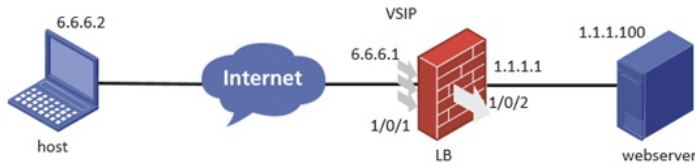


知 七层负载HTTPS重定向+HTTPS卸载访问webserver服务器异常

七层服务器负载均衡 郭尧 2020-09-27 发表

组网及说明



简要说明：通过webserver服务器提供http页面，采用nat模式组网，在LB设备上配置负载均衡实现host访问流量匹配VSIP虚地址后重定向到webserver服务器，此外出于安全性考虑，虚服务调用LB策略将HTTP页面重定向到HTTPS页面访问服务器，由于webserver只支持HTTP流量访问，因此本环境需要配置HTTPS卸载功能，使客户端到LB的流量经过加密传输，LB到webserver走HTTP流量访问

问题描述

终端访问web服务器异常，但是HTTP访问能够重定向到https加密传输，页面无线正常显示，如下：



过程分析

防火墙主要配置如下：

1、配置LB，分别配置实服务器，实服务组，负载均衡类和执行动作去匹配重定向，分别配置两个虚服务用于重定向到HTTPS和卸载HTTPS，最后导致CA和local证书在SSL策略调用，详情见下：

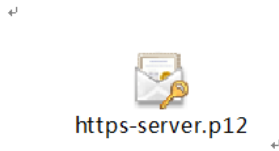
```
#
nqa template http 80 //配置HTTP健康险检测，默认就是使用的get方式
expect status 200 302 //配置期望返回内容
url http://1.1.1.100:8080/ //服务器URL进行探测
#
interface GigabitEthernet1/0/1 //对接客户端
port link-mode route
ip address 6.6.6.1 255.255.255.0
#
interface GigabitEthernet1/0/2 //对接服务器
port link-mode route
ip address 1.1.1.1 255.255.255.0
#
security-zone name http
import interface GigabitEthernet1/0/1
import interface GigabitEthernet1/0/2
#
server-farm http //配置实服务组，进行源地址哈希，调用探测模板
predictor hash address source
probe 80
#
loadbalance class http type http match-any
match 1 url //负载均衡匹配所有URL
#
loadbalance action http type http
redirect relocation https://%h%p //将http流量重定向为https
#
loadbalance policy 1 type http
class http action http //关联类和动作
#
real-server a //配置实服务器，指定访问端口，加入实服务组
```

```

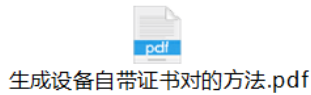
ip address 1.1.1.100
port 8080
server-farm http
#
virtual-server gy type http //配置负载均衡虚服务匹配策略进行HTTPS重定向
virtual ip address 6.6.6.1
port 8080
lb-policy 1 //调用负载均衡策略
default server-farm http //默认匹配实服务组
service enable
#
virtual-server http_unload type http //配置负载均衡虚服务进行https卸载
port 80 //配置https重定向后的端口号
virtual ip address 6.6.6.1
default server-farm http //默认匹配实服务组
ssl-server-policy gy //调用SSL策略进行https卸载
service enable
#
rule 0 name dzy
action pass

```

使用自签证书进行分离后导入PKI域，具体过程如下：
通过跳板机导出https-server



通过IE浏览器分离证书：
具体过程见下：



得到CA证书：

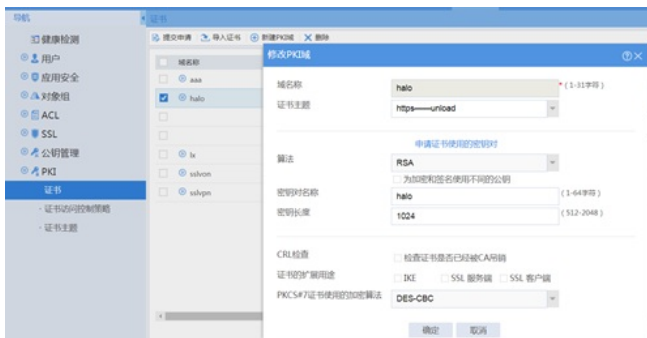


为了简便，这里在web界面进行证书导入和配置ssl策略

1、点击“对象 > PKI > 证书主题”，进入“证书主题”配置页面，点击“新建”，输入证书主题名称



1、依次点击“对象 > PKI > 证书”，进入PKI域配置及证书导入界面。点击“新建PKI域”，输入域名称，选择证书主题



依次点击“对象 > PKI > 证书”，进入PKI域配置及证书导入界面。点击“导入证书”，选择PKI域，证书类型选择“CA证书”，选择个人电脑本地的CA证书文件，这里已经导入成功



