

CompTIA

CV0-002

CompTIA Cloud+ Exam

Verified by IT Experts

*Pass your
exam in first
attempt*

**DEMO
QUESTIONS**

**BEST
SELLER**

Question: 1

A new browser version has been deployed to all users at a company. After the deployment, users report that they can no longer access the company's secure time-card system, which is hosted by a SaaS provider. A technician investigates and discovers a security error is received upon opening the site. If the browser is rolled back to the older version, the site is accessible again. Which of the following is the MOST likely cause of the security error users are seeing?

- A. SSL certificate expiration on the SaaS load balancers
- B. Federation issues between the SaaS provider and the company
- C. Obsolete security technologies implemented on the SaaS servers
- D. Unencrypted communications between the users and the application

Answer: C

Question: 2

CORRECT TEXT

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. Review the network architecture and supporting documents and fulfill these requirements: Part1:

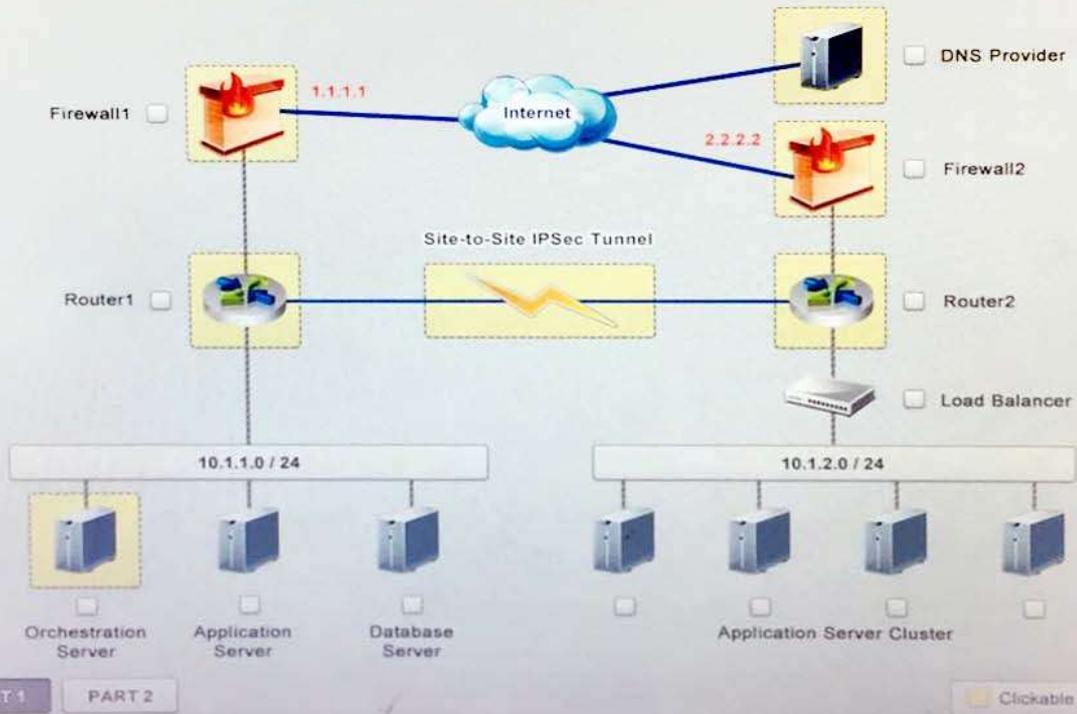
1. Analyze the configuration of the following components: DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestrator Server.
2. Identify the problematic device(s). Instructions:

If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Simulation

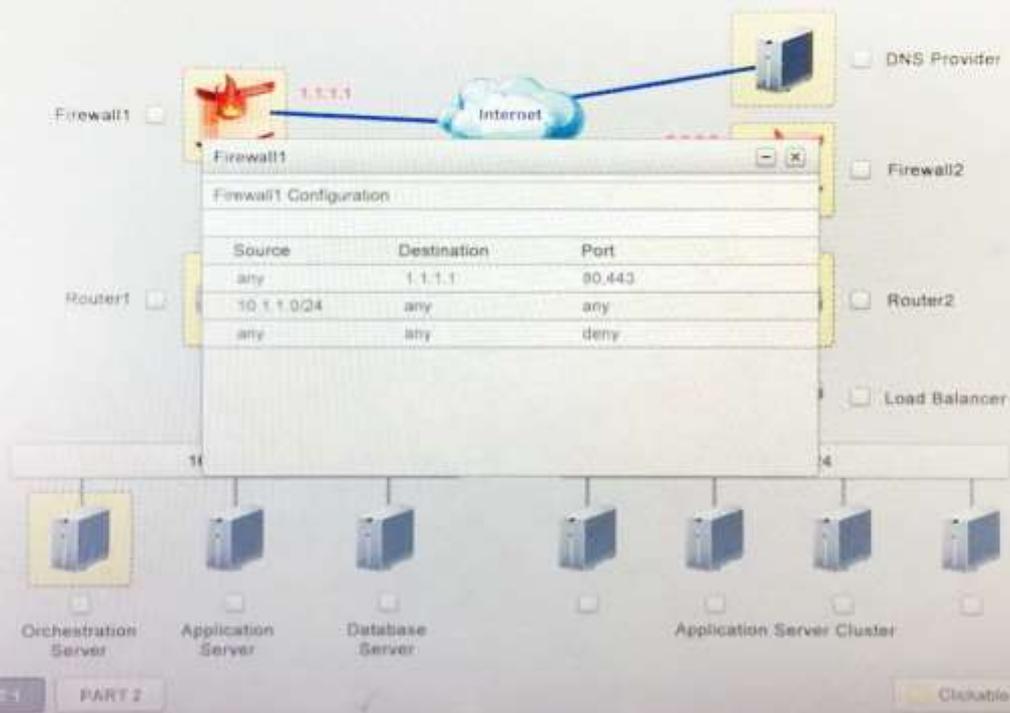
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



