

第8章 Cisco PIX防火墙 软件和硬件

- ❖ 防火墙技术的三种类型
- ❖ PIX防火墙的特性
- ❖ 硬件中的软件
- ❖ PIX防火墙的型号

防火墙的类型

防火墙可以定义为数据包过滤器、代理过滤器和状态型数据包过滤器3种类别之一。

❖ 数据包过滤器

采用TCP/IP数据包过滤器的防火墙通常在传送层或TCP/IP协议栈的Internet层分析网络数据流。只要在一个特定的网络中流动的数据是建立在标准的TCP/IP协议栈（或任何其他标准协议栈）之上，那么就可以对数据流进行过滤。在网络中流动的每个数据包中的字段是已知的（例如源IP地址、目的IP地址、源端口、目的端口）

数据包过滤器的一些缺点：

- 1>符合ACL规则的任意数据包都可以通过过滤器；
- 2>可以通过将数据包分片，使数据包通过过滤器；
- 3>很难正确地产生、实现并维护复杂的ACL；
- 4> 不能过滤某些服务（虽然可以指定端口号，但是对于一些应用，特别是比较新的多媒体应用，在会话开始之前，端口号是未知的）。

❖ 代理过滤器

代理过滤器是一种防火墙设备，它在开放系统互联（OSI）模型中较高的层次（通常是OSI模型的4到7层）上检查数据包。因为它检查会话中的更多细节，所以代理过滤器的功能非常强大，但是这同时也会影响端到端的吞吐量。这种设备通过要求用户采用代理的形式，与一个安全的系统进行通信，从而隐藏了有价值的数据。

代理过滤器可能会遇到下列问题：

- a>代理防火墙会产生单点故障，即如果对防火墙的访问受到危害，那么整个网络都将受到危害；
- b> 很难为防火墙增加新的服务；
- c> 在负载很重的情况下，代理防火墙工作得很慢；
- d> 由于代理防火墙必须采用一些操作系统服务来执行代理过程，所以他通常是建立在通用操作系统之上的。由此带来的问题是：增加了开销、降低了性能，而且由于通用操作系统是众所周知的，所以该操作系统容易被攻击的漏洞也是公开的。

❖ 状态型数据包过滤器

这种过滤器综合了前两者的优点，为每个穿过防火墙建立的会话保持完整地会话状态信息。每当为输入或输出数据流建立一条IP连接时，信息都被登记在状态型会话流列表中。Cisco PIX防火墙采用状态型数据包过滤器的方法。

这个方法之所以有效，是因为它：

- a>对单个数据包进行操作，并将单个数据包与已经建立起来的连接进行比较；
- b> 相对于数据包过滤或使用代理多滤器，它的处理性能水平更高；
- c> 为每条连接或无连接交易在列表中记录数据。这个列表将被作为参考点来决定数据包是属于一条已经存在的连接，还是来自一个未经授权的源。

PIX 防火墙特性

Cisco PIX防火墙提供下列好处和特性：

- ❖ 安全、实时的嵌入式系统——与对每个数据包进行全面处理的典型代理过滤器不同，PIX防火墙采用一种安全的、实时的嵌入式系统，增强了网络的安全性；
- ❖ 自适应安全算法（ASA）——它为Cisco PIX防火墙实现了状态型连接控制；
- ❖ 直通型代理——一种基于用户的、对输入和输出连接进行认证的方法，它的处理开销较低，因此相对于代理过滤器提高了处理性能。
- ❖ 状态型故障切换/热备份——Cisco PIX防火墙使我们能够在一种完全冗余的拓扑结构中，配置两个Cisco PIX防火墙单元

PIX防火墙的心脏是ASA。采用ASA时，PIX执行下列状态型数据包过滤过程：

- ❖ 它得到会话识别参数，比如每条TCP连接的IP地址和端口号；
- ❖ 它在状态型连接表中登记数据，并产生一个会话对象；
- ❖ 它将输入和输出数据包与连接表中的会话对象进行比较；
- ❖ 只有在存在一条适当的连接来准许的情况下，它才允许数据包通过PIX防火墙；
- ❖ 当连接被终止时，连接信息和会话对象将被最终删除。

PIX 防火墙的型号

- ❖ 下面是PIX防火墙当前可用的5种型号：
- ❖ Cisco Secure PIX 506——5种型号中最小的，506适用于高端的小型办公室/家庭办公室(SOHO)机构，具有10Mbit/s的测试吞吐量。
- ❖ Cisco Secure PIX 515——适用于中小型企业 and 远程办公环境，具有120Mbit/s的测试吞吐量，能够处理125 000个并发会话。
- ❖ Cisco Secure PIX 520——适用于大型企业和复杂的高端流量环境。它的吞吐量可以达到370Mbit/s，能够处理250 000个并发会话。

- ❖ Cisco Secure PIX 525——适用于企业和服务提供商，具有370Mbit/s的吞吐量，能够处理多达280 000个并发会话。
- ❖ Cisco Secure PIX 535——它是PIX 500系列最新和最大的补充，535适用于企业和服务商，具有1Gbit/s的吞吐量，能够处理500000个并发连接。