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:

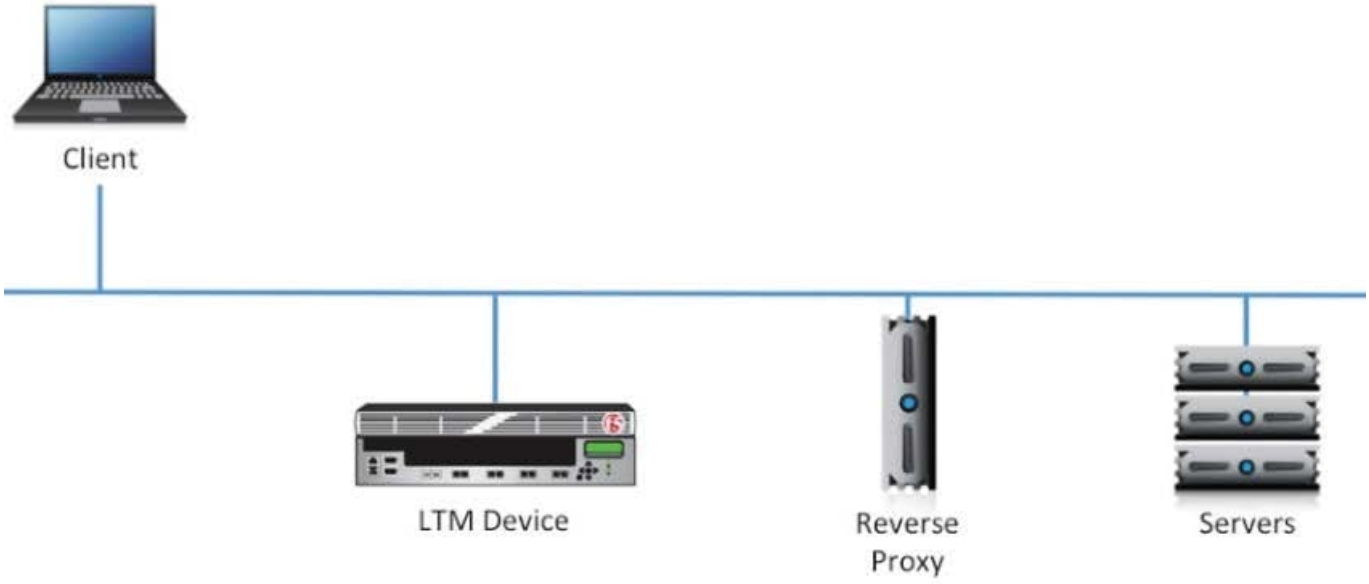
https://www.leads4pass.com/301b.html

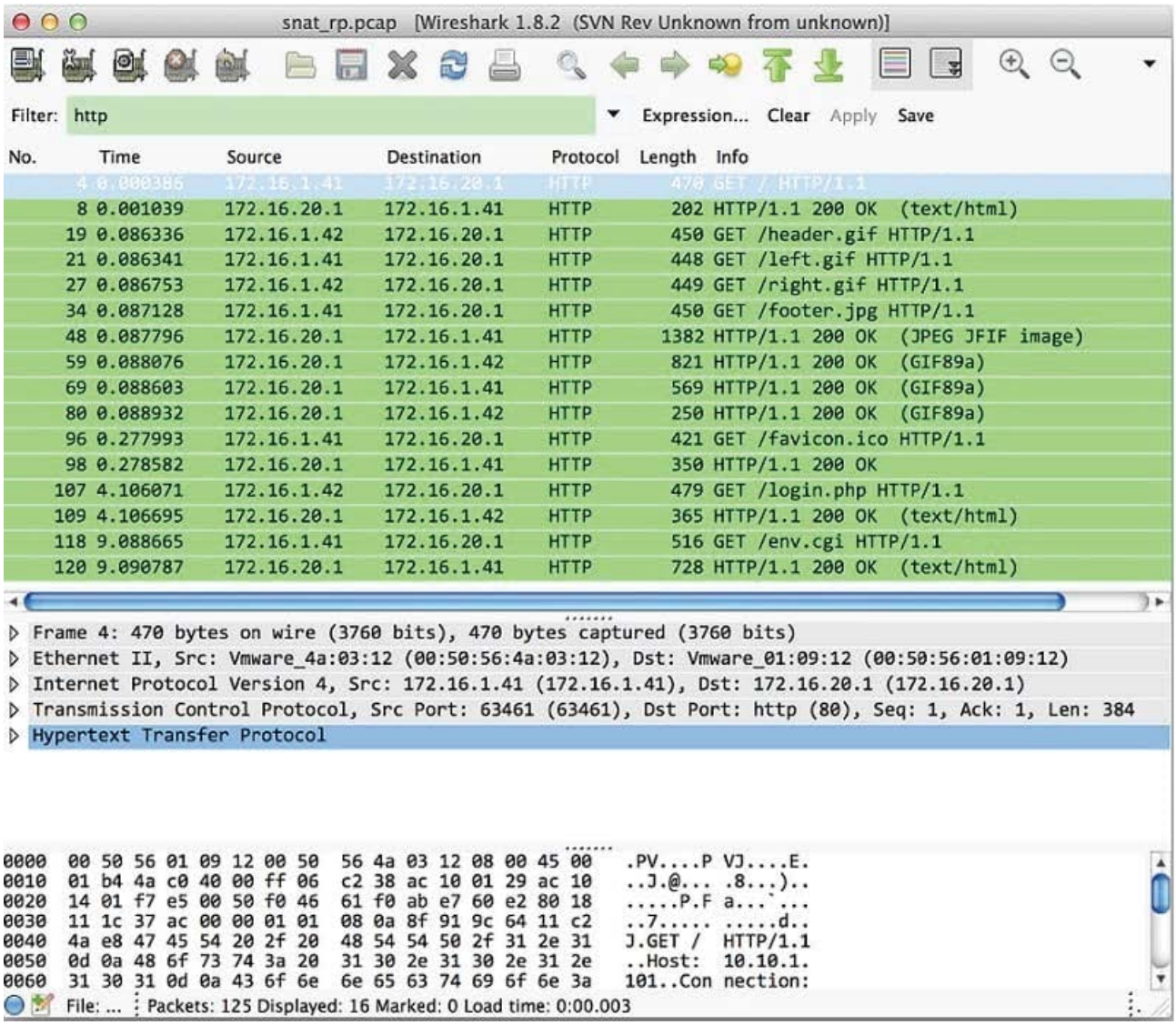
100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

