQL 注入
- 引发敏感信息泄露的错误
- 不可靠的密码系统应用
- 服务器错误配置
- 后门和调试选项
- 网站涂改
- 已知的平台漏洞
- 未知的应用攻击

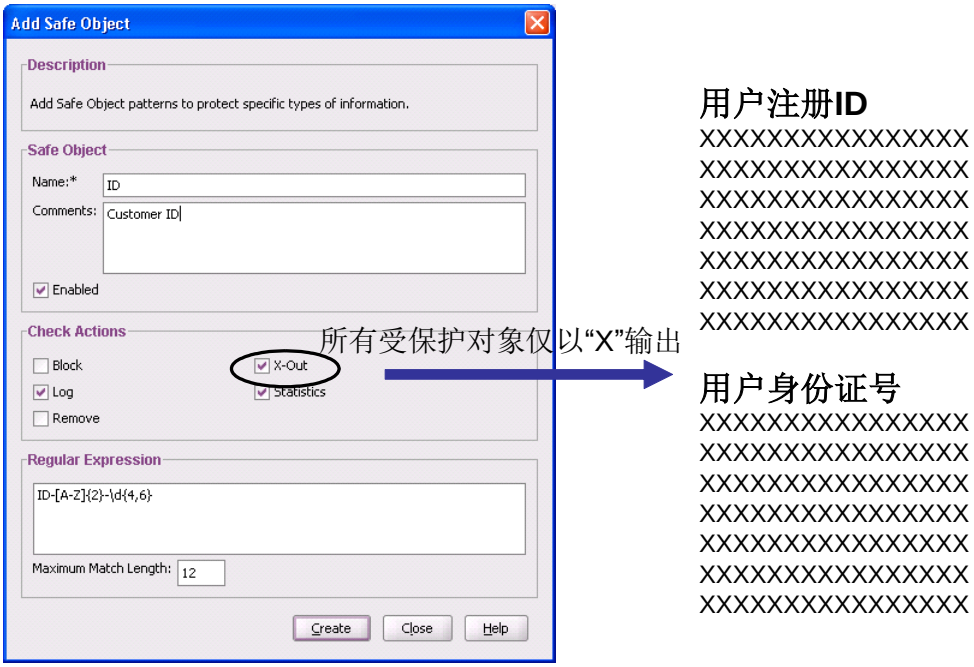
5.3.4.2 采用正向安全模型

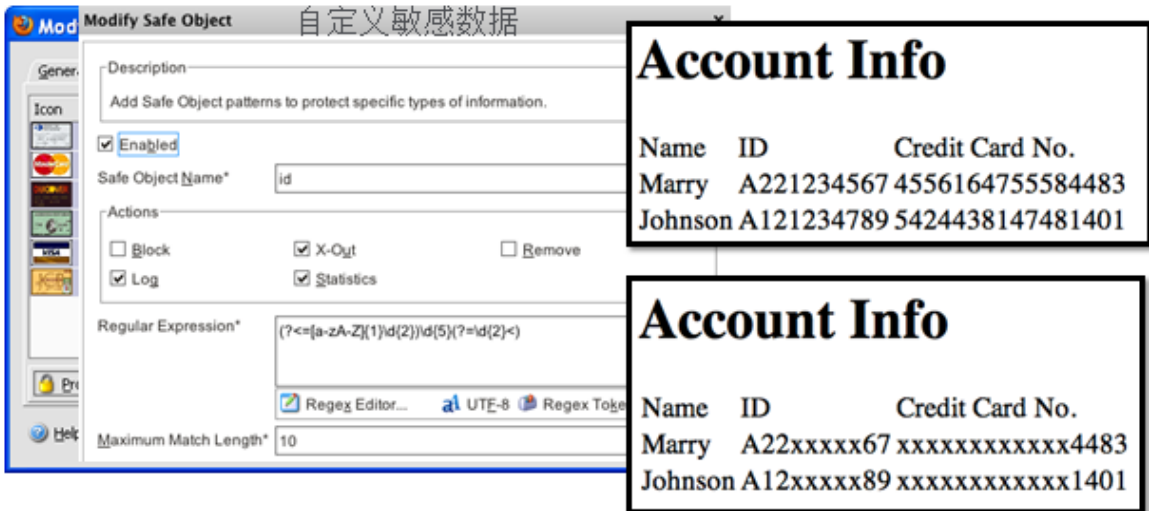
Citrix 应用防火墙 （Application Firewall）采用了正向安全模型来确

保执行正确的应用行为。这种安全模式不靠攻击特征符或签名匹配技术就能识别“合法”的应用行为，并阻止任何背离了正确应用交易模式的恶意行为。Citrix 应用防火墙（Application Firewall）是经过验证的可对从未出现过的攻击实施全天候防御的软件。

5.3.4.3业务对象保护模块

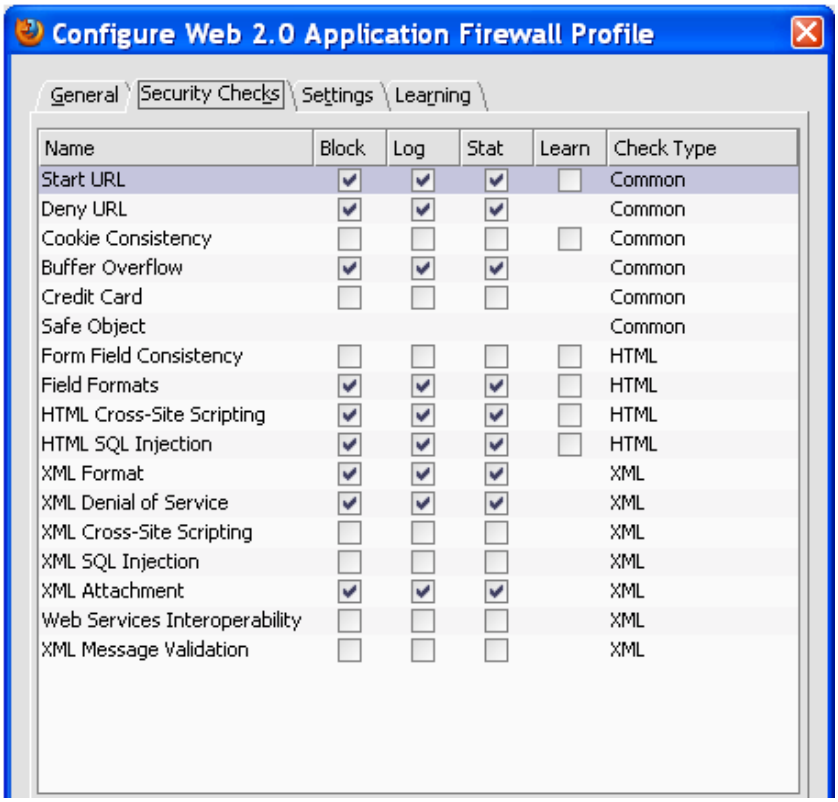
Citrix 应用防火墙（Application Firewall）实时阻止了敏感应用内容的无意泄露，这种无意的内容泄露会导致身份信息盗用行为。业务对象保护模块可保护像注册用户的账户信息等确定的对象以及其它自定义的数据对象的安全。通过检测错误泄露以及阻止或重写内容，业务对象保护模块协助企业满足了政府或行业委员会制定的行业法规。

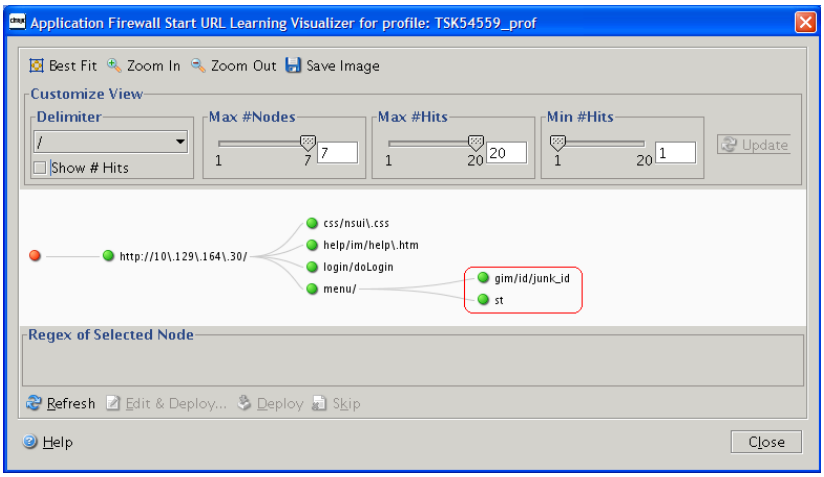


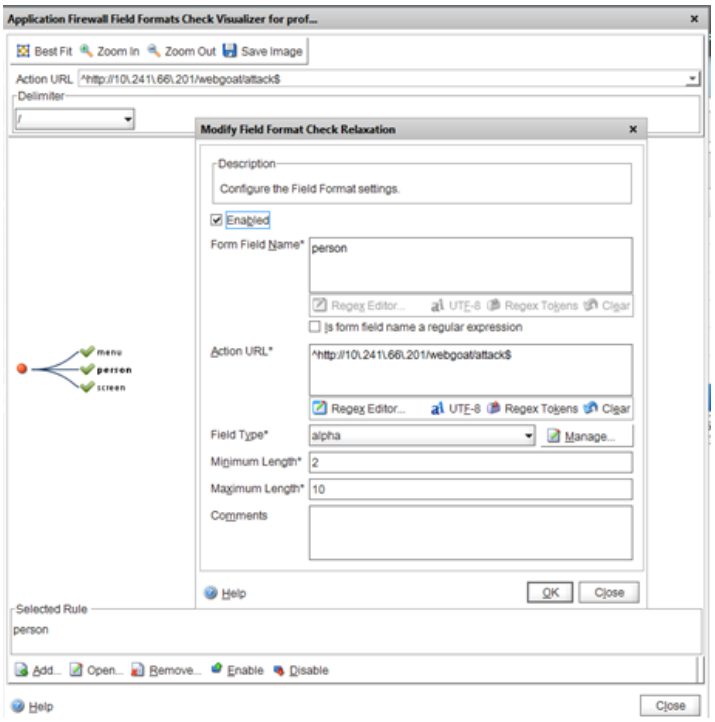


5.3.4.4 应用行为自学习引擎

Citrix 应用防火墙（Application Firewall）融合了第三代自学习引擎，这种引擎能学习到各个方面的应用行为，即使 Web 应用允许执行，这些行为也有可能会受到正向安全模型的阻止。一旦检测到应用行为，应用防火墙（Application Firewall）就会生成建议性可读策略，这会帮助应用安全部门能够更清楚地了解实际的应用行为，然后针对每个应用实施自定义安全策略。







5.3.4.5 应用处理性能

Citrix 应用防火墙（Application Firewall）的连接处理性能远远高过 Web 服务器，通过卸载 Web 服务器的 TCP 连接，应用防火墙有效地改善了应用性能和响应时间。应用防火墙与服务器之间的通信只采用了少量 TCP 常连接。

基于硅元件开发的专用 SSL 硬件可检测出加密信道中的恶意流量。通过减少服务器的加解密操作，SSL 加密和密钥生成 offload 改善了综合应用性能。

5.3.4.6分类保护 Web 应用的安全

Citrix 应用防火墙（Application Firewall）可利用每个 Web 应用的制定安全策略、控制、详细报告和记录数据来完全分离不同的交易，以确保企业每种 Web 应用能够得到量身定做的应用防护。

