

Exaactexams 301b Gregory 203q

Number: 301b
Passing Score: 800
Time Limit: 120 min
File Version: 14.0

Exam Code: 301b

Exam Name: LTM Specialist: Maintain & Troubleshoot



301b

QUESTION 1

A OneConnect profile is applied to a virtual server. The LTM Specialist would like the client source IP addresses within the 10.10.10.0/25 range to reuse an existing server side connection.

Which OneConnect profile source mask should the LTM Specialist use?

- A. 0.0.0.0
- B. 255.255.255.0
- C. 255.255.255.128
- D. 255.255.255.224
- E. 255.255.255.255

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

An LTM device is load balancing telnet and ssh applications in a client/server environment experiencing significant packet delay.

Which setting in the TCP profile should reduce the amount of packet delay?

- A. disable Bandwidth Delay
- B. disable Nagle's Algorithm
- C. enable Proxy Maximum Segment
- D. increase Maximum Segment Retransmissions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

An LTM device is load balancing SIP traffic. An LTM Specialist notices that sometimes the SIP request is being load balanced to the same server as the initial connection. Which setting in the UDP profile will make the LTM device more evenly distribute the SIP traffic?

- A. Enable Datagram LB
- B. Disable Datagram LB
- C. Set Timeout to Indefinite
- D. Set Timeout to Immediate

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Internet clients connecting to a virtual server to download a file are experiencing about 150 ms of latency and no packet loss.

Which built-in client-side TCP profile provides the highest throughput?

- A. tcp
- B. tcp-legacy
- C. tcp-lan-optimized
- D. tcp-wan-optimized

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Windows PC clients are connecting to a virtual server over a high-speed, low-latency network with no packet loss.

Which built-in client-side TCP profile provides the highest throughput for HTTP downloads?

- A. tcp
- B. tcp-legacy
- C. tcp-lan-optimized
- D. tcp-wan-optimized

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

Users are experiencing low throughput when downloading large files over a high-speed WAN connection. Extensive packet loss was found to be an issue but CANNOT be eliminated.

Which two TCP profile settings should be modified to compensate for the packet loss in the network? (Choose two.)

- A. slow start
- B. proxy options
- C. proxy buffer low
- D. proxy buffer high
- E. Nagle's algorithm

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

An LTM Specialist is working with an LTM device configured with 10 virtual servers on the same domain with a different key/cert pair per virtual. For exampleE. www.example.com; ftp.example.com; ssh.example.com; ftps.example.com.

What should the LTM Specialist do to reduce the number of objects on the LTM device?

- A. create a 0 port virtual server and have it answer for all protocols
- B. create a 0.0.0.0:0 virtual server thus eliminating all virtual servers
- C. create a transparent virtual server thus eliminating all virtual servers
- D. create a wildcard certificate and use it on all *.example.com virtual servers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:**QUESTION 8**

The pool members are serving up simple static web content.

The current virtual server configuration is given as follows:

```
tmsh list ltm virtual simple
ltm virtual simple {
    destination 10.10.10.10:80
    ip-protocol tcp
    mask 255.255.255.255
    profiles {
        http { }
        httpcompression { }
        oneconnect { }
        tcp { }
    }
    snat automap
    vlans-disabled
}
```

```
tmsh list ltm pool simple_pool
ltm pool simple_pool {
    members {
        10.10.10.11:80 {
            address 10.10.10.11    }
        10.10.10.12:80 {
            address 10.10.10.12    }
        10.10.10.12:80 {
            address 10.10.10.13    }
    }
}
```

Which three objects in the virtual server configuration can be removed without disrupting functionality of the virtual server? (Choose three.)

- A. tcp
- B. http
- C. oneconnect
- D. snat automap
- E. httpcompression

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

An LTM device is running BIG-IP v10.2.0 software. The LTM Specialist is tasked with upgrading the LTM device to BIG-IP v11.2.0 HF1. The LTM Specialist starts the upgrade process by selecting the uploaded Hotfix and installing to an unused volume. After 10 minutes, the LTM Specialist checks the status of the upgrade process and notices that the process is stalled at 0%.

What should the LTM Specialist verify?

- A. the selected volume has sufficient space available
- B. the base software version exists on the LTM device
- C. the LTM device has been restarted into maintenance mode
- D. the LTM device has an available Internet connection via the management interface

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A stand-alone LTM device is to be paired with a second LTM device to create an active/standby pair. The current stand-alone LTM device is in production and has several VLANs with floating IP addresses configured. The appropriate device service clustering (DSC) configurations are in place on both LTM devices.

Which two non-specific DSC settings should the LTM Specialist configure on the second LTM device to ensure no errors are reported when attempting to synchronize for the first time? (Choose two.)

- A. pools
- B. VLANs
- C. default route
- D. self IP addresses

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

What is the correct command to reset an LTM device to its default settings?

- A. tmsh reset-all default
- B. tmsh set /sys config defaults
- C. tmsh load /sys config default
- D. tmsh /util bigpipe reset-factory-defaults

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

In which file would the LTM Specialist find virtual server configurations?

- A. bigip.conf
- B. bigip_sys.conf
- C. bigip_base.conf
- D. profile_base.conf

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

An LTM Specialist must perform a hot fix installation from the command line.

What is the correct procedure to ensure that the installation is successful?

- A. import the hot fix to the /var/shared/images directory
check the integrity of the file with an md5 checksum
tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
- B. import the hot fix to the /var/shared/images directory
check the integrity of the file with an md5 checksum
tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>
- C. import the hot fix to the /shared/images directory
check the integrity of the file with an md5 checksum
tmsh apply sys software hotfix volume <volume_name> <hotfix_name>.iso
- D. import the hot fix to the /shared/images directory
check the integrity of the file with an md5 checksum
tmsh install sys software hotfix <hotfix_name>.iso volume <volume_name>

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

Which two alerting capabilities can be enabled from within an application visibility reporting (AVR) analytics profile? (Choose two.)

- A. sFlow
- B. SNMP
- C. e-mail
- D. LCD panel alert
- E. high speed logging (HSL)

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

What is a benefit provided by F5 Enterprise Manager?

- A. Enterprise Manager allows administrators to analyze traffic flow and create custom application IPS signatures.

- B. Enterprise Manager allows administrators to establish baseline application usage and generate an alert if an administrator set threshold for the application is exceeded.
- C. Enterprise Manager allows administrators to identify application vulnerabilities. Virtual patches are then automatically generated and applied to remediate the detected application vulnerability.
- D. Enterprise Manager allows administrators to monitor all application traffic. Configuration optimization suggestions based on the observed traffic patterns are then generated for the administrator to review and apply.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which two items can be logged by the Application Visibility Reporting analytics profile? (Choose two.)

- A. User Agent
- B. HTTP version
- C. HTTP Response Codes
- D. Per Virtual Server CPU Utilization

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Which file should be modified to create custom SNMP alerts?

- A. /config/alert.conf
- B. /etc/alertd/alert.conf
- C. /config/user_alert.conf
- D. /etc/alertd/user_alert.conf

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

An LTM Specialist has set up a custom SNMP alert.

Which command line tool should the LTM Specialist use to test the alert?

- A. logger
- B. logtest
- C. testlog
- D. snmptest

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

An LTM Specialist is customizing local traffic logging.

Which traffic management OS alert level provides the most detail?

- A. Alert
- B. Notice
- C. Critical
- D. Emergency
- E. Informational

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

A new web application is hosted at www.example.net, but some clients are still pointing to the legacy web application at www.example.com.

Which iRule will allow clients referencing www.example.com to access the new application?

- A.

```
when HTTP_REQUEST {  
  if {[HTTP::host] equals "www.example.*"}{  
    HTTP::redirect "http://www.example.net" }  
}
```
- B.

```
when HTTP_REQUEST {  
  if {[HTTP::host] equals "www.example.com"}{  
    HTTP::redirect "http://www.example.net" }  
}
```
- C.

```
when HTTP_DATA {  
  if {[HTTP::host] equals "www.example.*"}{  
    HTTP::redirect "http://www.example.net" }  
}
```
- D.

```
when HTTP_RESPONSE {  
  if {[HTTP::host] equals "www.example.com"}{  
    HTTP::redirect "http://www.example.net" }  
}
```

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Which iRule will instruct the client's browser to avoid caching HTML server responses?

- A.

```
when HTTP_REQUEST {  
  if {[HTTP::header Content-Type] equals "html"} {  
    HTTP::header insert Pragma "no-cache"  
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT"  
    HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate"  
  }  
}
```
- B.

```
when HTTP_REQUEST {  
  if {[HTTP::header Content-Type] contains "html"} {  
    HTTP::header insert Pragma "no-cache"  
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT"  
    HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate"
```

```
    }  
  }  
C. when HTTP_RESPONSE {  
    if {[HTTP::header Content-Type] contains "html"} {  
      HTTP::header insert Pragma "no-cache"  
      HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT"  
      HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate"  
    }  
  }  
D. when HTTP_RESPONSE {  
    if {[HTTP::header Content-Type] equals "html"} {  
      HTTP::header insert Pragma "no-cache"  
      HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT"  
      HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate"  
    }  
  }  
}
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

An IT administrator wants to log which server is being load balanced to by a user with IP address 10.10.10.25.

Which iRule should the LTM Specialist use to fulfill the request?

```
A. when SERVER_CONNECTED {  
  if { [IP::addr [IP::remote_addr]] equals 10.10.10.25 } {  
    log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }  
  }  
B. when CLIENT_ACCEPTED {  
  if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25 } {  
    log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }  
  }  
C. when SERVER_CONNECTED {  
  if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25 } {  
    log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }  
  }  
D. when CLIENT_ACCEPTED {
```

```
if { [IP::addr [IP::remote_addr] equals 10.10.10.25] } {  
  log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" }  
}
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

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

Section: (none)

Explanation

Explanation/Reference:**QUESTION 24**

A web application requires knowledge of the client's true IP address for logging and analysis purposes. Instances of the application that can decode X-Forwarded-For HTTP headers reside in pool_a, while pool_b instances assume the source IP is the true address of the client. Which iRule provides the proper functionality?

- A.

```
when HTTP_DATA {  
  if {[HTTP::header exists X-Forwarded-For]}{  
    pool pool_a  
  } else {  
    pool pool_b  
  }  
}
```
- B.

```
when HTTP_RESPONSE {  
  if {[HTTP::header exists X-Forwarded-For]}{  
    pool pool_a  
  } else {  
    pool pool_b  
  }  
}
```
- C.

```
when HTTP_REQUEST {  
  if {[HTTP::header exists X-Forwarded-For]}{  
    pool pool_a  
  } else {  
    pool pool_b  
  }  
}
```
- D.

```
when HTTP_OPEN {  
  if {[HTTP::header exists X-Forwarded-For]}{  
    pool pool_a  
  } else {  
    pool pool_b  
  }  
}
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which iRule will reject any connection originating from a 10.0.0.0/8 network?

- A. `when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::remote_addr] mask 8]
 switch $remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1 }
 default { pool http_pool }
 }
}`
- B. `when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::local_addr] mask 8]
 switch $remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1 }
 default { pool http_pool }
 }
}`
- C. `when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::client_addr] mask 255.0.0.0]
 switch $remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1 }
 default { pool http_pool }
 }
}`
- D. `when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::local_addr] mask 255.0.0.0]
 switch $remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1 }
 default { pool http_pool }
 }
}`

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

There is a fault with an LTM device load balanced trading application that resides on directly connected VLAN vlan-301. The application virtual server is 10.0.0.1:80 with trading application backend servers on subnet 192.168.0.0/25. The LTM Specialist wants to save a packet capture with complete payload for external analysis.

Which command should the LTM Specialist execute on the LTM device command line interface?

- A. tcpdump -vvv -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- B. tcpdump -vvv -s 0 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- C. tcpdump -vvv -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- D. tcpdump -vvv -s 0 -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

An LTM Specialist has just captured trace /var/tmp/trace.cap for site www.example.com while listening on virtual address 10.0.0.1:443 configured on partition ApplicationA. The data payload being captured is SSL encrypted.

Which command should the LTM Specialist execute to decrypt the data payload?

- A. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_d/Common:www.example.com.crt_1
- B. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1
- C. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_d/ApplicationA:www.example.com.crt_1
- D. ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_key_d/ApplicationA:www.example.com.key_1

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

An LTM Specialist must perform a packet capture on a virtual server with an applied standard FastL4 profile. The virtual server 10.0.0.1:443 resides on vlan301.

Which steps should the LTM Specialist take to capture the data payload successfully while ensuring no other virtual servers are affected?

- A. The standard FastL4 profile should have PVA acceleration disabled. Then the packet capture `tcpdump -ni vlan301` should be executed on the command line interface.
- B. The packet capture `tcpdump -ni vlan301` should be executed on the command line interface. There is no need to change profiles or PVA acceleration.
- C. A new FastL4 profile should be created and applied to the virtual server with PVA acceleration disabled. Then the packet capture `tcpdump -ni vlan301` should be executed on the command line interface.
- D. The LTM device is under light load. The traffic should be mirrored to a dedicated sniffing device. On the sniffing device, the packet capture `tcpdump -ni vlan301` should be executed.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

A new VLAN vlan301 has been configured on a highly available LTM device in partition ApplicationA. A new directly connected backend server has been placed on vlan301. However, there are connectivity issues pinging the default gateway. The VLAN self IPs configured on the LTM devices are 192.168.0.251 and 192.168.0.252 with floating IP 192.168.0.253. The LTM Specialist needs to perform a packet capture to assist with troubleshooting the connectivity.

Which command should the LTM Specialist execute on the LTM device command line interface to capture the attempted pings to the LTM device default gateway on VLAN vlan301?

- A. `tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.253'`
- B. `tcpdump -ni vlan301 'host 192.168.0.253'`
- C. `tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.251 or host 192.168.0.252'`
- D. `tcpdump -ni vlan301 'host 192.168.0.251 or host 192.168.0.252'`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 30**

An LTM device pool has suddenly been marked down by a monitor. The pool consists of members 10.0.1.1:443 and 10.0.1.2:443 and are verified to be listening. The affected virtual server is 10.0.0.1:80.

Which two tools should the LTM Specialist use to troubleshoot the associated HTTPS pool monitor via the command line interface? (Choose two.)

- A. curl
- B. telnet
- C. ssldump
- D. tcpdump

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:**QUESTION 31**

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

An application is configured on an LTM device:

Virtual server: 10.0.0.1:80 (VLAN vlan301)

SNAT IP: 10.0.0.1

Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)

Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only client traffic specifically for this virtual server?

- A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
- B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
- C. tcpdump -ni vlan301 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
- D. tcpdump -ni vlan302 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
- E. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

An LTM Specialist is running the following packet capture on an LTM device:

```
ssldump -Aed -ni vlan301 'port 443'
```

Which two SSL record message details will the ssldump utility display by default? (Choose two.)

- A. HTTP Version
- B. User-Agent
- C. ClientHello
- D. ServerHello
- E. Issuer

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:**QUESTION 34**

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

Section: (none)

Explanation

Explanation/Reference:**QUESTION 35**

An LTM Specialist is troubleshooting virtual server 10.0.0.1:443 residing on VLAN vlan301. The web application is accessed via www.example.com. The LTM Specialist wants to save a packet capture with complete decrypted payload for external analysis.

Which command should the LTM Specialist execute on the LTM device command line interface?

- A. tcpdump -vvv -s 0 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap
- B. tcpdump -vvv -s 0 -ni vlan301 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap

- C. ssldump -Aed -k
/config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1 >
/var/tmp/trace.cap
- D. ssldump -Aed -ni vlan301 -k
/config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1 >
/var/tmp/trace.cap

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

An application is configured on an LTM device:

Virtual server: 10.0.0.1:80 (VLAN vlan301)

SNAT IP: 10.0.0.1

Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)

Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only server traffic specifically for this application?

- A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
- B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
- C. tcpdump -ni vlan302 -s 0 'port 8080 and (host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap
- D. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

An LTM Specialist sees these entries in /var/log/ltm:

Oct 25 03:34:31 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443

Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443

Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443

Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) abortedD. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) abortedD. 172.16.20.1:443
Oct 25 03:34:33 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) abortedD. 172.16.20.1:443

Assume 172.16.20.0/24 is attached to the VLAN "internal."

What should the LTM Specialist use to troubleshoot this issue?

- A. curl -d - -k https://172.16.20.1
- B. ssldump -i internal host 172.16.20.1
- C. tcpdump -i internal host 172.16.20.1 > /shared/ssl.pcap ssldump < /shared/ssl.pcap
- D. tcpdump -s 64 -i internal -w /shared/ssl.pcap host 172.16.20.1 ssldump -r /shared/ssl.pcap

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:

```
when HTTP_REQUEST {  
  switch [HTTP::uri] {  
    "/WS1/ws.jsp" {  
      log local0. "[HTTP::uri]-Redirected to JSP Pool"  
      pool JSP  
    }  
    default { log local0. "[HTTP::uri]-Redirected to Non-JSP Pool"  
      pool NonJSP  
    }  
  }  
}
```

However, the iRule is NOT behaving as expected. Below is a snapshot of the log:

```
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/WS.jsp-Redirected to Non-JSP Pool
```

/ws1/WS.jsp-Redirected to Non-JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/ws1/ws.jsp-Redirected to Non-JSP Pool

What is the problem?

- A. The condition in the iRule is case sensitive.
- B. The 'switch' command in the iRule has been used incorrectly.
- C. The pool members of both pools need to be set up as case-insensitive members.
- D. The "Process Case-Insensitivity" option for the virtual server needs to be selected.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An LTM Specialist is tasked with ensuring that the syslogs for the LTM device are sent to a remote syslog server. The following is an extract from the config file detailing the node and monitor that the LTM device is using for the remote syslog server:

```
monitor
Syslog_15002 {
defaults from udp
dest *:15002
}

node 91.223.45.231 {
monitor Syslog_15002
screen RemoteSYSLOG
}
```

There seem to be problems communicating with the remote syslog server. However, the pool monitor shows that the remote server is up. The network department has confirmed that there are no firewall rules or networking issues preventing the LTM device from communicating with the syslog server. The department responsible for the remote syslog server indicates that there may be problems with the syslog server. The LTM Specialist checks the BIG-IP LTM logs for errors relating to the remote syslog server. None are found. The LTM Specialist does a tcpdump:

tcpdump -nn port 15002, with the following results:
21:28:36.395543 IP 192.168.100.100.44772 > 91.223.45.231.15002: UDP, length 19
21:28:36.429073 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169

21:28:36.430714 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181
21:28:36.840524 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169
21:28:36.846547 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181
21:28:39.886343 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 144

NotE. 192.168.100.100 is the self IP of the LTM device.

Why are there no errors for the remote syslog server in the log files?

- A. The -log option for tcpdump needs to be used.
- B. The monitor type used is inappropriate.
- C. The "verbose" logging option needs to be enabled for the pool.
- D. When the remote syslog sever fails, it returns to service before the timeout for the monitor has expired.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

Given a tcpdump on an LTM device from both sides of a connection on the External and Internal VLANs, how should an LTM Specialist determine if SNAT is enabled for a particular pool?

- A. by checking to see if the Source IP is carried through from the External Vlan to the Internal Vlan
- B. by checking to see if the Destination port is carried through from the External Vlan to the Internal Vlan
- C. by checking to see if the Source port is carried through from the External Vlan to the Internal Vlan
- D. by checking to see if the Destination IP is carried through from the External Vlan to the Internal Vlan

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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-Connection: 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:

```
when HTTP_REQUEST {  
  switch [HTTP::uri] {  
    "/ws1/ws.jsp" {  
      log local0. "[HTTP::uri]-Redirected to JSP Pool"    }  
  }  
}
```

```
pool JSP
}
default { log local0. "[HTTP::uri]-Redirected to Non-JSP Pool"
pool NonJSP

}
}
```

However, the iRule is NOT behaving as expected. Below is a snapshot of the log:

```
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/WS1/WS.jsp-Redirected to Non-JSP Pool
/ws1/WS.jsp-Redirected to Non-JSP Pool
/WS1/ws.jsp-Redirected to JSP Pool
/ws1/ws.jsp-Redirected to Non-JSP Pool
```

What should the LTM Specialist do to resolve this?

- A. Use the following switch -lc [HTTP::uri]
- B. Use the following switch [string tolower [HTTP::uri]]
- C. Set the "Case Sensitivity" option of each member to "None".
- D. Select the "Process Case-Insensitivity" option for the virtual server.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

An LTM device has a virtual server configured as a Performance Layer 4 virtual listening on 0.0.0.0:0 to perform routing of packets to an upstream router. The client machine at IP address 192.168.0.4 is attempting to contact a host upstream of the LTM device on IP address 10.0.0.99.

The network flow is asymmetrical, and the following TCP capture displays:

```
# tcpdump -nnni 0.0 'host 192.168.0.4 and host 10.0.0.99'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
05:07:55.499954 IP 192.168.0.4.35345 > 10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480
05:07:55.499983 IP 10.0.0.99.443 > 192.168.0.4.35345: R 1:1(0) ack 1 win 0
```

05:07:56.499960 IP 192.168.0.4.35345 > 10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480
05:07:56.499990 IP 10.0.0.99.443 > 192.168.0.4.35345: R 1:1(0) ack 1 win 0 4 packets captured

Which option within the fastL4 profile needs to be enabled by the LTM Specialist to prevent the LTM device from rejecting the flow?

- A. Loose Close
- B. Loose Initiation
- C. Reset on Timeout
- D. Generate Initial Sequence Number

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

An LTM Specialist has configured a virtual server for www.example.com, load balancing connections to a pool of application servers that provide a shopping cart application. Cookie persistence is enabled on the virtual server. Users are able to connect to the application, but the user's shopping cart fails to update. A traffic capture shows the following:

Request:

GET /cart/updatecart.php HTTP/1.1

Host: www.example.com

Connection: keep-alive

Cache-Control: max-age=0

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Cookie: BIGipServerwebstore_pool=353636524.20480.0000

Response:

HTTP/1.1 200 OK

Date: Wed, 24 Oct 2012 18:00:13 GMT

Server: Apache/2.2.22 (Ubuntu)

X-Powered-By: PHP/5.3.10-1ubuntu3.1

Set-Cookie: cartID=647A5EA6657828C69DB8188981CB5; path=/;

domain=wb01.example.com

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

No changes can be made to the application.

What should the LTM Specialist do to resolve the problem?

- A. Use an iRule to rewrite the cartID cookie domain.
- B. Create a universal persistence profile on the cartID cookie.
- C. Enable source address persistence as a fallback persistence method.
- D. Create a cookie persistence profile with "match across services" enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

An LTM Specialist has been asked to configure a virtual server to distribute connections between a pool of two application servers with addresses 172.16.20.1 and 172.16.20.2. The application servers are listening on TCP ports 80 and 443. The application administrators have asked that clients be directed to the same node for both HTTP and HTTPS requests within the same session.

Virtual servers vs_http and vs_https have been created, listening on 1.2.3.100:80 and 1.2.3.100:443, respectively. Which configuration option will result in the desired behavior?

- A. Create pool app_pool with members 172.16.20.1:any and 172.16.20.2:any
Assign app_pool as the default pool for both vs_http and vs_https
Disable port translation for vs_http and vs_https
- B. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80
Assign pool http_pool as the default pool for both vs_https and vs_https
Disable port translation for vs_https
Create an SSL persistence profile with "match across virtual servers" enabled
Assign the persistence profile to vs_http.
- C. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80
Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443
Assign http_pool as the default pool for vs_http
Assign https_pool as the default pool for vs_https
Create a source address persistence profile with "match across services" enabled
Assign the persistence profile to vs_http and vs_https
- D. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80
Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443

Assign http_pool as the default pool for vs_http
Assign https_pool as the default pool for vs_https
Create an SSL persistence profile with "match across virtual servers" enabled
Assign the persistence profile to vs_http

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

An LTM Specialist is investigating reports from users that SSH connections are being terminated unexpectedly. SSH connections are load balanced through a virtual server. The users experiencing this problem are running SQL queries that take upwards of 15 minutes to return with no screen output. The virtual server is standard with a pool associated and no other customizations.

What is causing the SSH connections to terminate?

- A. UDP IP ToS
- B. TCP idle timeout
- C. The virtual server has no persistence.
- D. The pool has Reselect Retries set to 0.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

Users in a branch office are reporting a website is always slow. No other users are experiencing the problem. The LTM Specialist tests the website from the external VLAN along with testing the servers directly. All tests indicate normal behavior. The environment is a single HTTP virtual server on the external VLAN with a single pool containing three HTTP pool members on the internal VLAN.

Which two locations are most appropriate to collect additional protocol analyzer data? (Choose two.)

- A. a user's machine
- B. the switch local to the user
- C. the LTM device's internal VLAN

- D. the LTM device's external VLAN
- E. a user's Active Directory authentication

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

An LTM Specialist has a single HTTPS virtual server doing SSL termination. No server SSL profile is defined. The pool members are on the internal VLAN answering on HTTP port 80. Users with certain browsers are experiencing issues.

Which two locations are most appropriate to gather packets needed to determine the SSL issue? (Choose two.)

- A. server interface
- B. user's computer
- C. LTM device's external VLAN
- D. LTM device's internal VLAN
- E. LTM device's management interface

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

A user is having issues with connectivity to an HTTPS virtual server. The virtual server is on the LTM device's external vlan, and the pools associated with the virtual server are on the internal vlan. An LTM Specialist does a tcpdump on the external interface and notices that the host header is incomplete.

In which location should the LTM Specialist put a traffic analyzer to gather the most pertinent data?

- A. server
- B. external VLAN
- C. internal VLAN
- D. client machine

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

An application owner claims an LTM device is delaying delivery of an HTTP application. The LTM device has two VLANs, an internal and an external. The application servers reside on the internal VLAN. The virtual server and clients reside on the external VLAN.

With appropriate filters applied, which solution is most efficient for obtaining packet captures in order to investigate the claim of delayed delivery?

- A. one capture on interface 0.0
- B. one capture on the internal interface
- C. one capture on the external interface
- D. one capture on the management interface

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

A client (10.10.1.30) connecting to an HTTPS virtual server (10.10.1.100) with a clientssl profile is getting an SSL error.

Which options will trace this issue?

- A. `tcpdump -i external -X -e -nn -vvv -w /shared/ssl_problem.cap port 443 and host 10.10.1.30`
`ssldump -r /shared/ssl_problem.cap -n -x`
- B. `tcpdump -i external -s 0 -w /shared/ssl_problem.cap port 443 and host 10.10.10.30 and host 10.10.1.100`
`ssldump -r /shared/ssl_problem.cap -n -x`
- C. `tcpdump -i external -X -s 0 -vvv src host 10.10.10.30 and dst host 10.10.1.100 and port 443`
`> /shared/ssl_problem.cap`
`ssldump -r /shared/ssl_problem.cap -n -x`
- D. `tcpdump -i external -X -e -nn -vv port 443 and host 10.10.1.100 and host 10.10.1.30 > /shared/ssl_problem.cap`

```
ssldump -n -x < /shared/ssl_problem.cap
```

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

An LTM device is deployed in a one-armed topology. The virtual server, clients, and web servers are connected on the LTM device internal VLAN. A client tries to connect to the virtual server and is unable to establish a connection. A packet capture from the LTM device internal VLAN shows that the HTTP request is being forwarded to the web server.

From which two additional locations should protocol analyzer data be collected? (Choose two.)

- A. network interface of web server
- B. network interface of client machine
- C. internal VLAN interface of LTM device
- D. external VLAN interface of LTM device
- E. any network interface of the Internet firewall

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

An LTM Specialist configures a new HTTP virtual server on an LTM device external VLAN. The web servers are connected to the LTM device internal VLAN. Clients trying to connect to the virtual server are unable to establish a connection. A packet capture shows an HTTP response from a web server to the client and then a reset from the client to the web server.

From which two locations could the packet capture have been collected? (Choose two.)

- A. network interface of web server
- B. network interface of client machine
- C. internal VLAN interface of the LTM device
- D. external VLAN interface of the LTM device

E. management VLAN interface of the LTM device

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

The LTM Specialist is writing a custom HTTP monitor for a web application and has viewed the content by accessing the site directly via their browser. The monitor continually fails. The monitor configuration is:

```
ltm monitor http /Common/exampleComMonitor {
defaults-from /Common/http
destination *:*
interval 5
recv "Recent Searches"
send "GET /app/feed/current?uid=20145 HTTP/1.1\r\nHost:
www.example.com\r\nAccept-Encoding: gzip, deflate\r\nConnection: close\r\n\r\n" time-until-up 0
timeout 16
}
```

A trace shows the following request and response:

Request:

```
GET /app/feed/current?uid=20145 HTTP/1.1
Host www.example.com
Accept-Encoding gzip, deflate
Connection: close
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Date Wed, 17 Oct 2012 18:45:52 GMT
Server Apache
Location https://example.com/login.jsp
Content-Encoding gzip
Content-Type text/html; charset=UTF-8
Set-Cookie: JSESSIONID=261EFFBDA8EC3036FBCC22D991AC6835; Path=/app/feed/current?uid=20145
What is the problem?
```

- A. The request does NOT include a User-Agent header.
- B. The HTTP monitor does NOT support monitoring jsp pages.

- C. The request does NOT include any cookies and the application is expecting a session cookie.
- D. The request includes an Accept-Encoding so the server is responding with a gzipped result and LTM monitors CANNOT handle gzipped responses.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

An LTM Specialist configures an HTTP monitor as follows:

```
ltm monitor http stats_http_monitor {  
    defaults-from http  
    destination *.*  
    interval 5  
    recv "Health check: OK"  
    send "GET /stats/stats.html HTTP/1.1\r\nHost: www.example.com\r\nAccept-EncodinG. gzip, deflate\r\n\r\nConnection: close\r\n\r\n\r\n"  
    time-until-up 0  
    timeout 16  
}
```

The monitor is marking all nodes as down. A trace of the HTTP conversation shows the following:

```
GET /stats/stats.html HTTP/1.1  
Host: www.example.com  
Accept-EncodinG. gzip, deflate  
Connection: close
```

```
HTTP/1.1 401 Authorization Required  
DatE. Tue, 23 Oct 2012 19:38:56 GMT  
Server: Apache/2.2.15 (Unix)  
WWW-AuthenticatE. Basic realm="Please enter your credentials" Content-LengtH. 480  
Connection: close  
Content-TypE. text/html; charset=iso-8859-1  
Which action will resolve the problem?
```

- A. Add an NTLM profile to the virtual server.
- B. Add a valid username and password to the monitor.
- C. Use an HTTPS monitor with a valid certificate instead.
- D. Add a backslash before the colon in the receive string.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

The following decoded TCPDump capture shows the trace of a failing health monitor.

