【MVS】F5 BIG-IP LTM HTTP XFF头插入配置说明

网络相关 **胡伟** 2025-02-19 发表

问题描述

【MVS】F5 BIG-IP LTM HTTP XFF头插入配置说明

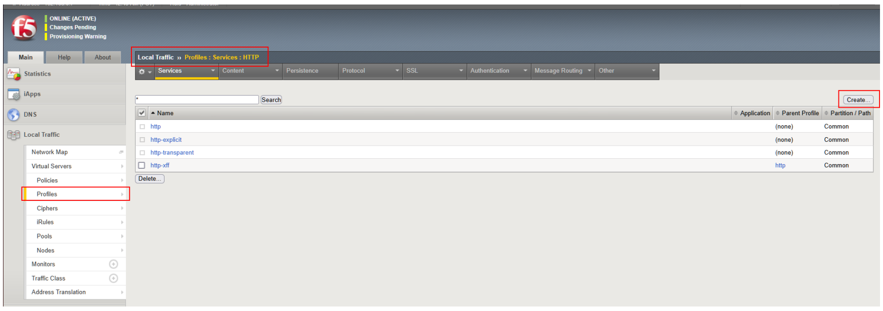
解决方法

F5 BIG-IP LTM虚服务配置SNAT时，客户端真实的源地址转换为F5设备上配置的地址，导致后端服务器无法获取真实的客户端地址，无法满足溯源等安全侧要求。可以在HTTP请求报文头中插入**X-Forwarded-For**字段来实现溯源功能，具体操作如下。

Enable the Insert X-Forwarded-For option in the HTTP profile

To configure the BIG-IP system to insert the original client IP address in an **X-Forwarded-For** HTTP header, perform the following procedure:

1. Log in to the Configuration utility.
2. Go to **Local Traffic** > **Profiles**.
3. For **Services**, select **HTTP**.
4. Select **Create**.

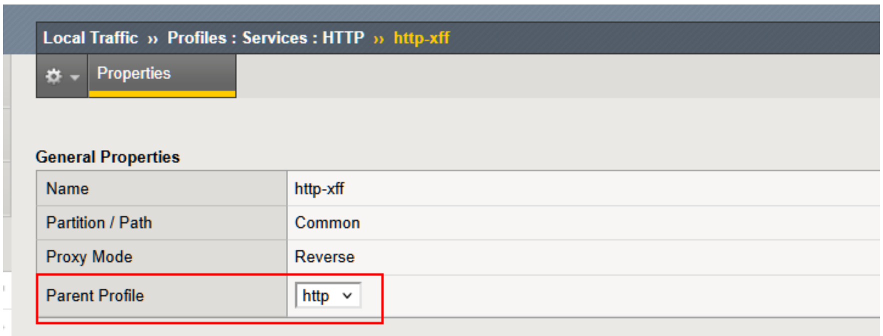


Local Traffic » Profiles : Services : HTTP

☑ Name	Application	Parent Profile	Partition / Path
□ http		(none)	Common
□ http-explicit		(none)	Common
□ http-transparent		(none)	Common
□ http-xff		http	Common

5. Enter a name for the HTTP profile.
6. Select the **Insert X-Forwarded-For** check box.

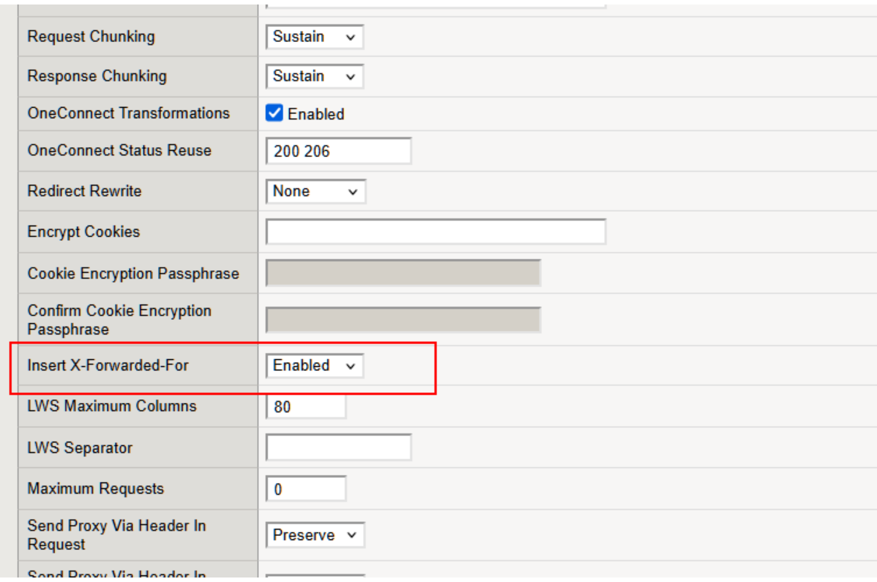
   Note: Older versions of BIG-IP software may display the option as **Insert XForwarded For** instead of **Insert X-Forwarded-For**.
7. For **Insert X-Forwarded-For**, select **Enabled**.