-- Exhibit





-- Exhibit -Refer to the exhibits. A virtual server has been configured for SSL offload on a single-arm network. On

average, the virtual server will be handling 100,000 connections, with a peak of 130,000 connections. Between the virtual server and the web servers there is a

single reverse proxy to provide site caching. The proxy is configured to perform source IP persistence before contacting the web servers. The site is logging users out immediately after logging them in. What should the LTM Specialist do to resolve this issue?

A. Add a source address persistence profile to the virtual server.

B. Create an iRule to add client IP persistence to a SNAT pool member.

C. Change the virtual server server-side TCP profile to tcp-lan-optimized.

D. Configure the virtual server HTTP profile to insert an X-Forwarded-For header.

Correct Answer: B

QUESTION 2

An LTM Specialist needs to modify the logging level for tcpdump execution events. Checking the BigDB Key, the following is currently configured:

sys db log.tcpdump.level {

value "Notice"

}

Which command should the LTM Specialist execute on the LTM device to change the logging level to informational?

A. tmsh set /sys db log.tcpdump.level value informational

B. tmsh set /sys db log.tcpdump.level status informational

C. tmsh modify /sys db log.tcpdump.level value informational

D. tmsh modify /sys db log.tcpdump.level status informational

Correct Answer: C

QUESTION 3

A customer needs to intercept all of the redirects its application is sending to clients. When a redirect is matched, the customer needs to log a message including the client IP address.

Which iRule should be used?

A. when HTTP_RESPONSE { if { [HTTP::is_3xx] } { log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"

}

}

B. when HTTP_REQUEST { if { [HTTP::is_301] } { log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"

}

}

C. when HTTP_REQUEST { if { [HTTP::is_redirect] } { log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"

}

}

D. when HTTP_RESPONSE { if { [HTTP::is_redirect] } { log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]"

}

}

Correct Answer: D

QUESTION 4

-- Exhibit

Capture through LTM device

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on External, link-type EN10MB (Ethernet), capture size 96 bytes

16:52:54.866907 IP 192.168.1.1.6789 > 192.168.1.211.443: S 2995699259:2995699259(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
16:52:54.866974 IP 192.168.1.211.443 > 192.168.1.1.6789: S 2305990363:2305990363(0) ack 2995699260 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868417 IP 192.168.1.1.6789 > 192.168.1.211.443: . ack 1 win 16425
16:52:54.868422 IP 192.168.1.1.6789 > 192.168.1.211.443: P 1:105(104) ack 1 win 16425
16:52:54.868451 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:52:54.868457 IP 192.168.1.211.443 > 192.168.1.1.6789: . ack 105 win 4484
16:52:57.869207 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:01.068627 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:53:04.268911 IP 192.168.1.144.6789 > 192.168.10.80.443: S 236216155:236216155(0) win 4380 <mss 1460,sackOK,eol>
16:53:07.468781 IP 192.168.1.211.443 > 192.168.1.1.6789: R 1:1(0) ack 105 win 4484
```

Capture direct to application server

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes

09:46:03.428985 IP 192.168.1.1.31214 > 192.168.10.80.8443: S 1295563595:1295563595(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:46:03.430000 IP 192.168.10.80.8443 > 192.168.1.1.31214: S 2962914236:2962914236(0) ack 1295563596 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 3>
09:46:03.430041 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 1 win 4380
09:46:03.463946 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 1:137(136) ack 1 win 4380
09:46:03.465072 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 137 win 864
09:46:03.466127 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1:139(138) ack 137 win 864
09:46:03.466150 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 139 win 4518
09:46:03.720163 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 137:196(59) ack 139 win 4518
09:46:03.720183 IP 192.168.1.1.31214 > 192.168.10.80.8443: P 196:542(346) ack 139 win 4518
09:46:03.721853 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 542 win 998
09:46:03.723009 IP 192.168.10.80.8443 > 192.168.1.1.31214: . 139:1599(1460) ack 542 win 998
09:46:03.723023 IP 192.168.10.80.8443 > 192.168.1.1.31214: P 1599:2693(1094) ack 542 win 998
09:46:03.723026 IP 192.168.10.80.8443 > 192.168.1.1.31214: F 2693:2693(0) ack 542 win 998
09:46:03.723060 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2693 win 7072
09:46:03.723072 IP 192.168.1.1.31214 > 192.168.10.80.8443: . ack 2694 win 7072
09:46:03.818084 IP 192.168.1.1.31214 > 192.168.10.80.8443: F 542:542(0) ack 2694 win 7072
09:46:03.819820 IP 192.168.10.80.8443 > 192.168.1.1.31214: . ack 543 win 998
```