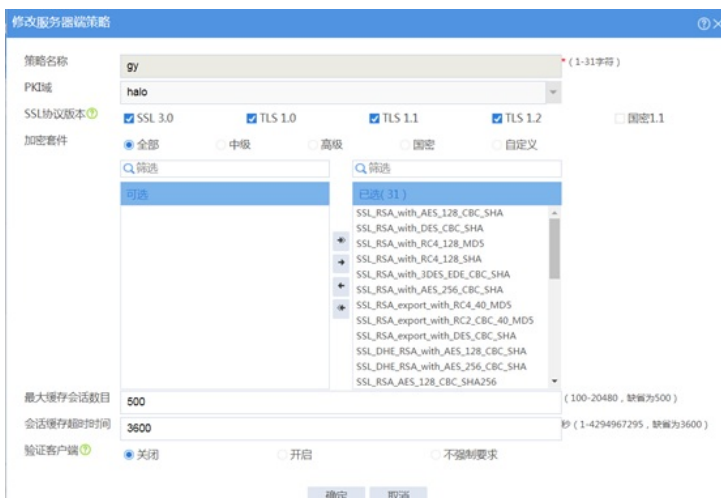
依次点击“对象 > PKI > 证书”，进入PKI域配置及证书导入界面。点击“导入证书”，选择PKI域，证书类型选择“本地证书”，选择个人电脑本地的local证书文件，输入密码、密钥对名称后确定



证书导入成功后如下：

PKI域	证书类型	证书名称	颁发日期	到期日期	操作
halo	CA	CN=H3C-HTTPS-Self-Signed-Certificate-884961...	2019-11-30 07:58:30	2019-11-25 07:58:30	🔍
	Local	CN=H3C-HTTPS-Self-Signed-Certificate-884961...	2019-11-30 07:58:30	2019-11-25 07:58:30	🔍

依次点击“对象 > SSL > 服务器端策略”，进入“服务器端策略”配置界面。点击“新建”，输入策略名称，选择PKI域、加密套件之后点击确定



配置后查看相关内容如下：

实服务器探测成功，状态正常

```

<F1030-NEW>dis real-server
Real server: a
Description:
State: Active
VPN instance:
Inherit VPN: Enable
IPv4 address: 1.1.1.100
IPv6 address: --
Port: 8080
Server farm: http
Weight: 100
Priority: 4
Cost: 0
Slow shutdown: Disabled
Connection limit: --
Rate limit:
Connections: --
HTTP requests: --
Bandwidth: --
Inbound bandwidth: --
Outbound bandwidth: --
Bandwidth busy:
Max bandwidth: --
Max inbound bandwidth: --
Max outbound bandwidth: --
Busy rate: 70
Inbound busy rate: 70
Outbound busy rate: 70
Busy recovery rate: 60
Inbound busy recovery rate: 60
Outbound busy recovery rate: 60
Probe information:
Dynamic weight: --
SNMPDCA busy state: --
Probe success criteria: All
Probe method
80
State
Succeeded

```

实服务组:

实服务组状态正常

```

<F1030-NEW>display server-farm
Server farm: http
Description:
Predictor: Hash address source IP
Proximity: Disabled
NAT: Enabled
SNAT pool:
Failed action: Keep
Active threshold: Disabled
Slow-online: Disabled
Selected server: Disabled
Busy action: Drop
Probe information:
Probe success criteria: All
Probe method:
80
TCP RST probe template:
TCP zero-window probe template:
HTTP passive probe template:
Auto-shutdown recovery time: 0
Total real server: 1
Active real server: 1
Real server list:
Name      State      VPN-instance  Address      Port  Weight Priority
a         Active                     1.1.1.100    8080  100    4

