理解CiscoPIX防火墙的转换和连接 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E7_90_86_E8_A7_A3Cisc_c101_142421.htm 1.ASA安全等级 默认情况下，Cisco PIX防火墙将安全等级应用到每一个接口。越安全的网络段， 安全级别越高。安全等级的范围从0~100,默认情况下，安全等级0适应于e0,并且它的默认名字是外部(outside),安全等级100适应于e1.并且它的 默认名字是inside. 使用name if 可以配置附加的任何接口，安全等级在1~99之间 e.g: nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 dmz security50 1.1自适应安全算法(ASA)允许流量从高安全等级段流向低安全等级段，不需要在安全策略中使用特定规则来允许这些连接，而只要用一个nat /global命令配置这些接口就行了。 1.2同时如果你想要低安全等级段流向一个高安全等级段的流量必须经过安全策略(如acl或者conduit). 1.3如果你把两个接口的安全等级设置为一样，那流量不能流经这些接口 请记得ASA是cisco pix防火墙上状态连接控制的关键。 2.传输协议 2.1首先请理解一下OSI的7层模型，说实话，如果你要做IT,那么这个OSI的7层模型一定要搞懂，也就像windows 的DNS一样，一定要花工夫在 上面。其中1~7是从物理层向上数的，物理层为第一层，应用层为第七层。 应用层 数据 表示层 数据 会话层 数据 传输层 Segment 网络层 Packet 数据链路层 Frame 物理层 Bit 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