Trace direct to application server

Started	Time Chart	!	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000	This page (index.html) is from Server 1								
+0.000		!	9.140	278	2480	GET	200		http://srv1.example.com/
+9.144		!	9.134	336	5079	GET	200		http://srv1.example.com/header.gif
+9.146		!	9.266	334	19307	GET	200		http://srv1.example.com/left.gif
+9.147		!	9.232	335	14644	GET	200		http://srv1.example.com/right.gif
+9.149		!	9.189	336	4192	GET	200		http://srv1.example.com/footer.jpg
	9.186 → 18.414 →	!	18.412	1619	45702	5 requests			

Trace through LTM device

Started	Time Chart	!	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000	This page (index.html) is from SSL Server 1								
+0.000		!	0.428	346	2650	GET	200		https://www.example.com/
+0.435		!	9.110	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/header.gif
+0.435		!	9.322	298	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/left.gif
+0.435		!	9.322	299	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/right.gif
+0.435		!	9.322	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.example.com/footer.jpg
	← 0.452 9.759 →	!	9.757	1543	2650	5 requests			

```
ltm virtual VS_HTTP {
    destination 10.10.17.100:http
    ip-protocol tcp
    mask 255.255.255.255
    pool Pool_HTTP
    profiles {
        customHTTP { }
        tcp { }
    }
    vlans-disabled
}
ltm pool Pool_HTTP {
    members {
        172.16.20.1:http {
            address 172.16.20.1
        }
    }
}
ltm profile http customHTTP {
    app-service none
    defaults-from http
    encrypt-cookies none
    fallback-host none
    fallback-status-codes none
    header-erase Host
    header-insert none
    insert-xforwarded-for disabled
    lws-separator none
    lws-width 80
    max-header-count 64
    max-header-size 32768
    max-requests 0
    oneconnect-transformations enabled
    pipelining enabled
    redirect-rewrite none
    request-chunking preserve
    response-chunking selective
    response-headers-permitted none
    security disabled
    via-request preserve
    via-response preserve
}
```

```
ltm virtual VS_HTTP {
    destination 10.10.17.100:http
    ip-protocol tcp
    mask 255.255.255.255
    pool Pool_HTTP
    profiles {
        http { }
        tcp { }
    }
    snat automap
    vlans-disabled
}
ltm pool Pool_HTTP {
    members {
        172.16.20.1:http {
            address 172.16.20.1
        }
        172.16.20.2:http {
            address 172.16.20.2
        }
        172.16.20.3:http {
            address 172.16.20.3
        }
    }
}
```

-- Exhibit -Refer to the exhibits.

An LTM Specialist is troubleshooting an application configured on an LTM device on a one- armed configuration. The application is NOT working through the LTM device but does work when accessed directly via the application servers. The

virtual server 192.168.1.211:443 is configured to SNAT using the address 192.168.1.144 and references a pool with the member 192.168.10.80:443. No Client or Server SSL profiles are associated. The LTM Specialist has collected two traffic

captures to help determine the issue.

What is the problem with the configuration on the LTM device?

A. Pool member is configured to use wrong port.

B. Pool member is configured for SSL off-loading.

C. Virtual server is configured to use wrong port.

D. Virtual server is configured without SSL Profiles.

Correct Answer: A

QUESTION 5

Given LTM device ltm log:

Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5: semaphore mcpd.running(1) held

Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5:

Sep 26 20:51:08 local/lb-d-1 warning promptstatusd[3695]: 01460005:4: mcpd.running(1) held, wait for mcpd

Sep 26 20:51:08 local/lb-d-1 info sod[3925]: 010c0009:6: Lost connection to mcpd - reestablishing.

Sep 26 20:51:08 local/lb-d-1 err bcm56xxd[3847]: 012c0004:3: Lost connection with MCP: 16908291 ... Exiting bsx_connect.cpp(174)

Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: MCP Exit Status

Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: Info: LACP stats (time now:1348717868) : no traffic

Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0014:6: Exiting...

Sep 26 20:51:08 local/lb-d-1 err lind[3842]: 013c0004:3: IO error on recv from mcpd - connection lost

Sep 26 20:51:08 local/lb-d-1 notice bigd[3837]: 01060110:5: Lost connection to mcpd with error 16908291, will reinit connection.

Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0004:3: Initial subscription for system configuration failed with error \\'\\'

Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0001:3: Connection to mcpd failed with error \\'011b0004:3: Initial subscription for system configuration failed with error \\'\\'\\'

Sep 26 20:51:08 local/lb-d-1 err csyncd[3851]: 013b0004:3: IO error on recv from mcpd - connection lost

.....skipping more logs.....

Sep 26 20:51:30 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running bcm56xxd is now responding.

Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running mcpd is now responding.

Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 010c0018:5: Standby

Which daemon failed?

A. promptstatusd

B. mcpd

C. sod

D. bcm56xxd

E. lind

Correct Answer: B

QUESTION 6

-- Exhibit

LTM device statistics

Search Reset Search

Status	Virtual Server	Partition / Path	Details	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total
	VS_HTTP	Common	View...	283.8K	2.4M	391	544	0	5	55

Search Reset Search

Status	Pool/Member	Partition / Path	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total
	Pool_HTTP	Common	193.9K	2.4M	284	347	0	5	55
	– 172.16.20.1:80	Common	103.4K	1.5M	163	206	0	1	18
	– 172.16.20.2:80	Common	90.1K	872.4K	120	141	0	2	18
	– 172.16.20.3:80	Common	416	0	1	0	0	2	19

-- Exhibit -Refer to the exhibit.

An LTM Specialist is investigating intermittent page load issues being reported by users.

What should the LTM Specialist do to resolve the issue?