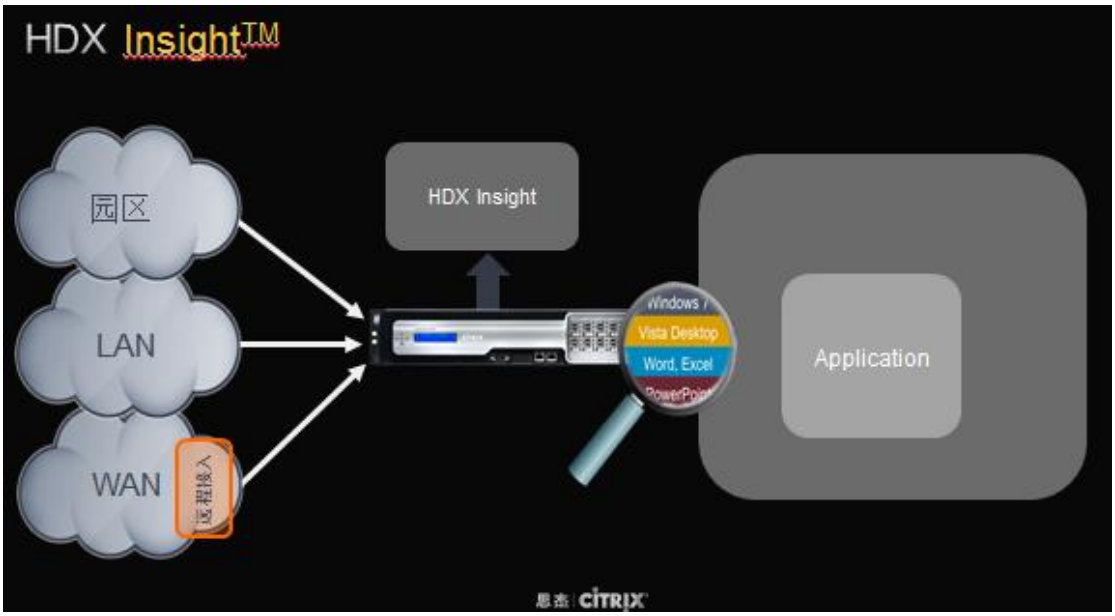
5.3.4.7 适应不断变化的业务需求

高级 Web 应用保护配置增加了高级 Web 应用的会话层分析保护功能，此高级 Web 应用包括了对敏感数据的已验证访问。而且保护范围扩展到 Cookie、格式字段和会话专用 URL 等动态生成的元素。这种保护对于电子商务、在线金融服务和安全的外联网应用都是强制性的，并且它还具备应用学习能力，针对行为可能会违背默认安全策略的某些应用帮助管理员创建安全策略的可管理例外。

5.3.5 SSL VPN

当用户需要远程访问和管理自己的 Web 站点时，无需额外的远程客户端软件，而直接采用普通的客户端技术即可为远程用户提供全面的、安全的远程接入技术，同时采用了行业标准的 SSL 技术保护机密内容。NetScaler SSL VPN 技术允许终端用户远程访问任何应用，包括非 Web 客户端/服务器应用在内。

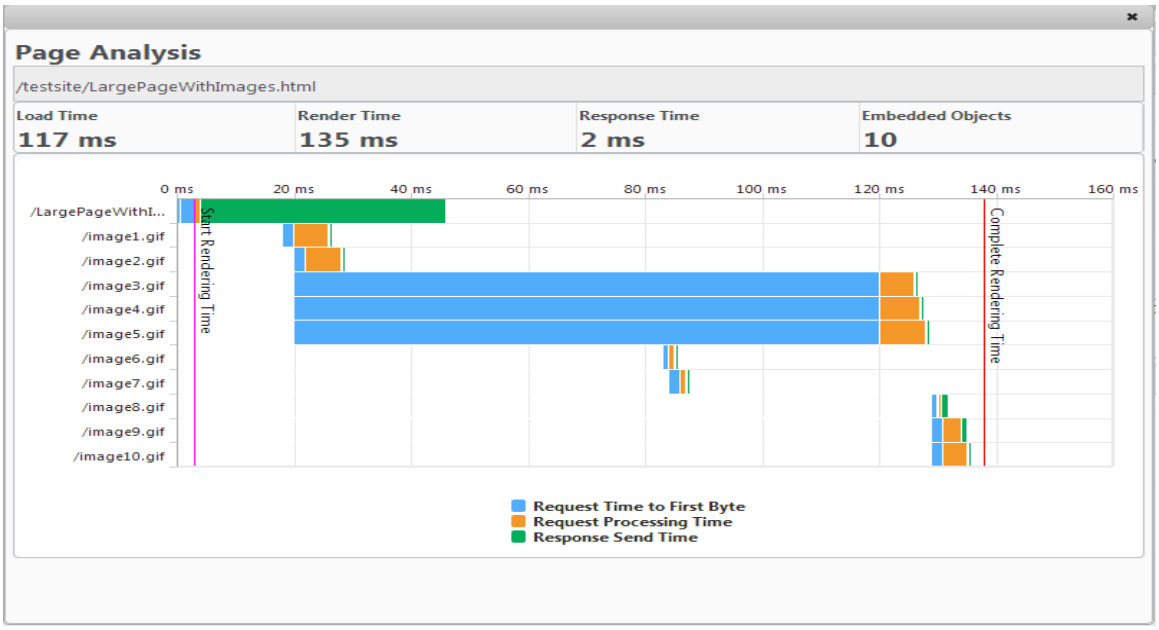
5.4 HDX Insight 用户体验监控功能

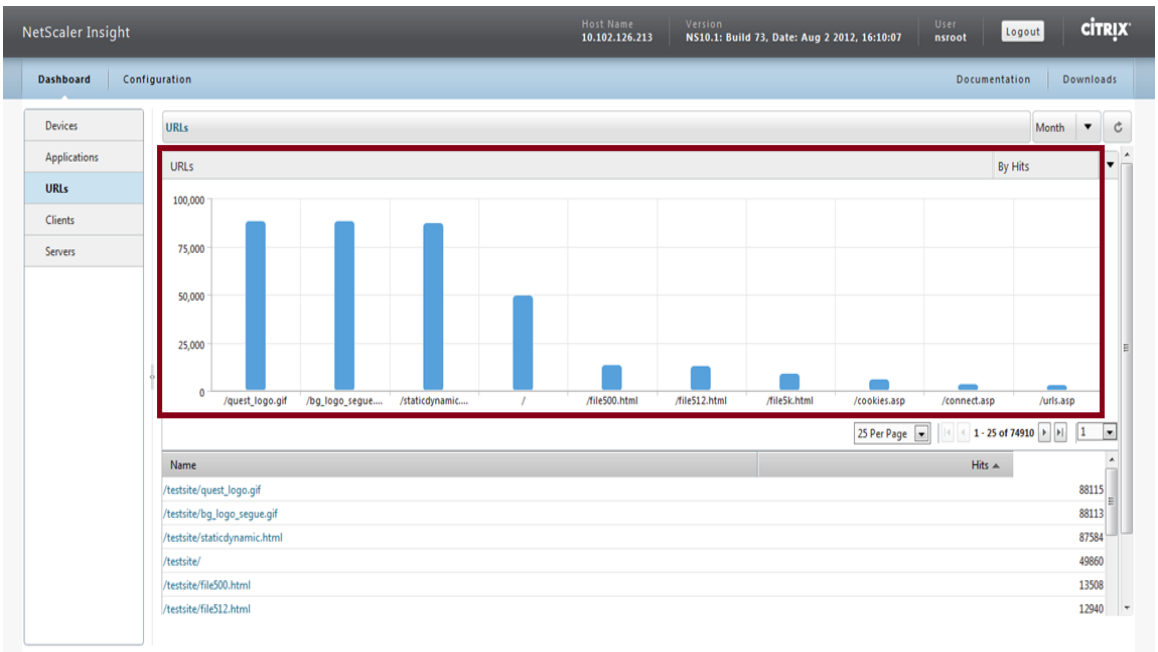


当交易请求和响应通过 Web 应用交付基础架构以及在终端用户的 Web 浏览器上执行响应时，HDX Insight 都能够透明地监测 Web 应用性能。通过直接监测 Web 应用交付基础架构和网页本身，HDX Insight 为 IT 管理人员提供了影

响应用性能的重要因素的独特的细粒度可视性。

当应用性能出现异常时，NetScaler 还可以提供定量的报告，帮助运维人员定位出故障出现在服务器，网络还是客户端。





6 产品性能数据表

特性	铂金版	企业版	标准版
应用可用性			
4 层负载均衡和 7 层内容交换	●	●	●
数据库负载均衡	●	●	●
AppExpert 速率控制	●	●	●
IPv6 支持	●	●	●
全局负载均衡（GSLB）	●	●	○
动态路由协议	●	●	
浪涌保护和优先队列	●	●	
TriScale™ 群集	○	○	○
应用加速			
客户端和服务器 TCP 优化	●	●	●
Citrix® AppCompress™ for HTTP	●	●	○
Citrix® AppCache™	●	○	
NetScaler CloudConnectors™	○	○	○
Citrix® Branch Repeater™ 客户端	●		
应用安全性			
4 层 DoS 攻击防护	●	●	●
7 层内容过滤和 HTTP/ URL 重写	●	●	●
NetScaler Gateway™, SSL VPN	●	●	●
XenMobile NetScaler Connector	●	●	●
支持 SAML2	●	●	●
7 层 DoS 攻击防护	●	●	
流量管理 AAA	●	●	
思杰应用防火墙并包括 XML 安全防护	●	○	
NetScaler Cloud Bridge	●		
简单的管理			
AppFlow™	●	●	●
AppExpert 可视化策略生成器	●	●	●
ActionAnalytics（行为分析）	●	●	●
AppExpert service callouts，模板和 Visualizers	●	●	●
基于角色的管理和 AAA 管理	●	●	●
配置向导	●	●	●
本地 Citrix Web Interface	●	●	●
思杰控制中心	●	●	
Citrix® EdgeSight® for NetScaler	●	○	
Web 2.0 优化			
Rich Internet 应用支持和 XML XPath 支持	●	●	●
高级服务器卸载	●	●	
降低 TCO			
TCP 缓冲	●	●	●
TCP 和 SQL 连接复用	●	●	●
SSL 卸载和加速	●	●	●
缓存重定向，包括多层支持	●	●	

● = 标准 ○ = 可选

注：独立购买选项不适用于 NetScaler VPX 虚拟设备。

NetScaler 平台	MPX 22120	MPX 22100	MPX 22080	MPX 22060	MPX 22040
平台属性					
处理器	双 Intel E5-2690 处理器	双 Intel E5-2690 处理器	双 Intel E5-2690 处理器	双 Intel E5-2690 处理器	双 Intel E5-2690 处理器
内存	256 GB	256 GB	256 GB	256 GB	256 GB
存储类型	HDD + SSD	HDD + SSD	HDD + SSD	HDD + SSD	HDD + SSD
以太网端口	24x10GBASE-X SFP+ 或 24x10GBASE-X SFP+ 和12x1000BASE-X SFP（光纤或铜缆）(NEBS/T)	24x10GBASE-X SFP+ 或 24x10GBASE-X SFP+ 和12x1000BASE-X SFP（光纤或铜缆）(NEBS/T)	24x10GBASE-X SFP+ 或 24x10GBASE-X SFP+ 和12x1000BASE-X SFP（光纤或铜缆）(NEBS/T)	24x10GBASE-X SFP+ 或 24x10GBASE-X SFP+ 和12x1000BASE-X SFP（光纤或铜缆）(NEBS/T)	24x10GBASE-X SFP+ 或 24x10GBASE-X SFP+ 和12x1000BASE-X SFP（光纤或铜缆）(NEBS/T)
收发器支持	10GE SFP+：SR，LR 1 GE SFP：SX，LX	10GE SFP+：SR，LR 1 GE SFP：SX，LX	10GE SFP+：SR，LR 1 GE SFP：SX，LX	10GE SFP+：SR，LR 1 GE SFP：SX，LX	10GE SFP+：SR，LR 1 GE SFP：SX，LX
按需付费（Pay as you grow）和 BurstPack 许可证升级		可选择升级到 MPX 22120	可选择升级到 MPX 22100 MPX 22120	可选择升级到 MPX 22080 MPX 22100 MPX 22120	可选择升级到 MPX 22060 MPX 22080 MPX 22100 MPX 22120
平台性能					
系统吞吐量（Gbps）	120	100	80	60	40
HTTP 请求/秒	4,700,000	4,500,000	4,000,000	3,500,000	2,600,000
TCP 新建连接/秒	8,500,000	8,000,000	7,000,000	6,400,000	4,800,000
SSL交易/秒（2K 密钥证书）	560,000 155,000 (NEBS)	460,000 130,000 (NEBS)	340,000 80,000 (NEBS)	225,000 65,000 (NEBS)	120,000 40,000 (NEBS)
SSL 吞吐量（Gbps）	75 42 (NEBS)	65 35 (NEBS)	55 30 (NEBS)	45 22 (NEBS)	35 18 (NEBS)
压缩吞吐量（Gbps）	14.7	14	12.5	11	8
最大实例数（SDX 机型）	不适用	不适用	不适用	不适用	不适用
平台机械、环境和规格					
电源	双电源	双电源	双电源	双电源	双电源
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz
可选 DC 电源	支持	支持	支持	支持	支持
最大功耗	1100w 3753 BTU/Hr	1100w 3753 BTU/Hr	1100w 3753 BTU/Hr	1100w 3753 BTU/Hr	1100w 3753 BTU/Hr
一般功耗	850W 2900 BTU/Hr	850W 2900 BTU/Hr	850W 2900 BTU/Hr	850W 2900 BTU/Hr	850W 2900 BTU/Hr
重量（磅）	58	58	58	58	58
高度	2U	2U	2U	2U	2U
宽度	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架
深度	28” / 71.2 cm	28” / 71.2 cm	28” / 71.2 cm	28” / 71.2 cm	28” / 71.2 cm
运行温度	0-40C	0-40C	0-40C	0-40C	0-40C
允许的相对湿度	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝
安全性认证	CSA	CSA	CSA	CSA	CSA
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES
合规性	符合 RoHS; NEBS Level 3	符合 RoHS; NEBS Level 3	符合 RoHS; NEBS Level 3	符合 RoHS; NEBS Level 3	符合 RoHS; NEBS Level 3

