Free Questions for CV0-003 by actualtestdumps

Shared by Donovan on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After accidentally uploading a password for an IAM user in plain text, which of the following should a cloud administrator do FIRST?

Options:

A) Identify the resources that are accessible to the affected IAM user

B) Remove the published plain-text password

C) Notify users that a data breach has occurred

D) Change the affected IAM user's password

E) Delete the affected IAM user

Answer:

B

Question 2

Question Type: MultipleChoice

SIMULATION

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.

INSTRUCTIONS

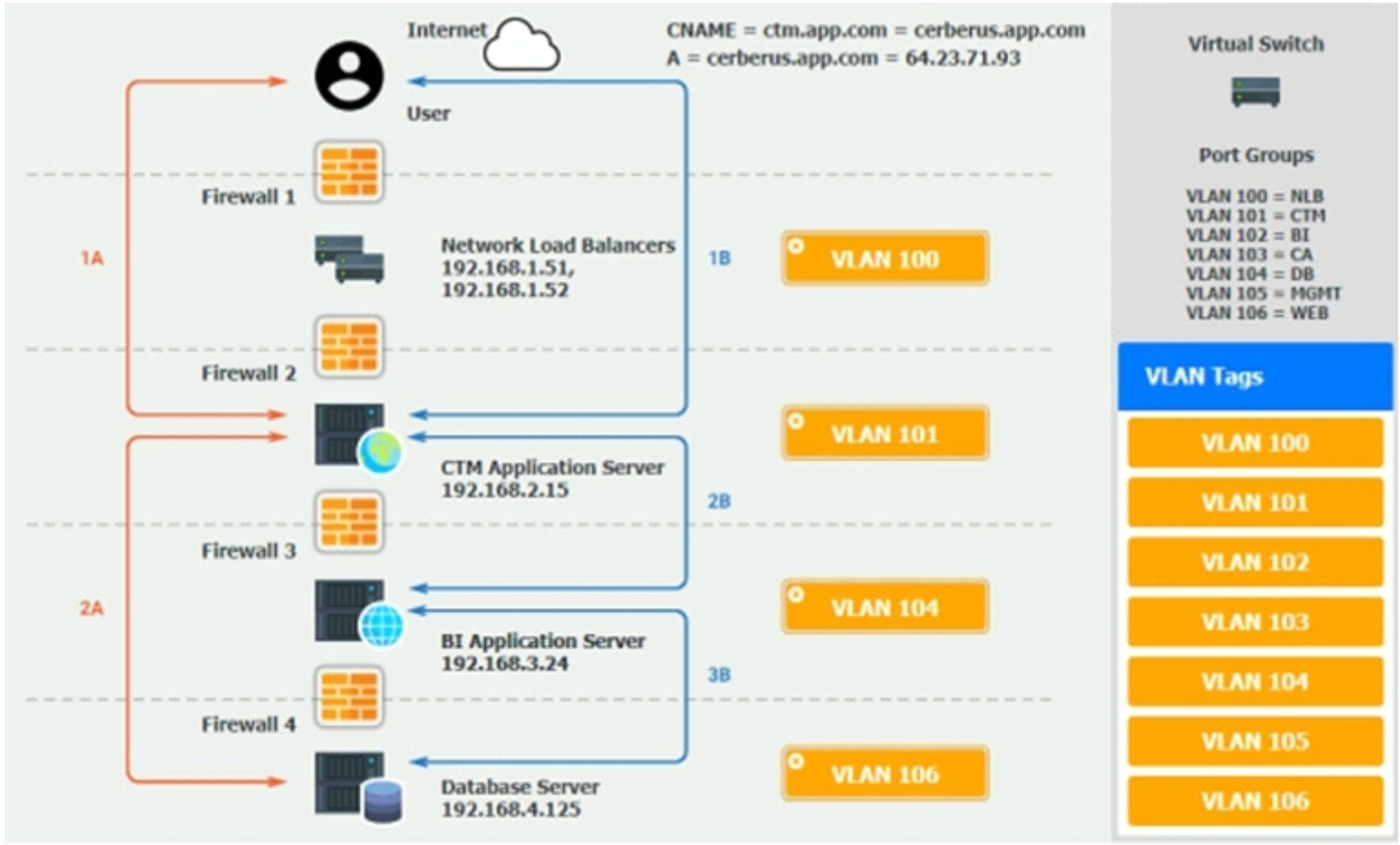
You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.

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.

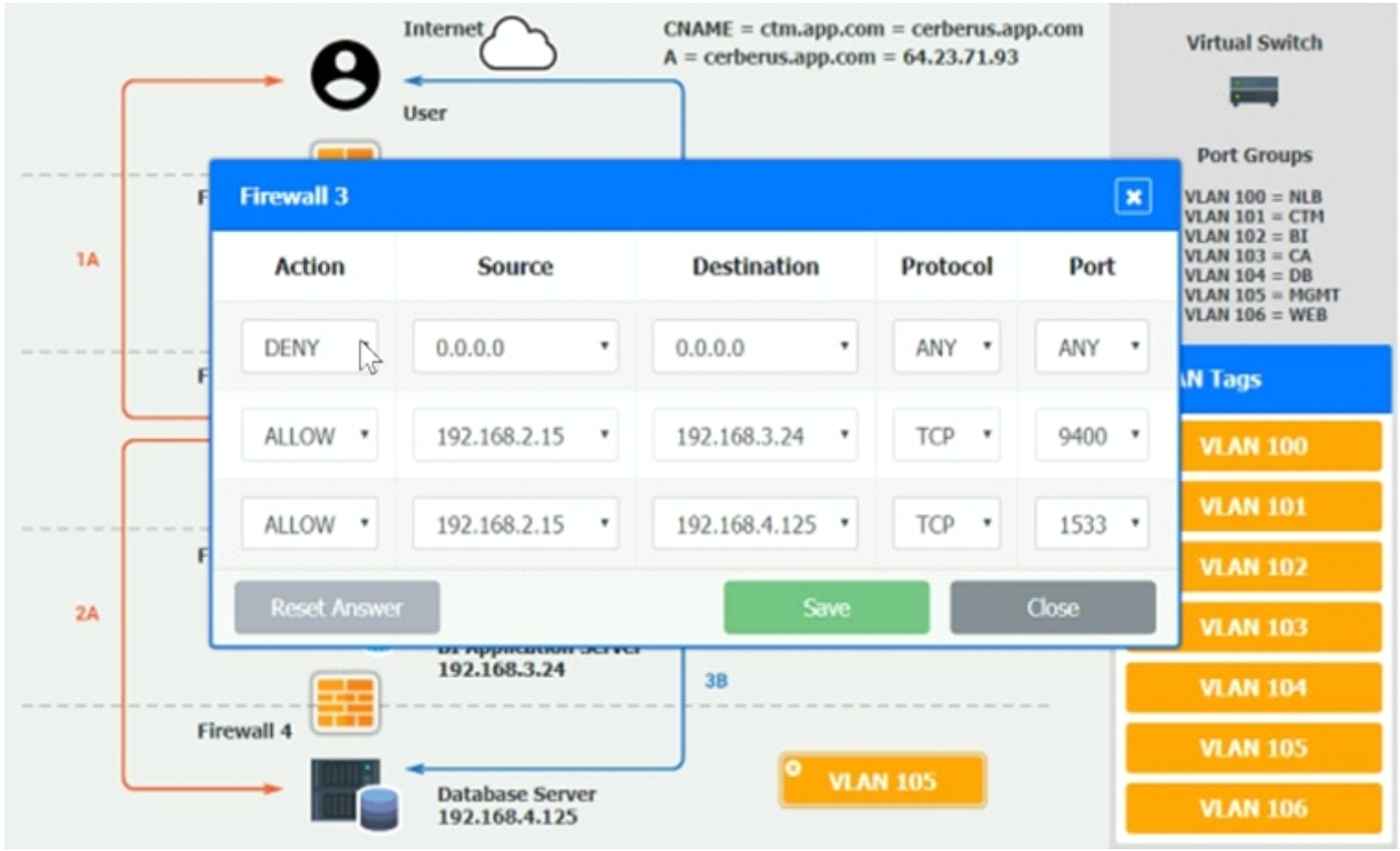
Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed.

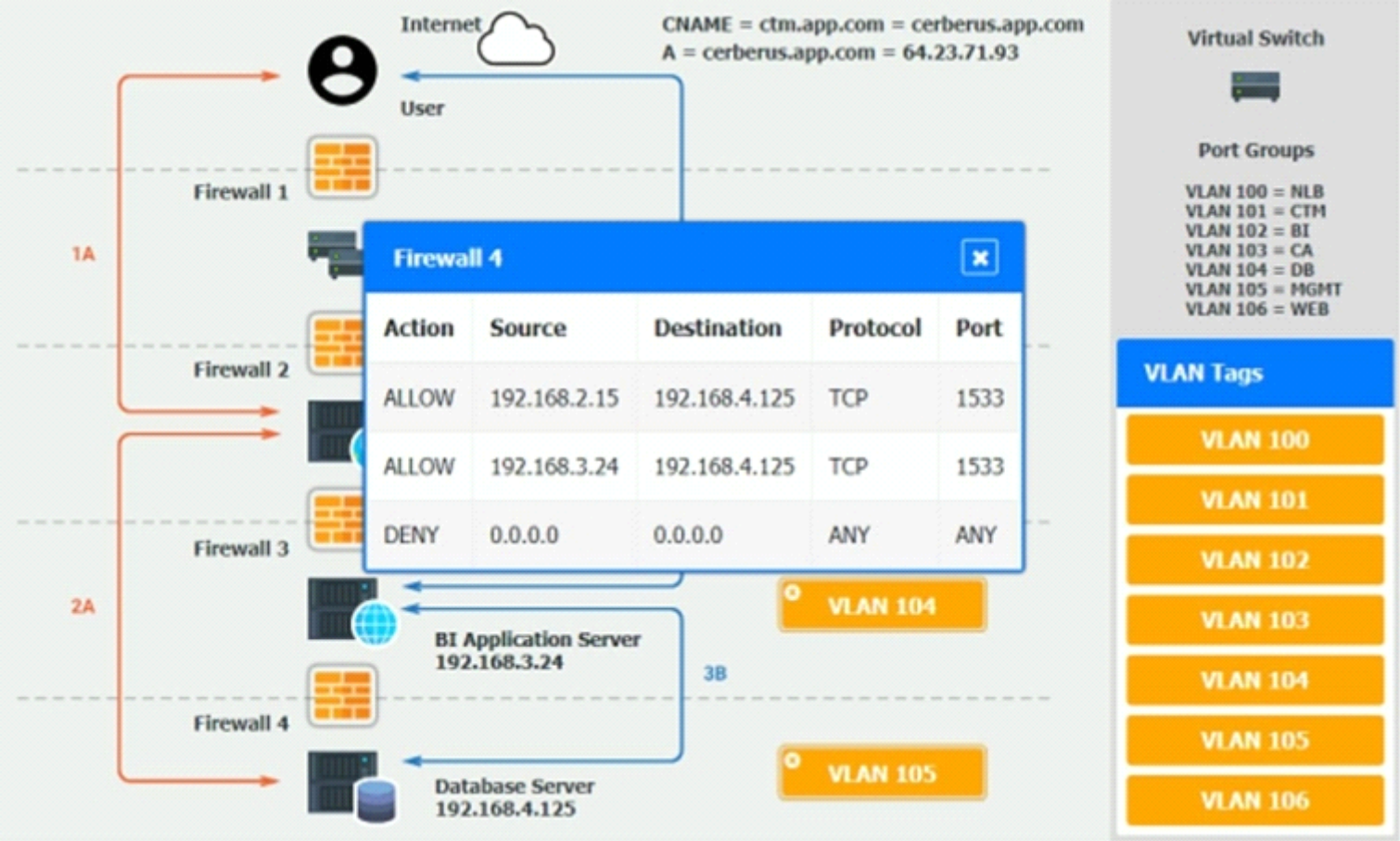
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


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
1A
Firewall 2
Firewall 3
2A
Firewall 4
192.168.3.24
3B
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
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
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
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
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
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
1A
2A
3B
192.168.3.24
Firewall 4
Database Server
192.168.4.125
VLAN 105
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106



Options:

A) On firewall 3, change the DENY 0.8.8.0 entry to rule 3 not rule 1.