A. Remove HTTP monitor on the pool.

B. Assign an HTTP monitor to the pool.

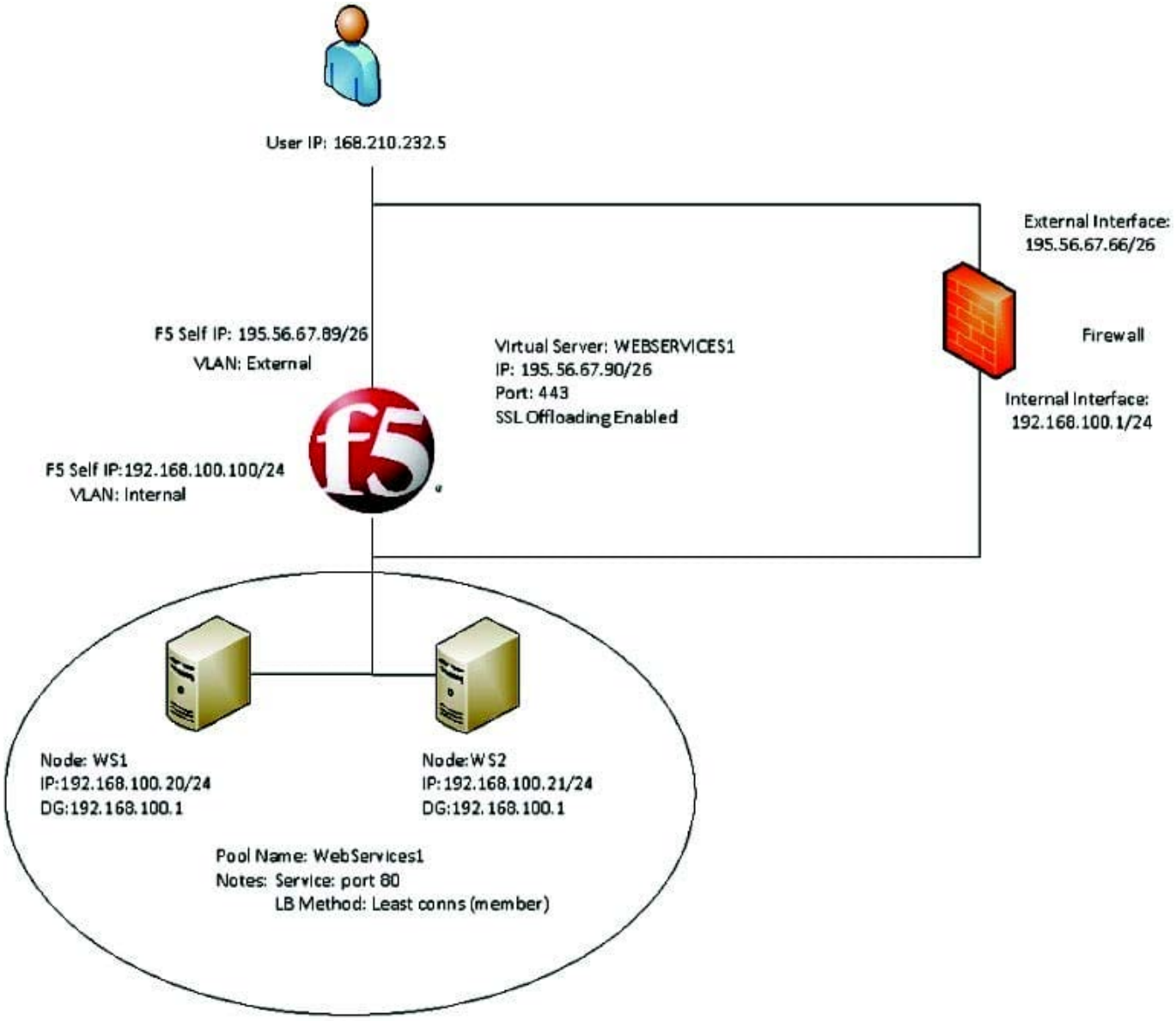
C. Select least connections load balancing method on virtual server.

D. Remove least connections load balancing method on virtual server.

Correct Answer: B

QUESTION 7

-- Exhibit -



-- Exhibit -Refer to the exhibit.

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

The LTM Specialist is seeing a client source IP of 168.210.232.5 in the tcpdump. However, the client source IP is actually 10.123.17.12.

Why does the IP address of 10.123.17.12 fail to appear in the tcpdump?

A. The LTM device performed NAT on the individual\\'s IP address.

B. The Secure Network Address Translation (SNAT) pool on the virtual server is activated.

C. Network Address Translation (NAT) has occurred in the path between the client and the LTM device.

D. The individual\\'s data stream is being routed to the LTM device by a means other than the default route.

Correct Answer: C

QUESTION 8

An LTM Specialist has a OneConnect profile and HTTP profile configured on a virtual server to load balance an HTTP application.

The following HTTP headers are seen in a network trace when a client connects to the virtual server:

Clientside: GET / HTTP/1.1 Host: 192.168.136.100 User-Agent: Mozilla/5.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-EncodinG. gzip, deflate Connection: keep-alive

Serverside: HTTP/1.1 200 OK DatE. 5 Jun 1989 17:06:55 GMT Server: Apache/2.2.14 (Ubuntu) Vary: Accept-Encoding Content-EncodinG. gzip Content-LengtH. 3729 X-Cnection: close Content-TypE. text/html

The LTM Specialist notices the OneConnect feature is working incorrectly.

Why is OneConnect functioning incorrectly?