```
00:00:13.245104 IP 10.29.29.60.51947 > 10.0.0.12.http: P 1:59(58) ack 1 win 46 <nop,nop,timestamp 2494782300 238063789> out slot1/tmm3 lis=
0x0000: 4500 006e 3b19 4000 4006 ce0c 0a1d 1d3c      E..n;.@.@.....<
0x0010: 0a00 000c caeb 0050 8be5 aca3 dd65 e3e1      .....P.....e..
0x0020: 8018 002e 1b41 0000 0101 080a 94b3 5b5c      .....A.....[\
0x0030: 0e30 90ad 4745 5420 2f74 6573 745f 7061      .O..GET./test_pa
0x0040: 6765 2e68 746d 6c20 4854 5450 312e 310d      ge.html.HTTP1.1.
0x0050: 0a48 6f73 743a 200d 0a43 6f6e 6e65 6374      .Host:...Connect
0x0060: 696f 6e3a 2043 6c6f 7365 0d0a 0d0a 0105      ion:..Close.....
0x0070: 0100 0003 00                .....
00:00:13.245284 IP 10.0.0.12.http > 10.29.29.60.51947: . ack 59 win 362 <nop,nop,timestamp 238063789 2494782300> in slot1/tmm3 lis=
0x0000 0ffd 0800 4500 00c9 6f68 4000 8006 755d      ....E...oh@...u]
0x0010 0a29 0015 0a29 0103 0050 e0d6 4929 90eb      .)...)...P..l)..
0x0020 6f12 d83c 8019 fab3 9b31 0000 0101 080a      o..<.....1.....
0x0030 0068 4e10 5240 6150 4854 5450 2f31 2e31      .hN.R@aPHTTP/1.1
0x0040 2034 3030 2042 6164 2052 6571 7565 7374      .400.Bad.Request
0x0050 0d0a 436f 6e74 656e 742d 5479 7065 3a20      ..Content-Type:.
0x0060 7465 7874 2f68 746d 6c0d 0a44 6174 653a      text/html..Date:
0x0070 2054 6875 2c20 3231 204a 616e 2032 3031      .Mon,.01.Jan.201
0x0080 3020 3138 3a35 383a 3537 2047 4d54 0d0a      2.00:00:01.GMT..
0x0090 436f 6e6e 6563 7469 6f6e 3a20 636c 6f73      Connection:.clos
0x00a0 650d 0a43 6f6e 7465 6e74 2d4c 656e 6774      e..Content-Lengt
0x00b0 683a 2032 300d 0a0d 0a3c 6831 3e42 6164      h:..20....<h1>Bad
0x00c0 2052 6571 7565 7374 3c2f 6831 3e          .Request</h1>
```

The health monitor is sending the string shown in the capture; however, the server response is NOT as expected. The correct response should be an HTML page including the string 'SERVER IS UP'.

What is the issue?

- A. The /test_page.html does NOT exist on the web server.
- B. Incorrect syntax in send string. 'HTTP1.1' should be 'HTTP/1.1'.
- C. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.

D. The wrong HTTP version is specified in the send string. Version 1.2 should be used instead of version 1.1.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

An LTM device is monitoring pool members on port 80. The LTM device is using an HTTP monitor with a send string of GET / and a blank receive string.

What would cause the pool members to be marked down?

- A. A pool member responds with an HTTP 200 series response code.
- B. A pool member responds with an HTTP 300 series response code.
- C. A pool member responds with an HTTP 400 series response code.
- D. A pool member responds with an HTTP 500 series response code.
- E. A pool member does NOT acknowledge the connection SYN on port 80.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

An LTM device is monitoring three pool members. One pool member is being marked down.

What should the LTM Specialist enable to prevent the server from being flooded with connections once its monitor determines it is up?

- A. manual resume
- B. packet shaping
- C. hold down timer
- D. slow ramp timer
- E. fastest load balance algorithm

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:****QUESTION 59**

An LTM device is serving an FTP virtual server that has three pool members. The FTP pool members are monitored via TCP port 21. Customers are reporting that they are able to log in, but are sometimes unable to upload files to the server.

Which monitor should the LTM Specialist configure to verify that the servers can handle file uploads?

- A. FTP
- B. Inband
- C. External
- D. Scripted
- E. Real Server

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:****QUESTION 60**

An LTM HTTP pool has an associated monitor that sends a string equal to 'GET /test.html'.

Which two configurations could an LTM Specialist implement to allow server administrators to disable their pool member servers without logging into the LTM device? (Choose two.)

- A. Set monitor to transparent and ask the server team to set string `TRANSPARENT' in test.html.
- B. Set `receive string' equal to 'SERVER UP' and ask the server team to set string `SERVER DOWN' in test.html.
- C. Set `alias' equal to 'SERVER DOWN' and ask the server team to set string `SERVER DOWN' in test.html.
- D. Set `receive disable string' equal to 'SERVER DOWN' and ask the server team to set string `SERVER DOWN' in test.html.
- E. Set `disable pool member' equal to 'SERVER UP' and ask the server team to set string `SERVER DOWN' in test.html.

Correct Answer: BD

Section: (none)

Explanation**Explanation/Reference:**

QUESTION 61

An LTM Specialist is receiving reports from customers about multiple applications failing to work properly. The LTM Specialist looks at the services running and notices that the bigd process has NOT started.

How are monitored LTM device objects marked when the bigd process is stopped?

- A. red or offline
- B. blue or unchecked
- C. green or available
- D. unchanged until bigd is restarted

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

An LTM Specialist is setting up a monitor for an HTTP 1.1 server. The response to a GET / is:

HTTP/1.1 302 Moved Temporarily

Location: http://www.example.com/new/location.html

Which send string settings should the LTM Specialist use to force a proper response?

- A. GET / HTTP/1.0\r\nHost: host.domain.com\r\nConnection: Close\r\n\r\n
- B. GET /new/location.html HTTP/1.1\r\nHost: www.example.com\r\nConnection: Close\r\n\r\n
- C. GET / HTTP/1.1\r\nHost: www.example.com/new/location.html\r\nConnection: Close\r\n\r\n
- D. GET /new/location.html HTTP/1.1\r\nHost: host.domain.com/new/locations.html\r\nConnection: Close\r\n\r\n

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

An LTM Specialist defines a receive string in the HTTP monitor and then assigns it to the HTTP pool. The monitor has an interval of 5 seconds and a timeout of 16 seconds.

If the receive string is NOT seen in the the HTTP payload after 20 seconds, how does the LTM device mark the monitor status?

- A. offline
- B. unknown
- C. available
- D. unavailable
- E. forced offline

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

An LTM Specialist receives a request to monitor the network path through a member, but NOT the member itself.

Which monitor option should the LTM Specialist enable or configure?

- A. Reverse
- B. Up interval
- C. Transparent
- D. Alias address
- E. Time until up

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

An LTM Specialist is creating a custom EAV monitor.

In which directory should the LTM Specialist upload the script?

- A. /usr/monitor
- B. /usr/monitors
- C. /config/monitors
- D. /usr/bin/monitors
- E. /config/templates

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

An FTP monitor is NOT working correctly.

Which three pieces of information does the LTM Specialist need to provide to ensure a properly working FTP monitor? (Choose three.)

- A. alias
- B. File path
- C. username
- D. password
- E. FTP server port
- F. FTP server IP address

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

Which iRule statement demotes a virtual server from CMP?

- A. set ::foo 123
- B. set static::foo 123
- C. persist source_addr 1800

D. [class match \$HTTP_CONTENT contains my_data_class]

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

What is the effect of an iRule error such as referencing an undefined variable?

- A. The iRule execution will continue with the next statement.
- B. The execution of the current event within the iRule will be terminated.
- C. The iRule execution will be terminated, and both the client and server side connections will be reset.
- D. The connection will continue, but the iRule will NOT be executed again for the lifetime of the connection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

What does the following iRule do?

```
when CLIENT_ACCEPTED {  
  if { [matchclass [IP::client_addr] equals WebClient1-Whitelist1] }{  
    #log local0. "Valid client IP: [IP::client_addr] - forwarding traffic"  
    #Pool WebClient1  
  
  } else {  
    log local0. "Invalid client IP: [IP::client_addr] - discarding"  
    discard  
  }  
}
```

- A. The iRule compares a client IP to a list. If the client IP is on the list, discard and log the discard.
- B. The iRule compares a client IP to a list. If the client IP is NOT on the list, discard and log the discard.
- C. The iRule compares a client IP to a list. If the client IP is on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.

D. The iRule compares a client IP to a list. If the client IP is NOT on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the client.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

What do the following iRule commands do when they are used in the same iRule?

```
set hsl [HSL::open -proto UDP -pool syslog_server_pool]
```

```
HSL::send $hsl "<190> [HTTP::host] from [whereis [IP::client_addr] country continent state city zip] , IP: [IP::client_addr]"
```

- A. The commands set up a high-speed logging connection and then send the geographical database to the server.
- B. The commands set up a high-speed logging connection and then send the host header and client geographical detail to the connection.
- C. The commands set up a high-speed logging connection and then send the host header, HTTP payload, and client geographical detail to the connection.
- D. The commands set up a high-speed logging connection to the LTM device and then send the host header and client geographical detail to the connection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

An LTM Specialist configures the following iRule on an LTM device:

```
when HTTP_REQUEST {  
    if {[string tolower [HTTP::uri]] contains "/URI1/" } {  
        pool Pool1  
    }  
    elseif {[string tolower [HTTP::uri]] contains "/URI2/" } {  
        pool Pool2  
    }  
    elseif {[string tolower [HTTP::uri]] contains "/URI3/" } {  
        pool Pool3  
    }  
}
```

```
else { pool Pool4}  
}
```

Given the following request: `http://www.example.comURI1/index.html?fu=bar&pass=1234`

Which pool will be selected by the iRule?

- A. Pool1
- B. Pool2
- C. Pool3
- D. Pool4

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Given the iRule:

```
when HTTP_REQUEST {  
  if {[HTTP::username] ne ""} and ([HTTP::password] ne "") {  
    log local0. "client ip [IP::remote_addr] credentials provided [HTTP::username] [HTTP::password]"  
  }  
  else {  
    pool old_application_pool  
  }  
}
```

The associated virtual server has a default pool named `new_application_pool`.

Which functionality does the iRule provide?

- A. Allows clients with credentials to access the `old_application_pool` and logs the access of clients without credentials to the `new_application_pool`.
- B. Allows clients without credentials to access the `old_application_pool` and logs the access of clients with credentials to the `new_application_pool`.
- C. Allows clients with credentials to access the `old_application_pool` and logs the attempted access of clients with credentials to the `new_application_pool`.
- D. Allows clients without credentials to access the `old_application_pool` and logs the attempted access of clients without credentials to the `new_application_pool`.

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:****QUESTION 73**

Which three HTTP headers allow an application server to determine the client's language compatibility, browser, operating system type, and compression compatibility? (Choose three.)

- A. Accept
- B. Accept-Encoding
- C. Accept-Language
- D. Host
- E. User-Agent

Correct Answer: BCE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 74**

A web application requires the client to provide the destination server and service identification.

Which HTTP header will supply this information?

- A. Host
- B. From
- C. Expect
- D. Connection

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 75**

A web application is meant to log the URI of the resource that responded to the client's initial Request-URI.

Which HTTP header will supply this information?

- A. Via
- B. Server
- C. Trailer
- D. Referer

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

The end users of a web application need to verify that their browsers received the complete message-body from the web server.

Which HTTP header will accomplish this?

- A. Range
- B. Expect
- C. Accept-Ranges
- D. Content-Length

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

An HTTP 1.1 application utilizes chunking.

Which header should be used to notify the client's browser that there are additional HTTP headers at the end of the message?

- A. ETag
- B. From
- C. Trailer

D. Expect

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

A web application sends information about message integrity and content life time to the client.

Which two HTTP headers should be used in sending the client information? (Choose two.)

- A. ETag
- B. Expect
- C. Expires
- D. Content-MD5
- E. Content-Range
- F. Content-Length

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

A web developer has created a custom HTTP call to a backend application. The HTTP headers being sent by the HTTP call are:

GET / HTTP/1.1
User-Agent: MyCustomApp (v1.0)
Accept: text/html
Cache-Control: no-cache
Connection: keep-alive
Cookie: somecookie=1

The backend server is responding with the following:

HTTP/1.1 400 Bad Request
Date: Wed, 20 Jul 2012 17:22:41 GMT

Connection: close

Why is the HTTP web server responding with a HTTP 400 Bad Request?

- A. The client request does NOT include a Host header.
- B. The User-Agent header contains an invalid character.
- C. The web server is NOT expecting a keep-alive connection.
- D. The web server is configured to accept HTTP 1.0 requests only.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

A client is attempting to log in to a web application that requires authentication. The following HTTP headers are sent by the client:

```
GET /owa/ HTTP/1.1
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
User-Agent: curl/7.26.0
Host: 10.0.0.14
Accept: */*
Accept-Encoding: gzip, deflate
```

The web server is responding with the following HTTP headers:

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html
Server: Microsoft-IIS/7.5
WWW-Authenticate: NTLM
Date: Wed, 16 Aug 1977 19:12:31 GMT
Content-Length: 1293
```

The client has checked the login credentials and believes the correct details are being entered.

What is the reason the destination web server is sending an HTTP 401 response?

- A. The username and password are incorrect.
- B. The server has an incorrect date configured.
- C. The client is using the wrong type of browser.

D. The wrong authentication mechanism is being used.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

The LTM device is configured to provide load balancing to a set of web servers that implement access control lists (ACL) based on the source IP address of the client. The ACL is at the network level and the web server is configured to send a TCP reset back to the client if it is NOT permitted to connect.

The virtual server is configured with the default OneConnect profile.

The ACL is defined on the web server as:

Permit: 192.168.136.0/24

Deny: 192.168.116.0/24

The packet capture is taken of two individual client flows to a virtual server with IP address 192.168.136.100.

Client A - Src IP 192.168.136.1 - Virtual Server 192.168.136.100:

Clientside:

09:35:11.073623 IP 192.168.136.1.55684 > 192.168.136.100.80: S 869998901:869998901(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>

09:35:11.073931 IP 192.168.136.100.80 > 192.168.136.1.55684: S 2273668949:2273668949(0) ack 869998902 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

09:35:11.074928 IP 192.168.136.1.55684 > 192.168.136.100.80: . ack 1 win 16425

09:35:11.080936 IP 192.168.136.1.55684 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425

09:35:11.081029 IP 192.168.136.100.80 > 192.168.136.1.55684: . ack 299 win 4678

Serverside:

09:35:11.081022 IP 192.168.136.1.55684 > 192.168.116.128.80: S 685865802:685865802(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

09:35:11.081928 IP 192.168.116.128.80 > 192.168.136.1.55684: S 4193259095:4193259095(0) ack 685865803 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 6>

09:35:11.081943 IP 192.168.136.1.55684 > 192.168.116.128.80: . ack 1 win 4380

09:35:11.081955 IP 192.168.136.1.55684 > 192.168.116.128.80: P 1:299(298) ack 1 win 4380

09:35:11.083765 IP 192.168.116.128.80 > 192.168.136.1.55684: . ack 299 win 108

Client B - Src IP 192.168.116.1 - Virtual Server 192.168.136.100:

Clientside:

```
09:36:11.244040 IP 192.168.116.1.55769 > 192.168.136.100.80: S 3320618938:3320618938(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
09:36:11.244152 IP 192.168.136.100.80 > 192.168.116.1.55769: S 3878120666:3878120666(0) ack 3320618939 win 4380 <mss 1460,nop,wscale
0,sackOK,eol>
09:36:11.244839 IP 192.168.116.1.55769 > 192.168.136.100.80: . ack 1 win 16425
09:36:11.245830 IP 192.168.116.1.55769 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:36:11.245922 IP 192.168.136.100.80 > 192.168.116.1.55769: . ack 299 win 4678
```

Serverside:

```
09:36:11.245940 IP 192.168.136.1.55684 > 192.168.116.128.80: P 599:897(298) ack 4525 win 8904
09:36:11.247847 IP 192.168.116.128.80 > 192.168.136.1.55684: P 4525:5001(476) ack 897 win 142
```

Why was the second client flow permitted by the web server?

- A. A global SNAT is defined.
- B. SNAT automap was enabled on the virtual server.
- C. The idle TCP session from the first client was re-used.
- D. A source address persistence profile is assigned to the virtual server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

An LTM Specialist is troubleshooting an HTTP monitor. The pool member is accessible directly through a browser, but the HTTP monitor is marking the pool member as down.

GET / HTTP/1.1

```
HTTP/1.1 400 Bad Request
Date: Tue, 23 Oct 2012 21:39:07 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4
mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Which issue is the pool member having?

- A. The pool member has too many concurrent connections.
- B. The pool member is rejecting the request because it is invalid.
- C. The pool member lacks the object requested by the monitor.
- D. The pool member is NOT accepting requests from the LTM device IP address.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "Unable to connect" in the browser, although connections directly to the pool member show the application is functioning correctly. The LTM device configuration is:

```
ltm virtual /Common/vs_https {  
  destination /Common/10.10.1.110:443  
  ip-protocol udp  
  mask 255.255.255.255  
  pool /Common/pool_https  
  profiles {  
    /Common/udp { }  
  }  
  translate-address enabled  
  translate-port enabled  
  vlans-disabled  
}
```

```
ltm pool /Common/pool_https {  
  members {  
    /Common/172.16.20.1:443 {  
      address 172.16.20.1  
    }  
  }  
}
```

What issue is the LTM Specialist experiencing?

- A. The virtual server is disabled on all VLANs.
- B. The pool member is marked down by a monitor.
- C. The pool member is marked down administratively.
- D. The virtual server is configured for the incorrect protocol.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the following HTTP request:

GET / HTTP/1.1

Host: www.example.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Cache-Control: no-cache

Connection: keep-alive

Cookie: somecookie=1

HTTP/1.1 200 OK

Server: Apache/2.2.15 (Unix)

Last-Modified: Wed, 12 Aug 2009 00:00:30 GMT

Accept-Ranges: bytes

Content-Length: 1063

X-Connection: close

Content-Type: text/html; charset=UTF-8

Vary: Accept-Encoding

Content-Encoding: gzip

Connection: Keep-Alive

Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched and therefore NOT modified.

Which header field is contributing to the issue?

- A. HTTP Method
- B. Cookie content

- C. User-Agent Value
- D. Accept-Encoding header

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the HTTP request below:

```
GET / HTTP/1.1
Host: www.f5.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Connection: keep-alive
Cookie: somecookie=1
```

Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched, and therefore NOT modified.

Which HTTP header should the LTM Specialist remove from the request to ensure the content can be matched and modified?

- A. Connection
- B. Accept
- C. Cache-Control
- D. Accept-Encoding

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

An LTM Specialist configured a virtual server to load balance a custom application. The application works when it is tested from within the firewall but it

fails when tested externally. The pool member address is 192.168.200.10:80. A capture from an external client shows:

```
GET /index.jsp HTTP/1.1
Host: 207.206.201.100
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:15.0) Gecko/20100101 Firefox/15.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: keep-alive
HTTP/1.1 302 Found
Date: Wed, 17 Oct 2012 23:09:55 GMT
Server: Apache/2.2.15 (CentOS)
Location: http://192.168.200.10/user/home.jsp
Content-Length: 304
Connection: close
```

What is the solution to this issue?

- A. Assign a SNAT pool to the virtual server.
- B. Add a Web Acceleration Profile to the virtual server.
- C. Configure redirect rewrite option in the HTTP profile.
- D. Configure a content filter on the backend web server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 87

There are three servers in the pool: 172.16.20.1, 172.16.20.2, and 172.16.20.3, with the virtual IP address 10.0.20.88.

A user CANNOT connect to an HTTP application. To understand the problem and find a solution, the LTM Specialist runs two concurrent traces on the LTM device, with the following results:

Trace on client side:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes

22:22:07.423759 IP 172.16.20.100.53875 > 10.0.20.88.80: S 998346084:998346084(0) win 5840 <mss 1460,sackOK,timestamp 67942058 0,nop,wscale 4>

22:22:07.424056 IP 10.0.20.88.80 > 172.16.20.100.53875: S 4671780:4671780(0) ack 998346085 win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2392362490 67942058,sackOK,eol>

22:22:07.424776 IP 172.16.20.100.53875 > 10.0.20.88.80: . ack 1 win 365 <nop,nop,timestamp 67942058 2392362490>

22:22:07.424790 IP 172.16.20.100.53875 > 10.0.20.88.80: P 1:149(148) ack 1 win 365 <nop,nop,timestamp 67942058 2392362490>

```
22:22:07.424891 IP 10.0.20.88.80 > 172.16.20.100.53875: . ack 149 win 4528 <nop,nop,timestamp 2392362491 67942058>  
22:22:12.024850 IP 10.0.20.88.80 > 172.16.20.100.53875: R 1:1(0) ack 149 win 4528
```

6 packets captured
6 packets received by filter
0 packets dropped by kernel

Trace on server side:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on internal, link-type EN10MB (Ethernet), capture size 96 bytes

```
22:22:07.424881 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp  
2392362491 0,sackOK,eol>
```

```
22:22:08.424893 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp  
2392363491 0,sackOK,eol>
```

```
22:22:09.625082 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp  
2392364691 0,sackOK,eol>
```

```
22:22:10.825194 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,sackOK,eol>
```

4 packets captured
4 packets received by filter
0 packets dropped by kernel

What should the LTM Specialist do to solve the problem?

- A. Edit the packet filter rules.
- B. Modify the monitor of the pool.
- C. Enable the virtual server.
- D. Configure the virtual server to use SNAT.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

An LTM Specialist is troubleshooting an HTTP monitor. The pool member is accessible directly through a browser, but the HTTP monitor is marking the pool member as down.

GET / HTTP/1.1

HTTP/1.1 400 Bad Request

Date: Tue, 23 Oct 2012 21:39:07 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4
mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

How should the LTM Specialist resolve this issue?

- A. Add '200 OK' to the monitor's receive string.
- B. Add 'Connection: close\r\n' to the monitor's send string.
- C. Change the interval on the monitor from 5 seconds to 30 seconds.
- D. Change the HTTP version in the send string from HTTP/1.1 to HTTP/1.0.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 89

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "The connection was reset" in the browser, although connections directly to the pool member show the application is functioning correctly.

```
ltm pool srv1_https_pool {  
  members {  
    192.168.2.1:https {  
      address 192.168.2.1  
    }  
  }  
}  
  
ltm virtual https_example_vs {  
  destination 192.168.1.155:https  
  ip-protocol tcp  
  mask 255.255.255.255  
  pool srv1_https_pool  
  profiles {  
    http { }  
    tcp { }  
  }  
  snat automap  
  vlans-disabled
```

```
}
```

How should the LTM Specialist resolve this issue?

- A. Enable HTTP monitoring on the pool.
- B. Add a ClientSSL profile to the virtual server.
- C. Disable SNAT Automap on the virtual server.
- D. Remove the HTTP profile from the virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 90

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "Unable to connect" in the browser, although connections directly to the pool member show the application is functioning correctly.

The LTM configuration is:

```
ltm virtual /Common/vs_https {  
  destination /Common/10.10.1.110:443  
  ip-protocol udp  
  mask 255.255.255.255  
  pool /Common/pool_https  
  profiles {  
    /Common/udp { }  
  }  
  translate-address enabled  
  translate-port enabled  
  vlans-disabled  
}
```

```
ltm pool /Common/pool_https {  
  members {  
    /Common/172.16.20.1:443 {  
      address 172.16.20.1  
    }  
  }  
}
```

How should the LTM Specialist resolve this issue?

- A. Remove an HTTP monitor from the pool.
- B. Add an HTTP profile to the virtual server.
- C. Enable the pool member on the correct VLAN.
- D. Select the correct protocol for the virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 91

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

What is the issue?

- A. The port 80 pool member is deleting the user's session cookie.
- B. The port 443 pool member is deleting the user's session cookie.
- C. The port 80 and port 443 connections are balanced to the same node.
- D. The port 80 and port 443 connections are balanced to different nodes.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

How should the LTM Specialist resolve this issue?

- A. Add an HTTP profile to both virtual servers.
- B. Enable SNAT Automap on both virtual servers.
- C. Create a custom persistence profile and enable "Map Proxies."
- D. Create a custom persistence profile and enable "Match Across Services."

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 93

An LTM device has been configured to log the reasons for generating TCP RST packets.

The following log entry occurs:

"01230140:3: RST sent from 192.168.1.100:80 to 192.168.1.124:39272, [0x112d82a:1721] {peer} TCP RST from remote system."

Which condition will trigger this log entry?

- A. A virtual server connection limit has been reached.
- B. The host at the other end terminated the TCP connection.
- C. The LTM device reset the connection because no pool members are available.
- D. The LTM device has reached the maximum number of allowed attempts to send the data segment to the affected TCP connection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

An LTM device supports two power supplies. The value of the BigDB key "platform.powersupplymonitor" is equal to enable.

Where would the error message be visible if one of the power supplies fails or is NOT plugged in?

- A. visible only via the console
- B. in the /var/log/ltm log file

- C. in the /var/log/kern.log file
- D. in the /var/log/tmm log file

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 95

An LTM Specialist loads a UCS file generated on a different LTM device and receives the following error message:

"mcpd[2395]: 01070608:0: License is not operational (expired or digital signature does not match contents)"

Which command should the LTM Specialist use to prevent the error?

- A. tmsh show /sys license
- B. tmsh show /sys hardware
- C. bigpipe config save /config.ucs
- D. tmsh load /sys /ucs rma <path/to/UCS>
- E. tmsh load /sys ucs <path/to/UCS> no-license

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

These log entries can have different root causes:

Jun 28 05:01:21 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: enabled
Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071431:5: Attempting to connect to CMI peer 1.1.1.2 port 6699
Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071432:5: CMI peer connection established to 1.1.1.2 port 6699
Jun 28 05:01:26 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: disabled, all peers are connected

Which two commands should be used to obtain additional information on these entries? (Choose two.)

- A. tmsh show /sys mcpd

- B. bigstart status mcpd
- C. tmsh modify /sys db log.mcpd.level value debug
- D. tmsh modify /sys db log.cmi.level value debug

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 97

An LTM Specialist wants to allow access to the Always On Management (AOM) from the network.

Which two methods should the LTM Specialist use to configure the AOM interface? (Choose two.)

- A. Configure the AOM IP from the front panel buttons and LCD.
- B. Choose the network configurator in the AOM menu on the serial port.
- C. Configure the AOM network address in the GUI under System>Platform.
- D. Log in to the Host via ssh, "ssh aom", and modify the network configuration file.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 99

An LTM Specialist with the Administrator role and terminal access of "tmsh" logs in via ssh and is in the Traffic Manager Shell. The LTM Specialist wants to enter the bash shell to review log files.

Which command does the LTM Specialist need to run to access the bash shell?

- A. exit
- B. quit
- C. run /cli bash
- D. run /util bash

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100

Which command will identify the active LTM device currently handling client traffic?

- A. b ha table show
- B. tmsh list /sys ha-status
- C. tmsh show /cm traffic-group
- D. tmsh run /sys failover standby
- E. tmsh show /sys ha-status all-properties

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

Which command should an LTM Specialist use on the command line interface to show the health of RAID array hard drives?

- A. tmsh show /sys raid disk
- B. tmsh show /ltm raid disk
- C. tmsh show /sys raid status
- D. tmsh show /ltm disk status

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

Which command line interface command will check if the BIG-IP platform contains a packet velocity ASIC (PVA)?

- A. bigpipe platform show | grep -i pva
- B. tmsh show /sys hardware pva status
- C. tmsh show /sys hardware | grep -i pva
- D. tmsh show /ltm hardware | grep -i pva

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

Which two subsystems could the LTM Specialist utilize to access an LTM device with lost management interface connectivity? (Choose two.)

- A. AOM
- B. ILO
- C. SCCP

D. ALOM

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 104

A BIG-IP Operator has made a grave error and deleted a few virtual servers on the active LTM device fronting the web browsing proxies. The BIG-IP Operator has NOT yet performed a configuration sync.

Which command should the LTM Specialist execute on the active LTM device to force a failover to the standby node and restore web browsing?

- A. tmsh /sys failover standby
- B. tmsh run /sys failover standby
- C. tmsh /sys failover status standby
- D. tmsh run /sys failover status standby

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 105

The output of a tmsh command is: ----- Net::Interface Name Status Bits Bits Errs Errs Drops Drops Colli In Out
 In Out In Out sions ----- 1.1 down 0 0 0 0 0 0 1.2 up 191.4K 0 0 0 374 0 0 1.3 down 0 0 0 0 0
 0 0 1.4 up 22.5K 0 0 0 44 0 0 2.1 miss 0 0 0 0 0 0 2.2 miss 0 0 0 0 0 0 0 mgmt up 43.2G 160.0G 0 0 0 0 0

Which command was executed on the LTM device to show the output?

- A. tmsh show /net interface
- B. tmsh /net show interface status
- C. tmsh /net show interface
- D. tmsh show /net interface status

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 106**

Given:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/md11	248M	248M	0	100%	/
/dev/md13	3.0G	76M	2.8G	3%	/config
/dev/md12	1.7G	1.1G	476M	71%	/usr
/dev/md14	3.0G	214M	2.6G	8%	/var
/dev/md0	30G	2.2G	26G	8%	/shared
/dev/md1	6.9G	288M	6.3G	5%	/var/log
none	3.9G	452K	3.9G	1%	/dev/shm
none	3.9G	19M	3.9G	1%	/var/tmstat
none	3.9G	1.2M	3.9G	1%	/var/run
prompt	4.0M	12K	4.0M	1%	/var/prompt
/dev/md15	12G	8.3G	3.1G	74%	/var/lib/mysql

Which command is used to produce this output?

- A. df
- B. du
- C. lsof
- D. ps
- E. vmstat

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 107**

An LTM Specialist realizes that a datacenter engineer has changed the console baud rate.

Which command determines the current baud rate via the command line interface?

- A. tmsh show /ltm console

- B. tmsh show /sys console
- C. tmsh list /sys baud-rate
- D. tmsh list /net baud-rate

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

The LTM device is configured for RADIUS authentication. Remote logins are failing and the LTM Specialist must verify the RADIUS configuration. How should the LTM Specialist check the RADIUS server and shared secret configured on the LTM device?

- A. tmsh show running-config /auth radius
- B. tmsh show running-config /sys auth radius
- C. tmsh show running-config /auth configuration
- D. tmsh show running-config /sys auth radius-server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

An F5 LTM Specialist needs to perform an LTM device configuration backup prior to RMA swap.

Which command should be executed on the command line interface to create a backup?

- A. bigpipe config save /var/tmp/backup.ucs
- B. tmsh save /sys ucs /var/tmp/backup.ucs
- C. tmsh save /sys config /var/tmp/backup.ucs
- D. tmsh save /sys config ucs /var/tmp/backup.ucs

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 110**

An LTM Specialist notices the following error on the stdout console:

```
mcpd[2395]: 01070608:0: License is not operational(expired or digital signature does not match contents)
```

Which command should be executed to verify the LTM device license?

- A. bigpipe version
- B. tmsh show /sys license
- C. tmsh /util bigpipe version
- D. tmsh show /sys license status

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:**QUESTION 111**

Given the log entry:

```
011f0005:3: HTTP header (32800) exceeded maximum allowed size of 32768 (Client sidE. vip=/Common/VS_web profile=http pool=/Common/POOL_web client_ip=10.0.0.1)
```

Which HTTP profile setting can be modified temporarily to resolve the issue?

- A. Increase Maximum Requests
- B. Decrease Maximum Requests
- C. Increase Maximum Header Count
- D. Decrease Maximum Header Count
- E. Increase Maximum Header size
- F. Decrease Maximum Header size

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:**QUESTION 112**

Which command should the LTM Specialist use to determine the current system time?

- A. date
- B. time
- C. uname -a
- D. ntpq -p

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 113**

An LTM Specialist connects to an LTM device via the serial console cable and receives unreadable output. The LTM Specialist is using the appropriate cable and connecting it to the correct serial port.

Which command should the LTM Specialist run through ssh to verify that the baud rate settings for the serial port are correct on the LTM device?

- A. tmsh list /sys console
- B. tmsh edit /sys console
- C. tmsh show /sys console
- D. tmsh show /ltm console

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:**QUESTION 114**

The active LTM device in a high-availability (HA) pair performs a failover at the same time the network team reports an outage of a switch on the network.

Which two items could have caused the failover event? (Choose two.)

- A. a VLAN fail-safe setting
- B. a monitor on a pool in an HA group
- C. the standby LTM that was rebooted
- D. an Auditor role that has access to the GUI
- E. the standby LTM that lost connectivity on the failover VLAN

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 115

An active/standby pair of LTM devices deployed with network failover are working as desired. After external personnel perform maintenance on the network, the LTM devices are active/active rather than active/standby. No changes were made on the LTM devices during the network maintenance.

Which two actions would help determine the cause of the malfunction? (Choose two.)

- A. checking that the configurations are synchronized
- B. checking the configuration of the VLAN used for failover
- C. checking the configuration of the VLAN used for mirroring
- D. checking the open ports in firewalls between the LTM devices
- E. checking synchronization of system clocks among the network devices

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 116

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. promptstatsd
- B. mcpd
- C. sod
- D. bcm56xxd
- E. lind

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 117

In preparation for a maintenance task, an LTM Specialist performs a "Force to Standby" on LTM device Unit 1. LTM device Unit 2 becomes active as expected. The maintenance task requires the reboot of Unit 1. Shortly after the reboot is complete, the LTM Specialist discovers that Unit 1 has become active and Unit 2 has returned to standby.

What would cause this behavior?

- A. Unit 1 is set with the redundancy state preference of active in devices groups.
- B. Unit 1 is set with the redundancy state preference of active in high availability.
- C. A traffic group is configured with Auto Failback, and Unit 1 is the default device.
- D. A device group is configured with Auto Failback, and Unit 1 is the default device.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 118

A high-availability (HA) pair configuration uses only the hardwire serial cable connection to determine device state. A power outage occurs to the PDU powering the active unit. The standby unit takes over the active role as expected.

How is the peer unit able to determine the active unit is unavailable?

- A. voltage loss on serial cable
- B. no data stream received on serial port
- C. no response on management interface
- D. no heartbeat packets received on self IPs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

While investigating the cause of a device failover, an LTM Specialist discovers the following events in /var/log/ltm:

```
01010029:5: Clock advanced by 518 ticks
01010029:5: Clock advanced by 505 ticks
01010029:5: Clock advanced by 590 ticks
01010029:5: Clock advanced by 568 ticks
01010029:5: Clock advanced by 1681 ticks
01010029:5: Clock advanced by 6584 ticks
01140029:5: HA daemon_heartbeat tmm fails action is failover and restart.
010c0026:5: Failover condition, active attempting to go standby.
```

Which issue caused the failover?

- A. NTP being out of sync
- B. TMM being descheduled

- C. VLAN Fail-safe heartbeats
- D. HA missing heartbeat packets

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

A failover event is recorded in the log messages:

```
Jan 01 00:00:50 BIG-IP notice sod[5855]: 01140029:5: HA proc_running tmm fails action is go offline and down links.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0050:5: Sod requests links down.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0054:5: Offline for traffic group /Common/traffic-group-1.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c003e:5: Offline
Jan 01 00:00:50 BIG-IP notice logger: /usr/bin/tmipsecd --tmmcount 4 ==> /usr/bin/bigstart stop racoon
Jan 01 00:00:50 BIG-IP info lacpd[5502]: 01160016:6: Failover event detected. (Switchboard failsafe disabled while offline)
Jan 01 00:00:51 BIG-IP err bcm56xxd[5296]: 012c0010:3: Failover event detected. Marking external interfaces down. bsx.c(3633)
Jan 01 00:00:51 BIG-IP info bcm56xxd[5296]: 012c0015:6: Link: 1.1 is DOWN
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143c:5: Connection to CMI peer 10.0.0.3 has been removed
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143a:5: CMI reconnect timer: enabled
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 01071431:5: Attempting to connect to CMI peer 10.0.0.3 port 6699
```

What is the cause of the failover?

- A. TMM failed, and VLAN fail-safe initiated the failover.
- B. TMM failed, and system fail-safe initiated the failover.
- C. Loss of connection to CMI peer 10.0.0.3 initiated the failover.
- D. A switchboard failure caused system fail-safe to initiate the failover.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 121

An LTM Specialist has just manually failed the active LTM device over to the standby LTM device. The LTM Specialist notices the newly active LTM device is NOT currently receiving traffic. The LTM Specialist verifies the newly active device is responding to ARP but still no traffic is hitting the virtual

servers. The LTM Specialist also notices that the virtual servers eventually start responding.

What should be added to the configuration to resolve the problem?

- A. vlan failsafe
- B. floating self IP
- C. network failover
- D. MAC masquerading
- E. connection mirroring

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 122

An LTM Specialist is troubleshooting an issue where one LTM device in a three LTM device group is failing to synchronize after a synchronize to group command is issued. The LTM Specialist verifies there are no packet filters, port lock down, or network issues preventing the connection.

What are two reasons the synchronization group is having issues? (Choose two.)

- A. Certificates expired on all of the peer LTM devices.
- B. Certificates stored for the device trusts on all of the peer LTM devices are corrupted.
- C. Admin passwords changed on one of the peer LTM devices that are able to synchronize.
- D. Admin password changed on the LTM device NOT receiving the synchronized configurations.
- E. Certificates stored for the device trusts on the LTM device NOT receiving the configuration are corrupted.

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 123

An LTM Specialist configures two LTM devices in a high-availability pair with trusts established and device groups configured properly using network failover. After several months, the LTM Specialist notices that changes made to one LTM device do NOT cause the synchronization status to update to "changes pending," and this device does NOT synchronize with the device group.

Which two steps should the LTM Specialist take to identify the issue? (Choose two.)

- A. Verify that NTP is synchronized.
- B. Verify the network connectivity between the devices.
- C. Verify that the devices are not using self-signed certificates.
- D. Verify that ConfigSync is using the management IP address.
- E. Verify that port lockdown on the ConfigSync interface is set to allow port 1026.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

An HA pair of LTM devices configured in Active-Standby mode stops responding to traffic and causes an outage. The Active device becomes Standby, but the partner device stays in Standby mode instead of taking over as Active. A reboot and restart of the services brings the LTM device to Active mode for a short time, but then it goes into Standby mode again.

Which two configuration components caused this condition? (Choose two.)

- A. VLAN Fail-safe
- B. System Fail-safe
- C. Gateway Fail-safe
- D. Switch Board Failure
- E. Link down on Failover

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

A device group is made up of four members: LTM-A, LTM-B, LTM-C, and LTM-D. An LTM Specialist makes a configuration change on LTM-B. Later, a different LTM Specialist notices a "changes pending" message on all devices. When logged into LTM-D, the LTM Specialist attempts to config-sync to the device group. The sync operation fails.

Why is the LTM Specialist on LTM-D unable to synchronize the configuration to the group?

- A. The changes made on LTM-B are invalid.
- B. LTM-D has the lowest commit-id of the group.
- C. NTP is NOT configured on the devices in the group.
- D. LTM-B is the device eligible to initiate a config-sync.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

A failover event is recorded in the following log messages:

```
Jan 01 00:56:56 BIG-IP notice mcpd[5318]: 01070727:5: Pool /Common/my-pool member /Common/10.0.0.10:80 monitor status down.  
Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0045:5: Leaving active, group score 10 peer group score 20.  
Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0052:5: Standby for traffic group /Common/traffic-group-1.  
Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0018:5: Standby  
Jan 01 00:57:06 BIG-IP notice logger: /usr/bin/tmipsecd --tmmcount 4 ==> /usr/bin/bigstart stop racoon
```

What is the cause of the failover?

- A. The HA group score changed.
- B. No traffic is seen on traffic-group-1.
- C. The peer device left the traffic group.
- D. The racoon service stopped responding.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 127

An LTM device pair is configured for failover and connection mirroring. The LTM devices are configured with virtual servers for HTTP, HTTPS with SSL offload, and SSH. An event occurs that causes a failover. HTTP and SSH sessions active at the time of failover remain active, but HTTPS sessions are dropped.

What is the root cause of this problem?

- A. The SSL certificates on the LTM devices do NOT match.
- B. Connection mirroring is incompatible with clientssl profiles.
- C. SNAT automap was NOT enabled for the HTTPS virtual servers.
- D. Connection mirroring was NOT enabled for the HTTPS virtual servers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

-- Exhibit

```
ltm profile httpclass acct_class {
    app-service none
    defaults-from httpclass
    paths { glob:/accounting }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass marketing_class {
    app-service none
    defaults-from httpclass
    paths { glob:/marketing }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass default_class {
    app-service none
    defaults-from httpclass
    pool srv2_http_pool
    redirect none
}
ltm virtual http_vs {
    destination 192.168.1.155:http
    http-class {
        acct_class
        marketing_class
        default_class
    }
    ip-protocol tcp
    mask 255.255.255.255
    pool srv2_http_pool
    profiles {
        http { }
        tcp { }
    }
    snat automap
    vlans-disabled
}
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is reviewing the virtual server configuration on an LTM device.

