# 山石网科应用交付 AX 系列——服务器负载均衡（SLB）技术白皮书

## 一、应用系统面临的挑战

应用系统是企业为用户提供高质量服务，提高市场竞争力的重要平台，也是构建企业商业模式的基础。随着企业业务的扩张和访问用户的增多，传统的应用系统面临着种种挑战，比如：

- 缺少冗余备份措施的应用服务器容易出现单点故障，甚至导致业务中断。
- 应用服务器的扩容跟不上业务和用户的增长速度，服务质量差。
- 类似于“双 11”的活动带来的峰值业务流量压力。
- 网络结构的调整、系统的维护升级影响到应用系统的不间断运行。

要应对系统所面临的种种挑战，行之有效的技术方式是采用服务器负载均衡（SLB）技术来提供可用性、可扩展性和安全性的保障，为业务系统的不间断运营保驾护航。

## 二、服务器负载均衡的技术实现

作为传统的网络负载均衡产品的升级和进化，山石网科应用交付 AX 系列（以下简称山石网科 ADC）支持完善的负载均衡功能，包括链路负载均衡（LLB）、服务器负载均衡（SLB）和全局负载均衡（GSLB），其中应用最普遍的就是服务器负载均衡。

服务器负载均衡是指在多台服务器对外提供服务的情况下，ADC 可以接收客户端的请求，并依据特定算法将请求分担到多台服务器。在服务器器负载均衡场景下，客户端访问应用系统的典型过程如下：

1. 用户在浏览器中输入要访问的域名，比如 www.hillstonenet.com.cn, 该动作首先会触发向本地 DNS 服务器的域名解析行为。
2. DNS 服务器将 www.hillstonenet.com.cn 解析为 IP 地址，假定为 100.100.0.23 返回给用户。这个 IP

地址实际上是 ADC 上配置的对外提供服务的虚拟 IP 地址，并非服务器的真实 IP。

3. 客户端向 100.100.0.23 发送访问请求。

4. ADC 设备接受请求，并代理客户端将请求发给后台真实的服务器；当 ADC 接收到服务器的回应后，再将回应报文转发给客户端。

5. 根据不同的负载均衡算法，ADC 可以将来自客户端的请求发送到相同的或不同的服务器上。

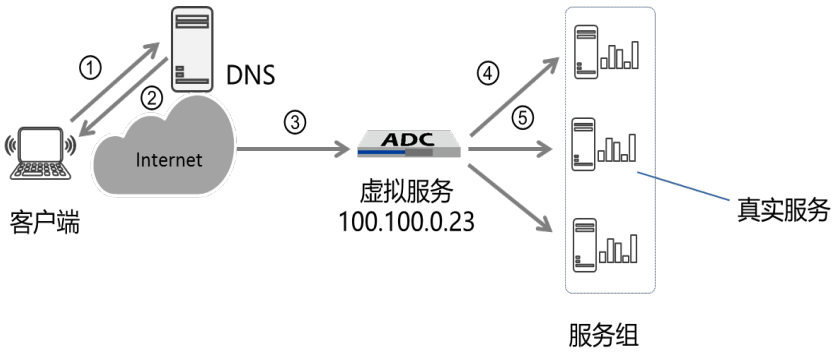


图 1 服务器负载均衡的工作过程

## 2.1 服务器负载均衡的部署模式

山石网科 ADC 在作为服务器负载均衡使用时，可以以三种模式执行：反向代理模式、透明模式三角传输模式。

- **反向代理模式**

在反向代理模式下，ADC 在将客户端的请求报文转发给服务器时，采用了自己的 IP 地址来替换客户端的原始 IP。这样带来的问题是服务器将无法知晓有哪些 IP 的客户端访问了自己。作为解决方案，山石网科 ADC 可以在用户的 HTTP 包头中加入 X-Forwarded-For 字段，用它记录客户端的 IP 地址。

采用反向代理模式的优点是，ADC 可以采用连接复用技术来减少后台服务器的负载，改善应用系统的性能。

- **透明模式**

透明模式是指 ADC 在转发用户请求时，不改变用户的原始 IP 地址，将客户端的连接定向到特定的服务器上。由于不改写报文的源 IP，服务器可以记录原始 IP 的访问行为，但由于每个客户端请求的源 IP 地址都不一样，在透明模式下无法利用连接复用技术改善应用系统的性能。

在透明模式下，需要保障从服务器端来的回应报文必须经过 ADC 设备。

- **三角传输模式**

三角传输模式是为上下行流量差异大的应用系统而特别设计的，比如 VOD 点播系统，上行流量小而下行流量大，采用三角传输模式可以更好的提升这类系统的服务效率。三角传输模式保证了流媒体服务的高性能，在该模式下，用户请求通过 ADC 被分担到某一个服务器上，而服务器返还的响应数据则可以不通过 ADC 而直接发送到客户端。