A. Client must support HTTP/1.0.

B. Client must support HTTP keep-alive.

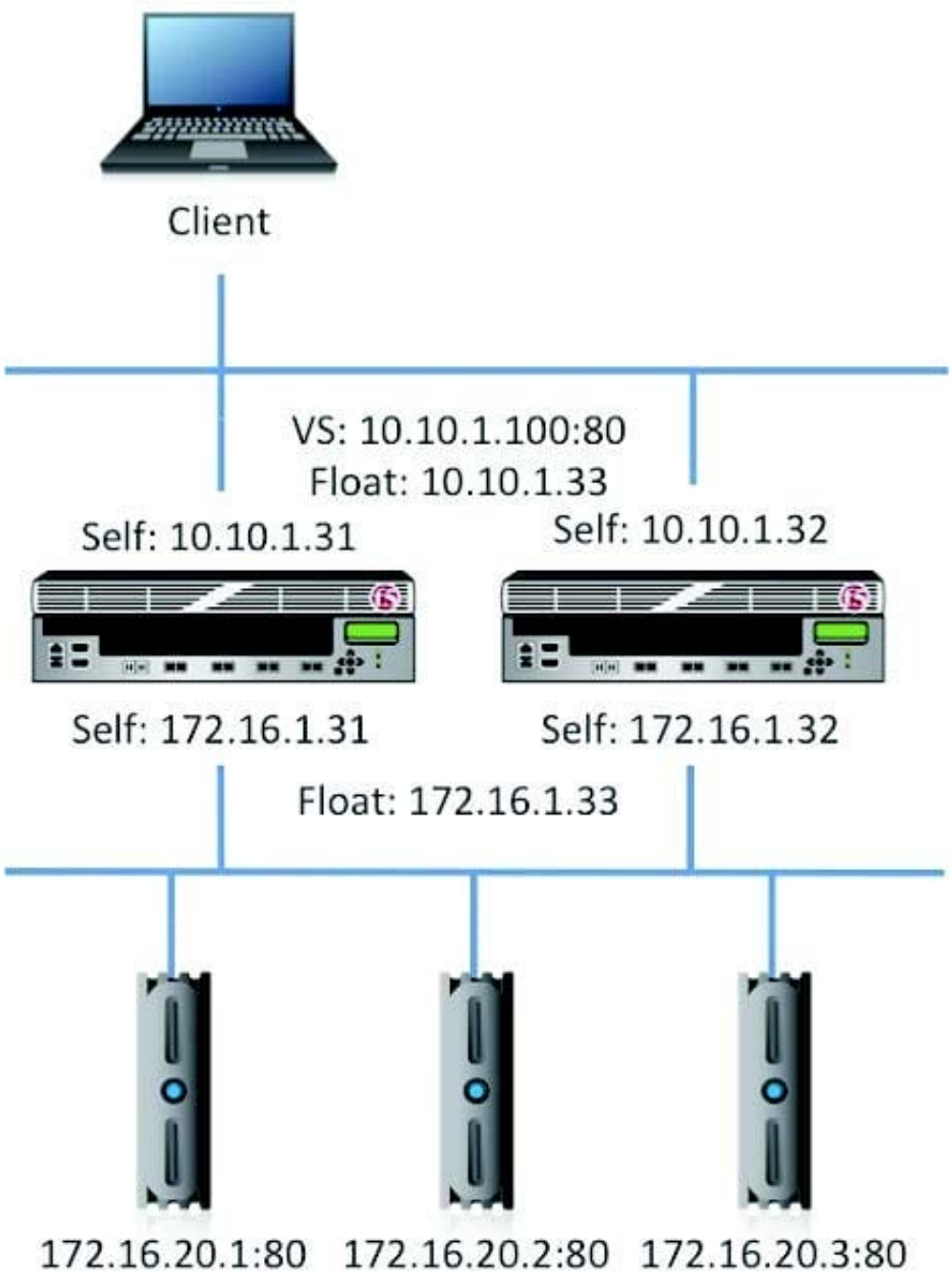
C. Server must support HTTP/0.9.

D. Server must support HTTP keep-alive.

Correct Answer: D

QUESTION 9

-- Exhibit



-- Exhibit -Refer to the exhibit.

A server administrator notices that one server is intermittently NOT being sent any HTTP requests. The server logs display no issues. The LTM Specialist notices log entries stating the node (172.16.20.1) status cycling between down and up.

The pool associated with the virtual server (10.10.1.100) has a custom HTTP monitor applied. Which tcpdump filter will help trace the monitor?

A. tcpdump -i internal port 80 and host 172.16.1.31

B. tcpdump -i external port 80 and host 10.10.1.100

C. tcpdump -i internal port 80 and host 172.16.1.33

D. tcpdump -i external port 80 and host 172.16.20.1

Correct Answer: A

QUESTION 10

-- Exhibit

```
1 1  0.2423 (0.2423)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
1 2  0.2432 (0.0008)  S>CShort record
1    0.2432 (0.0000)  S>C  TCP FIN
New TCP connection #2: 168.210.232.5(24782) <-> 193.33.229.103(443)
2 1  0.2393 (0.2393)  C>S  Handshake
      ClientHello
        Version 3.2
        cipher suites
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_DSS_WITH_AES_256_CBC_SHA
         TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
                  NULL
Unknown SSL content type 72
2 2  0.2404 (0.0010)  S>CShort record
2    0.2404 (0.0000)  S>C  TCP FIN
2 3  0.4738 (0.2333)  C>S  Alert
    level           fatal
    value           unexpected_message
2    0.4742 (0.0003)  C>S  TCP FIN
1 3  0.4857 (0.2425)  C>S  Alert
    level           fatal
    value           unexpected_message
1    0.4857 (0.0000)  C>S  TCP FIN
```

-- Exhibit -Refer to the exhibit.

A client attempts to connect from a Google Chrome browser to a virtual server on a BIG-IP LTM. The virtual server is SSL Offloaded. When the client connects, the client receives an SSL error. The client receives the same errors when

trying Mozilla Firefox and Internet Explorer browsers.

