

知 SecPath F100-C-G5(V7) 针对域名做安全策略不生效

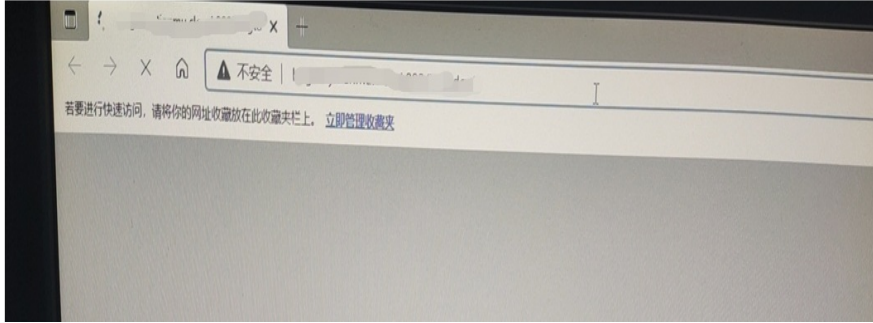
域间策略/安全域 陈美静 2023-12-27 发表

问题描述

用户实际访问的域名是：<http://aaa> 该域名在公网上可正常访问。做了DNS代理，终端DNS地址是防火墙地址。服务器是外网的，域名在公网就能访问。

测试过，抓包，包终端访问的所有ip都加到对象组里，报文示踪里显示访问的，都加到对象组里。

无法访问自己设置的可以访问的地址，后续可以进入访问页面但打不开嵌套页面的内容。



过程分析

1、先检查是否正确做了dns snooping或者dns代理，设备使用基于域名的策略过滤用户流量时，需要获取域名对应的IP地址才能真正实现流量过滤；

2、查看抓包（清除浏览器缓存后抓包，做了策略和方通所有各抓包一次）：

①是正常有tcp报文交互的，但访问网页时对对方的304,正常情况应该是200。

33	1.542619	172.16.10.12	119.3.201.57	HTTP	653 GET /hngtdcy/ HTTP/1.1
34	1.542679	192.168.1.4	119.3.201.57	HTTP	653 GET /hngtdcy/ HTTP/1.1
37	1.600182	119.3.201.57	192.168.1.4	TCP	60 802 → 12957 [ACK] Seq=1 Ack=600 Win=76 Len=0
38	1.600230	119.3.201.57	172.16.10.12	TCP	54 802 → 54486 [ACK] Seq=1 Ack=600 Win=76 Len=0
39	1.604828	119.3.201.57	192.168.1.4	HTTP	327 HTTP/1.1 304 Not Modified
40	1.604845	119.3.201.57	172.16.10.12	HTTP	327 HTTP/1.1 304 Not Modified
51	1.650517	172.16.10.12	119.3.201.57	TCP	60 54486 → 802 [ACK] Seq=600 Ack=274 Win=511 Len=0
52	1.650562	192.168.1.4	119.3.201.57	TCP	54 12957 → 802 [ACK] Seq=600 Ack=274 Win=511 Len=0

②服务器回应没修改，客户端可能带着之前缓存一直在访问，清除缓存再次访问测试还是不行。

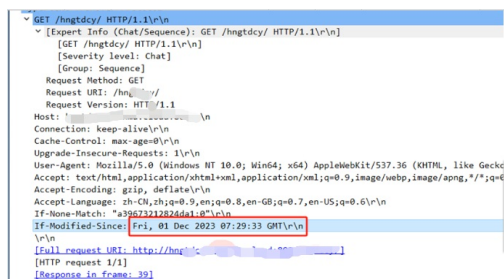
```
Status Code: 304  
[Status Code Description: Not Modified]  
Response Phrase: Not Modified
```

③从无法访问的抓包中，发现其http get请求中携带了时间戳，且该时间戳与实际北京时间相距太大，怀疑服务器收到相关get后，导致回应304。客户端192.168.1.4发的包带的缓存是12月1号的时间 服务器回应304没修改。

将FW上的时区调整为东八区观察，及

```
clock timezone Lisbon add 00:00:00 /修改为clock timezone UTC add 00:00:00
```

```
clock protocol none
```