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

Answer:

B

Question 3

Question Type: **MultipleChoice**

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).

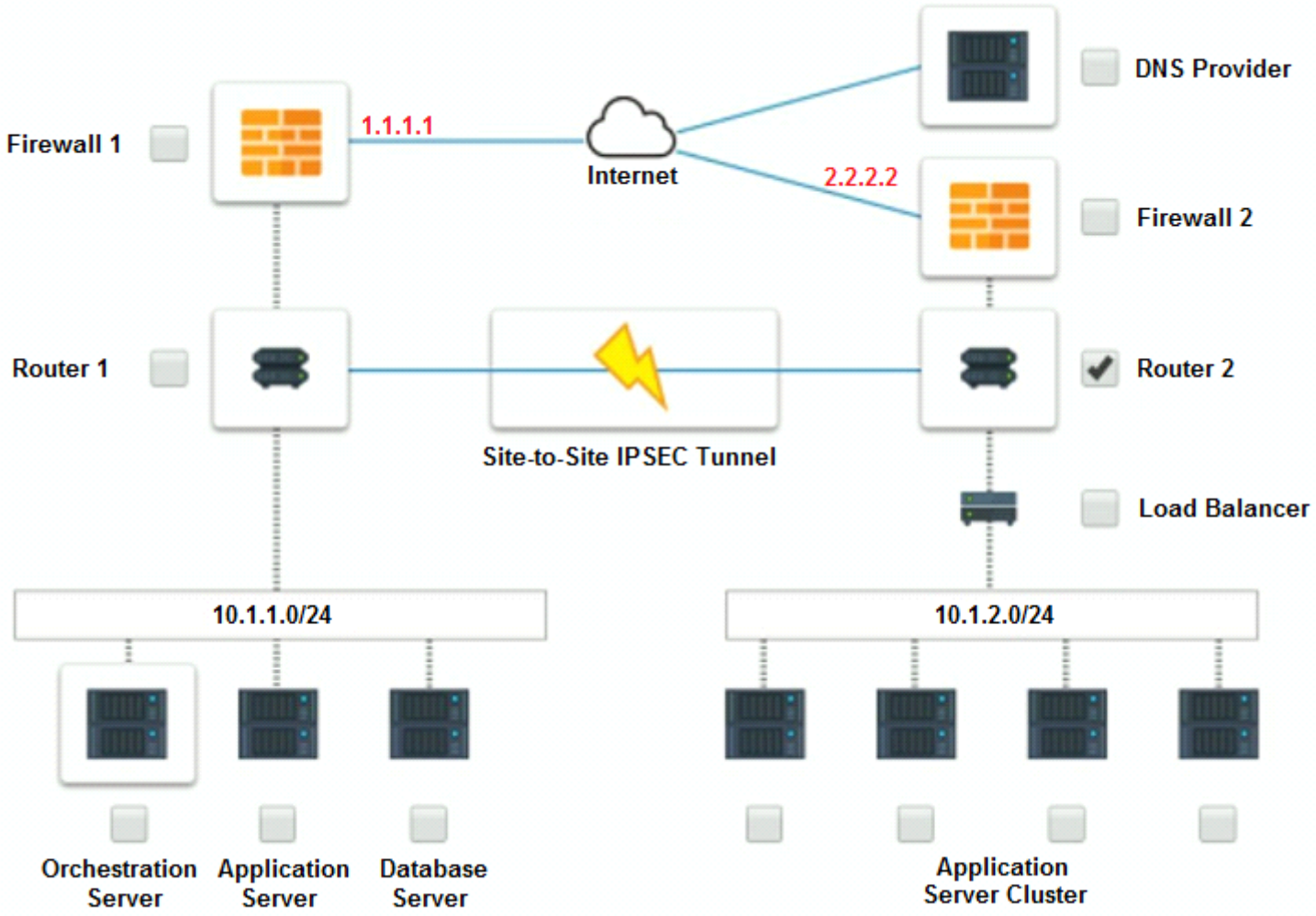
Part 2:

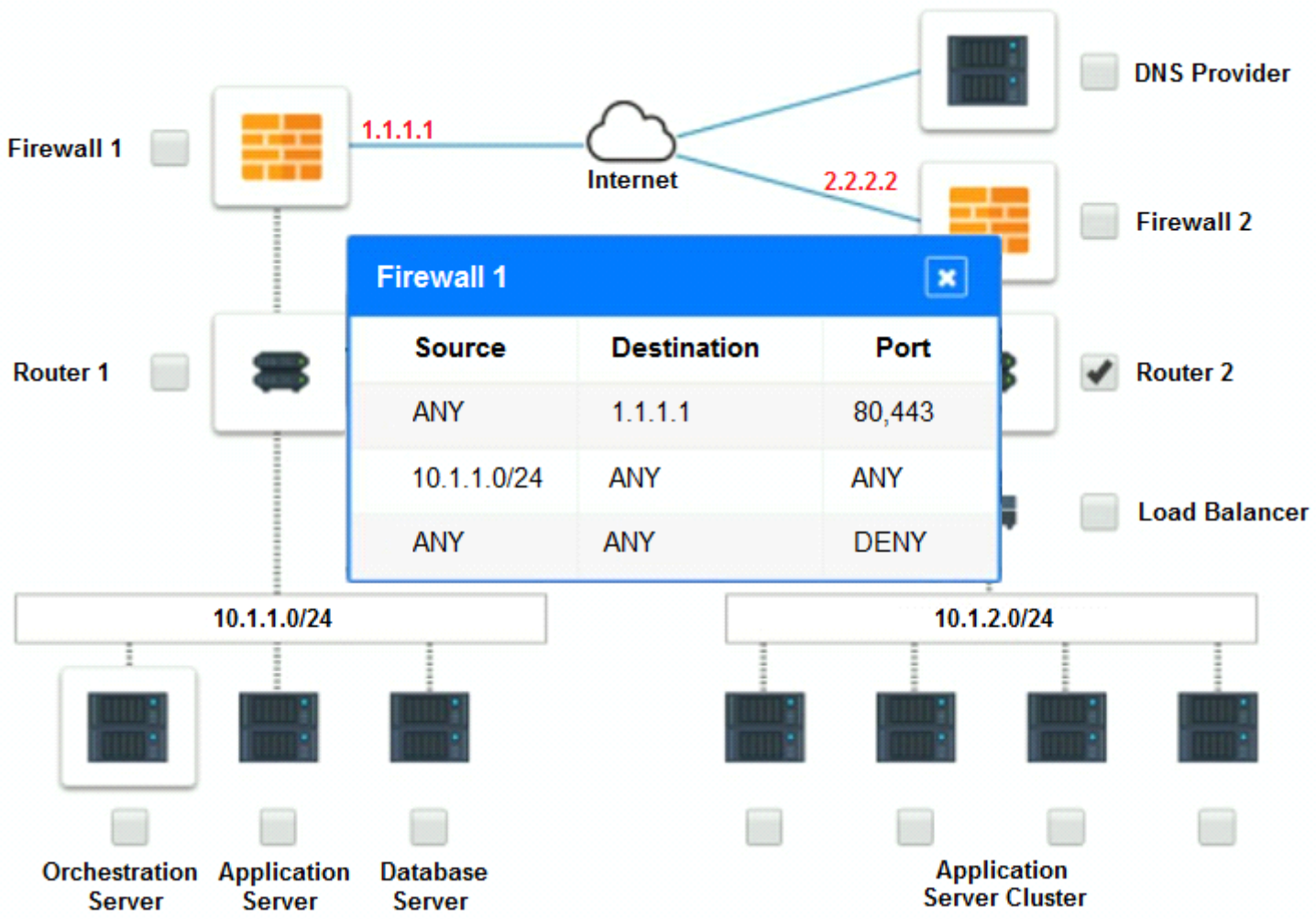
Identify the correct options to provide adequate configuration for hybrid cloud architecture.

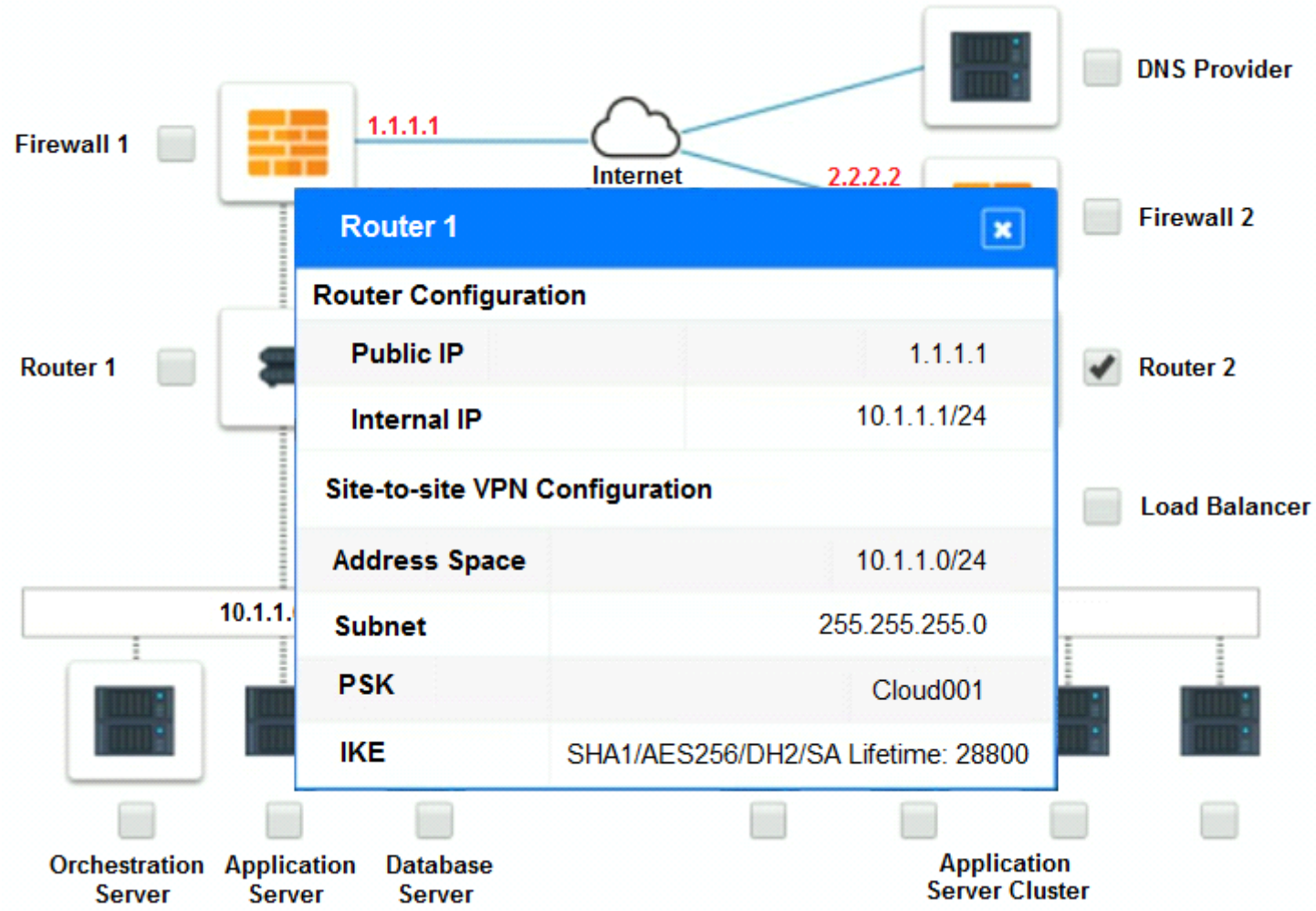
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