```

虚服务:

http重定向

```
F1030-NEW>display virtual-server
virtual server: gy
Description:
Type: HTTP
State: Active
VPN instance:
Virtual IPv4 address: 6.6.6.1/32
Virtual IPv6 address: --
Port: 8080
Primary server farm: http (in use)
Backup server farm:
Primary sticky:
Backup sticky:
LB policy: 1
LB limit-policy:
Connection limit: --
Rate limit:
  Connections: --
  Bandwidth: --
  Inbound bandwidth: --
  Outbound bandwidth: --
SSL server policy:
SSL client policy:
Redirect relocation:
Redirect return-code: 302
Sticky:
Sticky synchronization: Disabled
Bandwidth busy protection: Disabled
Interface bandwidth statistics: Disabled
Route advertisement: Disabled
Cache policy:
Customlog content:
```

https卸载

```

Virtual server: http_unload
Description:
Type: HTTP
State: Active
VPN instance:
Virtual IPv4 address: 6.6.6.1/32
Virtual IPv6 address: --
Port: 443
Primary server farm: http (in use)
Backup server farm:
Primary sticky:
Backup sticky:
LB policy:
LB limit-policy:
Connection limit: --
Rate limit:
Connections: --
Bandwidth: --
Inbound bandwidth: --
Outbound bandwidth: --
SSL server policy: gy
SSL client policy:
Redirect relocation:
Redirect return-code: 302
Sticky:
Sticky synchronization: Disabled
Bandwidth busy protection: Disabled
Interface bandwidth statistics: Disabled
Route advertisement: Disabled
Cache policy:

```

根据异常web页面显示，http能够重定向https，说明匹配了LB策略的虚服务，但是页面无法正常显示，却能够提示无法显示此页，在webserver侧抓包发现，webserver接收到的流量为https加密的TLS，webserver只支持http访问，所以无法正常显示

解决方法

分析配置发现，虚服务配置端口有误

```

virtual-server gy type http //配置负载均衡虚服务匹配策略进行HTTPS重定向
virtual ip address 6.6.6.1
port 8080
lb-policy 1 //调用负载均衡策略
default server-farm http //默认匹配实服务组
service enable
#
virtual-server http_unload type http //配置负载均衡虚服务进行https卸载
port 80 //配置https重定向后的端口号
virtual ip address 6.6.6.1
default server-farm http //默认匹配实服务组
ssl-server-policy gy //调用SSL策略进行https卸载
service enable

```

访问时终端指定端口8080所以能够匹配虚服务gy，经过https加密后，端口变为443的https端口，此时http_unload虚服务端口为80，所以无法匹配上，报文只匹配gy虚服务转发到实服务器，过去的仍然是https流量，所以无法正常访问

修改配置

```

virtual-server gy type http //配置负载均衡虚服务匹配策略进行HTTPS重定向
virtual ip address 6.6.6.1
lb-policy 1 //调用负载均衡策略
default server-farm http //默认匹配实服务组

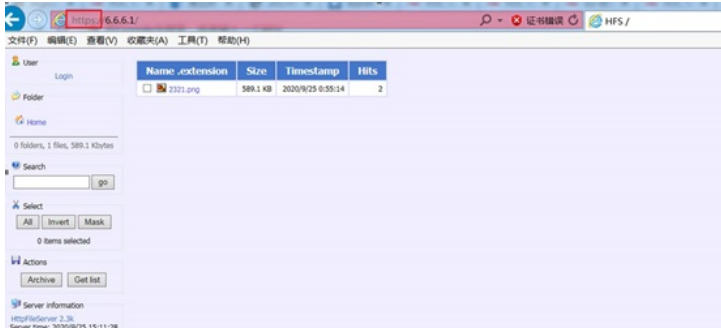
```

```

service enable
#
virtual-server http_unload type http //配置负载均衡虚服务进行https卸载
port 443 //配置https重定向后的端口号
virtual ip address 6.6.6.1
default server-farm http //默认匹配实服务组
ssl-server-policy gy //调用SSL策略进行https卸载
service enable

```

不指定端口访问，使用默认的http端口80匹配gy虚服务，后转换成443端口匹配http_unload进行https卸载，到webserver流量为http可以正常访问，如下：