修改后还是反馈不行，无法访问。

④从正常访问抓包看，服务器多次回应301重定向，所以要访问这个域名，要将这些重定向url全部放通才行。

No.	Time	Source	Destination	Protocol	Length	Time to 1st byte
19	2023-12-15 23:36:24.948869	172.16.10.12	119.3.201.57	TCP	66	128 59470 → 802 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	2023-12-15 23:36:24.964934	119.3.201.57	172.16.10.12	TCP	66	46 802 → 59470 [SYN, ACK] Seq=0 Ack=1 Win=29208 Len=0 MSS=1408 SACK_PERM=1 WS=512
23	2023-12-15 23:36:24.965404	172.16.10.12	119.3.201.57	TCP	60	128 59470 → 802 [ACK] Seq=1 Ack=1 Win=131584 Len=0
41	2023-12-15 23:36:27.184327	172.16.10.12	119.3.201.57	HTTP	480	128 GET /static/js/config/8E68B2838E58D8097/ndhg2021.js HTTP/1.1
64	2023-12-15 23:36:27.127722	119.3.201.57	172.16.10.12	TCP	54	46 802 → 59470 [ACK] Seq=1 Ack=427 Win=30720 Len=0
68	2023-12-15 23:36:27.128352	119.3.201.57	172.16.10.12	HTTP	615	46 HTTP/1.1 301 Moved Permanently (text/html)
101	2023-12-15 23:36:27.176353	172.16.10.12	119.3.201.57	TCP	60	128 59470 → 802 [ACK] Seq=427 Ack=562 Win=130816 Len=0
+ 415	2023-12-15 23:36:50.178726	172.16.10.12	119.3.201.57	HTTP	525	128 GET /static/images/gtocy/8E58D8A2E78A8B863201.png HTTP/1.1
120	2023-12-15 23:36:50.208620	119.3.201.57	172.16.10.12	HTTP	609	46 HTTP/1.1 301 Moved Permanently (text/html)
429	2023-12-15 23:36:50.205805	172.16.10.12	119.3.201.57	HTTP	525	128 GET /static/images/gtocy/8E58D8A2E78A8B863208.png HTTP/1.1
446	2023-12-15 23:36:50.229096	119.3.201.57	172.16.10.12	HTTP	609	46 HTTP/1.1 301 Moved Permanently (text/html)
453	2023-12-15 23:36:50.275352	172.16.10.12	119.3.201.57	TCP	60	128 59470 → 802 [ACK] Seq=1369 Ack=1672 Win=131584 Len=0

解决方法

1、不用带https, 将url全部加入策略

```

Location: https://...js
Content-Type: application/javascript
V-Download-Bu: ACD MET...

Location: https://...g\
V-Download-Bu: ACD MET...

Location: https://...g\
V-Download-Bu: ACD MET...

Location: https://...?zsrncbg2023.js
Content-Type: application/javascript
V-Download-Bu: ΔCP Nf(\n\n

Location: https://...js
V-Download-Bu: ACD MET...

Location: https://...s)
V-Download-Bu: ACD MET...

GET /static/js/config/8E68B2838E58D8097/ndhg2021.js HTTP/1.1
Host: h5.yitia.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/106.0
Referer: http://h5.yitia.com/cloud/02/gtocy/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN;q=0.9,en-US;q=0.6

HTTP/1.1 301 Moved Permanently
Date: Fri, 15 Dec 2023 07:36:31 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 191
Connection: keep-alive
Location: https://cdn.bootcdn.net/ajax/libs/...

<head>
<title>...</title>
</head>
<body>
<div>...</div>
</body>
</html>
MIME-Version: 1.0
Content-Type: text/html
Content-Length: 191
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/106.0
Referer: http://h5.yitia.com/cloud/02/gtocy/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN;q=0.9,en-US;q=0.6

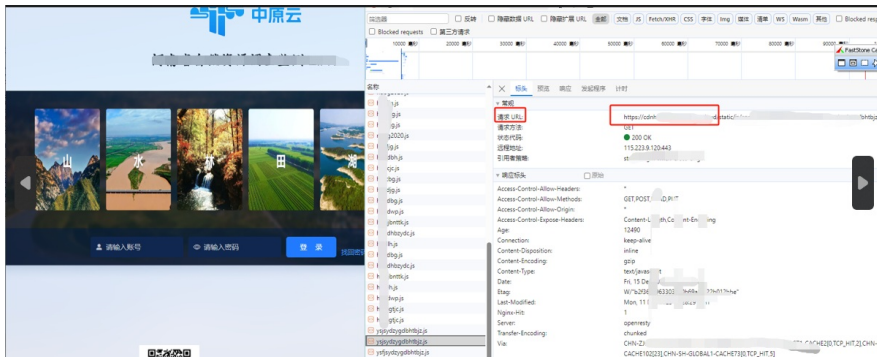
HTTP/1.1 301 Moved Permanently
Date: Fri, 15 Dec 2023 07:36:34 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 188
Connection: keep-alive
Location: https://cdn.bootcdn.net/ajax/libs/...

<head>
<title>...</title>
</head>
<body>
<div>...</div>
</body>
</html>
MIME-Version: 1.0
Content-Type: text/html
Content-Length: 188
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/106.0
Referer: http://h5.yitia.com/cloud/02/gtocy/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN;q=0.9,en-US;q=0.6

HTTP/1.1 301 Moved Permanently
Date: Fri, 15 Dec 2023 07:36:34 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 188
Connection: keep-alive
Location: https://cdn.bootcdn.net/ajax/libs/...

<head>
<title>...</title>
</head>
<body>
<div>...</div>
</body>
</html>
MIME-Version: 1.0
Content-Type: text/html
Content-Length: 188
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/106.0
Referer: http://h5.yitia.com/cloud/02/gtocy/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN;q=0.9,en-US;q=0.6
  
```

2、嵌套页面打不开: F12找, 网络下面



- webapi.amap.com
- cdn.bootcdn.net
- api.tianditu.gov.cn
- restapi.amap.com
- unpkg.com//全部加进去即可