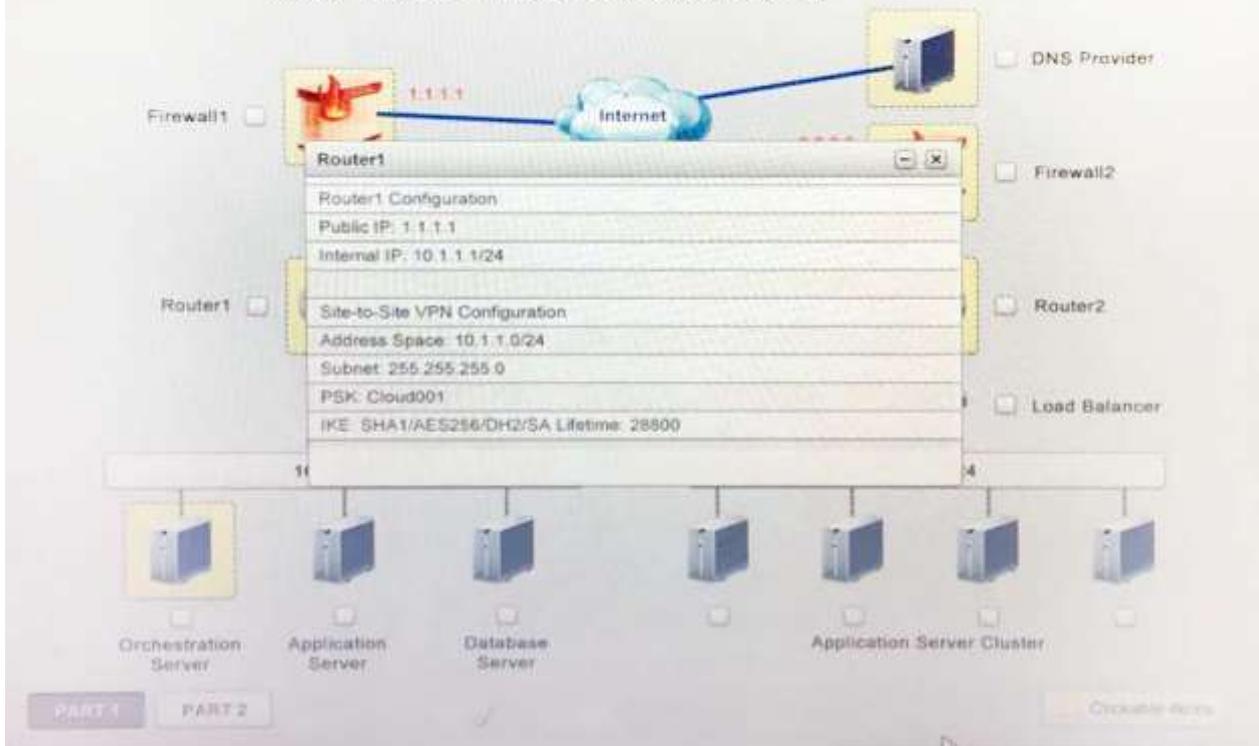
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



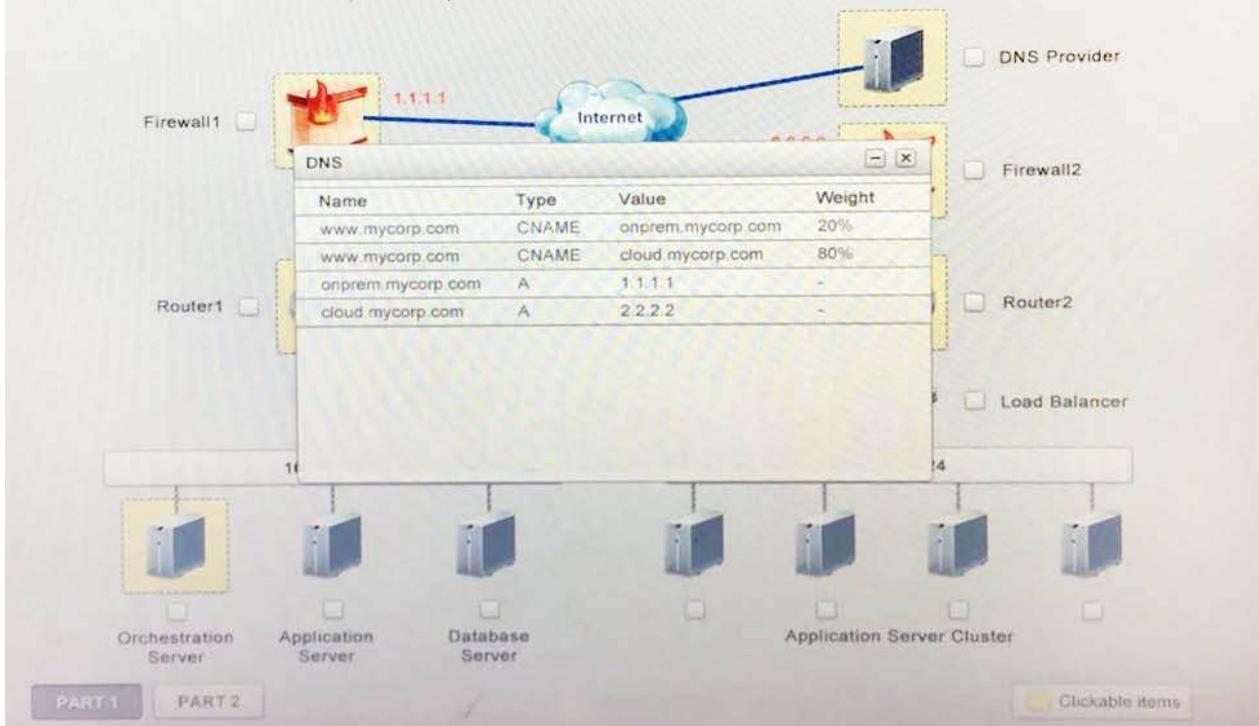
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



