



# 应用交付产品

SuperAD

技术白皮书

上海弘积信息科技有限公司

# 技术白皮书

# 目录

1 概述 .....	4
2 系统特点 .....	5
2.1 超强的处理能力 .....	5
2.2 整合下一代数据中心 .....	6
2.3 完备的功能支持 .....	7
2.4 系统的高可用性 .....	7
2.5 强大的安全保护 .....	8
2.6 易于部署和维护 .....	8
2.7 绿色环保的理念 .....	9
3 技术介绍 .....	10
3.1 高性能硬件体系架构 .....	11
3.2 完善的负载均衡特性 .....	12
3.2.1 应用负载均衡算法 .....	12
3.2.2 高级健康检查技术 .....	13
3.2.3 多种会话保持技术 .....	14
3.2.4 全面的负载均衡技术 .....	15
3.2.5 全局服务器负载均衡 .....	15
3.2.6 链路负载均衡 .....	16
3.3 全面加速和应用优化 .....	16
3.3.1 TCP 连接复用 .....	16
3.3.2 内容缓存 .....	17
3.3.3 HTTP 压缩 .....	17
3.3.4 SSL 加速 .....	18
3.4 完善的安全防护能力 .....	19
3.4.1 坚实的系统架构 .....	19
3.4.2 抗 DDoS 攻击 .....	19
3.4.3 源 NAT 转换 .....	19
3.4.4 邮件安全处理 .....	20
3.4.5 自定义安全策略 .....	20

3.5 快速设备故障切换.....	20
3.6 灵活的应用控制.....	22
4 功能列表.....	23
5 组网应用.....	27
5.1 单臂部署.....	27
5.2 双机部署.....	27
5.3 多数据中心部署.....	28

## 1 概述

近年来，随着智能终端、电子商务、在线视频、网银、证券等应用在网络上越来越多、越来越深入，现有的网络基础链路再好，例如万兆交换、千兆路由、光纤布线，都会出现关键应用访问速度慢等诸多问题，究其原因有以下几个方面：

- **服务器的处理能力无法满足需求**

众所周知，随着访问用户数量的增加，很多网站和应用服务器正面临着越来越大的压力，由于不能及时处理用户的访问请求，导致大量用户的流失，大大降低了服务质量和工作效率，简单的依靠提升硬件性能并不能真正解决用户访问请求高速增长的问题。

- **广域网性能无法满足应用需求**

随着智能终端的普及和云计算的兴起，很多企业都在开展数据中心建设，用户对于数据中心远程接入的需求在不断增长。由于广域网带宽普遍较低，从而造成访问时延很大、访问速度变慢、用户体验很差的局面。

- **网络的安全性比较脆弱**

伴随着电子商务、网上交易等应用的发展，同时也带来了诸多的信息安全隐患。黑客、病毒、恶意攻击等影响网络安全的行为也在增多。如不采取有效措施，会造成网络访问变慢甚至无法访问的情况。

弘积 SuperAD 系列应用交付产品就是为适应目前网络的现状及应用的高速增长需求而设计的。产品采用最新的多核多处理器技术，可提供高性能的 4-7 层应用处理能力，系统独有的超级并行操作系统 SPOS (Super Parallel Operating System) 在提供高性能的同时，通过丰富的特性和灵活的脚本定制功能可以确保应用的可用性和可靠性。

系统支持各种应用优化技术，包括：缓存、压缩、连接复用及 SSL 加速等，结合全局负载均衡技术 (GSLB)，可以最大程度的优化用户的广域网访问体验。

系统具有良好的安全防护功能，可以使其部署在相关网络中全面保护和抵抗各类网络攻击，确保关键业务的持续运行。

## 2 系统特点

### 2.1 超强的处理能力

系统采用了多核技术，目前多核技术已经成为应用层网络设备的风向标，其对应用的强大处理能力，使SuperAD系列应用交付设备的性能得到了数倍提升；同时，SuperAD系列产品采用了独创的超级并行处理架构 (SPOS)，使L4-L7处理性能有了巨大飞跃。结合各种应用优化技术：TCP连接复用、HTTP压缩、快速缓存以及SSL加速等，显著改善用户体验，减少了50%甚至更多的响应时间，降低了重复的TCP处理次数，从而降低了40%的服务器的负载，极大地提高应用性能。SPOS架构使得系统表现出强大的性能，能够满足用户当前和以后扩展

的需求。在多个功能同时启用的情况下，不会引起设备性能的明显下降。

## 2.2 整合下一代数据中心

### 云计算及虚拟化

为应对云计算时代的到来，针对数据中心的解决方案，产品全面支持虚拟化技术，包括基于服务器运行环境的虚拟化操作系统，可以与主流的虚拟化软件进行有效整合，性能同样卓越；设备自身也支持虚拟化，可以最大效率的利用系统资源，对用户使用透明；同时可以提供基于角色及虚拟化的管理等功能。系统可以支持 VMware 等虚拟化应用，实现智能的虚拟网络控制。

### OpenFlow 及 SDN

OpenFlow 及 SDN(Software Defined Network)技术能够利用软件更好地控制网络，允许优化网络行为以最大程度的满足用户需求。

系统提供功能强大的 API 接口），通过灵活的编程控制和接口调用，可以允许第三方应用配置并监控设备；同时系统还为用户提供高级可编程脚本技术（eRule），更精确地检测数据包内容，为网络带来无与伦比的应用流量管理的灵活性。

通过系统提供的 API 及 eRule 接口，可以与 OpenFlow 及 SDN 很好的配合工作，结合 OpenFlow 及 SDN 的编程能力及系统强大的可编程接口，充分发挥 OpenFlow 及 SDN 支持的网络所带来的益处，交付高可用及弹性的网络及应用，提供基于 OpenFlow 与 SDN 的 4-7 层应用交付解决方案，以实现 ADC 平滑整合到 SDN 网络之中。