NetScaler 平台	MPX/SDX[1] 21550	MPX/SDX[1] 20550	MPX/SDX[1] 19550	MPX/SDX[1] 17550
平台属性				
处理器	双 Intel X5680 处理器	双 Intel X5680 处理器	双 Intel X5680 处理器	双 Intel X5680 处理器
内存	96 GB	96 GB	96 GB	96 GB
存储类型	HDD + SSD	HDD + SSD	HDD + SSD	HDD + SSD
以太网端口	8x 10GBASE-X SFP+	8x 10GBASE-X SFP+	8x 10GBASE-X SFP+	8x 10GBASE-X SFP+
收发器支持	10GE SFP+：SR，LR	10GE SFP+：SR，LR	10GE SFP+：SR，LR	10GE SFP+：SR，LR
按需付费（Pay as you grow）和 BurstPack 许可证升级		可选择升级到 MPX/SDX 21550	可选择升级到 MPX/SDX 20550 MPX/SDX 21550	可选择升级到 MPX/SDX 19550 MPX/SDX 20550 MPX/SDX 21550
平台性能				
系统吞吐量（Gbps）	50	40	30	20
HTTP 请求/秒	3,700,000	3,500,000	3,000,000	2,400,000
TCP 新建连接/秒	5,500,000	5,000,000	4,500,000	4,000,000
SSL 交易/秒（2K 密钥证书）	98,000	73,000（MPX）68,000（SDX）	50,000	33,000
SSL 吞吐量（Gbps）	11	10	9	8
压缩吞吐量（Gbps）	11（MPX）/ 10（SDX）	9	8	7
最大实例数（SDX 机型）	40	40	40	40
平台机械、环境和规格				
电源	双电源	双电源	双电源	双电源
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz
可选 DC 电源	支持	支持	支持	支持
最大功耗	850w 2219 BTU/Hr	850w 2219 BTU/Hr	850w 2219 BTU/Hr	850w 2219 BTU/Hr
一般功耗	570W 1945 BTU/Hr	570W 1945 BTU/Hr	570W 1945 BTU/Hr	570W 1945 BTU/Hr
重量（磅）	49	49	49	49
高度	2U	2U	2U	2U
宽度	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架
深度	28” / 71.2 cm	28” / 71.2 cm	28” / 71.2 cm	28” / 71.2 cm
运行温度	0-40C	0-40C	0-40C	0-40C
允许的相对湿度	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝
安全性认证	CSA	CSA	CSA	CSA
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES
合规性	RoHS	RoHS	RoHS	RoHS

NetScaler 平台	MPX/SDX[1] 20500	MPX/SDX[1] 18500	MPX/SDX[1] 16500
平台属性			
处理器	双 Intel Xeon E5645 处理	双 Intel Xeon E5645 处理器	双 Intel Xeon E5645 处理器
内存	48 GB	48 GB	48 GB
存储类型	HDD + SSD	HDD + SSD	HDD + SSD
以太网端口	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）
收发器支持	10 GE SFP+：SR，LR 1 GE SFP：SX，LX	10 GE SFP+：SR，LR； 1 GE SFP：SX，LX	10 GE SFP+：SR，LR； 1 GE SFP：SX，LX
按需付费（Pay as you grow）和 BurstPack 许可证升级		可选择升级到 MPX /SDX 20500	可选择升级到 MPX / SDX 18500 MPX / SDX 20500
平台性能			
系统吞吐量（Gbps）	42	36	24
HTTP 请求/秒（MPX/SDX）	2,700,000 / 2,300,000	2,500,000	2,000,000
TCP 新建连接/秒	4,200,000	3,500,000	3,500,000
SSL 交易/秒 （2K 密钥证书）	45,000	34,000	28,000
SSL吞吐量（Gbps）	11 / 10.4	10.5	10
压缩吞吐量（Gbps）	8 / 7.1	7.0	6.0
最大实例数（SDX 机型）	20	20	20
平台机械、环境和规格			
电源	双电源	双电源	双电源
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz
可选 DC 电源	支持	支持	支持
最大功耗	650w 2219 BTU/Hr	650w 2219 BTU/Hr	650w 2219 BTU/Hr
一般功耗	500W 1706 BTU/Hr	500W 1706 BTU/Hr	500W 1706 BTU/Hr
重量（磅）	45	45	45
高度	2U	2U	2U
宽度	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架
深度	28” / 71 cm	28” /71 cm	28”/71 cm
运行温度	0-40C	0-40C	0-40C
允许的相对湿度	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝
安全性认证	CSA	CSA	CSA
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC，CE，VCCI，CNS， AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS， AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS， AN/NES
合规性	符合 RoHS；NEBS Level 3 要求	符合 RoHS；NEBS Level 3 要求	符合 RoHS；NEBS Level 3 要求

NetScaler 平台	MPX/SDX[1]14500	MPX / SDX[1] 13500	MPX / SDX1 11500
平台属性			
处理器	双 Intel Xeon E5645 处理器	双 Intel Xeon E5645 处理器	双 Intel Xeon E5645 处理器
内存	48 GB	48 GB	48 GB
存储类型	HDD + SSD	HDD + SSD	HDD + SSD
以太网端口	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）	4x 10GBASE-X SFP+ 和 8x 1000BASE-X SFP （光接口或铜接口）
收发器支持	10 GE SFP+：SR，LR； 1 GE SFP：SX，LX	10 GE SFP+：SR，LR 1 GE SFP：SX，LX	10 GE SFP+：SR，LR 1 GE SFP：SX，LX
按需付费（Pay as you grow）和 BurstPack 许可证升级	可选择升级到 MPX / SDX 16500 MPX / SDX 18500 MPX / SDX 20500	可选择升级到 MPX / SDX 14500 MPX / SDX 16500 MPX / SDX 18500 MPX / SDX 20500	可选择升级到 MPX / SDX 13500 MPX / SDX 14500 MPX / SDX 16500 MPX / SDX 18500 MPX / SDX 20500
平台性能			
系统吞吐量（Gbps）	18	12	8
HTTP 请求/秒（MPX/SDX）	1,800,000	1,600,000	1,200,000
TCP 新建连接/秒	2,600,000	1,300,000	1,000,000
SSL交易/秒 （2K 密钥证书）	22,000	19,000	15,000
SSL 吞吐量（Gbps）	7	6.5	6
压缩吞吐量（Gbps）	5	4.5	3.5
最大实例数（SDX 机型）	20	20	20
平台机械、环境和规格			
电源	双电源	双电源	双电源
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz
可选 DC 电源	支持	支持	支持
最大功耗	650w 2219 BTU/Hr	650w 2219 BTU/Hr	650W 2219 BTU/Hr
一般功耗	500W 1706 BTU/Hr	500W 1706 BTU/Hr	500W 1706 BTU/Hr
重量（磅）	45	45	45
高度	2U	2U	2U
宽度	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297， DIN 41494 SC48D 机架宽度，带安装支架
深度	28”/71 cmm	28”/71 cm	28”/71 cm
运行温度	0-40C	0-40C	0-40C
允许的相对湿度	5%-95%，无冷凝	5%-95%，无冷凝	5%-95%，无冷凝
安全性认证	CSA	CSA	CSA
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES
合规性	符合 RoHS；NEBS Level 3 要求	符合 RoHS；NEBS Level 3 要求	符合 RoHS；NEBS Level 3 要求

NetScaler 平台	MPX/SDX 8800	MPX/SDX 8600	MPX/SDX 8400	MPX 8200
平台属性				
处理器	Intel E3-1275 处理器	Intel E3-1275 处理器	Intel E3-1275 处理器	Intel E3-1275 处理器
内存	32 GB	32 GB	32 GB	32 GB
存储类型	SSD	SSD	SSD	SSD
以太网端口	6x 10/100/1000 BASE-T 和 6x1000BASE-X SFP（光接口或铜接口） 或 6x 10/100/1000 BASE-T 和 2x10G BASE-X SFP+	6x 10/100/1000 BASE-T 和 6x1000BASE-X SFP（光接口或铜接口） 或 6x 10/100/1000 BASE-T 和 2x10G BASE-X SFP+	6x 10/100/1000 BASE-T 和 6x1000BASE-X SFP（光接口或铜接口） 或 6x 10/100/1000 BASE-T 和 2x10G BASE-X SFP+	6x 10/100/1000 BASE-T 和 6x1000BASE-X SFP（光接口或铜接口） 或 6x 10/100/1000 BASE-T 和 2x10G BASE-X SFP+
收发器支持	10GE SFP+: SR, LR; 1 GE SFP: SX, LX	10GE SFP+: SR, LR; 1 GE SFP: SX, LX	10GE SFP+: SR, LR; 1 GE SFP: SX, LX	10GE SFP+: SR, LR; 1 GE SFP: SX, LX
按需付费（Pay as you grow）和 BurstPack 许可证升级		可选择升级到 MPX 8800	可选择升级到 MPX 8600 MPX 8800	可选择升级到 MPX 8400 MPX 8600 MPX 8800
平台性能				
系统吞吐量（Gbps）	8	6	4	2
HTTP 请求/秒	1,000,000	900,000	600,000	350,000
TCP 新建连接/秒	900,000	770,000	400,000	250,000
SSL 交易/秒（2K 密钥证书）	11,000	9,000(MPX) 10,000(SDX)	7,600(MPX) 8,000(SDX)	6,500
SSL吞吐量（Gbps）	6	5.5	4(MPX) 3.5(SDX)	2
压缩吞吐量（Gbps）	3.5	3.2	2.4	2
最大实例数（SDX 机型）	5	5	5	不适用
平台机械、环境和规格				
电源	单电源 加可选的第 2 套备用电源	单电源 加可选的第 2 套备用电源	单电源 加可选的第 2 套备用电源	单电源 加可选的第 2 套备用电源
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz
可选 DC 电源	支持	支持	支持	支持
最大功耗	250W 853 BTU/Hr	250W 853 BTU/Hr	250W 853 BTU/Hr	250W 853 BTU/Hr
一般功耗	185W 631 BTU/Hr	185W 631 BTU/Hr	185W 631 BTU/Hr	185W 631 BTU/Hr
重量（磅）	32	32	32	32
高度	1U	1U	1U	1U
宽度	EIA 310-D, IEC 60297, DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D, IEC 60297, DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D, IEC 60297, DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D, IEC 60297, DIN 41494 SC48D 机架宽度，带安装支架
深度	24" / 61 cm	24" / 61 cm	24" / 61 cm	24" / 61 cm
运行温度	0-40C	0-40C	0-40C	0-40C
允许的相对湿度	10%-90%，无冷凝	10%-90%，无冷凝	10%-90%，无冷凝	10%-90%，无冷凝
安全性认证	CSA	CSA	CSA	CSA
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES	FCC（Part 15 Class A），DoC, CE, VCCI, CNS, AN/NES
合规性	RoHS	RoHS	RoHS	RoHS