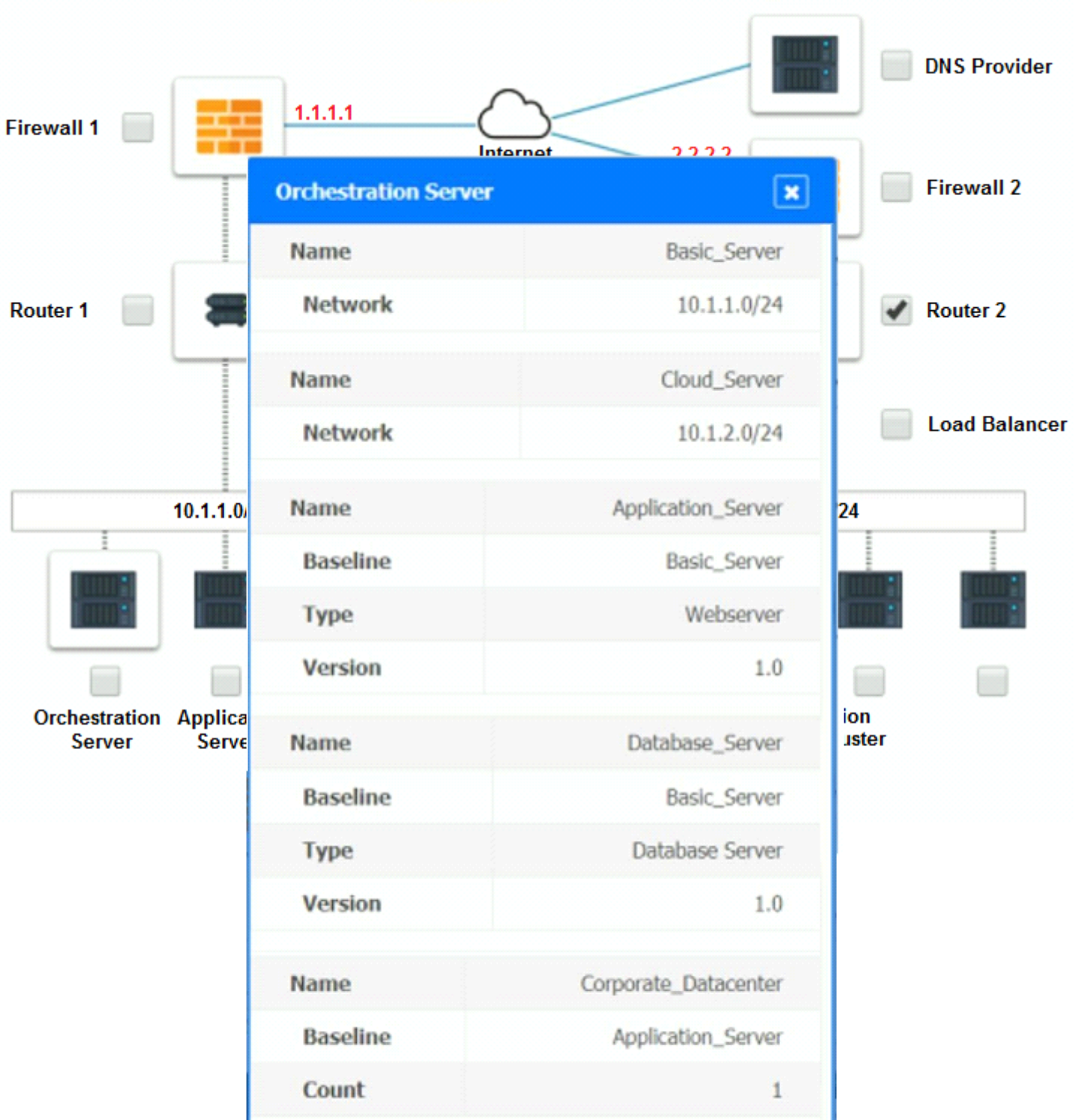
Part 1:

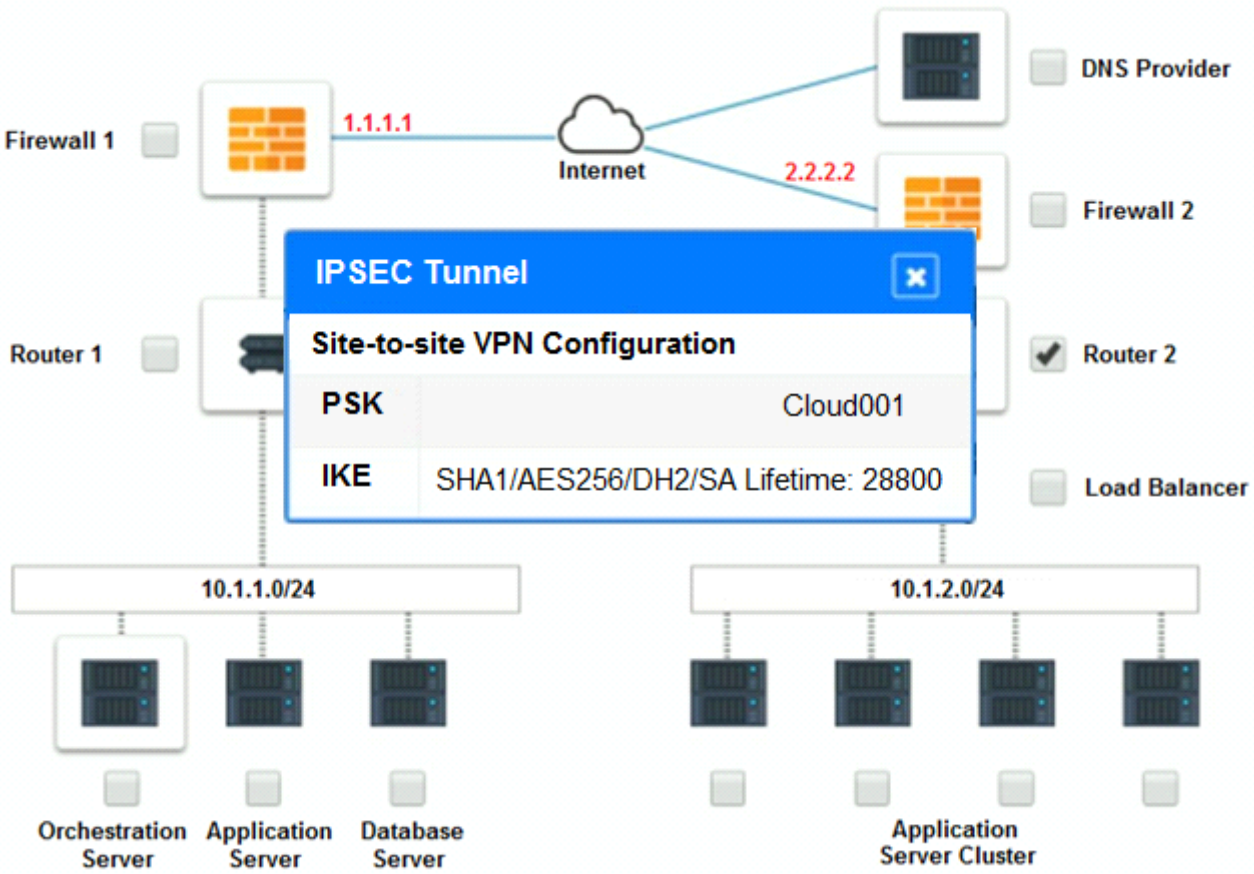
Cloud Hybrid Network Diagram

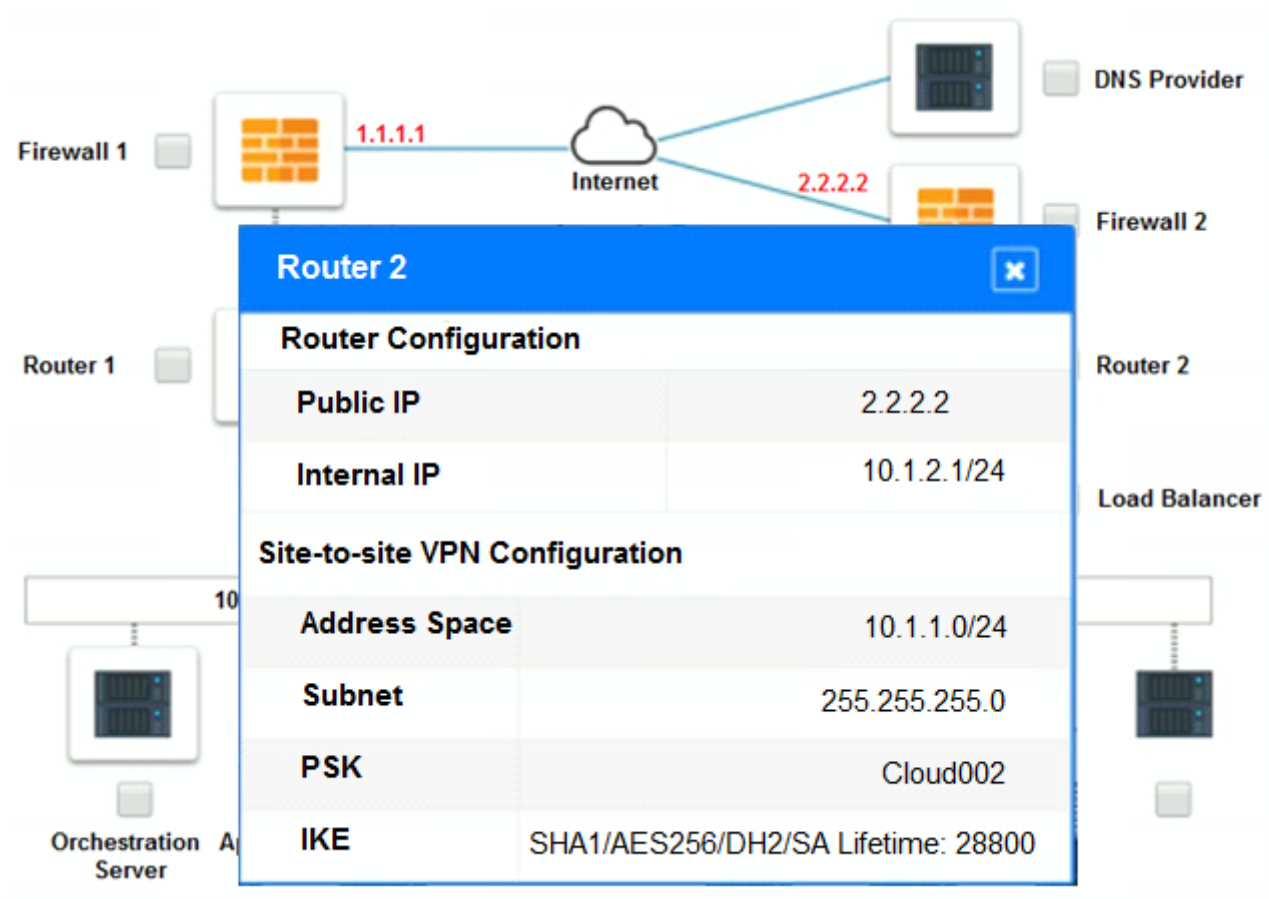

DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 2
Site-to-Site IPSEC Tunnel
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

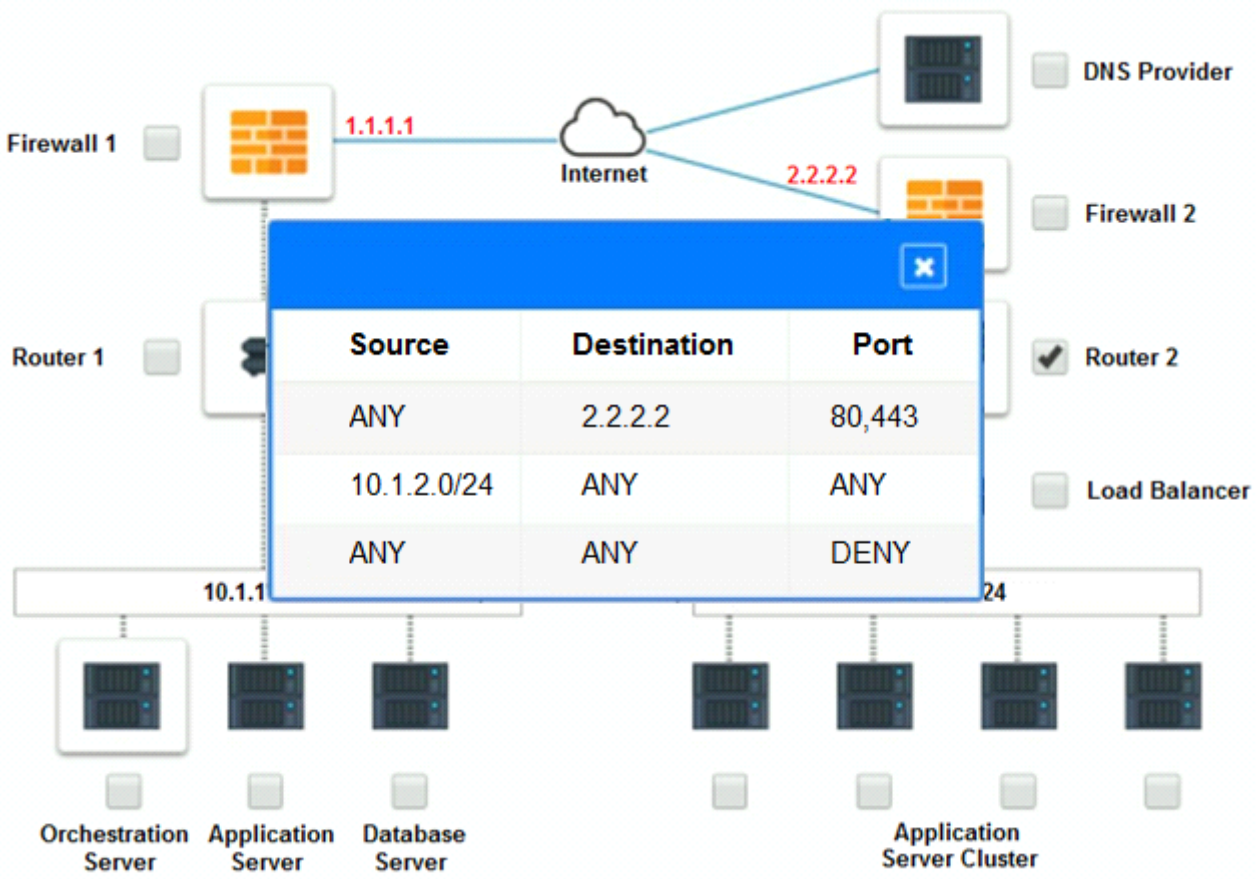

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Firewall 1
Source
Destination
Port
ANY
1.1.1.1
80,443
10.1.1.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

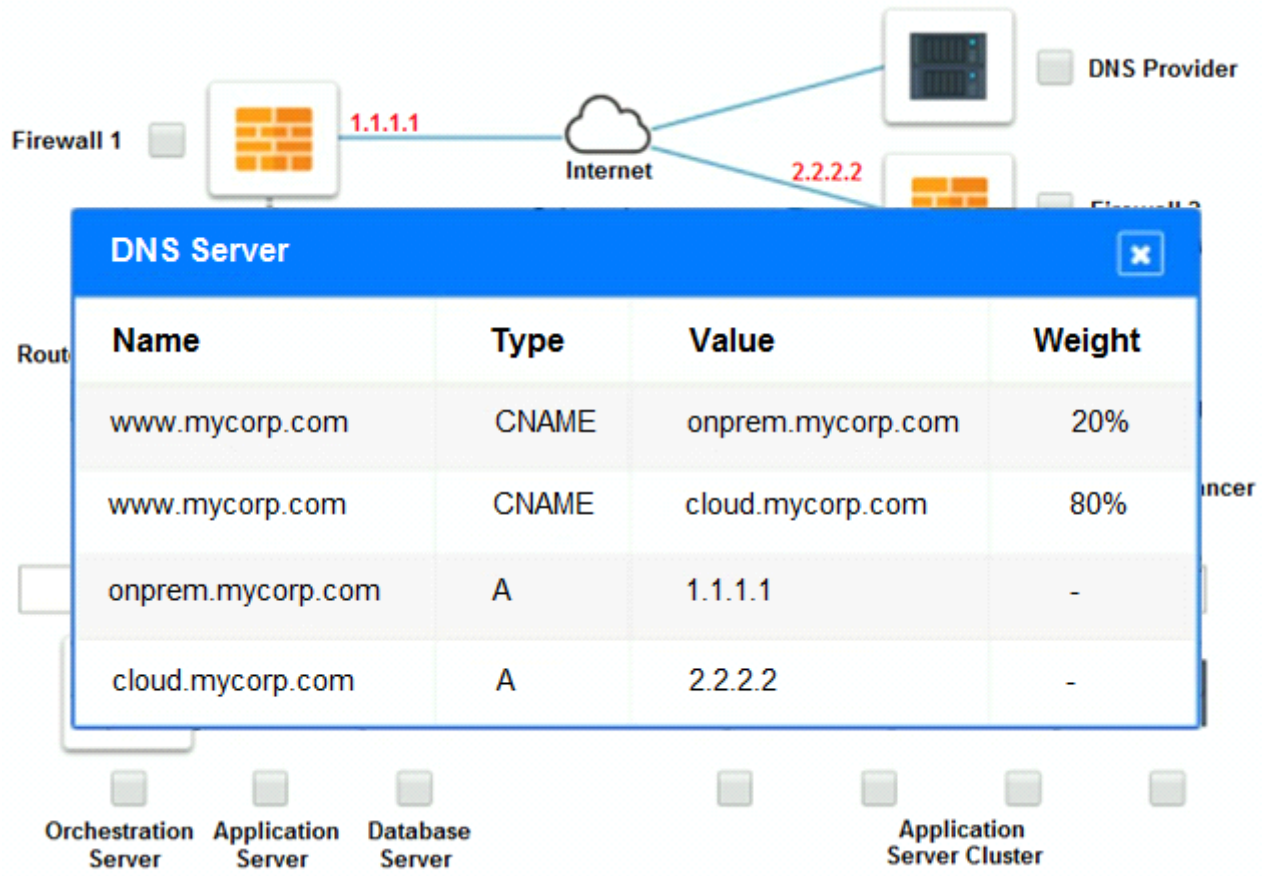

DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 1
Router Configuration
Public IP
1.1.1.1
Internal IP
10.1.1.1/24
Router 2
Site-to-site VPN Configuration
Load Balancer
Address Space
10.1.1.0/24
10.1.1.
Subnet
255.255.255.0
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800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


Firewall 1
1.1.1.1
Internet
DNS Provider
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


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 1
Router 2
Load Balancer
Orchestration Server
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


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 2
Load Balancer
Source
Destination
Port
ANY
2.2.2.2
80,443
10.1.2.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1
24
Orchestration Server
Application Server
Database Server
Application Server Cluster



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.

Options:

A) Deploy a Replica of the Database Server in the Cloud Provider

B) Update the PSK (Pre-shared key) in Router 2

C) Update the A record on the DNS from 2.2.2.2 to 1.1.1.1.

D) Promote deny All to allow All in Firewall 1 and Firewall 2.

E) Change the Address Space on Router 2.

F) Change internal IP Address of Router 1

G) Reverse the Weight property in the two CNAME records on the DNS

H) Add the Application Server at on-premises to the Load Balancer.

Answer:

B, E

Explanation:

* Change the Address Space on Router2

* Update the PSK (Pre-shared key in Router2)

Question 4

Question Type: MultipleChoice

After accidentally uploading a password for an IAM user in plain text, which of the following should a cloud administrator do FIRST?

Options:

A) Identify the resources that are accessible to the affected IAM user

B) Remove the published plain-text password

C) Notify users that a data breach has occurred

D) Change the affected IAM user's password

E) Delete the affected IAM user

Answer:

B

Question 5

Question Type: MultipleChoice

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).

