301B Q&As

BIG-IP Local Traffic Manager (LTM) Specialist: Maintain & Troubleshoot

Pass F5 301B Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/301b.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by F5 Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Given this as the first packet displayed of an ssldump:

2 2 1296947622.6313 (0.0001) S>CV3.1(74) Handshake

ServerHello

Version 3.1

random[32]=

19 21 d7 55 c1 14 65 63 54 23 62 b7 c4 30 a2 f0

b8 c4 20 06 86 ed 9c 1f 9e 46 0f 42 79 45 8a 29

session_id[32]=

c4 44 ea 86 e2 ba f5 40 4b 44 b4 c2 3a d8 b4 ad

4c dc 13 0d 6c 48 f2 70 19 c3 05 f4 06 e5 ab a9

cipherSuite TLS_RSA_WITH_RC4_128_SHA

compressionMethod NULL

In reviewing the rest of the ssldump, the application data is NOT being decrypted.

Why is ssldump failing to decrypt the application data?

A. The application data is encrypted with SSLv3.

B. The application data is encrypted with TLSv1.

C. The data is contained within a resumed TLS session.

D. The BigDB Key Log.Tcpdump.Level needs to be adjusted.

Correct Answer: C

QUESTION 2

An LTM Specialist troubleshooting an issue looks at the following /var/log/ltm entries:

Oct 2 04:52:42 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)

Oct 2 05:37:16 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)

Oct 2 05:57:32 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53

(proto 17)

Oct 2 06:30:03 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)

Oct 2 06:37:44 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)

Oct 2 06:47:05 slot1/tmm5 crit tmm5[21732]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)

Which configuration item should the LTM Specialist review to fix the issue?

A. SNAT Pool

B. Pool Member

C. Port Lockdown

D. Virtual Server Port Translation

Correct Answer: A

QUESTION 3

-- Exhibit -- Exhibit -

```
[~]$ openssl s_client -connect 172.16.20.1:443
CONNECTED(00000003)
depth=0 /O=TurnKey Linux/OU=Software appliances
verify error:num=18:self signed certificate
verify return:1
depth=0 /O=TurnKey Linux/OU=Software appliances
verify return:1
---
Certificate chain
 0 s:/O=TurnKey Linux/OU=Software appliances
   i:/O=TurnKey Linux/OU=Software appliances
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICgzCCAeygAwIBAgIJAImLXVLJqYzBMA0GCSqGSIb3DQEBBQUAMDYxFjAUBgNV
BAoTDVR1cm5LZXkgTGludXgxHDAaBgNVBAsTE1NvZnR3YXJlIGFwcGxpYW5jZXMw
HhcNMTAwNDE1MTkxNDQzWhcNMjAwNDEyMTkxNDQzWjA2MRYwFAYDVQQKEw1UdXJu
S2V5IExpbnV4MRwwGgYDVQQLExNTb2ZOd2FyZSBhcHBsaWFuY2VzMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCVlgenrRHsav6R+M/xYyooMJVpXWZbzeKu04ro
euadY0KOwwa2zF9jaD0HDIJ3MtnVYaHMsHZvqoo1Q8EfohP85RfHrO4kMxtvAefm
s1qGE7MkmIxLtwYjjWXmwxW7sCFLl9kt6pFOatzqeK3WxbdM5yF/RTHF4R/vyKQI
2lYf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBRG5CDKtOlkiiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMaW51eDEcMBoGA1UECxMTU29mdHdhcmUgYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEANo2TuXFVZKWG
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhpl
RGH2+IqwglEPB7K6eudRy0D9GqzMHZrdMo9d3ewPB3BqjOrPhs5yRTgNrZHyasJr
ZAiCzekf24SwNpmhfHyyam88N2+WgqU=
-----END CERTIFICATE-----
subject=/O=TurnKey Linux/OU=Software appliances
issuer=/O=TurnKey Linux/OU=Software appliances
---
No client certificate CA names sent
---
SSL handshake has read 1211 bytes and written 328 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: E457C0A12201A70C4E65511A1CD35D7738B1073068D7DB164F2D7413D4487ACC
    Session-ID-ctx:
    Master-Key: 45D7A671DB99F6891B8A580C29F0173EF8F677F0972383C9AD652EAFA035E6C0706F31D16F41646296695E332CB11E0D
    Key-Arg   : None
    Start Time: 1351286146
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
```

Refer to the exhibit.

An LTM Specialist is troubleshooting an issue with SSL and is receiving the error shown when connecting to the virtual server. When connecting directly to the pool member, clients do NOT receive this message, and the application functions correctly. The LTM Specialist exports the appropriate certificate and key from the pool member and imports them into the LTM device. The LTM Specialist then creates the Client SSL profile and associates it with the virtual server. What is the issue?