## 2.3 完备的功能支持

SuperAD 系列产品将多种功能集于一体：可以做到本地服务器负载均衡、链路负载均衡，也能实现多数据中心的全局负载均衡，还可以对 DNS，Cache 服务器等做负载均衡。对于一些特殊而复杂的功能需求，系统支持可编程脚本 eRule，可以深度定制用户的需求，这是许多负载均衡设备难以做到的。同时产品还提供很多优化的功能，例如连接复用、SSL 加速、HTTP 压缩、缓存等。对网络也可以全面的支持，IPv4/v6、静态及动态路由、地址转换、链路汇聚、访问控制等，这些功能为设备提供了很高的性价比。SuperAD 设备对于服务器、操作系统以及应用平台的类型都没有限制，只要保证访问的内容一致即可。而且当服务器性能不够时，只需要简单得添加服务器即可，而不需要对网络结构和系统进行改造，体现了极好的扩充性。

## 2.4 系统的高可用性

系统支持丰富的L3-L7应用服务器负载均衡功能，以此提升企业应用和网络的可用性。

- 应用层面：通过对应用协议做深层次的精确分析，能够提供完善的应用负载均衡和内容交换能力；全面的应用健康检查机制，能够及时诊断出异常的服务器或应用，并在条件满足的情况下重新与其建立连接。
- 网络层面：服务器负载均衡能够根据应用、服务器及链路的健康状况，使用负载均衡算法智能调整流量并自动完成切换；Flow Control功能可以保障重要业务的优先运行；支持802.3ad链路聚合，允许将多个端口进行捆绑，进一步提高了链路的带宽和可靠性。

- 设备层面：SuperAD系列产品可以实现2台设备的主-备或主-主模式及多台设备的集群模式组网，可以对当前会话进行同步，在一台设备出现问题的时候，另一台设备能够快速接管（设备切换速度为次秒级），整个过程不会引起业务的中断，体现了极高的可靠可用性。设备支持冗余电源，进一步增强了系统的高度可用性，保障企业应用的稳定性及业务的连续性。

## 2.5 强大的安全保护

系统可采用HTTPS，SSH等加密手段进行网络管理，避免明文通讯对设备直接访问带来的安全隐患，设备可以只开放特定服务的端口，保护服务器不被端口扫描，系统内置了对SYN-FLOOD、ICMP-FLOOD、UDP-FLOOD、PING FLOOD 等DDoS攻击的防护功能，加上卓越的性能，对服务器的防护效果十分明显，使网络应用具有很高的安全性。

系统可以提供功能强大的SSL加解密处理和与CA证书以及客户端证书集成的能力。它可以制定灵活的策略实现基于证书身份的访问和授权，非常适合于网上银行、电子交易等类型的应用。

FWLB技术为网络带来了真正的安全，高性能的访问控制列表(ACL)，网络地址翻译(NAT)以及基于状态的数据包检测手段，可以阻止某些解决方案无法发现的应用层攻击。

## 2.6 易于部署和维护

产品支持单臂、透明、路由、双机、三角传输等多种部署方式，可根据用户的组网情况灵活的选择。

SuperAD系列产品安装简单，可以通过WebUI图形化界面进行直观的配置和管理，也可



以使用SNMP方便管理。系统内置各种模板及网络分析工具，支持丰富的log和数据统计功能，使用、维护和排除故障十分方便。

SuperAD产品支持广泛的企业级应用，包括：Microsoft Exchange Server、Microsoft Office Communication Server、Microsoft Office SharePoint Server、Windows2008 Terminal Services、IIS Server 、Oracle Application Server、Oracle Web Logic、Apache Server、Juniper SSL VPN等几十种应用，可以使用智能模板对这些应用进行快速部署。

## **2.7 绿色环保的理念**

系统依靠独创的SPOS架构，极大的提高了系统性能，使单位性能的功耗比同类产品降低60%；同时结合完备的功能支持，大大简化了企业的网络结构，因而减少了能源和机架空间的消耗。将虚拟化技术应用于数据中心解决方案可节省了60%的电力消耗、40%的服务器机架、30%的网络带宽需求，做到了真正的绿色环保。

### 3 技术介绍

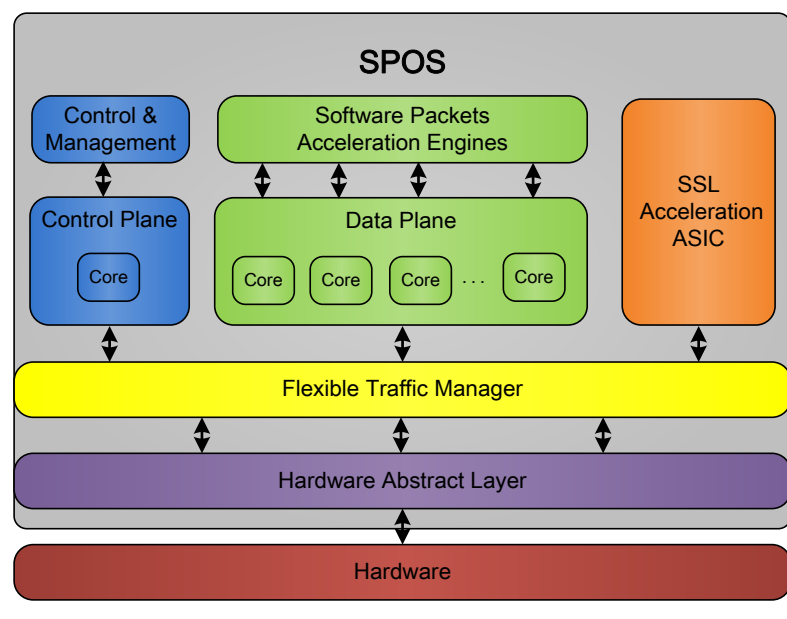
SuperAD 应用交付产品具备先进的 4-7 层应用负载均衡处理能力，设备对外提供虚拟服务，使用负载均衡算法将用户的请求均衡到后端多台真实的服务上，通过健康检查，可以准确的判断应用的工作和服务状态，一旦发现应用不能提供服务，则将其从服务组中移除。SuperAD 产品能够为各种应用提供优化和加速，并增强整个系统的安全性。通过全面的负载均衡、健康检查和应用优化加速功能，提升应用系统的性能，更好的适应和满足应用和业务发展的需要。