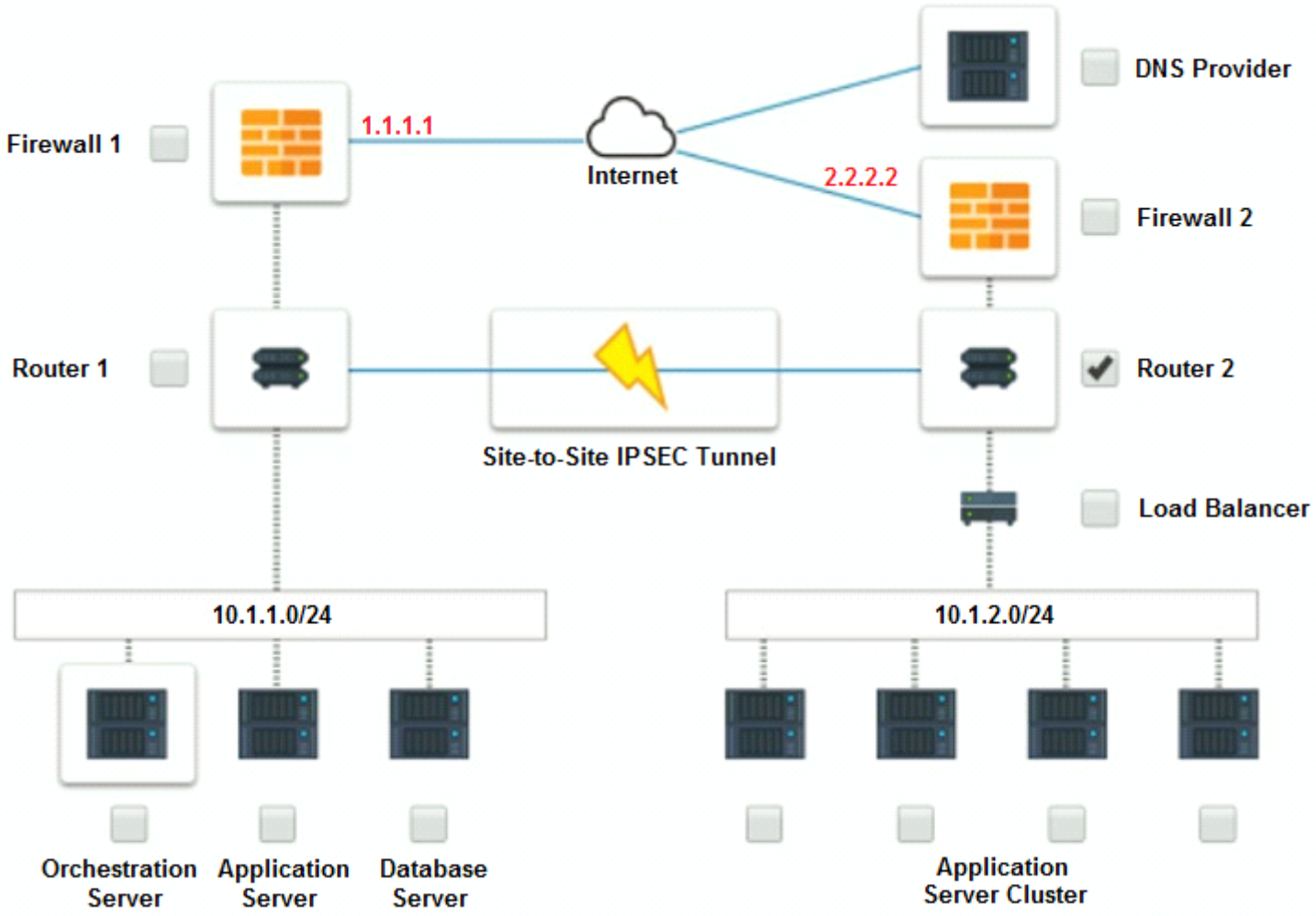
Part 2:

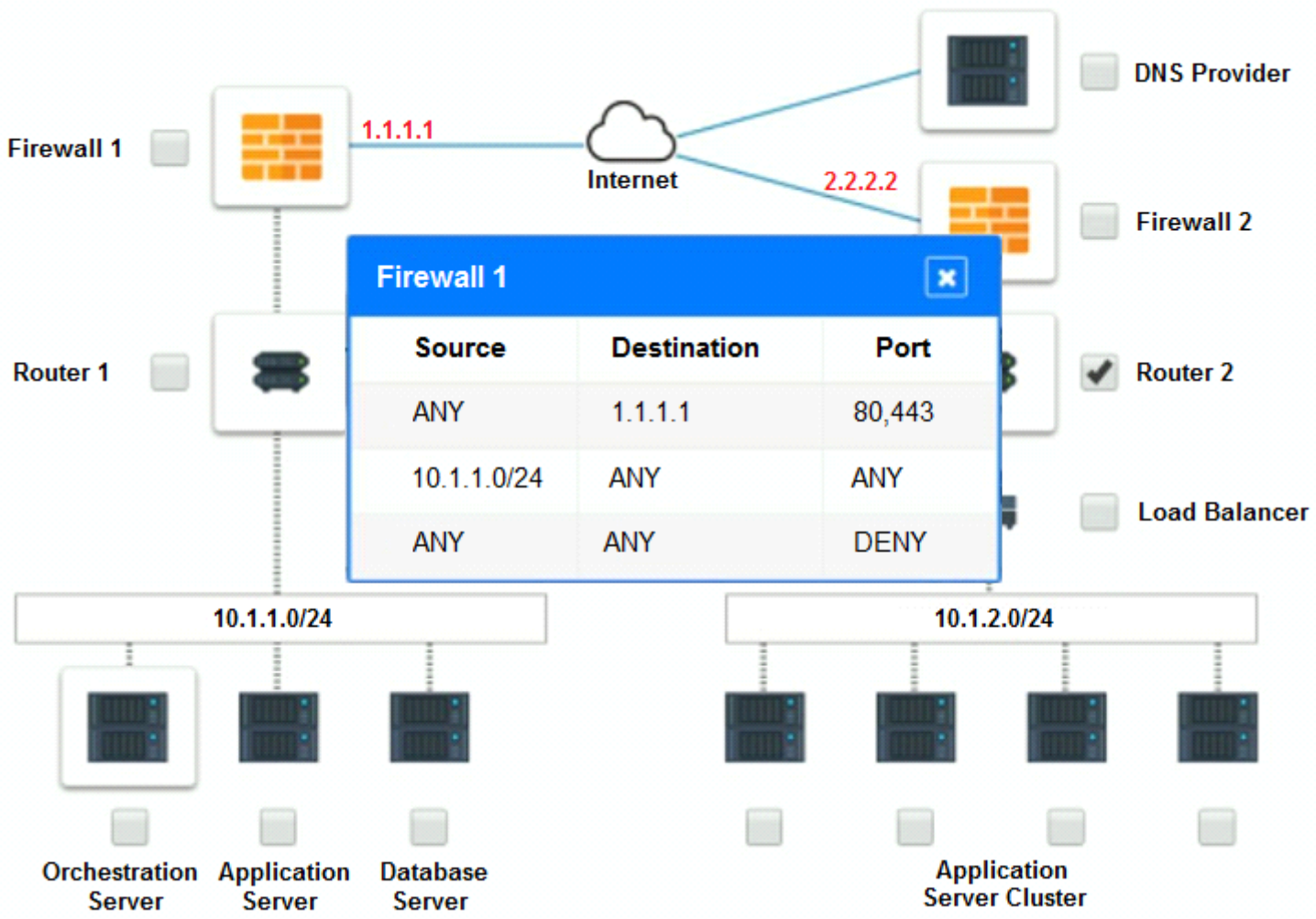
Identify the correct options to provide adequate configuration for hybrid cloud architecture.

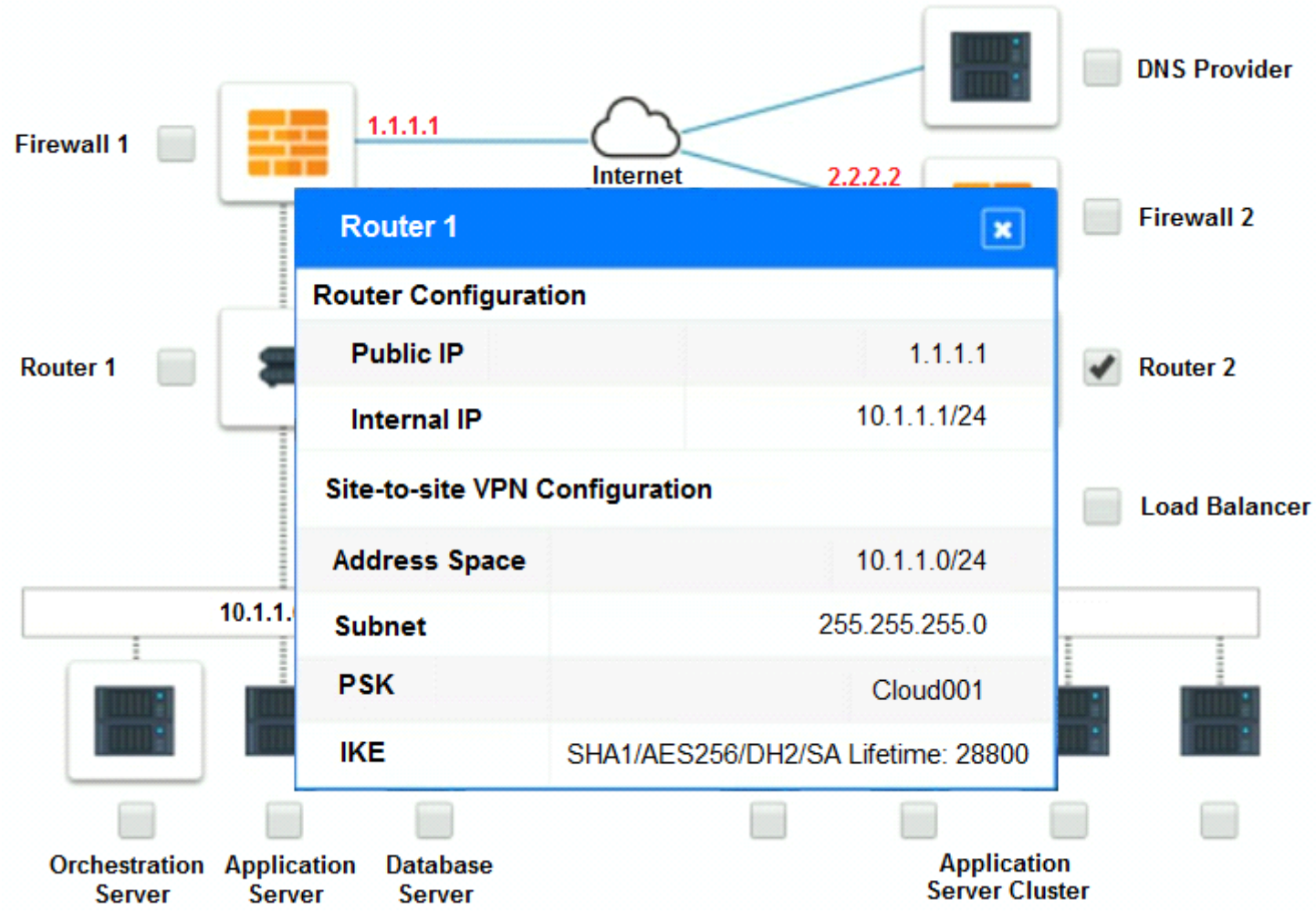
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