The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit. How should this be resolved?

A. Set the virtual server to listen on port 443 (HTTPS).

B. Upgrade the client to support the appropriate SSL cipher suite.

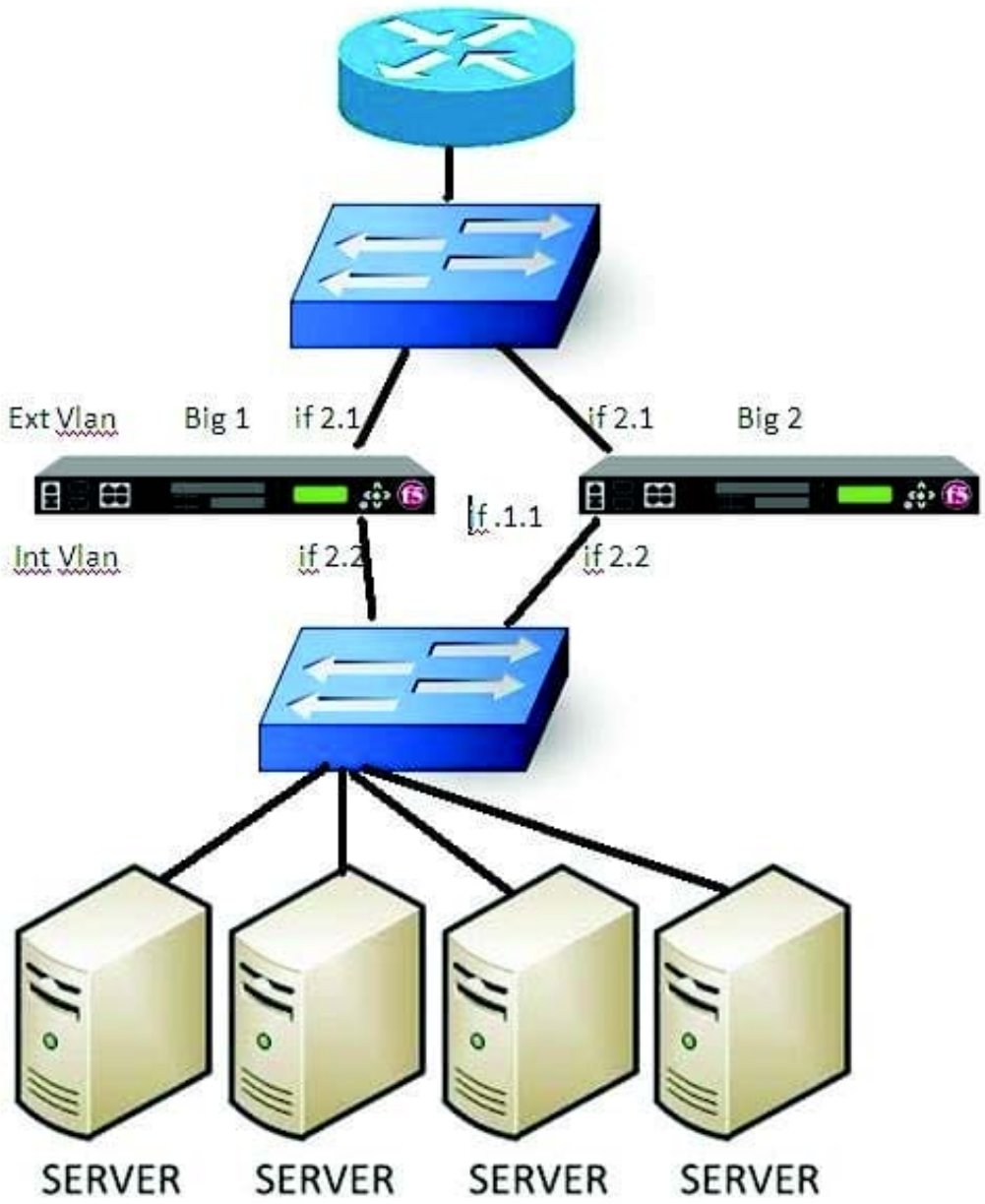
C. Select the appropriate "SSL Profile (Client)" in the virtual server settings.

D. Adjust the SSL key length in the SSL profile to match the minimum required by the client.

Correct Answer: C

QUESTION 11

-- Exhibit



-- Exhibit -Refer to the exhibit.

A failover has just occured on BIG-IP1. BIG-IP2 is now active and manages traffic as expected. Both Bigip\\'s are set with a gateway failsafe to check the reachability of the main border router.

Switches have performed as expected.

Where should the LTM Specialist check for potential issues?

A. Network Interface 2.1 of BIG-IP 2

B. Network Interface 2.1 of BIG-IP 1

C. Network Interface 2.2 of BIG-IP 2

D. Network Interface 2.2 of BIG-IP 1

E. Network Interface 1.1 of BIG-IP 1

F. Network Interface 1.1 of BIG-IP 2

Correct Answer: B

QUESTION 12

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.