## 2.2 服务器负载均衡的策略和算法

在山石网科 ADC 中，服务器负载均衡的实现方式需要通过负载均衡策略（SLB Policy）和负载均衡算法（SLB Methods）来定义。山石网科 ADC 提供了丰富的负载均衡策略和算法以满足不同应用系统的特定需求。

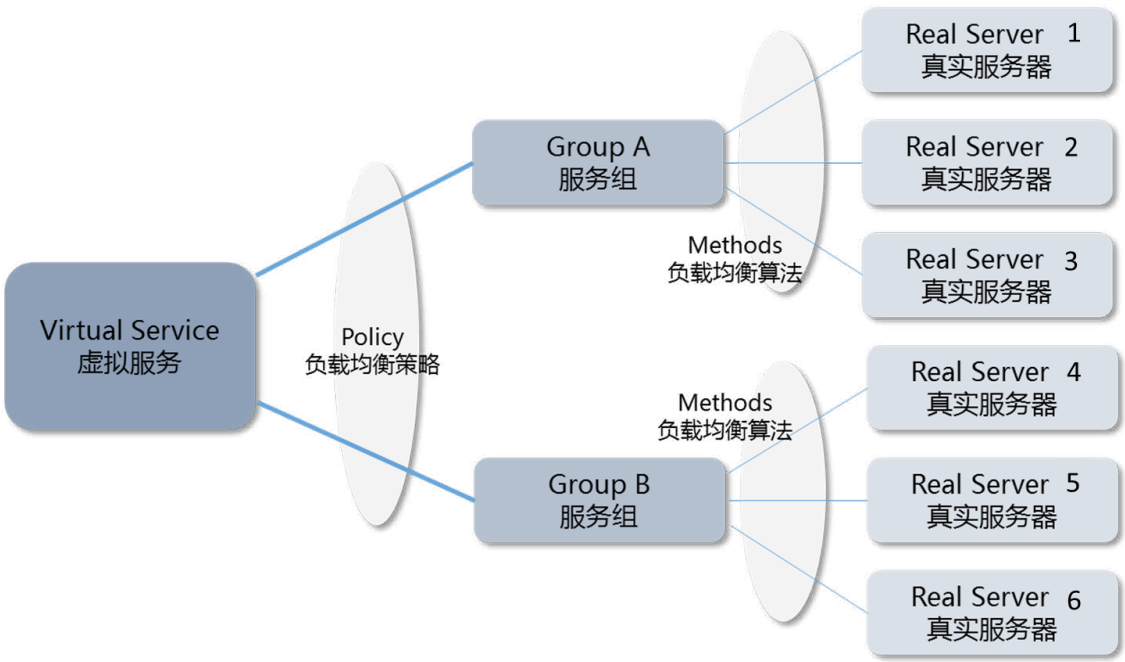


图 2、山石网科 ADC 的负载均衡策略和算法

服务器负载均衡算法（SLB Methods）是在建立服务组时所定义的参数之一，不同的服务器负载均衡算法决定了请求数据在服务组内的不同后台服务器中的分配方式。依据不同的负载均衡算法，当数据到达 ADC 设备时，设备会向服务组内的后台服务器做出类似轮流转发、根据探测结果做出转发决定等转发行为。

山石网科 ADC 支持超过 20 种的负载均衡算法，可以将这些算法分为持续性算法、非持续性算法、基于 SNMP 的算法和基于优先级的算法等四类，每一类包含不同的内嵌算法，如轮循算法、最少连接算法、最

短响应时间算法、散列算法等等。

- **非持续性算法（ Non-Persistent）：** 一个客户端的不同的请求可能被分配到一个服务组中的不同的真实服务器上进行处理。主要有：轮循算法、最少连接算法、响应速度算法等。
- **持续性算法（ Persistent）：** 从一个特定的客户端发出的请求都被分配到一个服务组中的同一个真实服务器上进行处理。主要包括：基于 IP 的算法、基于报头 / 请求的算法、基于 Cookie 的算法等。
- **SNMP-based 算法：** 基于特定的 SNMP 信息选择合适的服务器，例如：CPU 利用率，硬盘的型号以及内存的状态。ADC 设备定期发送 SNMP 请求到真实服务器，并根据服务器回应的数据进行流量分配，从而实现服务器负载均衡的目的。
- **基于优先级的算法：** 可以对每个后台服务器设定不同的优先级，正常情况下，客户端的请求总是选择一个优先级最高的可用后台服务器，优先级低的不接受请求。当优先级最高的后台服务器不能提供服务时，由次优先级的可用后台服务器接管。