### 3.1 高性能硬件体系架构

SuperAD 应用交付产品采用最新的多核 CPU，结合自主研发的超级并行操作系统 (SPOS)，实现了极具扩展性的超高性能平台。SuperAD 产品通过整合最先进的软硬件技术，实现了丰富功能特性和高性能的完美结合。

#### 高级并行操作系统 (SPOS)

SPOS是自主研发的操作系统，充分利用了多核CPU在应用流量处理上的优势，能够对运行在每个L4-L7多CPU上的数据包进行优化，实现4-7层的应用流量在多CPU间的动态健壮地分配和处理，多CPU间零加锁，零内存争用，零拷贝缓冲管理，可以做到对L4-L7协议和服务管理实时优化。



系统独创的多CPU并行超级计算架构，结合丰富的2-3层网络功能，4-7层优化加速技术，可以利用定制脚本对4-7层应用流量进行处理，从而对所有应用进行加速、扩展，并确保应用安全性。通过向系统高性能CPU以及高速内存进行数据包均衡分配，SPOS可避免由于一个或多个CPU内核过载造成的性能瓶颈问题，使得系统表现出很强大的性能，在多个功能同时启用的情况下，不会引起设备性能的明显下降。

## 3.2 完善的负载均衡特性

### 3.2.1 应用负载均衡算法

系统支持丰富的负载均衡算法，利用 VIP (Virtual IP) 将多台真实服务 (Real Service) 资源虚拟为一台虚拟服务 (Virtual Service)。系统可以根据真实服务器的性能和健康状况，选择最佳的服务器响应用户的应用请求，充分利用所有的服务器资源。提供十几种灵活的负载均衡算法：

- 轮询 (Round Robin)：按顺序将连接分配给一个服务组中的服务器。轮询方式对所有服务器同等对待，而与连接的数量或响应时间无关。该算法相对简单，运行稳定。
- 加权轮询 (Weighted Round Robin)：加权轮询算法根据每台服务器设定的加权值来分配请求，服务器收到的连接数与其权值成正比。
- 最小连接 (Least Connection)：最小连接是一种动态调度算法，它通过检测服务器与 SuperAD 设备建立的连接数来估计服务器的负载情况，并将新的连接请求分配到当前连接数最小的服务器。
- 加权最小连接 (Weighted Least Connection)：加权最小连接是与最小连接算法相似，不同之处在于分配连接时需要考虑当前服务器的权重值。
- 优先级 (Priority)：在这种方式下，SuperAD 设备会将请求优先发送给优先级较高的服务器，当高优先级的服务器出现故障时，才将请求发送给优先级较低的服务器。

- 最小响应时间 (Fastest Response Time) : SuperAD 设备会检测与各服务器建立 TCP 连接的时间, 并选择响应时间最短的服务器发送请求。
- IP 地址哈希 (IP Hash) : SuperAD 设备根据源、目的 IP 地址的 Hash 值进行负载均衡。
- URL 哈希 (URL Hash) : SuperAD 设备根据 Web 请求中 URL 的 Hash 值来选择服务器, 这种算法能够保证相同的 URL 请求转发到相同的服务器进行处理。在采用 Cache 服务器的环境中, 能够提高 Cache 服务器的命中率。

### 3.2.2 高级健康检查技术

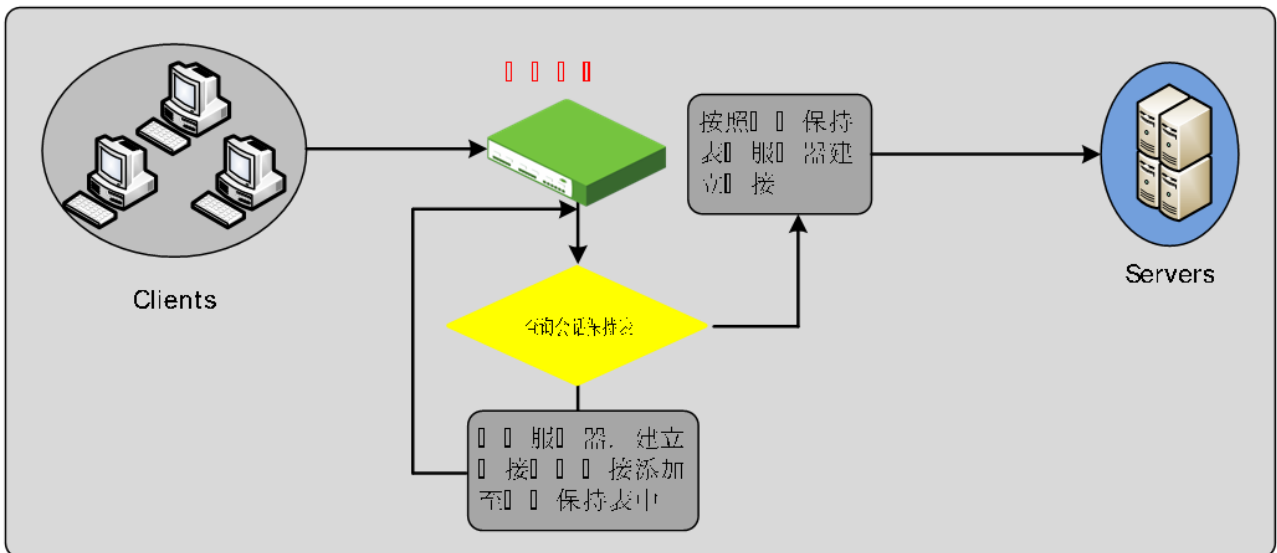
系统的高级健康检查技术具有极大的灵活性, 可以对各类应用及服务器进行探测, 确保所有应用及设备的可靠性。可利用已有的或自定义的健康检查策略, 对服务器及其应用的健康状态进行监测, 确保单个应用服务失效不会对访问造成影响。

系统支持 L3-L7 健康检查方法。通过周期性的检查服务器及其应用服务的健康状态, 保证整个应用的可靠性, 在不同的网络层采用不同的方式进行健康检查。

- L3: 通过 ICMP 协议检查系统当前的健康状态。
- L4: 通过向 TCP/UDP 端口发送连接请求, 检查当前应用端口的健康状态。
- L7: 通过向应用 (如: HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP) 发送指定的代码并判断返回值确定当前应用的健康状态。
- 基于脚本的健康检查: 根据具体的应用进行自定义脚本检查, 能够对服务进行深度健康检测。