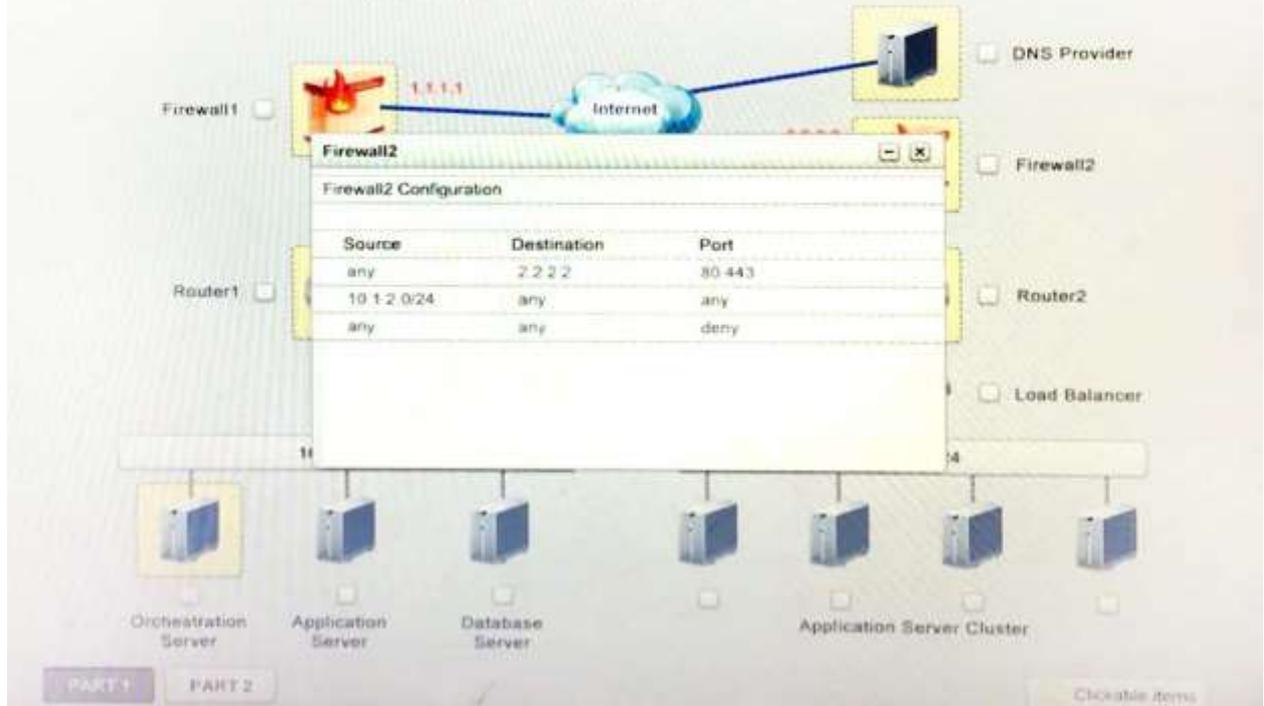
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