NetScaler 平台	MPX 5650	MPX5550	VPX 10/200/1000/3000
平台属性			
处理器	Intel E3-1225 处理器	Intel E3-1225 处理器	最低服务器要求：双核服务器[2]，CPU 支持 Intel® VTx 或 AMD-V™ 技术 • Citrix® XenServer™ 5（update 3 或更高版本） • Windows Server 2008 R2，带 Hyper-V • VMWare ESX/ESXi 3.5 或更高版 • 4G RAM/20 GB 硬盘 • 虚拟化引擎支持的 NIC
内存	8 GB	8 GB	
以太网端口	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T	
收发器支持			
按需付费（Pay as you grow）和 BurstPack 许可证升级		可选择升级到 MPX 5650	可选择升级到 VPX 200， VPX 1000 和 VPX 3000
平台性能			
系统吞吐量（Gbps）	1	0.5	最高 3.0[3] 最高 100,000
HTTP 请求/秒	250,000	175,000	
TCP 新建连接/秒	168,000	117,000	
SSL 交易/秒 （2K 密钥证书）	10,000 / 2,000	7,500 / 1,500	最高 100
SSL 吞吐量（Gbps）	1	0.5	最高 1.0
压缩吞吐量（Gbps）	1	0.5	最高 0.75
最大实例数（SDX 机型）	不适用	不适用	不适用
平台机械、环境和规格			
电源	单电源	单电源	取决于选择的服务器平台
输入电压和频率范围	100-240VAC，全范围，47-63 Hz	100-240VAC，全范围，47-63 Hz	
可选 DC 电源	无	无	
功率消耗	300w 1110 BTU/Hr	300w 1110 BTU/Hr	
重量（磅）	32	32	
高度	1U	1U	
宽度	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	EIA 310-D，IEC 60297，DIN 41494 SC48D 机架宽度，带安装支架	
深度	24” / 61 cm	24” / 61 cm	
运行温度	0-40C	0-40C	
允许的相对湿度	10%-90%，无冷凝	10%-90%，无冷凝	
安全性认证	CSA	CSA	
电磁辐射认证和敏感度标准	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	FCC（Part 15 Class A），DoC，CE，VCCI，CNS，AN/NES	
合规性	RoHS	RoHS	

技术规范

4 层-7 层流量管理

4 层负载均衡（LB）

- 支持的协议 TCP，UDP，FTP，HTTP，HTTPS，DNS（TCP 和 UDP），SIP（over UDP），RTSP，RADIUS，DIAMETER，SQL，RDP，IS-IS
- 算法：循环算法，最少包，最低带宽，最少连接，响应时间，散列（URL，域，源地址 IP，目的 IP 和 CustomID），SNMP 协议度量，服务器应用状态协议（SASP）
- 会话保持：源地址，cookie，服务器，组，SSL 会话，SIP CALLID，令牌，JSESSIONID
- 会话协议：TCP，UDP，SSL_TCP，Multipath TCP，SPDY
- 服务器监控：Ping，TCP，URL，ECV，基于脚本的健康检查，动态服务器响应时间
- 链路负载均衡
- Citrix Branch Repeater 负载均衡

7 层内容交换

- 策略：URL，URL Query，URL 通配符，域，源 / 目的 IP，HTTP 报头，Custom，HTTP 和 TCP 有效负载值，UDP
- 基于输入数据包协议的交换请求

数据库负载均衡

- 支持：Microsoft SQL Server 和 MySQL
- 内容交换算法包括用户和数据库名称等 SQL 查询参数和命令参数
- 基于令牌的负载均衡功能，可提供高级配置来支持持久性和容错部署

TriScale 群集[8]

- “向外扩展（Scale-Out）”，可将最多 32 台 NetScaler 设备群集部署到单一系统镜像中
- Configuration Coordinator 节点支持集中管理和同步
- 可兼容“按需付费（Pay-As-You-Grow）”和 Burst Pack 性能升级
- 流量分配机制包括：Equal Cost Multiple Path（ECMP）、Linksets 和 Cluster Link Aggregation Group（CLAG）
- 适用于 NetScaler MPX，SDX 和 VPX 的各种版本
- 模块可以配置在集群内所有节点上，也可以通过“spotted VIPS”只添加到所选的部分节点上

基于速率的策略实施

- 根据每秒连接数、每秒数据包数或使用的带宽触发 NetScaler 策略
- 基于报头或有效负载信息的源或目标

流量域（Traffic Domains）

- 允许重叠 IP 地址
- 在单一设备中支持独立的路由数据流
- 实现基本的多租户实施

全局负载均衡（GSLB）

- 算法：站点健康，地理接近性，网络接近性，连接，带宽，AG-E SSL VPN 用户
- 站点健康状态检查，连接负载，数据包速 率，SNMP 协议度量

浪涌保护和优先级排队[6]

- TCP 连接和 HTTP 请求的自适应速率控制
- 关键应用请求的优先交易发送

应用加速

TCP 优化

- 复用，缓冲，连接保活（Connection Keep-alive），窗口缩放，选择性确认，Fast Ramp，TCP Westwood

Appcompress

- 基于 Gzip 的 HTTP 流量 AppCache 压缩[5]
- 静态和动态应用内容高速缓存
- HTTP GET 和 POST 方法支持
- 根据 HTTP 报头和正文值定义策略

NetScaler CloudConnectors

- 现场（On-premise）代理，提供对称 TCP 优化、数据压缩和重复数据删除功能
- 在 NetScaler MPX、SDX 和 VPX 上提供

应用安全性

DoS 攻击防护

- 在防止以下攻击的同时继续为合法用户提供服务：SYN Flood，HTTP DoS 和 Ping of Death
- ICMP 和 UDP 速率控制

内容改写和响应控制

- 基于策略的 HTTP 报头和有效负载信息双向改写
- 基于策略的传入的请求重定向
- Body URL 改写
- Responder 模块
- 定制响应和重定向
- 策略路由
- 网络感知策略

DNSSEC

- DNS 代理
- 权威 DNS
- DNS 签名

数据包过滤

- 3 层和 4 层访问控制列表（ACL）
- 网络地址转换（NAT）
- IPv4/IPv6 网络地址转换（NAT）

NetScaler 应用防火墙，混合安全模式[6]

- 有效的安全模式可防止：缓冲区溢出，CGI-BIN 参数处理，表格 / 隐藏字段处理，强制浏览，信息块或会话中毒，Broken ACL，跨站点脚本编写（XSS），命令注入，SQL Injection，引发敏感信息泄露的错误，不可靠的密码系统应用，Server Misconfiguration，后门和调试选项，基于速率的策略实施，Well-known Platform Vulnerabilities，零时差攻击，跨站请求伪造（CSRF）、信用卡和其它敏感数据泄露防止。
- 基于签名的安全模式，可防止 L7 和 HTTP 应用漏洞。
- 与第三方扫描工具相集成
- 通用事件格式（CEF）日志
- XML 安全：XML 拒绝服务（xDoS），
- XML SQL injection 和跨站点脚本编写 XML 消息验证，格式检查，WS-I 基本配置文件合规性，XML、xPath Injection Attachment 检查、X Query Injection 保护
- WSDL 扫描防护
- 附件检查
- URL 转换
- Cookie 代理和加密
- SOAP 数组攻击保护

安全的远程访问

- 集成 Citrix NetScaler Gateway 企业版 SSL VPN
- 端点分析
- SAML 双因子验证和客户端证书验证；NetScaler 中保存的单点登录后台服务的密码
- 客户端侧高速缓存清除
- 安全证书
- 7 层内容过滤
- AAA 流量管理
- 支持 SAML2 和 NTLMv1/2，通过单点登录（SSO）配置 NetScaler
- Active Directory，LDAP，RADIUS，TACACS +，OCSP

NetScaler Cloud Bridge[7]

- 通过 IPSec 安全性实现的网络连接保护
- 通过基于 GRE 的网络桥接实现数据中心扩展

支持XenMobile MDM[9]

- 前端优化，可扩展用于支持 100,000 多名并发用户
- XenMobile NetScaler Connector（XNC）可提供设备级授权服务
- 应用级策略控制的 SSL VPN 隧道，用于支持移动客户端

技术规范

网络集成

- 静态路由，受监控的静态路由，加权静态路由
- OSPF，RIP1/2，BGP5
- VLAN 802.1Q
- 链路聚合 802.3ad
- IPv6 到 IPv4 的 Stateful 网络地址转换和 DNS64
- 从 IPv4 到 IPv6 的静态和无状态网络地址转换

高可用性

- 主动 / 被动
- 主动 / 主动
- VRRP
- ECMP
- 连接镜像

简化的安装和管理

用户界面

- 图形应用显示器
- 基于 Web 的安全 GUI
- CLI，Telnet，SSH，控制台
- 实时性能视图
- LB，GSLB 应用防火墙和 EdgeSight for NetScaler 配置向导
- Citrix® XenApp® 配置向导

策略管理

- AppExpert 可视化策略生成器
- 通过 HTTP 服务请求的策略扩展
- AppExpert 模板
- AppExpert Visualizers

思杰控制中心[6]

- 200 多台 NetScaler 设备的集中配置和管理

NetScaler Insight Center和AppFlow：

- NetScaler Insight Center 是一种可实现流量可视性的软件解决方案，包括 HDX Insight 和 Web Insight，基于 AppFlow。
- HDX Insight 对 ICA 会话进行分析，为 XenApp/XenDesktop 会话提供故障排除、网络分析和端到端性能。铂金版可提供历史统计数据
- Web Insight 可监控实时 Web 应用流量，帮助进行容量规划并确保达到服务水平协议（SLA）要求。
- AppFlow 基于标准的 NetFlow/IPFIX（Internet Protocol Flow Information Export）解决方案
- 由领先的性能监控和管理厂商提供支持
- 为 HTTP、SSL、TCP 和 SSL/TCP 流量提供交易可视性

ActionAnalytics（行为分析）

- 汇聚实时流量统计数据，并用于制定动态策略
- 图表制作和分析工具

EdgeSight for NetScaler[6]

- 实时和历史用户体验监控
- Web 应用性能服务水平管理的趋势分析和报告

第 3 方管理支持

- SNMPv1、SNMPv2 和 SNMPv3：NetScaler MIB 和 MIB-II 支持
- Microsoft System Center Operations Management（SCOM）支持
- Manager（SCVMM）支持
- XML/SOAP API 实现自动应用驱动配置

实时整合日志

- 将日志功能从多台应用服务器卸载到集中的管理服务器上

原生 Web Interface

- Citrix XenApp 和 XenDesktop 的集成 Web Interface Server
- 支持 JAVA 环境，MPX 和 VPX 平台运行 NetScaler nCore OS
- 验证方式包括：LDAP、RADIUS、NTLM、TACACS+、Client Certificate
- 通过内置的 SSL VPN 管理 HTTPS 请求
- 通过 NetScaler GUI 根据向导进行配置
- 登录页定制
- 包括 Smart Access、平滑漫游、STA 服务器冗余和会话可靠性

降低总体拥有成本

缓存重定向[6]

