网络防火墙设计中的重点问题（2） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/470/2021_2022__E7_BD_91_E7_BB_9C_E9_98_B2_E7_c67_470706.htm 显然，此时防火墙还必须实现路由转发，使内外网之间的数据包能够透明的转发。另外， 防火墙要起到防火墙的作用，显然还需要把数据包上传给本身应用层处理（此时实现应用层代理、过滤等功能），此时需要端口转发来实现（？这个地方不是十分清 楚，也没找到相关资料）。透明模式和非透明模式在网络拓扑结构上的最大区别就是：透明模式的两块网卡（与路由器相连的和与内网相连的）在一个网段（也和子 网在同一个网段）；而非透明模式的两块网卡分别属于两个网段（内网可能是内部不可路由地址，外网则是合法地址）。 这个过程如下：1. 用ARP代理实现路由器和子网的透明连接（网络层） 2. 用路由转发在IP层实现数据包传递（IP层） 3. 用端口重定向实现IP包上传到应用层（IP层） 前边我们讨论过透明代理，和这里所说的防火墙的透明模式是两个概念。透明代理主要是为实现内网主机可以透明的访问外网，而无需考虑自己是不可路由地址还是可路由地址。内网主机在使用内部网络地址的情况下仍然可以使用透明代理，此时防火墙 既起到网关的作用又起到代理服务器的作用（显然此时不是透明模式）。需要澄清的一点是，内外网地址的转换（即NAT，透明代理也是一种特殊的地址转换）和透明模式之间并没有必然的联系。透明模式下的防火墙能实现透明代理，非透明模式下的防火墙（此时它必然又是一个网关）也能实现透明代理。它们的共同点在于可以简化内网客户的设置而已。 目前国内大

多防火墙都实现了透明代理，但实现了透明模式的并不多。这些防火墙可以很明显的从其广告中看出来：如果哪个防火墙实现了透明模式，它的广告中肯定会和透明代理区分开而大书特书的。 5．可靠性 防火墙系统处于网络的关键部位，其可靠性显然非常重要。一个故障频频、可靠性很差的 产品显然不可能让人放心，而且防火墙居于内外网交界的关键位置，一旦防火墙出现问题，整个内网的主机都将根本无法访问外网，这甚至比路由器故障（路由器的 拓扑结构一般都是冗余设计）更让人无法承受。 防火墙的可靠性也表现在两个方面：硬件和软件。 国外成熟厂商的防火墙产品硬件方面的可靠性一般较高，采用专门硬件架构且不必多说，采用PC架构的其硬件也多是专门设计，系统各个部分从网络接口到存储设备（一般为电子硬盘）集成在一起（一块板子），这样自然提高了产品的可靠性。 国内则明显参差不齐，大相径庭，大多直接使用PC架构，且多为工业PC，采用现成的网卡，DOC/DOM作为存储设备。工业PC虽然可靠性比普通PC要高不少，但是毕竟其仍然是拼凑式的，设备各部分分立，从可靠性的角度看显然不如集成的（著名的水桶原理）。国内已经有部分厂家意识到了这个问题，开始自行设计硬件。但大多数厂家还是从成本的角度考虑使用通用PC架构。 另外一方面，软件可靠性的提高也是防火墙优劣的主要差别所在。而国内整个软件行业的可靠性体系还没有成熟，软件可靠性测试大多处于极其初级的水平（可靠性测试和bug测试完全是两个概念）。一方面是可靠性体系建立不起来，一方面是为了迎合用户的需求和跟随网络应用的不断发展，多数防火墙厂商一直处于不断的扩充和修改中，其可靠性更不能让人恭

维。 总的来说，如同国内大多数行业（除了少数如航天、航空）一样，网络安全产品特别是防火墙的可靠性似乎还没有引起人们的重视。 6．市场定位 市场上防火墙的售价极为悬殊，从数万元到数十万元，甚至到百万元不等。由于用户数量不同，用户安全要求不同，功能要求不同，因此防火墙的价格也不尽相同。厂商因而也有所区分，多数厂家还推出模块化产品，以符合各种不同用户的要求。总的说来，防火墙是以用户数量作为大的分界线。如checkpoint的一个报价：CheckPoint Firewall-1 4.1 25user 19000.00 CheckPoint Firewall-1 4.1 50user 31000.00 CheckPoint Firewall-1 4.1 100user 51000.00 CheckPoint Firewall-1 4.1 250user 64000.00 CheckPoint Firewall-1 4.1 无限用户 131000.00 从用户量上防火墙可以分为： a． 10－25用户： 这个区间主要用户为单一用户、家庭、小型办公室等小型网络环境。防火墙一般为10M（针对硬件防火墙而言），两网络接口，涵盖防火墙基本功能：包过滤、透明模式、网络地址转换、状态检测、管理、实时报警、日志。一般另有可选功能：VPN、带宽管理等等。这个区间的防火墙报价一般在万元以上2万元以下（没有VPN和带宽管理的价格更低）。据调查，这个区间的防火墙反而种类不多，也许是国内厂商不屑于这个市场的缘故？ b． 25－100用户 这个区间用户主要为小型企业网。防火墙开始升级到100M，三或更多网络接口。VPN、带宽管理往往成为标准模块。这个区间的防火墙报价从3万到15万不等，根据功能价格有较大区别。相对来说，这个区间上硬件防火墙价格明显高于软件防火墙。目前国内防火墙绝大部分集中在这个区间中。 c． 100－数百用户 这个区间主要为中型企业网，重要网站、ISP、ASP、数

据中心等使用。这个区间的 防火墙较多考虑高容量、高速度、低延迟、高可靠性以及防火墙本身的健壮性。并且开始支持双机热备份。这个区间的防火墙报价一般在20万以上。这样的中高端 防火墙国内较少，有也是25－100用户的升级版，其可用性令人怀疑。 d. 数百用户以上 这个区间是高端防火墙，主要用于校园网、大型IDC等等。我们接触较少，不多做讨论。当然其价格也很高端，从数十万到数百万不等。 总的来说，防火墙的价格和用户数量、功能模块密切相关，在用户数量相同的情况下，功 能越多，价格就越贵。
如Netscreen的百兆防火墙： NetScreen-100f(AC Power) -带防火墙 流量控制等功能,交流电源,没有VPN功能报价在￥260,000
而在此基础上增加了128位VPN功能的报价则高出5万元：
￥317,500 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com