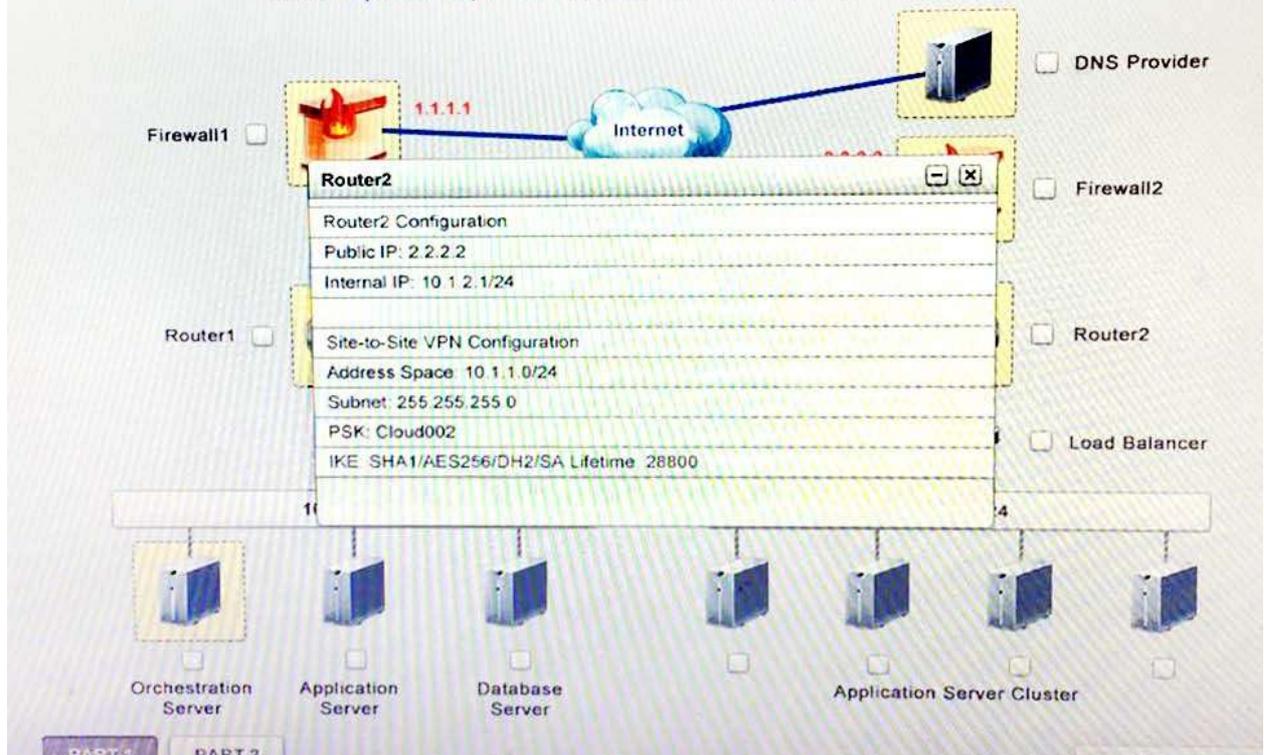
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



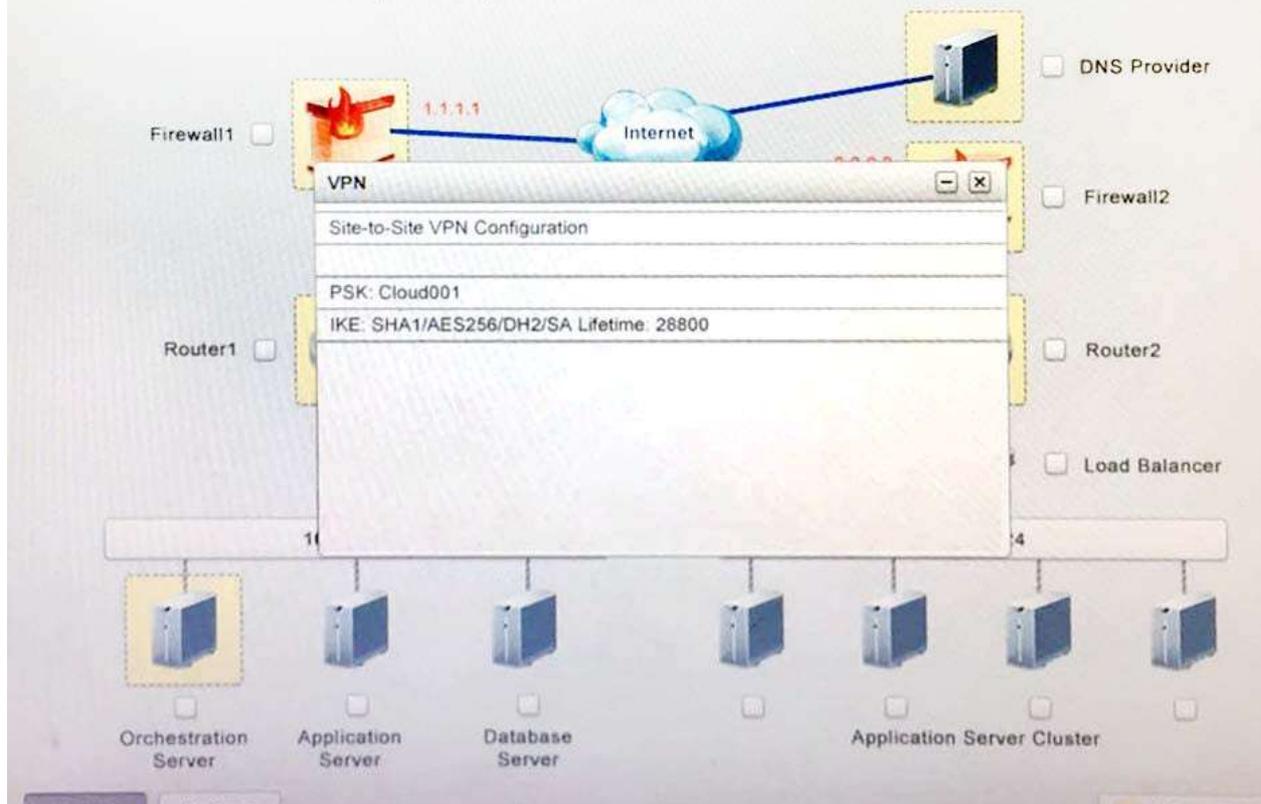
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