### 3.2.3 多种会话保持技术

会话保持在负载均衡中应用广泛，尤其对于一些特定的网络应用，如以网银服务为例，一个客户与服务器通常需要经过好几次的交互过程才能完成一笔交易或者一个请求。这种交互过程往往前后是有密切关联关系的，后台服务器通常需要所有这些相关的交互过程，在一定时间内都由一台服务器完成，而不能被均衡到不同的服务器上处理。下图描述了会话保持的工作流程：



系统支持如下会话保持技术：

- 基于源 IP 地址的会话保持：将同一个源 IP 地址的连接或者请求认为是同一个用户，根据会话保持策略，在会话保持有效期内，将这些发自同一个源 IP 地址的连接/请求都转发到同一台服务器。
- 基于 Cookie 的会话保持：利用 HTTP 协议中的 Cookie 功能来实现会话保持功能。当客户端的请求中带有 SuperAD 设备设置的 Cookie 信息，则设备根据 Cookie 中的信息来选择服务器；当客户端的请求中没有 Cookie 信息，则设备按照算法选择服务器，同时，在服务器响应的 response 头部中，插入 Cookie 信息来实现会话保持。

- 基于目的 IP 的会话保持:将同一个目的 IP 地址的连接或者请求,根据会话保持策略,在会话保持有效期内进行会话保持。
- 基于SSL ID的会话保持:当SSL会话建立时,会产生Session ID,该Session ID在系统中是唯一的,可以应用该ID值来进行会话保持。当用户想与该服务器再次建立连接时,可以通过会话中的Session ID识别该用户并进行会话保持。

### 3.2.4 全面的负载均衡技术

SuperAD设备全面支持L4-L7服务器负载均衡功能,包括:TCP、UTP、HTTP、HTTPS、FTP、SMTP、SIP、Radius等二十余种具体协议;支持包括VoIP及流媒体、邮件安全、网络安全、认证计费、异地灾备、内容缓存等多种具体应用;支持URL交换/重写、HTTP Header插入/重写、内容交换等多种HTTP负载均衡技术;可根据URL和HTTP信息进行流量的分配和处理;每个URL都可以重定向到某组服务器,从而提供优化的Web交换性能。

### 3.2.5 全局服务器负载均衡

全局服务器负载均衡(GSLB: Global Server Load Balancing)可以根据策略将用户的请求分配到分布在各地的提供相同服务的站点上,以实现多个站点之间的流量均衡。SuperAD设备可以同时监控多个站点/服务器以及应用的状态,通过DNS技术将客户请求引导到最佳的站点,提高整个应用系统的可靠性,减少带宽成本,支持应用系统的站点级冗余和快速的透明故障切换,实现灾难恢复。

系统可以根据站点可用性、站点负载和站点响应时间在全球范围内重新引导客户端流量,还可以测量根据往返延迟时间和地理位置而定义的客户端/服务器邻近性。所有这些功能都可以与网络现有的DNS服务器配合起来在部署GSLB时帮助最大程度地减少网络中断。

### 3.2.6 链路负载均衡

链路负载均衡可以解决多链路下流量分担的问题，为用户的多链路的网络应用提供了最好的解决方案。通过 SuperAD 的链路负载分担功能，能够对用户多链路的网络应用提供基于 Inbound 和 Outbound 的链路负载分担功能，解决多链路下流量分担的问题。通过 SuperAD 产品的部署很好的解决了南北电信互联互通、链路冗余、链路智能切换、链路负载、加速流量处理速度、提高服务响应速度等问题。

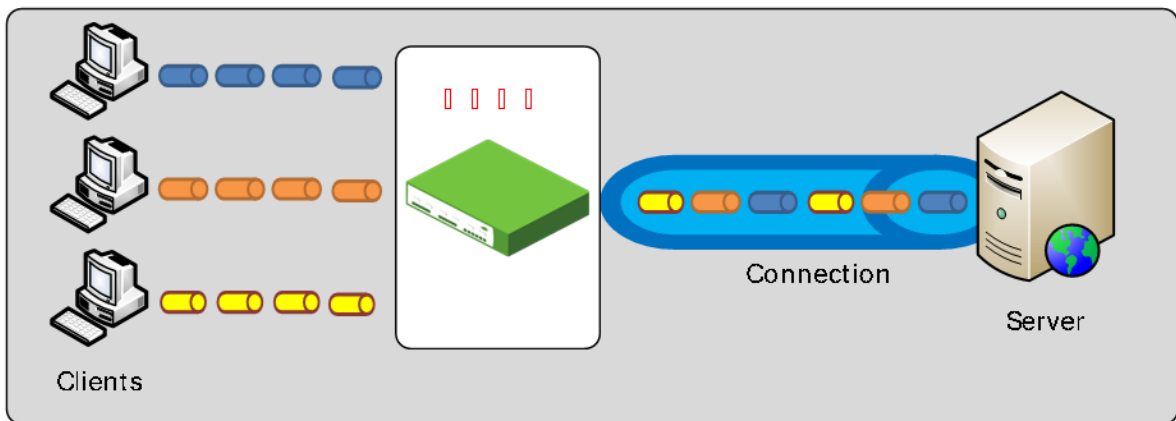
链路负载均衡支持的算法包括：动态监测、轮询、加权轮询及加权最少连接等多种算法，支持链路过载保护，同时支持连接保持、DNS 代理、策略路由及静态路由等功能，可确保多链路场景对于特殊应用访问的支持。

## 3.3 全面加速和应用优化

### 3.3.1 TCP 连接复用

TCP 连接复用 (TCP Multiplexing) 技术主要是为了解决 TCP/IP 协议在处理 HTTP 请求时的低效率问题，通过该技术，能够大大改善现有系统的总体性能。通过将前端多个客户的 HTTP 请求复用到后端与服务器建立的一个 TCP 连接上，不用一对一的方式把每一个 HTTP/TCP 连接从客户端传递到服务器，减少与服务器之间由于新建 TCP 连接所带来的延迟，并能够最大限度的降低客户端请求对后端服务器并发连接数的需求。