Which two actions should the LTM Specialist perform to minimize the virtual server configuration? (Choose two.)

- A. Remove 'snat automap' from the virtual server.
- B. Remove the 'http' profile from the virtual server.
- C. Remove the 'default_class' from the virtual server.
- D. Combine 'acct_class' and 'marketing_class' into one class and update associations on the virtual server.
- E. Combine 'marketing_class' and 'default_class' into one class and update associations on the virtual server.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

-- Exhibit

```
ltm node /test/10.1.1.1 {  
    address 10.1.1.1  
}  
ltm node /test/10.1.1.2 {  
    address 10.1.1.2  
}  
ltm node /test/10.1.1.3 {  
    address 10.1.1.3  
}  
ltm pool /test/test1_pool {  
    members {  
        /test/10.1.1.1:80 {  
            address 10.1.1.1  
        }  
        /test/10.1.1.2:8080 {  
            address 10.1.1.2  
        }  
    }  
}  
ltm pool /test/test2_pool {  
    members {  
        /test/10.1.1.1:8080 {  
            address 10.1.1.1  
        }  
        /test/10.1.1.3:8080 {  
            address 10.1.1.3  
        }  
    }  
}  
ltm virtual /test/test1_vs {  
    destination /test/172.16.20.1:80  
    ip-protocol tcp  
    mask 255.255.255.255  
    pool /test/test2_pool  
    profiles {  
        /Common/http { }  
        /Common/tcp { }  
    }  
    translate-address enabled  
    translate-port enabled  
    vlans-disabled  
}  
ltm virtual-address /test/172.16.20.1 {  
    address 172.16.20.1  
    mask 255.255.255.255  
    traffic-group /Common/traffic-group-1  
}
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is reviewing the 'test' partition.

Which objects, in order, can be removed from the partition?

- A. delete pool test1_pool, delete node 10.1.1.2
- B. delete node 10.1.1.2, delete pool test2_pool
- C. delete pool test1_pool, delete node 10.1.1.2, delete node 10.1.1.1
- D. delete virtual test1_vs, delete pool test2_pool, delete node 10.1.1.1
- E. delete pool test1_pool, delete pool test2_pool, delete node 10.1.1.3

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 130

-- Exhibit

```
ltm rule /Common/vs1-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs1") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs1/app/"
return
}
}
}

ltm rule /Common/vs2-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs2") && not ([HTTP::uri] starts_with "/app4") } {
HTTP::redirect "https://vs2/app4/"
return
}
}
}

ltm rule /Common/vs3-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs3") && not ([HTTP::uri] starts_with "/app2") } {
HTTP::redirect "https://vs3/app2/"
return
}
}
}

ltm rule /Common/vs4-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs4") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs4/app/"
return
}
}
}

ltm rule /Common/vs5-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs5") && not ([HTTP::uri] starts_with "/app3") } {
HTTP::redirect "https://vs5/app3/"
return
}
}
}
```

-- Exhibit --

Refer to the exhibit.

Which two items can be consolidated to simplify the LTM configuration? (Choose two.)

- A. /Common/vs1-https-redirect
- B. /Common/vs2-https-redirect
- C. /Common/vs3-https-redirect
- D. /Common/vs4-https-redirect
- E. /Common/vs5-https-redirect

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

-- Exhibit

-- Exhibit --

Refer to the exhibit.

Which pool can be removed without affecting client traffic?

- A. ftp_pool
- B. http_pool
- C. server1_80
- D. server_pool

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

-- Exhibit

Profiles	
Select Profile	tcp
Clear Profile Statistics	
Connections	
Open	0
Accepted	693
Not Accepted	0
Established	461
Failed	0
Expired	0
Abandoned	0
Miscellaneous	
Received Reset	0
Bad Checksum	0
Malformed Segment	0
Segment out of Order	0
Received SYN Cookie	0
Received Bad SYN Cookie	0
SYN Cache Overflow	0
Retransmitted Segments	0

Configuration:	Advanced
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http
HTTP Compression Profile	httpcompression
Web Acceleration Profile	optimized-caching

Profiles	
Select Profile	optimized-caching
Clear Profile Statistics	
Cache	
Cache Size (bytes)	50.5K
Total Cached Items	1
Total Evicted Items	0
Cache Hits / Misses	
	Count
Hits	232
Misses (Cacheable)	1
Misses (Uncacheable)	0

Profiles

Select Profile

httpcompression

Clear Profile Statistics

Content Type Compression	Pre-Compress	Post-Compress
HTML	0	0
CSS	0	0
JS	0	0
XML	0	0
SGML	0	0
Plain	23.6M	23.7M
Image	0	0
Video	0	0
Other	0	0
Total	23.6M	23.7M

Profiles	
Select Profile	
Clear Profile Statistics	
Requests	
GET	
POST	
Version 0.9	
Version 1.0	
Version 1.1	
Max Requests	
Total	
Responses	
Successful	
Redirection	
Client Errors	
Server Errors	
Version 0.9	
Version 1.0	
Version 1.1	
Response Size	
Responses	
Miscellaneous	
Set Cookie In	

-- Exhibit --

Refer to the exhibit.

Which profile could be removed or changed on this virtual server to reduce CPU load on the LTM device without increasing server side bandwidth usage?

- A. tcp
- B. http
- C. httpcompression
- D. optimized-caching

Correct Answer: C

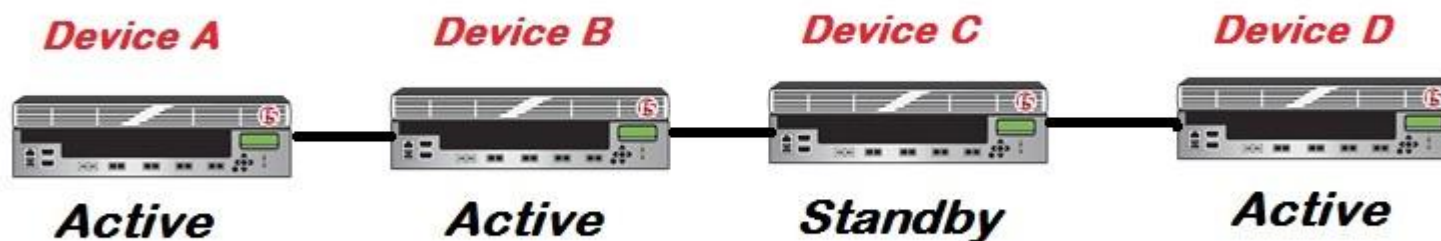
Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

-- Exhibit



-- Exhibit --

Refer to the exhibit.

An LTM Specialist is upgrading the LTM devices.

Which device should be upgraded first?

- A. Device A
- B. Device B
- C. Device C
- D. Device D

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

-- Exhibit

An SSH configuration error exposes a potential vulnerability - CVE-2012-1493

Recommended upgrade version
10.2.4 11.0.0.HF2 11.1.0.HF3 11.2.0

Solution Links
[SOL13600](#)

Heuristic Name
H386652

Was this helpful?
 Yes No

[Details](#)

Related Changes
ID 379600

Description
An SSH configuration error in the default SSH configuration may allow unauthorized remote users to gain privileged access to the system.

Recommendation resolution
Upgrade to an unaffected version. For workaround information, refer to the linked Solution.

Additional Information
The current configuration appears to be vulnerable.

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is working on an LTM 11.0.0 installation and has identified a security vulnerability as shown in the exhibit. The LTM Specialist is tasked with applying the latest available hotfix to resolve the problem.

Which procedure resolves the problem?

- A. Browse to System > Software Management > Hotfix List.
Import TMOS 11.2.0 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- B. Browse to System > Software Management > Hotfix List.
Import 11.1.0.HF3 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- C. Browse to System > Software Management > Image List.
Import TMOS 11.2.0 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- D. Browse to System > Software Management > Image List.
Import 11.1.0.HF3 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

-- Exhibit

Hostname: V11-BigIP-A.local
IP Address: 10.0.0.231

Date: Oct 17, 2012
Time: 1:12 PM (EDT)

User: admin
Role: Administrator



ONLINE (ACTIVE)
Not All Devices Synced

Main

Help

About



Statistics



iApp



Wizards



Global Traffic



Local Traffic



Access Policy



Device Management



Network



System

Configuration

Device Certificates

File Management

Disk Management

Software Management

License

Resource Provisioning

Platform

System » **Software Management : Image List**



Image List

Hotfix List

Antivirus Check Updates

Boot Locations

Installed Images

Product	Version	Build	Disk	Boot Location
BIG-IP	11.2.1	797.0	HD1	HD1.1
BIG-IP	11.1.0	2268.0	HD1	HD1.2
BIG-IP	11.2.1	797.0	HD1	HD1.3

Available Images

<input checked="" type="checkbox"/>	Status	Software Image
<input type="checkbox"/>	<input checked="" type="checkbox"/>	BIGIP-11.1.0.1943.0.iso
<input type="checkbox"/>	<input checked="" type="checkbox"/>	BIGIP-11.2.1.797.0.iso

Delete

Install...

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has uploaded a qkview to F5 iHealth.

Within the GUI, what is the correct procedure to comply with the recommendation shown in the exhibit?

- A. Obtain product version image from release.f5.com.
Overwrite existing image with new product version image.
Select product version image and click Install.
Select the available disk and volume set name.
- B. Obtain product version image from images.f5.com.
Overwrite existing image with new product version image.
Select product version image and click Install.
Select the available disk and volume set name.
- C. Obtain product version image from downloads.f5.com.
Import product version image.
Install image onto BIG-IP platform.
Select product version image and click Install.
Select the available disk and volume set name.
- D. Log a call requesting the product version image via websupport.f5.com Import product version image.
Install image onto BIG-IP platform.
Select product version image and click Install.
Select the available disk and volume set name.

Correct Answer: C

Section: (none)






Explanation

Explanation/Reference:



QUESTION 136

-- Exhibit

Status**Diagnostics**

Results	 3 High  1 Medium  2 Low
Recommendation	 Upgrade to version: 11.2.0 or higher
Status	 No new potential issues identified since last update.

Errors

Extraction	 No errors during QKView extraction.
Diagnostics	 No errors during diagnostics run.

-- Exhibit --

Refer to the exhibit.

Which step should an LTM Specialist take next to finish upgrading to HD1.3?

- A. Install image to HD1.3
- B. Install hotfix to HD1.3
- C. Activate HD1.3
- D. Relicense HD1.3

Correct Answer: C

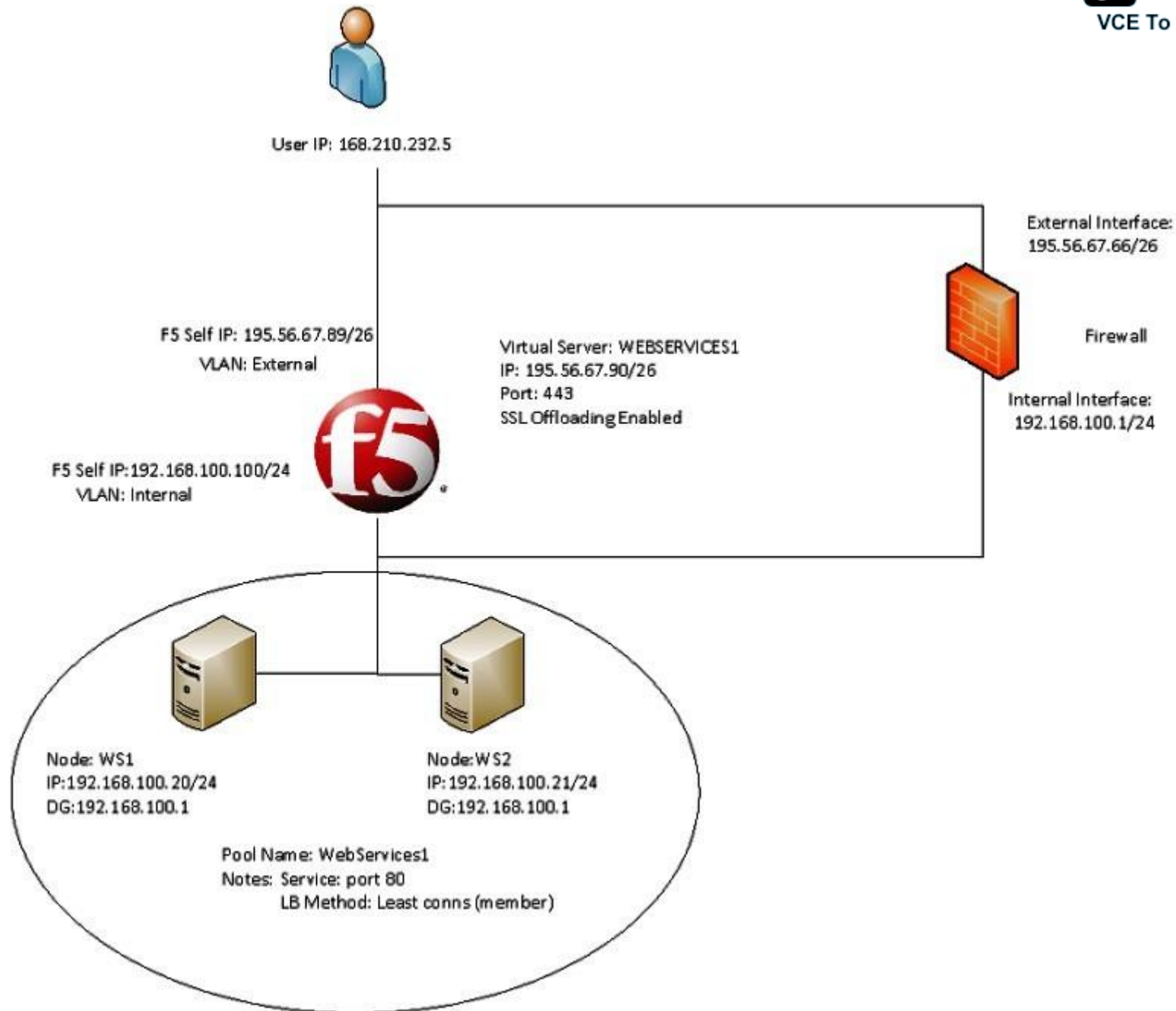
Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

-- Exhibit



-- Exhibit --

Refer to the exhibit.

Users receive an error when attempting to connect to the website <https://website.com>. The website has a DNS record of 195.56.67.90. The upstream ISP has confirmed that there is nothing wrong with the routing between the user and the LTM device.

The following tcpdump outputs have been captured:

External Vlan, filtered on IP 168.210.232.5

00:25:07.598519 IP 168.210.232.5.33159 > 195.56.67.90.https: S 1920647964:1920647964(0) win 8192 <mss 1450,nop,nop,sackOK>

00:25:07.598537 IP 195.56.67.90.https > 168.210.232.5.33159: S 2690691360:2690691360(0) ack 1920647965 win 4350 <mss 1460,sackOK,eol>

00:25:07.598851 IP 168.210.232.5.33160 > 195.56.67.90.https: S 2763858764:2763858764(0) win 8192 <mss 1450,nop,nop,sackOK>

00:25:07.598858 IP 195.56.67.90.https > 168.210.232.5.33160: S 1905576176:1905576176(0) ack 2763858765 win 4350 <mss 1460,sackOK,eol>

Internal Vlan, filtered on IP 168.210.232.5

00:31:46.171124 IP 168.210.232.5.33202 > 192.168.100.20.http: S 2389057240:2389057240(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

What is the problem?

- A. The filters on the tcpdumps are incorrect.
- B. The DNS entry for website.com is incorrect.
- C. The virtual server 'WEBSERVICES1' is listening on the incorrect port.
- D. The firewall is dropping the connection coming from the pool members returned to the client.
- E. The subnet masks of the pool members of pool WebServices1 and the f5 'Internal' Vlan are incorrect.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 138

-- 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. After trying Mozilla Firefox and Internet Explorer browsers, the client still receives the same errors.

The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit.
What is the problem?

- A. The SSL key length is incorrect.
- B. The BIG-IP LTM is NOT serving a certificate.
- C. The BIG-IP LTM is NOT listening on port 443.
- D. The client needs to be upgraded to the appropriate cipher-suite.

Correct Answer: B

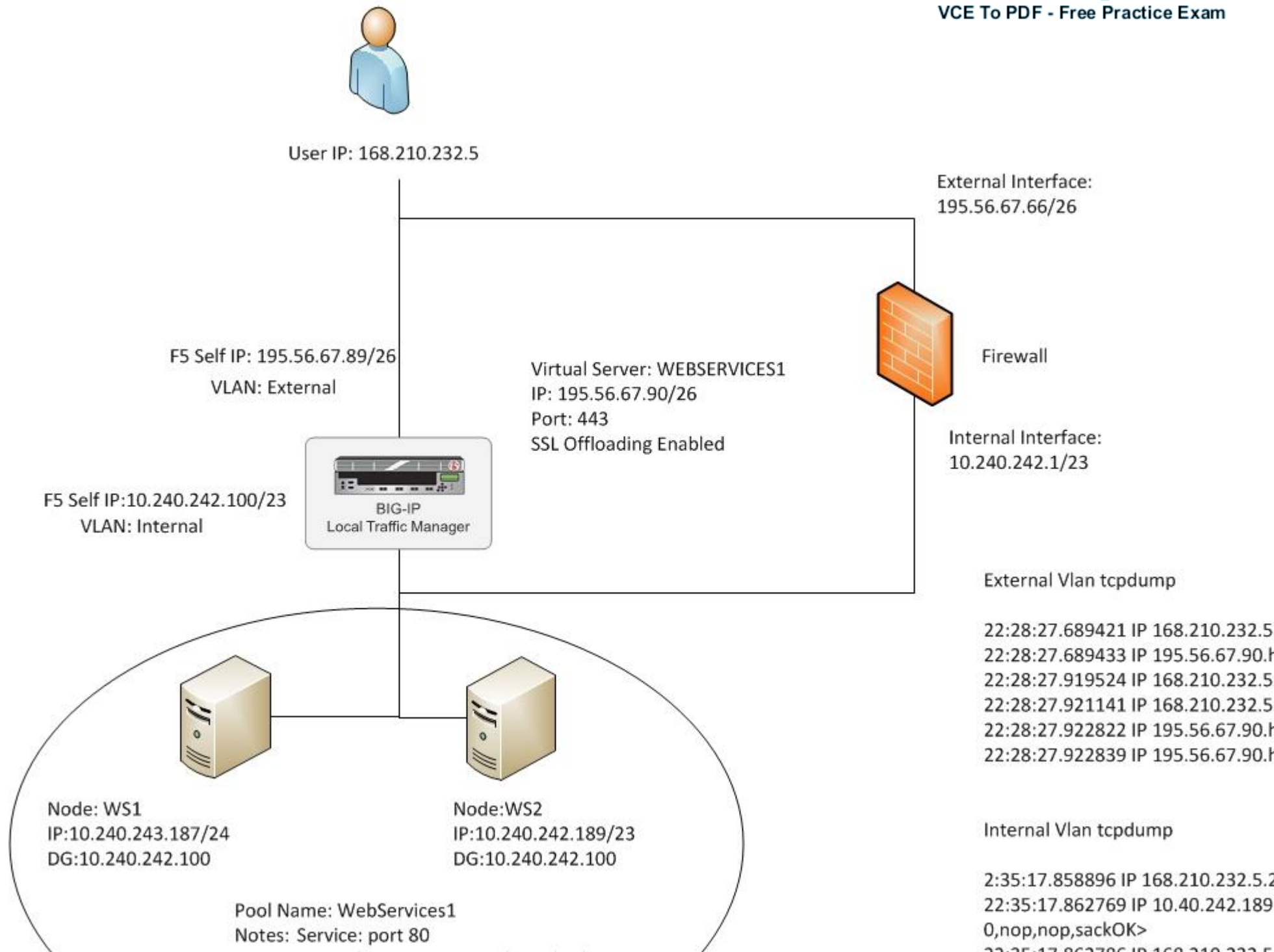
Section: (none)

Explanation

Explanation/Reference:

QUESTION 139

-- Exhibit



-- Exhibit --

Refer to the exhibit.

An LTM Specialist has a virtual server set up on the LTM device as per the exhibit. The LTM Specialist receives reports of intermittent issues. Some clients are connecting fine while others are failing to connect.

The LTM Specialist does a tcpdump on the relevant interfaces, with the following results extracted:
What is causing the intermittent issues?

- A. The firewall is dropping the packets from WS1.
- B. The default gateway is inaccessible from WS1.
- C. The load balancing (LB) method is inappropriate.
- D. The pool members have been set up as an active/standby pair, with WS1 as the standby.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 140

-- Exhibit

External Vlan tcpdump:

```
16:38:10.184240 IP 168.210.232.5.59156 > 66.212.246.58.1990: S 1208467898:1208467898(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,
16:38:10.184249 IP 66.212.246.58.1990 > 168.210.232.5.59156: S 2009182511:2009182511(0) ack 1208467899 win 4140 <mss 1460,nop,ws
16:38:10.454030 IP 168.210.232.5.59156 > 66.212.246.58.1990: . ack 1 win 5
16:38:52.809723 IP 168.210.232.5.31084 > 66.212.246.58.1991: S 2991752264:2991752264(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,
16:38:52.809734 IP 66.212.246.58.1991 > 168.210.232.5.31084: S 2217364875:2217364875(0) ack 2991752265 win 4140 <mss 1460,nop,ws
16:38:52.737749 IP 168.210.232.5.59172 > 66.212.246.58.2002: S 3158709238:3158709238(0) win 8192 <mss 1380,nop,wscale 8,nop,nop,
16:38:52.737766 IP 66.212.246.58.2002 > 168.210.232.5.59172: S 7716150:7716150(0) ack 3158709239 win 4140 <mss 1460,nop,wscale 0
16:38:53.007421 IP 168.210.232.5.59172 > 66.212.246.58.2002: . ack 1 win 5
16:38:53.078216 IP 168.210.232.5.31084 > 66.212.246.58.1991: . ack 1 win 5
16:43:21.434766 IP 168.210.232.5.59156 > 66.212.246.58.1990: R 830:830(0) ack 94934 win 0
```

Internal Vlan tcpdump:

```
16:38:11.887217 IP 168.210.232.5.10033 > 10.240.243.65.1989: S 2408612037:2408612037(0) win 4380 <mss 1460,nop,wscale 0,sackOK,e
16:38:11.887559 IP 10.240.243.65.1989 > 168.210.232.5.10033: S 165435577:165435577(0) ack 2408612038 win 8192 <mss 1310,nop,nop,
16:38:11.887566 IP 168.210.232.5.10033 > 10.240.243.65.1989: . ack 1 win 4380
16:38:53.007459 IP 168.210.232.5.59172 > 10.240.243.66.2002: S 26149351:26149351(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.007908 IP 10.240.243.66.2002 > 168.210.232.5.59172: S 3860985485:3860985485(0) ack 26149352 win 8192 <mss 1310,nop,nop,
16:38:53.007916 IP 168.210.232.5.59172 > 10.240.243.66.2002: . ack 1 win 4380
16:38:53.078499 IP 168.210.232.5.31084 > 10.240.242.197.1991: S 2788170026:2788170026(0) win 4380 <mss 1460,nop,wscale 0,sackOK,
16:38:53.078861 IP 10.240.242.197.1991 > 168.210.232.5.31084: S 2169754248:2169754248(0) ack 2788170027 win 8192 <mss 1310,nop,w
16:38:53.078871 IP 168.210.232.5.31084 > 10.240.242.197.1991: . ack 1 win 4380
16:43:29.434782 IP 168.210.232.5.10033 > 10.240.243.65.1989: R 181:181(0) ack 88278 win 65535
```

-- 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 is tasked with finding the cause of the problem.

The LTM Specialist has the tcpdump extract and knows the client software has at least one connection to a VS on port 1990. However, when a tcpdump runs on the internal VLAN, there is no record of port 1990 in the tcpdump.

Why is there no record of port 1990 in the tcpdump?

- A. The LTM device drops the connection.
- B. Port 1990 is a well-known port, so its use is restricted.
- C. The LTM device performs a Port Address Translation (PAT).

D. The LTM device performs a Network Address Translation (NAT).

Correct Answer: C

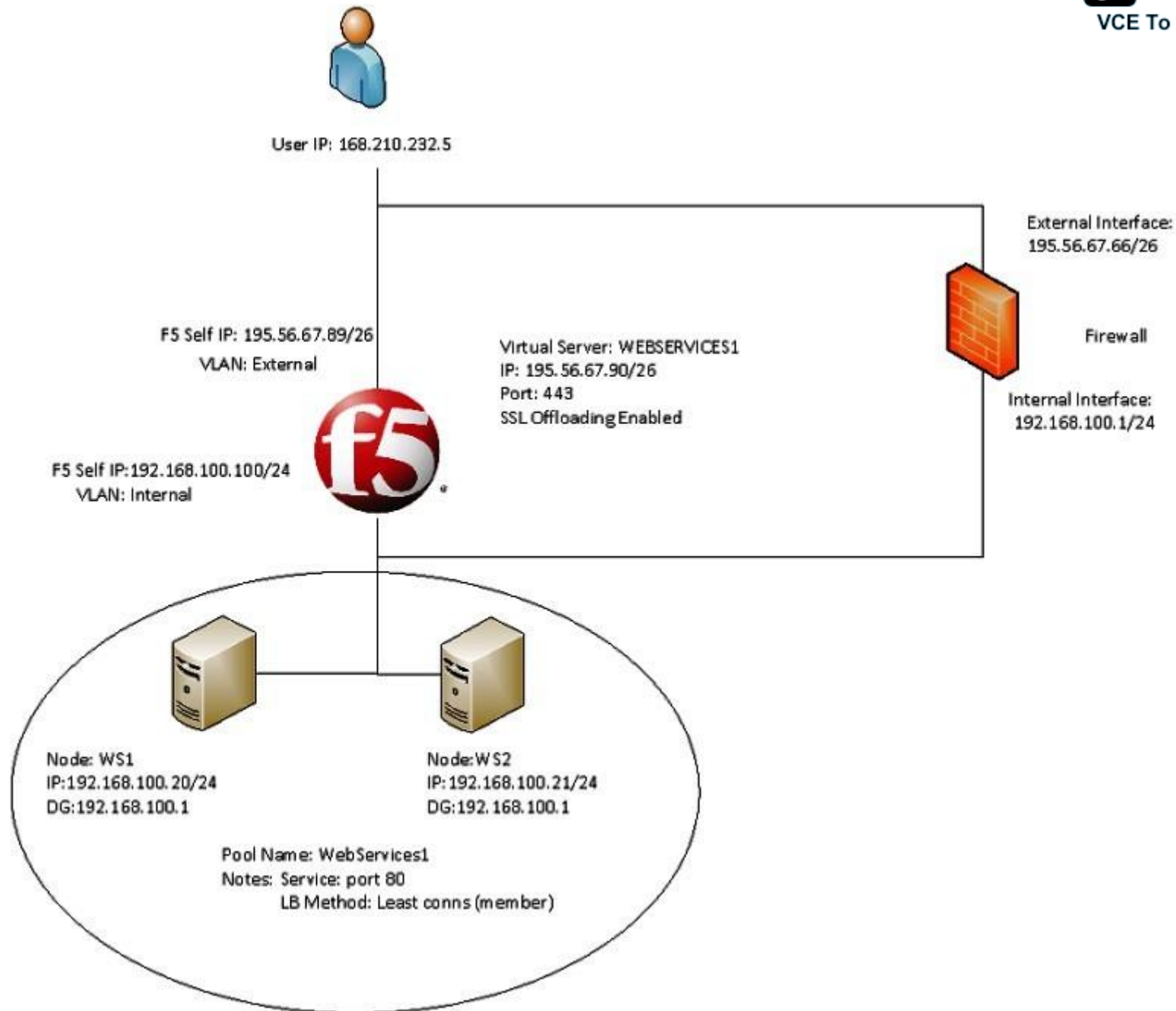
Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

-- 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

-- 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

-- 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 has the tcpdump extract. The client loses connection with the LTM device.

Where is the reset originating?

- A. the local switch
- B. the application server
- C. the device initiating the connection
- D. the destination device of the initial connection

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 143

-- Exhibit

Virtual Server details

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp-wan-optimised
Protocol Profile (Server)	tcp-lan-optimised
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	None
FTP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None
Authentication Profiles	None
RTSP Profile	None
SMTP Profile	None
Diameter Profile	None
SIP Profile	None
Statistics Profile	None
SNAT Pool	None
Rate Class	None
Traffic Class	None
Connection Limit	None
Connection Mirroring	None
Address Translation	Enabled
Port Translation	Enabled
Source Port	Preserve
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None

Pool details:

10.40.242.12: 443
 10.40.242.13: 443

-- Exhibit --

Refer to the exhibit.

An LTM device is used to load balance web content over a secure channel.

The developers of the web content have done a trace using an HTTP profiler application. They believe that allowing the LTM device to compress traffic to the client will improve performance. The client can utilize GZIP or deflate compression algorithms.

An LTM Specialist must implement the compression.

The LTM Specialist has completed the following actions:

1. Create the relevant profile.
2. Apply the relevant profile to the virtual server (VS).

After applying the relevant profile, the LTM device is failing to compress the traffic. Instead, the traffic is being served with an error.

What is the problem?

- A. The incorrect compression algorithm is applied to the compression profile.
- B. The LTM device CANNOT SSL offload the traffic in order to read and compress it.
- C. The Protocol Profile (Client) option of "Allow Compression" needs to be enabled.
- D. The Protocol Profile (Server) option of "Allow Compression" needs to be enabled.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

-- Exhibit

source-address - 78.24.213.79:443 - 10.72.250.52:80

TMM	0
Mode	source-address
Key	168.210.232.5
Age (sec.)	140
Virtual Name	VS1
Virtual Addr	78.24.213.79:443
Node Addr	10.72.250.52:80
Pool Name	CDN-ITS
Client Addr	168.210.232.5

source-address - 78.24.213.79:443 - 10.72.250.52:80

TMM	1
Mode	source-address
Key	82.171.210.22
Age (sec.)	404
Virtual Name	VS1
Virtual Addr	78.24.213.79:443
Node Addr	10.72.250.52:80
Pool Name	CDN-ITS
Client Addr	82.171.210.22

source-address - 78.24.213.79:443 - 10.72.250.60:80

TMM	0
Mode	source-address
Key	78.24.213.193
Age (sec.)	9
Virtual Name	VS1
Virtual Addr	78.24.213.79:443
Node Addr	10.72.250.60:80
Pool Name	CDN-ITS
Client Addr	78.24.213.193

source-address - 78.24.213.79:443 - 10.72.250.60:80

TMM	1
Mode	source-address
Key	78.24.213.193
Age (sec.)	10
Virtual Name	VS1
Virtual Addr	78.24.213.79:443
Node Addr	10.72.250.60:80

-- Exhibit --

Refer to the exhibit.

A virtual server is set up on an LTM device as follows:

Virtual server address 78.24.213.79

Default Persistence Profile. source_addr, 600s.

Pool Name. Pool1

Pool Members: 10.72.250.52:80 and 10.72.250.60:80 (both on Internal Vlan)

There are several current connections to the virtual server, and pool member 10.72.250.52:80 has been set to a "Disabled" state.

A tcpdump on the Internal Vlan shows traffic going to 10.72.250.52:80.

How soon after the persistence table query was run can existing connections be refreshed/renewed to ensure that no requests are sent to 10.72.250.52?

- A. 196 seconds
- B. 460 seconds
- C. 539 seconds
- D. 590 seconds
- E. 591 seconds

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

-- 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 146

-- Exhibit