除了基本的负载均衡算法，也可以给服务器分配不同的加权值来调整分配的流量，以使性能更优的服务器获得更多的负载。此外，为了避免服务器因过载而崩溃，可为实际服务器指定最大连接阈值来避免该服务器过载。

负载均衡策略用于将虚拟服务和服务组绑定在一起。通过使用负载均衡策略，管理员可以控制 OSI 模型二至七层的负载均衡决定。虚拟服务使用策略绑定到一个服务组上，一个单个的服务组可以同时分配给不同的虚拟服务。下面列举了 ADC 设备所支持的负载均衡策略。

| 基本策略 | 保持策略 | QoS 策略 |
|---|---|---|
| 重定向（Redirect）<br>静态（Static）<br>默认（Default）<br>备份（Backup） | 保持 URL<br>保持 Cookie<br>重写 Cookie<br>插入 Cookie<br>URL Hash<br>RADIUS Username<br>RADIUS Session ID | QoS Cookie<br>QoS Hostname<br>QoS URL<br>QoS Network<br>QoS Client Port<br>QoS Body<br>Regular Expression<br>Header |

表 1. 负载均衡策略

不同类型的负载均衡策略具有不同的优先级，通常情况下，多个 ADC 设备的服务器负载均衡策略可以配置到同一个服务器负载均衡虚拟服务中，并且 ADC 设备将基于最高优先级的策略来转发请求。

关于山石网科 ADC 的负载均衡策略及算法的详细说明，可以参考《山石网科 ADC 产品用户手册》。

### 2.3 服务器健康检查

在进行服务器负载均衡功能的同时，山石网科 ADC 需要对服务器的运行状态进行健康检查，以便在应用系统工作异常时，将后续的访问请求转发到其它正常工作的服务器进行处理，保障业务的连续性。针对服务器故障的处理，对用户层面是完全透明的。

山石网科 ADC 对服务器的健康检查，可采用如下多种方式:

1. ICMP 检查：利用 ICMP 可检查服务器的网络工作是否正常。
2. TCP 检查：ADC 跟服务器的服务端口建立 TCP 连接，检查服务器的服务是否正常。
3. UDP 检查：针对 DNS 服务进行检查，可及时判断 DNS 服务是否正常。
4. TCPS 检查：与 Real Services 进行 SSL 协议握手，检查是否能成功建立连接。
5. HTTP 检查：采用 HTTP 的检查，来验证服务器提供的服务是否正常。
6. DNS 检查、Radius 检查：检查 DNS 服务器和 Radius 服务器的健康状态。
7. Script TCP 和 Script UDP 检查：通过脚本检查 TCP 服务或 UDP 服务工作是否健康。
8. Web 页面的关键词检查：在后台服务的回答中查找关键词，如果能找到了，该确认后台服务是好的，否则认为后台服务不正常。

通过上述健康检查机制，可以确保服务器为用户提供正确可靠的服务。当其中的任何一台或几台服务器需要离线维护或出现故障时，山石网科 ADC 设备能够通过预先配置的多种智能健康检查机制，及时发现不能正常处理应用的服务器，避免了因为某台服务器的故障而影响到业务的连续性。

## 三、安全特性及应用性能增强

当前的应用系统通常采用 Web Server、Application Server、Database Server 多层结构设计，支持前端浏览器访问或客户端访问方式。在应用系统平台中，山石网科 ADC 除了可以实现 Web 服务器组、应用服务器组的负载均衡功能，还可以提供网络层及应用层安全防护功能，以及通过连接复用、内容压缩等技术实现应用性能的增强。

### 3.1 端到端的安全保障

安全是应用交付的重要组成部分，山石网科 ADC 具备如下安全能力:

- 支持地址翻译技术（NAT）和安全地址映射，隐藏了后台服务器真实的 IP 地址和业务端口，可以保

护业务系统免受黑客攻击的影响。

- 支持 L3-L7 访问控制、访问日志与告警，支持网络层及应用层 DDos 攻击防护。
- 基于 HTTP 代理的工作方式，支持 HTTP 访问方法控制、URL 过滤、HTTP/DNS 缓存、强制 HTTPS 重定向。
- 产品的管理全部采用 SSH 和 HTTPS，可以保护产品自身免于内部或互联网上的攻击。
- 可配置的加密套件和最低加密强度，支持密钥和证书的防篡改保护。

除了上述安全特性，山石网科 ADC 可以和山石网科下一代防火墙、Web 应用防火墙、山石云·格、山石云·界、内网安全等产品配合使用，为应用系统构建从网络接入到数据中心的端到端安全交付方案。

