F1020 Firewall HTTPS Video Filtering Failure Experience Example

Security 蒋笑添 2020-09-27 Published

Network Topology

null

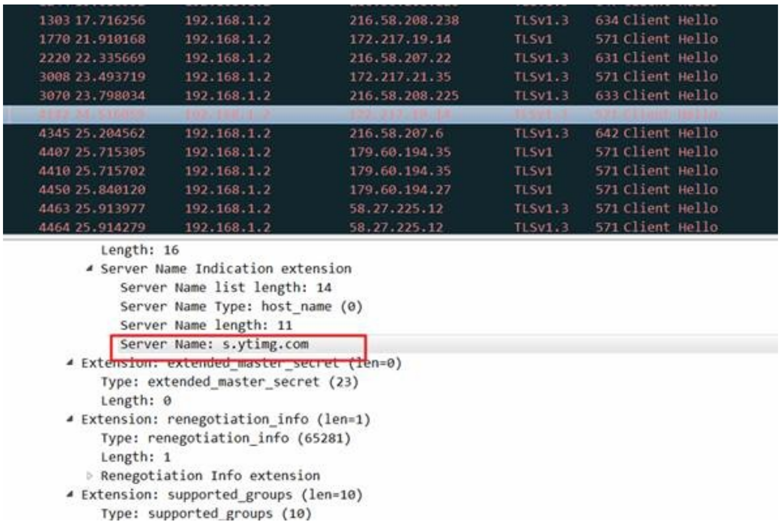
Problem Description

F1020 firewall uses Feature 9345P18 version + 1.0.47 URL signature library, configure URL blacklist test to block youtube and facebook unsuccessfully, URL filtering logs show successful, but the terminal can still access the website.

Process Analysis

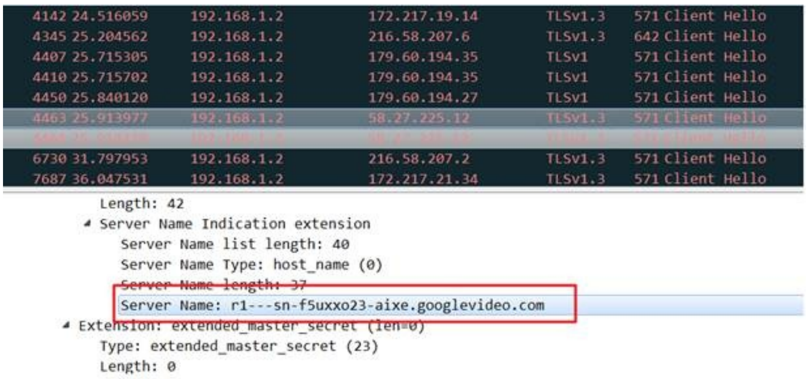
The current firewall and corresponding version is implemented by URL filtering blacklist. The mechanism is: when HTTPS traffic filtering is enabled, the SNI (Sever Name Indication extension) field in the Client HELLO message sent by the client is directly detected without decrypting HTTPS traffic. Get the server domain name from which the user is accessing, and use the obtained domain name to match the URL filtering policy.

By capturing the complete process of website access by the client, it is found that there are more SNI fields in youtube and facebook when the terminal initiates the access to the above sites. In addition to the domain name of the main site, there are also several sub-sites accessing the below sites. The firewall failed to block the specified traffic.



