从VPN登陆BOMC的方案

2013-5-31

## 一、VPN登陆

需要为BOMC再单独建设一个VPN站点，外网用户可以通过该VPN站点登陆VPN。登陆成功后，会为该用户分配一个私网的IP地址。关于VPN这块内容，会有专业人员负责，这里不再详细说明。

## 二、互联网域

在互联网域主机（10.96.24.181）上架设一个BOMC的web反向代理服务器，用户使用分配的私网IP，通过指定的端口（28080，48080）访问该web反向代理服务器，该web反向代理服务器把请求转入核心域BOMC的web，然后把核心域BOMC的web响应再通过web反向代理服务器转出给外网用户。

## 三、核心域

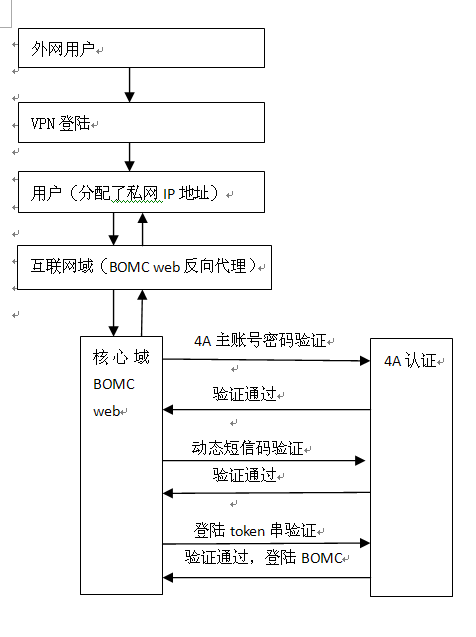
目前核心域有两台BOMC的web服务器（10.87.21.52，10.87.21.110），用来和4A进行交互，完成登陆认证和把登陆日志传给4A；用来接收来自互联网域的请求，并完成响应。

## 四、和4A的登陆认证

和4A的登陆认证全部在核心域进行，具体过程如下：

1. 用户请求登陆界面，输入4A主账号和密码
2. 调用4A服务验证主账号和密码
3. 主账号验证通过后，登陆界面显示短信码输入框，同时用户收到短信码
4. 用户输入短信码
5. 调用4A服务验证短信码
6. 短信码验证通过后，界面会显示出该4A主账号对应的所有BOMC从账号
7. 用户选择一个BOMC从账号，点击登陆
8. 调用4A的创建token服务，获得一个token字符串
9. 使用该token串登陆BOMC
10. 在BOMC里面调用4A服务，并把该token串传给4A进行验证
11. token串验证通过后，跳转到BOMC的首页，已经登陆成功BOMC

## 五、全过程流程图



## 六、登陆日志

登陆时，由BOMC的sso把登陆日志通过socket的方式传给4A，其中日志内容中会带有从VPN登陆等关键字，来标明该用户是从VPN登陆的。

## 七、BOMC登陆过程详解

bomc开发自己的登录页面，通过4A账号+密码进行认证。强认证方式只保留短信密钥方式，通过调用4A提供的webservice服务接口，实现所有认证功能。4A在认证成功后，会将登录日志发送给审计库中，bomc登录系统后，所有的操作日志也要发送给4A审计系统。以下为整个登录过程的时序图，请查看:

