

## 某局点WX6108E 本地转发集中portal认证https 重定向失败问题处理经验案例

Portal 刘文峰 2017-12-17 发表

某局点采用WX6108E部署无线网络，当前业务流量比较大，采用的本地转发的方式，但是后期由于需要做准入控制，在ap和ac 上部署portal 认证，配置完本地转发集中portal 认证之后，测试http 重定向都很正常，但是测试https 重定向失败，查看ap上的配置都无任何问题，后续让客户采集debug portal 和抓包分析。

AP关键配置信息：

```
portal server h3c ip 10.1.0.202 key cipher $c$3$H4RiqbGhyEUJ3fpjcTvO46BknTKkvoXnXg== url http://10.1.0.202:8097/web/scwp/auth/authIndex server-type cmcc
portal free-rule 0 source ip any destination ip 112.29.132.0 mask 255.255.255.0
portal free-rule 1 source ip any destination ip 10.1.0.22 mask 255.255.255.255
portal free-rule 2 source ip any destination ip 114.114.114.114 mask 255.255.255.255
portal free-rule 3 source ip any destination ip 211.138.180.2 mask 255.255.255.255
portal free-rule 4 source ip any destination ip 10.1.0.200 mask 255.255.255.255
portal free-rule 5 source interface GigabitEthernet1/0/1 destination any
portal free-rule 6 source ip any destination ip 10.1.0.23 mask 255.255.255.255
portal free-rule 7 source ip any destination ip 117.71.17.96 mask 255.255.255.255
portal free-rule 8 source ip any destination ip 10.1.0.201 mask 255.255.255.255
portal free-rule 9 source ip any destination ip 10.1.0.202 mask 255.255.255.255
portal free-rule 10 source ip any destination ip 10.1.0.203 mask 255.255.255.255
portal free-rule 11 source ip any destination ip 10.1.0.204 mask 255.255.255.255
portal free-rule 12 source ip any destination ip 10.1.0.205 mask 255.255.255.255
portal free-rule 13 source ip any destination ip 10.1.0.206 mask 255.255.255.255
portal free-rule 14 source ip any destination ip 10.1.0.207 mask 255.255.255.255
portal free-rule 15 source ip any destination ip 10.1.0.208 mask 255.255.255.255
portal free-rule 16 source ip any destination ip 10.1.0.209 mask 255.255.255.255
portal url-param include user-mac param-name wlanstamac
portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanuserfirsturl
portal url-param include user-ip param-name wlanuserip
portal url-param include ssid param-name ssid
portal host-check wlan
#
portal https-redirect server-policy h3c
ssl server-policy h3c
```

debug portal 信息：

```
*Dec 6 12:48:41:896 2017 test TCPHEAT/7/TCPHEAT_DEBUG: State of connection with source IP 10.15.34.52 is ESTABLISHED!
*Dec 6 12:48:41:896 2017 test TCPHEAT/7/TCPHEAT_DEBUG: PT_TCP TLS Info Description: Send TLS 1.0 Alert [length 0002], warning close_notify
*Dec 6 12:48:41:896 2017 test TCPHEAT/7/TCPHEAT_DEBUG: A connection of N/A deleted!
*Dec 6 12:48:41:896 2017 test TCPHEAT/7/TCPHEAT_DEBUG: State of connection with source IP N/A changed from ESTABLISHED to CLOSE_WAIT! //第一次三次握手，tcp被关闭了
*Dec 6 12:48:41:897 2017 test TCPHEAT/7/TCPHEAT_DEBUG: Source MAC = 7c7a-91a9-cb03 VLAN = 2119
Dec 6 12:48:41:898 2017 test DPORAL/7/DP_PORTAL_DEBUG:
Matched Redirect ACL.
IfName=Vlan-interface2119, PortName=WLAN-BSS0, SrcIP=10.15.34.52, DstIP=183.232.231.172, Flow=0!
*Dec 6 12:48:41:899 2017 test TCPHEAT/7/TCPHEAT_DEBUG: Source MAC = 7c7a-91a9-cb03 VLAN = 2119
45 00 00 28 78 d0 40 00 80 06 b6 27 0a 0f 22 34
b7 e8 e7 ac ca e3 01 bb 00 87 31 1a b4 cb 3d 01
50 10 fa f0 f8 fe 00 00
*Dec 6 12:48:41:900 2017 test TCPHEAT/7/TCPHEAT_DEBUG: State of connection with source IP 10.15.34.52 is SYN_RECV!
```

\*Dec 6 12:48:41:900 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: State of connection with source IP 10.15.34.52 changed from SYN\_RECVD to ESTABLISHED!

\*Dec 6 12:48:41:900 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: State of connection with source IP 10.15.34.52 is ESTABLISHED!

\*Dec 6 12:48:41:900 2017 test DPPORTAL/7/DP\_PORTAL\_DEBUG:  
Matched Redirect ACL.  
IfName=Vlan-interface2119, PortName=WLAN-BSS0, SrcIP=10.15.34.52, DstIP=183.232.231.172, Flow=0!

\*Dec 6 12:48:41:903 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: State of connection with source IP 10.15.34.52 is ESTABLISHED!

\*Dec 6 12:48:41:903 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: The Packet Header len is 40,ulBodyLen 235

\*Dec 6 12:48:41:903 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Success to copy data From Mbuf.

\*Dec 6 12:48:41:903 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: BIO wrote 235 bytes into SSL.

\*Dec 6 12:48:41:904 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Recv TLS 1.0 Handshake [length 00e6], ClientHello

\*Dec 6 12:48:41:904 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Send TLS 1.0 Handshake [length 004a], ServerHello

\*Dec 6 12:48:41:904 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Send TLS 1.0 Handshake [length 0318], Certificate

\*Dec 6 12:48:41:904 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Send TLS 1.0 Handshake [length 0004], ServerHelloDone

\*Dec 6 12:48:41:904 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: BIO read 885 bytes from SSL.

\*Dec 6 12:48:41:905 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Processed SSL handshake.

\*Dec 6 12:48:42:121 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Recv TLS 1.0 ChangeCipherSpec [length 0001]

\*Dec 6 12:48:42:121 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Recv TLS 1.0 Handshake [length 0010], Finished

\*Dec 6 12:48:42:122 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Send TLS 1.0 ChangeCipherSpec [length 0001]

\*Dec 6 12:48:42:122 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: PT\_TCP TLS Info Description: Send TLS 1.0 Handshake [length 0010], Finished

\*Dec 6 12:48:42:122 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: BIO read 59 bytes from SSL.

\*Dec 6 12:48:42:122 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Processed SSL handshake.

\*Dec 6 12:48:42:128 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: State of connection with source IP 10.15.34.52 is ESTABLISHED!

\*Dec 6 12:48:42:129 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: The Packet Header len is 40,ulBodyLen 890

\*Dec 6 12:48:42:129 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Success to copy data From Mbuf.

\*Dec 6 12:48:42:129 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: BIO wrote 890 bytes into SSL.

\*Dec 6 12:48:42:129 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: decrypt data success,the packet total length is 868.

\*Dec 6 12:48:42:130 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Copy simple packet len is (828).

\*Dec 6 12:48:42:130 2017 test PORTAL/7/PORTAL\_DEBUG: The user (10.15.34.52) redirect url is <http://10.1.0.202:8097/web/scwp/auth/authIndex?wlanuserip=10.15.34.52&ssid=i-hefei&wlanapmac=38-97-D6-A1-94-E0&wlanacip=192.168.110.12&wlanstamac=7C-7A-91-A9-CB-03&wlanuserfirsturl=https://www.baidu.com>. //第二次重定向成功了,但是浏览器没正常弹出来

\*Dec 6 12:48:42:130 2017 test PORTAL/7/PORTAL\_DEBUG: The user (10.15.34.52) redirect success.

\*Dec 6 12:48:42:130 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: BIO read 917 bytes from SSL.

\*Dec 6 12:48:42:131 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Compose https redirect packet successfully.

\*Dec 6 12:48:42:131 2017 test TCPHEAT/7/TCPHEAT\_DEBUG: Processed SSL application data .

\*Dec 6 12:48:42:131 2017 test DPPORTAL/7/DP\_PORTAL\_DEBUG:  
抓包信息:

No.	Time	Source	Destination	Protocol	Length	Info
125	2017-12-06 13:01:10.760709	183.232.231.172	10.15.34.52	TCP	54	443 → 51938 [RST] Seq=945 Win=8192 Len=0
126	2017-12-06 13:01:10.761147	183.232.231.172	10.15.34.52	TCP	58	443 → 51939 [SYN, ACK] Seq=0 Ack=1 Min=8192 Len=0 MSS=
127	2017-12-06 13:01:10.761299	10.15.34.52	183.232.231.172	TCP	54	51939 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
128	2017-12-06 13:01:10.761592	10.15.34.52	183.232.231.172	TLSv1	289	Client Hello
129	2017-12-06 13:01:10.768983	183.232.231.172	10.15.34.52	TLSv1	939	Server Hello, Certificate, Server Hello Done
130	2017-12-06 13:01:10.769514	10.15.34.52	183.232.231.172	TLSv1	380	Client Key Exchange, Change Cipher Spec, Encrypted
131	2017-12-06 13:01:10.986615	183.232.231.172	10.15.34.52	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
132	2017-12-06 13:01:10.986615	10.15.34.52	183.232.231.172	TLSv1	944	Application Data, Application Data
133	2017-12-06 13:01:10.993974	183.232.231.172	10.15.34.52	TLSv1	971	Application Data
134	2017-12-06 13:01:10.994939	10.15.34.52	183.232.231.172	TCP	54	51939 → 443 [FIN, ACK] Seq=1452 Ack=1862 Win=64400
135	2017-12-06 13:01:11.000403	183.232.231.172	10.15.34.52	TCP	54	443 → 51939 [RST] Seq=1862 Win=8192 Len=0
289	2017-12-06 13:01:12.631708	10.15.34.52	183.232.231.172	TCP	66	51961 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 MS=25
290	2017-12-06 13:01:12.633916	183.232.231.172	10.15.34.52	TCP	58	443 → 51961 [SYN, ACK] Seq=0 Ack=1 Min=8192 Len=0 MSS=
291	2017-12-06 13:01:12.634059	10.15.34.52	183.232.231.172	TCP	54	51961 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
292	2017-12-06 13:01:12.634453	10.15.34.52	183.232.231.172	TLSv1	289	Client Hello

通过抓包信息查看，发现设备在不停和服务器交互，并多次进行重定向到不同的地址，当重定向到某个地址时，会出现400 Bad Request，初步怀疑是服务器问题，但是客户表示服务器和其他厂家的设备对接portal都很正常，就和我们有问题，后续让代理商重新测试其他厂家，并反馈正常的抓包来对比。

```
Stream Content
GET /web/scwp/auth/authForward/?wlanuserip=10.15.34.52&ssid=i-hefei&wlanapmac=38-97-D6-A1-94-E0&wlanacip=192.168.110.12&wlanstamac=7C-7A-91-A9-CB-03&wlanuserfirsturl=https://www.baidu.com&t=wed%20Dec%2006%202017%2013:01:11%20GMT+0800%20(C.....)
HTTP/1.1
Host: 10.1.0.202:8097
Connection: Keep-Alive
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/xaml+xml, application/x-ms-xbap, */*
Accept-Language: zh-Hans-CN, zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0; SE 2.X MetaSr 1.0) like Gecko
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=E4bc415D11836F197590A17C53355A88
HTTP/1.1 400 Bad Request
Server: nginx/1.11.10
Date: wed, 06 Dec 2017 05:01:11 GMT
Transfer-Encoding: chunked
Connection: keep-alive
```

最终代理商拿其他厂家的AP 对接服务器发现https 重定向也不行，之前客户反馈有误，最终定位为服务器问题，建议找服务器厂家帮忙定位问题。

1.V5 AC和AP portal 支持https重定向，但是需要特殊配置和版本要求，参考下面说明：

V5 (R2509P52版本特性变更说明)：

先配置个ssl server-policy

ssl server-policy xxx

再跟portal https-redirect关联起来就行了

portal https-redirect server-policy xxx

ssl server-policy内容可以为空，V5自带自签名证书。但会出现告警提示，“继续浏览”即可。

关于告警，只能解决特定域名，无法解决所有域名。客户可以自己购买“受信任”的证书倒入，倒入方式参考配置手册的SSL配置。受信任证书不是“万能”的，证书机构颁发证书时，会有一个CN限制的，简单说就是个域名限制，只有访问的域名跟这个CN匹配，才能信任通过。