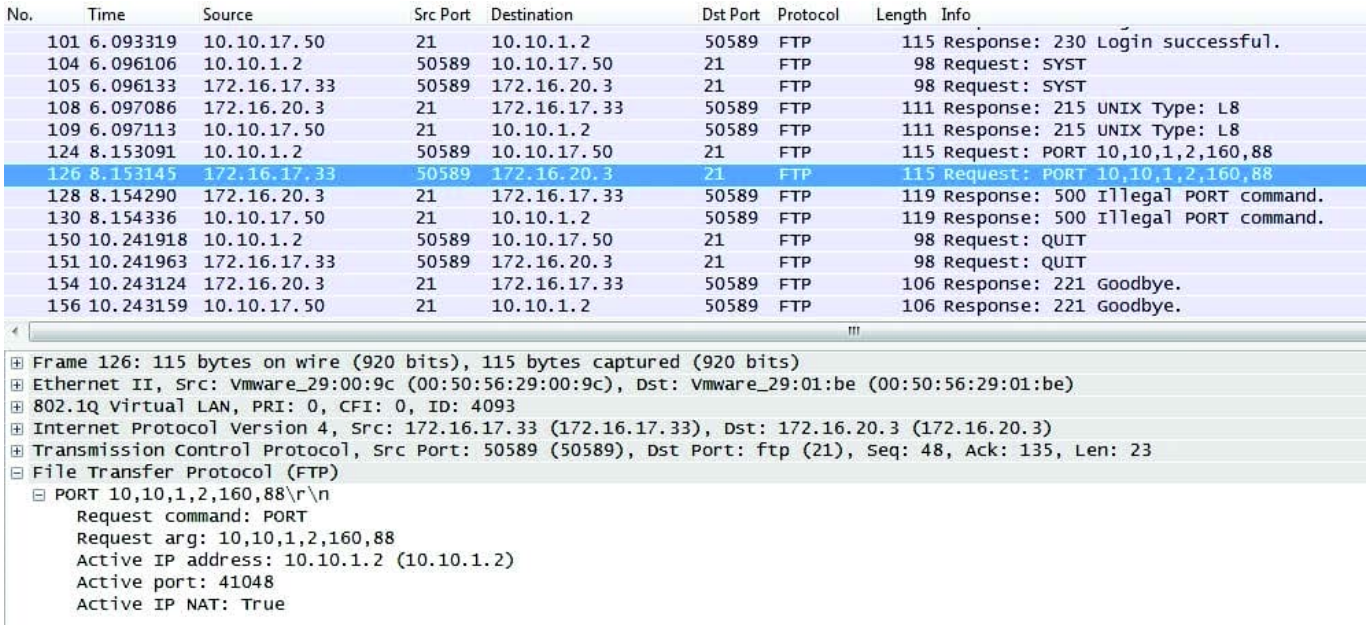
D. The BigDB Key Log.Tcpdump.Level needs to be adjusted.

Correct Answer: C

QUESTION 13

-- Exhibit -- Exhibit -Refer to the exhibit. An LTM Specialist is investigating reports that users are unable to perform some commands through an FTP virtual server. The users are receiving the FTP error "500 Illegal PORT command."

The virtual server is configured to SNAT using



No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
101	6.093319	10.10.17.50	21	10.10.1.2	50589	FTP	115	Response: 230 Login successful.
104	6.096106	10.10.1.2	50589	10.10.17.50	21	FTP	98	Request: SYST
105	6.096133	172.16.17.33	50589	172.16.20.3	21	FTP	98	Request: SYST
108	6.097086	172.16.20.3	21	172.16.17.33	50589	FTP	111	Response: 215 UNIX Type: L8
109	6.097113	10.10.17.50	21	10.10.1.2	50589	FTP	111	Response: 215 UNIX Type: L8
124	8.153091	10.10.1.2	50589	10.10.17.50	21	FTP	115	Request: PORT 10,10,1,2,160,88
126	8.153145	172.16.17.33	50589	172.16.20.3	21	FTP	115	Request: PORT 10,10,1,2,160,88
128	8.154290	172.16.20.3	21	172.16.17.33	50589	FTP	119	Response: 500 Illegal PORT command.
130	8.154336	10.10.17.50	21	10.10.1.2	50589	FTP	119	Response: 500 Illegal PORT command.
150	10.241918	10.10.1.2	50589	10.10.17.50	21	FTP	98	Request: QUIT
151	10.241963	172.16.17.33	50589	172.16.20.3	21	FTP	98	Request: QUIT
154	10.243124	172.16.20.3	21	172.16.17.33	50589	FTP	106	Response: 221 Goodbye.
156	10.243159	10.10.17.50	21	10.10.1.2	50589	FTP	106	Response: 221 Goodbye.

```
⊞ Frame 126: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
⊞ Ethernet II, Src: Vmware_29:00:9c (00:50:56:29:00:9c), Dst: Vmware_29:01:be (00:50:56:29:01:be)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 4093
⊞ Internet Protocol Version 4, Src: 172.16.17.33 (172.16.17.33), Dst: 172.16.20.3 (172.16.20.3)
⊞ Transmission Control Protocol, Src Port: 50589 (50589), Dst Port: ftp (21), Seq: 48, Ack: 135, Len: 23
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 10,10,1,2,160,88\r\n
      Request command: PORT
      Request arg: 10,10,1,2,160,88
      Active IP address: 10.10.1.2 (10.10.1.2)
      Active port: 41048
      Active IP NAT: True
```

automap. The LTM Specialist performs a capture on the server side of the LTM device. Why is the server returning this error?