Local Traffic » Profiles : Services : HTTP » http-xff

General Properties

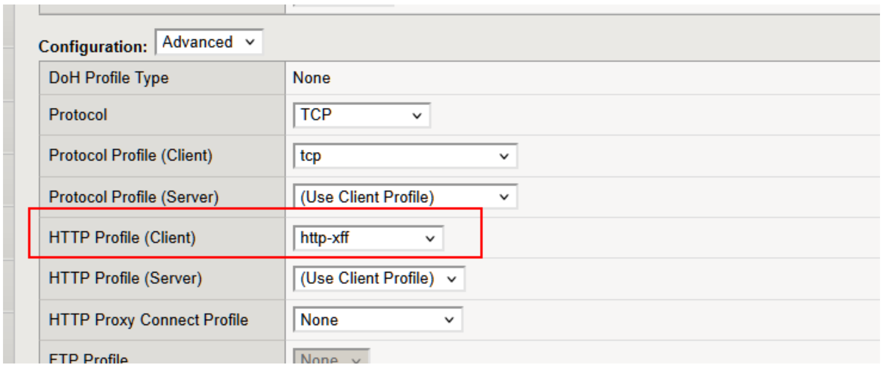
Name	http-xff
Partition / Path	Common
Proxy Mode	Reverse
Parent Profile	http



Request Chunking	Sustain
Response Chunking	Sustain
OneConnect Transformations	☑ Enabled
OneConnect Status Reuse	200 206
Redirect Rewrite	None
Encrypt Cookies	
Cookie Encryption Passphrase	
Confirm Cookie Encryption Passphrase	
Insert X-Forwarded-For	Enabled
LWS Maximum Columns	80
LWS Separator	
Maximum Requests	0
Send Proxy Via Header In Request	Preserve
Send Proxy Via Header In	

8. Select **Finished**.

   You must now associate the new HTTP profile with the virtual server.

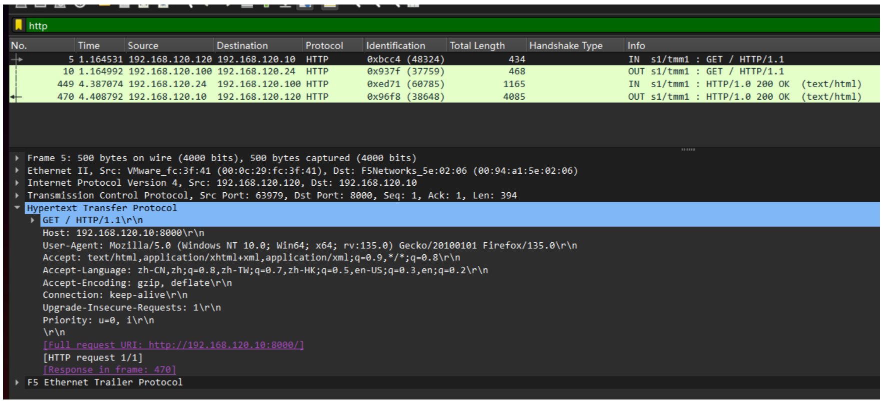


Configuration: Advanced

DoH Profile Type	None
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http-xff
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None