```
13:20:26.194324 IP 10.10.1.1.42923 > 172.16.20.2.ftp: S 1642091015:1642091015(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,
13:20:26.196505 IP 172.16.20.2.ftp > 10.10.1.1.42923: S 3574712268:3574712268(0) ack 1642091016 win 5792 <mss 1460,sackOK
13:20:26.196514 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 1 win 4380 <nop,nop,timestamp 2403895573 9643612>
13:20:26.199257 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 1:21(20) ack 1 win 724 <nop,nop,timestamp 9643615 2403895573>
13:20:26.199274 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 21 win 4400 <nop,nop,timestamp 2403895575 9643615>
13:20:28.436817 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 1:15(14) ack 21 win 4400 <nop,nop,timestamp 2403897813 9643615>
13:20:28.438230 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 15 win 724 <nop,nop,timestamp 9645855 2403897813>
13:20:28.438234 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 21:55(34) ack 15 win 724 <nop,nop,timestamp 9645855 2403897813>
13:20:28.438251 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 55 win 4434 <nop,nop,timestamp 2403897814 9645855>
13:20:30.860614 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 15:29(14) ack 55 win 4434 <nop,nop,timestamp 2403900237 9645855>
13:20:30.901297 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 29 win 724 <nop,nop,timestamp 9648319 2403900237>
13:20:40.864453 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 55:78(23) ack 29 win 724 <nop,nop,timestamp 9658281 2403900237>
13:20:40.864522 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 78 win 4457 <nop,nop,timestamp 2403910241 9658281>
13:20:40.865948 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 29:35(6) ack 78 win 4457 <nop,nop,timestamp 2403910242 9658281>
13:20:40.867799 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 35 win 724 <nop,nop,timestamp 9658284 2403910242>
13:20:40.867803 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 78:97(19) ack 35 win 724 <nop,nop,timestamp 9658284 2403910242>
13:20:40.867816 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 97 win 4476 <nop,nop,timestamp 2403910244 9658284>
13:20:47.199810 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 35:43(8) ack 97 win 4476 <nop,nop,timestamp 2403916576 9658284>
13:20:47.201215 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 97:128(31) ack 43 win 724 <nop,nop,timestamp 9664618 2403916576>
13:20:47.201233 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 128 win 4507 <nop,nop,timestamp 2403916577 9664618>
13:20:47.202263 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 43:67(24) ack 128 win 4507 <nop,nop,timestamp 2403916578 9664618>
13:20:47.203810 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 128:179(51) ack 67 win 724 <nop,nop,timestamp 9664620 2403916578>
13:20:47.203822 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 179 win 4558 <nop,nop,timestamp 2403916580 9664620>
13:20:47.205035 IP 10.10.1.1.42923 > 172.16.20.2.ftp: P 67:82(15) ack 179 win 4558 <nop,nop,timestamp 2403916581 9664620>
13:20:47.206441 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp
13:20:47.245894 IP 172.16.20.2.ftp > 10.10.1.1.42923: . ack 82 win 724 <nop,nop,timestamp 9664663 2403916581>
13:20:50.205908 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp
13:20:56.205528 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp
13:21:08.205649 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp
13:21:32.205498 IP 172.16.20.2.ftp-data > 10.10.1.1.38030: S 3599538288:3599538288(0) win 5840 <mss 1460,sackOK,timestamp
13:21:47.204625 IP 172.16.20.2.ftp > 10.10.1.1.42923: P 179:216(37) ack 82 win 724 <nop,nop,timestamp 9724623 2403916581>
13:21:47.204646 IP 10.10.1.1.42923 > 172.16.20.2.ftp: . ack 216 win 4595 <nop,nop,timestamp 2403976581 9724623>
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist configures a virtual server to load balance to a pool of FTP servers. File transfers are failing. The virtual server is configured as follows:

```
ltm virtual ftp_vs {  
  destination 10.10.1.103:ftp  
  ip-protocol tcp  
  mask 255.255.255.255  
  pool ftp_pool  
  profiles {  
    tcp {}  
  }  
  vlans-disabled  
}
```

Which change will resolve the problem?

- A. Add an FTP monitor to the pool.
- B. Add an FTP profile to the virtual server.
- C. Enable loose initiation in the TCP profile.
- D. Increase the TCP timeout value in the TCP profile.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

-- Exhibit

No.	Time	Source	Src Port	Destination	Dst Port	Protocol	Length	Info
114	17.145218	172.16.20.3	21	10.10.1.2	50645	TCP	92	ftp > 50645 [ACK] Seq=116 Ack=48 win=
115	17.145221	172.16.20.3	21	10.10.1.2	50645	FTP	111	Response: 215 UNIX Type: L8
117	17.145252	10.10.1.2	50645	172.16.20.3	21	TCP	92	50645 > ftp [ACK] Seq=48 Ack=135 win=
132	20.937633	10.10.1.2	50645	172.16.20.3	21	FTP	116	Request: PORT 10,10,1,2,162,211
135	20.942198	172.16.20.3	21	10.10.1.2	50645	FTP	143	Response: 200 PORT command successful
137	20.942235	10.10.1.2	50645	172.16.20.3	21	TCP	92	50645 > ftp [ACK] Seq=72 Ack=186 win=
141	20.945471	10.10.1.2	50645	172.16.20.3	21	FTP	98	Request: LIST
144	20.948418	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 win=584
145	20.987396	172.16.20.3	21	10.10.1.2	50645	TCP	92	ftp > 50645 [ACK] Seq=186 Ack=78 win=
147	23.947014	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 win=584
150	29.946271	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 win=584
153	41.946358	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 win=584
157	65.946527	172.16.20.3	20	10.10.1.2	41683	TCP	100	ftp-data > 41683 [SYN] Seq=0 win=584

-- 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 LTM Specialist performs a capture on the server side of the LTM device.

What is the issue with the application?

- A. data connection failing
- B. LIST command disallowed
- C. PORT command disallowed
- D. command connection failing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 148

-- Exhibit

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

```

-- 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 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 149

-- Exhibit

```
13:59:08.704108 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53347 > 172.16.20.2.53347
13:59:08.704144 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 74: 172.16.20.2.http > 10.10.1.30.53347
13:59:08.705365 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.53347
13:59:08.705632 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 399: 10.10.1.30.53347 > 172.16.20.2.53347
13:59:08.705647 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347
13:59:08.706277 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 528: 172.16.20.2.http > 10.10.1.30.53347
13:59:08.706346 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347
13:59:08.708576 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.53347
13:59:08.711554 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 66: 10.10.1.30.53347 > 172.16.20.2.53347
13:59:08.711578 00:0c:29:2d:d7:13 > 00:0c:29:ba:eb:70, ethertype IPv4 (0x0800), length 66: 172.16.20.2.http > 10.10.1.30.53347
13:59:10.440561 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.53480
13:59:10.440589 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480
13:59:13.439632 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.53480
13:59:13.439658 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480
13:59:16.639821 00:0c:29:ba:eb:70 > 00:0c:29:2d:d7:13, ethertype IPv4 (0x0800), length 78: 10.10.1.30.53480 > 172.16.20.3.53480
13:59:16.639842 00:0c:29:2d:d7:13 > 00:0c:29:36:b6:06, ethertype IPv4 (0x0800), length 74: 172.16.20.3.http > 10.10.1.30.53480
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist configures a virtual server that balances HTTP connections to a pool of three application servers. Approximately one out of every three connections to the virtual server fails.

Which two actions will resolve the problem? (Choose two.)

- A. Assign a custom HTTP monitor to the pool.

- B. Enable SNAT automap on the virtual server.
- C. Verify that port lockdown is set to allow port 80.
- D. Verify the default gateway on the application servers.
- E. Increase the TCP timeout value in the default TCP profile.

Correct Answer: BD

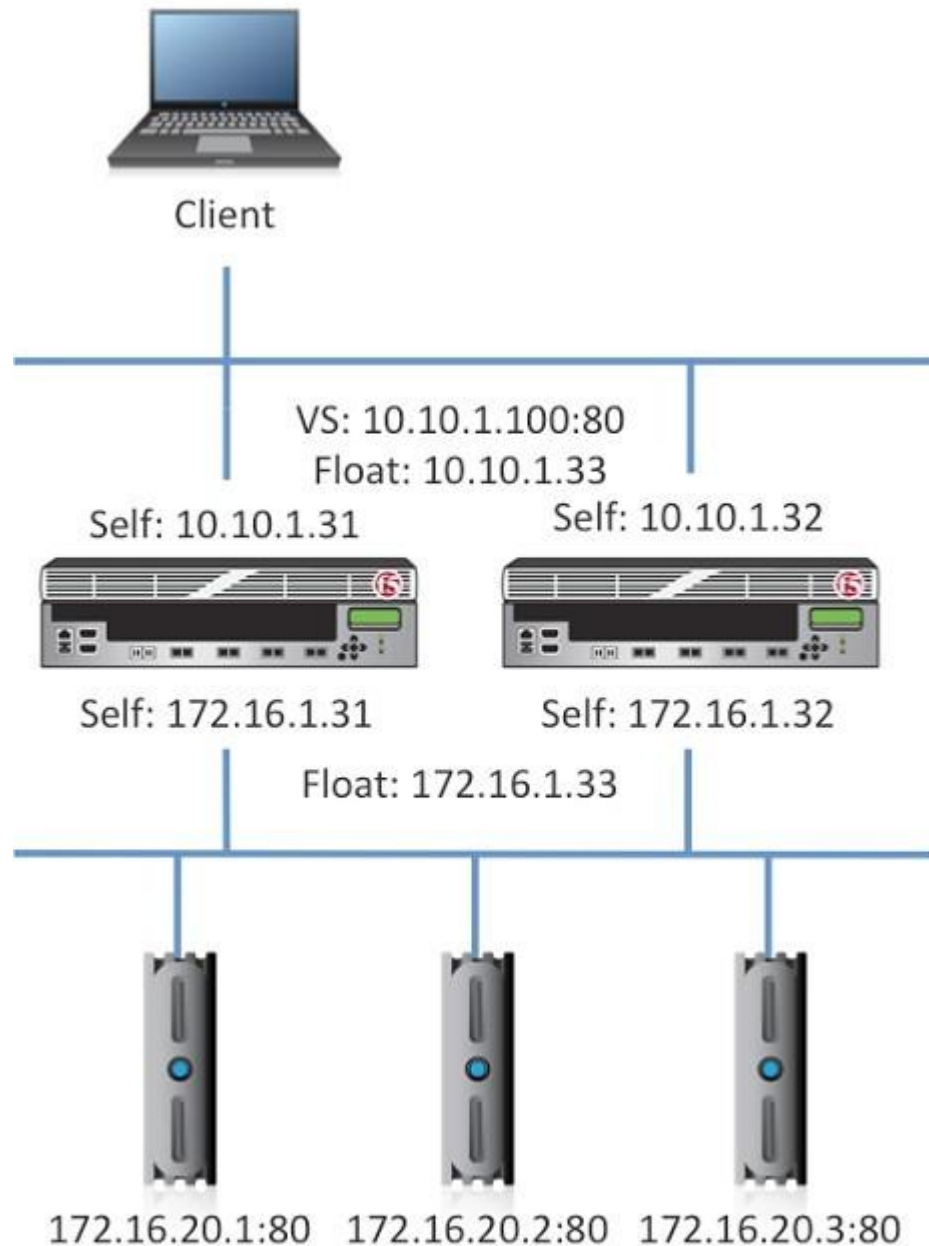
Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

-- 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

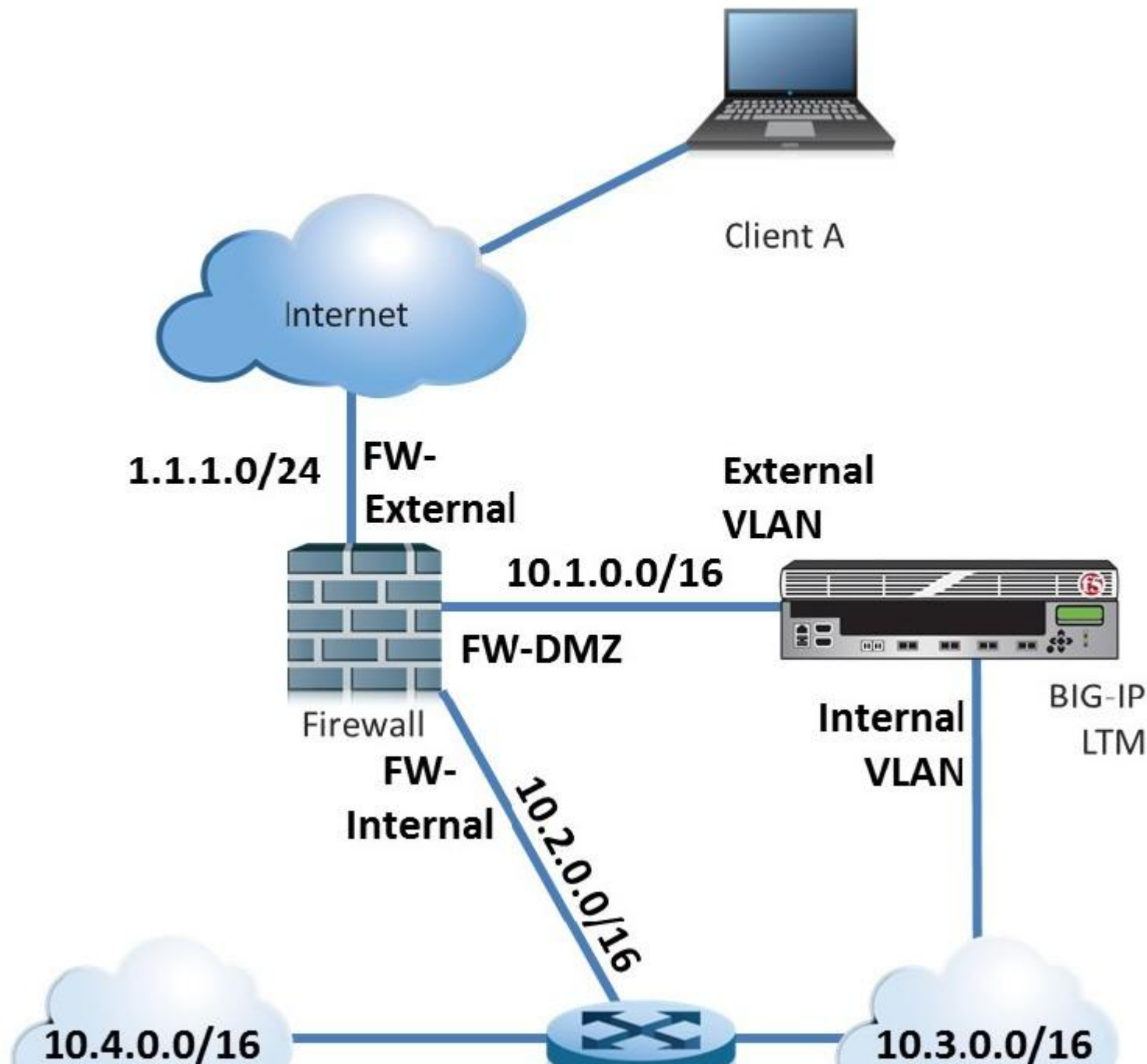
Section: (none)

Explanation

Explanation/Reference:

QUESTION 151

-- Exhibit



-- Exhibit --

Refer to the exhibit.

A layer 2 nPath routing configuration has been deployed. A packet capture contains a client connection packet with the following properties:

Source IP: <Virtual Server>

Destination IP: <Client A>

At which two locations could the packet capture have been taken? (Choose two.)

- A. the network interface of web server
- B. the DMZ interface of the Internet firewall
- C. the internal interface of the Internet firewall
- D. the external VLAN interface of the LTM device

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

-- Exhibit

Monitor definition:

```
ltm monitor http test2 {  
    defaults-from http  
    destination *:*  
    interval 5  
    recv "200 OK"  
    send "GET /webmail HTTP/1.1\\r\\nHost: webmail.example.com\\r\\nConnection: close\\r\\n\\r\\n"  
    time-until-up 0  
    timeout 16  
}
```

HTTP Headers from tcpdump:

```
GET /webmail HTTP/1.1  
Host: webmail.example.com  
Connection: close
```

```
HTTP/1.1 301 Moved Permanently  
Date: Tue, 16 Oct 2012 20:23:22 GMT  
Server: Apache/2.2.3 (CentOS)  
Location: http://webmail.example.com/webmail/  
Content-Length: 327  
Connection: close
```

-- Exhibit --

Refer to the exhibit.

An HTTP monitor always marks the nodes in the pool as down. The monitor's definition and the HTTP headers from the monitor request and response are provided.

What is the issue?

- A. The response is compressed.
- B. The send string is incorrect.
- C. The monitor timeout is too short.
- D. The monitor is NOT configured to follow the redirect.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
-- Exhibit


```
ltm monitor http http_head {
    defaults-from http
    destination *:*
    interval 5
    recv <html>
    send "HEAD / HTTP/1.0\\r\\n\\r\\n"
    time-until-up 0
    timeout 16
}
ltm pool srv1_http_pool {
    members {
        192.168.2.1:http {
            address 192.168.2.1
            session monitor-enabled
            state down
        }
    }
    monitor http_head
}
```

TCPDUMP Output:

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Date: Wed, 24 Oct 2012 18:45:53 GMT
```

```
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
```

```
X-Powered-By: PHP/5.4.4
```

```
Connection: close
```

```
Content-Type: text/html
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser. However, the monitor is marking the member as down. The LTM Specialist captures the monitor traffic via tcpdump.

What is the issue?

- A. The server is marking the connection as closed.
- B. The pool member is rejecting the monitor request.
- C. The monitor request is NOT returning the page body.
- D. The 'time-until-up' setting on the monitor is incorrect.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

-- Exhibit

```
ltm monitor http http_head {
    defaults-from http
    destination *:*
    interval 5
    recv <html>
    send "HEAD / HTTP/1.0\\r\\n\\r\\n"
    time-until-up 0
    timeout 16
}
ltm pool srv1_http_pool {
    members {
        192.168.2.1:http {
            address 192.168.2.1
            session monitor-enabled
            state down
        }
    }
    monitor http_head
}
```

TCPDUMP Output:

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Date: Wed, 24 Oct 2012 18:45:53 GMT
```

```
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
```

```
X-Powered-By: PHP/5.4.4
```

```
Connection: close
```

```
Content-Type: text/html
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting a new HTTP monitor on a pool. The pool member is functioning correctly when accessed directly through a browser, although the monitor is marking the member as down. As part of the troubleshooting, the LTM Specialist has captured the monitor traffic via tcpdump.

How should the LTM Specialist resolve this issue?

- A. Add the 'http' monitor to the pool.
- B. Add the 'icmp' monitor to the node.
- C. Modify the receive string to valid content.
- D. Correct the firewall rules on the pool member.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

-- Exhibit

```

00:00:13.245104 IP 10.29.29.60.51947 > 10.0.0.12.http: P 1:59(58) ack 1 win 46 <nop,nop,timestamp 238063789 2494782300> in slot1
0x0000: 4500 006e 3b19 4000 4006 ce0c 0a1d 1d3c E..n;.@.@.....<
0x0010: 0a00 000c caeb 0050 8be5 aca3 dd65 e3e1 .....P.....e..
0x0020: 8018 002e 1b41 0000 0101 080a 94b3 5b5c .....A.....[\
0x0030: 0e30 90ad 4745 5420 2f74 6573 745f 7061 .0..GET./test_pa
0x0040: 6765 2e68 746d 6c20 4854 5450 312e 310d ge.html.HTTP/1.1.
0x0050: 0a48 6f73 743a 200d 0a43 6f6e 6e65 6374 .Host:...Connect
0x0060: 696f 6e3a 2043 6c6f 7365 0d0a 0d0a 0105 ion:.Close.....
0x0070: 0100 0003 00 .....

00:00:13.245284 IP 10.0.0.12.http > 10.29.29.60.51947: . ack 59 win 362 <nop,nop,timestamp 238063789 2494782300> in slot1
0x0000: 4500 0260 a62e 4000 4006 6105 0a00 000c E..`..@.@.a.....
0x0010: 0a1d 1d3c 0050 bf46 fa3b dc73 bb22 2817 ...<.P.F.;.s."(.
0x0020: 8018 016a 5738 0000 0101 080a 0e37 7a5f ...jW8.....7z_
0x0030: 94f8 7d87 4854 5450 2f31 2e31 2034 3034 ..}.HTTP/1.1.404
0x0040: 204e 6f74 2046 6f75 6e64 0d0a 4461 7465 .Not.Found..Date
0x0050: 3a20 5765 642c 2032 3420 4f63 7420 3230 :.Mon,.01.Jan.20
0x0060: 3132 2032 323a 3530 3a34 3320 474d 540d 00.00:00:01.GMT.
0x0070: 0a53 6572 7665 723a 2041 7061 6368 652f .Server:.Apache.
0x00c0: 0d0a 436f 6e74 656e 742d 4c65 6e67 7468 ..Content-Length
0x00d0: 3a20 3332 370d 0a43 6f6e 6e65 6374 696f :.327..Connectio
0x00e0: 6e3a 2063 6c6f 7365 0d0a 436f 6e74 656e n:.close..Conten
0x00f0: 742d 5479 7065 3a20 7465 7874 2f68 746d t-Type:.text/htm
0x0100: 6c3b 2063 6861 7273 6574 3d69 736f 2d38 l;.charset=iso-8
0x0110: 3835 392d 310d 0a0d 0a3c 2144 4f43 5459 859-1....<!DOCTY
0x0120: 5045 2048 544d 4c20 5055 424c 4943 2022 PE.HTML.PUBLIC."
0x0130: 2d2f 2f49 4554 462f 2f44 5444 2048 544d -//IETF//DTD.HTM
0x0140: 4c20 322e 302f 2f45 4e22 3e0a 3c68 746d L.2.0//EN">.<htm
0x0150: 6c3e 3c68 6561 643e 0a3c 7469 746c 653e l><head>.<title>
0x0160: 3430 3420 4e6f 7420 466f 756e 643c 2f74 Ooops.Sorry..</t
0x0170: 6974 6c65 3e0a 3c2f 6865 6164 3e3c 626f itle>.</head><bo
0x0180: 6479 3e0a 3c68 313e 4e6f 7420 466f 756e dy>.<h1>Not.Foun
0x0190: 643c 2f68 313e 0a3c 703e 5468 6520 7265 d</h1>.<p>Your.r
0x01a0: 7175 6573 7465 6420 5552 4c20 2f74 6573 quest.could.not
0x01b0: 745f 7061 6765 2e68 746d 6c20 7761 7320 be.completed.by.
0x01c0: 6e6f 7420 666f 756e 6420 6f6e 2074 6869 this.server..Sor
0x01d0: 7320 7365 7276 6572 2e3c 2f70 3e0a 3c68 ry.....</p>.<h
0x01e0: 723e 0a3c 6164 6472 6573 733e 4170 6163 r>.<address>Apac
0x01f0: 6865 2f32 2e32 2e34 2028 5562 756e 7475 he/x.x.x.(xxxxxx
0x0200: 2920 5048 502f 352e 322e 332d 3175 6275 ).PHP/x.x.x-lubu
0x0210: 6e74 7536 2e35 206d 6f64 5f73 736c 2f32 ntu6.5.mod_ssl/2
0x0220: 2e32 2e34 204f 7065 6e53 534c 2f30 2e39 .2.4.OpenSSL/x.x
0x0230: 2e38 6520 5365 7276 6572 2061 7420 2050 .8e.Server.at..P
0x0240: 6f72 7420 3830 3c2f 6164 6472 6573 733e ort.80</address>
0x0250: 0a3c 2f62 6f64 793e 3c2f 6874 6d6c 3e0a .</body></html>.
0x0260: 0105 0101 0002 00 .....

```

-- Exhibit --

Refer to the exhibit.

The decoded TCPDump capture is a trace of a failing health monitor. The health monitor is sending the string shown in the capture; however, the server response is NOT as expected. The receive string is set to 'SERVER IS UP'.

What is the solution?

- A. The GET request Host header field requires a host name.
- B. Incorrect syntax in send string. 'HTTP/1.1' should be 'HTTP1.1'.
- C. The /test_page.html does NOT exist on the web server and should be added.
- D. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

-- Exhibit

Hostname: V11-BigIP-B.local
IP Address: 127.0.0.1

Date: Oct 17, 2012
Time: 1:59 PM (EDT)

User: admin
Role: Administrator



ONLINE (STANDBY)
Changes Pending

Main

Help

About

Welcome



Statistics

Dashboard

Module Statistics

Performance



iApp



Wizards



Global Traffic



Local Traffic



Access Policy



Device Management



Network



System



Setup

Support

User Documentation

Technical documentation for this product, including user guides and release notes, is available on the Ask F5 Technical Support web site.

- [User Documentation](#)

Preferences

On the System Preferences screen, you can customize the general preferences for the Configuration Utility.

- [System Preferences](#)

Additional Setup Options

Use the following additional configuration options to refine the system setup, once you have initially configured the system using the Setup Utility.

- [System Device Certificate](#)
- [DNS](#)
- [NTP](#)
- [SNMP](#)
- [User Authentication](#)

Setup Utility

Run the Setup Utility again to make changes to basic device settings and standard network configuration.

- [Run the Setup Utility](#)

Ask F5

Ask F5 features quick support case generator provides unlimited access

- [Visit Ask F5](#)

Solution Center

The Solution Center features Success Stories, Tutorials

- [Visit the Solution Center](#)

DevCentral

DevCentral provides new techniques, and community forum to share best practices

- [Visit DevCentral](#)

Modules

F5 BIG-IP devices are adaptable to changing applications, security, and other applications

- [Visit BIG-IP Modules](#)

Plug-ins

Downloads

-- Exhibit --

Refer to the exhibit.

Which step should an LTM Specialist take to utilize AVR?

- A. provision AVR
- B. reboot the device
- C. install the AVR add-on
- D. license the device for AVR

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

-- Exhibit

General Configuration

Profile Name	<input type="text" value="avr_example"/>		
Partition / Path	Common		
Parent Profile	<input type="text" value="analytics"/>		
Profile Description	<div></div>		
Statistics Logging Type	<input checked="" type="checkbox"/> Internal <input type="checkbox"/> External		<input checked="" type="checkbox"/>
Traffic Capturing Logging Type	<input type="checkbox"/> Internal <input type="checkbox"/> External		<input checked="" type="checkbox"/>
SMTP Configuration	None (Note: Setting can be changed only through the default analytics profile.)		
Notification Type	<input checked="" type="checkbox"/> Syslog <input type="checkbox"/> SNMP <input type="checkbox"/> E-mail		<input checked="" type="checkbox"/>
Trust XFF	<input checked="" type="checkbox"/> Enable		<input type="checkbox"/>
Transaction Sampling Ratio	Sample all transactions (Note: Setting can be changed only through the default analytics profile.)		

Included Objects

<input type="checkbox"/>	Name	Destination	Service Port	Partition / Path
No records to display.				
<input type="button" value="Add..."/> <input type="button" value="Delete"/>				

Statistics Gathering Configuration

Custom ☐

Collected Metrics	<input checked="" type="checkbox"/> Server Latency <input type="checkbox"/> Page Load Time <input checked="" type="checkbox"/> Throughput <input type="checkbox"/> User Sessions	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Collected Entities	<input type="checkbox"/> URLs <input type="checkbox"/> Countries <input type="checkbox"/> Client IP Addresses <input checked="" type="checkbox"/> Response Codes <input type="checkbox"/> User Agents <input checked="" type="checkbox"/> Methods	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Alerts and Notifications Configuration

Add New Rule	Alert when	<input type="text" value="Average TPS"/>	is	<input type="text" value="below"/>	<input type="text" value=""/>	Trans/sec, for
		<input type="text" value=""/>	seconds in	<input type="text" value="an Application"/>	<input type="button" value="Add"/>	
	<input type="checkbox"/>	<input type="text" value="Rule"/>			<input type="button" value="Edit"/>	

-- Exhibit --

Refer to the exhibit.

An LTM Specialist sets up AVR alerts and notifications for a specific virtual server if the server latency exceeds 50ms. The LTM Specialist simulates a fault so that the server latency is consistently exceeding the 50ms threshold; however, no alerts are being received.

Which configuration should the LTM Specialist modify to achieve the expected results?

- A. The rule should be adjusted to trigger when server latency is above 50ms.
- B. SNMP alerting should be enabled to allow e-mail to be sent to the support team.
- C. User Agents needs to be enabled to ensure the correct information is collected to trigger the alert.
- D. The metric "Page Load Time" needs to be enabled to ensure that the correct information is collected.

Correct Answer: A

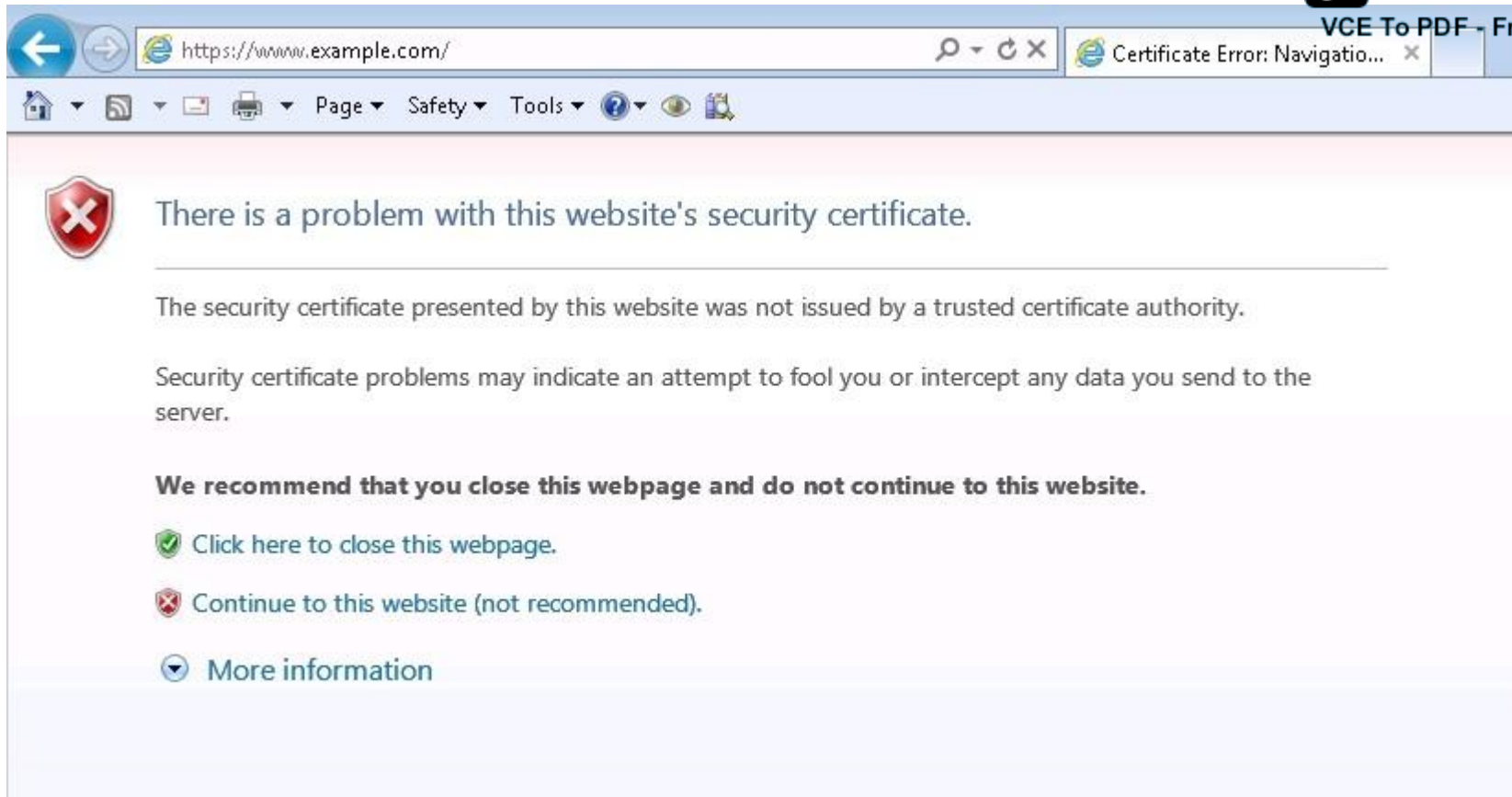
Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

-- Exhibit



```
15:36:14.385939 IP 192.168.1.216.35137 > 192.168.1.1.80: S 379008507:379008507(0) win 14600 <mss 1460,sackOK,timestamp 2
E..<7f@.@...,.....A.P..5.....9.....
.g.1.....
15:36:14.387168 IP 192.168.1.1.80 > 192.168.1.216.35137: S 2457418989:2457418989(0) ack 379008508 win 65535 <mss 1460,nop
E..<.I@.@..H.....P.A.y<...5.....
..pJ.g.1.....
15:36:14.387504 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1 win 115 <nop,nop,timestamp 2322043443 2864934986> out s
E..47g@.@...3.....A.P..5..y<....s.....
.g.3..pJ.....
15:36:14.387833 IP 192.168.1.216.35137 > 192.168.1.1.80: P 1:8(7) ack 1 win 115 <nop,nop,timestamp 2322043443 2864934986
E..;7h@.@...+.....A.P..5..y<....s@i.....
.g.3..pJGET /
.....
15:36:14.389329 IP 192.168.1.1.80 > 192.168.1.216.35137: P 1:1216(1215) ack 8 win 8326 <nop,nop,timestamp 2864934988 232
E....M@.@.....P.A.y<...6... .f.....
..pL.g.3
<html><head><title>Load Balancing</title></head><body>
<h2>BIG-IP Load Balancing Test Page</h2>
<br><br>

<table cellpadding="4">
  <tr>
    <td width=35% align=right><b>Server Address:</b></td>
    <td align=left style="color:#347C17"><b>192.168.1.1:80</b></td>
  </tr>
  <tr>
    <td width=35% align=right><b>Client Address:</b></td>
    <td align=left style="color:#800000"><b>192.168.1.216:35137</b></td>
  </tr>
</table>
</body></html>
.....
15:36:14.389333 IP 192.168.1.1.80 > 192.168.1.216.35137: F 1216:1216(0) ack 8 win 8326 <nop,nop,timestamp 2864934989 232
.....N@.@..K.....P.A.yA...6... ..
..pM.g.3.....
15:36:14.390225 IP 192.168.1.216.35137 > 192.168.1.1.80: . ack 1216 win 137 <nop,nop,timestamp 2322043445 2864934988> ou
E..47i@.@...1.....A.P..6..yA.....
.g.5..pL.....
15:36:14.390230 IP 192.168.1.216.35137 > 192.168.1.1.80: F 8:8(0) ack 1217 win 137 <nop,nop,timestamp 2322043445 2864934
E..47j@.@...0.....A.P..6..yA.....
.g.5..pM.....
15:36:14.391575 IP 192.168.1.1.80 > 192.168.1.216.35137: . ack 9 win 8325 <nop,nop,timestamp 2864934990 2322043445> in s
E..4.P@.@...I.....P.A.yA...6... ..
.....
..pN.g.5.....
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an HTTP monitor that is marking a pool member as down. Connecting to the pool member directly through a browser shows the application is up and functioning correctly.