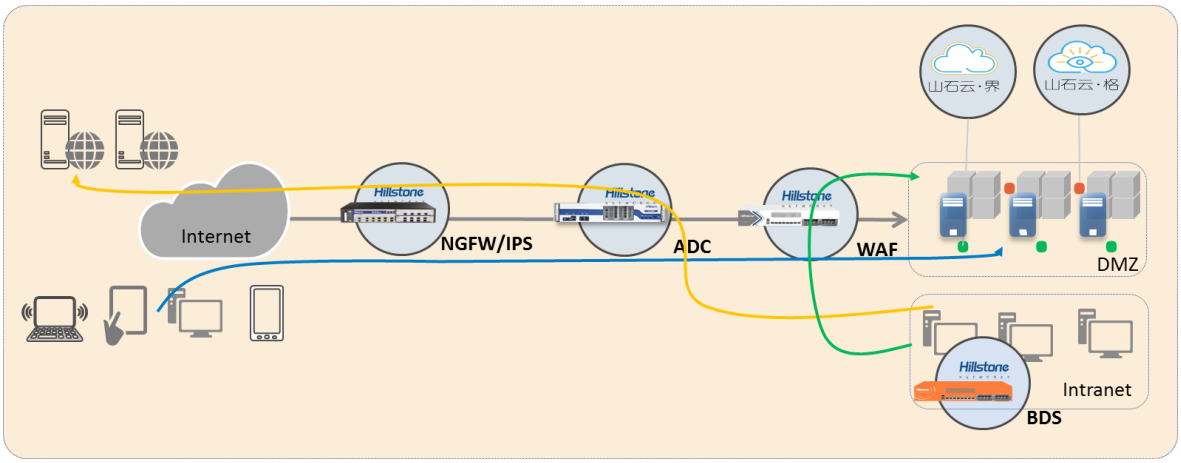


图 3. 山石网科端到端安全防护方案

## 3.2 连接复用技术（Connection Multiplexing）

在反向代理模式下，山石网科 ADC 支持通过连接复用技术减小后台服务器的负载，提升应用平台的处理能力。

- 山石网科 ADC 预先与后台服务器之间建立多个连接，并保持住它们（每个服务器最多预先建立 20 个连接）。
- 当有客户端请求被分配到某个后台服务器上时，山石网科 ADC 从预先建立的连接池中选择一个连接，在此连接上发送客户端的请求，一个连接可以被用来传送多个请求。

通过连接复用技术，为后台服务器节省了建立、拆除和维持客户端连接所需要的资源；也使得整个应用系统在突发流量下能保持更高的处理能力。

### 3.3 HTTP 压缩

HTTP 压缩是一种对 Web 服务器返回浏览器的内容进行压缩的方式。HTTP 压缩使用公共域压缩算法来压缩服务器上的 HTML、JavaScript、CSS 和其他文本文件。利用 HTTP 压缩技术，山石网科 ADC 可将 HTTP 的传输性能提升为原来的 5 倍，大幅节省传送网络服务与其他动态内容时所需的带宽。

### 3.4 内容缓存

随着用户数量的增加，Web 服务器的负载会越来越大，这时用户必须投资更换或增加服务器，势必会增加管理成本。山石网科 ADC 的内容缓存可以有效地减轻服务器的负担，提高整个应用平台的处理能力。将山石网科 ADC 放在服务器的前端，通过 ADC 上的内存缓存来响应用户的请求，服务器仅处理动态的内容，可以最大化的提高网络用户访问本网站内容的速度。

### 3.5 SSL 卸载

在安全问题层出不穷的今天，基于 Web 的应用需要一个更安全的网络承载环境，SSL(Secure Sockets Layer 安全套接层）加密技术因此而出现。SSL 的主要目标是为两个通信主体提供数字证书身份验证、保密、可靠的信道，并能够防数据篡改。目前，互联网上超过 50% 的流量已经采用 SSL 来进行保护，尤其是网银、支付等安全性要求较高的应用，已经普遍采用 SSL 加密的部署形式。

由于SSL运算需要耗费大量的CPU资源和内存资源，势必造成服务器资源的巨大消耗，进而影响交易的质量。山石网科 ADC 采用专用硬件来替代应用服务器进行 SSL 加解密处理，确保在进行安全交易和其它应用时具有快速和可靠的连接，减轻服务器上 CPU 密集型处理的负担，大幅缩短服务器的响应时间。

## 四、服务器负载均衡的客户价值

通过山石网科 ADC 的服务器负载均衡解决方案，能够完美解决应用系统所面临的各种问题，确保业务系统的可用性、可扩展性、安全性和性能保障。

- 在多台服务器之间合理分配流量，消除服务器负载不平衡的现象。
- 多台服务器互为备份，解决业务系统的单点故障隐患。
- 通过 SSL 卸载、连接复用等技术，提高业务系统的整体处理性能。
- 结合山石网科下一代防火墙等安全产品，提供端到端的安全交付。