- 自动将内容未缓存在 NetScaler 上 的请求定向到缓存服务器集群
- 高速缓存服务器支持多层负载均衡

注：

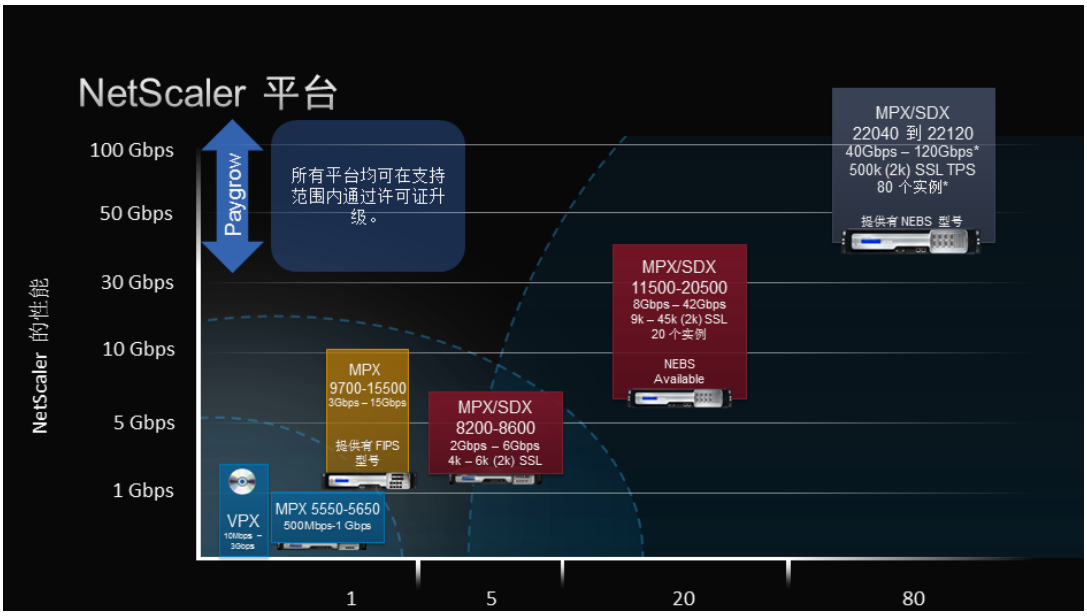
1. 每秒 SQL 请求数（RPS）在某些型号中受速率限制。VPX 10 到 VPX 1000：200。MPX 5500、5550、5650、7500 和 9500：1000。MPX 8200：2000。MPX 8400 和 8600：5000。所有其它型号无 SQL RPS 速率限制。
2. 各 SDX 型号带有铂金版许可证，包括 5 个 NetScaler 实例（SDX 8400 和 SDX 8600 除外，这两个型号包含 2 个实例）。思杰还提供包含 3 或 5 个实例的 NetScaler 包。所有实例均可配置用于任何 NetScaler 版本。
3. 所列硬件需求适用于 NetScaler VPX nCore 版本。
4. XenServer 和 Hyper-V 上运行的 VPX 的最大 HTTP 吞吐量最高为 3Gbps。
5. 使用 3DES 算法，使用 RC4 算法可支持最多 1,000 个并发用户。
6. 仅在 NetScaler Enterprise 和 Platinum 版中提供。
7. 仅在铂金版中提供；不适用于标准版或企业版。
8. 通过许可证升级在所有 MPX, SDX (包括 22000 系列) 和 VPX 设备版本中提供。
9. 推荐使用带 AppCache 的企业版或铂金版

7 Netscaler 帮助企业构建灵活的数据中心

当前，作为企业构建自有数据中心最重要的一点是“灵活”，能够随着业务的增长实现按需扩容，即帮助企业降低了总体拥有成本，又实现了绿色 IT。Citrix Netscaler 作为企业数据中心的一个重要组成的基础架构平台，能够从三个维度辅助企业构建一个灵活的数据中心。

7.1 向上扩展

在同一个硬件平台上通过 license 的更新来实现性能提升，不需要重新购买硬件。每款设备都有其所能提供的最大处理性能，超过该型号最大处理性能后需要进行设备型号更换，来满足更高的业务处理需求。Netscaler 提供了不同级别的硬件设备来满足用户的需求。



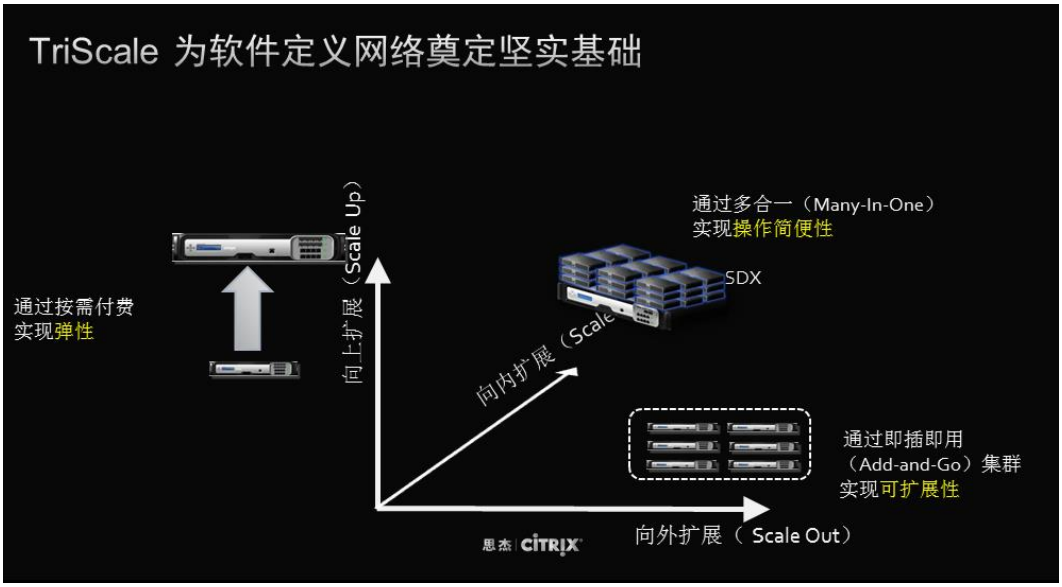
7.2 向内扩展

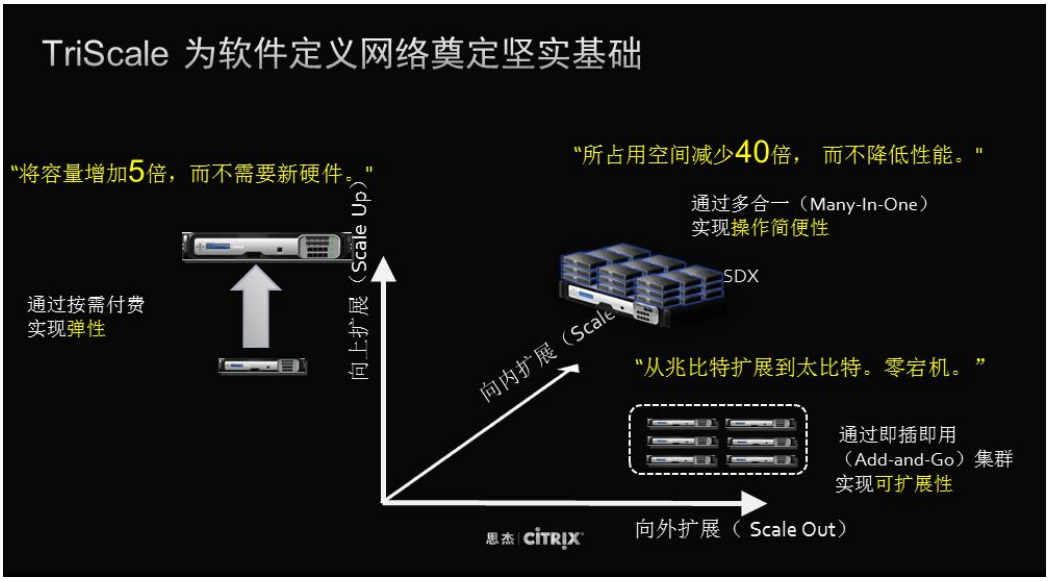
企业往往因为有多部门，多应用，多安全域的划分，所以针对每种情况，企业通常的做法是购买多个设备来部署到不同的应用前端，不同的区域中，实现 AND 的功能。这种做法往往要耗费更多的时间和成本，造成数据中心的空间浪费。Netscaler SDX 平台，通过在单一设备上创建多个虚拟实例来满足用户的需求，提供更好地性价比。SDX 最大的优势在于提供多实例的同时，每个实例都是相互独立的，硬件资源也是独立分配。任何一个虚拟实例的不可用都不会

影响其他虚拟实例的工作。

7.3 向外扩展

传统的设备部署模式均为两台设备主备部署或者双活部署，主备模式提供高可用，双活模式在提供高可用的同时，更好地提高设备利用率。但是，当业务增长到一定程度，主备或者双活模式均无法提供更好地服务。Netscaler Cluster 模式，将多台同型号的 Netscaler 绑定为一个集群，同时对外提供服务，即实现了高可用又实现了高性能处理。





综上所述，Netscaler Triscale 技术帮助企业更好地实现了数据中心的构建，为今后企业的数据中心向云计算数据中心发展提供更有利的基础平台架构。

8 产品部署方案

逻辑上位于客户端和服务器之间的 NetScaler 可以以两种物理模式部署：双臂模式和单臂模式。

8.1 双臂部署模式

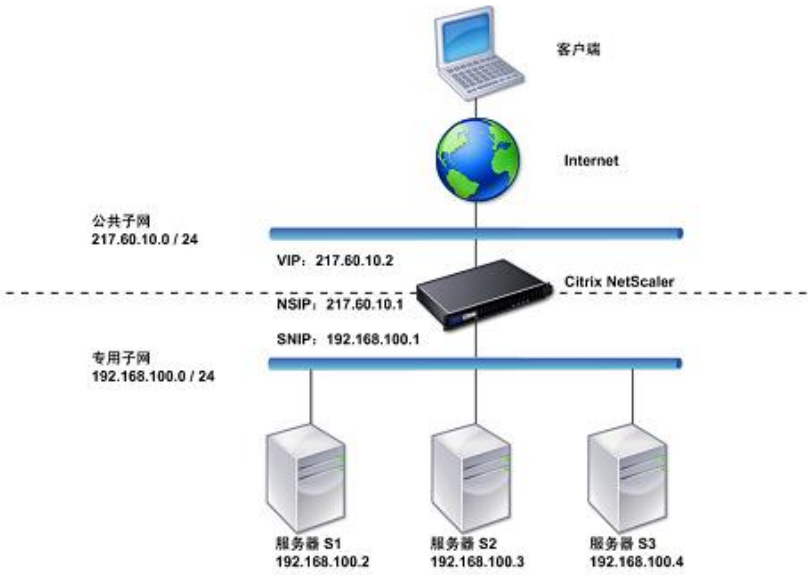
在双臂拓扑中，一个网络接口连接至客户端网络，另一个网络接口连接至服务器网络。此拓扑可能要求重新连接网络设备，但对网络中其它设备的配置所做的更改几乎可以忽略。

8.1.1 双臂多子网部署

这是一种最常用的拓扑，其中 NetScaler 内嵌放置在客户端和服务器之间，并配置一个虚拟服务器来处理客户端请求。此拓扑在客户端和服务器位于不同子网时使用。在大多数情况下，客户端和服务器分别位于公共和专用子网上。

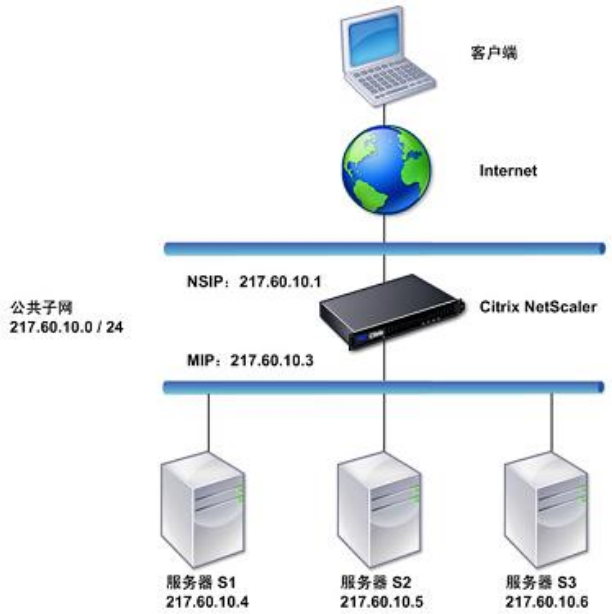
下图描述了以双臂模式部署 NetScaler 来管理服务器 S1、S2 和 S3 的方案。这些服务器位于公共网络上。NetScaler 上配置了一个 HTTP 类型的虚拟服务器，HTTP 服务运行在这些服务器上。这些服务器位于专用子网上，NetScaler 上配置了一个 SNIP 与这些服务器进行通信。

NSIP 和 VIP 位于公共子网 217.60.10.1 上。 SNIP 和这些服务器位于专用子网 192.168.100.1/24 上。



8.1.2 双臂透明部署

此拓扑在客户端需要直接访问服务器的情况下使用。此模式中不使用虚拟服务器。服务器 IP 地址必须为公共 IP，因为客户端需要它们。在此示例中，NetScaler 放置在客户端和服务器之间，因此流量必须经过 NetScaler。必须启用 L2 模式以桥接数据包。NSIP 和 MIP 位于同一公共子网 217.60.10.0/24 上，如下图所示：