```
ltm monitor http http_mon {  
  defaults-from http  
  destination *:*  
  interval 5  
  recv "200 OK"  
  send "GET /\r\n"  
  time-until-up 0  
  timeout 16  
}
```

What is the issue?

- A. The HTTP headers are compressed.
- B. The pool member is responding with a 404.
- C. The pool member is responding without HTTP headers.
- D. The request is NOT being received by the pool member.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

-- 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-----
MIICGzCCAeygAwIBAgIJAImlXVLJqYzBMA0GCSqGSIb3DQEBBQUAMDYxZjAUBgNV
BAoTDVR1cm5LZXkgTGluZXgHDAaBgNVBASTE1NvZnR3YXJlIGFwcGxpYW5jZXMw
HhcNMTAwNDE1MTkxNDQzWhcNMjAwNDEyMTkxNDQzWjA2MRYwFAYDVQQKEw1UdXJu
S2V5IExpbnV4MRwwGgYDVQQLEExNTb2Z0d2FyZSBhcHBsaWFuY2VzMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCvlgendrRHsavr6R+/M/xYyooMJVpXWZbzeKu04ro
eudY0KOWwa2zF9jaD0HDIJ3MtnVYAHMSHZvqoolQ8EfohP85RfHrO4kMxtvAefm
slqGE7MkmIxLtwYjjWXmwxW7sCFL19kt6pFOatzqeK3WxbDM5yF/RTHF4R/vyKQI
2lyf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBERG5CDKtOlkiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMAW5leDEcMBoGA1UECXMtU29mdHdhcmUgYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAWGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEANo2TuXFVZKwG
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhpl
RGH2+IqwgLEPB7K6eudRy0D9GqzMhZrdMo9d3ewPB3BqjOrPhs5yRTgNrZHyasJr
ZAiCzekf24SwNpmhfHyam88N2+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: F457C0A12201A70C4E65511A1CD35D7738B1073068D7DB164E2D7413D4487ACC
```

-- Exhibit --

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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

-- Exhibit

New TCP connection #1: 10.1.1.1(32021) <-> 10.1.1.2(443)

```

1 1 1351011538.3477 (0.1562) C>S Handshake
    ClientHello
        Version 3.0
        cipher suites
        SSL_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA
        SSL_DHE_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_AES_256_CBC_SHA
        SSL_RSA_WITH_CAMELLIA_256_CBC_SHA
        SSL_RSA_WITH_AES_256_CBC_SHA
        SSL_DHE_DSS_WITH_RC4_128_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_DSS_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_AES_128_CBC_SHA256
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_AES_128_CBC_SHA
        SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
        NULL
1 2 1351011538.3477 (0.0000) S>C Handshake
    ServerHello
        Version 3.0
        session_id[0]=

        cipherSuite          SSL_RSA_WITH_RC4_128_SHA
        compressionMethod    NULL
1 3 1351011538.3477 (0.0000) S>C Handshake
    Certificate
1 4 1351011538.3477 (0.0000) S>C Handshake
    CertificateRequest
        certificate_types          rsa_sign
        certificate_authority
        30 81 98 31 0b 30 09 06 03 55 04 06 13 02 55 53
        31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
        0e 06 03 55 04 07 01 07 53 65 61 74 74 6c 65 31
        12 30 10 06 03 55 04 0a 13 09 4d 79 43 6f 6d 70
        61 6e 79 31 0b 30 09 06 03 55 04 0b 13 02 49 54
        31 1e 30 df 06 03 55 04 03 13 15 6c 6f 63 61 6c
        68 6f 73 74 2e 6c 6f 63 61 6c 64 6f 6d 61 69 6e
        31 29 30 27 06 09 2a 86 48 86 f7 0d 01 09 01 16
        1a 72 6f 6f 74 40 6c 6f 63 61 6c 68 6f 73 74 2e
  
```


-- Exhibit --

Refer to the exhibit.

A user is unable to access a secure application via a virtual server.

What is the cause of the issue?

- A. The client authentication failed.
- B. The virtual server does NOT have a pool configured.
- C. The client and server CANNOT agree on a common cipher.
- D. The virtual server does NOT have a client SSL profile configured.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 161

-- Exhibit

```
ltm pool srv1_https_pool {  
    members {  
        192.168.2.1:https {  
            address 192.168.2.1  
        }  
    }  
}  
  
ltm virtual https_example_vs {  
    destination 192.168.1.155:https  
    ip-protocol tcp  
    mask 255.255.255.255  
    pool srv1_https_pool  
    profiles {  
        http { }  
        tcp { }  
    }  
    snat automap  
    vlans-disabled  
}
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "The connection was reset" in the browser. Connections directly to the pool member show the application is functioning correctly.

What is the issue?

- A. The pool member is failing the monitor check.
- B. The pool member default gateway is set incorrectly.
- C. The virtual server is configured with the incorrect SNAT address.
- D. The virtual server is processing encrypted traffic as plain-text HTTP.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 162

-- Exhibit

```
ltm node 192.168.2.1 {  
    address 192.168.2.1  
    session user-disabled  
    state up  
}  
ltm pool srv1_http_pool {  
    members {  
        192.168.2.1:http {  
            address 192.168.2.1  
        }  
    }  
}  
ltm profile http http-example {  
    app-service none  
    defaults-from http  
    header-erase Accept-Encoding  
    via-host-name ltm_prod.example.com  
    via-request append  
}  
ltm virtual srv1_http_vs {  
    destination 192.168.1.155:http  
    ip-protocol tcp  
    mask 255.255.255.255  
    pool srv1_http_pool  
    profiles {  
        http-example { }  
        tcp { }  
    }  
    vlans-disabled  
}
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting a virtual server. Both the virtual server and the pool are showing blue squares for their statuses, and new clients report receiving "The connection was reset" through their browsers. Connections directly to the pool member are successful.

What is the issue?

- A. The pool member is disabled.
- B. The node is marked as disabled.
- C. The HTTP profile has incorrect settings.
- D. The virtual server is disabled on all VLANs.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

-- Exhibit

```
21:48:50.118288 IP 10.0.0.2.49662 > 10.0.0.1.http: S 2982039927:2982039927(0) win 8192
21:48:50.118323 IP 10.0.0.1.http > 10.0.0.2.49662: S 4109615223:4109615223(0) ack 2982039928 win 4248
21:48:50.278582 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 1 win 16638 in slot1/tmm2 lis=/Common/test-vs
21:48:50.280165 IP 10.0.0.2.49662 > 10.0.0.1.http: P 1:560(559) ack 1 win 16638 in slot1/tmm2 lis=/Common/test-vs
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg
Accept-Language: en-GB
User-Agent: Mozilla/4.0
Accept-Encoding: gzip, deflate
Host: 10.0.0.1
Connection: Keep-Alive
21:48:50.280270 IP 10.0.0.1.http > 10.0.0.2.49662: . ack 560 win 4807 out slot1/tmm2 lis=/Common/test-vs
21:48:50.283344 IP 10.0.0.1.http > 10.0.0.2.49662: P 1:122(121) ack 560 win 4807 out slot1/tmm2 lis=/Common/test-vs
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm=""
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
21:48:50.642340 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 122 win 16607 in slot1/tmm2 lis=/Common/test-vs
21:48:54.676670 IP 10.0.0.2.49662 > 10.0.0.1.http: P 560:1158(598) ack 122 win 16607 in slot1/tmm2 lis=/Common/test-vs
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg
Accept-Language: en-GB
User-Agent: Mozilla/4.0
Accept-Encoding: gzip, deflate
Host: 10.0.0.1
Connection: Keep-Alive
Authorization: Basic YWRtaW46YWRtaW4=
21:48:54.676781 IP 10.0.0.1.http > 10.0.0.2.49662: . ack 1158 win 5405 out slot1/tmm2 lis=/Common/test-vs
21:48:54.679242 IP 10.0.0.1.http > 10.0.0.2.49662: P 122:243(121) ack 1158 win 5405 out slot1/tmm2 lis=/Common/test-vs
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm=""
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
21:48:55.031314 IP 10.0.0.2.49662 > 10.0.0.1.http: . ack 243 win 16577 in slot1/tmm2 lis=/Common/test-vs
```

-- Exhibit --

Refer to the exhibit.

A user is unable to access an application.

What is the root cause of the problem?

- A. The User-Agent is incorrect.
- B. The 'Content-Length' is zero.
- C. The user failed authentication.
- D. The GET request uses the wrong syntax.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

-- Exhibit

```
ltm monitor http memberA_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberB_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberC_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an HTTP monitor that is marking a pool member as down. Connecting to the pool member directly through a browser shows the application is up and functioning correctly.

How should the send string be modified to correct this issue?

- A. GET /\r\n\r\n
- B. GET / HTTP/1.0\r\n\r\n
- C. GET /\r\nHost: \r\n\r\n
- D. GET /\r\nHTTP/1.0\r\n\r\n

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 165

-- Exhibit


```
19:29:38.095440 IP 10.0.0.2.15885 > 10.0.0.1.http: S 233558736:233558736(0) win 8192 <mss 1416,nop,wscale 2,nop,nop,sack
  0x0000: 0b71 0800 4500 0034 35b8 4000 7606 5844 .q..E..45.@.v.XD
  0x0010: ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d0 ...N...K>..P....
  0x0020: 0000 0000 8002 2000 b961 0000 0204 0588 .....a.....
  0x0030: 0103 0302 0101 0402 0105 0101 0001 00 .....
19:29:38.095485 IP 10.0.0.1.http > 10.0.0.2.15885: S 2486948624:2486948624(0) ack 233558737 win 4248 <mss 1460,nop,wscal
  0x0000: 0b71 0800 4500 0034 a9d4 4000 ff06 5b27 .q..E..4...@...['
  0x0010: ac1d 1d4b ac11 014e 0050 3e0d 943b d310 ...K...N.P>...;..
  0x0020: 0deb d2d1 8012 1098 6243 0000 0204 05b4 .....bC.....
  0x0030: 0103 0300 0402 0000 011c 0100 0001 172f ...../
  0x0040: 436f 6d6d 6f6e 2f61 7263 682d 6263 6172 Common/test-vs

19:29:38.251761 IP 10.0.0.2.15885 > 10.0.0.1.http: . ack 1 win 16638 in slot1/tnml lis=/Common/test-vs
  0x0000: 0b71 0800 4500 0028 35d9 4000 7706 572f .q..E..(5.@.w.W/
  0x0010: ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d1 ...N...K>..P....
  0x0020: 943b d311 5010 40fe 71a7 0000 011c 0101 .;..P.@.q.....
  0x0030: 0001 172f 436f 6d6d 6f6e 2f61 7263 682d .../Common/arch-
  0x0040: 6263 6172 642d 7465 7374 bcard-test

19:29:38.252723 IP 10.0.0.2.15885 > 10.0.0.1.http: P 1:426(425) ack 1 win 16638 in slot1/tnml lis=/Common/test-vs
  0x0000: 0b71 0800 4500 01d1 35da 4000 7706 5585 .q..E...5.@.w.U.
  0x0010: ac11 014e ac1d 1d4b 3e0d 0050 0deb d2d1 ...N...K>..P....
  0x0020: 943b d311 5018 40fe 558e 0000 4745 5420 .;..P.@.U...GET.
  0x0030: 2f42 4947 2d49 505f 4d6f 6475 6c65 5f49 /some-file-name.
  0x0060: 7064 6620 4854 5450 2f31 2e31 0d0a 4163 pdf.HTTP/1.1..Ac
  0x0070: 6365 7074 3a20 2a2f 2a0d 0a52 616e 6765 cept:..*/*..Range
  0x0080: 3a20 6279 7465 733d 3234 3537 3630 2d32 :.bytes=245760-2
  0x0090: 3632 3134 330d 0a41 6363 6570 742d 456e 62143..Accept-En
  0x00a0: 636f 6469 6e67 3a20 677a 6970 2c20 6465 coding:.gzip,.de
  0x00b0: 666c 6174 650d 0a55 7365 722d 4167 656e flate..User-Agen
  0x00c0: 743a 204d 6f7a 696c 6c61 2f34 2e30 2028 t:.Mozilla/4.0.(
  0x00d0: 636f 6d70 6174 6962 6c65 3b20 4d53 4945 compatible;.MSIE
  0x00e0: 2038 2e30 3b20 5769 6e64 6f77 7320 4e54 .8.0;.Windows.NT
  0x00f0: 2036 2e31 3b20 574f 5736 343b 2054 7269 .6.1;.WOW64;.Tri
  0x0100: 6465 6e74 2f34 2e30 3b20 534c 4343 323b dent/4.0;.SLCC2;
  0x0110: 202e 4e45 5420 434c 5220 322e 302e 3530 ..NET.CLR.2.0.50
  0x0120: 3732 373b 202e 4e45 5420 434c 5220 332e 727;.NET.CLR.3.
  0x0130: 352e 3330 3732 393b 202e 4e45 5420 434c 5.30729;.NET.CL
  0x0140: 5220 332e 302e 3330 3732 393b 204d 6564 R.3.0.30729;.Med
  0x0150: 6961 2043 656e 7465 7220 5043 2036 2e30 ia.Center.PC.6.0
  0x0160: 3b20 2e4e 4554 342e 3043 3b20 496e 666f ;.NET4.0C;.Info
  0x0170: 5061 7468 2e33 3b20 2e4e 4554 342e 3045 Path.3;.NET4.0E
  0x0180: 3b20 4d53 2d52 5443 204c 4d20 383b 2041 ;.MS-RTC.LM.8;.A
  0x0190: 736b 5462 4f52 4a2f 352e 3135 2e31 2e32 skTbORJ/5.15.1.2
  0x01a0: 3232 3239 290d 0a48 6f73 743a 2031 3732 2229)..Host:.10.
  0x01b0: 2e32 392e 3239 2e37 350d 0a43 6f6e 6e65 0.0.1.....Conne
```

-- Exhibit --

Refer to the exhibit.

A user is unable to access an HTTP application via a virtual server.

What is the cause of the failure?

- A. The host header requires a host name.
- B. The virtual server is in the disabled state.
- C. The Connection: Keep-Alive header is set.
- D. There is no pool member available to service the request.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

-- Exhibit

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
```

```
HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Location: https://www.example.com
Date: Tue, 23 Oct 2012 18:05:57 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: sessionId=a4531785-7012-46aa-b5fe-a54be482b61a; path=/
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is performing an HTTP trace on the client side of the LTM device and notices there are many undesired headers being sent by the server in the response. The LTM Specialist wants to remove all response headers except "Set-Cookie" and "Location."

How should the LTM Specialist modify the HTTP profile to remove undesired headers from the HTTP response?

- A. Enter the desired header names in the 'Request Header Insert' field.
- B. Enter the undesired header names in the 'Request Header Erase' field.
- C. Enter the undesired header names in the 'Response Header Erase' field.
- D. Enter the desired header names in the 'Response Headers Allowed' field.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 167

-- Exhibit

```
ltm pool /Common/pool_lamp_http {
    load-balancing-mode least-connections-member
    members {
        /Common/Server_lamp_1:80 {
            address 172.16.20.1
        }
        /Common/Server_lamp_2:80 {
            address 172.16.20.2
        }
        /Common/Server_lamp_3:80 {
            address 172.16.20.3
        }
    }
    monitor /Common/http
}
ltm virtual /Common/vs_http_lamp {
    destination /Common/10.0.20.88:80
    ip-protocol tcp
    mask 255.255.255.255
    pool /Common/pool_lamp_http
    profiles {
        /Common/http { }
        /Common/tcp { }
    }
    translate-address enabled
    translate-port enabled
    vlans-disabled
}
```

-- Exhibit --

Refer to the exhibit.

Users report that a web application works incorrectly. Sometimes contextual data displayed on the web pages is accurate; other times it is inaccurate.

The LTM administrator looks at the connection table with a filter on one of the client IP addresses currently connected using the command "tmsh show sys connection cs-client-addr 10.0.20.1" with the following results:

```
10.0.20.1:60048 10.0.20.88:80 10.0.20.1:60048 172.16.20.1:80 tcp 3 (tmm: 0) 10.0.20.1:60050 10.0.20.88:80 10.0.20.1:60050 172.16.20.3:80 tcp 3 (tmm: 0) 10.0.20.1:60047 10.0.20.88:80 10.0.20.1:60047 172.16.20.2:80 tcp 3 (tmm: 0) 10.0.20.1:60049 10.0.20.88:80 10.0.20.1:60049 172.16.20.1:80 tcp 3 (tmm: 0)
```

What is the solution to the problem?

- A. Synchronize the clock of the LTM device with NTP.
- B. Modify the load balancing method attached to the pool.
- C. Set up an HTTP cookie insert profile in the virtual server.
- D. Modify the setup of the monitor bound to the pool used by the application.

Correct Answer: C

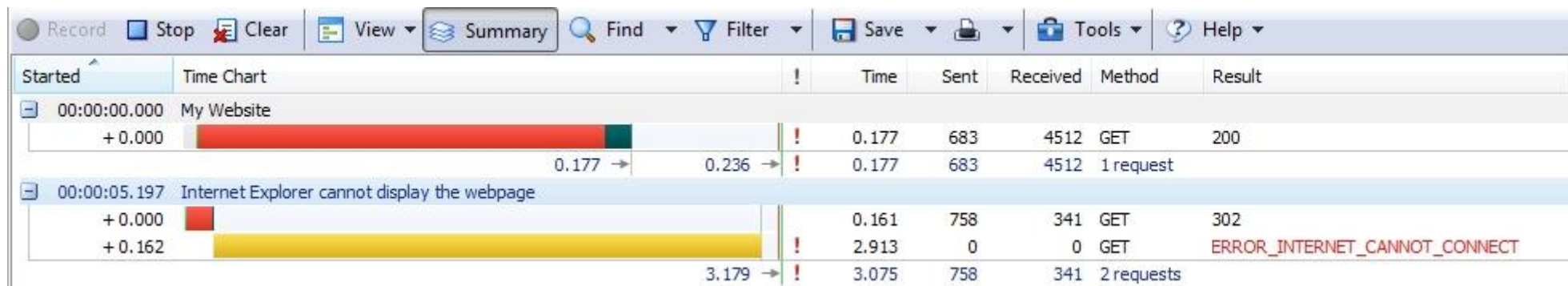
Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

-- Exhibit



-- Exhibit --

Refer to the exhibit.

The virtual server is listening on port 443.

What is the solution to the problem?

- A. Add an SSL Client profile to the existing virtual server.
- B. Modify the virtual server HTTP Profile to 'Redirect RewritE. All'.
- C. Modify the virtual server TCP profile to disable Nagle's Algorithm.
- D. Modify the virtual server HTTP Profile to 'Redirect RewritE. Matching'.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 169

-- Exhibit

Direct to application server:

Request:

GET / HTTP/1.1

Host: 172.16.20.21

Connection: keep-alive

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 200 OK

Date: Wed, 24 Oct 2012 19:11:46 GMT

Server: Apache/2.2.22 (Ubuntu)

Last-Modified: Fri, 08 Jun 2012 13:32:31 GMT

ETag: "a0b21-b1-4cif608458836"

Accept-Ranges: bytes

Content-Length: 177

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Through LTM:

Request:

GET / HTTP/1.1

Host: www.example.com

Connection: keep-alive

Cache-Control: max-age=0

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 301 Moved Permanently

Date: Wed, 24 Oct 2012 19:17:47 GMT

Server: Apache/2.2.22 (Ubuntu)

Location: https://www.example.com/

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=iso-8859-1

Transfer-Encoding: chunked

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has created a virtual server to balance connections to a pool of application servers and offload SSL decryption. Clients connect to the application at <https://www.example.com/>. The virtual server is configured with a clientssl profile but no serverssl profile. The application servers are listening on ports 80 and 443. Users are unable to connect to the application through the virtual server but are able to connect directly to the application server.

What is the root cause of the error?

- A. The LTM device is chunking responses.
- B. The LTM device is redirecting users to HTTPS.
- C. The pool members are configured with the wrong port.
- D. The application servers are redirecting users to HTTPS.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 170

-- Exhibit

Through LTM Device:
 New TCP connection #1: 172.16.1.3(63936) <-> 172.16.20.21(443)

```

1 1 0.0013 (0.0013) 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
        TLS_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_AES_256_CBC_SHA256
      Unknown value 0xff
      compression methods
        NULL
1 2 0.0038 (0.0025) S>C Handshake
    ServerHello
      Version 3.1
      session_id[32]=
        7c 00 d2 cf 81 f8 cd ab 6b 48 c0 9a cc 19 df f7
        12 5f f2 c8 2a a2 e8 ef 1e f1 10 41 61 99 6d 27
      cipherSuite      TLS_RSA_WITH_RC4_128_SHA
      compressionMethod NULL
1 3 0.0038 (0.0000) S>C Handshake
    Certificate
1 4 0.0038 (0.0000) S>C Handshake
    CertificateRequest
      certificate_types      rsa_sign
      certificate_types      dss_sign
      certificate_types      unknown value
      certificate_authority
        30 81 90 31 0b 30 09 06 03 55 04 06 13 02 55 53
        31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
        0e 06 03 55 04 07 13 07 53 65 61 74 74 6c 65 31
        14 30 12 06 03 55 04 0a 13 0b 45 78 61 6d 70 6c
        65 2e 43 6f 6d 31 14 30 12 06 03 55 04 0b 13 0b
        45 6e 67 69 6e 65 65 72 69 6e 67 31 36 30 34 06
        03 55 04 03 13 2d 43 4e 3d 4a 6f 68 6e 20 55 73
        65 72 2c 4f 55 3d 45 6e 67 69 6e 65 65 72 69 6e
        67 2c 44 43 3d 65 78 61 6d 70 6c 65 2c 44 43 3d
        63 6f 6d
      ServerHelloDone
1 5 0.0040 (0.0002) C>S Handshake
    Certificate
1 6 0.0042 (0.0002) C>S Handshake
  
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has created a virtual server to load balance traffic to a pool of HTTPS servers. The servers use client certificates for user authentication. The virtual server has clientssl, serverssl, and http profiles enabled. Clients are unable to connect to the application through the virtual server. Clients are able to connect to the application servers directly.

What is the root cause of the problem?

- A. The application server does NOT support 2048-bit keys.
- B. The clientssl profile is NOT set to require a client certificate.
- C. The LTM device does NOT trust the issuing CA of the client certificate.
- D. The application server does NOT see the client certificate due to SSL offload.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 171

-- Exhibit

Client side of LTM Device:

```
GET / HTTP/1.1
User-Agent: curl/7.21.0 (i486-pc-linux-gnu) libcurl/7.21.0 OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.15 libssh2/1.2.6
Host: 172.16.80.80
Accept: */*
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Oct 2012 16:17:21 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Tue, 23 Oct 2012 16:14:06 GMT
ETag: "17f655-1d-4ccbc425aaf80"
Accept-Ranges: bytes
Content-Length: 29
Vary: Accept-Encoding
Content-Type: text/html
X-Pad: avoid browser bug
Set-Cookie: BIGipServermy_http_pool=1679034890.20480.0000; path=/
```

Server side of LTM device:

```
GET / HTTP/1.1
User-Agent: curl/7.21.0 (i486-pc-linux-gnu) libcurl/7.21.0 OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.15 libssh2/1.2.6
Host: 172.16.80.80
Accept: */*
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Oct 2012 16:17:21 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Tue, 23 Oct 2012 16:14:06 GMT
ETag: "17f655-1d-4ccbc425aaf80"
Accept-Ranges: bytes
Content-Length: 29
Vary: Accept-Encoding
Content-Type: text/html
X-Pad: avoid browser bug
```

-- Exhibit --

Refer to the exhibit.

A web application is configured to allow sessions to continue even after a user computer is shut down for the night. A new LTM device is configured to load balance the web application to several servers. The application owner reports that application users are logged out of the web application whenever their browser is restarted or computer is rebooted.

What is the problem?

- A. The virtual server does NOT have persistence configured.
- B. The virtual server does NOT have persistence mirroring configured.
- C. The cookie set by the LTM device does NOT have an "Expires" value.
- D. The cookie set by the server is NOT being passed to client by the LTM device.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 172

-- Exhibit

Through LTM Device:

New TCP connection #1: 172.16.1.3(63936) <-> 172.16.20.21(443)

```

1 1 0.0013 (0.0013) 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
        TLS_RSA_WITH_AES_128_CBC_SHA256
        TLS_RSA_WITH_AES_256_CBC_SHA256
        Unknown value 0xff
        compression methods
            NULL
1 2 0.0038 (0.0025) S>C Handshake
    ServerHello
        Version 3.1
        session_id[32]=
            7c 00 d2 cf 81 f8 cd ab 6b 48 c0 9a cc 19 df f7
            12 5f f2 c8 2a a2 e8 ef 1e f1 10 41 61 99 6d 27
        cipherSuite      TLS_RSA_WITH_RC4_128_SHA
        compressionMethod
            NULL
1 3 0.0038 (0.0000) S>C Handshake
    Certificate
1 4 0.0038 (0.0000) S>C Handshake
    CertificateRequest
        certificate_types      rsa_sign
        certificate_types      dss_sign
        certificate_types      unknown value
        certificate_authority
            30 81 90 31 0b 30 09 06 03 55 04 06 13 02 55 53
            31 0b 30 09 06 03 55 04 08 13 02 57 41 31 10 30
            0e 06 03 55 04 07 13 07 53 65 61 74 74 6c 65 31
            14 30 12 06 03 55 04 0a 13 0b 45 78 61 6d 70 6c
            65 2e 43 6f 6d 31 14 30 12 06 03 55 04 0b 13 0b
            45 6e 67 69 6e 65 65 72 69 6e 67 31 36 30 34 06
            03 55 04 03 13 2d 43 4e 3d 4a 6f 68 6e 20 55 73
            65 72 2c 4f 55 3d 45 6e 67 69 6e 65 65 72 69 6e
            67 2c 44 43 3d 65 78 61 6d 70 6c 65 2c 44 43 3d
            63 6f 6d
        ServerHelloDone
1 5 0.0040 (0.0002) C>S Handshake
    Certificate
1 6 0.0040 (0.0000) C>S Handshake
    ClientKeyExchange
  
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist creates a virtual server to load balance traffic to a pool of HTTPS servers. The servers use client certificates for user authentication. The virtual server has clientssl, serverssl, and http profiles enabled. Clients are unable to connect to the application through the virtual server, but they are able to connect to the application servers directly.

Which change to the LTM device configuration will resolve the problem?

- A. Install the server certificate/key and enable Proxy SSL.
- B. Use the serverssl-insecure-compatible serverssl profile.
- C. Configure the clientssl profile to require a client certificate.
- D. Install the client's issuing Certificate Authority certificate on the LTM device.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 173

-- Exhibit

Client IP address: 10.0.0.1
Virtual Server: 11.0.0.1
Web Server: 12.0.0.1

Capture taken on Web server interface eth1:12.0.0.1

```
01:35:35.141396 IP 10.0.0.1.35285 > 12.0.0.1.http: S 3230388980:3230388980(0) win 8192 <mss 1416,nop,wscale 8,nop,nop,sackOK,eol>
01:35:35.141466 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,eol>
01:35:35.177621 IP 10.0.0.1.25079 > 12.0.0.1.http: P 3570570638:3570571021(383) ack 1931745822 win 255
01:35:35.184475 IP 12.0.0.1.http > 10.0.0.1.25079: . 1:1417(1416) ack 383 win 700
01:35:35.184517 IP 12.0.0.1.http > 10.0.0.1.25079: . 1417:2833(1416) ack 383 win 700
01:35:35.184533 IP 12.0.0.1.http > 10.0.0.1.25079: P 2833:3905(1072) ack 383 win 700
01:35:35.297647 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66
01:35:35.337992 IP 10.0.0.1.25079 > 12.0.0.1.http: . ack 2833 win 259
01:35:35.539349 IP 10.0.0.1.25079 > 12.0.0.1.http: . ack 3905 win 255
01:35:38.945404 IP 12.0.0.1.http > 10.0.0.1.35285: S 2242263384:2242263384(0) ack 3230388981 win 5840 <mss 1460,nop,nop,sackOK,eol>
01:35:39.096377 IP 10.0.0.1.35285 > 12.0.0.1.http: . ack 1 win 66 <nop,nop,sack 1 {0:1}>
```

Capture taken on LTM interface 0.0

