更に上のクオリティ
更に上のサービス!

問題集

ITEXAMPASS

https://www.itexampass.jp

１年で無料進級することに提供する

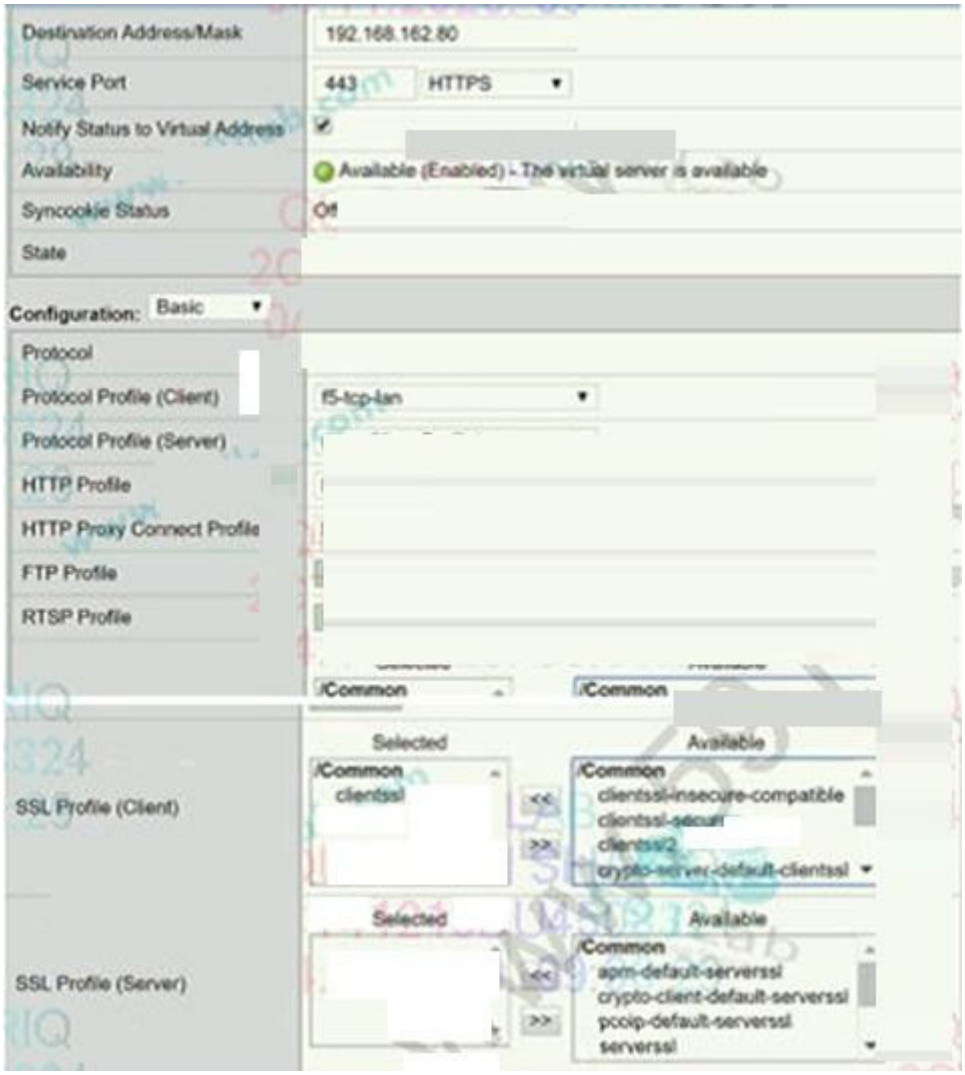
Exam : 201

Title : TMOS Administration

Version : DEMO

1.A user needs to determine known security vulnerabilities on an existing BIG-IP appliance and how to remediate these vulnerabilities.
Which action should the BIG-IP Administrator recommend?
A. Verify the TMOS version and review the release notes
B. Create a UCS archive and upload to Health
C. Create a UCS archive and open an F5 Support request
D. Generate a view and upload to Heath
Answer: D

2.Refer to the exhibit.



A BIG-IP Administrator needs to deploy an application on the BIG-IP system to perform SSL offload and re-encrypt the traffic to pool members.
During testing, users are unable to connect to the application.
What must the BIG-IP Administrator do to resolve the issue?
A. Remove the configured SSL Profile (Client)
B. Configure Protocol Profile (Server) as splitsession-default-tcp
C. Enable Forward Proxy in the SSL Profile (Client)
D. Configure an SSL Profile (Server)

Answer: D
Explanation:
According to the requirements of the subject, the client and server must be configured with ssl profile.

3.A BIG-IP device is configured with both an internal external and two Corporate VLANs. The virtual server has SNAT enabled and is set to listen on all VLANs Auto Last Hop is disabled. The Corporate users are on 10.0.0.0./24 and 172.16.0.0/12. The BIG-IP has a Self-IP on the 1.0.0.0.0./24 subnet. Internet users are able to access the virtual server. Only some of the Corporate users are able to connect
to the virtual server A BIG-IP Administrator performs a tcpdump on the BIG-IP and verifies that traffic is arriving from users in 10.0.0.0/24.
What should the BIG-IP Administrator do to correct this behaviour?
A. Disable the server on the internal VLAN
B. Add a static route for the 172.16.0.0/12 subnet
C. Change the default route to point to the extra firewall
D. Modify the default route of the servers to point to the BIG-IP device
Answer: B

4.A node is a member of various pools and hosts different web applications. If a web application is unavailable, the BIG-IP appliance needs to mark the pool member down for that application pool.
What should a BIG-IP Administrator deploy at the pool level to accomplish this?
A. A UDP monitor with a custom interval/timeout
B. A combination of ICMP + TCP monitor
C. An HTTP monitor with custom send/receive strings
D. A TCP monitor with a custom interval/timeout
Answer: C
Explanation:
Requiring all traffic to be HTTPS access requires HTTP requests to be redirected directly to HTTPS.

5.The ICMP monitor has been assigned to all nodes. In addition, all pools have been assigned custom monitors. The pool is marked available.
If a pool is marked available (green) which situation is sufficient to cause this?
A. All of the pool member nodes are responding to the ICMP monitor as expected.
B. Less than 50% of the pool member nodes responded to the ICMP echo request.
C. All of the members of the pool have had their content updated recently and their responses no longer match the monitor.
D. Over 25% of the pool members have had their content updated and it no longer matches the receive rule of the custom monitor. The other respond as expected.
Answer: D