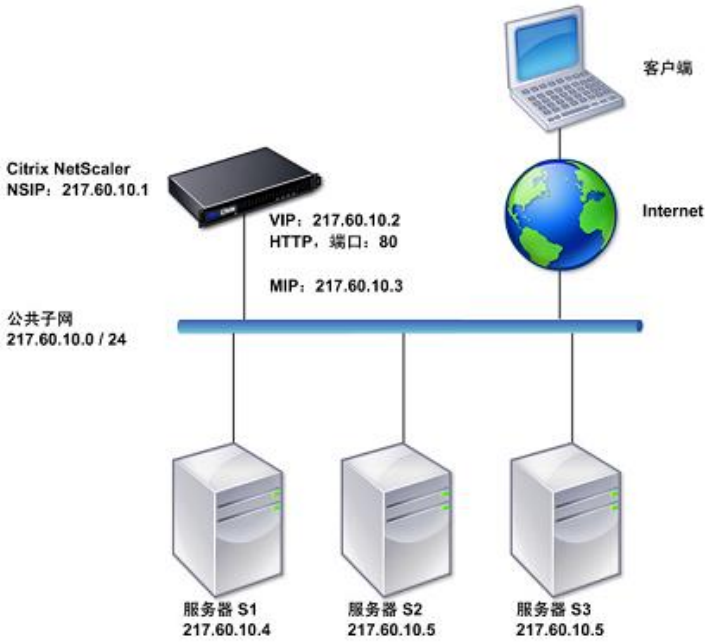


8.2 单臂部署模式

由于单臂部署模式不会对网络结构有任何改动，因此单臂部署模式是 NetScaler 最常用的部署模式，本节将探讨两个常用的单臂拓扑，其中一个具有单个子网，另一个具有多个子网。

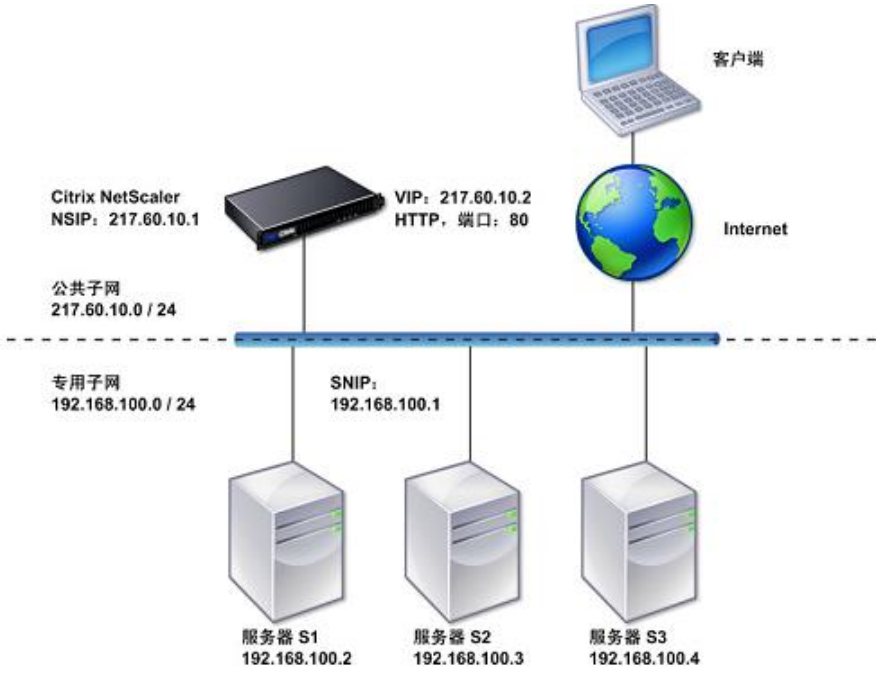
8.2.1 单臂单子网部署

此拓扑在客户端和服务器位于相同子网时使用。请设想一下以单臂模式部署 NetScaler 来管理服务器 S1、 S2 和 S3 的方案。 NetScaler 上配置了一个 HTTP 类型的虚拟服务器， HTTP 服务运行在这些服务器上。 NetScaler IP address (NSIP)、映射 IP 地址 (MIP) 和服务器 IP 地址位于同一公共子网 217.60.10.0/24 上。



8.2.2 单臂多子网部署

此拓扑在客户端和服务器位于不同子网时使用。请设想一下以单臂模式部署 NetScaler 来管理服务器 S1、S2 和 S3 的方案，这些服务器连接至网络上的交换机 SW1。NetScaler 上配置了一个 HTTP 类型的虚拟服务器， HTTP 服务运行在这些服务器上。这三个服务器位于专用子网上，因此通过 NetScaler 配置了一个子网 IP 地址 (SNIP) 与它们进行通信。



8.3 高可靠性部署（主备模式与双主模式）

8.3.1 双机热备模式

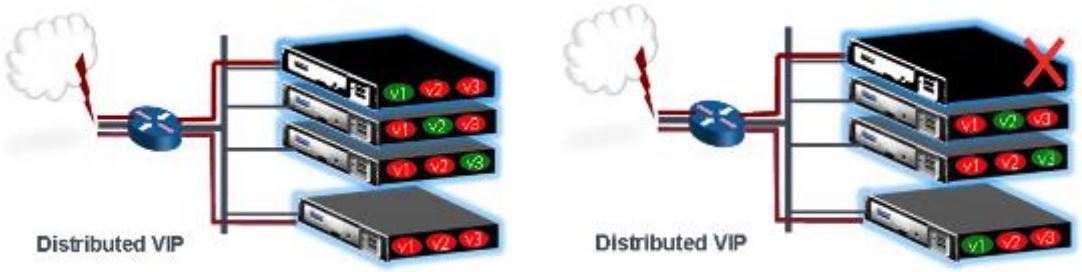
为了避免单一 NetScaler 出现故障，可以中部署两台 NetScaler 工作在高可用模式，其中一台设备积极地接受连接并管理服务器，辅助设备则监控第一台设备。在高可用性配置中，积极地接受连接并管理服务器的 NetScaler 被称为主要设备，另一台被称为辅助设备。如果主要设备出现故障，则辅助设备将成为主要设备并开始积极的接受连接。

高可用性对中的每台 NetScaler 通过发送被称为心跳消息或健康状况检查的定期消息来监控另一台设备，从而确定对等节点的健康状况或状态。如果主要设备的健康状况检查失败，则辅助设备将在特定时间期内重试连接。 如果在特定时间期内重试不成功，则辅助设备将在被称为故障转移的流程中接管主要设备的职责。下图显示两个高可用性配置，其中一个配置以单臂模式部署 NetScaler，另一个配置以双臂模式部署 NetScaler。

NetScaler 进行主备切换的依据为心跳信息是否中断，在 NetScaler 中用户可以自定义心跳信息发送频率时间范围在 200ms — 1000ms，默认为 200ms。

8.3.2 双主模式

Citrix NetScaler 产品除了支持主/备模式的高可靠部署模式外，还支持多台 NetScaler 设备互备功能，利用这种独特的功能，我们可以将多台（>3）NetScaler 设备组成一个 NetScaler 设备资源池，通过 VRRP 将整个系统的应用 VIP 分布在不同的设备上，如果当某台 NetScaler 设备发生硬件故障时，其上的应用 VIP 自动切换到其它 NetScaler 设备上继续对外提供服务。



借助 NetScaler NS pool 配置，多台设备组成资源池，即可增强 NetScaler 的可扩展性和整体处理能力，又能够保障个别设备发生故障时进行切换保护。而不像扩展只有主用/备用或主用/主用配置那样，要求成对增加设备并重新设计网络。

9 产品管理与监控

网络设备集中大量部署，产品易于管理和状态监控非常重要，NetScaler 提供管理与监控的多种方法，下文将对这些方法进行描述。

9.1 产品管理方法

9.1.1 Console CLI

用户可以通过将工作站连接至 NetScaler 的控制台端口来访问 CLI，也可以通过 SSH 从同一网络中的任何工作站连接。

使用交叉电缆将 NetScaler 的串行端口连接至 PC 串行端口，然后启动“超级终端”程序或任何其它终端仿真程序。输入登录用户名称和口令，然后按 ENTER 键。 CLI 提示 (>) 将显示在工作站显示器上。

9.1.2 SSH

用户可以通过 SSH 协议来访问 CLI，SSH 协议是用于从同一网络中的任何工作站远程访问 NetScaler 的首选远程访问方法。在在用户的工作站上，运行 SSH 客户端访问初始配置期间分配给 NetScaler 的 NSIP，并选择 SSH1 或 SSH2 作为协议。连接后，以 nsroot 身份登录，使用在初始配置期间分配的管理密码，以下输出将出现在 SSH 客户端屏幕上：

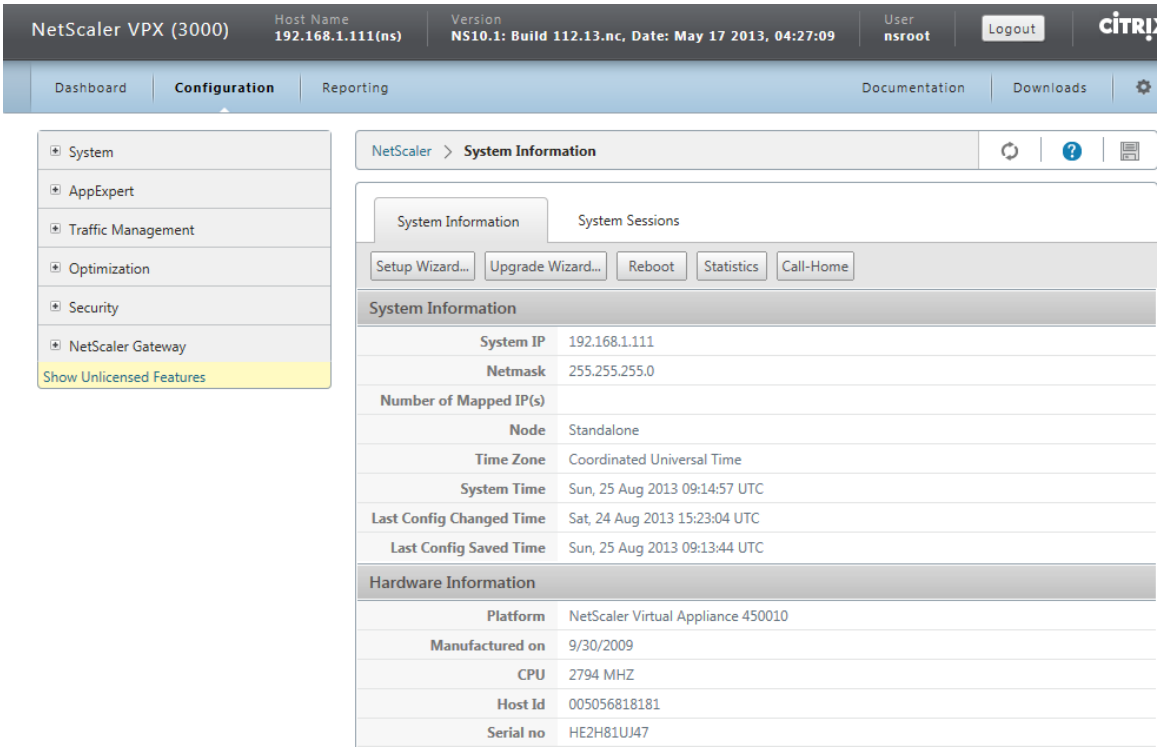
```
login as: nsroot
nsroot@10.102.29.60's password:
Last login: Wed May 23 17:18:31 2007
Done
```

