FortiAC +FortiAP 外置 Portal 与微信认证延伸方案测试介绍

版本	1.0
时间	2015 年 3 月
支持的版本	FortiOS v5.2.x，FortiAP5.0.x
作者	李威峰、谢惠存
状态	草稿
反馈	support_cn@fortinet.com

目录

介绍.....3
拓扑.....3
组件.....3
工作原理.....3
Portal 认证延伸.....6
1. 根据终端类型弹出不同的 Portal.....6
2. 一键上网（免认证）.....7
微信认证.....9
认证流程与原理.....9
微信认证例外 IP 地址.....11
IOS 微信认证注意事项.....12

介绍

Portal 认证与微信认证目前在企业认证较为普遍（当然还有扫二维码认证方式），Fortinet 之前文档已经对 FG 配合外置 Portal 认证做过详细的介绍。

从技术原理上讲，微信认证与 portal 认证都是使用 HTTP 流量触发 URL 重定向方式，仅仅是对于客户端体验不同。

目前 FGT 与宁顿配合可以实现不同终端类型弹出不同的 Portal 页面。

比如 PC 适合 PC 屏幕 Portal 页面，手机弹出适合手机屏幕比较简洁的 Portal 界面，这些需要 FGT 与 Portal 服务器紧密配合。

本文主要外置 Portal 认证与微信认证做一个延伸的介绍。

拓扑

|----------Radius（服务器）
无线客户端（win7, IOS Android）-- FortiAP223----FortiAC（FGT）---外置 Portal（微信服务器）

AP-AC 使用集中转发模式，非常简单。

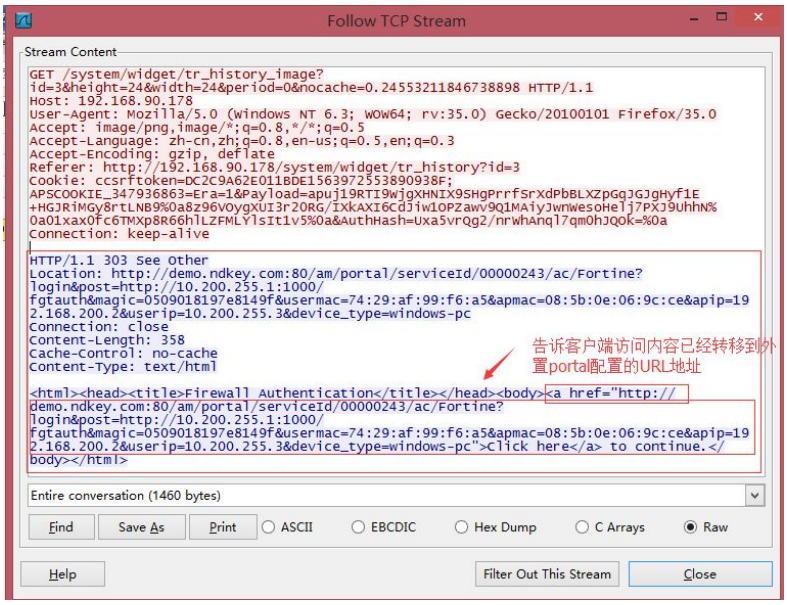
组件

序号	组件名称	软件版本	数量	备注
1	FGT60C	V5.2.3	1	FortiAC （无线控制器）
2	FortiAP-223B	V5.0.9	1	无线 AP
3	外置 Portal 与微信服务器		1	本次采用上海宁顿平台
4	Radius 服务器		1	本次测试采用上海宁顿平台

工作原理

让我们再回顾一下原理：

1. 无线客户端发起访问 HTTP 请求。
2. FortiAC 使用 HTTP 代理方式欺骗无线客户端并告诉客户端访问在在外置 portal 中配置的 URL 地址，并携带一些参数和值，此处很重要。此时 portal 服务器根据此做进一步的判断（弹出不同的页面，把客户端 IP 或 mac 入到库中）



<a
href="http://demo.ndkey.com:80/am/portal/serviceId/00000243/ac/Fortine?login&
post=http://10.200.255.1:1000/fgtauth&magic=0509018197e8149f&usermac=74:29:
af:99:f6:a5&apmac=08:5b:0e:06:9c:ce&apip=192.168.200.2&userip=10.200.255.3&d
evice_type=windows-pc">Click here to continue.</body></html>

其中

href="http://demo.ndkey.com:80/am/portal/serviceId/00000243/ac/Fortine 重定向的 URL（外置 portal 地址）
post=http://10.200.255.1:1000/fgtauth 为 FortiAC SSID 接口的 IP 地址。即无线终端从 FortiAC 的发起访问的那个接口的 IP 地址。

magic=0509018197e8149 为此会话的 ID，每次都不一样。

usermac=74:29:af:99:f6:a5 无线终端 MAC 地址
apmac=08:5b:0e:06:9c:ce AP 的 MAC 地址
apip=192.168.200.2 AP 的 IP 地址
userip=10.200.255.3 无线终端的 IP 地址
device_type=windows-pc" 无线终端的设备类型

3. 客户端与重定向后的 URL 页面建立连接，弹出外置 portal 认证窗口


宁盾WIFI
旨在挖掘
商用WiFi
经营价值
发送验证码成功
确定
短信验证登录
手机号码
13581646752
验证码
发送验证码
我已阅读并接受免责声明条款
登录
wifi.ndkey.com


宁盾WIFI
旨在挖掘
商用WiFi
经营价值
短信验证登录
手机号码
13581646752
验证码
6743
发送验证码
我已阅读并接受免责声明条款
登录
wifi.ndkey.com


中国移动 3G
51% 14:37
10657109030760
【宁盾科技】您的密码是：6743，凭此手机号和密码免费登录本店免费WiFi，祝您愉快！
3/6
周五 19:08
【宁盾科技】您的密码是：6743，凭此手机号和密码免费登录本店免费WiFi，祝您愉快！
3/6
周五 19:10
【宁盾科技】您的密码是：5090，凭此手机号和密码免费登录本店免费WiFi，祝您愉快！
3/10
今天 14:36
来自~威峰
64 / 1

输入手机号，发送验证码。

4. 输入完用户名和密码后，最重要的在这个地方：

外置 Portal 中的 form 中的 method 方法为 post， Action 为：http://10.200.255.1:1000/fgtauth 这是 FortiAC 无线 SSID 接口的 IP 地址。
即无线客户端点击登录按钮后 把用户名和密码等一些参数和值提交给 FortiAC 的 IP。

<form method="post" action="http://10.200.255.1:1000/fgtauth"><input type="hidden" name="4Tredir" value="http://www.ndkey.com?stage=4&revisit=false&language=zh-CN,zh;q=0.8&terminalMac=74%3A29%3AAF%3A99%3AF6%3AA5&loginName=13581646752"/><input type="hidden" name="magic" value="060a0b849de794e2"/><input type="hidden" name="username" value="13581646752{#}62QH61KLAFT2"/><input type="hidden" name="password" value="gLrW5NN7LF7l"/><input type="submit" id="dkeysubmit" style="display:none"/></form></body></html>

5. FGT 收到用户名和密码后到第三方 Radius 认证，如果成功，则认证通过。

Portal 认证延伸

根据此原理，能够实现：

1. 根据终端类型弹出不同的 Portal

因为 FGT 已经把终端类型（涉及终端识别技术，DHCP 选项，HTTP UA 等）通过 URL 参数的方式送给 Portal 服务器，Portal 服务器据此判断设备类型，弹出不同

的 Portal。

PC 弹出如下的 portal：

Android 手机弹出如下的 Portal：

2. 一键上网（免认证）

在无线终端第一次认证后，再次上网时，不需要重新获取密码。可以直接点击我

要上网的页面。

原理：
因为 FGT 在第一次 URL 重定向过程中已经把 MAC 地址送到 Radius 的数据库中。

第二次上网重定向时，外置 Portal 判断该 MAC 地址的用户是否在数据库中，如果在，弹出一键上网 Portal。
用户名是手机号，密码生成在 HTTP 页面中（仅仅是无线终端看不到，实际上是有的）。

对于 FGT 来说，没有一键上网一说，并不知道这个客户之前已经认证过。则是一次新的认证过程。

微信认证

认证流程与原理

原理与 Portal 类似，当没有加关注时，通过普通的 HTTP 报文也能触发重定向的 URL。但是微信服务器（Portal）会给一个空白的页面，用户无法操作。

只有加入关注并进入 我要上网后，点击确定此时才提交用户名和密码。

用户名为终端 MAC 地址，密码动态生成（目前有用户提出用户名为微信号方式，正在测试中）。

流程：

1.扫描二维码，加关注：

2.加关注


中国移动 3G
63% 16:21
详细资料
宁盾科技华南测试1
功能介绍
用于上海宁盾科技提供测试.
查看历史消息
关注

3. 找到我要上网书签


中国移动 3G
64% 16:13
微信WIFI认证
请连接WIFI: SSID
如果您已连接, 请 点击此处 登录
如果您还未连接，请记住以下wifi密码:
pfo4(30分钟内有效)

4. 点击

触发了认证

微信我要上网按钮动作：

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /></head><body onload="document.getElementById('dkeysubmit').click();"><form method="post" action="http://10.200.255.1:1000/fgtauth"><input type="hidden" name="4Tredir" value="http://www.ndkey.com?stage=4&revisit=false&language=zh-CN&terminalMac=58%3A1F%3A28%3A0A%3A55%3A2B&loginName=58%3A1F%3A28%3A0A%3A55%3A2B"/><input type="hidden" name="magic" value="03060c85a1b6ffd5"/><input type="hidden" name="username" value="58:1F:28:0A:55:2B{#}7E5R1WWR0CMH"/><input type="hidden" name="password" value="Xe7c7w=IB>&D"/><input type="submit" id="dkeysubmit" style="display:none"/></form></body></html>

微信认证例外 IP 地址

http://dns.weixin.qq.com/cgi-bin/micromsg-bin/newgetdns?uin=0&clientversion=620888369&scene=0&net=1&md5=222d8e4ddf9d2054cfb12cf5400eff0c&devicetype=android-17&lan=zh_CN&sigver=1

分别找出：wx.qlogo.cn，long.weixin.qq.com，short.weixin.qq.com，extshort.weixin.qq.com 所对应的 IP 地址，加在免认证策略里面。

注意：不同的 DNS 解析不同的 IP 地址，实际使用时一般需要使用三大运营商（联通。电信 移动）手机解析 IP 地址并加入到认证例外的防火墙策略中。否则的会出现需要重启微信 APP，因为你加的列表不全（比如手机使用联通的 DNS 解析到一些 IP），但你在防火墙仅仅放行了电信 DNS 解析的 IP。

IOS 微信认证注意事项

因为 IOS 自带链路探测功能，如果连接到此 SSID 不能出 internet ，需要把 IOS

探测的地址加入 FGT 策略到免认证列表，否则不给你连接到该 SSID 的机会。

以下为 IOS 探测的网址：

以下为测试的域名：

1	www.appleiphonecell.com
2	captive.apple.com
3	www.itools.info
4	www.ibook.info
5	www.airport.us
6	www.thinkdifferent.us

对应的 IP 地址：

1	23.207.103.91
2	23.33.54.18
3	23.44.167.91
4	23.67.183.91
5	96.7.103.91
6	23.42.71.91
7	23.34.105.211
8	23.59.167.91
9	23.42.184.50
10	23.47.232.190
11	23.77.23.91
12	23.194.87.91
13	23.61.91.190
14	23.218.12.50
15	23.2.38.95
16	23.46.135.91
17	172.225.213.179
18	218.205.66.94
19	23.64.251.249
20	23.58.250.189

参考：

http://www.tuicool.com/articles/Irq6ra

参考资料

http://www.tuicool.com/articles/Irq6ra