```
17:32:30.828126 IP 10.0.0.1.10120 > 11.0.0.1.http: S 3414174673:3414174673(0) win 8192 <mss 1416,nop,wscale 2,nop,nop,sackOK,eol>
17:32:30.828172 IP 11.0.0.1.http > 10.0.0.1.10120: S 1751596785:1751596785(0) ack 3414174674 win 4248 <mss 1460,nop,wscale 0,sackOK,eol>
17:32:30.981747 IP 10.0.0.1.10120 > 11.0.0.1.http: . ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982820 IP 10.0.0.1.10120 > 11.0.0.1.http: P 1:560(559) ack 1 win 16638 in slot1/tmm0 lis=/Common/my_virtual
17:32:30.982871 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
17:32:30.982878 IP 11.0.0.1.http > 10.0.0.1.10120: . ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
17:32:33.982895 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
17:32:37.182627 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
17:32:40.382728 IP 10.0.0.1.10120 > 12.0.0.1.http: S 2896210787:2896210787(0) win 4380 <mss 1460,sackOK,eol> out slot1/tmm0
17:32:43.582864 IP 11.0.0.1.http > 10.0.0.1.10120: R 1:55(54) ack 560 win 4807 out slot1/tmm0 lis=/Common/my_virtual
```

-- Exhibit --

Refer to the exhibit.

A pair of LTM devices are configured for HA. The LTM Specialist observes from a capture that there is a successful connection from a client directly to a web server and an unsuccessful connection from a client via the LTM device to the same web server.

Which two solutions will solve the configuration problem? (Choose two.)

- A. Configure SNAT on the pool.
- B. Configure SNAT on the virtual server.
- C. Change server default gateway to point at LTM internal self IP.
- D. Change server default gateway to point at LTM internal floating IP.

Correct Answer: BD

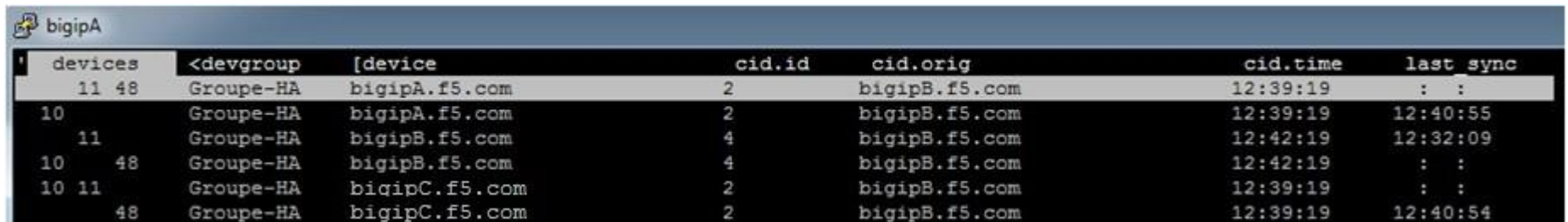
Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

-- Exhibit



devices	<devgroup	[device	cid.id	cid.orig	cid.time	last sync
11 48	Groupe-HA	bigipA.f5.com	2	bigipB.f5.com	12:39:19	: :
10	Groupe-HA	bigipA.f5.com	2	bigipB.f5.com	12:39:19	12:40:55
11	Groupe-HA	bigipB.f5.com	4	bigipB.f5.com	12:42:19	12:32:09
10 48	Groupe-HA	bigipB.f5.com	4	bigipB.f5.com	12:42:19	: :
10 11	Groupe-HA	bigipC.f5.com	2	bigipB.f5.com	12:39:19	: :
48	Groupe-HA	bigipC.f5.com	2	bigipB.f5.com	12:39:19	12:40:54

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting a sync-failover group of three BIG-IP LTM devices. The command used is "tmsh run cm watch-devicegroup-device."

What does the output mean?

- A. Configuration is synchronized between all the devices.
- B. Configuration is not synchronized. Some modifications have been done on bigipA.
- C. Configuration is not synchronized. Some modifications have been done on bigipB.
- D. Configuration is not synchronized. Some modifications have been done on bigipC.

Correct Answer: C
 Section: (none)
 Explanation

Explanation/Reference:

QUESTION 175

-- Exhibit

Net::Interface															
Name	Status	Mac-Addr	MTU	Bits In	Bits Out	Pkts In	Pkts Out	Mcast In	Mcast Out	Drops In	Drops Out	Errs In	Errs Out	Colli sions	Me
1.1	up	0:1:d7:a8:4d:c4	1500	275.3G	43.1G	62.7M	30.8M	7.3M	246	223.9M	0	0	0	0	1000T
1.2	down	0:1:d7:a8:4d:c5	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.3	down	0:1:d7:a8:4d:c6	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.4	down	0:1:d7:a8:4d:c7	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.5	down	0:1:d7:a8:4d:c8	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.6	down	0:1:d7:a8:4d:c9	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.7	down	0:1:d7:a8:4d:ca	1500	0	0	0	0	0	0	0	0	0	0	0	n
1.8	down	0:1:d7:a8:4d:cb	1500	0	0	0	0	0	0	0	0	0	0	0	n
2.1	miss	0:1:d7:a8:4d:cc	1500	0	0	0	0	0	0	0	0	0	0	0	n
2.2	miss	0:1:d7:a8:4d:cd	1500	0	0	0	0	0	0	0	0	0	0	0	n
mgmt	up	0:1:d7:a8:4d:c1	1500	76.6G	138.1G	113.8M	22.5M	6.4M	123	0	0	2.2M	0	2.2M	100TX

-- Exhibit --

Refer to the exhibit.

Based on the output of the tmsh interface show command, what is the issue?

- A. There is a duplex mismatch on the management interface.
- B. Interfaces 2.1 and 2.2 are defective and need replacement.
- C. Flow Control is NOT configured on the management interface.
- D. There are too many drops on inbound traffic on interface 1.1.

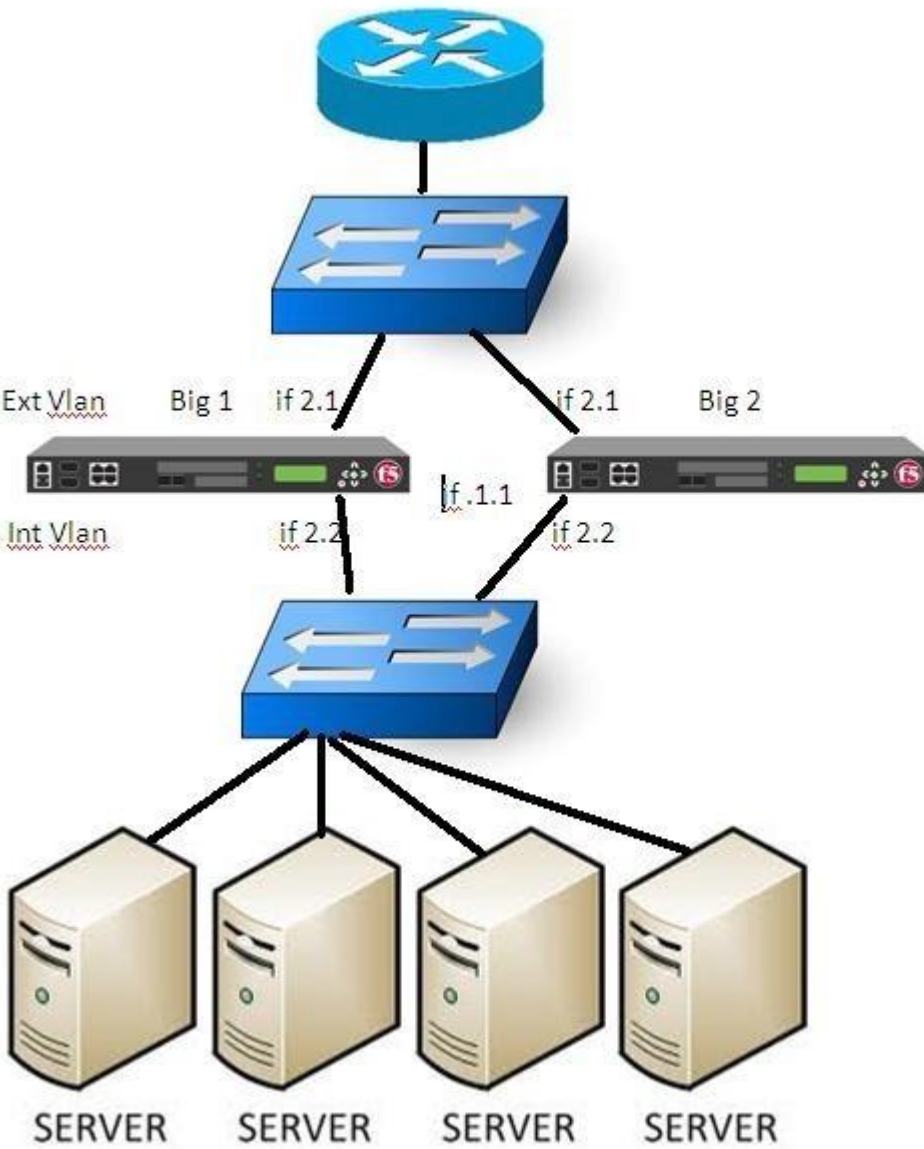
Correct Answer: A
 Section: (none)

Explanation

Explanation/Reference:

QUESTION 176

-- Exhibit



-- Exhibit --

Refer to the exhibit.

A failover has just occurred 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 177

-- Exhibit

```
ltm node /Common/192.168.44.1 {
    address 192.168.44.1
}
ltm node /Common/192.168.44.2 {
    address 192.168.44.2
}
ltm pool /Common/bigip1_gw_pool {
    gateway-failsafe-device /Common/BIGIP1.example.com
    members {
        /Common/192.168.44.1:0 {
            address 192.168.44.1
        }
    }
    min-up-members 1
    min-up-members-checking enabled
    monitor /Common/icmp_gw_monitor
}
ltm pool /Common/bigip2_gw_pool {
    gateway-failsafe-device /Common/BIGIP2.example.com
    members {
        /Common/192.168.44.2:0 {
            address 192.168.44.2
        }
    }
    min-up-members 1
    min-up-members-checking enabled
    monitor /Common/icmp_gw_monitor
}
ltm monitor gateway-icmp /Common/icmp_gw_monitor {
    defaults-from /Common/gateway_icmp
    destination 1.2.2.254:*
    interval 5
    time-until-up 0
    timeout 16
}
net route /Common/external_default_gateway {
    gw 192.168.44.1
    network default
}
```

-- Exhibit --

Refer to the exhibit.

A pair of LTM devices are deployed in a high-availability (HA) pair as the diagram shows. After inserting a new rule on the firewalls, the LTM devices become Standby. The rule drops all outbound sessions to the Internet. Only inbound connections are allowed from the Internet. There are no other changes to the environment.

What triggered the LTM device failover?

- A. HA Group
- B. Auto Failback
- C. VLAN Failsafe
- D. Gateway Failsafe

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 178

-- Exhibit

```
ltm pool /Common/my_admin_pool {
  members {
    /Common/10.0.0.1:80 {
      address 10.0.0.1
    }
    /Common/10.0.0.2:80 {
      address 10.0.0.2
    }
  }
}

ltm pool /Common/my_default_pool {
  members {
    /Common/10.0.0.4:80 {
      address 10.0.0.4
    }
    /Common/10.0.0.5:80 {
      address 10.0.0.5
    }
  }
}

ltm virtual /Common/my_virtual_server {
  destination /Common/10.0.0.1:80
  ip-protocol tcp
  mask 255.255.255.255
  pool /Common/my_default_pool
  profiles {
    /Common/http { }
    /Common/tcp { }
  }
  rules {
    /Common/my_iRule
  }
  snat automap
}

sys ha-group my_ha_group {
  active-bonus 10
  pools {
    /Common/my_default_pool {
      threshold 2
      weight 20
    }
  }
}

trunks {
  my_trunk {
    10.0.0.1:10000
  }
}
```

-- Exhibit --

Refer to the exhibit.

A pair of LTM devices is configured for HA.

What happens if the pool member server with IP address 10.0.0.4 becomes totally unresponsive to the active LTM device, but is still responsive to the standby LTM device?

- A. The HA-group will disable the trunk my_trunk.
- B. The HTTP application will be unavailable via the LTM device.
- C. The HA-group will initiate a fail-over because the threshold is set to 2.
- D. The HA-group will initiate a fail-over because the HA-Group score will be zero.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 179

-- Exhibit

Virtual Server	Destination	Service Port	Default Pool
intranet_it	10.1.1.10	8080	web_it
intranet_hr	10.1.1.10	443	web_hr
intranet_sales	10.1.1.10	8081	web_sales
intranet_finance	10.1.1.10	8083	web_finance
intranet_engineering	10.1.1.10	8085	web_engineering

Pool	Monitor	Pool Members
web_it	http_it	10.2.2.102, 10.2.2.105
web_hr	https_hr	10.2.2.101, 10.2.2.102
web_sales	http_sales	10.2.2.101, 10.2.2.102
web_finance	http_finance	10.2.2.101, 10.2.2.102
web_engineering	http_engineering	10.2.2.102, 10.2.2.105

-- Exhibit --

Refer to the exhibits.

Every monitor has the same Send String, Recv String, and an Alias of *:. The LTM Specialist simplifies the configuration to minimize the number of monitors.

How many unique monitors remain?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 180

-- Exhibit

```
ltm monitor http memberA_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberB_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
ltm monitor http memberC_mon {
    defaults-from http
    destination *:*
    interval 5
    send "GET /\r\n"
    time-until-up 0
    timeout 16
}
```

```
ltm pool member_pool {  
  members {  
    memberA:http {  
      address 192.168.30.10  
      monitor memberA_mon  
      session monitor-enabled  
      state down  
    }  
    memberB:http {  
      address 192.168.30.20  
      monitor memberB_mon  
      session monitor-enabled  
      state down  
    }  
    memberC:http {  
      address 192.168.30.30  
      monitor memberC_mon  
      session monitor-enabled  
      state down  
    }  
  }  
}
```

-- Exhibit --

Refer to the exhibits.

How should the LTM Specialist minimize the configuration?

- A. Remove the pool member level monitors.
- B. The configuration is as minimized as possible.
- C. Create a single monitor and apply it to each pool member.
- D. Create a single monitor, apply it to the pool, and remove the pool member level monitors.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 181

-- Exhibit

```
ltm virtual Route_172.16.10 {
    destination 172.16.10.0:any
    ip-forward
    mask 255.255.255.0
    profiles {
        fastL4 { }
    }
    translate-address disabled
    translate-port disabled
    vlans-disabled
}
ltm virtual Route_172.16.20 {
    destination 172.16.20.0:any
    ip-forward
    mask 255.255.255.0
    profiles {
        fastL4 { }
    }
    translate-address disabled
    translate-port disabled
    vlans-disabled
}
ltm virtual Route_172.16.30 {
    destination 172.16.30.0:any
    ip-forward
    mask 255.255.255.0
    profiles {
        fastL4 { }
    }
    translate-address disabled
    translate-port disabled
    vlans-disabled
}
ltm virtual Route_all {
    destination 0.0.0.0:any
    ip-forward
    mask any
    profiles {
        fastL4 { }
    }
    translate-address disabled
    translate-port disabled
    vlans-disabled
}
```

Statistics Type	Virtual Servers
Data Format	Normalized
Auto Refresh	Disabled <input type="button" value="Refresh"/>

[illegible]

Refer to the exhibits.

www.vceplus.com - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - VCE Exam Simulator - VCE Online - IT Certifications

Which solution has the simplest configuration changes while maintaining functionality and basic security?

- A. Remove 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24, and keep 0.0.0.0/0.0.0.0 enabled on all VLANs.
- B. Replace 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24, with 172.16.0.0/16, and keep 0.0.0.0/0.0.0.0.
- C. Enable 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24 on ingress VLAN(s), and enable 0.0.0.0/0.0.0.0 on egress VLAN(s).
- D. Enable 172.16.10.0/24, 172.16.20.0/24, and 172.16.30.0/24 on egress VLAN(s), and enable 0.0.0.0/0.0.0.0 on ingress VLAN(s).

Correct Answer: C

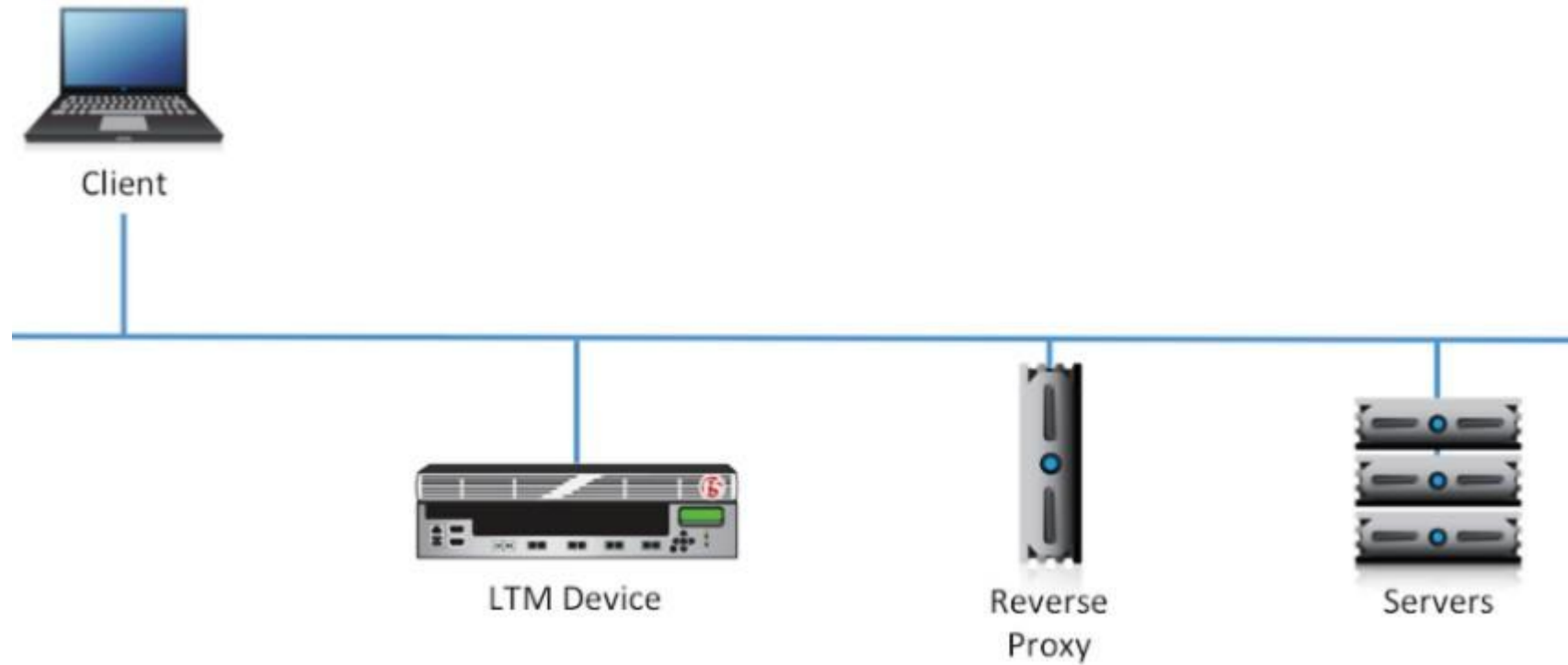
Section: (none)

Explanation

Explanation/Reference:

QUESTION 182

-- Exhibit



snat_rp.pcap [Wireshark 1.8.2 (SVN Rev Unknown from unknown)]

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000386	172.16.1.41	172.16.20.1	HTTP	470	GET / HTTP/1.1
8	0.001039	172.16.20.1	172.16.1.41	HTTP	202	HTTP/1.1 200 OK (text/html)
19	0.086336	172.16.1.42	172.16.20.1	HTTP	450	GET /header.gif HTTP/1.1
21	0.086341	172.16.1.41	172.16.20.1	HTTP	448	GET /left.gif HTTP/1.1
27	0.086753	172.16.1.42	172.16.20.1	HTTP	449	GET /right.gif HTTP/1.1
34	0.087128	172.16.1.41	172.16.20.1	HTTP	450	GET /footer.jpg HTTP/1.1
48	0.087796	172.16.20.1	172.16.1.41	HTTP	1382	HTTP/1.1 200 OK (JPEG JFIF image)
59	0.088076	172.16.20.1	172.16.1.42	HTTP	821	HTTP/1.1 200 OK (GIF89a)
69	0.088603	172.16.20.1	172.16.1.41	HTTP	569	HTTP/1.1 200 OK (GIF89a)
80	0.088932	172.16.20.1	172.16.1.42	HTTP	250	HTTP/1.1 200 OK (GIF89a)
96	0.277993	172.16.1.41	172.16.20.1	HTTP	421	GET /favicon.ico HTTP/1.1
98	0.278582	172.16.20.1	172.16.1.41	HTTP	350	HTTP/1.1 200 OK
107	4.106071	172.16.1.42	172.16.20.1	HTTP	479	GET /login.php HTTP/1.1
109	4.106695	172.16.20.1	172.16.1.42	HTTP	365	HTTP/1.1 200 OK (text/html)
118	9.088665	172.16.1.41	172.16.20.1	HTTP	516	GET /env.cgi HTTP/1.1
120	9.090787	172.16.20.1	172.16.1.41	HTTP	728	HTTP/1.1 200 OK (text/html)

Frame 4: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits)

Ethernet II, Src: Vmware_4a:03:12 (00:50:56:4a:03:12), Dst: Vmware_01:09:12 (00:50:56:01:09:12)

Internet Protocol Version 4, Src: 172.16.1.41 (172.16.1.41), Dst: 172.16.20.1 (172.16.20.1)

Transmission Control Protocol, Src Port: 63461 (63461), Dst Port: http (80), Seq: 1, Ack: 1, Len: 384

Hypertext Transfer Protocol

```

0000  00 50 56 01 09 12 00 50 56 4a 03 12 08 00 45 00  .PV...P VJ...E.
0010  01 b4 4a c0 40 00 ff 06 c2 38 ac 10 01 29 ac 10  ..J.@... .8...).
0020  14 01 f7 e5 00 50 f0 46 61 f0 ab e7 60 e2 80 18  ....P.F a... ..
0030  11 1c 37 ac 00 00 01 01 08 0a 8f 91 9c 64 11 c2  ..7..... ..d..
0040  4a e8 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  J.GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20 31 30 2e 31 30 2e 31 2e  ..Host: 10.10.1.
0060  31 30 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a  101..Con nection:

```

File: ... Packets: 125 Displayed: 16 Marked: 0 Load time: 0:00.003

-- 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

Section: (none)

Explanation

Explanation/Reference:

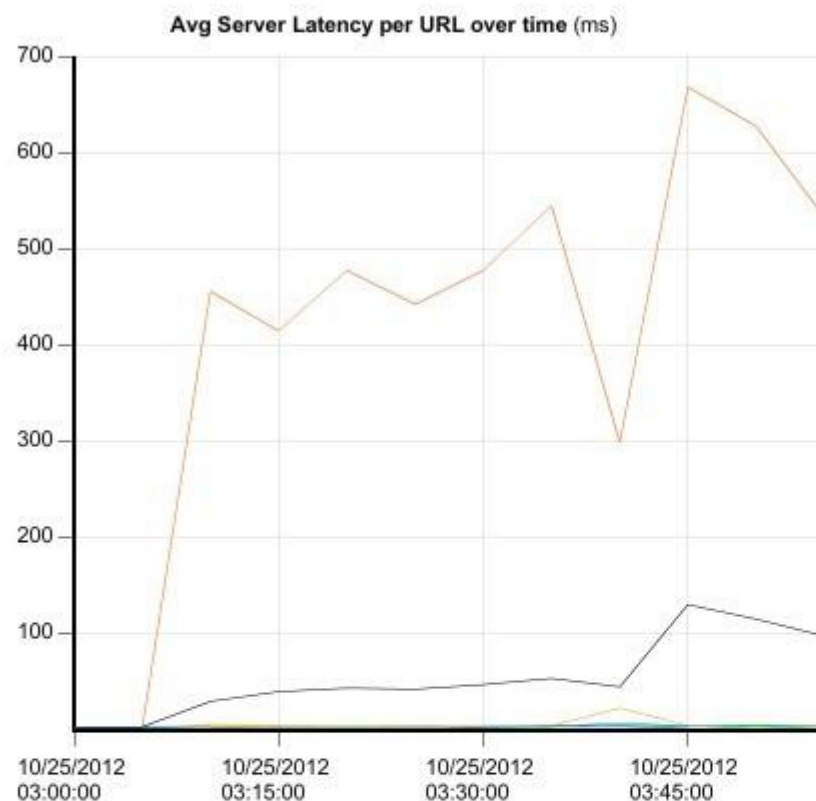
QUESTION 183

-- Exhibit

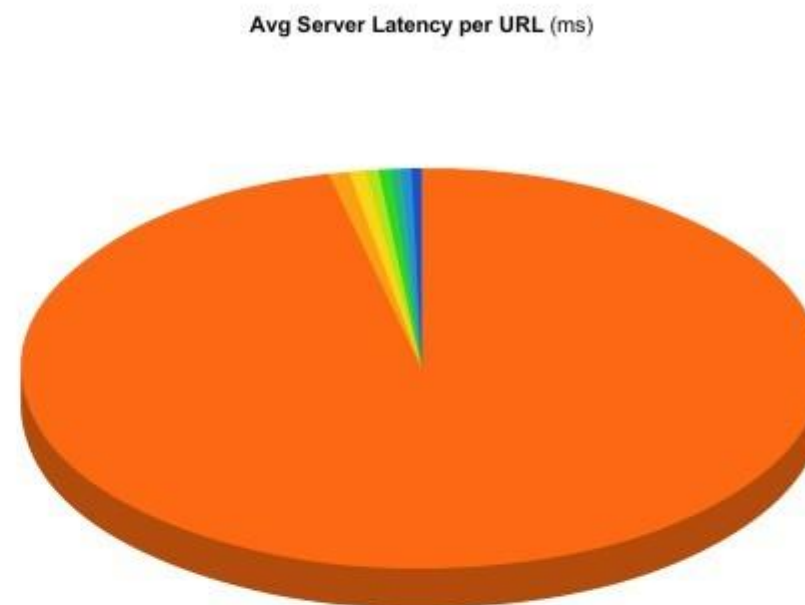
View By:

Time Period:

[Expand Advanced Filters](#)



Display method:

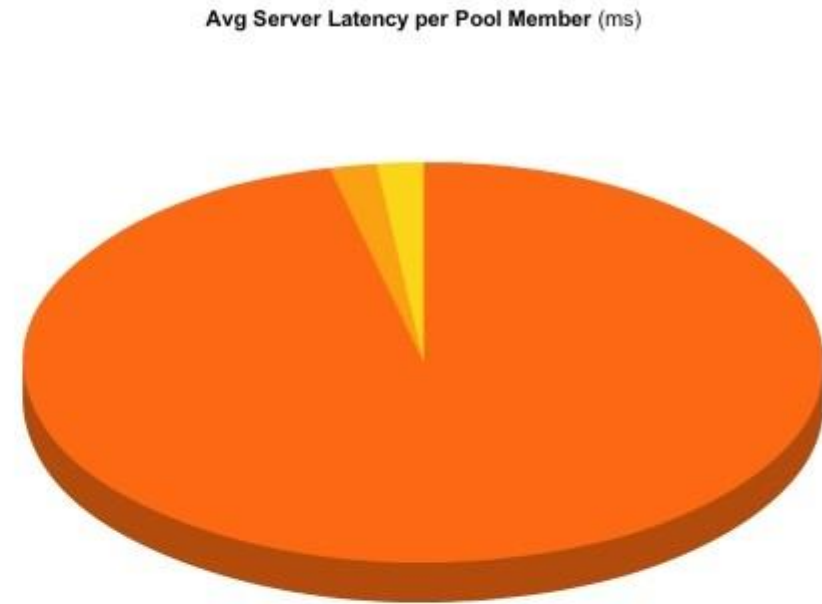
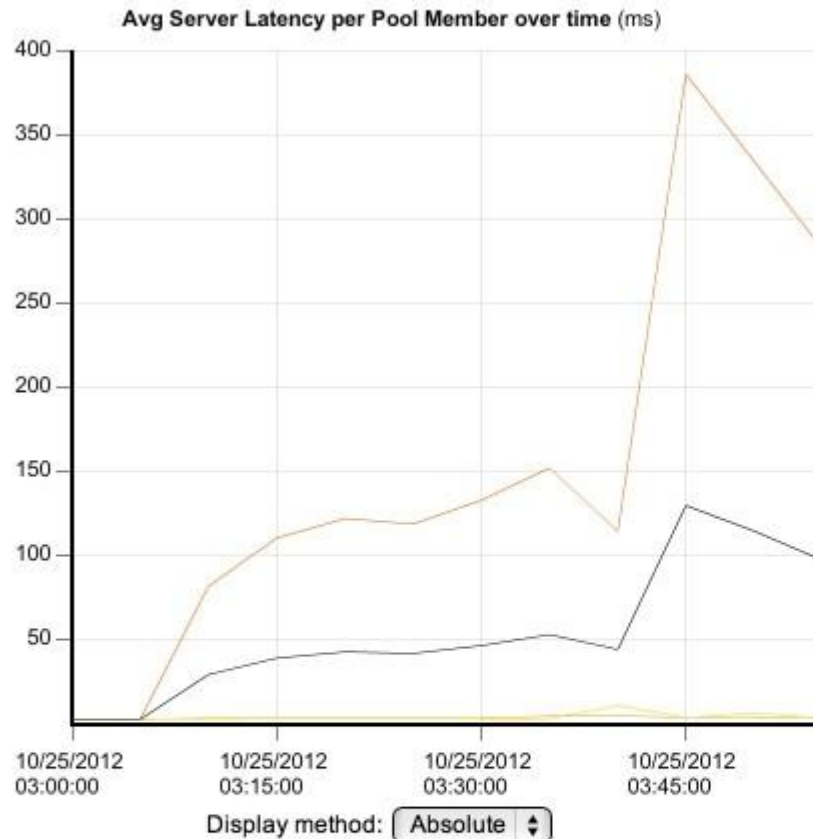


Measurement to display:

Details

<input checked="" type="checkbox"/>	#	URL	Avg Server Latency (ms)	Max Server Latency (ms)	Transactions
<input checked="" type="checkbox"/>	1	/slow1.php	502.12	1,551.00	459
<input checked="" type="checkbox"/>	2	/page14.cgi	4.33	408.00	506
<input checked="" type="checkbox"/>	3	/env.cgi	3.45	6.00	51
<input checked="" type="checkbox"/>	4	/not-logged-in.php	2.67	4.00	12
<input checked="" type="checkbox"/>	5	/safari.jpg	2.56	213.00	1,247
<input checked="" type="checkbox"/>	6	/slow2.php	2.21	12.00	358
<input checked="" type="checkbox"/>	7	/reflector.php	2.18	6.00	11

View By: **Pool Members** Time Period: **Last Hour** [Expand Advanced Filters](#)



Measurement to display:
Avg Server Latency (ms)

Details

<input checked="" type="checkbox"/>	#	Pool Member	Avg Server Latency (ms)	Max Server Latency (ms)	Transactions
<input checked="" type="checkbox"/>	1	172.16.20.3:80	158.36	1,551.00	1,462
<input checked="" type="checkbox"/>	2	172.16.20.2:80	3.13	121.00	1,460
<input checked="" type="checkbox"/>	3	172.16.20.1:80	3.11	408.00	1,462
<input checked="" type="checkbox"/>	4	Total	54.89	1,551.00	4,384

Total: 3

-- 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

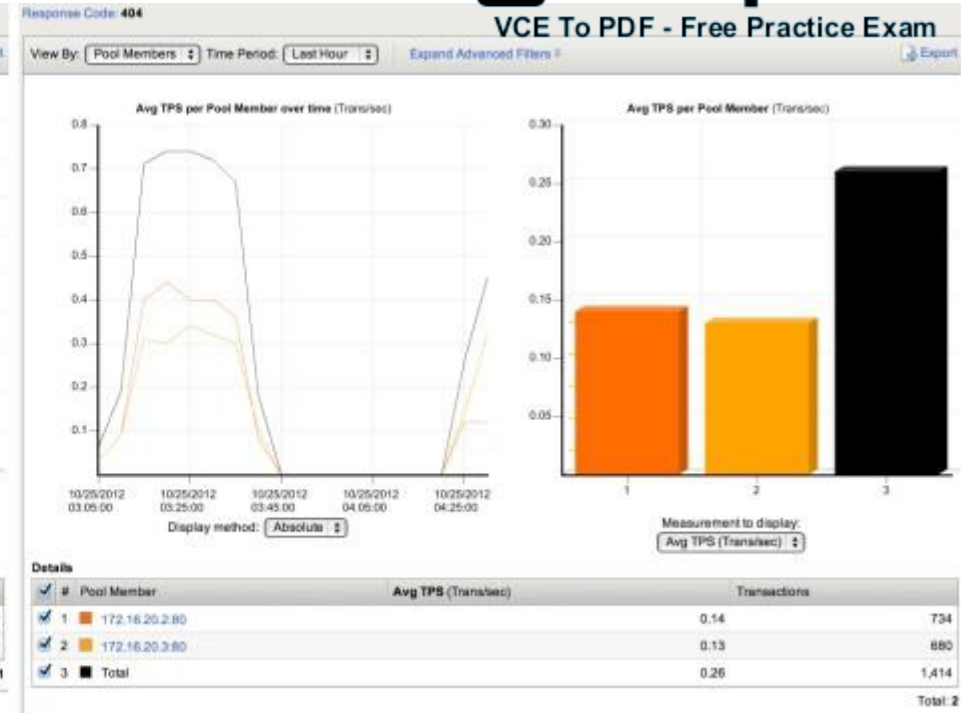
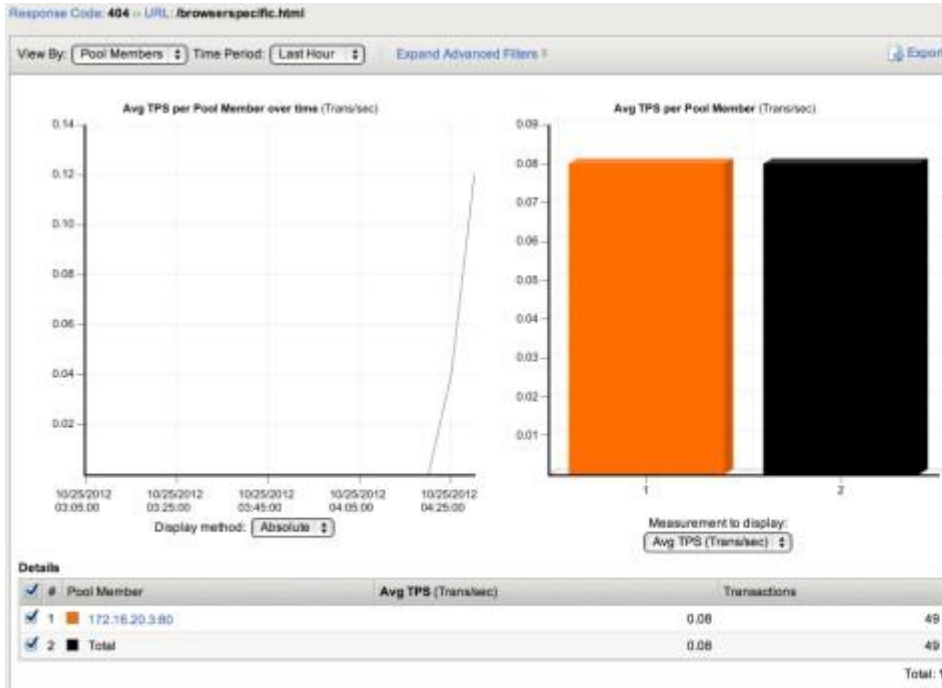
Section: (none)

Explanation

Explanation/Reference:

QUESTION 184

-- Exhibit



Response Code: 404 » Pool Member: 172.16.20.2:80

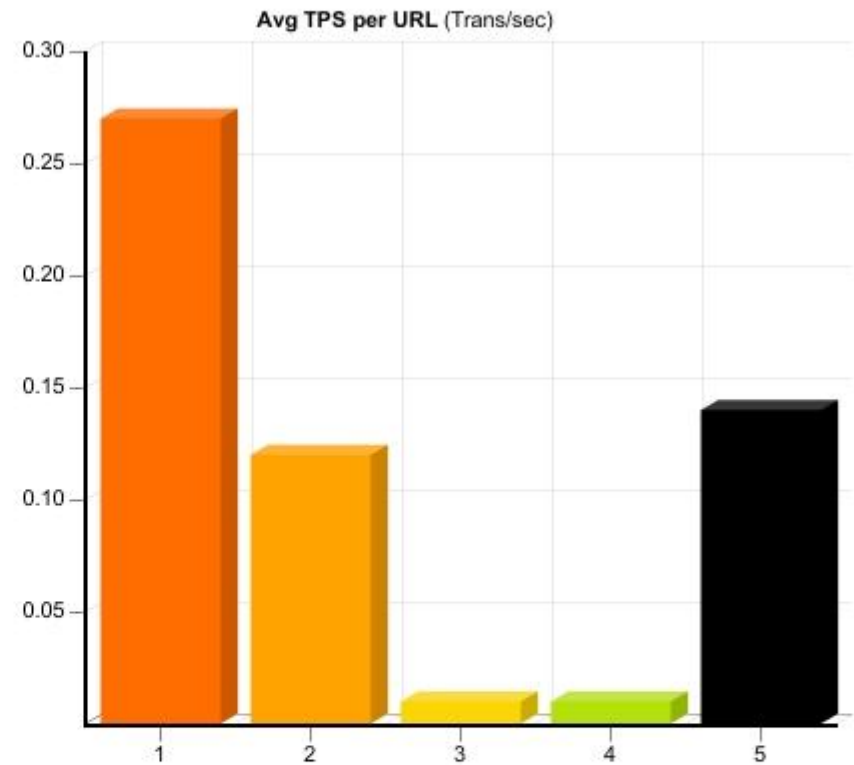
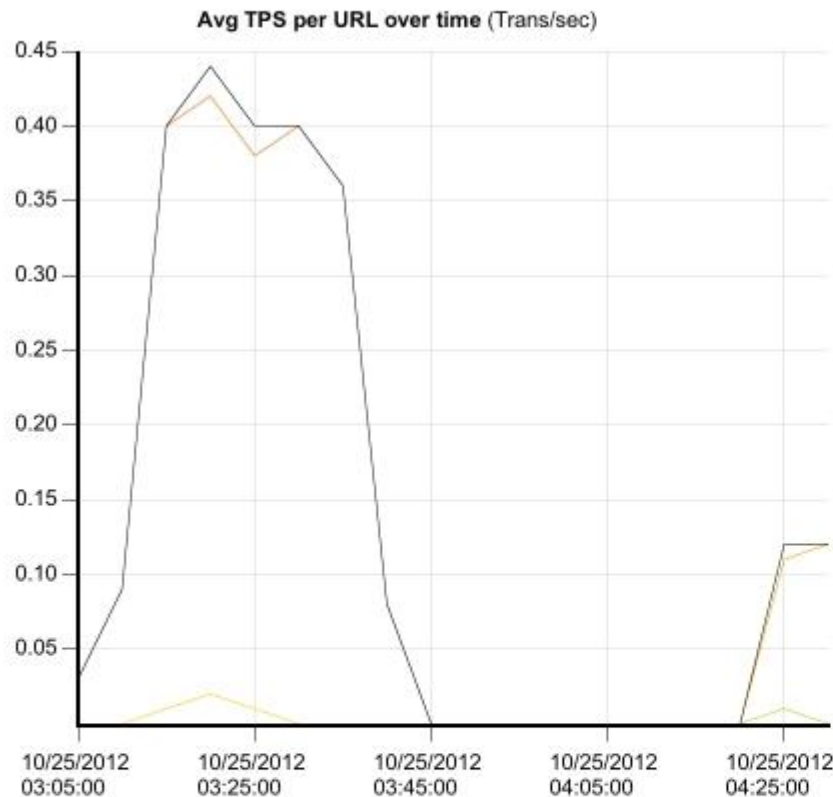
View By:

Time Period:

[Expand Advanced Filters](#)

[Export](#)

View By:



Measurement to display:

Details

<input checked="" type="checkbox"/>	#	URL	Avg TPS (Trans/sec)	Transactions
<input checked="" type="checkbox"/>	1	/favicon.ico	0.27	650
<input checked="" type="checkbox"/>	2	/text.one	0.12	69
<input checked="" type="checkbox"/>	3	/not-logged-in.php	0.01	11
<input checked="" type="checkbox"/>	4	/text.txt	0.01	4
<input checked="" type="checkbox"/>	5	Total	0.14	734

Total: 4

Details

<input checked="" type="checkbox"/>	#
<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	2

-- Exhibit --

Refer to the exhibits.

Which two servers are missing two frequently used URLs? (Choose two.)

- A. 172.16.20.1 /text.one /text.txt
- B. 172.16.20.2 /text.one /text.txt
- C. 172.16.20.1 /text.txt /browserspecific.html
- D. 172.16.20.2 /text.one /browserspecific.html
- E. 172.16.20.3 /text.one /browserspecific.html

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 185

-- Exhibit

General Configuration

Profile Name	avr_slow		
Partition / Path	Common		
Parent Profile	analytics		
Profile Description			
Statistics Logging Type	<input checked="" type="checkbox"/> Internal <input type="checkbox"/> External		
Traffic Capturing Logging Type	<input type="checkbox"/> Internal <input type="checkbox"/> External		
SMTP Configuration	None (Note: Setting can be changed only through the default analytics profile.)		
Notification Type	<input type="checkbox"/> Syslog <input type="checkbox"/> SNMP <input type="checkbox"/> E-mail		
Trust XFF	<input checked="" type="checkbox"/> Enable		
Transaction Sampling Ratio	Sample all transactions (Note: Setting can be changed only through the default analytics profile.)		

Included Objects

	<input type="checkbox"/>	Name	Destination	Service Port	Partition / Path
Virtual Servers	<input type="checkbox"/>	vs_http	10.10.1.100	80	Common
	<input type="checkbox"/>	vs_https	10.10.1.103	443	Common
		<input type="button" value="Add..."/> <input type="button" value="Delete"/>			

Statistics Gathering Configuration

Custom ☒

Collected Metrics	<input checked="" type="checkbox"/> Server Latency <input checked="" type="checkbox"/> Page Load Time <input checked="" type="checkbox"/> Throughput <input checked="" type="checkbox"/> User Sessions Timeout: <input type="text" value="5"/> minutes	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Collected Entities	<input checked="" type="checkbox"/> URLs <input type="checkbox"/> Countries <input checked="" type="checkbox"/> Client IP Addresses <input type="checkbox"/> Response Codes <input type="checkbox"/> User Agents <input checked="" type="checkbox"/> Methods	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>

Note: Changes you make might take up to 10 minutes to be reflected in the charts.

General Properties

Name	vs_https
Partition / Path	Common
Description	
Type	Standard
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.1.103
Service Port	443 HTTPS
Availability	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http
HTTP Compression Profile	None
Web Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	<div> <div>Selected</div> <div>Available</div> <div> <div>/Common clientssl</div> <div><<</div> <div>>></div> <div>/Common clientssl-insecure-compatible wom-default-clientssl</div> </div> </div>

-- Exhibit --

Refer to the exhibits.

When observing the AVR statistics for the HTTPS_VS, an LTM Specialist realizes that HTTP status codes are NOT being recorded.

How should the LTM Specialist modify the configuration to record the HTTP status codes?

- A. assign a streaming profile to the virtual server
- B. assign client SSL and server SSL profiles to the virtual server
- C. enable Statistics Logging Type, External on the analytics profile
- D. enable Collected Entities, Response Codes on the analytics profile

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 186

-- Exhibit

HTTP Headers for Direct Request:

Request #1:

GET / HTTP/1.1
Host: 172.16.20.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.40 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response #1:

HTTP/1.1 200 OK
Date: Tue, 23 Oct 2012 16:51:23 GMT
Server: Apache/2.2.15 (Unix)
Last-Modified: Tue, 23 Oct 2012 16:44:12 GMT
ETag: "205c5-ab8-4ccbae000f00"
Accept-Ranges: bytes
Content-Length: 2744
Connection: close
Content-Type: text/html; charset=UTF-8

Request #2:

GET /page2 HTTP/1.1
Host: 172.16.20.1
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.40 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://172.16.20.1/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response #2:

HTTP/1.1 302 Found
Date: Tue, 23 Oct 2012 17:03:27 GMT
Server: Apache/2.2.15 (Unix)
Location: http://172.16.20.1/page2.php
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1

Request #3:

HTTP Headers for Request through LTM Device:

Request #1:

```
GET / HTTP/1.1
Host: 10.10.1.103
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.40 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
```

Response #1:

```
HTTP/1.1 200 OK
Date: Tue, 23 Oct 2012 16:02:18 GMT
Server: Apache/2.2.15 (Unix)
Last-Modified: Mon, 03 Sep 2012 11:54:38 GMT
ETag: "20582-a46-4c8cace5d1b80"
Accept-Ranges: bytes
Content-Length: 2630
Connection: close
Content-Type: text/html; charset=UTF-8
```

Request #2:

```
GET /page2 HTTP/1.1
Host: 10.10.1.103
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.40 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://10.10.1.103/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
```

Response #2:

```
HTTP/1.1 302 Found
Date: Tue, 23 Oct 2012 16:02:19 GMT
Server: Apache/2.2.15 (Unix)
Location: http://10.10.1.103/page2.php
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Request #3:

```
GET http://10.10.1.103/env.cgi HTTP/1.1
```

-- Exhibit --

Refer to the exhibits.

A customer requests to offload SSL for an internal website. The front page of the website loads correctly; however, selecting links on the page fails.

How should the LTM Specialist fix the issue?

- A. Create a new SNAT pool.
Add internal network IPs to the SNAT pool.
Add the SNAT pool to the VS.
- B. Create a new HTTP profile.
Enable Insert X-Forwarded-For.
Add the new HTTP profile to the VS.
- C. Create a new HTTP profile.
Enable redirect rewrite.
Add the new HTTP profile to the VS.
- D. Create a new Server SSL profile.
Enable Proxy SSL.
Add the Server SSL profile to the VS.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 187

-- 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,n
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
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,sacko
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,sacko
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,sacko
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,sa
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,
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.exam
+ 9.144		!	9.134	336	5079	GET	200		http://srv1.exam
+ 9.146		!	9.266	334	19307	GET	200		http://srv1.exam
+ 9.147		!	9.232	335	14644	GET	200		http://srv1.exam
+ 9.149		!	9.189	336	4192	GET	200		http://srv1.exam
			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.exa
+ 0.435		!	9.110	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.exa
+ 0.435		!	9.322	298	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.exa
+ 0.435		!	9.322	299	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.exa
+ 0.435		!	9.322	300	0	GET	ERROR_INTERNET_CONNECTION_ABORTED		http://www.exa
			← 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 188

-- Exhibit

Direct to application server:

Request:

GET / HTTP/1.1

Host: 172.16.20.21

Connection: keep-alive

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 200 OK

Date: Wed, 24 Oct 2012 19:11:46 GMT

Server: Apache/2.2.22 (Ubuntu)

Last-Modified: Fri, 08 Jun 2012 13:32:31 GMT

ETag: "a0b21-b1-4cif608458836"

Accept-Ranges: bytes

Content-Length: 177

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Through LTM:

Request:

GET / HTTP/1.1

Host: www.example.com

Connection: keep-alive

Cache-Control: max-age=0

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 301 Moved Permanently

Date: Wed, 24 Oct 2012 19:17:47 GMT

Server: Apache/2.2.22 (Ubuntu)

Location: https://www.example.com/

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=iso-8859-1

Transfer-Encoding: chunked

-- Exhibit --

Refer to the exhibit.

An LTM Specialist configures a virtual server to perform client-side encryption while allowing the server-side traffic to be unencrypted. Application owners report that images are failing to load through the virtual server; however, images load when going directly to the server.

What is the problem with the images loading through the virtual server?

- A. Image references are for HTTP objects, not HTTPS.
- B. Image references are for HTTPS objects, not HTTP.
- C. The virtual server does not have "SSL Offloading" enabled.
- D. The virtual server does not have an HTTP profile associated.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 189

-- 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,s
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,w
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
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,w
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,
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,
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,
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,
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,
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,
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,
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,
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.

What is the cause of the application access problem?

- A. The virtual server has SNAT disabled.
- B. The client has no route to the web server.
- C. The virtual server has address translation disabled.
- D. The web server is NOT responding on the correct port.
- E. The virtual server is NOT configured to listen on port 80.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 190

-- Exhibit


```
18:25:47.356188 IP 192.168.1.100.55596 > 192.168.1.155.8080: S 365083520:365083520(0) win 8192 <mss 1260,nop,wscale 2,no
....E..4cE@..../...d.....,.....
18:25:47.356218 IP 192.168.1.155.8080 > 192.168.1.100.55596: S 2357781217:2357781217(0) ack 365083521 win 3780 <mss 1460
....E..4.O@....#.....d....."...../test/http_custom_redirect_vs
18:25:47.357679 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redir
....E..(cF@....:....d.....,.....P.A7....."...../test/http_custom_redirect_vs
18:25:47.365725 IP 192.168.1.100.55596 > 192.168.1.155.8080: P 1:294(293) ack 1 win 16695 in slot1/tmm0 lis=/test/http_c
....E..McG@.....d.....,.....P.A7\
..GET / HTTP/1.1
Host: 192.168.1.155:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive

."...../test/http_custom_redirect_vs
18:25:47.365805 IP 192.168.1.155.8080 > 192.168.1.100.55596: P 1:105(104) ack 294 win 3780 out slot1/tmm0 lis=/test/http
....E....S@.....d.....,.....P.....HTTP/1.0 302 Found
Location: https://192.168.1.155:8080/
Connection: Keep-Alive
Content-Length: 0

."...../test/http_custom_redirect_vs
18:25:47.382739 IP 192.168.1.100.55597 > 192.168.1.155.8080: S 2429178084:2429178084(0) win 8192 <mss 1260,nop,wscale 2,
....E..4cH@.....,....d.....-....P..... ..!.....
18:25:47.382752 IP 192.168.1.155.8080 > 192.168.1.100.55597: S 197089061:197089061(0) ack 2429178085 win 3780 <mss 1460,
....E..4.V@.....d....-..W%.P....."...../test/http_custom_redirect_vs
18:25:47.384086 IP 192.168.1.100.55597 > 192.168.1.155.8080: . ack 1 win 16695 in slot1/tmm0 lis=/test/http_custom_redir
....E..(cI@....7....d.....-....P...W&P.A7....."...../test/http_custom_redirect_vs
18:25:47.384092 IP 192.168.1.100.55597 > 192.168.1.155.8080: P 1:89(88) ack 1 win 16695 in slot1/tmm0 lis=/test/http_cus
....E...cJ@.....d.....-....P...W&P.A7gN.....S...O..P.....x...z&u....i..!K..[v...7..(.....9.8...5.E.D.3.2...A....
..."...../test/http_custom_redirect_vs
18:25:47.384106 IP 192.168.1.155.8080 > 192.168.1.100.55597: . ack 89 win 3868 out slot1/tmm0 lis=/test/http_custom_redi
....E..(.Z@....$......d....-..W&..Q=P....."...../test/http_custom_redirect_vs
18:25:47.571574 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 105 win 16669 in slot1/tmm0 lis=/test/http_custom_red
....E..(cX@....(....d.....,.....JP.A..n..."...../test/http_custom_redirect_vs
18:27:42.414390 IP 192.168.1.100.55596 > 192.168.1.155.8080: F 294:294(0) ack 105 win 16669 in slot1/tmm0 lis=/test/http
....E..(h)@.....d.....,.....JP.A..m..."...../test/http_custom_redirect_vs
18:27:42.414425 IP 192.168.1.155.8080 > 192.168.1.100.55596: . ack 295 win 4073 out slot1/tmm0 lis=/test/http_custom_red
....E..(.@.....d.....,....J....P....."...../test/http_custom_redirect_vs
18:27:42.414431 IP 192.168.1.155.8080 > 192.168.1.100.55596: F 105:105(0) ack 295 win 4073 out slot1/tmm0 lis=/test/http
....E..(.@.....~.....d.....,....J....P....."...../test/http_custom_redirect_vs
18:27:42.415916 IP 192.168.1.100.55596 > 192.168.1.155.8080: . ack 106 win 16669 in slot1/tmm0 lis=/test/http_custom_red
```



```
ltm profile httpclass /test/http_custom_redirect {
    app-service none
    defaults-from httpclass
    pool none
    redirect https://[HTTP::host][HTTP::uri]
}
ltm pool eCommerce_https_pool {
    members {
        10.1.1.1:https {
            address 10.1.1.1
        }
    }
    partition test
}
ltm virtual /test/http_custom_redirect_vs {
    destination 192.168.1.155:8080
    http-class {
        /test/http_custom_redirect
    }
    ip-protocol tcp
    mask 255.255.255.255
    partition test
    profiles {
        http { }
        tcp { }
    }
    vlans-disabled
}
ltm virtual https_vs {
    destination /Common/192.168.1.155:https
    ip-protocol tcp
    mask 255.255.255.255
    partition test
    pool eCommerce_https_pool
    profiles {
        /Common/example.com {
            context clientside
        }
        /Common/serverssl-insecure-compatible {
            context serverside
        }
        /Common/tcp { }
    }
}
snat automap
vlans-disabled
```

-- Exhibit --

Refer to the exhibits.

An LTM Specialist is reconfiguring a virtual server to redirect all clients to HTTPS. Testing reveals that the redirect is functioning incorrectly. As part of the troubleshooting process, the LTM Specialist performs a packet capture.

What is the issue?

- A. The redirect is causing an infinite loop.
- B. The virtual server is missing a clientssl profile.
- C. The redirect is sending the client to the incorrect location.
- D. The virtual server is incorrectly processing the HTTP request.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 191

-- Exhibit

Packet capture through LTM device

```

09:26:40.158653 IP 172.16.1.3.54990 > 172.16.20.21.https: S 2815629254:2815629254(0) win 4380 <mss 1460,nop,wscale 0,no
  0x0000: 4500 0040 092b 4000 ff06 0554 ac10 0103 E..@.+@....T....
  0x0010: ac10 1415 d6ce 01bb a7d3 17c6 0000 0000 .....
  0x0020: b002 111c 4d2d 0000 0204 05b4 0103 0300 ....M-.....
  0x0030: 0101 080a 98bf 3a9d 0000 0000 0402 0000 .....:.....
09:26:40.160133 IP 172.16.20.21.https > 172.16.1.3.54990: S 4117971743:4117971743(0) ack 2815629255 win 14480 <mss 1460
  0x0000: 4500 003c 0000 4000 4006 cd83 ac10 1415 E..<...@.@.....
  0x0010: ac10 0103 01bb d6ce f573 431f a7d3 17c7 .....sC.....
  0x0020: a012 3890 7182 0000 0204 05b4 0402 080a ..8.q.....
  0x0030: 0003 8c90 98bf 3a9d 0103 0304 .....:.....
09:26:40.160143 IP 172.16.1.3.54990 > 172.16.20.21.https: . ack 1 win 4380 <nop,nop,timestamp 2562669215 232592>
  0x0000: 4500 0034 092e 4000 ff06 055d ac10 0103 E..4..@....]....
  0x0010: ac10 1415 d6ce 01bb a7d3 17c7 f573 4320 .....sC.
  0x0020: 8010 111c c7bd 0000 0101 080a 98bf 3a9f .....:
  0x0030: 0003 8c90 .....
09:26:40.160150 IP 172.16.1.3.54990 > 172.16.20.21.https: P 1:442(441) ack 1 win 4380 <nop,nop,timestamp 2562669215 232
  0x0000: 4500 01ed 0930 4000 ff06 03a2 ac10 0103 E....0@.....
  0x0010: ac10 1415 d6ce 01bb a7d3 17c7 f573 4320 .....sC.
  0x0020: 8018 111c b0a8 0000 0101 080a 98bf 3a9f .....:
  0x0030: 0003 8c90 4745 5420 2f20 4854 5450 2f31 ....GET./..HTTP/1
  0x0040: 2e31 0d0a 486f 7374 3a20 7777 772e 6578 ..1..Host:..www.ex
  0x0050: 616d am
09:26:40.163290 IP 172.16.20.21.https > 172.16.1.3.54990: . ack 442 win 972 <nop,nop,timestamp 232592 2562669215>
  0x0000: 4500 0034 cfb0 4000 4006 fdda ac10 1415 E..4..@.@.....
  0x0010: ac10 0103 01bb d6ce f573 4320 a7d3 1980 .....sC.....
  0x0020: 8010 03cc d354 0000 0101 080a 0003 8c90 .....T.....
  0x0030: 98bf 3a9f ...:
09:26:40.164206 IP 172.16.20.21.https > 172.16.1.3.54990: P 1:527(526) ack 442 win 972 <nop,nop,timestamp 232592 256266
  0x0000: 4500 0242 cfb1 4000 4006 fbcb ac10 1415 E..B..@.@.....
  0x0010: ac10 0103 01bb d6ce f573 4320 a7d3 1980 .....sC.....
  0x0020: 8018 03cc c59e 0000 0101 080a 0003 8c90 .....
  0x0030: 98bf 3a9f 3c21 444f 4354 5950 4520 4854 ...:<!DOCTYPE.HT
  0x0040: 4d4c 2050 5542 4c49 4320 222d 2f2f 4945 ML.PUBLIC."-//IE
  0x0050: 5446 TF
09:26:40.164226 IP 172.16.1.3.54990 > 172.16.20.21.https: . ack 527 win 4906 <nop,nop,timestamp 2562669219 232592>
  0x0000: 4500 0034 0934 4000 ff06 0557 ac10 0103 E..4.4@....W....
  0x0010: ac10 1415 d6ce 01bb a7d3 1980 f573 452e .....sE.
  0x0020: 8010 132a c1e4 0000 0101 080a 98bf 3aa3 ...*.....:
  0x0030: 0003 8c90 .....
09:26:40.165322 IP 172.16.20.21.https > 172.16.1.3.54990: F 527:527(0) ack 442 win 972 <nop,nop,timestamp 232592 256266
  0x0000: 4500 0034 cfb2 4000 4006 fdd8 ac10 1415 E..4..@.@.....
  0x0010: ac10 0103 01bb d6ce f573 452e a7d3 1980 .....sE.....
  0x0020: 8010 03cc d145 0000 0101 080a 0003 8c90 .....
  0x0030: 0003 8c90 .....

```


Packet capture direct to application server

```

09:36:28.845154 IP 1.1.2.150.55073 > 172.16.20.21.https: S 3718695743:3718695743(0) win 65535 <mss 1460,nop,wscale 3,nop
  0x0000: 4500 0040 f88c 4000 4006 7e6f 0101 0296 E..@...@.~o....
  0x0010: ac10 1415 d721 01bb dda6 cb3f 0000 0000 .....!.....?....
  0x0020: b002 ffff 0a53 0000 0204 05b4 0103 0303 .....S.....
  0x0030: 0101 080a 28da be52 0000 0000 0402 0000 ....(..R.....
09:36:28.845218 IP 1.1.2.150.55073 > 172.16.20.21.https: S 3718695743:3718695743(0) win 65535 <mss 1460,nop,wscale 3,nop
  0x0000: 4500 0040 f88c 4000 3f06 7f6f 0101 0296 E..@...@.?..o....
  0x0010: ac10 1415 d721 01bb dda6 cb3f 0000 0000 .....!.....?....
  0x0020: b002 ffff 0a53 0000 0204 05b4 0103 0303 .....S.....
  0x0030: 0101 080a 28da be52 0000 0000 0402 0000 ....(..R.....
09:36:28.846583 IP 172.16.20.21.https > 1.1.2.150.55073: S 1893621123:1893621123(0) ack 3718695744 win 14480 <mss 1460,s
  0x0000: 4500 003c 0000 4000 4006 7700 ac10 1415 E..<...@.@.w.....
  0x0010: 0101 0296 01bb d721 70de 5d83 dda6 cb40 .....!p.]....@
  0x0020: a012 3890 48df 0000 0204 05b4 0402 080a ..8.H.....
  0x0030: 0005 cb6f 28da be52 0103 0304 ...o(..R....
09:36:28.848001 IP 172.16.20.21.https > 1.1.2.150.55073: S 1893621123:1893621123(0) ack 3718695744 win 14480 <mss 1460,s
  0x0000: 4500 003c 0000 4000 3f06 7800 ac10 1415 E..<...@.@.x.....
  0x0010: 0101 0296 01bb d721 70de 5d83 dda6 cb40 .....!p.]....@
  0x0020: a012 3890 48df 0000 0204 05b4 0402 080a ..8.H.....
  0x0030: 0005 cb6f 28da be52 0103 0304 ...o(..R....
09:36:28.848010 IP 1.1.2.150.55073 > 172.16.20.21.https: . ack 1 win 65535 <nop,nop,timestamp 685424212 379759>
  0x0000: 4500 0034 8891 4000 4006 ee76 0101 0296 E..4...@.@..v....
  0x0010: ac10 1415 d721 01bb dda6 cb40 70de 5d84 .....!.....@p.].
  0x0020: 8010 ffff b036 0000 0101 080a 28da be54 .....6.....(..T
  0x0030: 0005 cb6f ...o
09:36:28.848020 IP 1.1.2.150.55073 > 172.16.20.21.https: . ack 1 win 65535 <nop,nop,timestamp 685424212 379759>
  0x0000: 4500 0034 8891 4000 3f06 ef76 0101 0296 E..4...@.@..v....
  0x0010: ac10 1415 d721 01bb dda6 cb40 70de 5d84 .....!.....@p.].
  0x0020: 8010 ffff b036 0000 0101 080a 28da be54 .....6.....(..T
  0x0030: 0005 cb6f ...o
09:36:28.849049 IP 1.1.2.150.55073 > 172.16.20.21.https: P 1:378(377) ack 1 win 65535 <nop,nop,timestamp 685424212 37975
  0x0000: 4500 01ad faf8 4000 4006 7a96 0101 0296 E.....@.@.z.....
  0x0010: ac10 1415 d721 01bb dda6 cb40 70de 5d84 .....!.....@p.].
  0x0020: 8018 ffff 7e10 0000 0101 080a 28da be54 ....~.....(..T
  0x0030: 0005 cb6f 1603 0101 7401 0001 7003 0150 ...o....t...p..P
  0x0040: 896a 8bb0 c37c 5a0d 89fa 8a3c 69a7 6fc8 .j....|Z....<i.o.
  0x0050: 4e80 N.
09:36:28.849058 IP 1.1.2.150.55073 > 172.16.20.21.https: P 1:378(377) ack 1 win 65535 <nop,nop,timestamp 685424212 37975
  0x0000: 4500 01ad faf8 4000 3f06 7b96 0101 0296 E.....@.@.{.....
  0x0010: ac10 1415 d721 01bb dda6 cb40 70de 5d84 .....!.....@p.].
  0x0020: 8018 ffff 7e10 0000 0101 080a 28da be54 ....~.....(..T
  0x0030: 0005 cb6f 1603 0101 7401 0001 7003 0150 ...o....t...p..P
  0x0040: 896a 8bb0 c37c 5a0d 89fa 8a3c 69a7 6fc8 .j....|Z....<i.o.

```

-- Exhibit --

Refer to the exhibits.

An LTM Specialist has configured a virtual server to distribute connections to a pool of application servers and to offload SSL processing. The application fails to work as expected when connecting to the virtual server. It does work when clients connect directly to the application. Two packet captures were taken at the application server.

What is the root cause of the problem?

- A. The application servers are NOT listening on port 80.
- B. The LTM device is sending non-SSL traffic to an SSL port.
- C. The virtual server does NOT have a clientSSL profile assigned.
- D. The SSL handshake between the LTM device and the server is failing.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 192

-- Exhibit

General Properties	
Name	vs_https
Partition / Path	Common
Description	
Type	Standard
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.10.1.103
Service Port	443 HTTPS
Availability	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced	
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	http
HTTP Compression Profile	None
Web Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	<div> <div>Selected</div> <div>Available</div> </div> <div> <div>/Common clientssl</div> <div><< >></div> <div>/Common clientssl-insecure-compatible wom-default-clientssl</div> </div>

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is troubleshooting an issue with an application configured on an LTM device. The application works properly when accessed directly via the servers; however, it does not work when accessed via the LTM device. 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. The virtual server has no Client or Server SSL profiles associated.

Which configuration change will allow the application to function through the virtual server?

- A. Change pool member port to 8443.
- B. Change virtual server port to 8443.
- C. Add SSL off-loading to the pool member.
- D. Add Client and Server SSL profiles to the virtual server.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 193

-- Exhibit

-- Exhibit --

Refer to the exhibit.

An administrator created a monitor to a pool member web server, which resulted in a pool member that is marked red. The administrator knows the web server is working when it is accessed from another computer.

What should the administrator do to correct the problem?

- A. Change the default gateway on the server.
- B. Create a SNAT in the LTM device configuration.
- C. Change the route to the client in the LTM configuration.
- D. Change the username and/or password on the monitor.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 194

-- Exhibit

Direct to application server:

Request:

GET / HTTP/1.1

Host: 172.16.20.21

Connection: keep-alive

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 200 OK

Date: Wed, 24 Oct 2012 19:11:46 GMT

Server: Apache/2.2.22 (Ubuntu)

Last-Modified: Fri, 08 Jun 2012 13:32:31 GMT

ETag: "a0b21-b1-4cif608458836"

Accept-Ranges: bytes

Content-Length: 177

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Through LTM:

Request:

GET / HTTP/1.1

Host: www.example.com

Connection: keep-alive

Cache-Control: max-age=0

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko)

Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Response:

HTTP/1.1 301 Moved Permanently

Date: Wed, 24 Oct 2012 19:17:47 GMT

Server: Apache/2.2.22 (Ubuntu)

Location: https://www.example.com/

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html; charset=iso-8859-1

Transfer-Encoding: chunked

-- Exhibit --

Refer to the exhibits.

An LTM Specialist configures a virtual server for an internal application to perform client-side encryption while allowing the server-side traffic to be unencrypted. Application users report that images are NOT loading through the virtual server; however, images load when going directly to the server.

What should the LTM Specialist configure to allow the images to load through the virtual server?

- A. HTTP profile with "SSL Offload" enabled
- B. HTTP profile with "SSL Offload" disabled
- C. Stream profile with source "http:" and target "https:"
- D. Stream profile with target "http:" and source "https:"

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 195

-- Exhibit

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,sa
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,
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
```

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,n
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
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,sacko
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,sacko
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,sacko
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
```

-- Exhibit --

Refer to the exhibits.

An LTM Specialist is troubleshooting an issue with one of the virtual servers on an LTM device, and all requests are receiving errors. Testing directly against the server generates no errors. The LTM Specialist has captured the request and response on both client and server sides of the LTM device.

What should the LTM Specialist do to fix this issue?

- A. Remove "header-erase Host" in http profile.
- B. Configure SNAT Automap on the virtual server.
- C. Assign OneConnect profile to the virtual server.
- D. Set "redirect-rewrite" to "selective" in http profile.