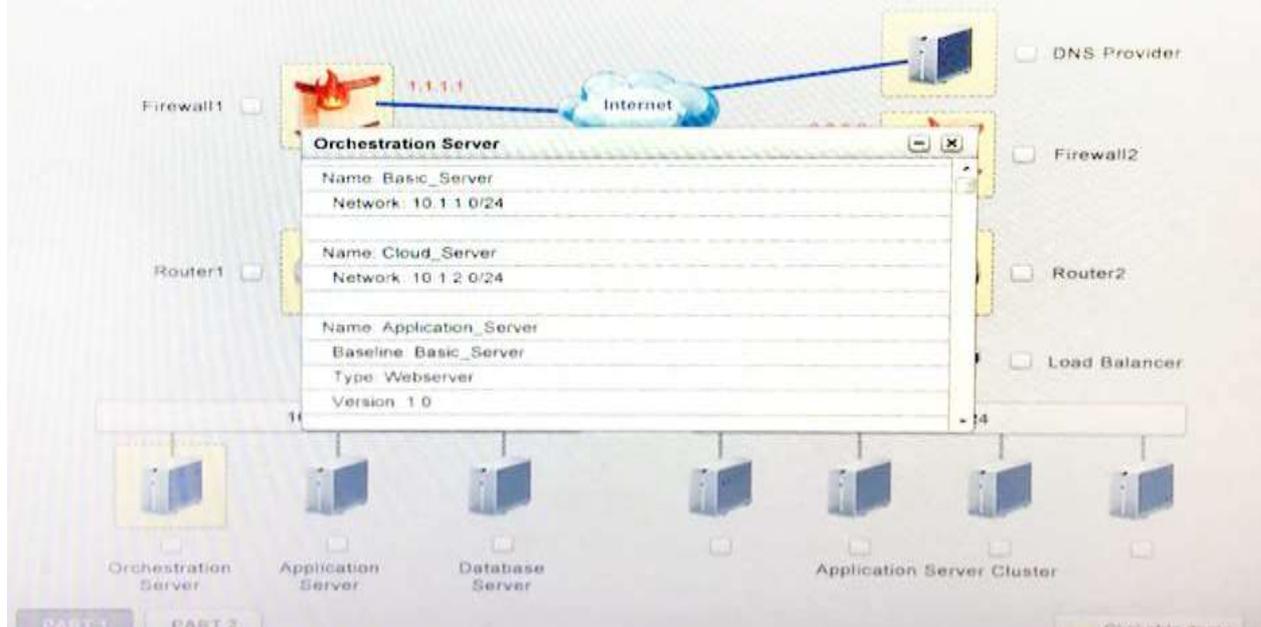
PART 1

Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.