A. The SSL certificate and key have expired.

B. The SSL certificate and key do NOT match.

C. The client CANNOT verify the certification path.

D. The common name on the SSL certificate does NOT match the hostname of the site.

Correct Answer: C

QUESTION 4

-- Exhibit

```
PACKET CAPTURE DIRECT TO WEB SERVER

19:50:28.497103 IP 172.31.5.100.49715 > 10.31.80.23.80: S 751670031:751670031(0) win 8192 <mss 1460,nop,wscale
2,nop,nop,sackOK>
19:50:28.501117 IP 10.31.80.23.80 > 172.31.5.100.49715: S 1684731463:1684731463(0) ack 751670032 win 8192 <mss
1460,nop,wscale 8,nop,nop,sackOK>
19:50:28.502839 IP 172.31.5.100.49715 > 10.31.80.23.80: . ack 1 win 16425
19:50:28.524386 IP 172.31.5.100.49715 > 10.31.80.23.80: P 1:249(248) ack 1 win 16425
19:50:28.527024 IP 10.31.80.23.80 > 172.31.5.100.49715: P 1:344(343) ack 249 win 256
19:50:28.738115 IP 172.31.5.100.49715 > 10.31.80.23.80: . ack 344 win 16339
19:50:30.855229 IP 172.31.5.100.49716 > 10.31.80.23.80: S 3248492897:3248492897(0) win 8192 <mss 1460,nop,wscale
2,nop,nop,sackOK>
19:50:30.858672 IP 10.31.80.23.80 > 172.31.5.100.49716: S 1034885901:1034885901(0) ack 3248492898 win 8192 <mss
1460,nop,wscale 8,nop,nop,sackOK>
19:50:30.861972 IP 172.31.5.100.49716 > 10.31.80.23.80: . ack 1 win 16425
19:50:30.861980 IP 172.31.5.100.49716 > 10.31.80.23.80: P 1:202(201) ack 1 win 16425
19:50:30.865070 IP 10.31.80.23.80 > 172.31.5.100.49716: P 1:1406(1405) ack 202 win 256
19:50:30.867112 IP 172.31.5.100.49716 > 10.31.80.23.80: R 202:202(0) ack 1406 win 0


PACKET CAPTURE THROUGH LTM DEVICE

EXTERNAL VLAN
20:05:33.719423 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:33.958133 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.722498 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.972779 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:42.723128 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,nop,sackOK>
20:05:42.972755 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,nop,sackOK>

INTERNAL VLAN
20:05:33.719791 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:33.958189 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.722525 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:36.972805 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
20:05:42.723147 IP 172.31.5.100.49734 > 172.31.200.200.80: S 3265616310:3265616310(0) win 8192 <mss 1460,nop,nop,sackOK>
20:05:42.972776 IP 172.31.5.100.49735 > 172.31.200.200.80: S 2304966925:2304966925(0) win 8192 <mss 1460,nop,nop,sackOK>
```

-- Exhibit -Refer to the exhibits.

Users are able to access the application when connecting directly to the web server but are unsuccessful when connecting to the virtual server. Return traffic bypasses the LTM device using Layer 2 nPath routing.

Which configuration change resolves this problem?

A. Enable a SNAT pool on the LTM device.

B. Disable address translation on the LTM device.

C. Configure a route on the web server to the client subnet.

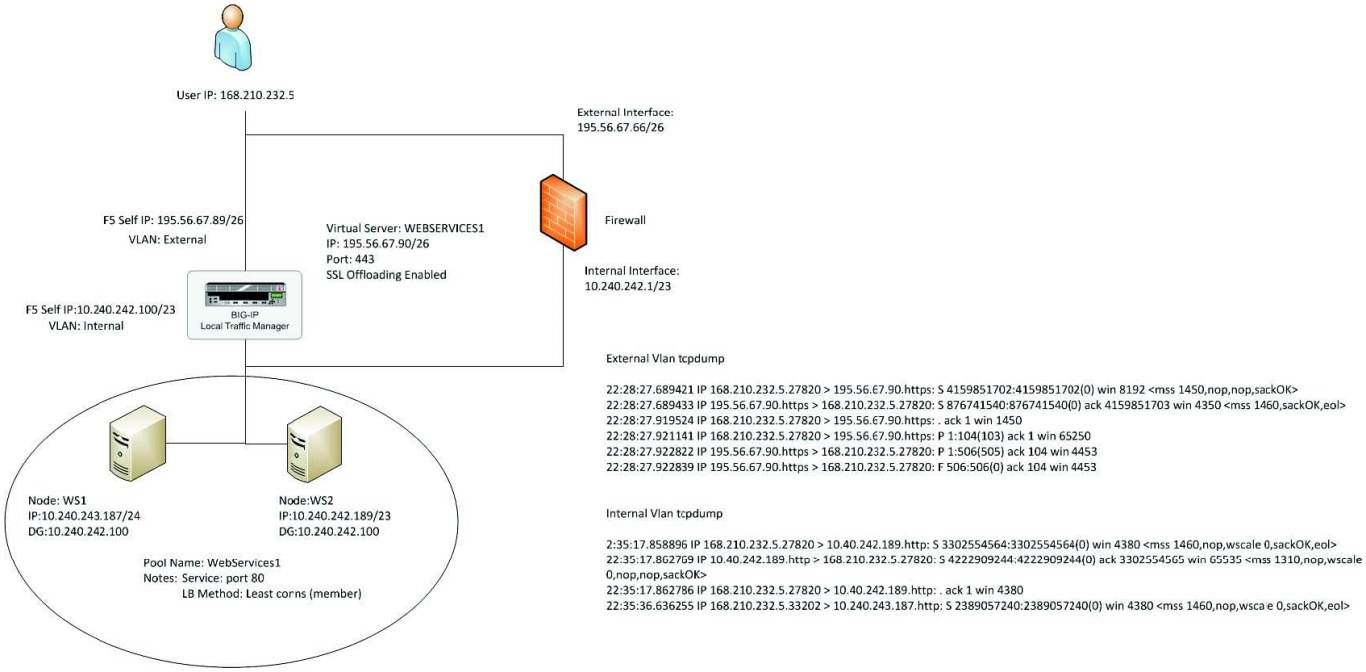
D. Configure the virtual server to listen on port 80 on the LTM device.

E. Configure the VIP address on the loopback interface of the web server.

Correct Answer: E

QUESTION 5

-- Exhibit -



-- Exhibit -Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem.

The LTM Specialist has the tcpdump extract and knows the client source IP is 168.210.232.5.

Assuming no wildcard virtual servers, how many distinct virtual servers does the client connect to on the LTM device?

A. 2

B. 3

C. 4

D. 6

Correct Answer: B