AR系列路由器防火墙的分类

姚忆斌 2007-01-15 发表

AR系列路由器防火墙的分类

Q：在AR系列路由器上，防火墙分为哪几类，它们的原理是什么？
A：一般把防火墙分为两类：网络层防火墙、应用层防火墙。网络层的防火墙主要获取数据包的包头信息，如协议号、源地址、目的地址和目的端口等，或者直接获取包头的一段数据；而应用层的防火墙则对整个信息流进行分析。
常见的防火墙有以下几种：
应用网关（Application Gateway）：检验通过此网关的所有数据包中的应用层的数据。如FTP应用网关，对于连接的Client端来说是一个FTP Server，对于Server端来说是一个FTP Client。连接中传输的所有FTP数据包都必须经过此FTP应用网关。
电路级网关（Circuit-Level Gateway）：此电路指虚电路。在TCP或UDP发起（Open）一个连接或电路之前，验证该会话的可靠性。只有在握手被验证为合法且握手完成之后，才允许数据包的传输。一个会话建立后，此会话的信息被写入防火墙维护的有效连接表中。数据包只有在它所含的会话信息符合该有效连接表中的某一条目（Entry）时，才被允许通过。会话结束时，该会话在表中的条目被删掉。电路级网关只对连接在会话层进行验证。一旦验证通过，在该连接上可以运行任何一个应用程序。以FTP为例，电路层网关只在一个FTP会话开始时，在TCP层对此会话进行验证。如果验证通过，则所有的数据都可以通过此连接进行传输，直至会话结束。
包过滤（Packet Filter）：对每个数据包按照用户所定义的项目进行过滤，如比较数据包的源地址、目的地址等是否符合规则。包过滤不管会话的状态，也不分析数据。如用户规定允许端口是21或者大于等于1024的数据包通过，则只要端口符合该条件，数据包便可以通过此防火墙。如果配置的规则比较符合实际应用的话，在这一层能够过滤掉很多有安全隐患的数据包。
地址转换（NAT）：地址转换又称地址代理，它实现了私有网络访问外部网络的功能。地址转换的机制就是将私有网络内主机的IP地址和端口替换为路由器的外部网络地址和端口，以及从路由器的端口转换为私有网络主机的IP地址和端口，即<私有地址+端口>与<公有地址+端口>之间的转换。私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的IP地址。