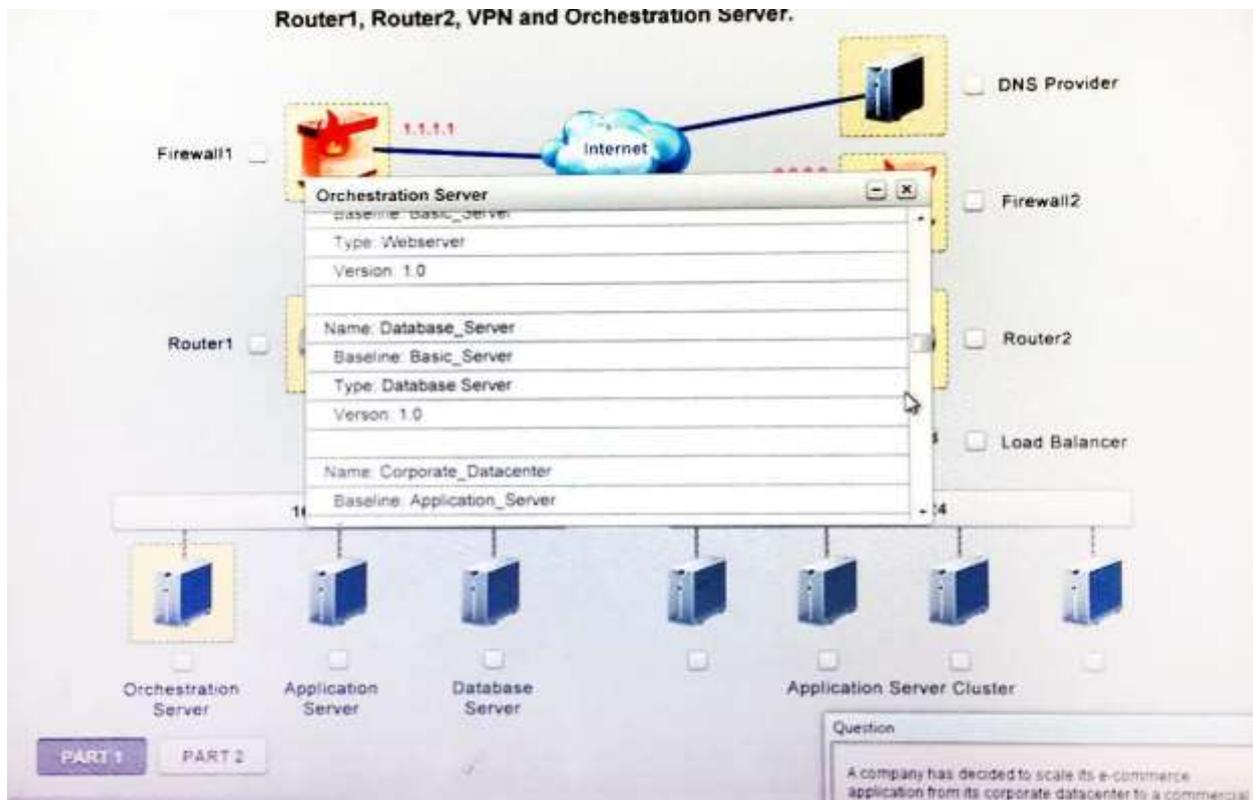


PART 1

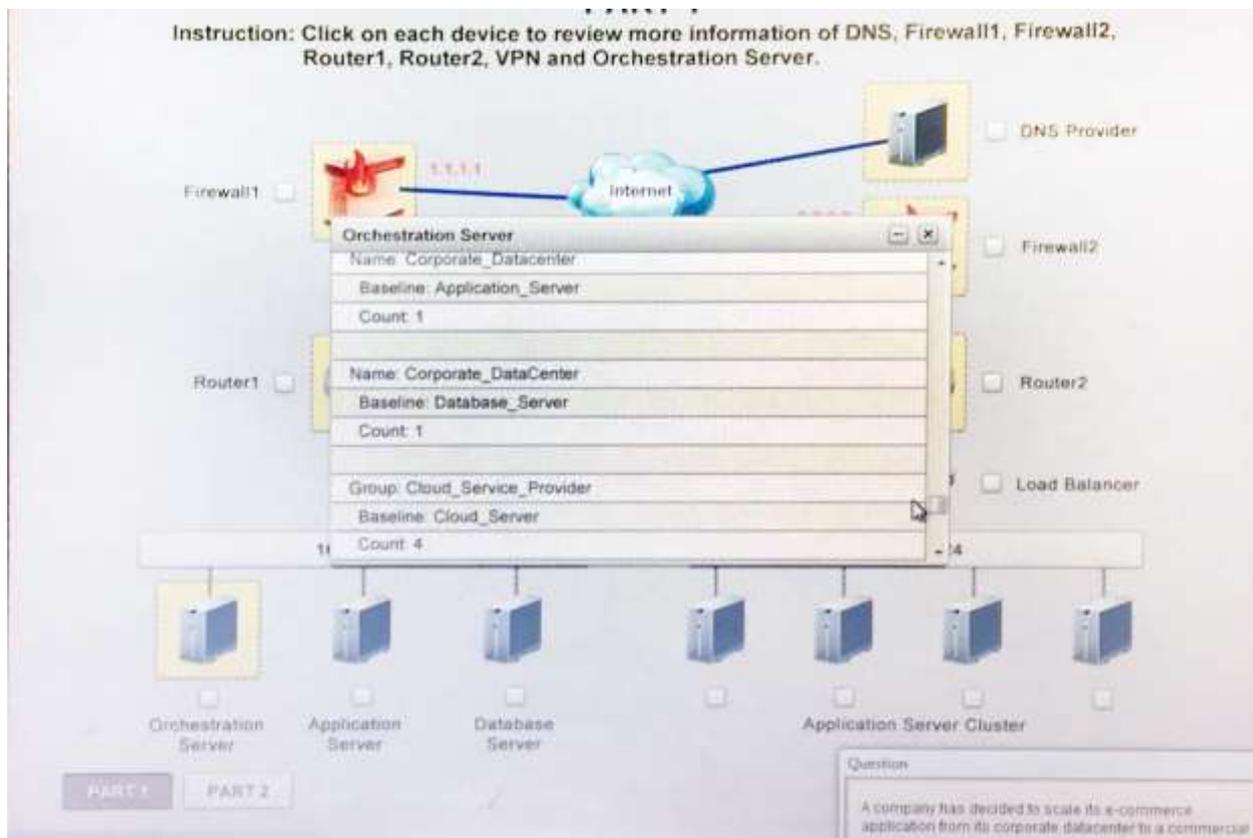
Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