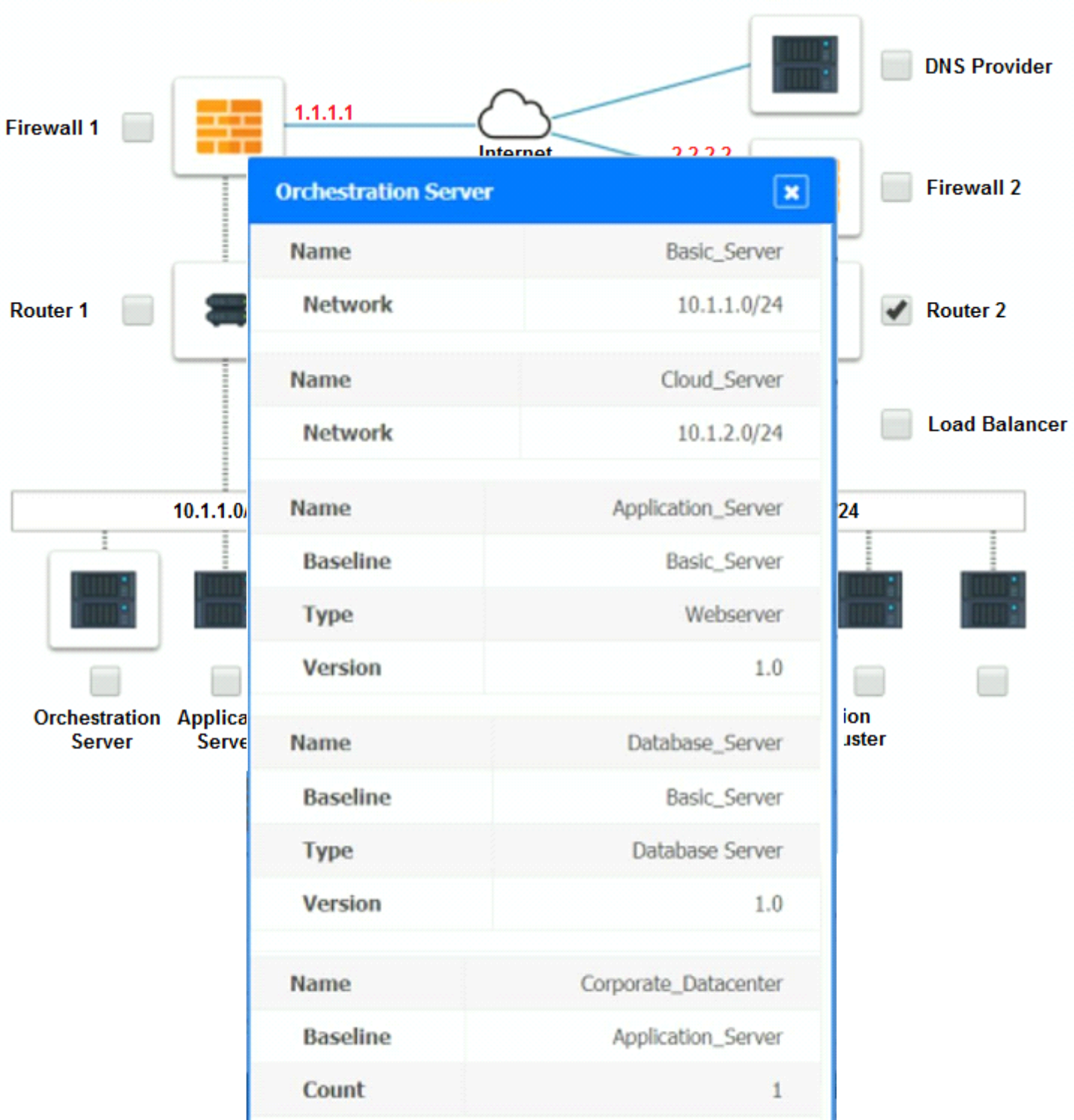
Part 1:

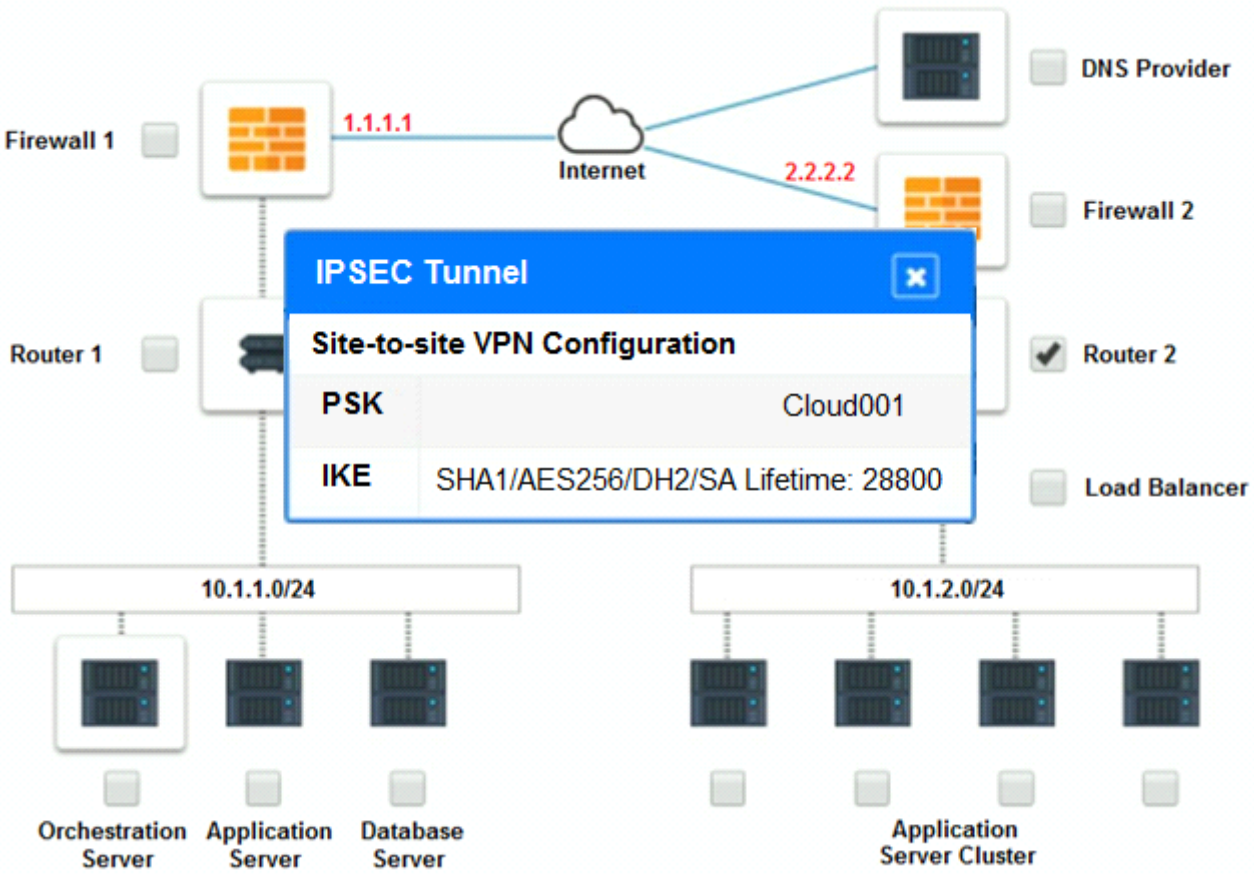
Cloud Hybrid Network Diagram

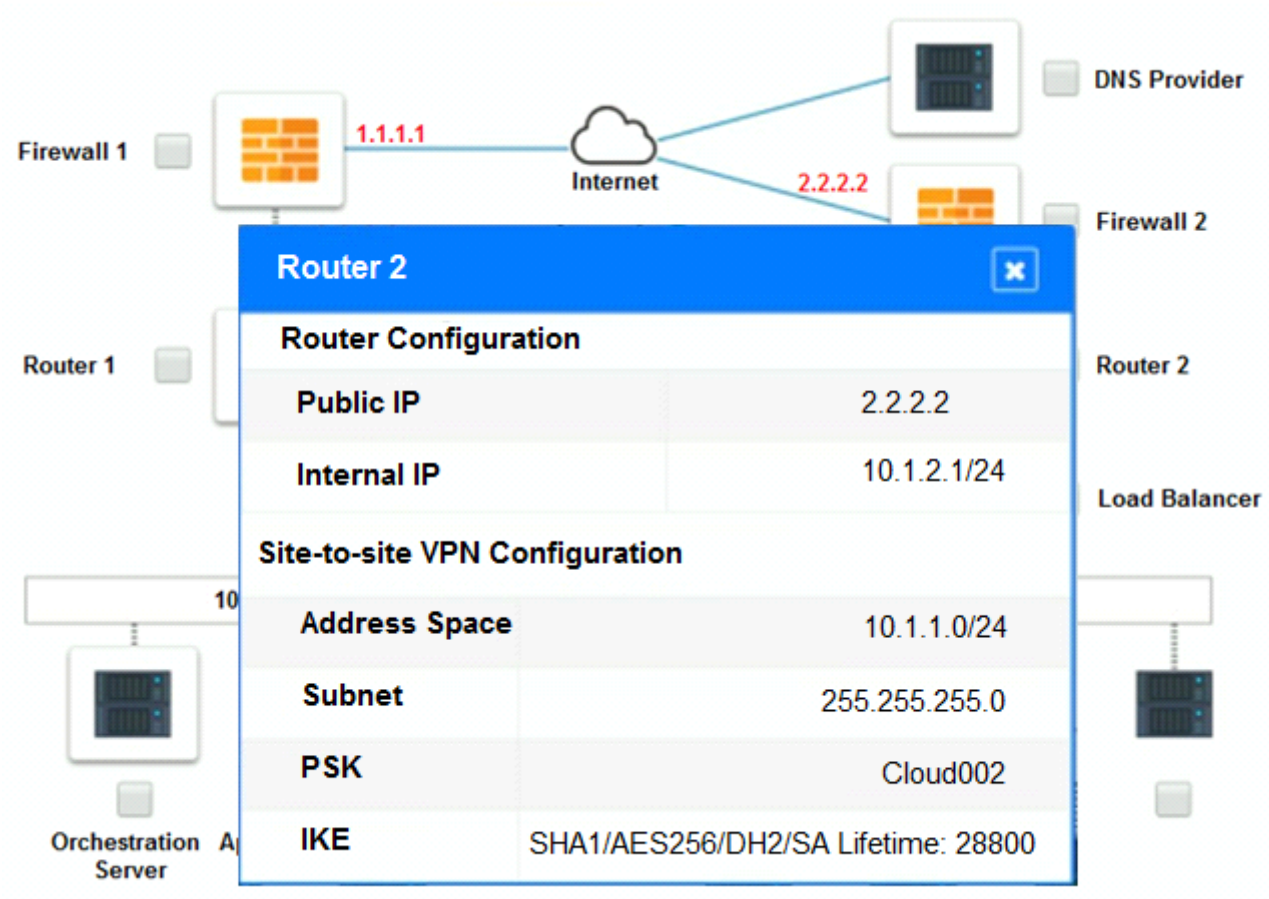

DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 2
Site-to-Site IPSEC Tunnel
Load Balancer
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