9.1.3 HTTP/HTTPS

NetScaler 支持通过基于 Java 技术的 GUI 界面进行配置管理，支持的协议包括 HTTP 与 HTTPS，具体方法如下：

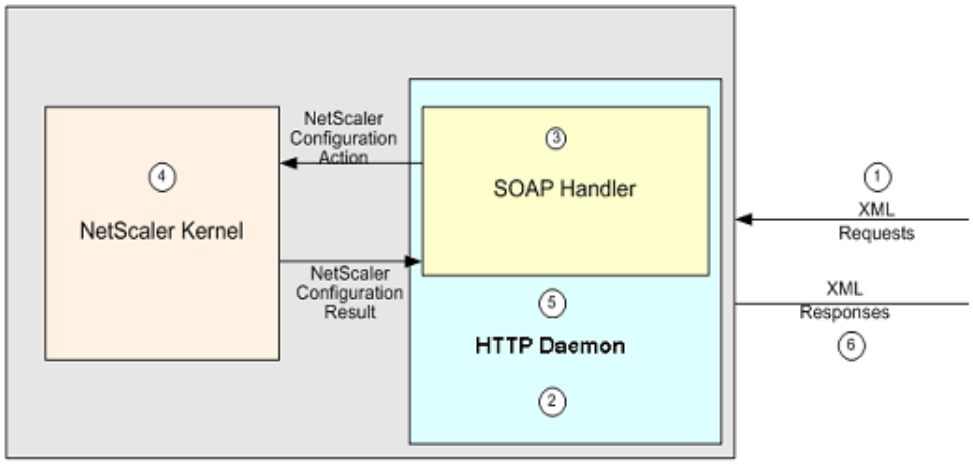
- 在 Web 浏览器中，输入 NetScaler 的 NSIP 和端口号：HTTP(S) ://<NSIP>，此时将出现 Java 插件图标；

- 单击 Java 插件图标，然后按照屏幕提示将插件安装程序复制到工作站的硬盘中。Java 插件安装程序图标 （例如 j2re-1.4.2_04 -win）显示在计算机上的指定位置；
- 双击插件安装程序图标，然后按照屏幕提示安装插件；
- 返回到 Web 浏览器，然后再次单击 Java 插件图标以显示 GUI 登录屏幕，管理与控制界面截屏如下图所示：



9.1.4 XML API

NetScaler 可以使用外部应用编程接口 (API) 进行配置。API 允许创建自定义客户端应用程序以配置和监控 NetScaler 的状态。它基于 SOAP over HTTP。同时，NetScaler 提供 API 接口的开发指导。NetScaler 对 XML API 的结构如下图所示：



9.1.5 集中网管软件

Citrix 的集中管理软件 Command Center 可对全网部署的 NetScaler 产品进行集中管理， Command Center 使网络管理员和运营团队能够轻松地通过单个统一控制台，对其整个全局应用交付基础架构进行集中化控制和管理。集中化管理为管理员提供了整个企业网的可视性以及自动实现多台设备的日常管理任务。

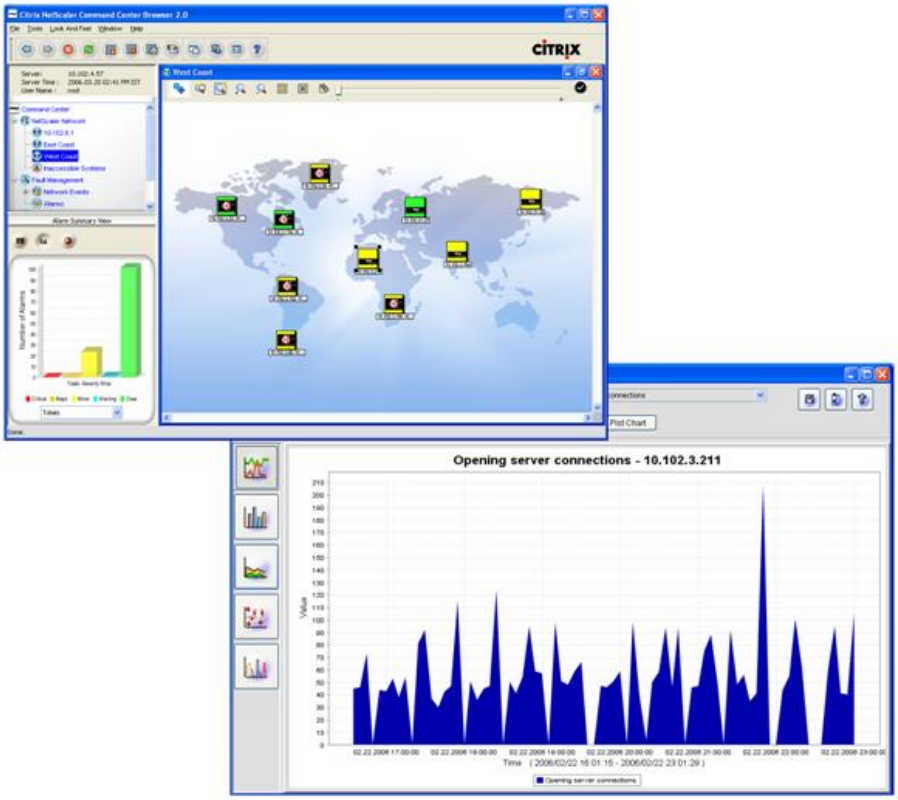
Command Center 是大规模部署思杰应用网络基础架构的理想解决方案，它可扩展到支持数以百计的独立设备，无论这些设备是否处于一个或多个数据中心，或在多个远程分支机构。基于角色的管理策略对用户或用户组可以访问哪些设备或管理功能提供了细粒度的控制。

Command Center 软件可安装在基于 Windows 或 Red Hat Linux 的服务器上。通过基于浏览器的客户端或通过可下载的 Java applet 都可支持对 Command Center 的访问。在这两种情况下，用户必须进行身份验证，然后才可以访问 Command Center。这样确保了管理员无论身处何地都可以从任意客户端设备（台式机、笔记本电脑、智能手机）安全地访问 Command Center 控制台，以更改配置或监控系统健康状况。基本管理功能包括：

- 设备发现
- 设备错误管理
- 设备配置管理
- 设备日志审计
- 设备性能监控

- …… ……

Command Center 管理界面如下所示：



9.1.5.1集中网管软件安装最小硬件支持

- 中央处理器类型: Pentium 4
- 处理器主频： 1.2 GHz
- 内存：1 GB RAM
- 硬盘空间：20GB

9.1.5.2集中网管软件操作系统支持

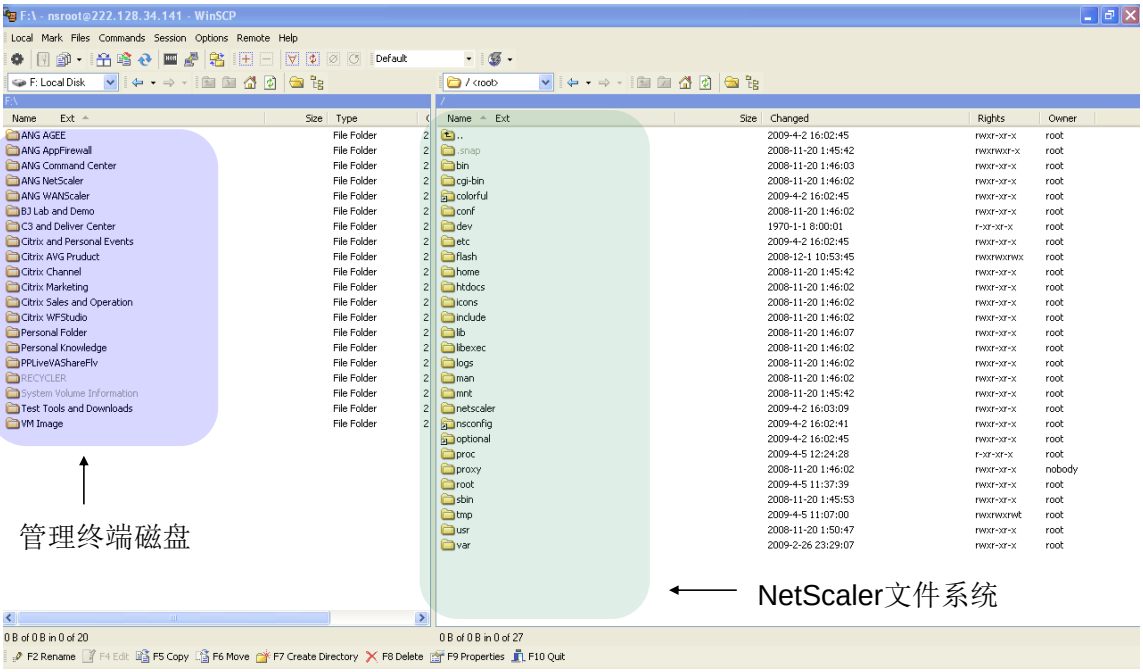
- Windows • Windows 2000 Service Pack 3 and Service Pack 4
- Windows 2003 Service Pack 2
- Red Hat Enterprise Linux AS 4.0
- Red Hat Enterprise Linux ES 4.0

9.1.5.3集中网管软件数据库类型支持

- MySQL
- Oracle
- Microsoft SQL Sever

9.1.6 SFTP

用户可以通过 SFTP（Secure File Transfer Protocol）协议从同一网络中的任何工作站连接，连接后可以从 NetScaler 设备终导入导出各种文件和日志记录。常用的 SFTP 工具为 WinSCP，可从互联网下载，操作界面如下图所示：

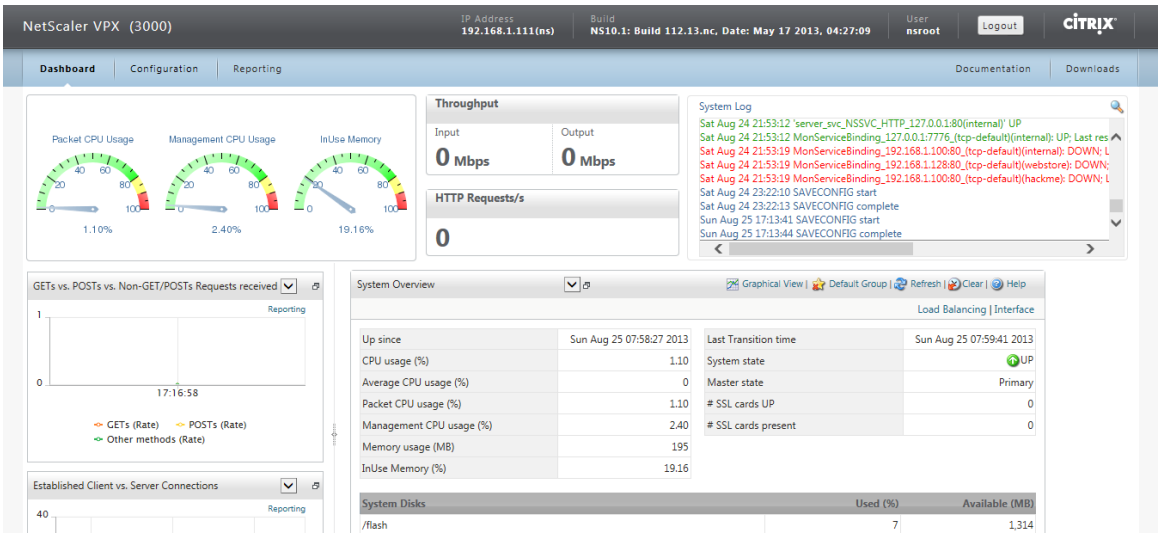


9.2 产品监控

9.2.1 内嵌 Deshboard

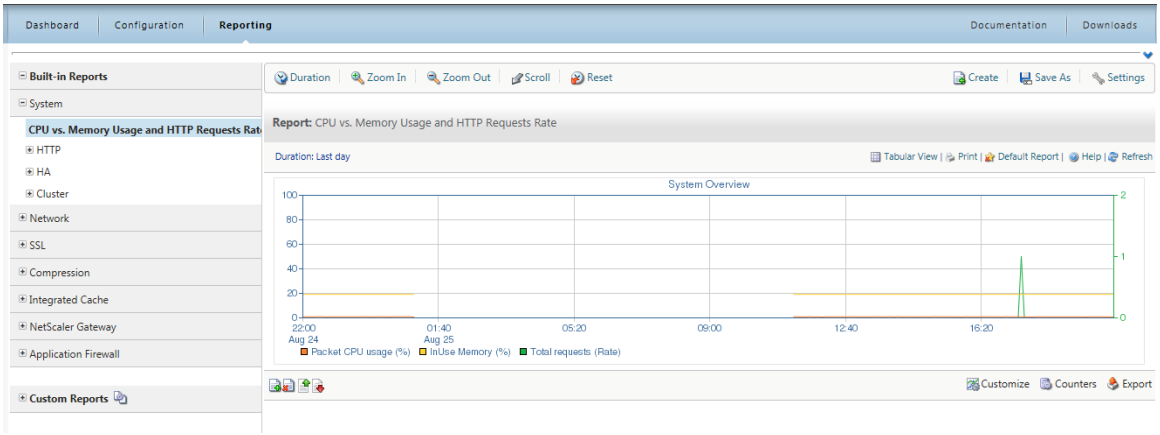
NetScaler 设备本身具有实时状态统计的功能，可以从 Monitor 界面下查看当前的连接数，虚拟服务器访问流量，端口状态等各种统计数据，也可以从 Deshboard 界面下查看这些数据的图形化表现。