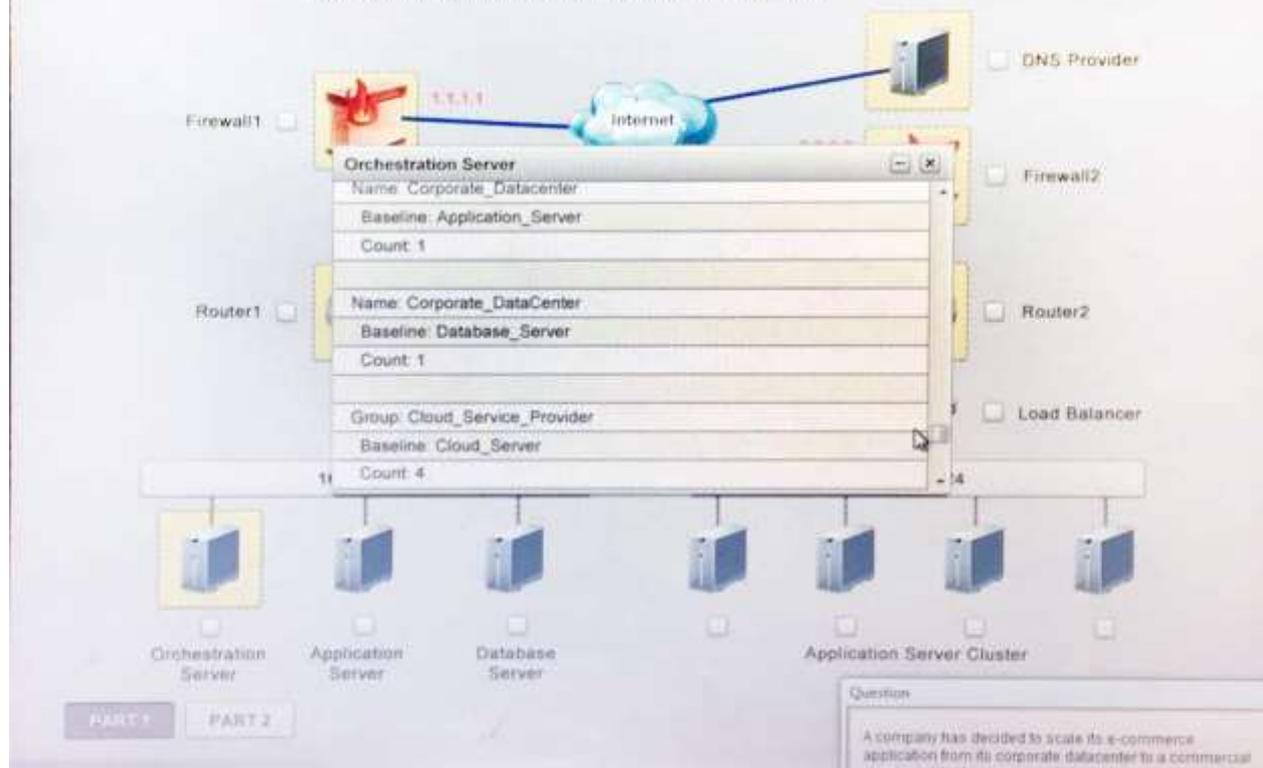
Router1, Router2, VPN and Orchestration Server.



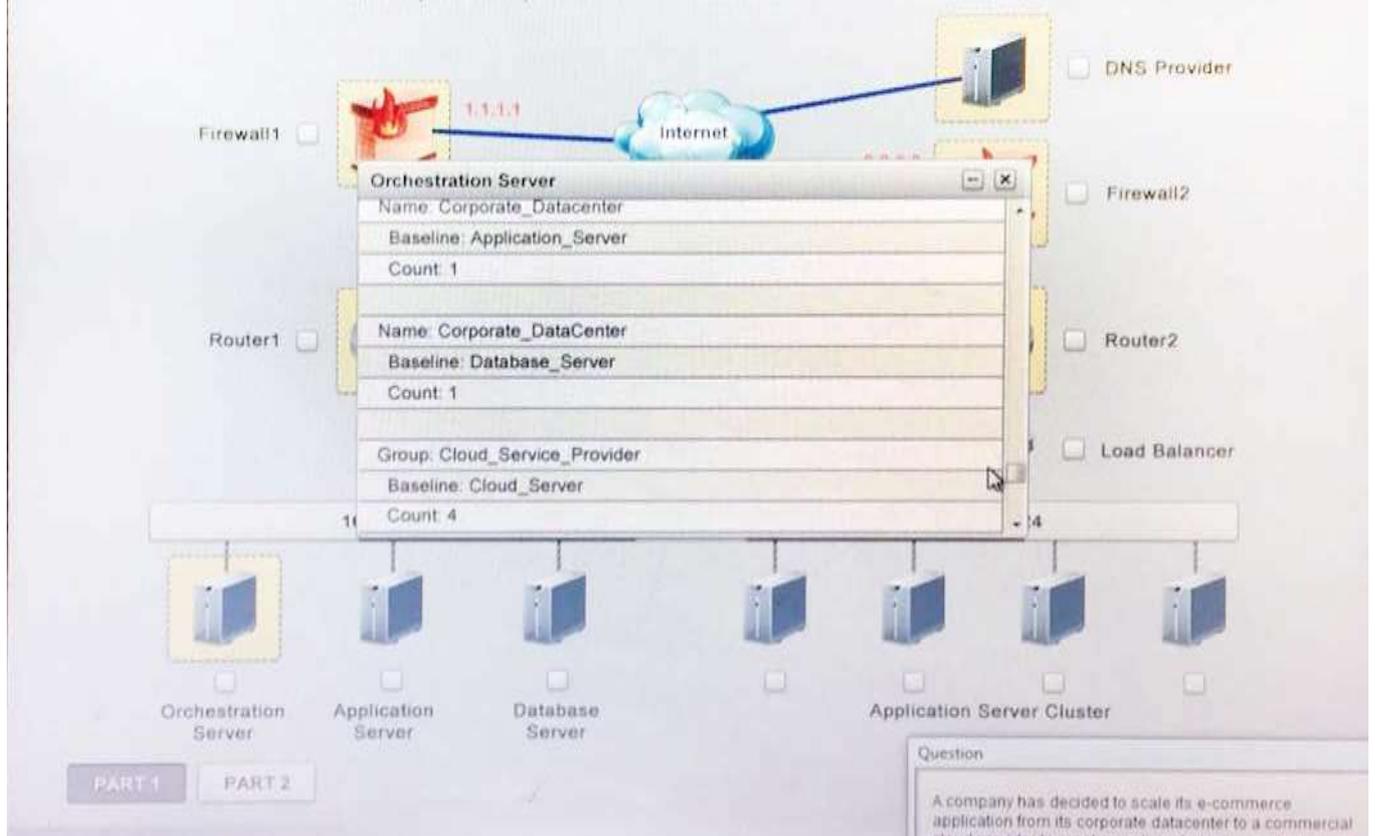
Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



Instruction: Click on each device to review more information of DNS, Firewall1, Firewall2, Router1, Router2, VPN and Orchestration Server.