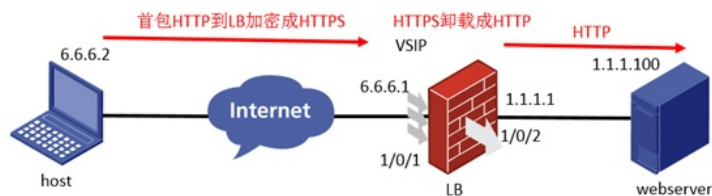


Host可以访问服务器页面，可以看到http访问请求已经被重定向成https了，由于使用的是自签证书，所以这里会提示证书错误，点击继续访问就可以了

这个过程分析如下：

- 1、终端发起http访问请求，<http://6.6.6.1>，这个默认端口是80端口，会匹配到虚服务gy，虚服务调用了LB策略进行https重定向完成
- 2、重定向后，如果报文直接匹配实服务器地址去转换是无法正常访问的，因为webserver不支持https访问，所以重定向后又匹配虚服务http_unload，端口是443的https端口，虚服务调用了SLL策略会进行https卸载，然后去匹配默认实服务器转换目的地址到webserver，实现http访问

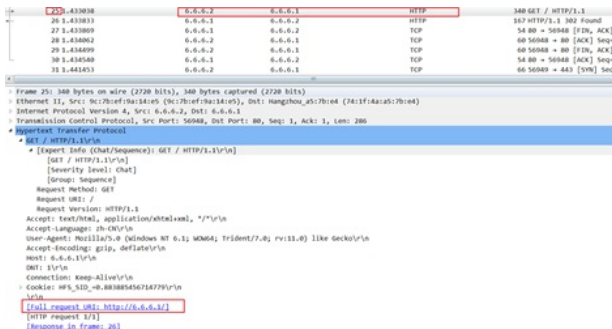
1、整个过程如下：



这样既可以实现访问http的webserver，又可以将终端数据进行加密，提高了安全

分析抓包结果：

- 1、host发起http访问，第26个报文，6.6.6.2到6.6.6.1是http的url请求



- 2、经过LB策略重定向回包，第27个回包报文重定向成https

```

No.  Time           Source            Destination      Protocol  Length  Info
-----
25  1.433038        6.6.6.2          6.6.6.1          HTTP      348  GET / HTTP/1.1
26  1.433833        6.6.6.1          6.6.6.2          HTTP      167  HTTP/1.1 302 Found
27  1.433869        6.6.6.1          6.6.6.2          TCP        60  56948 → 80 [FIN, A
28  1.434062        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [ACK] S
29  1.434499        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [FIN, A
30  1.434540        6.6.6.1          6.6.6.2          TCP        60  56948 → 80 [ACK] S
31  1.441453        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [FIN, A
32  1.441632        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [ACK] S
33  1.442288        6.6.6.2          6.6.6.1          TCP        60  56948 → 443 [ACK]
34  1.442745        6.6.6.2          6.6.6.1          TLSv1.2   246  Client Hello
35  1.449604        6.6.6.1          6.6.6.2          TLSv1.2   899  Server Hello, Cert
36  1.449915        6.6.6.2          6.6.6.1          TCP        60  56949 → 443 [ACK]
37  1.478530        6.6.6.2          6.6.6.1          TLSv1.2   236  Client Key Exchang
38  1.484757        6.6.6.1          6.6.6.2          TLSv1.2   161  Change Cipher Spec

```

```

> Frame 26: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits)
> Ethernet II, Src: Hangzhou_a57b:e4 (74:1f:4a:a5:7b:e4), Dst: 9c:7b:ef:9a:14:e5 (9c:7b:ef:9a:14:e5)
> Internet Protocol Version 4, Src: 6.6.6.2, Dst: 6.6.6.1
> Transmission Control Protocol, Src Port: 80, Dst Port: 56948, Seq: 1, Ack: 287, Len: 113
> Hypertext Transfer Protocol
  > HTTP/1.1 302 Found
    [Expert Info (Chat/Sequence): HTTP/1.1 302 Found]
    [HTTP/1.1 302 Found]
    [Severity Level: chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 302
    [Status Code Description: Found]
    Response Phrase: Found
    Cache-Control: no-cache
    Connection: close
    Content-Length: 0
    Location: https://6.6.6.1/
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000795000 seconds]
    [Request in frame: 25]

