**[反向代理服务器的工作原理](http://blog.csdn.net/keyeagle/article/details/6723408)**

**一  概述**

               反向代理（Reverse Proxy）方式是指以代理服务器来接受Internet上的连接请求，然后将请求转发给内部网络上的服务器；并将从服务器上得到的结果返回给Internet上请求连接的客户端，此时代理服务器对外就表现为一个服务器。

               通常的代理服务器，只用于代理内部网络对Internet的连接请求，客户机必须指定代理服务器,并将本来要直接发送到Web服务器上的http请求发送到代理服务器中。当一个代理服务器能够代理外部网络上的主机，访问内部网络时，这种代理服务的方式称为反向代理服务。

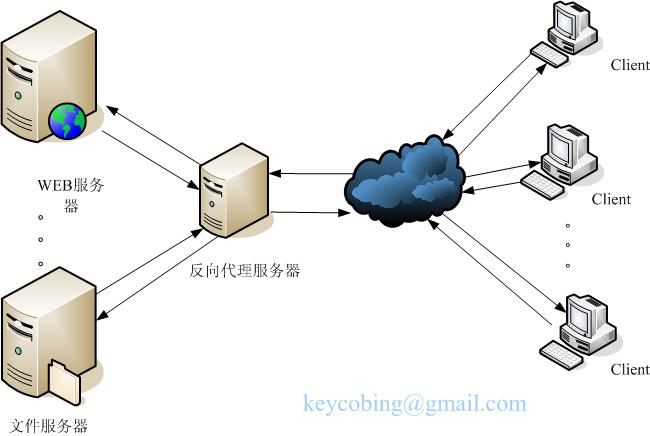


图1  反向代理服务器的基本原理

       二  反向代理服务器的工作原理

                    反向代理服务器通常有两种模型，它可以作为内容服务器的替身，也可以作为内容服务器集群的负载均衡器。

              1，作内容服务器的替身

                     如果您的内容服务器具有必须保持安全的敏感信息，如信用卡号数据库，可在防火墙外部设置一个代理服务器作为内容服务器的替身。当外部客户机尝试访问内容服务器时，会将其送到代理服务器。实际内容位于内容服务器上，在防火墙内部受到安全保护。代理服务器位于防火墙外部，在客户机看来就像是内容服务器。

                   当客户机向站点提出请求时，请求将转到代理服务器。然后，代理服务器通过防火墙中的特定通路，将客户机的请求发送到内容服务器。内容服务器再通过该通道将结果回传给代理服务器。代理服务器将检索到的信息发送给客户机，好像代理服务器就是实际的内容服务器（参见图 2）。如果内容服务器返回错误消息，代理服务器会先行截取该消息并更改标头中列出的任何 URL，然后再将消息发送给客户机。如此可防止外部客户机获取内部内容服务器的重定向 URL。

                  这样，代理服务器就在安全数据库和可能的恶意攻击之间提供了又一道屏障。与有权访问整个数据库的情况相对比，就算是侥幸攻击成功，作恶者充其量也仅限于访问单个事务中所涉及的信息。未经授权的用户无法访问到真正的内容服务器，因为防火墙通路只允许代理服务器有权进行访问。

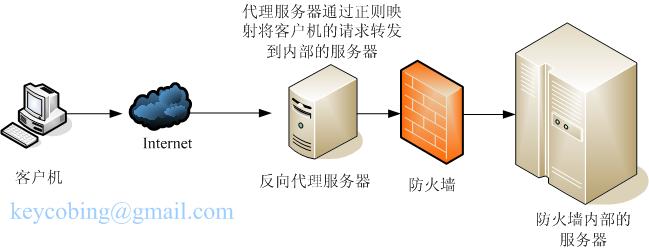


图2  反向代理服务器作为内容服务器的替身

                   可以配置防火墙路由器，使其只允许特定端口上的特定服务器（在本例中为其所分配端口上的代理服务器）有权通过防火墙进行访问，而不允许其他任何机器进出。

               2，作为内容服务器的负载均衡器

                   可以在一个组织内使用多个代理服务器来平衡各 Web 服务器间的网络负载。在此模型中，可以利用代理服务器的高速缓存特性，创建一个用于负载平衡的服务器池。此时，代理服务器可以位于防火墙的任意一侧。如果 Web 服务器每天都会接收大量的请求，则可以使用代理服务器分担 Web 服务器的负载并提高网络访问效率。

                   对于客户机发往真正服务器的请求，代理服务器起着中间调停者的作用。代理服务器会将所请求的文档存入高速缓存。如果有不止一个代理服务器，DNS 可以采用“循环复用法”选择其 IP 地址，随机地为请求选择路由。客户机每次都使用同一个 URL，但请求所采取的路由每次都可能经过不同的代理服务器。

                   可以使用多个代理服务器来处理对一个高用量内容服务器的请求，这样做的好处是内容服务器可以处理更高的负载，并且比其独自工作时更有效率。在初始启动期间，代理服务器首次从内容服务器检索文档，此后，对内容服务器的请求数会大大下降。

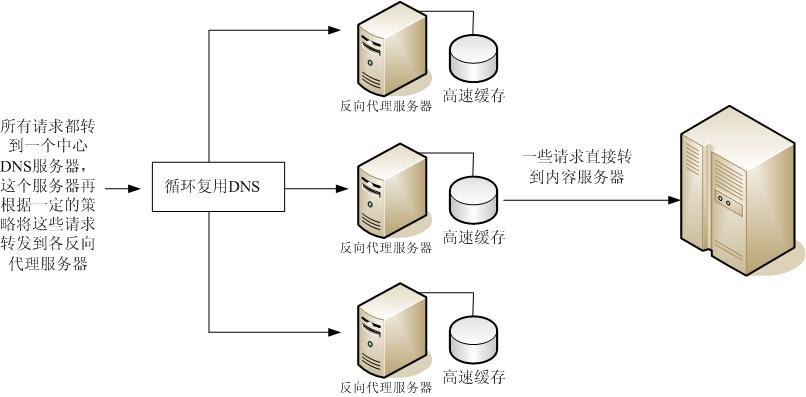


图3  反向代理服务器作为负载均衡器