部署IOS防火墙认证代理(AP) PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/284/2021_2022__E9_83_A8_E7_BD_B2IOS_E9_c101_284188.htm 目前，介于互联网的很多不安全因素，很多中小型企业还没有部署防火墙，作为一种临时过渡的手段，广泛地使用到了Authentication Proxy，简称AP. 回顾一下，锁和密钥，它要求用户先TELNET到路由器上进行认证，然后，TELNET被路由器终止，并为用户建立一个动态的ACL条目以便允许流量通过路由器，这是一个极好的特性，但同时存在一些不足： 1）主要为拔号用户开发的，这里只有一个用户访问路由器接口。 2）应用到该接口的扩展ACL只有一个动态条目，所有用户必须共享该ACL，这样就不能执行基于每个用户的限制。 3）它要求首先TELNET到路由器上要求用户知道该认证过程。该过程必须在用户可以访问动态ACL条目中指定的资源前首先发生。 为了克服这些不足，CISCO开发了认证代理（AP）。AP基本上是锁和密钥的增强版，是CISCO IOS防火墙特性集的一部分，类似于CISCO PIX的直通代理（CUT-THROUGH PROXY）。 通过一个实际访问过程来分析AP的工作步骤： 1）一个用户首先打开了到内部WEB服务器的HTTP连接 2）由于需要经过这台配置了AP的路由器，所以，路由器打开了HTTP认证机制，它截取HTTP连接请求。路由器发送一个输入用户名和密码的提示。 3）用户输入用户名和密码。 4）路由器接收到认证信息时，它会将它通过TACACS 或者RADIUS转发到AAA服务器。 5）AAA服务器认证用户，如果用户被成功认证，AAA服务器将用户访问档案发给路由器。访问档案基本上

是一个ACL语句组成的简化组，这些语句定义了允许用户访问什么。 6）如果用户认证成功，用户获得一个弹出窗口，表明认证成功。路由器将访问档案转换成实际的临时ACL条目，然后将这些条目在适当的输入方向激活。这些条目实际上允许了什么样的资源允许被该认证的用户访问。最后，实现了用户到指定资源的访问。 配置AP五个步骤：（1）在路由器中配置AAAAaa new-modelTacacs-server host ip_address timeout seconds key encryption_keyAaa authentication login default group tacacs Aaa authorization auth-proxy default group tacacs Aaa accounting auth-proxy default start-stop group tacacs （如果执行计帐） 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