### 3.3.2 内容缓存

内容缓存 (Content Cache) 能够有效的减轻服务器的负担，提高服务器的处理能力。通过将 Cache 服务器放在应用服务器的前端，将客户端反复访问的静态内容缓存在 SuperAD 设备的内存中，而服务器仅用于处理动态内容。当客户端发起 HTTP 请求时，SuperAD 设备将 Cache 中的静态内容直接返回给客户端，大大减轻了服务器的负载并节省了后端的网络带宽。最大化的提高网络用户访问网站内容的速度。

### 3.3.3 HTTP 压缩

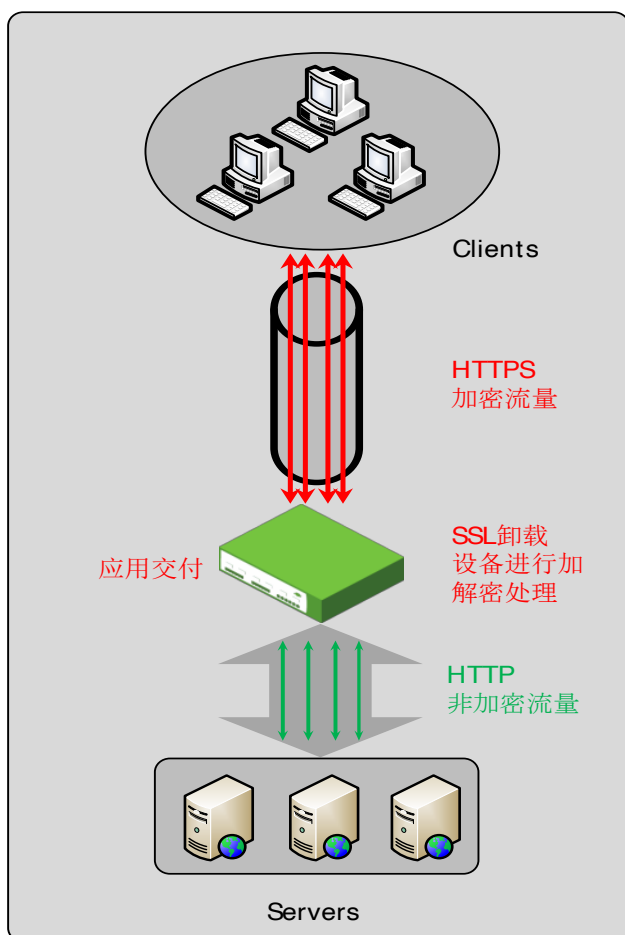
SuperAD 设备支持标准的 HTTP 压缩技术 (HTTP Compression)，能够对指定的内容进行压缩，从而可以在不增加额外的网络带宽的情况下加快用户的响应速度，提高整体系统的性能。

通过 HTTP 压缩，可以带来如下优势：

- 更快的页面下载速度：在采用压缩技术后，同样的页面传递到客户端的时间和流量大大减小，从而提高了客户端的页面下载速度。
- 更小的带宽消耗：支持广泛数据类型的压缩：例如HTTP, XML, Javascript等很多种类型的应用，启用带宽压缩所带来的带宽节省可以达到80%。

- 客户端自适应的压缩处理能力：设备可以通过探测到客户端的Round Trip Time来识别用户是通过宽带还是窄带方式上网，然后决定是否要对该用户启用HTTP压缩功能。
- 对用户完全透明：不需要在客户端安装程序，设备采用的压缩算法是目前常用 WEB 浏览器广泛支持的 GZIP 和 Deflate 算法，当设备开启 HTTP 压缩后功能后，当收到含有“Accept-Encoding: gzip”或“Accept-Encoding: deflate”的 HTTP 报头的 GET 请求时，设备对发出该请求的客户端的响应使用数据压缩。从而可以在不增加额外的网络带宽的情况下加快用户的响应速度，提高整体系统的性能。因此对用户完全透明，不需要预先安装客户端解压程序。

### 3.3.4 SSL 加速



SSL 加速工作原理如左图所示。客户端发起的 HTTPS 加密流量经过 SuperAD 设备进行解密，转换成 HTTP 流量交由服务器处理，从而大大缓解服务器的处理压力，从服务器返回流量经过设备加密处理后发至客户端，较好的保证了数据的安全性。

- SuperAD 设备采用 SSL 加速 ASIC 芯片进行 SSL 处理。对 CPU 资源密集型 SSL 加密和密钥交换过程进行加速，以降低服务器的工作负载。
- 由于 SSL 具有再利用和卸载能力，SuperAD 就可以对加密流量进行监测，从而确保了正

## 3.4 完善的安全防护能力

### 3.4.1 坚实的系统架构

系统采用专用操作系统 SPOS，整合了许多安全优化属性，如应用加速、带外管理、安全管理等，从架构上使系统的安全性得到极大地增强。

### 3.4.2 抗 DDoS 攻击

系统采用独有的操作系统内核进行 DDoS 攻击检测并提供异常数据包保护技术，对于可能造成服务器及应用瘫痪的拒绝服务攻击进行高效检测和预防。

系统采用 SYN Cookie 技术对 SYN Flood 攻击进行检测和预防，只有通过 TCP 三次握手的连接才会被放入会话表中，防止大量的 SYN 占用系统资源而造成的系统崩溃。

### 3.4.3 源 NAT 转换

系统的 Source NAT 技术具有高性能的网络地址转换（NAT）功能，可针对外部网络对数据中心资源进行隐藏。利用 Source NAT，可以创建基于策略的 NAT 规则，确保关键服务资源的安全性，并对网络流量进行智能化重新定向。

利用系统提供的双向 NAT 功能，可为物理服务器分配私网地址，从而帮助提高安全性和节省地址空间。SuperAD 设备还能够在物理服务器位于不同子网的环境中支持 NAT 功能，此项功能可在设计服务组时提供全面的网络设计灵活性。

### 3.4.4 邮件安全处理

支持 STARTTLS 协议,确保邮件流量从客户端到邮件服务器之间传输的都是加密的信息。在防垃圾邮件方面,设备可基于策略负载均衡(PSLB)定制黑/白名单,使邮件服务器处理邮件的能力大为提升。