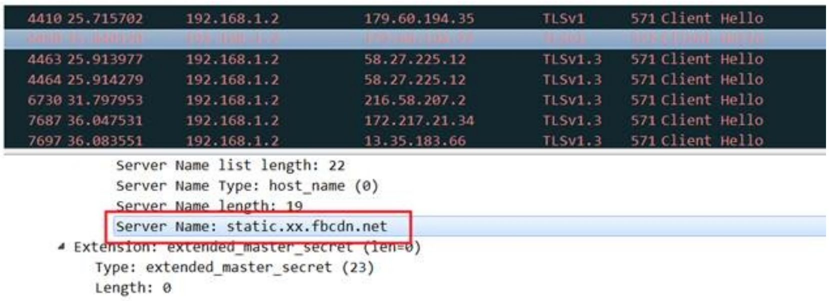
```
1303 17.716256   192.168.1.2   216.58.208.238   TLSv1.3   634 Client Hello
1770 21.910168   192.168.1.2   172.217.19.14    TLSv1     571 Client Hello
2220 22.335669   192.168.1.2   216.58.207.22    TLSv1.3   631 Client Hello
3008 23.493719   192.168.1.2   172.217.21.35    TLSv1.3   571 Client Hello
3070 23.798034   192.168.1.2   216.58.208.225   TLSv1.3   633 Client Hello
4142 24.516059   192.168.1.2   172.217.19.14    TLSv1.3   571 Client Hello
4345 25.204562   192.168.1.2   216.58.207.6     TLSv1.3   642 Client Hello
4407 25.715305   192.168.1.2   179.60.194.35    TLSv1     571 Client Hello
4410 25.715702   192.168.1.2   179.60.194.35    TLSv1     571 Client Hello
4450 25.840120   192.168.1.2   179.60.194.27    TLSv1     571 Client Hello
4463 25.913977   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
4464 25.914279   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
```

```
          Length: 16
        ◢ Server Name Indication extension
            Server Name list length: 14
            Server Name Type: host_name (0)
            Server Name length: 11
            Server Name: s.ytimg.com
      ◢ Extension: extended_master_secret (len=0)
          Type: extended_master_secret (23)
          Length: 0
      ◢ Extension: renegotiation_info (len=1)
          Type: renegotiation_info (65281)
          Length: 1
        ▷ Renegotiation Info extension
      ◢ Extension: supported_groups (len=10)
          Type: supported_groups (10)
```



```
4142 24.516059   192.168.1.2   172.217.19.14    TLSv1.3   571 Client Hello
4345 25.204562   192.168.1.2   216.58.207.6     TLSv1.3   642 Client Hello
4407 25.715305   192.168.1.2   179.60.194.35    TLSv1     571 Client Hello
4410 25.715702   192.168.1.2   179.60.194.35    TLSv1     571 Client Hello
4450 25.840120   192.168.1.2   179.60.194.27    TLSv1     571 Client Hello
4463 25.913977   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
4464 25.914279   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
6730 31.797953   192.168.1.2   216.58.207.2     TLSv1.3   571 Client Hello
7687 36.047531   192.168.1.2   172.217.21.34    TLSv1.3   571 Client Hello
```

```
          Length: 42
        ◢ Server Name Indication extension
            Server Name list length: 40
            Server Name Type: host_name (0)
            Server Name length: 37
            Server Name: r1---sn-f5uxxo23-aixe.googlevideo.com
      ◢ Extension: extended_master_secret (len=0)
          Type: extended_master_secret (23)
          Length: 0
```



```
4410 25.715702   192.168.1.2   179.60.194.35    TLSv1     571 Client Hello
4450 25.840120   192.168.1.2   179.60.194.27    TLSv1     571 Client Hello
4463 25.913977   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
4464 25.914279   192.168.1.2   58.27.225.12     TLSv1.3   571 Client Hello
6730 31.797953   192.168.1.2   216.58.207.2     TLSv1.3   571 Client Hello
7687 36.047531   192.168.1.2   172.217.21.34    TLSv1.3   571 Client Hello
7697 36.083551   192.168.1.2   13.35.183.66     TLSv1.3   571 Client Hello
```

```
            Server Name list length: 22
            Server Name Type: host_name (0)
            Server Name length: 19
            Server Name: static.xx.fbcdn.net
      ◢ Extension: extended_master_secret (len=0)
          Type: extended_master_secret (23)
          Length: 0
```

Solution

1. when you need to block HTTPS traffic to a site, such as only configuring the master domain name does not take effect, you need to grab packets to view the SNI field in the client hello message of https. The blacklist is configured by extracting the relevant SNI and using regular expressions. As in this example: *ytimg* *googlevideo* *fb* *fbcdn* .

2. or you can block youtube and facebook with the APR signature via security policy. current signature V7-ACG-APR-1.0.109 doesn"t have https signature for youtube and facabook, so you can"t block youtube and facebook with the APR signature. plan next version V7-ACG-APR-1.0.110 would be incorporated. Please update to the latest version of the signature library after the release.