```

3、重定向后的https报文多了加密层

```

No.  Time           Source            Destination      Protocol  Length  Info
-----
25  1.433038        6.6.6.2          6.6.6.1          HTTP      348  GET / HTTP/1.1
26  1.433833        6.6.6.1          6.6.6.2          HTTP      167  HTTP/1.1 302 Found
27  1.433869        6.6.6.1          6.6.6.2          TCP        60  56948 → 80 [FIN, A
28  1.434062        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [ACK] S
29  1.434499        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [FIN, A
30  1.434540        6.6.6.1          6.6.6.2          TCP        60  56948 → 80 [ACK] S
31  1.441453        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [FIN, A
32  1.441632        6.6.6.2          6.6.6.1          TCP        60  56948 → 80 [ACK] S
33  1.442288        6.6.6.2          6.6.6.1          TCP        60  56948 → 443 [ACK]
34  1.442745        6.6.6.2          6.6.6.1          TLSv1.2   246  Client Hello
35  1.449604        6.6.6.1          6.6.6.2          TLSv1.2   899  Server Hello, Cert
36  1.449915        6.6.6.2          6.6.6.1          TCP        60  56949 → 443 [ACK]
37  1.478530        6.6.6.2          6.6.6.1          TLSv1.2   236  Client Key Exchang
38  1.484757        6.6.6.1          6.6.6.2          TLSv1.2   161  Change Cipher Spec

```

```

> Frame 34: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
> Ethernet II, Src: 9c:7b:ef:9a:14:e5 (9c:7b:ef:9a:14:e5), Dst: Hangzhou_a57b:e4 (74:1f:4a:a5:7b:e4)
> Internet Protocol Version 4, Src: 6.6.6.2, Dst: 6.6.6.1
> Transmission Control Protocol, Src Port: 56949, Dst Port: 443, Seq: 1, Ack: 1, Len: 192
> Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello

```

4、经过https卸载后，发往webserver的请求报文为http，默认DNAT模式，转换目的地址变为1.1.1.10

0、源地址不变

```

No.  Time           Source            Destination      Protocol  Length  Info
-----
37  1.478530        6.6.6.2          6.6.6.1          TLSv1.2   236  Client Key Exchange, Change Ci
38  1.484757        6.6.6.1          6.6.6.2          TLSv1.2   161  Change Cipher Spec, Encrypted
39  1.484912        6.6.6.2          6.6.6.1          TCP        60  56949 → 443 [ACK] Seq=375 Ack=
40  1.494845        6.6.6.2          6.6.6.1          TLSv1.2   413  Application Data
41  1.494871        6.6.6.2          1.1.1.100       TCP        74  1882 → 8080 [SYN] Seq=0 Win=0
42  1.495150        1.1.1.100       6.6.6.2          TCP        74  8080 → 1882 [SYN, ACK] Seq=0 W
43  1.495230        6.6.6.2          1.1.1.100       TCP        66  1882 → 8080 [ACK] Seq=1 Ack=1
44  1.495845        6.6.6.2          1.1.1.100       HTTP      352  GET / HTTP/1.1
45  1.527470        1.1.1.100       6.6.6.2          TCP        260  8080 → 1882 [PSH, ACK] Seq=1 A
46  1.527886        6.6.6.1          6.6.6.2          TLSv1.2   313  Application Data
47  1.528066        1.1.1.100       6.6.6.2          TCP        1438  8080 → 1882 [ACK] Seq=108

```

```

> Frame 44: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
> Ethernet II, Src: Hangzhou_a57b:e5 (74:1f:4a:a5:7b:e5), Dst: c4:65:16:8f:38:a0 (c4:65:16:8f:38:a0)
> Internet Protocol Version 4, Src: 6.6.6.2, Dst: 1.1.1.100
> Transmission Control Protocol, Src Port: 1882, Dst Port: 8080, Seq: 1, Ack: 1, Len: 286
> Hypertext Transfer Protocol
  > GET / HTTP/1.1
    [Expert Info (Chat/Sequence): GET / HTTP/1.1]
    [GET / HTTP/1.1]
    [Severity Level: chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Accept: text/html,application/xhtml+xml,*/*
    Accept-Language: zh-CN
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
    Accept-Encoding: gzip, deflate
    Host: 6.6.6.1
    DNT: 1
    Connection: Keep-Alive
    Cookie: WFS_SID=8838845674779
    \r\n
    [Full request URI: http://6.6.6.1/]
    HTTP Product: 375

```

5、webserver回包也是回的http的url，由于源地址没变，所有回包的目的地为6.6.6.2

```

No.  Time           Source            Destination      Protocol  Length  Info
-----
44  1.495845        6.6.6.2          1.1.1.100       HTTP      352  GET / HTTP/1.1
45  1.527470        6.6.6.1          6.6.6.2          TCP        260  8080 → 1882 [PSH, A
46  1.527886        6.6.6.1          6.6.6.2          TLSv1.2   313  Application Data
47  1.528066        6.6.6.1          6.6.6.2          TCP        1438  8080 → 1882 [ACK] S
48  1.528940        6.6.6.1          6.6.6.2          TLSv1.2   1499  Application Data
49  1.529038        6.6.6.2          1.1.1.100       TCP        66  1882 → 8080 [ACK] S
50  1.529648        1.1.1.100       6.6.6.2          TCP        154  8080 → 1882 [PSH, ACK