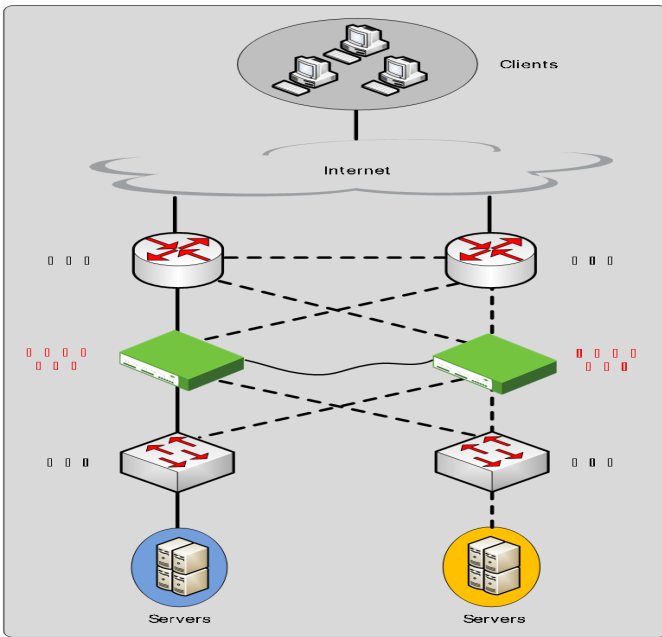
### 3.4.5 自定义安全策略

系统提供直观的 Web 管理模式,内置各种模板及向导,能快速部署复杂的安全策略。结合标准或扩展的访问控制列表(ACL)和灵活的 eRule 脚本开发工具,用户可为自己的应用系统定制最合适的安全策略。

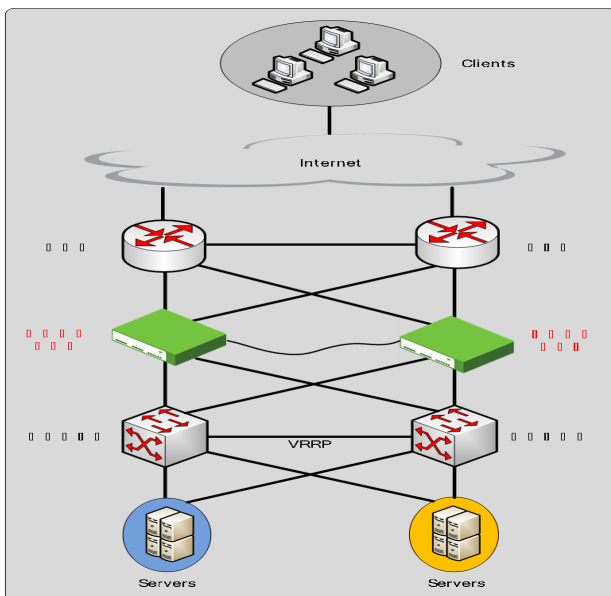
## 3.5 快速设备故障切换

尽管 SuperAD 设备的加入提高了后台服务器的高可用性,如果设备自身出现故障,将会导致整个应用系统停止工作。为了防止这种情况出现,可以采用冗余结构来保证自身设备的高可用性。系统支持两种冗余切换:主-备模式和主-主模式。

左图为主-备模式的典型组网,两台 SuperAD 设备只有一台在处理流量,另外一台不处理流量处于备份状态,随时准备接管主设备的业务处理。系统是通过广播报文来实现主-备设备的控制。对于每台 SuperAD 设备来说,存在有两种类型的 IP 地址:一种是本地地址,本地地址是唯一的,在同网段中不能有重复的地址出现;另外一种浮动地址,浮动地址是可以在两台设备之间漂移的。浮动地址全部在主机名上对外进行业务 ADD



两台设备主-备角色的选举通过设备的优先级 (Priority)、Group ID 及设备 MAC 地址等综合比较得出。两台 SuperAD 设备之间通过心跳接口传送心跳报文及同步连接信息。为不改变原有网络结构，设备支持透明接入模式。当链路出现故障、主设备异常时将触发主-备模式的切换，切换时间为次秒级，对业务几乎没有影响。



在主-主工作模式下，两台 SuperAD 设备都在处理业务流量，但每台设备都是处理不同的业务流量，同时互相监控，随时准备接管对端的业务流量，互为备份的工作模式。

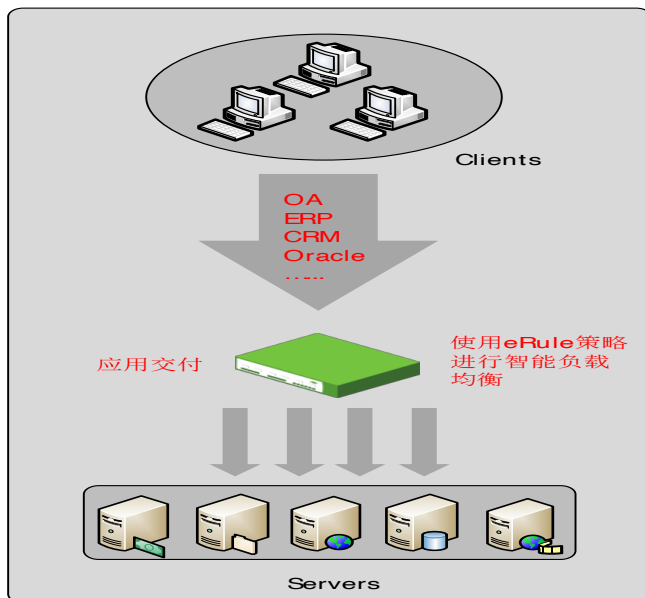
通过配置，高优先级的 SuperAD 设备和一个 Group 关联，实现主-主的流量转发。

主-主模式同时使用两个浮动地址，浮动地址是在两台设备之间漂移的，浮动地址对外进行免

### 3.6 灵活的应用控制

系统的 eRule 高级脚本技术能够实现灵活的应用控制,它是基于自主研发的 SPOS 架构。完善的 API 接口可以与 OpenFlow 及 SDN 很好的配合工作,为网络带来无与伦比的应用流量管理的灵活性。

eRule 为可编程脚本语言,它是 TCL 语言的扩展,简单易用。eRule 包含一个或者多个事件申明,以及在事件被触发时所执行 TCL 的代码。系统通过强大的 SPOS,已经隐藏了许多底层的内容,通过编写对于单一连接的处理模式,系统会自动地在每个连接中执行定义的规则,并且能达到非常高的效率。