实际操作效果如下：

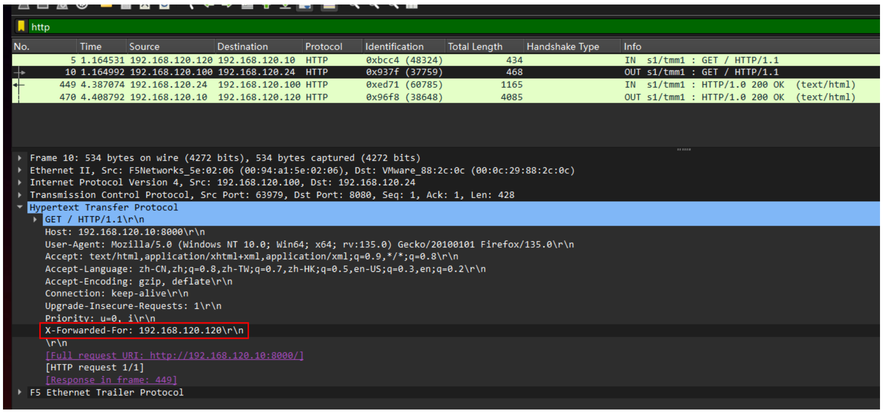
- 地址转换前



```
http
No.    Time     Source          Destination     Protocol Identification Total Length Handshake Type Info
     5 1.164531 192.168.120.120 192.168.120.10  HTTP     0xbcc4 (48324)          434                IN  s1/tmm1 : GET / HTTP/1.1
    10 1.164992 192.168.120.100 192.168.120.24  HTTP     0x937f (37759)          468                OUT s1/tmm1 : GET / HTTP/1.1
   449 4.387074 192.168.120.24  192.168.120.100 HTTP     0xed71 (60785)         1165                IN  s1/tmm1 : HTTP/1.0 200 OK  (text/html)
   470 4.408792 192.168.120.10  192.168.120.120 HTTP     0x96f8 (38648)         4085                OUT s1/tmm1 : HTTP/1.0 200 OK  (text/html)

Frame 5: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits)
Ethernet II, Src: VMware_fc:3f:41 (00:0c:29:fc:3f:41), Dst: F5Networks_5e:02:06 (00:94:a1:5e:02:06)
Internet Protocol Version 4, Src: 192.168.120.120, Dst: 192.168.120.10
Transmission Control Protocol, Src Port: 63979, Dst Port: 8000, Seq: 1, Ack: 1, Len: 394
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: 192.168.120.10:8000\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  \r\n
  [Full request URI: http://192.168.120.10:8000/]
  [HTTP request 1/1]
  [Response in frame: 470]
F5 Ethernet Trailer Protocol
```

- SNAT地址转换后



```
http
No.    Time     Source          Destination     Protocol Identification Total Length Handshake Type Info
     5 1.164531 192.168.120.120 192.168.120.10  HTTP     0xbcc4 (48324)          434                IN  s1/tmm1 : GET / HTTP/1.1
    10 1.164992 192.168.120.100 192.168.120.24  HTTP     0x937f (37759)          468                OUT s1/tmm1 : GET / HTTP/1.1
   449 4.387074 192.168.120.24  192.168.120.100 HTTP     0xed71 (60785)         1165                IN  s1/tmm1 : HTTP/1.0 200 OK  (text/html)
   470 4.408792 192.168.120.10  192.168.120.120 HTTP     0x96f8 (38648)         4085                OUT s1/tmm1 : HTTP/1.0 200 OK  (text/html)

Frame 10: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits)
Ethernet II, Src: F5Networks_5e:02:06 (00:94:a1:5e:02:06), Dst: VMware_88:2c:0c (00:0c:29:88:2c:0c)
Internet Protocol Version 4, Src: 192.168.120.100, Dst: 192.168.120.24
Transmission Control Protocol, Src Port: 63979, Dst Port: 8080, Seq: 1, Ack: 1, Len: 428
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: 192.168.120.10:8000\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i\r\n
  X-Forwarded-For: 192.168.120.120\r\n
  \r\n
  [Full request URI: http://192.168.120.10:8000/]
  [HTTP request 1/1]
  [Response in frame: 449]
F5 Ethernet Trailer Protocol
```