```

```

> Frame 44: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
> Ethernet II, Src: Hangzhou_a57b:e5 (74:1f:4a:a5:7b:e5), Dst: c4:65:16:8f:38:a0 (c4:65:16:8f:38:a0)
> Internet Protocol Version 4, Src: 6.6.6.2, Dst: 1.1.1.100
> Transmission Control Protocol, Src Port: 1882, Dst Port: 8080, Seq: 1, Ack: 1, Len: 286
> Hypertext Transfer Protocol
  > GET / HTTP/1.1
    [Expert Info (Chat/Sequence): GET / HTTP/1.1]
    [GET / HTTP/1.1]
    [Severity Level: chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Accept: text/html,application/xhtml+xml,*/*
    Accept-Language: zh-CN
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
    Accept-Encoding: gzip, deflate
    Host: 6.6.6.1
    DNT: 1
    Connection: Keep-Alive
    Cookie: WFS_SID=8838845674779
    \r\n
    [Full request URI: http://6.6.6.1/]

```

6、回包过程，源地址会转换成VIP地址进行回包，LB到host过程是https加密的TLSV1.2

```

44  1.495845        6.6.6.2          1.1.1.100       HTTP      352  GET / HTTP/1.1
45  1.527470        6.6.6.1          6.6.6.2          TCP        260  8080 → 1882 [PSH, ACK]
46  1.527886        6.6.6.1          6.6.6.2          TLSv1.2   313  Application Data
47  1.528066        6.6.6.1          6.6.6.2          TCP        1438  8080 → 1882 [ACK] Seq
48  1.528940        6.6.6.1          6.6.6.2          TLSv1.2   1499  Application Data
49  1.529038        6.6.6.2          1.1.1.100       TCP        66  1882 → 8080 [ACK] Seq
50  1.529648        1.1.1.100       6.6.6.2          TCP        154  8080 → 1882 [PSH, ACK

```

```

> Frame 45: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
> Ethernet II, Src: c4:65:16:8f:38:a0 (c4:65:16:8f:38:a0), Dst: Hangzhou_a57b:e5 (74:1f:4a:a5:7b:e5)
> Internet Protocol Version 4, Src: 1.1.1.100, Dst: 6.6.6.2
> Transmission Control Protocol, Src Port: 8080, Dst Port: 1882, Seq: 1, Ack: 287, Len: 194
  Source Port: 8080
  Destination Port: 1882
  [Stream Index: 3]
  [TCP Segment Len: 194]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 395 (relative sequence number)]
  Acknowledgment number: 287 (relative ack number)
  1000 ... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window size value: 257
  [Calculated window size: 65792]
  [Window size scaling factor: 256]
  Checksum: 0x023b (unverified)
  [Checksum Status: Unverified]
  Urgent pointer: 0
  Options: (2 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (194 bytes)

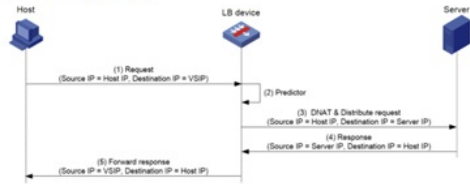
```

以上整个转发过程符合以下转换原理情况：

3. DNAT方式

在DNAT方式下，服务器需要通过更改缺省网关或配置静态路由，将发往主机的数据包发送到负载均衡设备上。DNAT方式的工作流程如图2-2所示。

图2-2 DNAT方式工作流程图



DNAT方式的工作流程简述如图2-1所示。

表2-1 DNAT方式工作流程简述

步骤	描述	源IP地址	目的IP地址
(1)	主机发送服务请求报文	Host IP	VSIP
(2)	负载均衡设备收到请求报文后，借助调度算法算出应将此请求分发给哪台服务器	-	-
(3)	负载均衡设备使用DNAT技术分发请求报文，把报文的目的地地址修改为服务器的IP地址	Host IP	Server IP
(4)	服务器接收并处理请求报文，返回响应报文	Server IP	Host IP
(5)	负载均衡设备收到响应报文后，将其源IP地址修改为VSIP后转发给主机	VSIP	Host IP