A. LIST command disallowed

B. PORT command disallowed

C. Active IP address in PORT command

D. Active IP address in LOGIN command

Correct Answer: C

QUESTION 14

-- Exhibit

```
New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)
3 1  0.0006 (0.0006)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
3 2  0.0009 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          ed 15 16 5f c2 9d bf 5e e6 70 0e a4 86 59 bf 27
          e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 67 e4 f7
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
3 3  0.0009 (0.0000)  S>C  Handshake
      Certificate
3 4  0.0009 (0.0000)  S>C  Handshake
      ServerHelloDone
New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)
4 1  0.0004 (0.0004)  C>S  Handshake
      ClientHello
        Version 3.1
        cipher suites
        TLS_RSA_WITH_RC4_128_SHA
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        Unknown value 0x3c
        Unknown value 0x3d
        Unknown value 0xff
        compression methods
                  NULL
4 2  0.0007 (0.0002)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72
          95 ef 43 e5 4e 10 f4 3b b2 3e 5c ec 5e ee 66 a8
        cipherSuite         TLS_RSA_WITH_RC4_128_SHA
        compressionMethod                   NULL
4 3  0.0007 (0.0000)  S>C  Handshake
      Certificate
4 4  0.0007 (0.0000)  S>C  Handshake
      ServerHelloDone
3    0.0015 (0.0006)  C>S  TCP RST
4    0.0010 (0.0003)  C>S  TCP RST
```

```
[~]$ 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)
---
```

-- Exhibit -Refer to the exhibits.

After upgrading LTM from v10 to v11, users are unable to connect to an application. The virtual server is using a client SSL profile for re-terminating SSL for payload inspection, but a server SSL profile is being used to re-encrypt the request.

A client side ssldump did NOT show any differences between the traffic going directly to the server and the traffic being processed by the LTM device. However, packet capture was done on the server, and differences were noted.

Which modification will allow the LTM device to process the traffic correctly?

A. Enable Strict Resume.

B. Change Secure Renegotiation to "Request."

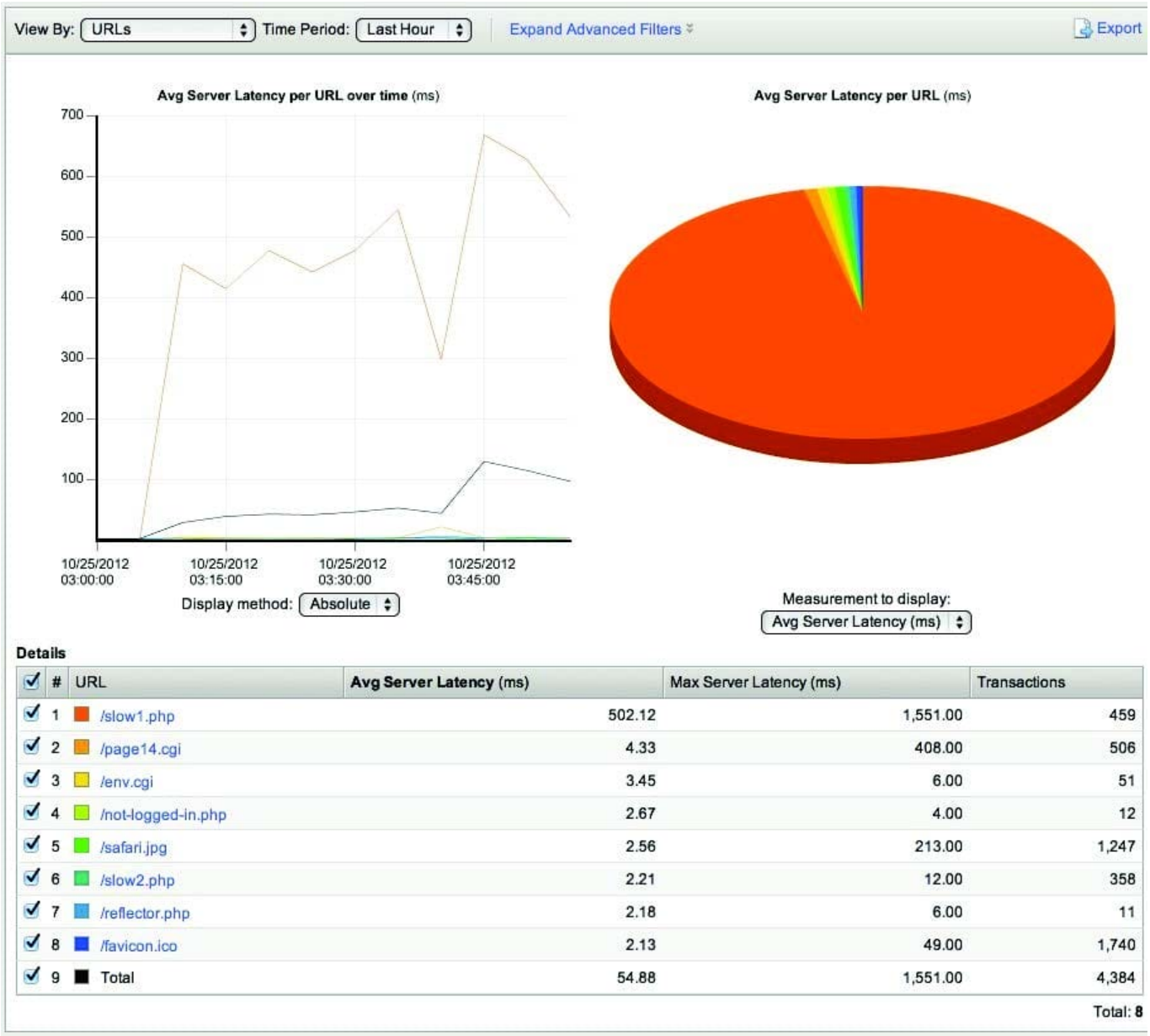
C. Enable ProxySSL option in the server SSL profile.

D. Change to different ciphers on the server SSL profile.

Correct Answer: B

QUESTION 15

-- Exhibit



-- Exhibit -Refer to the exhibits.

Which URL on which server is causing the highest latency for users?

A. /slow1.php on 172.16.20.3

B. /slow2.php on 172.16.20.1

C. /reflector.php on 172.16.20.2

D. /Compress.HTML on 172.16.20.1

Correct Answer: A