- 通过 eRule 策略控制,可以更精确地检测数据包内容,从而实现更加灵活的负载均衡功能;
- 可以将应用重定向到服务组、单一服务器或单一端口;
- 可以提供更加灵活复杂的健康检查手段;
- 通过细粒度的查找包的内容实现灵活准

## 4 功能列表

功能分类	具体功能	特点描述
应用交付	负载均衡	<ul style="list-style-type: none"><li>● 全面支持 L4/L7 层服务器负载均衡 SLB: TCP、UDP、HTTP、HTTPS、SIP、SMTP 等几十种协议<ul style="list-style-type: none"><li>▪ 完全 HTTP 代理</li><li>▪ 提供多种模板, 易于使用部署</li><li>▪ 高性能的 HTTP 报头/URL 交换</li><li>▪ URL 哈希</li><li>▪ 应用:<ul style="list-style-type: none"><li>✓ VoIP及流媒体: SIP Load Balancing</li><li>✓ 邮件安全: STARTTLS、POPS、LDAPS、SMTPS、</li></ul></li></ul></li></ul>

		<p>IMAPS</p> <ul style="list-style-type: none"> <li>✓ 网络安全: Firewall Load Balancing</li> <li>✓ 认证计费: Diameter Load Balancing</li> <li>✓ 黑白名单: Policy Server Load Balancing</li> <li>✓ 内容缓存: Transparent Cache Switching</li> </ul> <ul style="list-style-type: none"> <li>• 支持链路负载均衡 LLB <ul style="list-style-type: none"> <li>▪ 支持动态检测、轮询、加权轮询等多种算法</li> <li>▪ 支持连接保持, DNS代理, 链路过载保护, 策略选路、域名选路、静态选路及默认选路</li> </ul> </li> <li>• 支持全局负载均衡 GSLB <ul style="list-style-type: none"> <li>▪ 支持基于地理位置、最快响应时间、站点权重等十余种算法</li> <li>▪ 支持代理和服务器模式</li> <li>▪ 支持多种DNS记录: A、MX、CNAME、NS、TXT等</li> </ul> </li> </ul>
	均衡算法	<ul style="list-style-type: none"> <li>• 十几种负载均衡算法 <ul style="list-style-type: none"> <li>▪ 轮询、最小连接、加权轮询、加权最小连接、最快响应、哈希等</li> </ul> </li> </ul>
	健康检查	<ul style="list-style-type: none"> <li>• ICMP、TCP、UDP</li> <li>• HTTP、HTTPS、FTP、RTSP、SMTP、POP3、SNMP、DNS、RADIUS、LDAP</li> <li>• 支持自定义脚本健康检查</li> </ul>
	会话保持	<ul style="list-style-type: none"> <li>• 基于 Cookie 的会话保持</li> <li>• 基于源 IP 的会话保持</li> </ul>



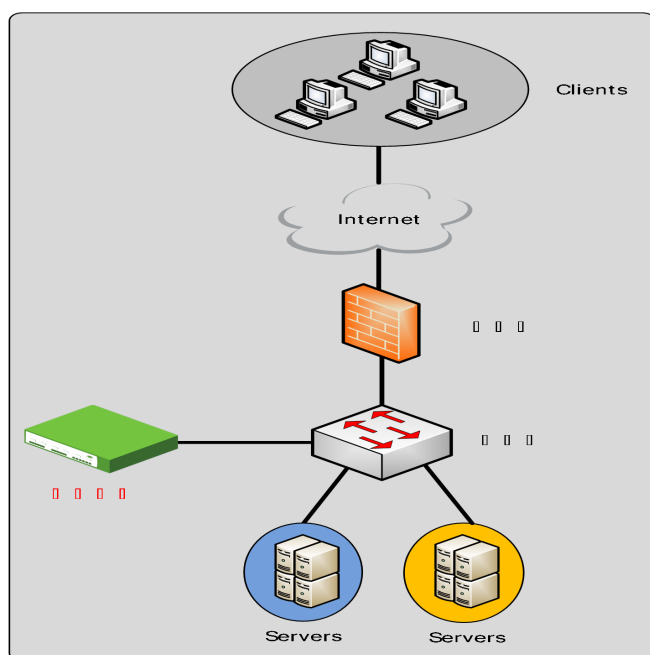
		<ul style="list-style-type: none"> <li>• 基于目的 IP 的会话保持</li> <li>• 基于 SSL ID 的会话保持</li> <li>• 基于脚本的会话保持</li> </ul>
	高级脚本eRule	<ul style="list-style-type: none"> <li>• eRule: 允许通过脚本对具体应用做深层的包检查和转换, 进行细粒度的控制</li> </ul>
应用优化	TCP连接复用	<ul style="list-style-type: none"> <li>• TCP连接复用</li> </ul>
	HTTP缓存	<ul style="list-style-type: none"> <li>• 服务器内容缓存</li> <li>• RAM 缓存</li> </ul>
	HTTP压缩	<ul style="list-style-type: none"> <li>• GZIP</li> <li>• Deflate</li> </ul>
	SSL加速	<ul style="list-style-type: none"> <li>• 基于硬件的 SSL 处理</li> <li>• SSL ID 复用</li> </ul>
安全防护	安全防护	<ul style="list-style-type: none"> <li>• 抗DDoS攻击</li> <li>• 连接限速及流量控制</li> <li>• IP异常检测</li> <li>• DNS应用防火墙</li> <li>• 邮件安全处理</li> </ul>
高可用性	HA	<ul style="list-style-type: none"> <li>• 主-主: Active-Active</li> <li>• 主-备: Active-Backup</li> <li>• 集群: Cluster</li> <li>• 次秒级切换速度</li> </ul>
网络特性	L2/L3	<ul style="list-style-type: none"> <li>• 支持透明和路由模式</li> <li>• 支持静态及动态路由 (RIP、OSPF、BGP)</li> <li>• 访问控制 (ACL)</li> </ul>

