



CERTSWARRIOR

CompTIA CV0-003

CompTIA Cloud+ Certification Exam

Questions&AnswersPDF

ForMoreInformation:

<https://www.certswarrior.com/>

Features:

- 90DaysFreeUpdates
- 30DaysMoneyBackGuarantee
- InstantDownloadOncePurchased
- 24/7OnlineChat Support
- ItsLatestVersion

Latest Version: 20.3

Topic 1, Exam Pool A

Question: 1

SIMULATION

A company has decided to scale its e-commerce application from its corporate datacenter to a commercial cloud provider to meet an anticipated increase in demand during an upcoming holiday. The majority of the application load takes place on the application server under normal conditions. For this reason, the company decides to deploy additional application servers into a commercial cloud provider using the on-premises orchestration engine that installs and configures common software and network configurations.

The remote computing environment is connected to the on-premises datacenter via a site-to-site IPSec tunnel. The external DNS provider has been configured to use weighted round-robin routing to load balance connections from the Internet.

During testing, the company discovers that only 20% of connections completed successfully.

INSTRUCTIONS

Review the network architecture and supporting documents and fulfill these requirements:

Part 1:

Analyze the configuration of the following components: DNS, Firewall 1, Firewall 2, Router 1, Router 2, VPN and Orchestrator Server.

Identify the problematic device(s).

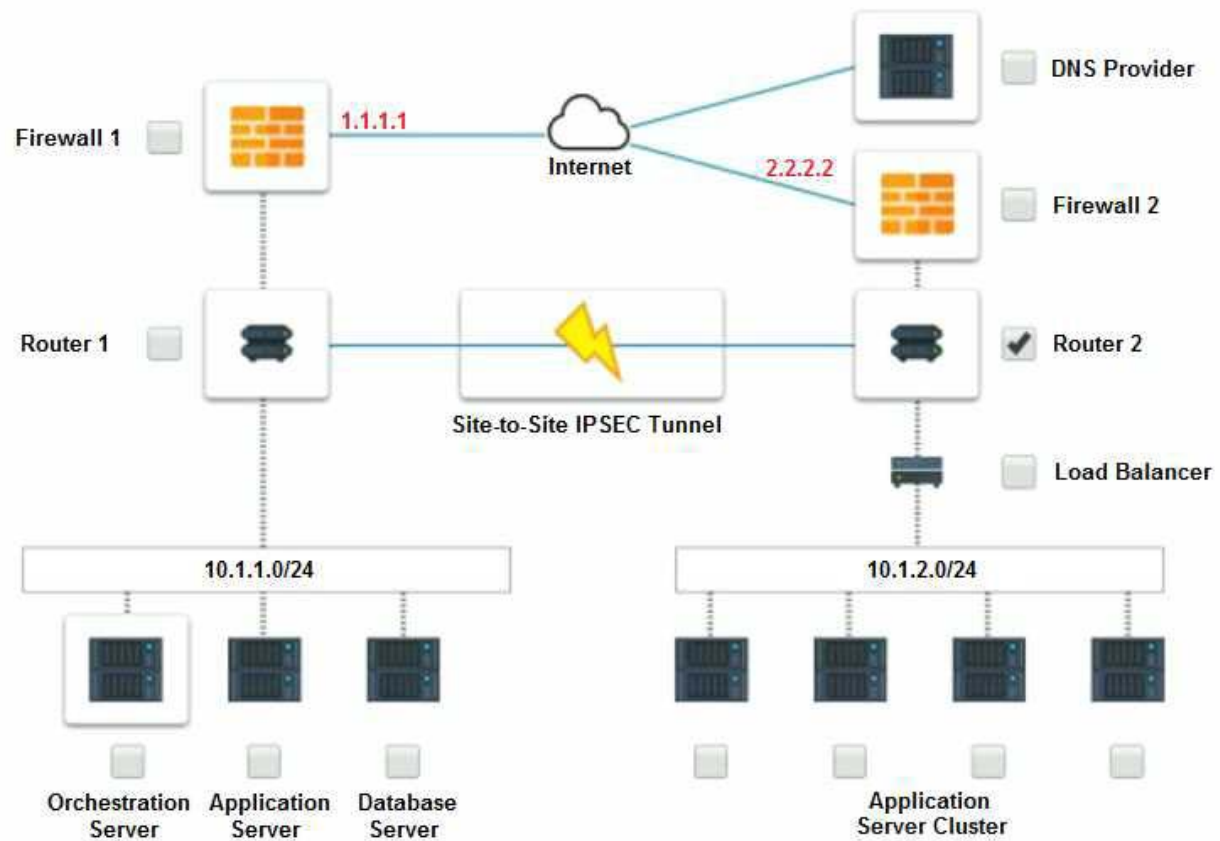
Part 2:

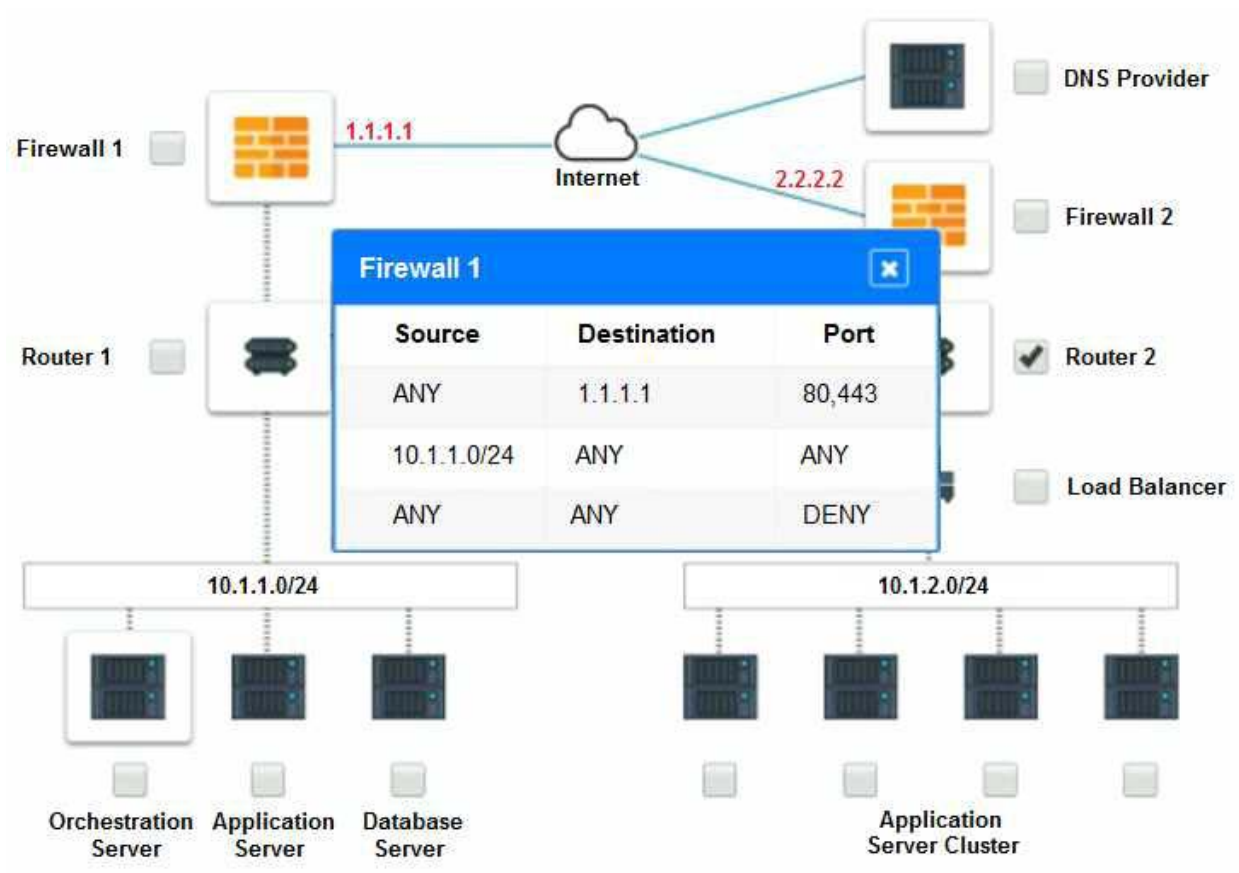
Identify the correct options to provide adequate configuration for hybrid cloud architecture.

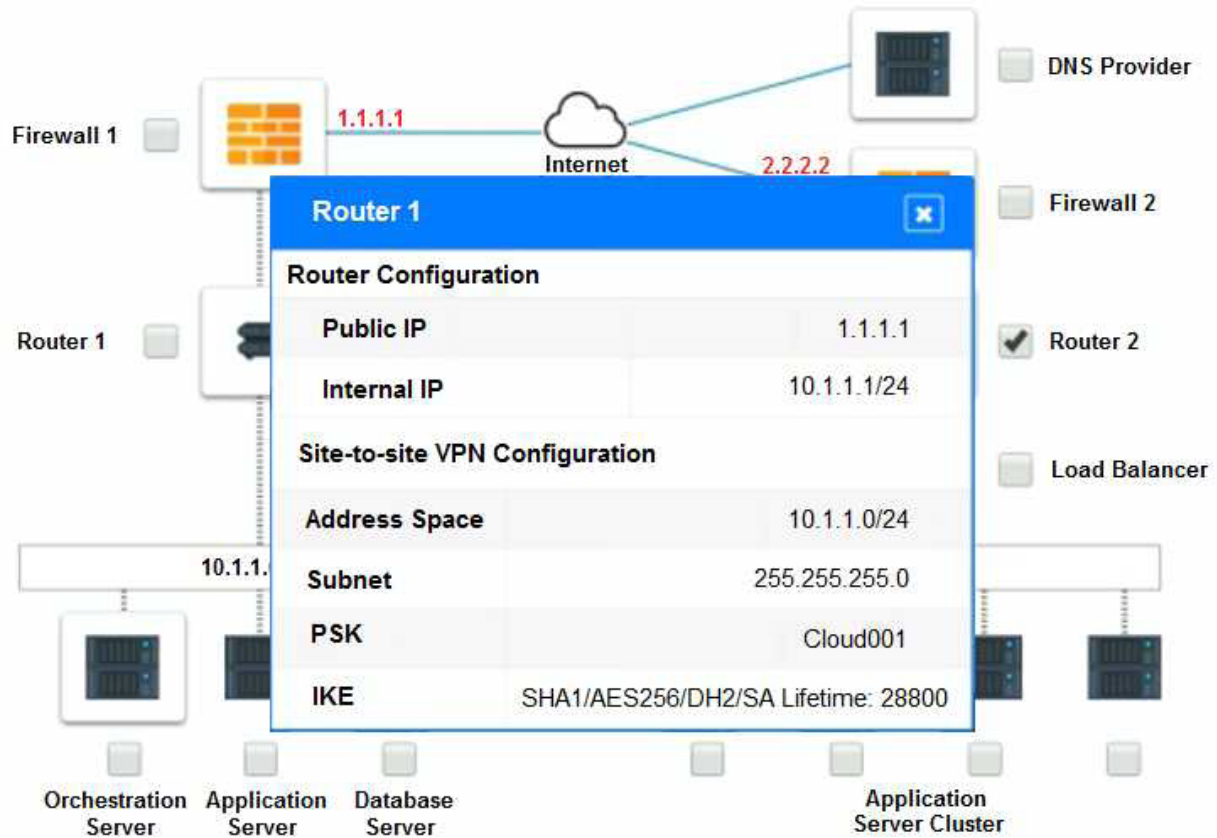
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

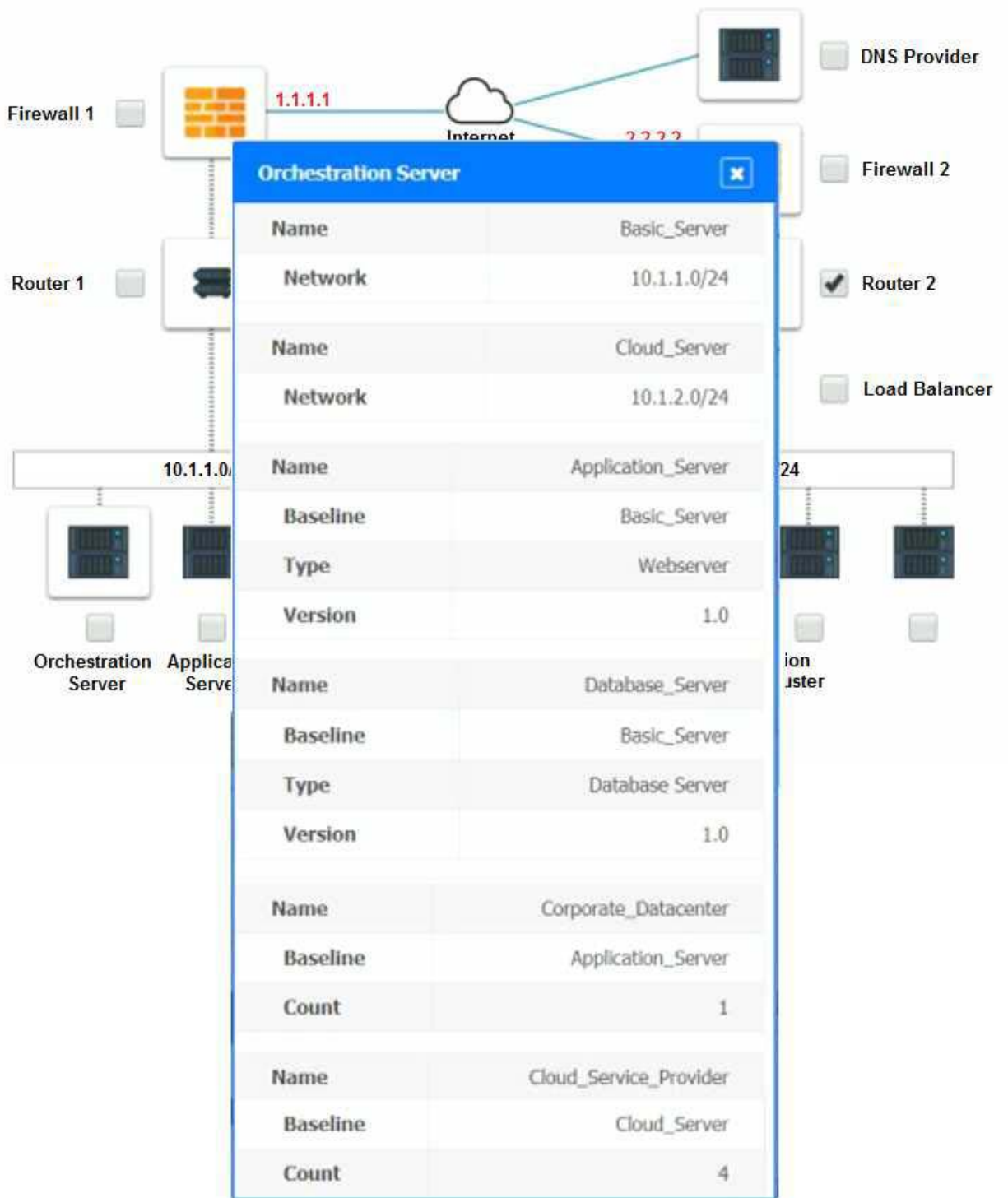
Part 1:

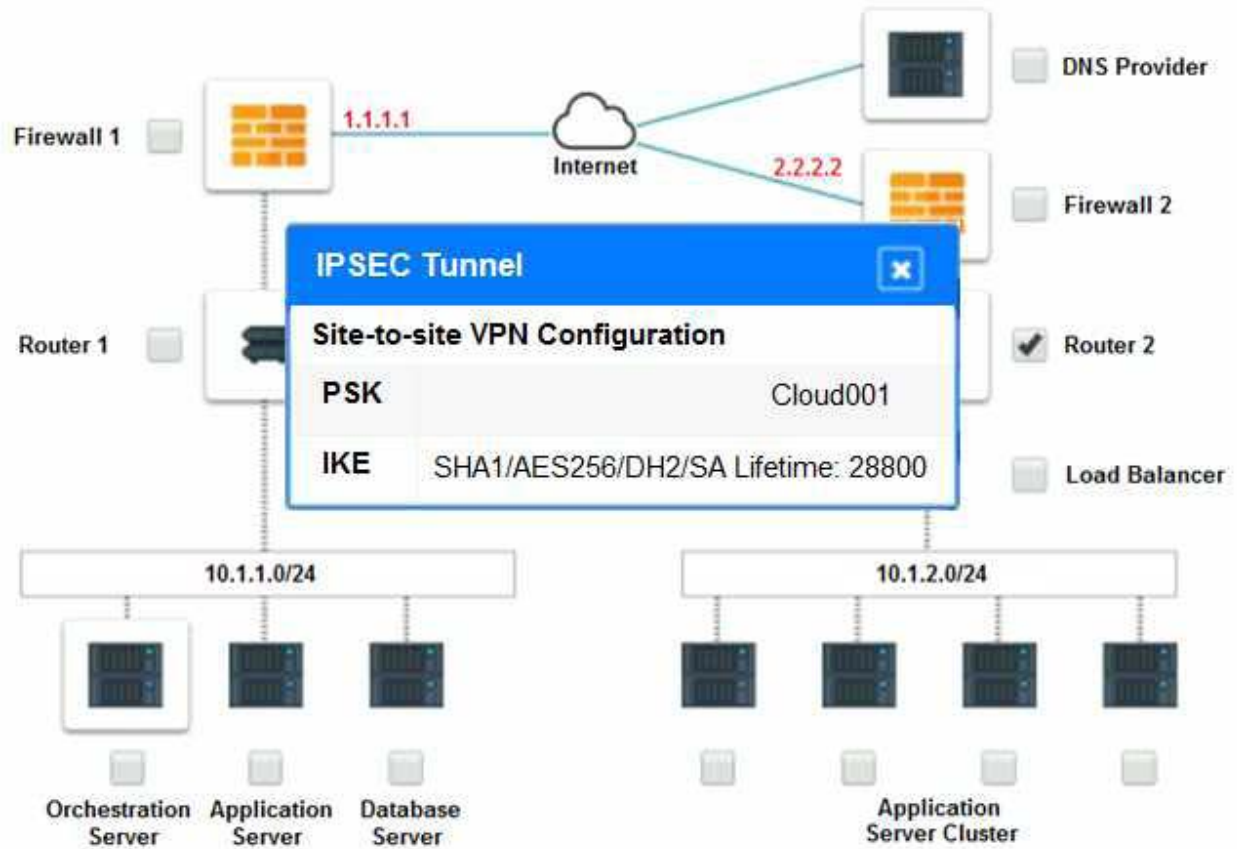
Cloud Hybrid Network Diagram

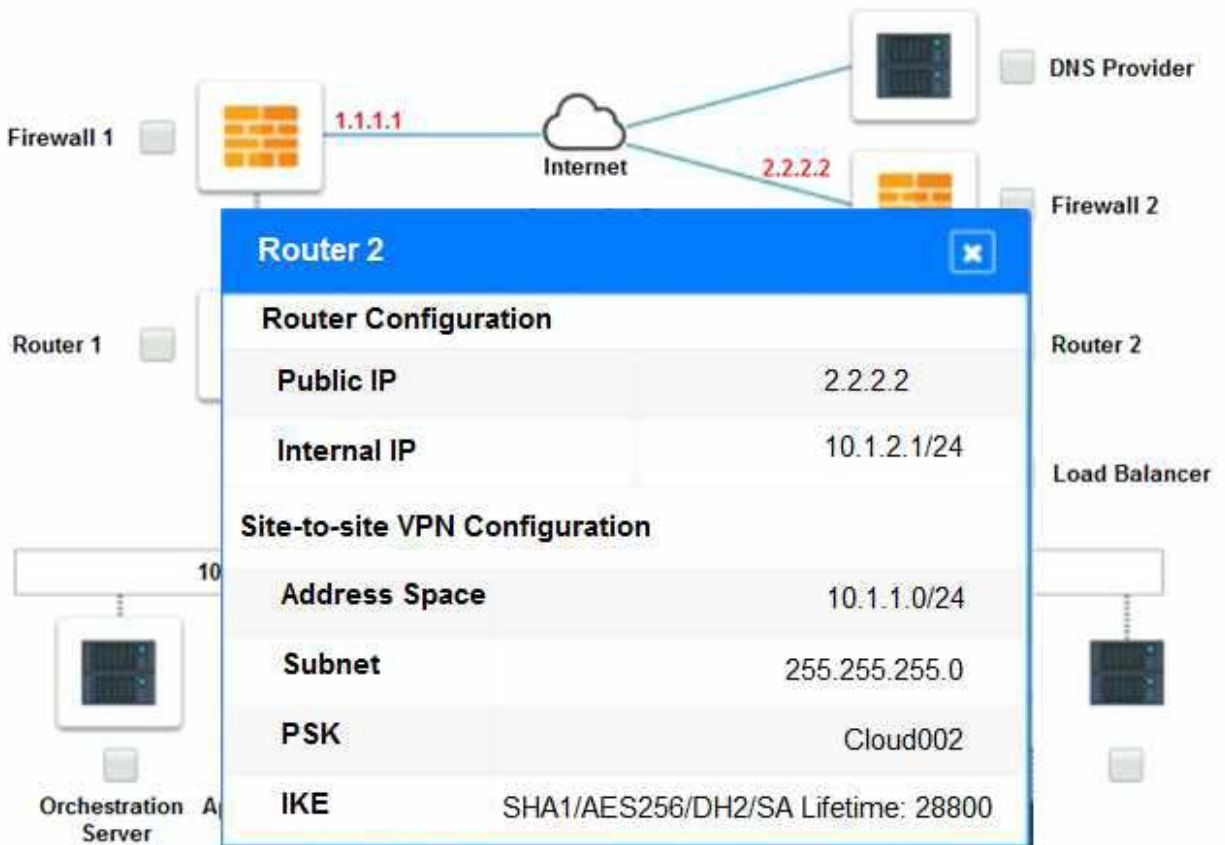


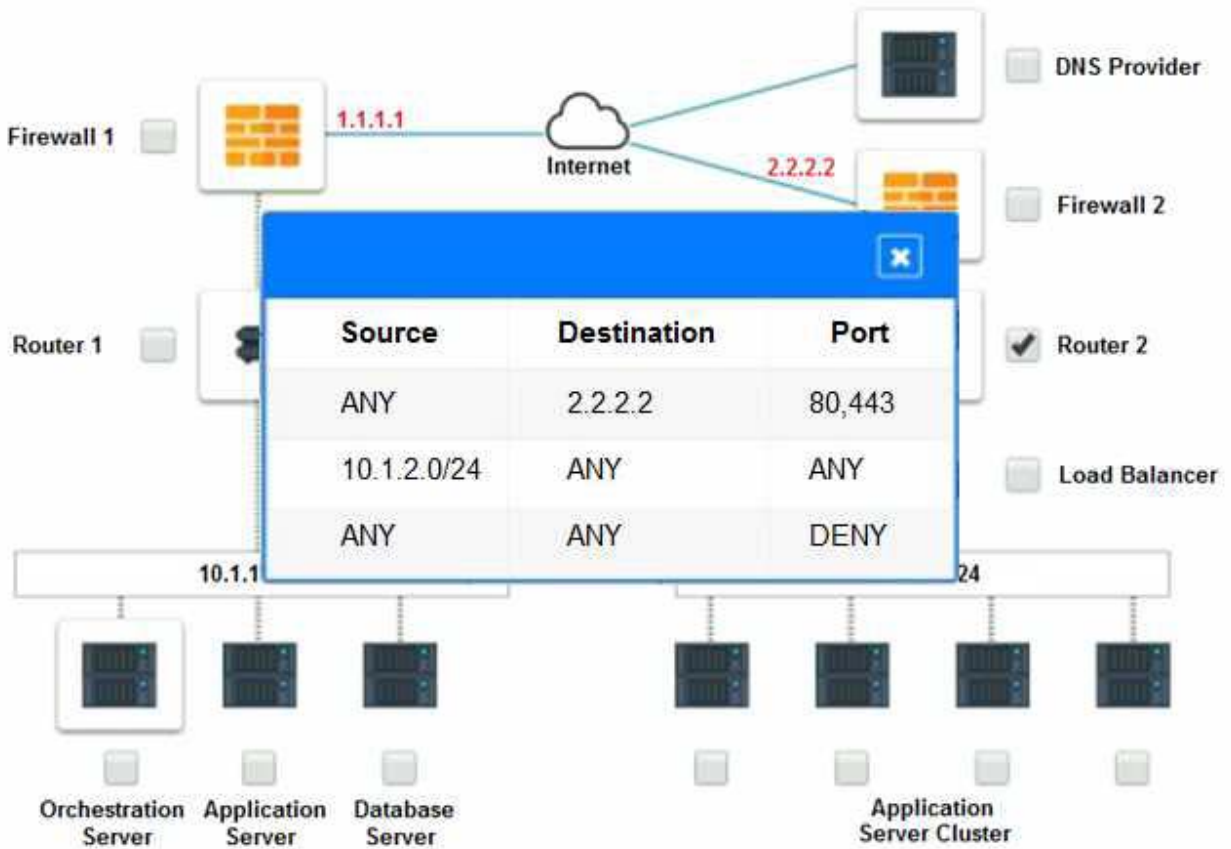


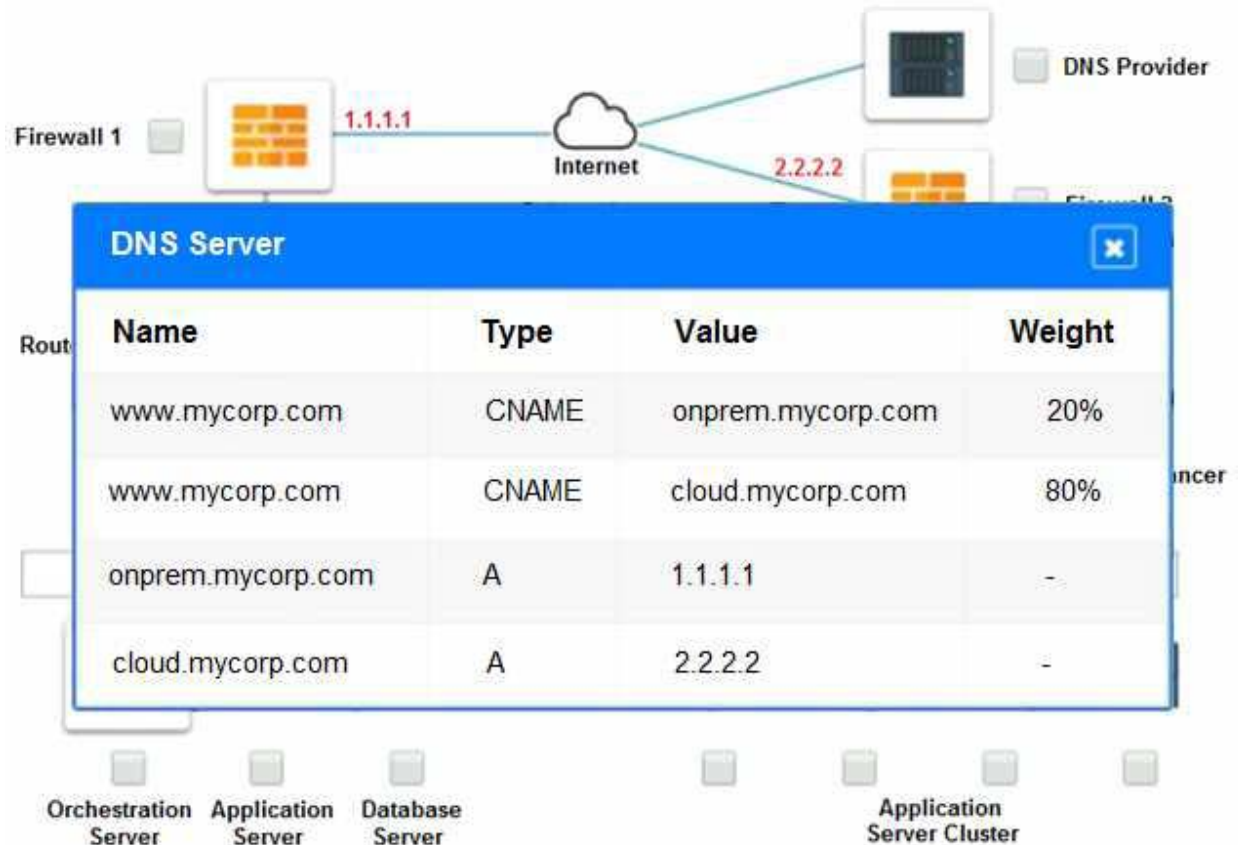












Part 2:

Only select a maximum of TWO options from the multiple choice question

- ☐ Deploy a Replica of the Database Server in the Cloud Provider.
- ☐ Update the PSK (Pre-shared key) in Router 2.
- ☐ Update the A record on the DNS from 2.2.2.2 to 1.1.1.1.
- ☐ Promote deny All to allow All in Firewall 1 and Firewall 2.
- ☐ Change the Address Space on Router 2.
- ☐ Change internal IP Address of Router 1.
- ☐ Reverse the Weight property in the two CNAME records on the DNS.
- ☐ Add the Application Server at on-premises to the Load Balancer.

Answer: See explanation below.

Explanation:

Part 1: Router 2

The problematic device is Router 2, which has an incorrect configuration for the IPSec tunnel. The IPSec tunnel is a secure connection between the on-premises datacenter and the cloud provider, which allows the traffic to flow between the two networks. The IPSec tunnel requires both endpoints to have matching parameters, such as the IP addresses, the pre-shared key (PSK), the encryption and authentication algorithms, and the security associations (SAs) .

According to the network diagram and the configuration files, Router 2 has a different PSK and a different address space than Router 1. Router 2 has a PSK of "1234567890", while Router 1 has a PSK of "0987654321". Router 2 has an address space of 10.0.0.0/8, while Router 1 has an address space of 192.168.0.0/16. These mismatches prevent the IPSec tunnel from establishing and encrypting the traffic between the two networks.

The other devices do not have any obvious errors in their configuration. The DNS provider has two CNAME records that point to the application servers in the cloud provider, with different weights to balance the load. The firewall rules allow the traffic from and to the application servers on port 80 and port 443, as well as the traffic from and to the VPN server on port 500 and port 4500. The orchestration server has a script that installs and configures the application servers in the cloud provider, using the DHCP server to assign IP addresses.

Part 2:

The correct options to provide adequate configuration for hybrid cloud architecture are:

Update the PSK in Router 2.

Change the address space on Router 2.

These options will fix the IPSec tunnel configuration and allow the traffic to flow between the onpremises

datacenter and the cloud provider. The PSK should match the one on Router 1, which is "0987654321". The address space should also match the one on Router 1, which is 192.168.0.0/16.

B. Update the PSK (Pre-shared key in Router2)

E. Change the Address Space on Router2

Question: 2

The QA team is testing a newly implemented clinical trial management (CTM) SaaS application that uses a business intelligence application for reporting. The UAT users were instructed to use HTTP and HTTPS. Refer to the application dataflow:

1A – The end user accesses the application through a web browser to enter and view clinical data.

2A – The CTM application server reads/writes data to/from the database server.

1B – The end user accesses the application through a web browser to run reports on clinical data.

2B – The CTM application server makes a SOAP call on a non-privileged port to the BI application server.

3B – The BI application server gets the data from the database server and presents it to the CTM application server.

When UAT users try to access the application using <https://ctm.app.com> or <http://ctm.app.com>, they get a message stating: "Browser cannot display the webpage." The QA team has raised a ticket to troubleshoot the issue.

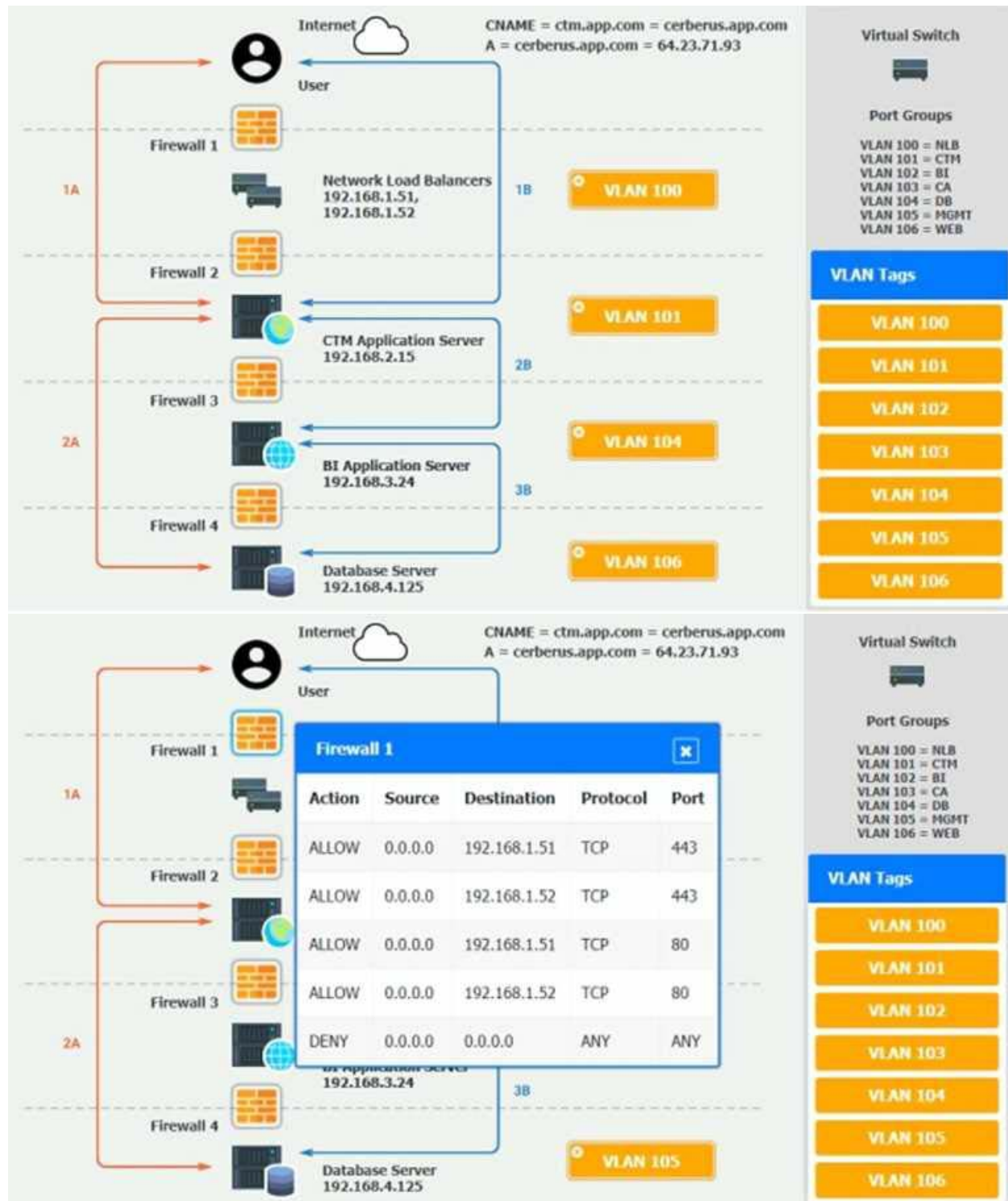
INSTRUCTIONS

You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.

You should ensure the firewall rules are allowing only the traffic based on the dataflow.

You have already verified the external DNS resolution and NAT are working.

Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Internet CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93

Virtual Switch

Port Groups

VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB

VLAN Tags

VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106

Firewall 2

Action	Source	Destination	Protocol	Port
ALLOW	192.168.1.51	192.168.2.15	TCP	88
DENY	192.168.1.52	0.0.0.0	TCP	80
ALLOW	0.0.0.0	127.0.0.1	UDP	88
DENY	127.0.0.1	64.23.71.93	ANY	443
ALLOW	64.23.71.93	192.168.1.51	UDP	1533
DENY	192.168.1.51	192.168.1.52	ANY	9400
DENY	192.168.2.15	192.168.2.24	TCP	443
DENY	192.168.2.24	192.168.3.24	TCP	443
DENY	192.168.3.24	192.168.4.125	TCP	443
DENY	192.168.4.125	0.0.0.0	ANY	ANY

Reset Answer Save Close

Database Server 192.168.4.125

VLAN 105

Internet CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93

Virtual Switch

Port Groups

VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB

VLAN Tags

VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106

Firewall 3

Action	Source	Destination	Protocol	Port
DENY	0.0.0.0	0.0.0.0	ANY	ANY
ALLOW	192.168.2.15	192.168.3.24	TCP	9400
ALLOW	192.168.2.15	192.168.4.125	TCP	1533

Reset Answer Save Close

Application Server 192.168.3.24

Firewall 4

Database Server 192.168.4.125

VLAN 105

Internet CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93

Virtual Switch

Port Groups

VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB

VLAN Tags

VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106

1A

2A

3B

3C

3D

3E

3F

3G

3H

3I

3J

3K

3L

3M

3N

3O

3P

3Q

3R

3S

3T

3U

3V

3W

3X

3Y

3Z

3AA

3AB

3AC

3AD

3AE

3AF

3AG

3AH

3AI

3AJ

3AK

3AL

3AM

3AN

3AO

3AP

3AQ

3AR

3AS

3AT

3AU

3AV

3AW

3AX

3AY

3AZ

3BA

3BB

3BC

3BD

3BE

3BF

3BG

3BH

3BI

3BJ

3BK

3BL

3BM

3BN

3BO

3BP

3BQ

3BR

3BS

3BT

3BU

3BV

3BW

3BX

3BY

3BZ

3CA

3CB

3CC

3CD

3CE

3CF

3CG

3CH

3CI

3CJ

3CK

3CL

3CM

3CN

3CO

3CP

3CQ

3CR

3CS

3CT

3CU

3CV

3CW

3CX

3CY

3CZ

3DA

3DB

3DC

3DD

3DE

3DF

3DG

3DH

3DI

3DJ

3DK

3DL

3DM

3DN

3DO

3DP

3DQ

3DR

3DS

3DT

3DU

3DV

3DW

3DX

3DY

3DZ

3EA

3EB

3EC

3ED

3EE

3EF

3EG

3EH

3EI

3EJ

3EK

3EL

3EM

3EN

3EO

3EP

3EQ

3ER

3ES

3ET

3EU

3EV

3EW

3EX

3EY

3EZ

3FA

3FB

3FC

3FD

3FE

3FF

3FG

3FH

3FI

3FJ

3FK

3FL

3FM

3FN

3FO

3FP

3FQ

3FR

3FS

3FT

3FU

3FV

3FW

3FX

3FY

3FZ

3GA

3GB

3GC

3GD

3GE

3GF

3GG

3GH

3GI

3GJ

3GK

3GL

3GM

3GN

3GO

3GP

3GQ

3GR

3GS

3GT

3GU

3GV

3GW

3GX

3GY

3GZ

3HA

3HB

3HC

3HD

3HE

3HF

3HG

3HH

3HI

3HJ

3HK

3HL

3HM

3HN

3HO

3HP

3HQ

3HR

3HS

3HT

3HU

3HV

3HW

3HX

3HY

3HZ

3IA

3IB

3IC

3ID

3IE

3IF

3IG

3IH

3II

3IJ

3IK

3IL

3IM

3IN

3IO

3IP

3IQ

3IR

3IS

3IT

3IU

3IV

3IW

3IX

3IY

3IZ

3JA

3JB

3JC

3JD

3JE

3JF

3JG

3JH

3JI

3JJ

3JK

3JL

3JM

3JN

3JO

3JP

3JQ

3JR

3JS

3JT

3JU

3JV

3JW

3JX

3JY

3JZ

3KA

3KB

3KC

3KD

3KE

3KF

3KG

3KH

3KI

3KJ

3KK

3KL

3KM

3KN

3KO

3KP

3KQ

3KR

3KS

3KT

3KU

3KV

3KW

3KX

3KY

3KZ

3LA

3LB

3LC

3LD

3LE

3LF

3LG

3LH

3LI

3LJ

3LK

3LL

3LM

3LN

3LO

3LP

3LQ

3LR

3LS

3LT

3LU

3LV

3LW

3LX

3LY

3LZ

3MA

3MB

3MC

3MD

3ME

3MF

3MG

3MH

3MI

3MJ

3MK

3ML

3MN

3MO

3MP

3MQ

3MR

3MS

3MT

3MU

3MV

3MW

3MX

3MY

3MZ

3NA

3NB

3NC

3ND

3NE

3NF

3NG

3NH

3NI

3NJ

3NK

3NL

3NO

3NP

3NQ

3NR

3NS

3NT

3NU

3NV

3NW

3NX

3NY

3NZ

3OA

3OB

3OC

3OD

3OE

3OF

3OG

3OH

3OI

3OJ

3OK

3OL

3OM

3ON

3OO

3OP

3OQ

3OR

3OS

3OT

3OU

3OV

3OW

3OX

3OY

3OZ

3PA

3PB

3PC

3PD

3PE

3PF

3PG

3PH

3PI

3PJ

3PK

3PL

3PM

3PN

3PO

3PP

3PQ

3PR

3PS

3PT

3PU

3PV

3PW

3PX

3PY

3PZ

3QA

3QB

3QC

3QD

3QE

3QF

3QG

3QH

3QI

3QJ

3QK

3QL

3QM

3QN

3QO

3QP

3QQ

3QR

3QS

3QT

3QU

3QV

3QW

3QX

3QY

3QZ

3RA

3RB

3RC

3RD

3RE

3RF

3RG

3RH

3RI

3RJ

3RK

3RL

3RM

3RN

3RO

3RP

3RQ

3RR

3RS

3RT

3RU

3RV

3RW

3RX

3RY

3RZ

3SA

3SB

3SC

3SD

3SE

3SF

3SG

3SH

3SI

3SJ

3SK

3SL

3SM

3SN

3SO

3SP

3SQ

3SR

3SS

3ST

3SU

3SV

3SW

3SX

3SY

3SZ

3TA

3TB

3TC

3TD

3TE

3TF

3TG

3TH

3TI

3TJ

3TK

3TL

3TM

3TN

3TO

3TP

3TQ

3TR

3TS

3TT

3TU

3TV

3TW

3TX

3TY

3TZ

3UA

3UB

3UC

3UD

3UE

3UF

3UG

3UH

3UI

3UJ

3UK

3UL

3UM

3UN

3UO

3UP

3UQ

3UR

3US

3UT

3UU

3UV

3UW

3UX

3UY

3UZ

3VA

3VB

3VC

3VD

3VE

3VF

3VG

3VH

3VI

3VJ

3VK

3VL

3VM

3VN

3VO

3VP

3VQ

3VR

3VS

3VT

3VU

3VV

3VW

3VX

3VY

3VZ

3WA

3WB

3WC

3WD

3WE

3WF

3WG

3WH

3WI

3WJ

3WK

3WL

3WM

3WN

3WO

3WP

3WQ

3WR

3WS

3WT

3WU

3WV

3WW

3WX

3WY

3WZ

3XA

3XB

3XC

3XD

3XE

3XF

3XG

3XH

3XI

3XJ

3XK

3XL

3XM

3XN

3XO

3XP

3XQ

3XR

3XS

3XT

3XU

3XV

3XW

3XX

3XY

3XZ

3YA

3YB

3YC

3YD

3YE

3YF

3YG

3YH

3YI

3YJ

3YK

3YL

3YM

3YN

3YO

3YP

3YQ

3YR

3YS

3YT

3YU

3YV

3YW

3YX

3YY

3YZ

3ZA

3ZB

3ZC

3ZD

3ZE

3ZF

3ZG

3ZH

3ZI

3ZJ

3ZK

3ZL

3ZM

3ZN

3ZO

3ZP

3ZQ

3ZR

3ZS

3ZT

3ZU

3ZV

3ZW

3ZX

3ZY

3ZZ



Answer: See explanation below.

Explanation:

On firewall 3, change the DENY 0.0.0.0 entry to rule 3 not rule 1.

Question: 3

A DevOps administrator is automating an existing software development workflow. The administrator wants to ensure that prior to any new code going into production, tests confirm the new code does not negatively impact existing automation activities.

Which of the following testing techniques would be BEST to use?

- A. Usability testing
- B. Regression testing
- C. Vulnerability testing
- D. Penetration testing

Answer: B

Explanation:

Regression testing is a type of testing that ensures that new code or changes to existing code do not break or degrade the functionality of the software. Regression testing is often used in software

development workflows to verify that new features or bug fixes do not introduce new errors or affect the performance of the software. Regression testing can help prevent negative impacts on existing automation activities by checking that the new code is compatible with the existing code and does not cause any unexpected failures or errors. Reference: [CompTIA Cloud+ Certification Exam Objectives](#), page 19, section 4.1

Reference: <https://www.softwaretestinghelp.com/regression-testing-tools-and-methods/>

Question: 4

A marketing team is using a SaaS-based service to send emails to large groups of potential customers. The internally managed CRM system is configured to generate a list of target customers automatically on a weekly basis, and then use that list to send emails to each customer as part of a marketing campaign.

Last week, the first email campaign sent emails successfully to 3,000 potential customers. This week, the email campaign attempted to send out 50,000 emails, but only 10,000 were sent.

Which of the following is the MOST likely reason for not sending all the emails?

- A. API request limit
- B. Incorrect billing account
- C. Misconfigured auto-scaling
- D. Bandwidth limitation

Answer: A

Explanation:

An API request limit is a restriction on the number of requests that can be made to a web service or application programming interface (API) within a certain time period. API request limits are often used by SaaS-based services to control the usage and traffic of their customers and prevent overloading or abuse of their resources. An API request limit can cause a failure to send all the emails if the marketing team exceeds the number of requests allowed by the SaaS-based service in a week. The service may reject or block any requests that go beyond the limit, resulting in fewer emails being sent than expected.

Reference: [CompTIA Cloud+ Certification Exam Objectives](#), page 13, section 2.5

Reference: <https://developers.google.com/analytics/devguides/config/mgmt/v3/limits-quotas>

Question: 5

A VDI administrator has received reports of poor application performance.

Which of the following should the administrator troubleshoot FIRST?

- A. The network environment
- B. Container resources
- C. Client devices
- D. Server resources

Answer: A

Explanation:

The network environment is the set of network devices, connections, protocols, and configurations that enable communication and data transfer between different systems and applications. The network environment can affect the performance of a virtual desktop infrastructure (VDI) by influencing factors such as bandwidth, latency, jitter, packet loss, and congestion. Poor network performance can result in slow or unreliable application delivery, degraded user experience, and reduced productivity. Therefore, troubleshooting the network environment should be the first step for a VDI administrator who receives reports of poor application performance. Reference: [CompTIA Cloud+ Certification Exam Objectives](#), page 17, section 3.4



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