无线portal认证的推送认证页面服务器和portal认证服务器不同的经验案例

Portal 裴锐霖 2015-11-08 发表

在做portal认证时，推送页面的服务器和完成portal认证的服务器不是同一台。即web服务器只负责给客户端推送认证页面，客户端填入用户名和密码，提交时，会提交给另外的portal服务器或AC，在此案例中是由AC来完成一个本地portal的认证。基本思路如下：

（1）AC开启local portal server。如下，ip是AC的IP，url是portal server的；

portal server p1 ip *x.x.x.x* url http://*y.y.y.y*/logon.htm server-type imc

（2）AC负责重定向，把用户的HTTP请求指引到第三方Portal server的登陆页面，配置free rule放通去往第三方Portal server；

（3）第三方Portal server推送的登陆页面内嵌了AC的local portal server URL；

（4）用户在第三方Portal server登陆页面上提交用户名/密码时实际上直接提交到AC的local portal server；

（5）AC跟Radius交互后负责推送认证成功页面或者认证失败页面；

（6）如果认证成功后还想推送广告页面，可以在认证成功页面窗口直接跳转到广告页面（也就没有了认证成功页面，没有了下线按钮），或者由认证成功页面自动新开一个窗口跳转到广告页面。

不能在最初的第三方portal server推送的登陆页面上跳转到广告页面。

具体原因：初始登陆页面是第三方portal server的，后续认证成功页面是AC的，用户终端上登陆页面和认证成功页面属于不同IP地址和端口，java脚本由于安全性是互相隔离无法访问的。所以通过认证成功页面中执行java脚本让登陆页面跳转广告页面完全不可行。

（7）用户的异常下线只能通过AC的流量检测idle-cut来识别。

（8）第三方portal server在用户的整个上网过程中，不保存用户信息，不直接跟AC交互，仅仅提供初始登陆页面和广告页面（广告页面有可能还是其他server提供），实现很简单。

第三方Portal server推送的登陆页面，内嵌关键内容如下，即提交用户名/密码直接指向AC的local portal server URL。

红色关键字是固定的，不要随便修改！x.x.x.x是AC的IP。

type=SUBMIT value='Logon' name='PtButton' style='width:60px;' onclick='form.action="http://x.x.x.x/portal/logon.cgi"+location.search;'>

网络由AC、AP、Web服务器，radius服务器组成。终端接入无线网络，终端访问网络的时候，AC负责把web页面重定向到web服务器，web服务器推送认证页面（在推送的web页面中携带了一段脚本）。客户端填入用户名密码，点击提交时，把用户名和密码提交给AC，AC此时就会完成一个完整的portal本地认证。

web服务器携带的脚本就是AC做本地认证时，所使用的默认url：http://192.168.63.200/portal/logon.html

```
 portal server portal ip 192.168.63.200 url http://192.168.0.13/ server-type imc
 portal free-rule 5 source ip any destination ip 192.168.0.13 mask 255.255.255.255
 portal local-server http
    portal redirect-url http://portal.ffan.com/loginsuccess
radius scheme portal
 server-type extended
 primary authentication 192.168.100.240
 primary accounting 192.168.100.240
 key authentication cipher $c$3$BwAluzyML+/+N6KRI260IUoL/wvqiA==
 key accounting cipher $c$3$3mx9N2Io9y0481kfoYZ/xs5caGKTeQ==
 user-name-format without-domain
domain imc
 authentication portal radius-scheme portal
 authorization portal radius-scheme portal
 accounting portal radius-scheme portal
 access-limit disable
 state active
 idle-cut enable 120 1024
 self-service-url disable
interface Vlan-interface30
 ip address 192.168.63.200 255.255.224.0
 portal server imc method direct
 portal domain imc
```

portal nas-ip 192.168.63.200
其他无线的配置和服务器的配置和传统的一样，在此不做详细描述。
注：其中192.168.63.200是AC本地接口地址，192.168.0.13是web服务器地址，http://portal.ffan.com/loginsuccess 是认证成功后跳转到想要的广告页面

<1> portal server portal ip 192.168.63.200 url http://192.168.0.13/ server-type imc
此处的ip地址是AC的vlan接口地址，即完成portal认证是的服务器。(注意：目前发现P29版本有个特点就是只要ip地址配置成AC的本地接口地址，那么在重定向时就默认成本地portal认证的页面，不会去重定向url后面的内容，所以P29版本是不能实现此需求的。)
<2> http://192.168.0.13/是第一次推送的认证页面。
<3> portal free-rule 5 source ip any destination ip 192.168.0.13 mask 255.255.255.255
需放通web服务器，以便客户端重定向成功时访问。
<4> portal local-server http 配置portal本地认证功能