		<ul style="list-style-type: none"> <li>• 网络地址转换 (NAT)</li> <li>• VLAN</li> </ul>
	LACP	<ul style="list-style-type: none"> <li>• 静态</li> <li>• 动态</li> </ul>
	IPv4/IPv6	<ul style="list-style-type: none"> <li>• 全面支持 IPv4/IPv6</li> </ul>
虚拟化	虚拟化	<ul style="list-style-type: none"> <li>• 虚拟化平台支持: VMWare/KVM/Hyper-V</li> <li>• 设备虚拟化</li> <li>• 基于角色的管理</li> <li>• 与 VMWare 与 H3C 虚拟化平台智能联动</li> <li>• 智能应用控制</li> </ul>
管理功能	管理功能	<ul style="list-style-type: none"> <li>• 提供可编程 API 接口</li> <li>• 独立的网络管理接口 (串口、管理口)</li> <li>• 基于 Web 的图形化用户界面 (GUI)</li> <li>• 支持工业标准的命令行接口</li> <li>• SNMP, Log, 告警</li> <li>• 端口镜像 (Port Mirroring)</li> <li>• 实时在线抓包工具</li> </ul>
统计功能	统计报表功能	<ul style="list-style-type: none"> <li>• 基于实时及 1 年历史的流量、性能统计数据</li> <li>• 可自动或手动生成各类报表</li> </ul>

## 5 组网应用

### 5.1 单臂部署

单臂部署方式对原有网络拓扑结构变动小，和应用无关的流量不会通过负载均衡设备。

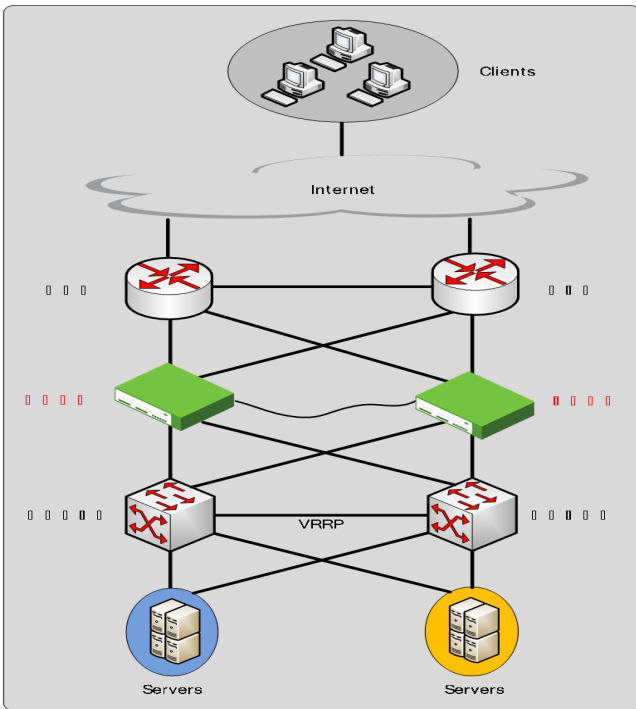


- SuperAD设备与汇聚层交换机之间只有一条链路或链路聚合组；
- 所有入出流量均通过该链路；
- 服务器网关指向汇聚层交换机；
- 对于需要负载均衡的流量，汇聚层将VIP的下一跳指向SuperAD设备；
- SuperAD设备的缺省路由指向汇聚层交换机；

在SuperAD设备上需要配置源IP地址转

### 5.2 双机部署

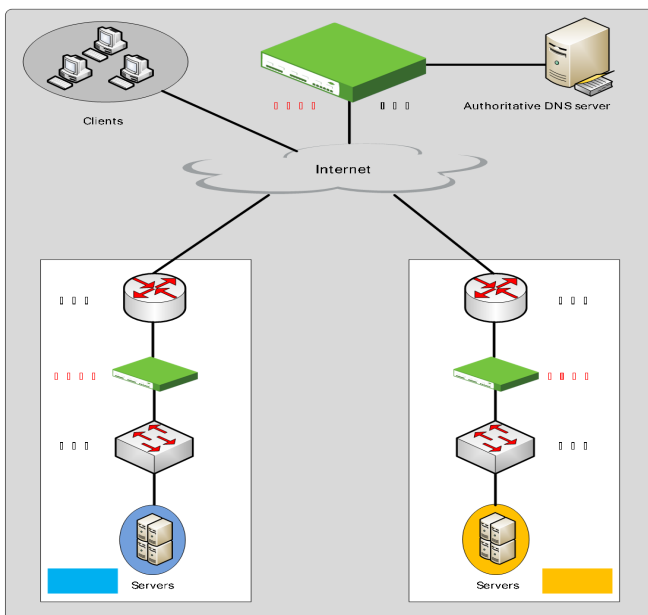
双机部署方式包括主-备和主-主两种，可以实现网络的高可用性；同时根据需要，可以实现透明或路由形式的双机部署。对于网络可靠性要求较高的用户需要使用双机模式进行网络部署。



- 假设左图 SuperAD 设备部署为主-备，当主机发生故障，或者检测到端口 down 掉，网关不通等现象时，会自动切换到备机，切换时间为次秒级；
- 负载均衡设备会监控服务器的健康状况，当发现服务器异常时，会自动把用户请求转发到备机；
- 由于会话同步机制，同一 Client 的会话可以确保由同一台 Server 来处理，而主的 Server 与备机 Server 也能够做到信息同步。

### 5.3 多数据中心部署

大型的企业或业务容灾要求非常高的用户都会部署有多个异地的数据中心，以保证其业务不间断的正常运行，而要整合多个IDC的资源并实现就近性访问，那就需要在多IDC使用GSLB进行网络部署。



- 通过智能 DNS 解析，SuperAD 控制器将用户的访问请求引导到最佳的站点，提高整个应用系统的可靠性，减少带宽成本；
- 可以根据策略将用户的请求分配到提供相同服务的两个站点上，以实现多个站点之间的流量均衡；
- SuperAD 设备支持应用系统的站点级冗余和快速的透明故障切换，实现灾难