

积极安全防御和 消极安全防御

在构建安全的网络环境的过程中，安全产品作为第一道安全防线，正受到越来越多用户的关注。

安全产品是指设置在不同网络或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据管理者的安全政策控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，安全产品是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。

从安全产品对各种攻击的应对方法来说，安全产品的工作原理有两种：积极安全防御模型和消极安全防御模型。下面分别介绍：

积极安全防御

积极安全防御的原理是：对正常的网络行为建立模型，把所有通过安全设备的网络数据拿来和保存在模型内的正常模式相匹配，如果不是这个正常范围以内，那么就认为是攻击行为，对其做出处理。这样做的最大好处是可以阻挡未知攻击，即：黑客才发现的不为人所知的攻击方式——网络安全的最大隐患。对这种方式来说，建立一个安全的、有效的模型就可以对各种攻击做出反应了。具有代表性的产品有网络防火墙、应用防火墙。

一个简单的例子就是网路防火墙中的状态检测技术，管理员可以配置基于网络地址、端口和协议的允许访问的规则，只要不是这些允许的访问，都禁止访问。在防火墙运行过程中，根据允许访问的规则建立动态状态表项，只有符合这些合法状态表项的访问数据才允许通过防火墙，其他的所有访问都禁止通行。网络防火墙在网络层做到了积极安全防御。但是对于应用层数据，由于网络防火墙不理解，所以对于应用层的攻击，网络防火墙也是无能为力的。

应用防火墙也是和网络防火墙一样，通过积极安全防御模型来防范攻击，但是最大的不同是应用防火墙建立的允许访问的规则是描述应用的，而不是描述网络地址、端口和协议号等网络层的信息。应用防火墙建立对应用描述的允许规则以后，对所有的应用层数据进行检查，判断是否允许通过的应用层数据，如果不

是，就禁止通行，这样的原理可以防护未知攻击，因为各种针对应用的攻击和未知的攻击都不包括在允许访问的应用层描述规则集中。

消极安全防御

消极安全防御的原理是：以已经发现的攻击方式，经过专家分析后给出其特征进而来构建攻击特征集，然后在网络数据中寻找与之匹配的行为，从而起到发现或阻挡的作用。它的缺点是使用被动安全防御体系的安全产品不能对未被发现的攻击方式做出反应。具有代表性的产品有部分入侵检测系统（IDS），入侵防御系统（IPS），病毒防火墙等。

消极安全防御的一个主要特征就是针对已知的攻击，建立攻击特征库，作为判断网络数据是否包含攻击特征的依据。使用消极安全防御模型的产品，可以作为网络安全防御体系中的一个补充，但是由于对未知攻击的无能为力以及不断的数据库更新，起到的作用比较有限，同时对网路的性能有一定的影响。

从上可以看出积极安全防御相对安全和有效，但是它的技术实现更加复杂。随着厂商对积极安全防御的重视，以及技术的不断发展，使用积极安全防御模型的安全产品将会日益完善。