Correct Answer: A

Section: (none)


Explanation

Explanation/Reference:

QUESTION 196

-- Exhibit

LTM device statistics

		Search	Reset Search			Bits		Packets		Connections	
<input checked="" type="checkbox"/>	Status	Virtual Server	Partition / Path	Details	In	Out	In	Out	Current	Maximum	To
<input type="checkbox"/>		VS_HTTP	Common	View...	283.8K	2.4M	391	544	0	5	55

				<div>Search</div> <div>Reset Search</div>					Bits		Packets		
<input checked="" type="checkbox"/>	Status	Pool/Member	Partition / Path	In	Out	In	Out	Cur					
<input type="checkbox"/>		Pool_HTTP	Common	193.9K	2.4M	284	347	0					
<input type="checkbox"/>		-- 172.16.20.1:80	Common	103.4K	1.5M	163	206	0					
<input type="checkbox"/>		-- 172.16.20.2:80	Common	90.1K	872.4K	120	141	0					
<input type="checkbox"/>		-- 172.16.20.3:80	Common	416	0	1	0	0					

-- 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 197

-- 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
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
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
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
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
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
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
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
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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 198

-- 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


```
[~]$ 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-----
MIICGzCCAeygAwIBAgIJAImlXVLJqYzBMA0GCSqGSIb3DQEBBQUAMDYxZjAUBgNV
BAoTDVR1cm5LZXkgTGluZXgHDAaBgNVBASTE1NvZnR3YXJlIGFwcGxpYW5jZXMw
HhcNMTAwNDE1MTkxNDQzWhcNMjAwNDEyMTkxNDQzWjA2MRYwFAYDVQQKEw1UdXJu
S2V5IExpbnV4MRwwGgYDVQQLEXNTb2Z0d2FyZSBhcHBsaWFuY2VzMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCvlgendrRHsavr6R+/M/xYyooMJVpXWZbzeKu04ro
eudY0KOWwa2zF9jaD0HDIJ3MtnVYahMsHZvqoolQ8EfohP85RfHrO4kMxtvAefm
slqGE7MkmIxLtwYjjWXmwxW7sCFL19kt6pFOatzqeK3WxbdM5yF/RTHF4R/vyKQI
2lyf/wIDAQABo4GYMIGVMB0GA1UdDgQWBBERG5CDKtOlkiix7sc2JjoVHajd2zBm
BgNVHSMEXzBdgBRG5CDKtOlkiix7sc2JjoVHajd26E6pDgwNjEWMBQGA1UEChMN
VHVybktleSBMaW5leDEcMBoGA1UECXMtU29mdHdhcmUgYXBwbGlhbmNlc4IJAImL
XVLJqYzBMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEANo2TuXFVZKwG
n6KznFgueLGzn+qgyIz0ZVG5PF8RRzHPYDAIDRU0MEReQHhI4CRImMAwTAFdmhpl
RGH2+Iqwg1EPB7K6eudRy0D9GqzMhZrdMo9d3ewPB3BqjOrPhs5yRTgNrZHyasJr
ZAiCzekf24SwNpmhfHyam88N2+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: F457C0A12201A70C4E65511A1CD35D7738B1073068D7DB164E2D7413D4487ACC
```

-- 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

Section: (none)

Explanation

Explanation/Reference:

QUESTION 199

-- Exhibit

```
Oct 25 09:24:04 bigip1 notice syslog-ng[2983]: syslog-ng starting up; version='2.0.8\'
Oct 25 09:24:36 bigip1 notice audispd: audispd initialized with q_depth=80 and 1 active plugins
Oct 25 09:24:38 bigip1 notice syslog-ng[2983]: Configuration reload request received, reloading configuration
Oct 25 09:25:55 bigip1 notice syslog-ng[2983]: Configuration reload request received, reloading configuration
Oct 25 09:35:44 bigip1 notice shutdown[8888]: Thu Oct 25 09:35:44 2012 : shutting down for system reboot on
2012-10-25T09:37:17-07:00 bigip1 notice boot_marker : ---===[ HD1.4 - BIG-IP 11.2.0 Build 2557.0 ]===---
Oct 25 09:37:19 bigip1 notice syslog-ng[2970]: syslog-ng starting up; version='2.0.8\'
Oct 25 09:37:51 bigip1 notice audispd: audispd initialized with q_depth=80 and 1 active plugins
Oct 25 09:37:53 bigip1 notice syslog-ng[2970]: Configuration reload request received, reloading configuration
Oct 25 09:39:02 bigip1 notice syslog-ng[2970]: Configuration reload request received, reloading configuration
```



```
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/http_pool
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/https_pool
Oct 25 09:29:05 tmm1 err tmm1[7355]: 01010028:3: No members available for pool /Common/ssh_pool
Oct 25 09:35:44 bigip1 notice overdog[4791]: 01140104:5: Watchdog touch disabled.
Oct 25 09:35:44 bigip1 info overdog[4791]: 01140101:6: Overdog daemon shutdown.
Oct 25 09:35:44 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id %promptstatus
Oct 25 09:35:44 bigip1 info promptstatusd[4790]: 01460007:6: Resuming log processing at this invocation; he
Oct 25 09:35:45 bigip1 notice logger: /bin/bash /etc/rc6.d/K03bigstart stop ==> /usr/bin/bigstart stop
Oct 25 09:35:46 bigip1 notice alertd[5636]: 01100043:5: logcheck Notice: Disconnect mcpd 0
Oct 25 09:35:46 bigip1 warning alertd[5636]: 01100002:4: alertd is going down.
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id csyncd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id cluster_file_op
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id BIGD_Subscrib
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id eventd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id %LACPD
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id lind
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id %istatsd
Oct 25 09:35:47 bigip1 notice mcpd[5206]: 01070410:5: Removed subscription with subscriber id logstatd
Oct 25 09:35:48 bigip1 info mcpd[5206]: 01070410:6: Per-invocation log rate exceeded; throttling.
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id cbrd
Oct 25 09:35:48 bigip1 notice scriptd[5641]: 014f0002:5: exiting
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id shell_publish
Oct 25 09:35:48 bigip1 info mcpd[5206]: 01070406:6: Per-invocation log rate exceeded; throttling.
Oct 25 09:35:48 bigip1 err mcpd[5206]: 01070069:3: Subscription not found in mcpd for subscriber Id stpd486
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id stpd4860-0
Oct 25 09:35:48 bigip1 notice sod[5970]: 010c0050:5: Sod requests links down.
Oct 25 09:35:48 bigip1 notice mcpd[5206]: 01070406:5: Removed publication with publisher id ha_table_publis
Oct 25 09:35:48 tmm crit tmm[7354]: 01010019:2: Caught signal 15, exiting
Oct 25 09:35:48 tmm1 crit tmm1[7355]: 01010019:2: Caught signal 15, exiting
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Received signal: SIGTERM (15)
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: 4.1 rx[OK 582 Bad 0] tx[OK 594 Bad 0]
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good rx at: 1351182947.482888
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good tx at: 1351182947.050705
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 rx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last 64 tx hist: 0x0000000000000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad rx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: : 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last four bad tx at: 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: : 0.000000 0.000000
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: 4.2 rx[OK 582 Bad 0] tx[OK 595 Bad 0]
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good rx at: 1351182947.482885
Oct 25 09:35:48 bigip1 info bcm56xxd[4863]: 012c0012:6: Last good tx at: 1351182947.050816
```

-- Exhibit --

Refer to the exhibits.

An LTM Specialist uses the information in the logs to determine the cause of a failover event in a high-availability (HA) pair.
What caused the failover?

- A. The overdog process crashed.
- B. The system was administratively rebooted.
- C. The process bcm56xxd received SIGTERM from the watchdog process.
- D. The configuration reload request caused the config to reload and the device to failover.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

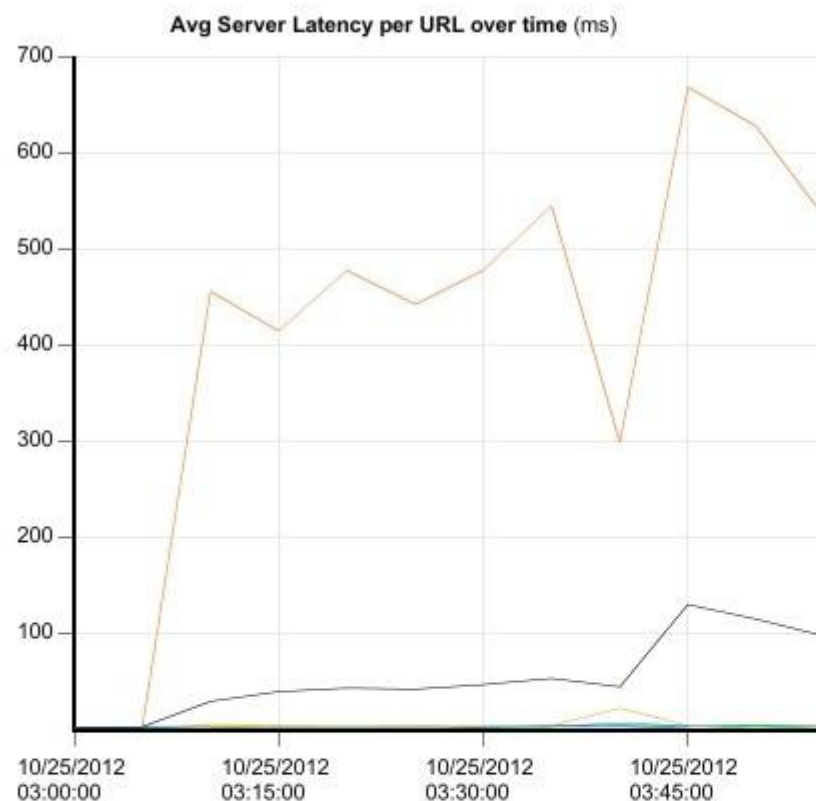
QUESTION 200

-- Exhibit

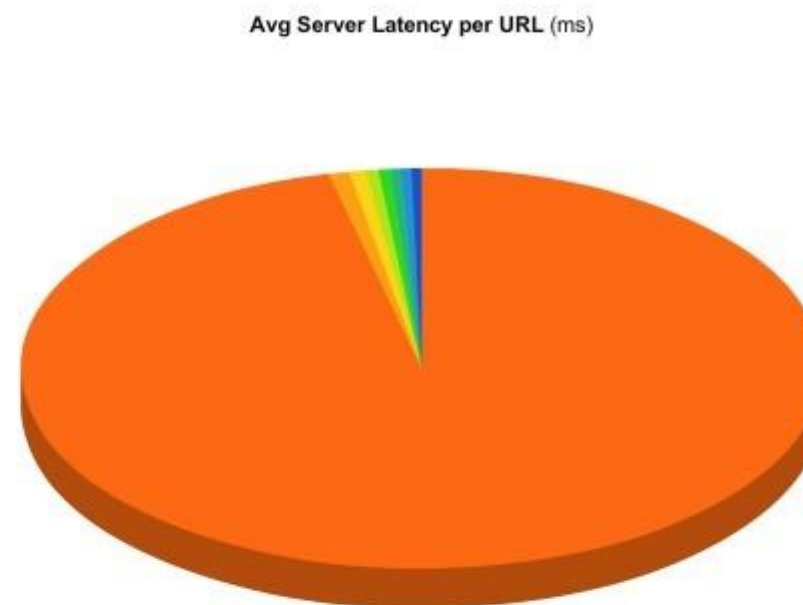
View By:

Time Period:

[Expand Advanced Filters](#)



Display method:



Measurement to display:

Details

<input checked="" type="checkbox"/>	#	URL	Avg Server Latency (ms)	Max Server Latency (ms)	Transactions
<input checked="" type="checkbox"/>	1	/slow1.php	502.12	1,551.00	459
<input checked="" type="checkbox"/>	2	/page14.cgi	4.33	408.00	506
<input checked="" type="checkbox"/>	3	/env.cgi	3.45	6.00	51
<input checked="" type="checkbox"/>	4	/not-logged-in.php	2.67	4.00	12
<input checked="" type="checkbox"/>	5	/safari.jpg	2.56	213.00	1,247
<input checked="" type="checkbox"/>	6	/slow2.php	2.21	12.00	358
<input checked="" type="checkbox"/>	7	/reflector.php	2.18	6.00	11

-- Exhibit --

Refer to the exhibit.

Which URL should be reported to the server/application team as getting user-visible errors?

- A. /env.cgi
- B. /page14.cgi
- C. /reflector.php
- D. /browserspecific.html

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 201

-- Exhibit

PACKET CAPTURE THROUGH LTM DEVICE - CONNECTING TO VIRTUAL SERVER

EXTERNAL VLAN

```
14:35:34.633300 IP 10.1.5.100.49857 > 10.3.20.20.80: F 1356:1356(0) ack 4557 win 16425
14:35:34.633315 IP 10.3.20.20.80 > 10.1.5.100.49857: . ack 1357 win 5735
14:35:34.634996 IP 10.3.20.20.80 > 10.1.5.100.49857: F 4557:4557(0) ack 1357 win 5735
14:35:34.636065 IP 10.1.5.100.49857 > 10.3.20.20.80: . ack 4558 win 16425
14:35:39.596671 IP 10.1.5.100.49862 > 10.3.20.20.80: S 2002327087:2002327087(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
14:35:39.596745 IP 10.3.20.20.80 > 10.1.5.100.49862: S 14638127:14638127(0) ack 2002327088 win 4380 <mss 1460,nop,wscale
14:35:39.598058 IP 10.1.5.100.49862 > 10.3.20.20.80: . ack 1 win 16425
14:35:39.599168 IP 10.1.5.100.49862 > 10.3.20.20.80: P 1:339(338) ack 1 win 16425
14:35:39.599187 IP 10.3.20.20.80 > 10.1.5.100.49862: . ack 339 win 4718
14:35:39.603044 IP 10.3.20.20.80 > 10.1.5.100.49862: P 1:342(341) ack 339 win 4718
14:35:39.643631 IP 10.1.5.100.49862 > 10.3.20.20.80: P 339:658(319) ack 342 win 16339
14:35:39.643664 IP 10.3.20.20.80 > 10.1.5.100.49862: . ack 658 win 5037
14:35:39.646203 IP 10.3.20.20.80 > 10.1.5.100.49862: P 342:1747(1405) ack 658 win 5037
14:35:39.653026 IP 10.1.5.100.49862 > 10.3.20.20.80: P 658:1007(349) ack 1747 win 16425
14:35:39.653072 IP 10.3.20.20.80 > 10.1.5.100.49862: . ack 1007 win 5386
14:35:39.654011 IP 10.1.5.100.49863 > 10.3.20.20.80: S 1569233346:1569233346(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
14:35:39.654095 IP 10.3.20.20.80 > 10.1.5.100.49863: S 1598764866:1598764866(0) ack 1569233347 win 4380 <mss 1460,nop,ws
14:35:39.655994 IP 10.3.20.20.80 > 10.1.5.100.49862: P 1747:3152(1405) ack 1007 win 5386
14:35:39.655966 IP 10.1.5.100.49863 > 10.3.20.20.80: . ack 1 win 16425
14:35:39.658973 IP 10.1.5.100.49862 > 10.3.20.20.80: P 1007:1356(349) ack 3152 win 16073
14:35:39.658989 IP 10.3.20.20.80 > 10.1.5.100.49862: . ack 1356 win 5735
14:35:39.660064 IP 10.3.20.20.80 > 10.1.5.100.49862: P 3152:4557(1405) ack 1356 win 5735
14:35:39.875355 IP 10.1.5.100.49862 > 10.3.20.20.80: . ack 4557 win 16425
```

INTERNAL VLAN

```
14:35:34.633317 IP 192.168.1.5.49857 > 192.168.1.100.80: F 2516122805:2516122805(0) ack 1308034121 win 8936
14:35:34.634973 IP 192.168.1.100.80 > 192.168.1.5.49857: F 1:1(0) ack 1 win 252
14:35:34.634993 IP 192.168.1.5.49857 > 192.168.1.100.80: . ack 2 win 8936
14:35:39.598151 IP 192.168.1.5.49862 > 192.168.1.100.80: S 2437134793:2437134793(0) win 4380 <mss 1460,nop,wscale 0,sack
14:35:39.600919 IP 192.168.1.100.80 > 192.168.1.5.49862: S 4240953911:4240953911(0) ack 2437134794 win 8192 <mss 1460,no
14:35:39.601215 IP 192.168.1.5.49862 > 192.168.1.100.80: . ack 1 win 4380
14:35:39.601221 IP 192.168.1.5.49862 > 192.168.1.100.80: P 1:339(338) ack 1 win 4380
14:35:39.603029 IP 192.168.1.100.80 > 192.168.1.5.49862: P 1:342(341) ack 339 win 256
14:35:39.603046 IP 192.168.1.5.49862 > 192.168.1.100.80: . ack 342 win 4721
14:35:39.643660 IP 192.168.1.5.49862 > 192.168.1.100.80: P 339:658(319) ack 342 win 4721
14:35:39.646180 IP 192.168.1.100.80 > 192.168.1.5.49862: P 342:1747(1405) ack 658 win 255
14:35:39.646207 IP 192.168.1.5.49862 > 192.168.1.100.80: . ack 1747 win 6126
14:35:39.653066 IP 192.168.1.5.49862 > 192.168.1.100.80: P 658:1007(349) ack 1747 win 6126
14:35:39.655978 IP 192.168.1.100.80 > 192.168.1.5.49862: P 1747:3152(1405) ack 1007 win 254
14:35:39.655997 IP 192.168.1.5.49862 > 192.168.1.100.80: . ack 3152 win 7531
14:35:39.656046 IP 192.168.1.5.49863 > 192.168.1.100.80: S 2540359239:2540359239(0) win 4380 <mss 1460,nop,wscale 0,sack
14:35:39.658047 IP 192.168.1.100.80 > 192.168.1.5.49863: S 1370955968:1370955968(0) ack 2540359240 win 8192 <mss 1460,
```

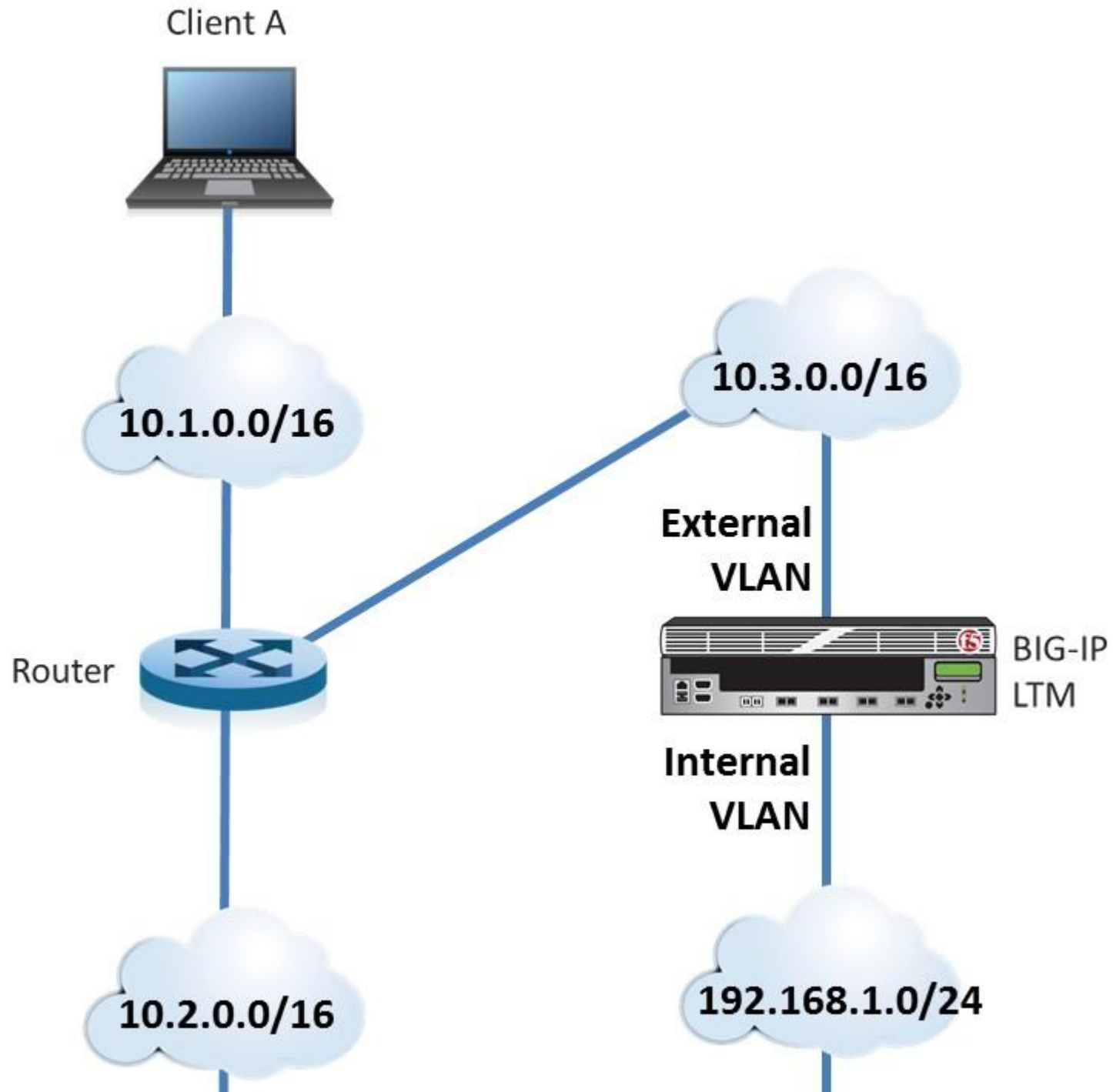

PACKET CAPTURE THROUGH LTM DEVICE - TRYING TO CONNECT DIRECTLY TO SERVER

EXTERNAL VLAN

```
14:32:49.057947 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:49.299299 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:52.077069 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:52.296629 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:58.092918 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,nop,sackOK>
14:32:58.312932 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,nop,sackOK>
```

INTERNAL VLAN

```
14:32:49.058417 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:49.299448 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:52.077090 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:52.296656 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,wscale 2,nop,nop>
14:32:58.092936 IP 10.1.5.100.49855 > 192.168.1.10.80: S 3803879960:3803879960(0) win 8192 <mss 1460,nop,nop,sackOK>
14:32:58.312960 IP 10.1.5.100.49856 > 192.168.1.10.80: S 2318792924:2318792924(0) win 8192 <mss 1460,nop,nop,sackOK>
```



-- Exhibit --

Refer to the exhibits.

Users are able to access the application when connecting to the virtual server but are unsuccessful when connecting directly to the application servers.
The LTM Specialist wants to allow direct access to the application servers.

Why are users unable to connect directly to the application servers?

- A. The router does NOT have a route to the server subnet.
- B. The web server does NOT have a correct default gateway.
- C. The LTM device does NOT have a SNAT on the External VLAN.
- D. The LTM device does NOT have an IP Forwarding virtual server on the Internal VLAN.
- E. The LTM device does NOT have an IP Forwarding virtual server on the External VLAN.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 202

-- Exhibit

PACKET CAPTURE AT LTM DEVICE - CONNECTING TO VIRTUAL SERVER

EXTERNAL VLAN

```
16:01:29.356966 IP 10.1.5.100.49885 > 10.3.20.20.80: S 2686165014:2686165014(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK,eol
16:01:29.357743 IP 10.3.20.20.80 > 10.1.5.100.49885: S 1853772182:1853772182(0) ack 2686165015 win 4380 <mss 1460,nop,wscale 2,nop,nop,sackOK,eol
16:01:29.359987 IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 1 win 16425
16:01:29.361309 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1:339(338) ack 1 win 16425
16:01:29.361327 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 339 win 4718
16:01:29.367040 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1:342(341) ack 339 win 4718
16:01:29.523013 IP 10.1.5.100.49885 > 10.3.20.20.80: P 339:658(319) ack 342 win 16339
16:01:29.523067 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 658 win 5037
16:01:29.526066 IP 10.3.20.20.80 > 10.1.5.100.49885: P 342:1747(1405) ack 658 win 5037
16:01:29.544197 IP 10.1.5.100.49886 > 10.3.20.20.80: S 2661471084:2661471084(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK,eol
16:01:29.544330 IP 10.3.20.20.80 > 10.1.5.100.49886: S 4091779980:4091779980(0) ack 2661471085 win 4380 <mss 1460,nop,wscale 2,nop,nop,sackOK,eol
16:01:29.544319 IP 10.1.5.100.49885 > 10.3.20.20.80: P 658:1007(349) ack 1747 win 16425
16:01:29.544329 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1007 win 5386
16:01:29.547133 IP 10.1.5.100.49886 > 10.3.20.20.80: . ack 1 win 16425
16:01:29.547026 IP 10.3.20.20.80 > 10.1.5.100.49885: P 1747:3152(1405) ack 1007 win 5386
16:01:29.575235 IP 10.1.5.100.49885 > 10.3.20.20.80: P 1007:1356(349) ack 3152 win 16073
16:01:29.575262 IP 10.3.20.20.80 > 10.1.5.100.49885: . ack 1356 win 5735
16:01:29.576974 IP 10.3.20.20.80 > 10.1.5.100.49885: P 3152:4557(1405) ack 1356 win 5735
16:01:29.797914 IP 10.1.5.100.49885 > 10.3.20.20.80: . ack 4557 win 16425
```

INTERNAL VLAN

```
16:01:29.360061 IP 192.168.1.5.49885 > 192.168.1.100.80: S 895389186:895389186(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol
16:01:29.364886 IP 192.168.1.100.80 > 192.168.1.5.49885: S 1666047010:1666047010(0) ack 895389187 win 8192 <mss 1460,nop,wscale 0,sackOK,eol
16:01:29.365020 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1 win 4380
16:01:29.365031 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1:339(338) ack 1 win 4380
16:01:29.366981 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1:342(341) ack 339 win 256
16:01:29.367073 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 342 win 4721
16:01:29.523051 IP 192.168.1.5.49885 > 192.168.1.100.80: P 339:658(319) ack 342 win 4721
16:01:29.526009 IP 192.168.1.100.80 > 192.168.1.5.49885: P 342:1747(1405) ack 658 win 255
16:01:29.526074 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 1747 win 6126
16:01:29.544329 IP 192.168.1.5.49885 > 192.168.1.100.80: P 658:1007(349) ack 1747 win 6126
16:01:29.547230 IP 192.168.1.5.49886 > 192.168.1.100.80: S 1454462415:1454462415(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol
16:01:29.546991 IP 192.168.1.100.80 > 192.168.1.5.49885: P 1747:3152(1405) ack 1007 win 254
16:01:29.547056 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 3152 win 7531
16:01:29.549134 IP 192.168.1.100.80 > 192.168.1.5.49886: S 786849220:786849220(0) ack 1454462416 win 8192 <mss 1460,nop,wscale 0,sackOK,eol
16:01:29.549159 IP 192.168.1.5.49886 > 192.168.1.100.80: . ack 1 win 4380
16:01:29.575259 IP 192.168.1.5.49885 > 192.168.1.100.80: P 1007:1356(349) ack 3152 win 7531
16:01:29.576958 IP 192.168.1.100.80 > 192.168.1.5.49885: P 3152:4557(1405) ack 1356 win 252
16:01:29.576978 IP 192.168.1.5.49885 > 192.168.1.100.80: . ack 4557 win 8936
16:01:34.564453 IP 192.168.1.5.49886 > 192.168.1.100.80: F 1:1(0) ack 1 win 4380
16:01:34.567472 IP 192.168.1.100.80 > 192.168.1.5.49886: R 1:1(0) ack 2 win 0
```

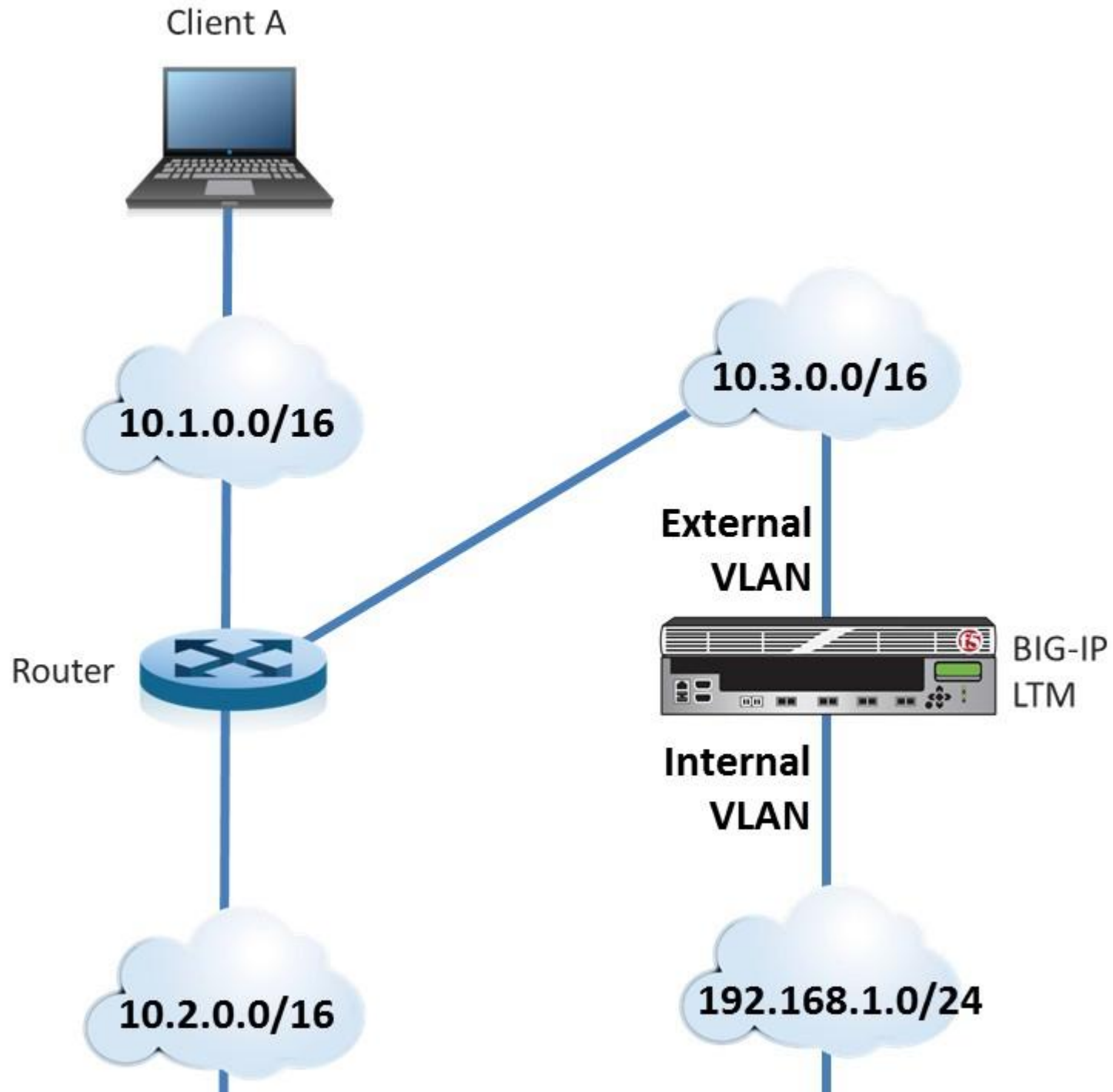
PACKET CAPTURE AT LTM DEVICE - TRYING TO CONNECT DIRECTLY TO SERVER

EXTERNAL VLAN

```
16:02:26.047441 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
16:02:26.285979 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
16:02:29.048674 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
16:02:29.283160 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,
16:02:35.065086 IP 10.1.5.100.49887 > 192.168.1.10.80: S 4152930596:4152930596(0) win 8192 <mss 1460,nop,nop,sackOK>
16:02:35.298372 IP 10.1.5.100.49888 > 192.168.1.10.80: S 1315604102:1315604102(0) win 8192 <mss 1460,nop,nop,sackOK>
```

INTERNAL VLAN

<no packets captured>



-- Exhibit --

Refer to the exhibits.

Users are able to access the application when connecting to the virtual server but are unsuccessful when connecting directly to the application servers.
The LTM Specialist wants to allow direct access to the application servers.

Which configuration change resolves this problem?

- A. Enable port 443 on the virtual server.
- B. Configure a SNAT pool on the LTM device.
- C. Disable address translation on the virtual server.
- D. Configure an IP Forwarding virtual server on the LTM device.
- E. Configure a route to the web server subnet on the network router.

Correct Answer: D

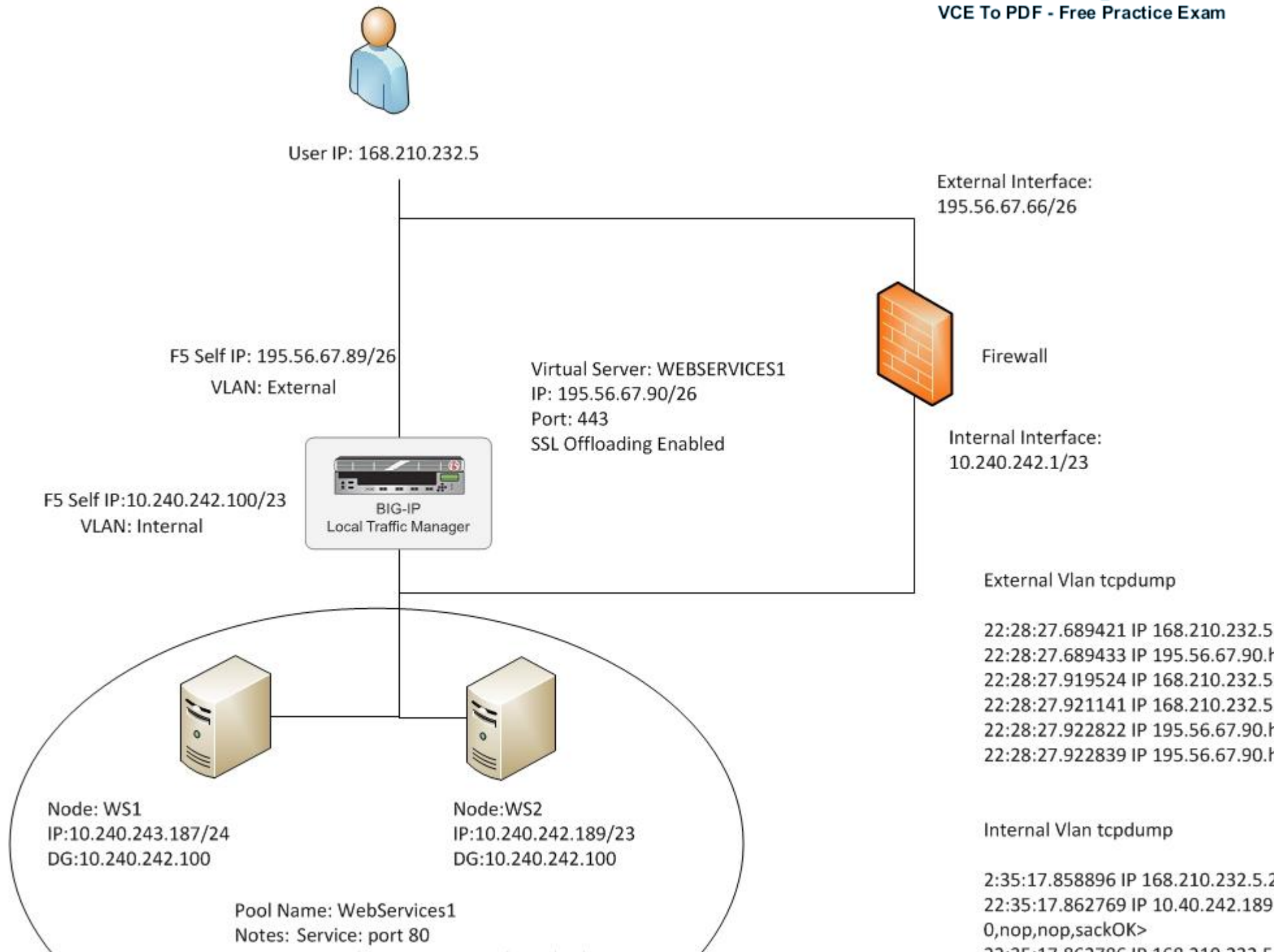
Section: (none)

Explanation

Explanation/Reference:

QUESTION 203

-- 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

Section: (none)

Explanation

Explanation/Reference: