CompTIA

CV0-003 Exam

CompTIA Cloud+ Certification Exam

Questions & Answers
Demo

Version: 14.0

Question: 1

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:

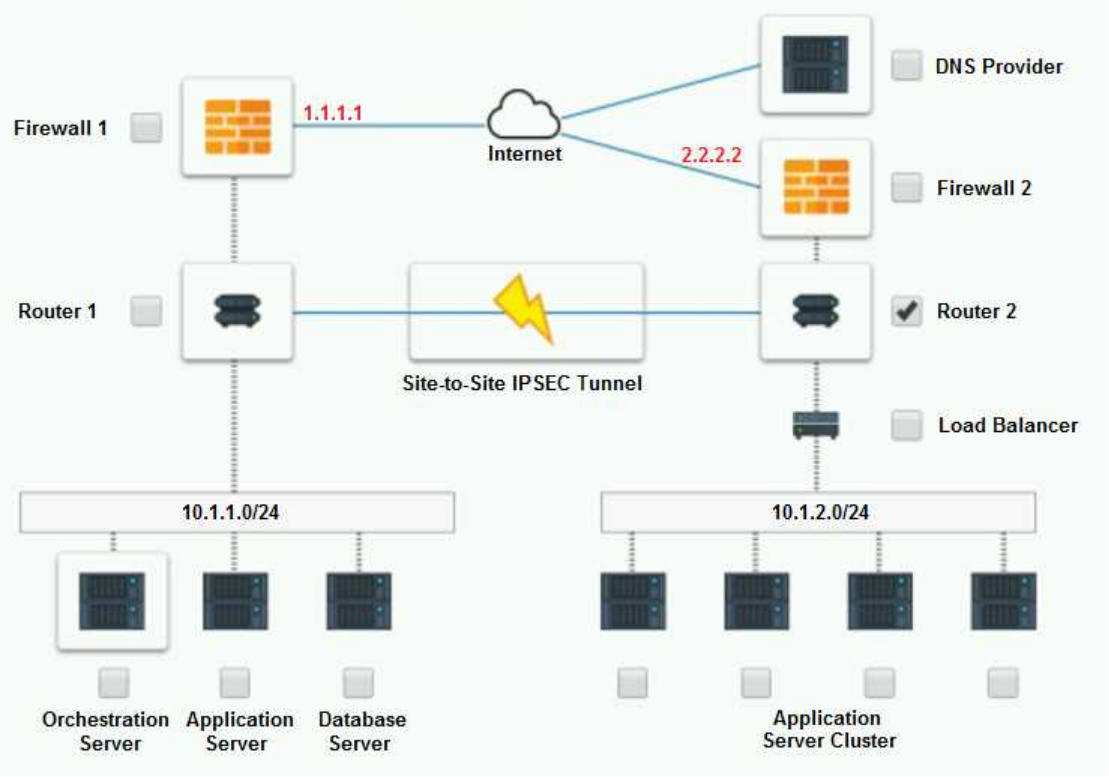
Part 1:
- Analyze the configuration of the following components: DNS, Firewall 1, Firewall 2, Router 1, Router 2, VPN and Orchestrator Server.
- Identify the problematic device(s).

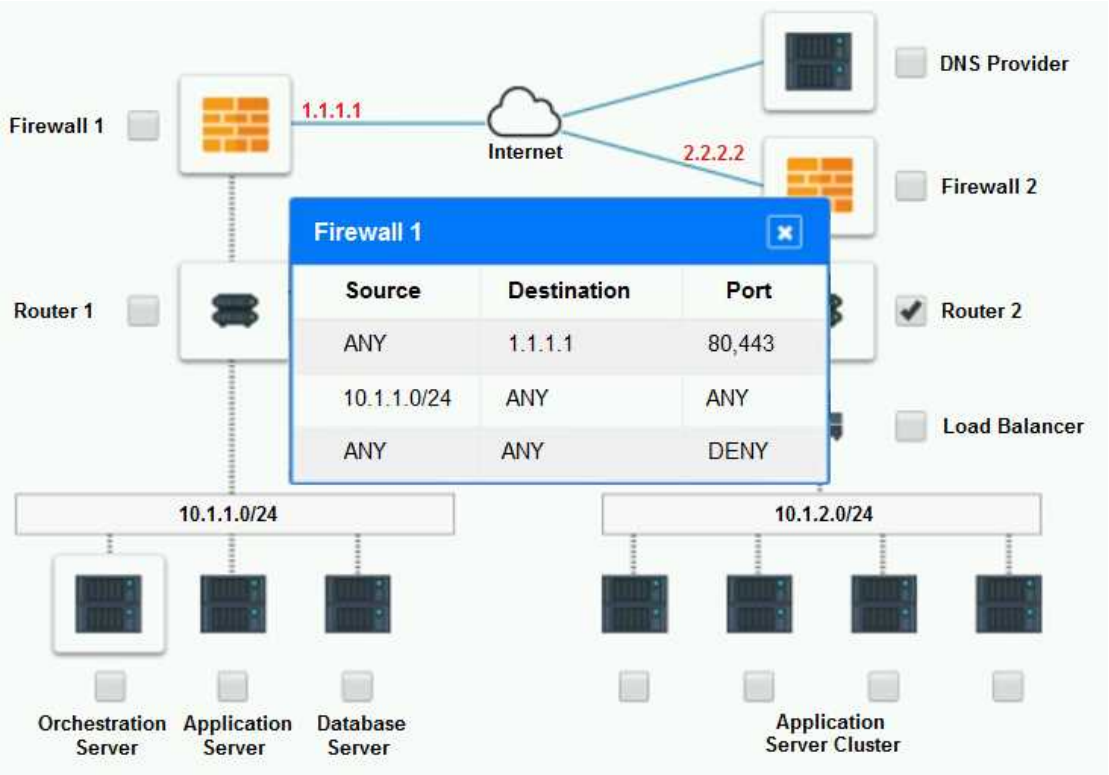
Part 2:
- Identify the correct options to provide adequate configuration for hybrid cloud architecture.

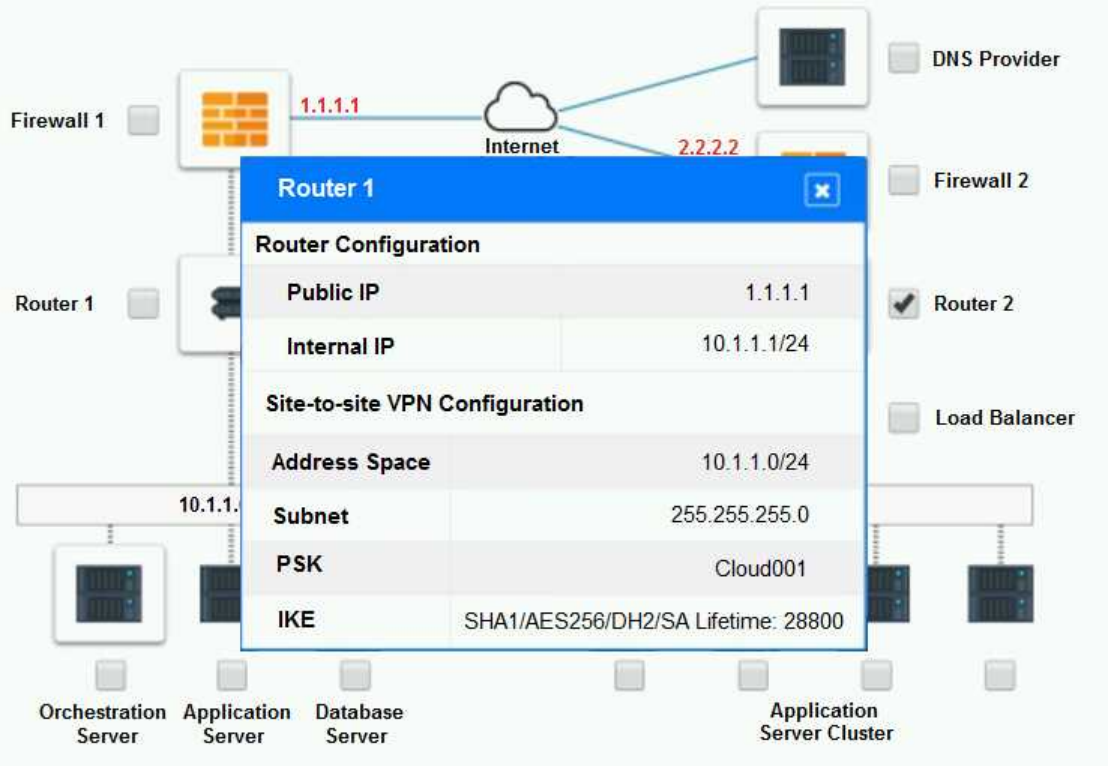
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

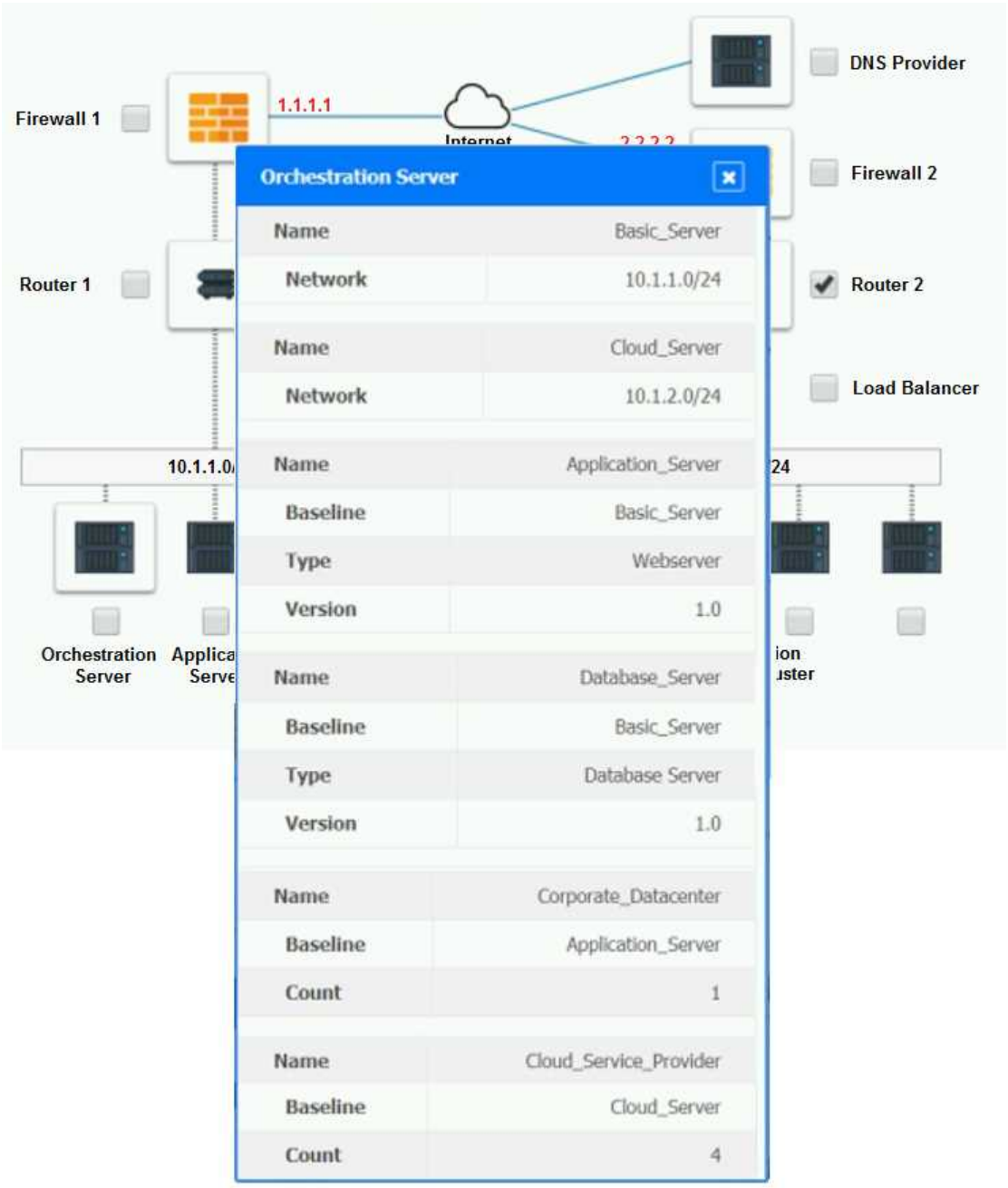
Part 1:

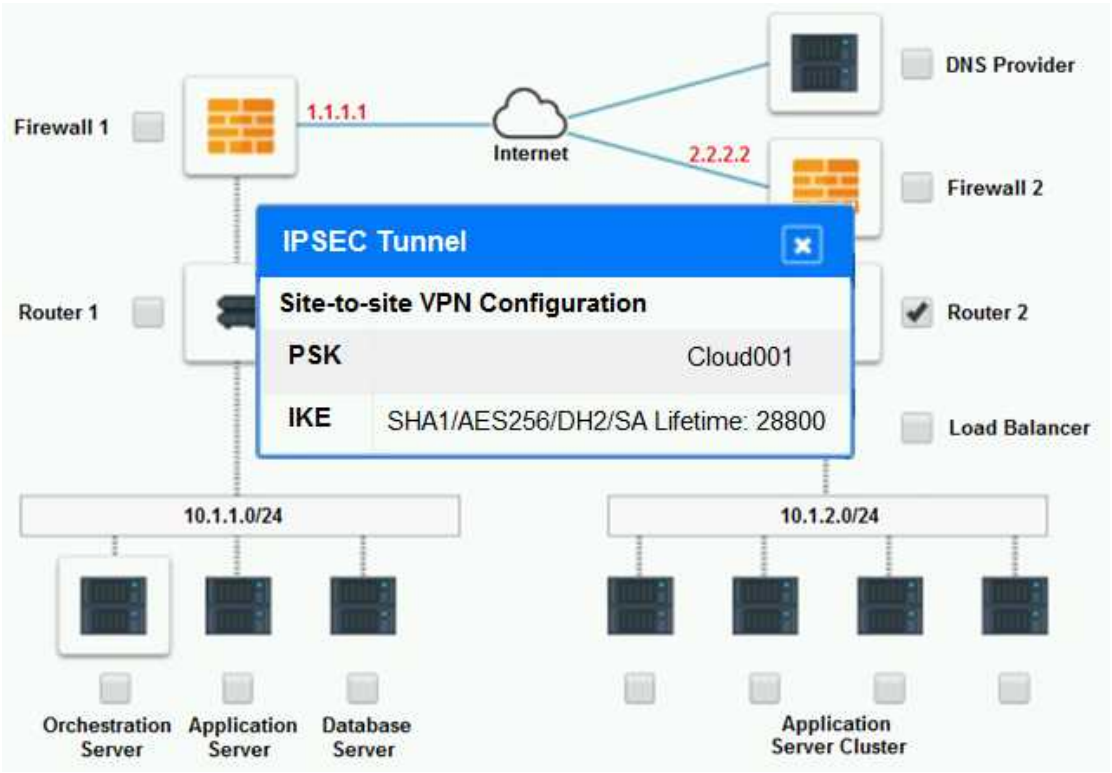
Cloud Hybrid Network Diagram

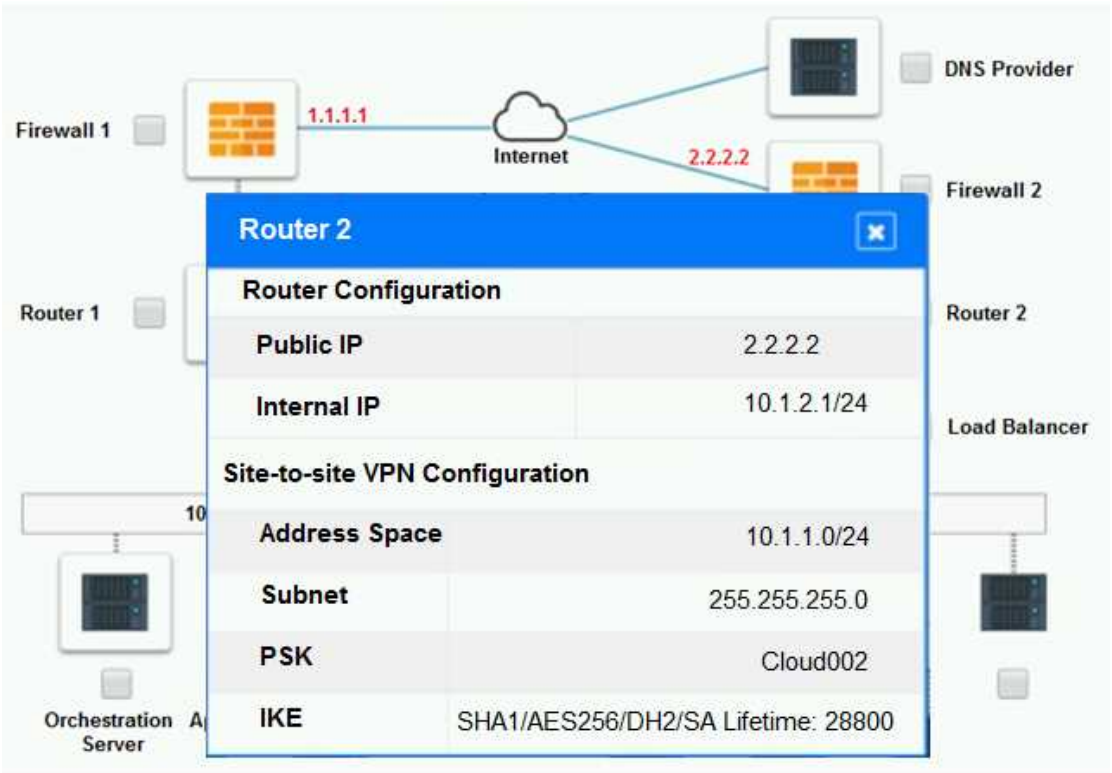

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Site-to-Site IPSEC Tunnel
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

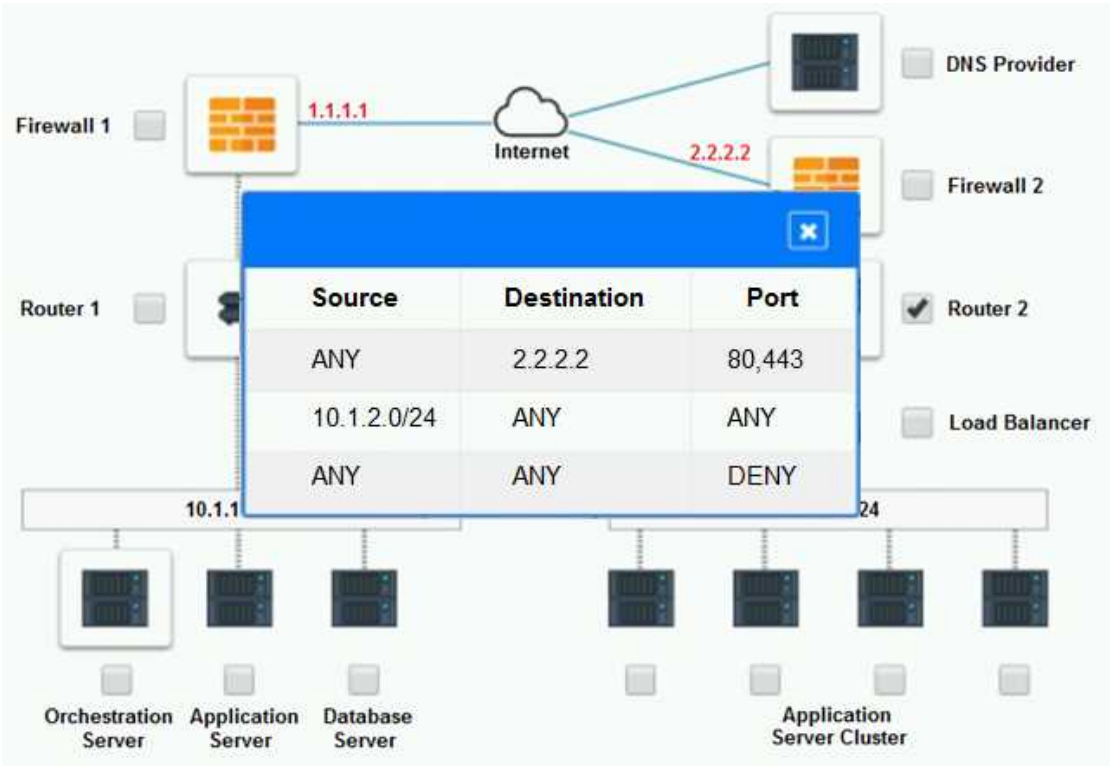

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Firewall 1
Source
Destination
Port
ANY
1.1.1.1
80,443
10.1.1.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

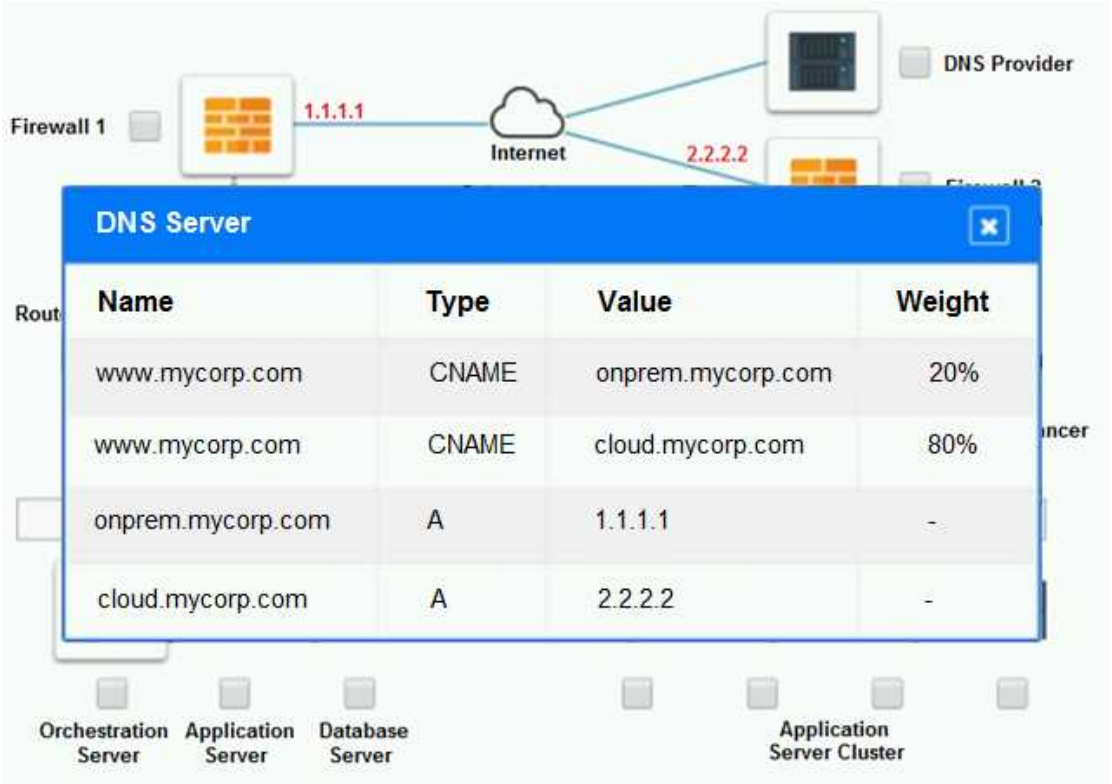

DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 1
Router Configuration
Public IP
1.1.1.1
Internal IP
10.1.1.1/24
Router 2
Site-to-site VPN Configuration
Load Balancer
Address Space
10.1.1.0/24
10.1.1.
Subnet
255.255.255.0
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Orchestration Server
Application Server
Database Server
Application Server Cluster


DNS Provider
Firewall 1
1.1.1.1
Internet
Firewall 2
Router 1
Router 2
Load Balancer
Orchestration Server
Name Basic_Server
Network 10.1.1.0/24
Name Cloud_Server
Network 10.1.2.0/24
Name Application_Server
Baseline Basic_Server
Type Webserver
Version 1.0
Name Database_Server
Baseline Basic_Server
Type Database Server
Version 1.0
Name Corporate_Datacenter
Baseline Application_Server
Count 1
Name Cloud_Service_Provider
Baseline Cloud_Server
Count 4


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
IPSEC Tunnel
Site-to-site VPN Configuration
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Router 1
Router 2
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 2
Router Configuration
Public IP
2.2.2.2
Internal IP
10.1.2.1/24
Site-to-site VPN Configuration
Address Space
10.1.1.0/24
Subnet
255.255.255.0
PSK
Cloud002
IKE
SHA1/AES256/DH2/SA Lifetime: 28800
Router 1
Router 2
Load Balancer
Orchestration Server





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 on-premises 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

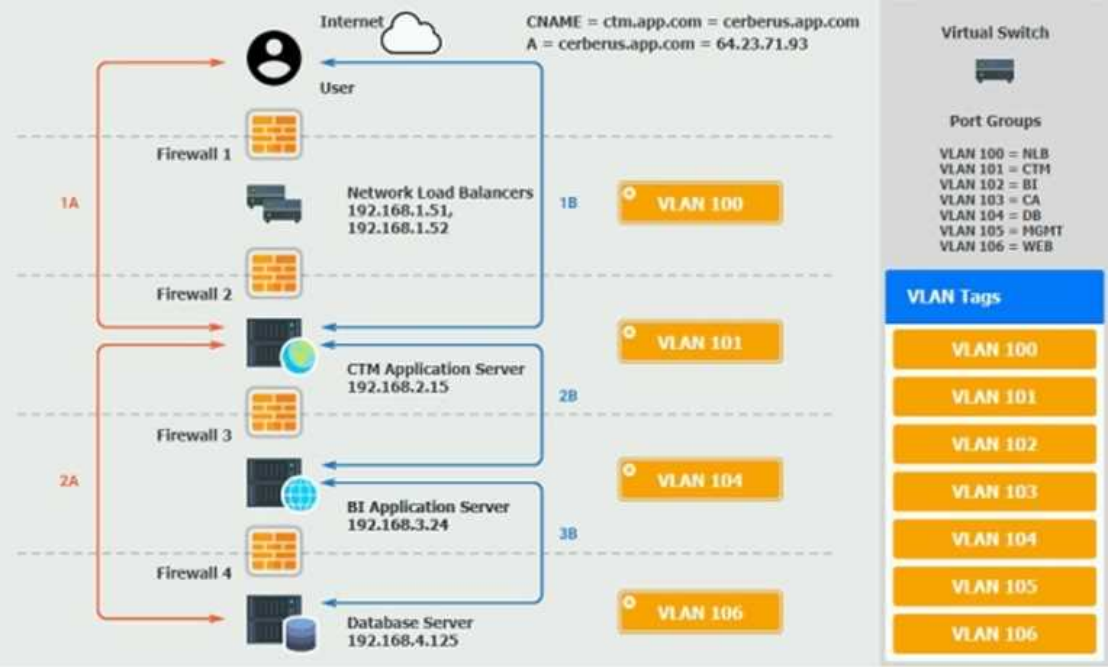
You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.

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.