Question: 3

DRAG DROP

A hosted file share was infected with CryptoLocker and now root cause analysis needs to be performed. Place the tasks in the correct order according to the troubleshooting methodology.

1		Establish a plan of action to resolve the problem and implement remediation
2		Establish a theory of probable cause
3		Document findings and outcomes
4		Identify the problem
5		Test the theory to determine cause
6		Verify full system functionality

Answer:

1	Identify the problem	Establish a plan of action to resolve the problem and implement remediation
2	Establish a theory of probable cause	Establish a theory of probable cause
3	Test the theory to determine cause	Document findings and outcomes
4	Establish a plan of action to resolve the problem and implement remediation	Identify the problem
5	Verify full system functionality	Test the theory to determine cause
6	Document findings and outcomes	Verify full system functionality

Question: 4

A company is seeking a new backup solution for its virtualized file servers that fits the following characteristics:

The files stored on the servers are extremely large. Existing files receive multiple small changes per day. New files are only created once per month.

All backups are being sent to a cloud repository.

Which of the following would BEST minimize backup size?

- A. Local snapshots
- B. Differential backups
- C. File-based replication
- D. Change block tracking

Answer: B

Reference:

<https://www.acronis.com/en-us/blog/posts/tips-tricks-better-business-backup-and-recovery-world-backup-day>

Question: 5

A company has deployed a four-node cluster in a COLO environment with server configurations listed below. The company wants to ensure there is 50% overhead for failover and redundancy. There are currently eight VMs running within the cluster with four vCPUs x32GB each. The company wants to better utilize its resources within the cluster without compromising failover and redundancy.

White Label Servers	Configuration (CPU x Memory GB)
Server 1	16x128
Server 2	16x128
Server 3	16x128
Server 4	16x128

Given the information above, which of the following should a cloud administrator do to BEST accommodate failover and redundancy requirements?

- A. Ensure hyperthreading is being utilized with physical server CPUs.
- B. Ensure dynamic resource allocation is being utilized.
- C. Overcommit memory, and the systems will allocate resources as required.
- D. Set hard limits for VM resources and turn on hyperthreading.

Answer: B

Question: 6

A courier company has virtualized its packing software application. The CSA needs to confirm the deployment is utilizing the correct amount of CPU per virtual instance. After confirming the deployment requirements, the CSA should log into the cloud services portal to ensure that:

- A. the VMs with the most CPU cores available have been selected.
- B. smaller VMs are being selected to reduce the total deployment cost.
- C. the deployment is utilizing the recommended amount of CPUs per VM.
- D. the alarms on CPU utilization have been enabled.

Answer: C

Question: 7

Due to a competitor's unlimited data plan, a service provider is struggling and wants to transform its business services to be more hosting oriented. A cloud architect is tasked to review current cloud resource capacity and provide recommendations and a plan for better resource utilization. Given the following report:

Name	Type	Utilization
Server1	Media	25%
Server2	Media	15%
Server3	Media	12%
Server4	Host	72%

Which of the following is the BEST option for the architect to suggest?

- A. Downsize by migrating all media services to one server and decommission two servers.
- B. Downsize by decommissioning servers 2 and 3 and reallocate media servers to hosts.
- C. Downsize by migrating all media services to one server, add one host server, and decommission one server.
- D. Upsize the hosting services by turning server 1 into a host server.

Answer: A

Question: 8

A cloud administrator is receiving alerts that the disk on several systems is 90% full. Upon reviewing the systems, the administrator determines that the log directory is using 50% of the disk. The company has a 14-day retention policy for all logs. Which of the following is the BEST solution to implement to minimize future alerts?

- A. Orchestrate a job to rotate the logs and upload to external storage.
- B. Delete any log files in the directory that are larger than 20MB.
- C. Archive the existing logs in the directory and upload to external storage.
- D. Add additional storage space to the log directory for the servers.

Answer: A

Question: 9

A company purchased a SaaS CRM application. The signed SLA meets year-round performance requirements. Three months after deployment, customers start reporting a slow application response time. System availability, connectivity, and proper functionality still meet the SL

- A. Which of the following is MOST likely the reason for the poor response time?
- A. Incorrect business requirements are invalidating the testing results.
 - B. Bandwidth restrictions are causing poor performance.
 - C. The application version is causing compatibility issues.
 - D. Inadequate documentation is affecting the user interface.

Answer: C

Question: 10

A cloud architect created a new delivery controller for a large VM farm to scale up according to organizational needs. The old and new delivery controllers now form a cluster. However, the new delivery controller returns an error when entering the license code. Which of the following is the MOST likely cause?

- A. A firewall is blocking the port on the license server.
- B. The existing license is for a lower version.
- C. The existing license is not supported for clusters.
- D. The existing license has expired.

Answer: A