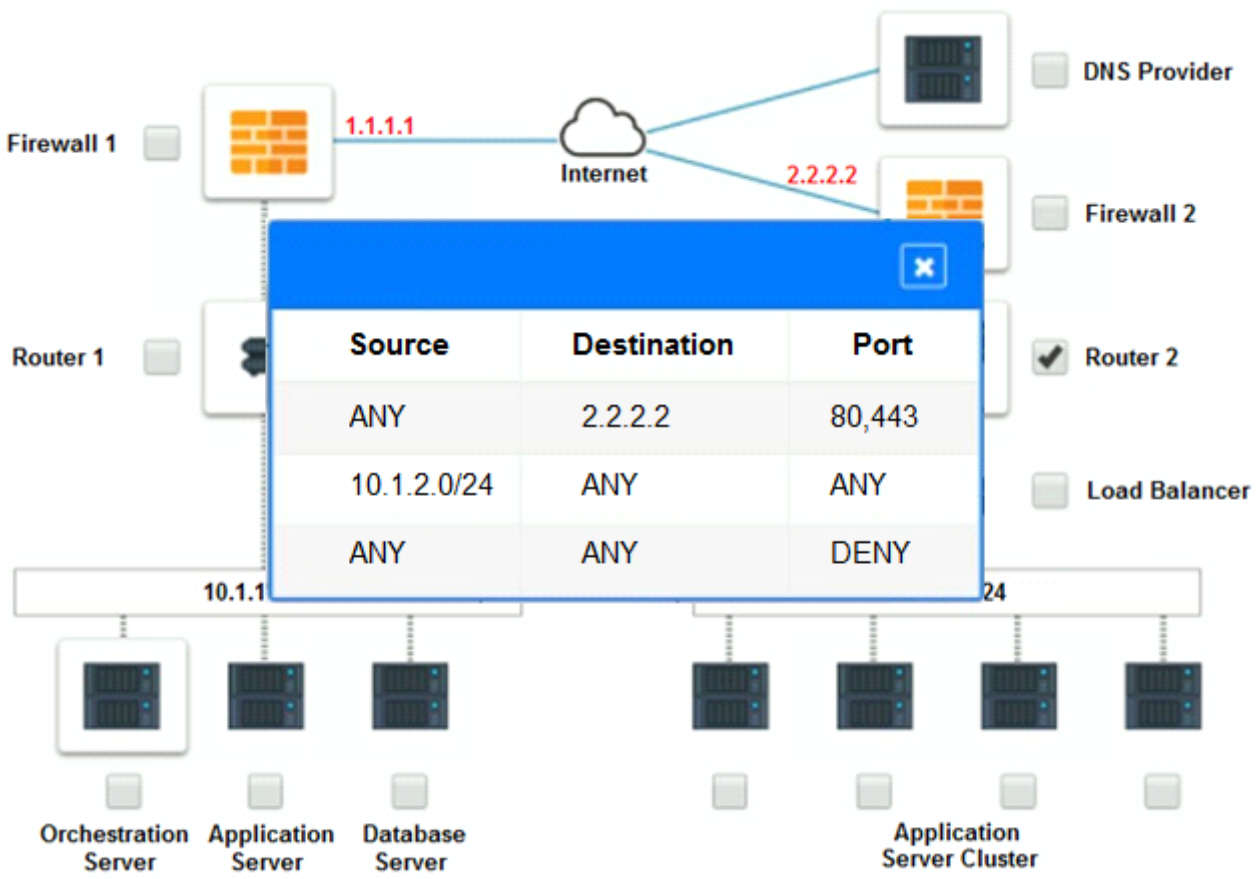

Firewall 1
1.1.1.1
Internet
2.2.2.2
DNS Provider
Firewall 2
Router 1
Router 2
Load Balancer
Firewall 1
Source
Destination
Port
ANY
1.1.1.1
80,443
10.1.1.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1.0/24
10.1.2.0/24
Orchestration Server
Application Server
Database Server
Application Server Cluster

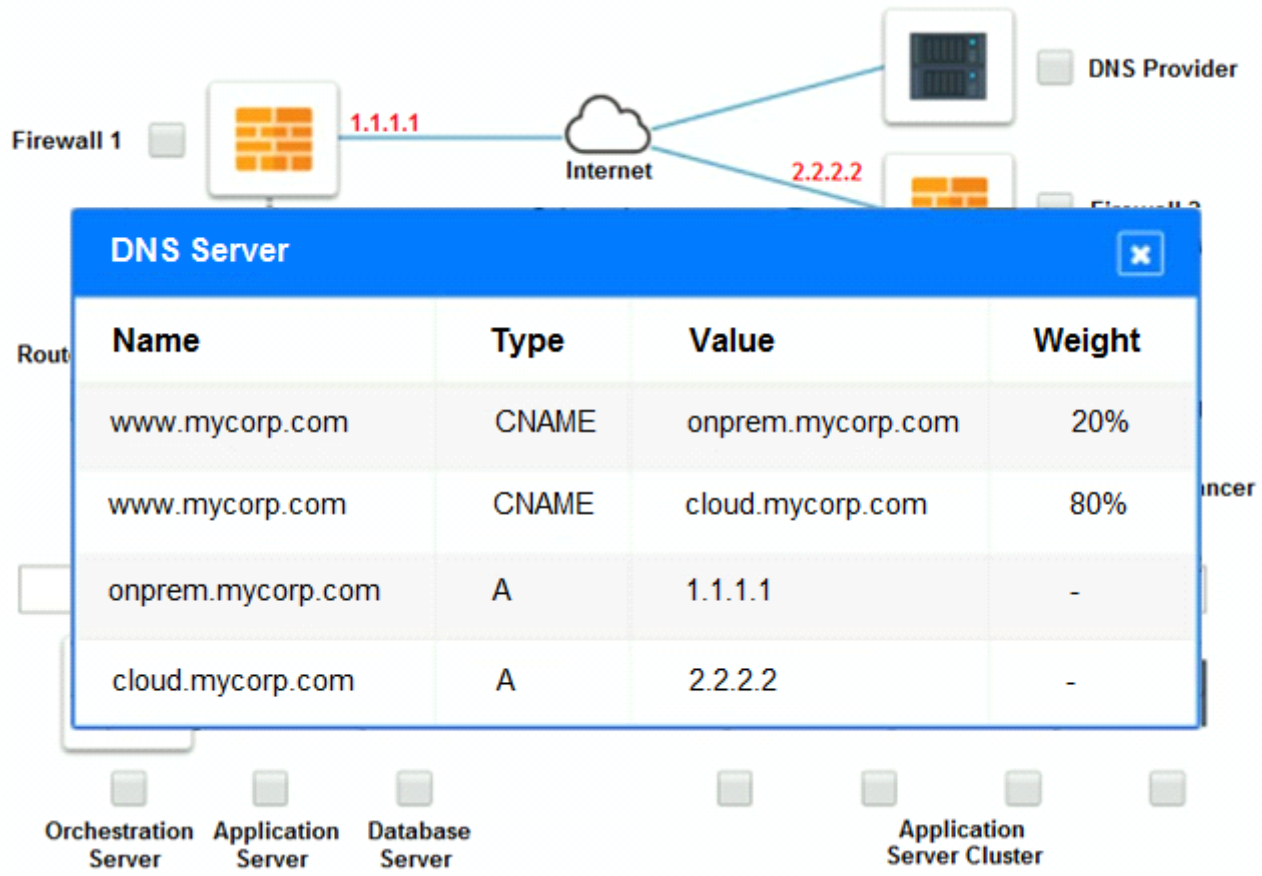

DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 1
Router Configuration
Public IP
1.1.1.1
Internal IP
10.1.1.1/24
Router 2
Site-to-site VPN Configuration
Load Balancer
Address Space
10.1.1.0/24
10.1.1.
Subnet
255.255.255.0
PSK
Cloud001
IKE
SHA1/AES256/DH2/SA Lifetime: 28800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


Firewall 1
1.1.1.1
Internet
DNS Provider
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


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 1
Router 2
Load Balancer
Orchestration Server
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


DNS Provider
Firewall 1
1.1.1.1
Internet
2.2.2.2
Firewall 2
Router 1
Router 2
Load Balancer
Source
Destination
Port
ANY
2.2.2.2
80,443
10.1.2.0/24
ANY
ANY
ANY
ANY
DENY
10.1.1
24
Orchestration Server
Application Server
Database Server
Application Server Cluster



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.

Options:

A) Deploy a Replica of the Database Server in the Cloud Provider

B) Update the PSK (Pre-shared key) in Router 2

C) Update the A record on the DNS from 2.2.2.2 to 1.1.1.1.

D) Promote deny All to allow All in Firewall 1 and Firewall 2.

E) Change the Address Space on Router 2.

F) Change internal IP Address of Router 1

G) Reverse the Weight property in the two CNAME records on the DNS

H) Add the Application Server at on-premises to the Load Balancer.

Answer:

B, E

Explanation:

* Change the Address Space on Router2

* Update the PSK (Pre-shared key in Router2)

Question 6

Question Type: MultipleChoice

SIMULATION

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.

INSTRUCTIONS

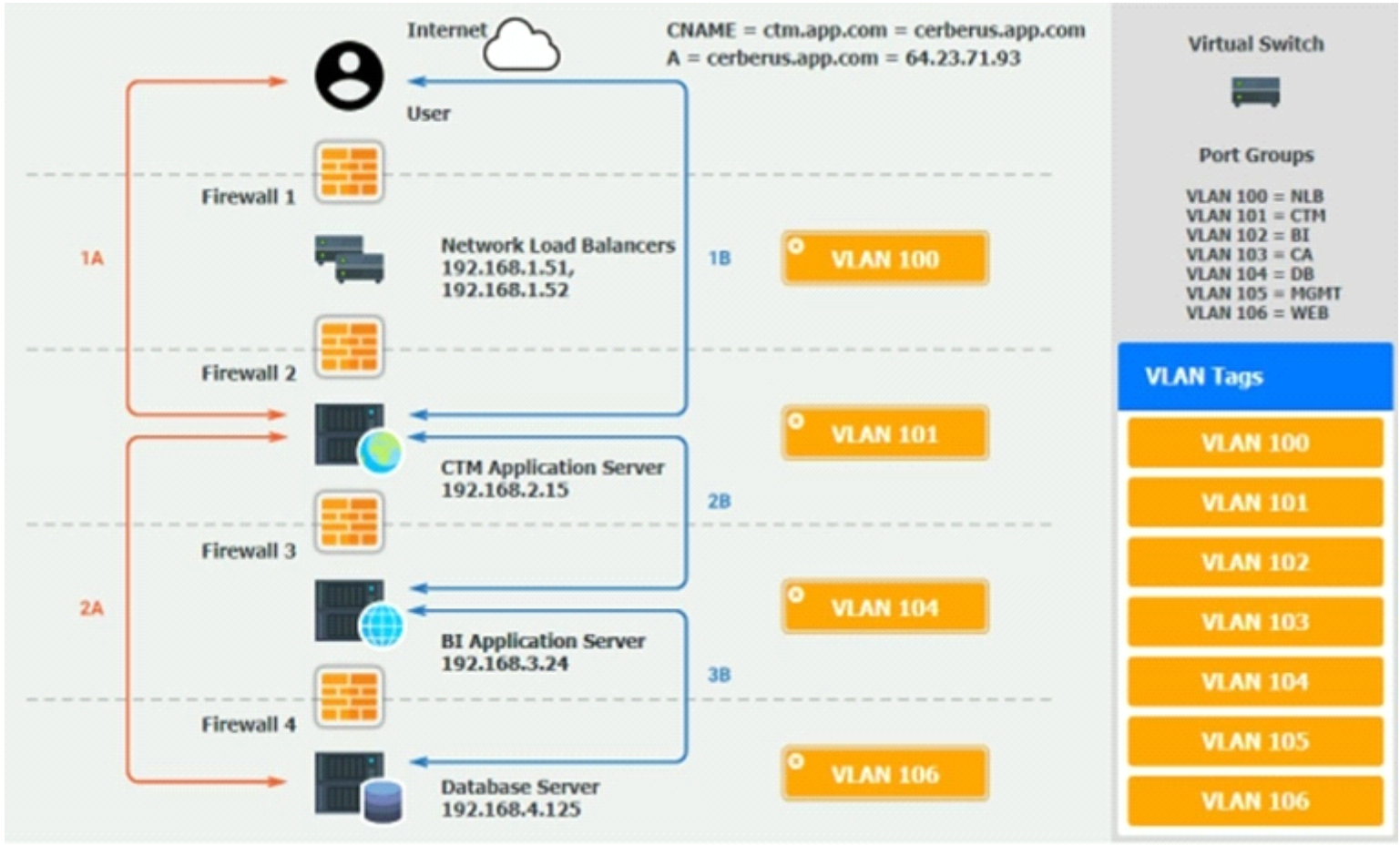
You are a cloud engineer who is tasked with reviewing the firewall rules as well as virtual network settings.

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.

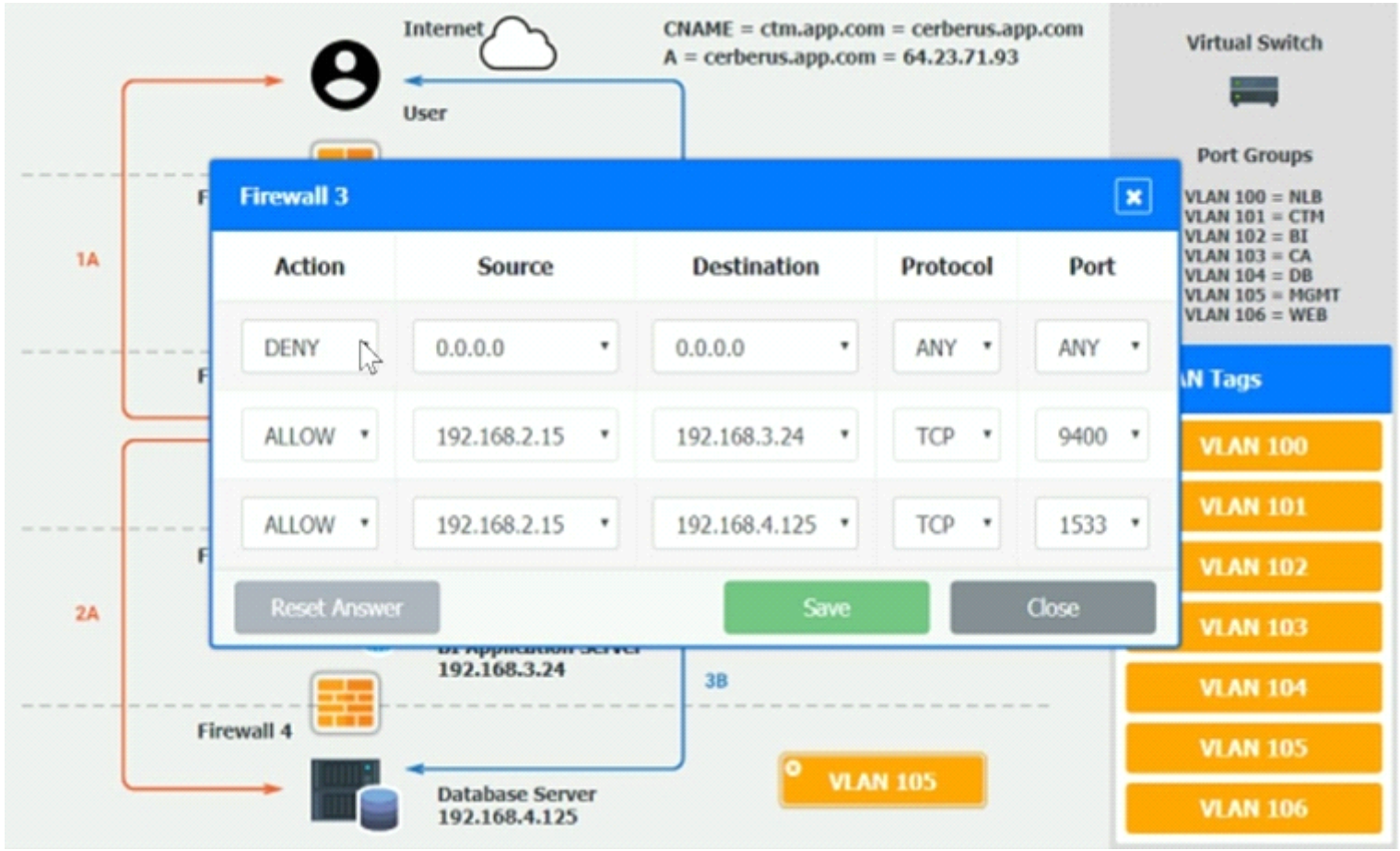
Verify and appropriately configure the VLAN assignments and ACLs. Drag and drop the appropriate VLANs to each tier from the VLAN Tags table. Click on each Firewall to change ACLs as needed.

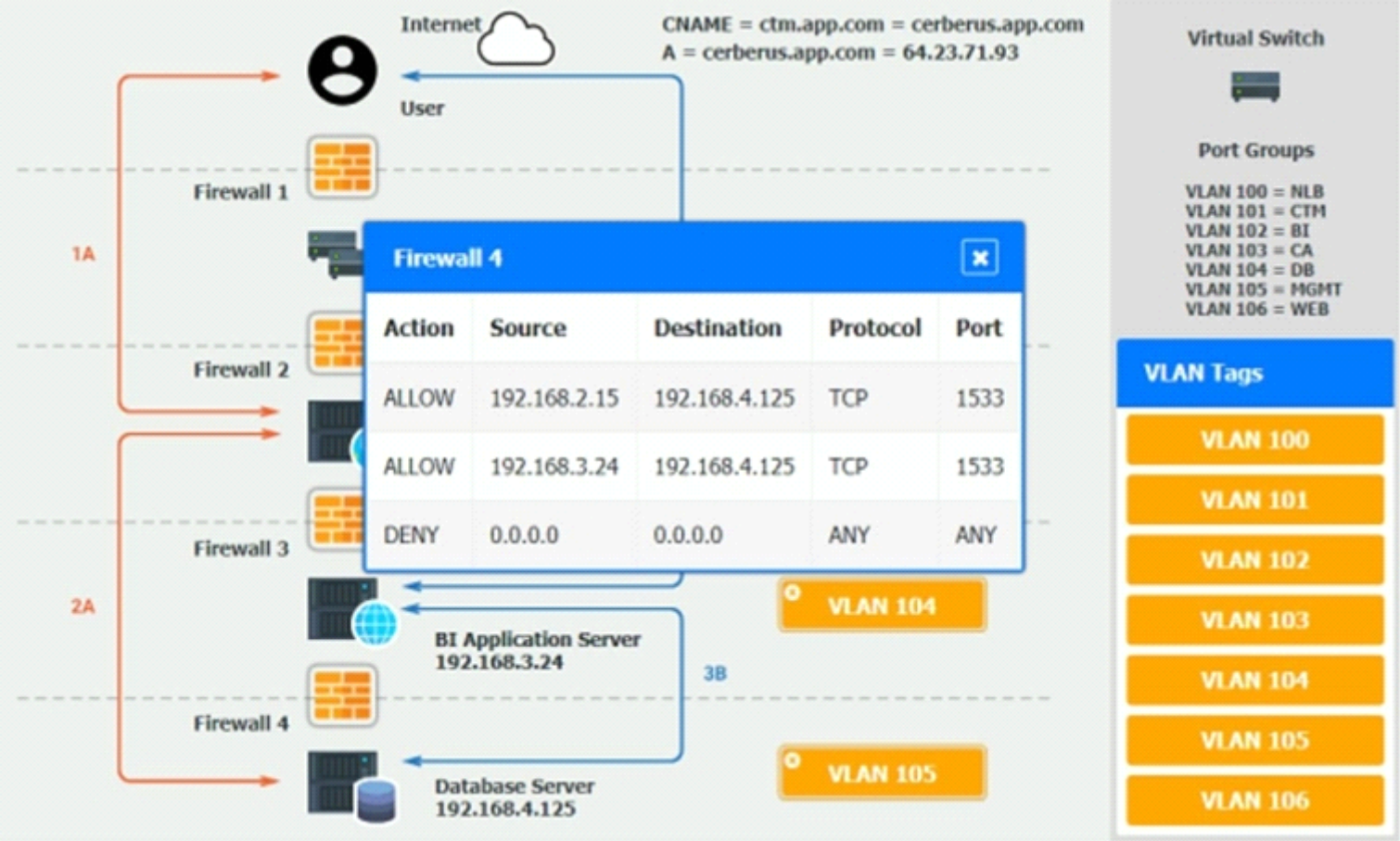
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


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
1A
Firewall 2
Firewall 3
2A
Firewall 4
192.168.3.24
3B
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
Port Groups
VLAN 100 = NLB
VLAN 101 = CTM
VLAN 102 = BI
VLAN 103 = CA
VLAN 104 = DB
VLAN 105 = MGMT
VLAN 106 = WEB
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
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
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
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
1A
2A
3B
192.168.3.24
Firewall 4
Database Server
192.168.4.125
VLAN 105
VLAN 100
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 105
VLAN 106



Options:

A) On firewall 3, change the DENY 0.8.8.0 entry to rule 3 not rule 1.

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

Answer:

B

To Get Premium Files for CV0-003 Visit

https://www.p2pexams.com/products/cv0-003

For More Free Questions Visit

https://www.p2pexams.com/comptia/pdf/cv0-003