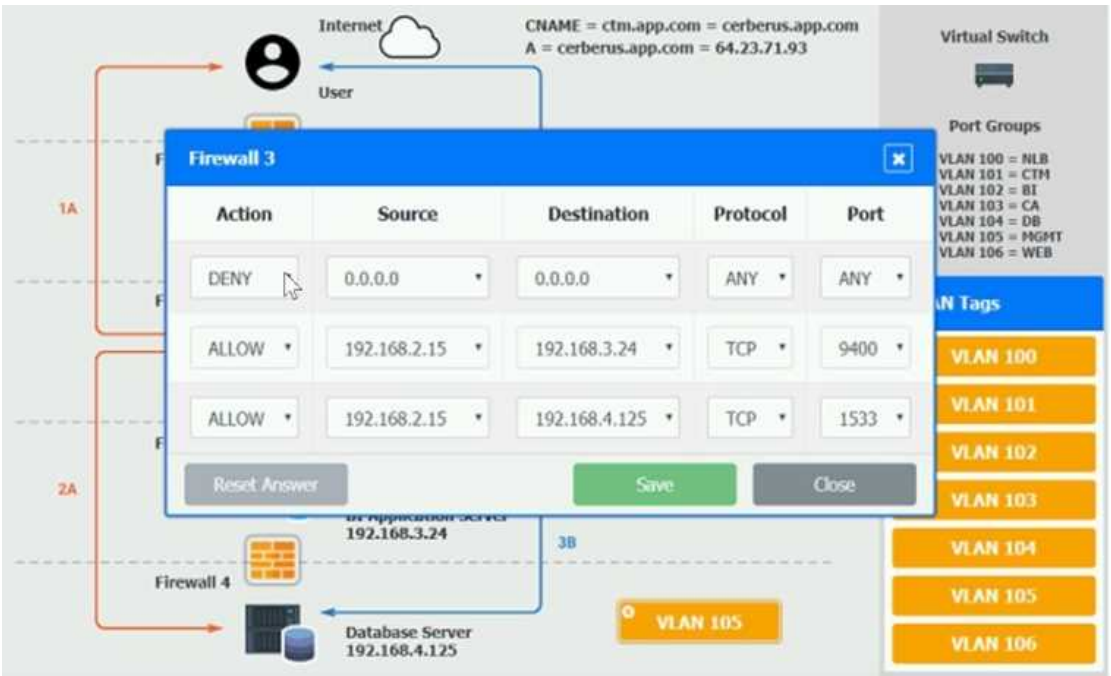
Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed.

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
User
Firewall 1
Network Load Balancers
192.168.1.51,
192.168.1.52
Firewall 2
CTM Application Server
192.168.2.15
Firewall 3
BI Application Server
192.168.3.24
Firewall 4
Database Server
192.168.4.125
1A
1B
2A
2B
3B
VLAN 100
VLAN 101
VLAN 104
VLAN 106
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


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
User
Firewall 1
Firewall 2
Firewall 3
Firewall 4
1A
2A
3B
192.168.3.24
Database Server
192.168.4.125
VLAN 105
Firewall 1
Action Source Destination Protocol Port
ALLOW 0.0.0.0 192.168.1.51 TCP 443
ALLOW 0.0.0.0 192.168.1.52 TCP 443
ALLOW 0.0.0.0 192.168.1.51 TCP 80
ALLOW 0.0.0.0 192.168.1.52 TCP 80
DENY 0.0.0.0 0.0.0.0 ANY ANY
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


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
Virtual Switch
Firewall 2
Action
Source
Destination
Protocol
Port
ALLOW
192.168.1.51
192.168.2.15
TCP
88
DENY
192.168.1.52
UDP
443
ANY
0.0.0.0
Reset Answer
Save
Close
1A
2A
Database Server
192.168.4.125
VLAN 105
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106


Internet
CNAME = ctm.app.com = cerberus.app.com
A = cerberus.app.com = 64.23.71.93
Virtual Switch
User
Firewall 3
Action
Source
Destination
Protocol
Port
DENY
0.0.0.0
ANY
ALLOW
192.168.2.15
192.168.3.24
TCP
9400
192.168.4.125
1533
Reset Answer
Save
Close
1A
2A
3B
Firewall 4
Database Server
192.168.4.125
VLAN 105
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106

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