NetScaler 的 Dashboard 统计界面如下所示：



9.2.2 内嵌报表功能

NetScaler 设备也会记录长时间的状态统计的信息，可以从 Reporting 界面下查看一段时间内的 CPU 利用率，内存利用率，TCP 连接数等各种统计数据，以 CPU 利用率为例，NetScaler 的 Reporting 历史记录图形化界面如下所示：



9.2.3 标准 Syslog 日志

syslog 用来记录用户对设备进行的操作和各种历史事件（例如，某时刻用户创建了一个”Vserver”，或者某时刻一个”Vserver”出现故障标识为”Down”了）。设备本身提供存放和浏览短期内的 syslog，如果需要存放长期的 syslog 记录，可通过关连到任何外部的第三方 syslog 日志服务器。

syslog 样例（不换行）

Jun 5 17:20:30 <local0.notice> 61.164.41.75 06/05/2008:09:20:30 GMT ns: EVENT DEVICEUP: Device "server_NSSVC_TCP_61.164.41.75:80(internal)" - State UP

9.2.4 标准 Weblog 日志

weblog 用来记录用户对站点进行访问的记录。如果设备本身提供存放和浏览短期内的 weblog，如果需要存放长期的 weblog 记录，可通过关连到外部的 web 日志服务器，NetScaler 随机附带 web 日志服务器的应用程序，无需安装数据库服务器。Weblog 服务器程序支持的操作系统包括 Windows，Linux 和 FreeBSD。

weblog 样例（不换行）

58.38.113.56 - - [01/Jun/2008:22:14:54 +0800] "GET /ws/configuration.pl HTTP/1.1" 200 4546 "http://61.164.41.75/ws/Top.pl" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)"

9.2.5 专有的 nslog 日志

nslog 用来记录设备状态信息，每 7 秒钟，NetScaler 抓取设备内部所有对象状态信息（例如吞吐量，CPU 利用率等），并且保存到 nslog 日志里面。每两天设备建立一个单独的日志文件，最多建立 100 个，即 200 天的日志记录。当设备出现故障或需要获取设备某一时刻状态信息的时候，可以找到相应的日志文件，下载后从中读取状态记录。

9.2.6 集中网管软件

Citrix 的集中管理软件 Command Center 可对全网部署的 NetScaler 产品进行集中管理和监控 。（详细内容请参见 7.1.5 集中管理软件）

9.2.7 支持 SNMP 的第三方网管

NetScaler 上的 SNMP 代理支持 SNMP 版本 1 (SNMPv1) 、SNMP 版本 2 (SNMPv2) 和 SNMP 版本 3 (SNMPv3) 。由于以双模式操作，因此代理可以处理 SNMPv2 查询，例如 Get-Bulk 和 SNMPv1 查询。SNMP 代理还发送符合 SNMPv2 的陷阱并支持 SNMPv2 数据类型，例如 counter64。在处理 SNMP 查询时，SNMPv1 管理器 （其它服务器上向 NetScaler 请求 SNMP 信息的程序）使用 NS-MIB-smiv1.mib 文件。 SNMPv2 管理器使用 NS-MIB-smiv2.mib 文件。NetScaler 支持以下特定于企业的 MIB：

- 标准 MIB-2 组的子集。提供 MIB-2 组 SYSTEM、 IF、 ICMP、 UDP 和 SNMP。
- 系统企业 MIB。提供特定于系统的配置和统计数据

SNMP 网络管理应用查询 NetScaler 上的 SNMP 代理。该代理在管理信息库 (MIB) 中搜索该网络管理应用请求的数据，并将数据发送给该应用。

要配置 NetScaler 的 SNMP 监控，用户需要设置陷阱和警报。SNMP 陷阱是代理生成的同步事件，用于告知异常条件。例如，如果要在 CPU 使用率高于 90% 时获得通知，可以启用陷阱并为该条件设置警报。以下示意图说明了启用并配置了 SNMP 的 NetScaler 的网络。

用户可以配置一个运行符合 SNMP 版本 1、2 或 3 的管理应用的工作站以访问 NetScaler。该工作站称为 SNMP 管理器。如果未配置 SNMP 管理器，NetScaler 将接受并响应来自网络上所有 IP 地址的 SNMP 查询。如果配置了一个或多个 SNMP 管理器，NetScaler 将仅接受并响应来自那些指定 IP 地址

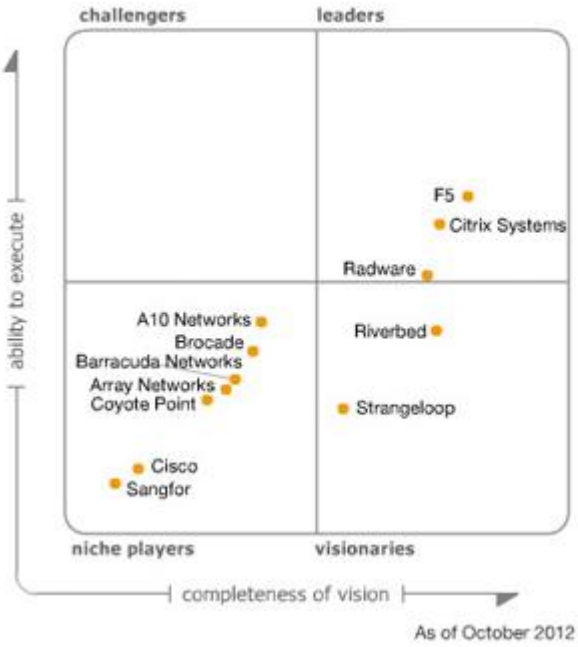
的 SNMP 查询。在指定 SNMP 管理器的 IP 地址时，可以使用 netmask 参数从整个子网授予访问权限。最多可以添加 100 个 SNMP 管理器或网络。

10 第三方评测

NetScaler 系列产品近年来多次在权威机构的评测中得到好评，本章将选取近两年 Gartner Group（全球最具权威的 IT 研究与顾问咨询公司）对应用交付控制器市场的评测，NetScaler 已经在该评测中连续多年评为业界领导者。

10.1 2012 年 Gartner Group 应用交付控制器魔术象限

Figure 1. Magic Quadrant for Application Delivery Controllers



图中两个坐标轴的意思分别为：

- Ability to Execute 坐标主要反映目前产品特性，价格以及用户体验等方面，具体评定指标包括，产品和服务，公司生存能力，销售及价格，市场对产品的反应，市场执行能力，客户体验，运营。
- Completeness of Vision 主要反映公司以及产品发展策略各方面因素，具体评定指标包括，对市场的理解，市场策略，销售策略，产品策略，公司业务模型，行业策略，更新与改进能力，区域策略。

Gartner Group 对 NetScaler 的评价为：

- 创新的 TriScale 架构巩固了 Citrix NetScaler 灵活的，较高性价比的部署模型：

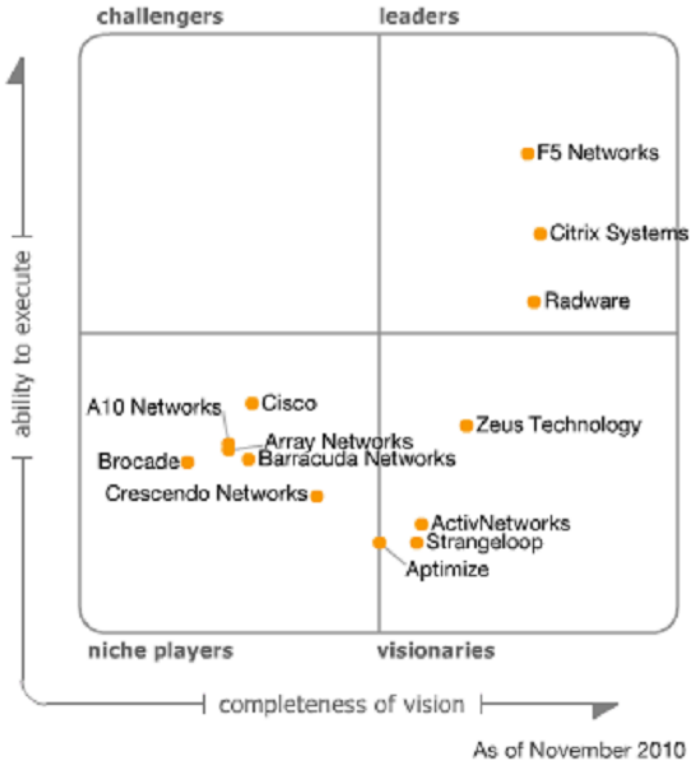
- 向上扩展(pay as you grow),
- 向内扩展(SDX)
- 向外扩展（Clustering）.

- 思杰具备覆盖全球的支持和服务机构
- 思杰具备杰出流量和应用监控报表，具有非常强的 SSL 优化（2048/4096 位密钥）能力
- 思杰很好的整合了“云策略”，CloudBridge 集成易于配置的 Ipsec VPN，广域网优化技术，实现数据中心连接。CloudConnector 加速 IaaS/SaaS 应用

内容摘自《Magic Quadrant for Application Delivery Controllers》

10.2 2010 年 Gartner Group 应用交付控制器魔术象限

Figure 1. Magic Quadrant for Application Delivery Controllers



Source: Gartner (November 2010)

图中两个坐标轴的意思分别为：

- Ability to Execute 坐标主要反映目前产品特性，价格以及用户体验等方面，具体评定指标包括，产品和服务，公司生存能力，销售及价格，市场对产品的反应，市场执行能力，客户体验，运营。
- Completeness of Vision 主要反映公司以及产品发展策略各方面因素，具体评定指标包括，对市场的理解，市场策略，销售策略，产品策略，公司业务模型，行业策略，更新与改进能力，区域策略

Gartner Group 对 NetScaler 的评价为：

- Citrix NetScaler 比其竞争对手提供更全面的应用交付领域的远景，并且提供业界第一个虚拟 ADC 解决方案；
- Citrix NetScaler 在高性能 ADC 中提供大量高级应用交付特性，并且具备良好声誉。同时，NetScaler VPX 虚拟化 ADC 解决方案带来新的机会;
- Citrix 传统软件公司的经验，使其能够更好的理解应用环境;
- Citrix 在 ADC 市场销售业绩连续增长

内容摘自《Magic Quadrant for Application Delivery Controllers》

10.3 2009 年 Gartner Group 应用交付控制器魔术象限

Figure 1. Magic Quadrant for Application Delivery Controllers

Source: Gartner (September 2009)

图中两个坐标轴的意思分别为：

- Ability to Execute 坐标主要反映目前产品特性，价格以及用户体验等方面，具体评定指标包括，产品和服务，公司生存能力，销售及价格，市场对产品的反应，市场执行能力，客户体验，运营。
- Completeness of Vision 主要反映公司以及产品发展策略各方面因素，具体评定指标包括，对市场的理解，市场策略，销售策略，产品策略，公司业务模型，行业策略，更新与改进能力，区域策略

Gartner Group 对 NetScaler 的评价为：

- Citrix 基于日益丰富的高级产品功能，在高性能 ADC 市场具有较高的声誉；
- Citrix 具有全球范围的技术支持渠道，利用丰富的产品线如服务器、应用以及桌面虚拟化到应用交付产品和广域网加速产品，形成强大的解决方案能力；

- Citrix 近期发布的基于软件的 NetScaler VPX 产品增加了在应用交付市场的机会，可以在客户开发/测试环境部署基于 Xen Server 的软件 ADC 产品 NetScaler VPX；
- Citrix 做为传统软件解决方案厂商，对应用软件领域有更深的理解；
- Citrix 公司具有坚固的财务支持，并在不断的增加 ADC 应用交付市场份额 。

内容摘自《Magic Quadrant for Application Delivery Controllers》