Demo Questions

CompTIA CAS-003 Exam

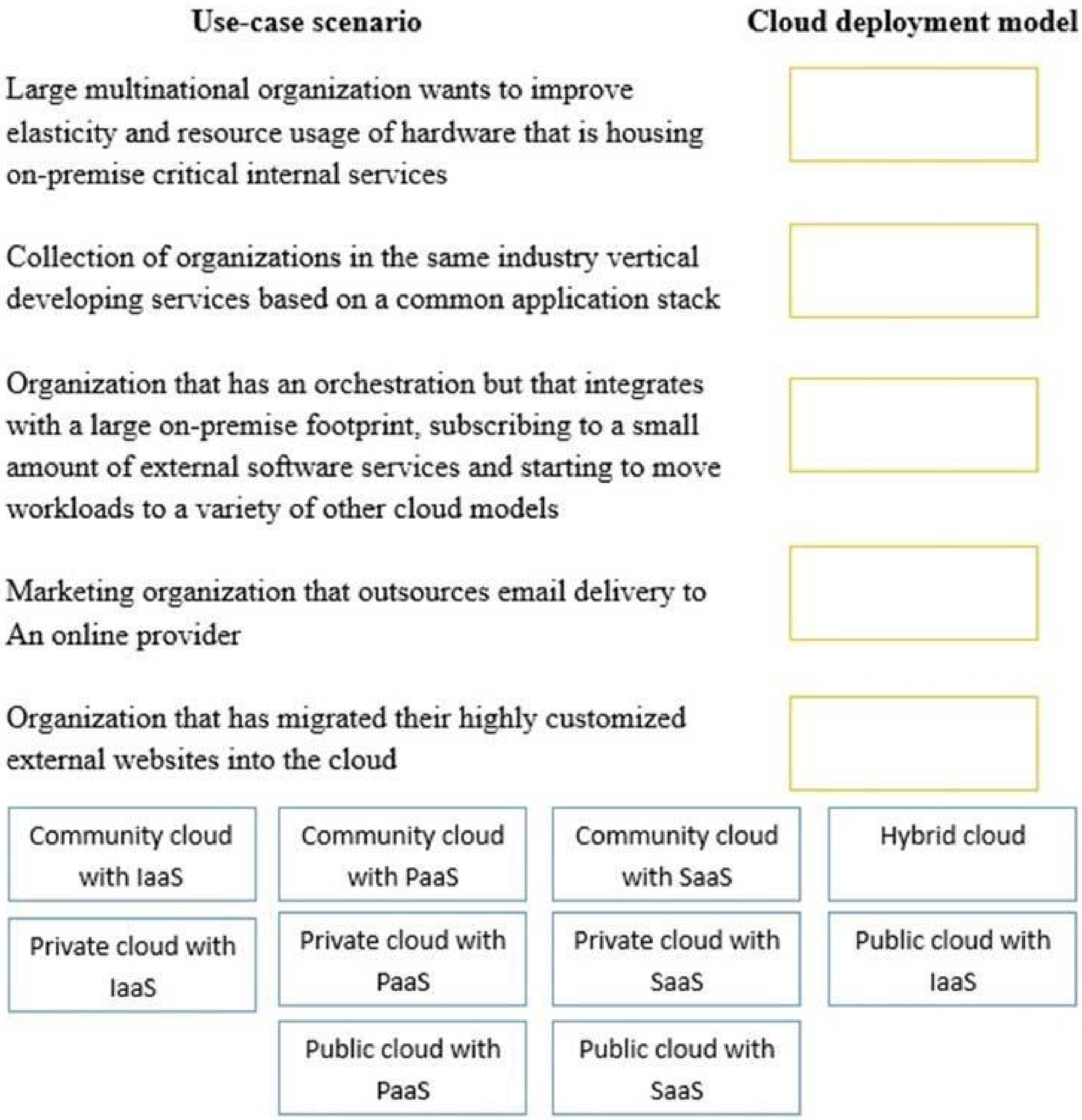
CompTIA Advanced Security Practitioner (CASP) CAS-003

Thank you for downloading CAS-003 Exam PDF

Question #1*Topic 1*

DRAG DROP -
Drag and drop the cloud deployment model to the associated use-case scenario. Options may be used only once or not at all.

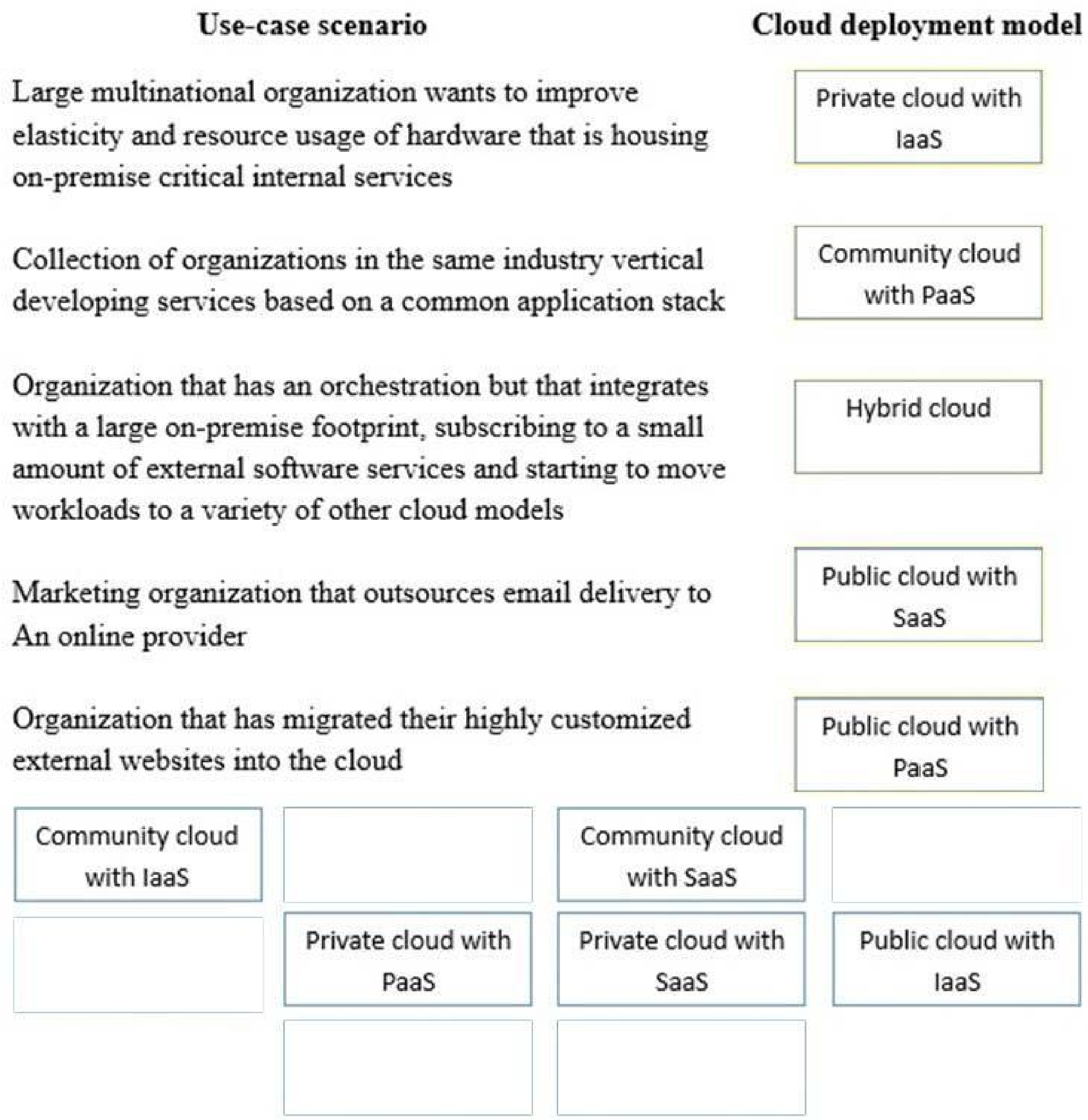
Select and Place:



Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	
Collection of organizations in the same industry vertical developing services based on a common application stack	
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	
Marketing organization that outsources email delivery to An online provider	
Organization that has migrated their highly customized external websites into the cloud	

Community cloud with IaaS	Community cloud with PaaS	Community cloud with SaaS	Hybrid cloud
Private cloud with IaaS	Private cloud with PaaS	Private cloud with SaaS	Public cloud with IaaS
	Public cloud with PaaS	Public cloud with SaaS	

Correct Answer:



Use-case scenario	Cloud deployment model
Large multinational organization wants to improve elasticity and resource usage of hardware that is housing on-premise critical internal services	Private cloud with IaaS
Collection of organizations in the same industry vertical developing services based on a common application stack	Community cloud with PaaS
Organization that has an orchestration but that integrates with a large on-premise footprint, subscribing to a small amount of external software services and starting to move workloads to a variety of other cloud models	Hybrid cloud
Marketing organization that outsources email delivery to An online provider	Public cloud with SaaS
Organization that has migrated their highly customized external websites into the cloud	Public cloud with PaaS

Community cloud with IaaS

Community cloud with SaaS

Private cloud with PaaS

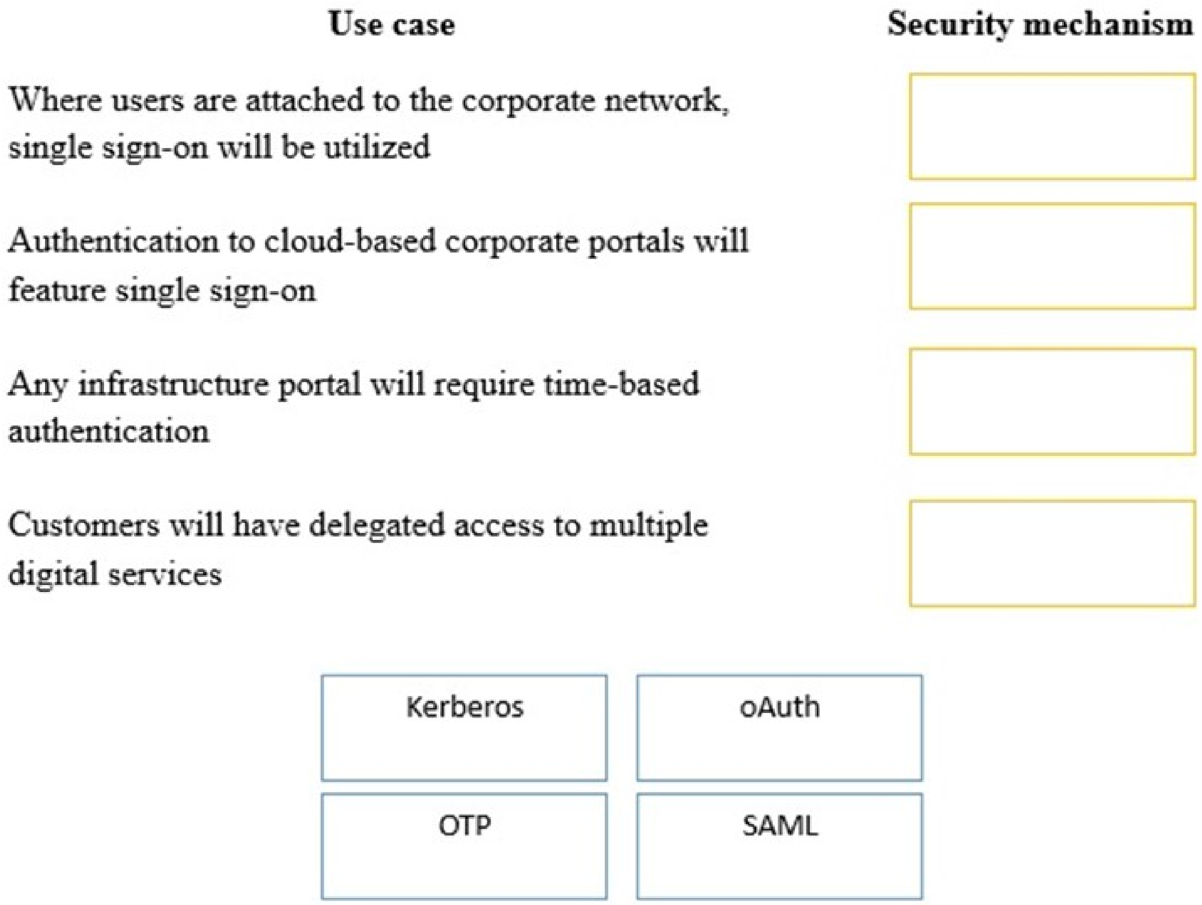
Private cloud with SaaS

Public cloud with IaaS

Question #2*Topic 1*

DRAG DROP -
A security consultant is considering authentication options for a financial institution. The following authentication options are available. Drag and drop the security mechanism to the appropriate use case. Options may be used once.

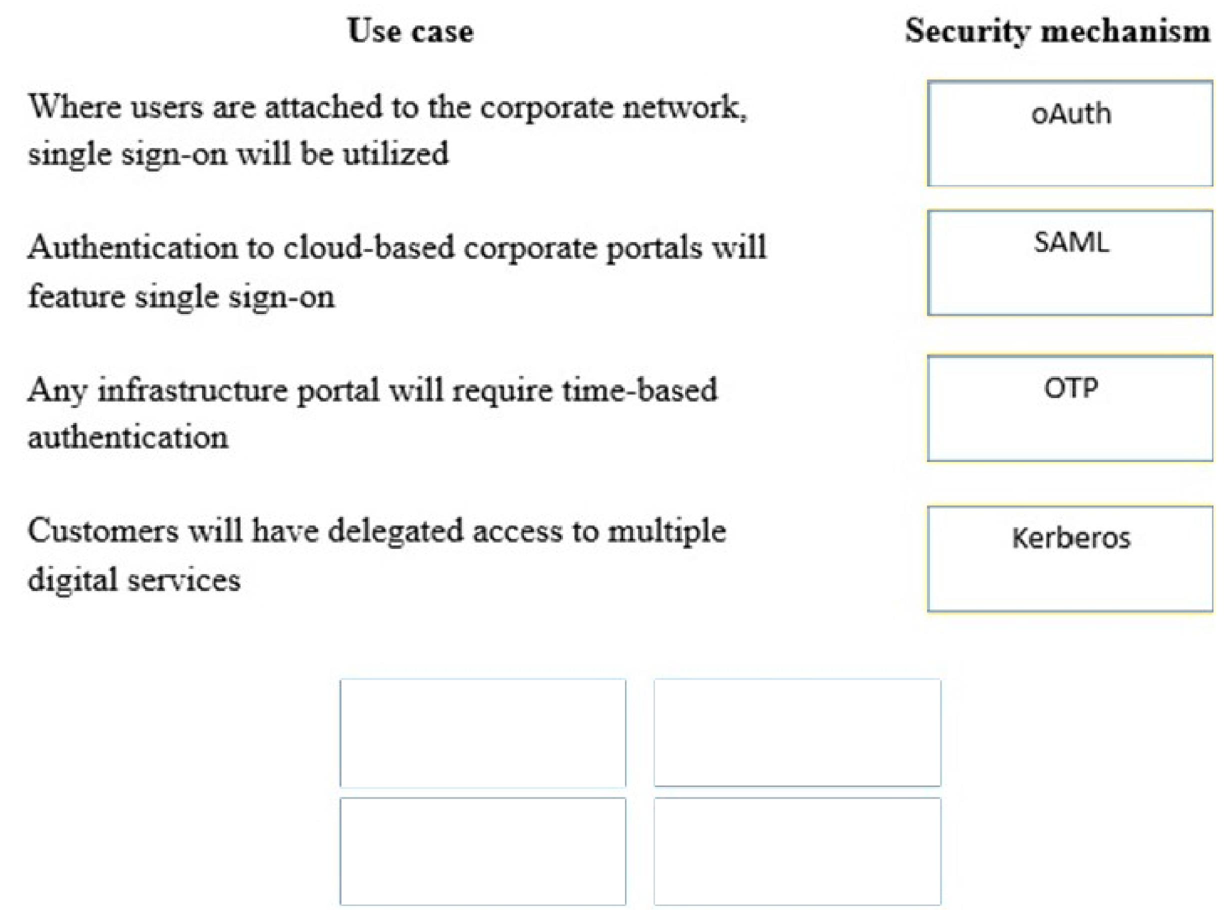
Select and Place:



Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	
Authentication to cloud-based corporate portals will feature single sign-on	
Any infrastructure portal will require time-based authentication	
Customers will have delegated access to multiple digital services	

Kerberos	oAuth
OTP	SAML

Correct Answer:



Use case	Security mechanism
Where users are attached to the corporate network, single sign-on will be utilized	oAuth
Authentication to cloud-based corporate portals will feature single sign-on	SAML
Any infrastructure portal will require time-based authentication	OTP
Customers will have delegated access to multiple digital services	Kerberos

Question #3*Topic 1*

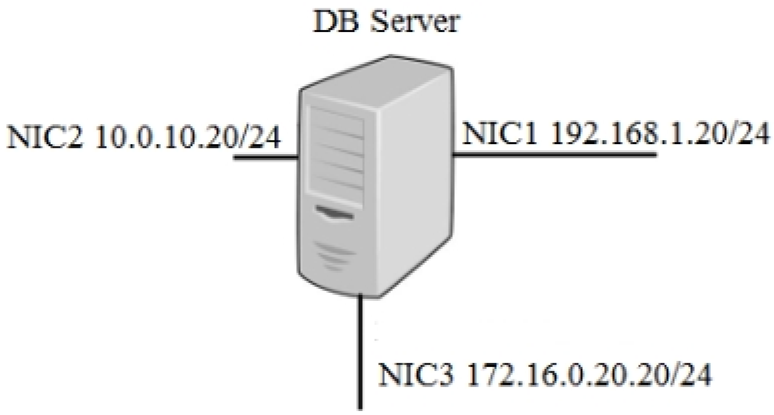
An infrastructure team is at the end of a procurement process and has selected a vendor. As part of the final negotiations, there are a number of outstanding issues, including:
1. Indemnity clauses have identified the maximum liability
2. The data will be hosted and managed outside of the company's geographical location
The number of users accessing the system will be small, and no sensitive data will be hosted in the solution. As the security consultant on the project, which of the following should the project's security consultant recommend as the NEXT step?

- A. Develop a security exemption, as it does not meet the security policies
- B. Mitigate the risk by asking the vendor to accept the in-country privacy principles
- [✓ C. Require the solution owner to accept the identified risks and consequences]
- D. Review the entire procurement process to determine the lessons learned

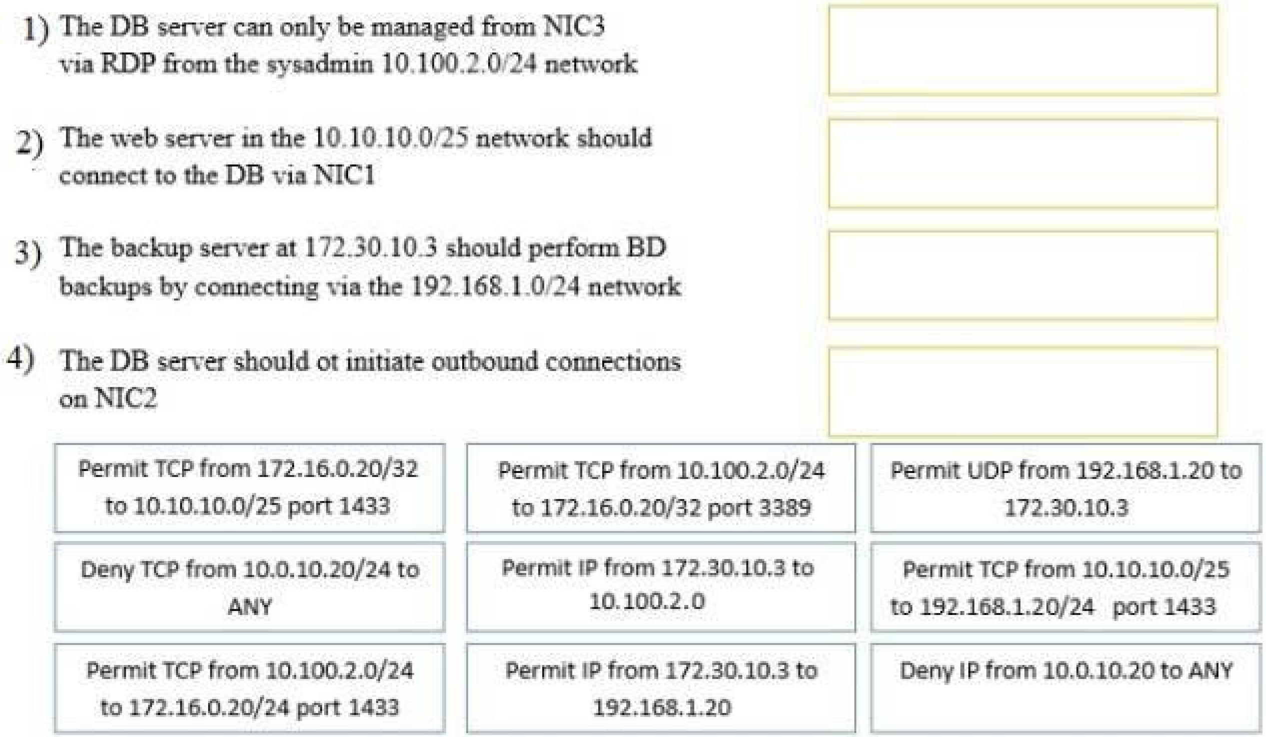
Correct Answer: *C*

Question #4*Topic 1*

DRAG DROP -
A security administrator must configure the database server shown below to comply with the four requirements listed. Drag and drop the appropriate ACL that should be configured on the database server to its corresponding requirement. Answer options may be used once or not at all.



Select and Place:



1) The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network

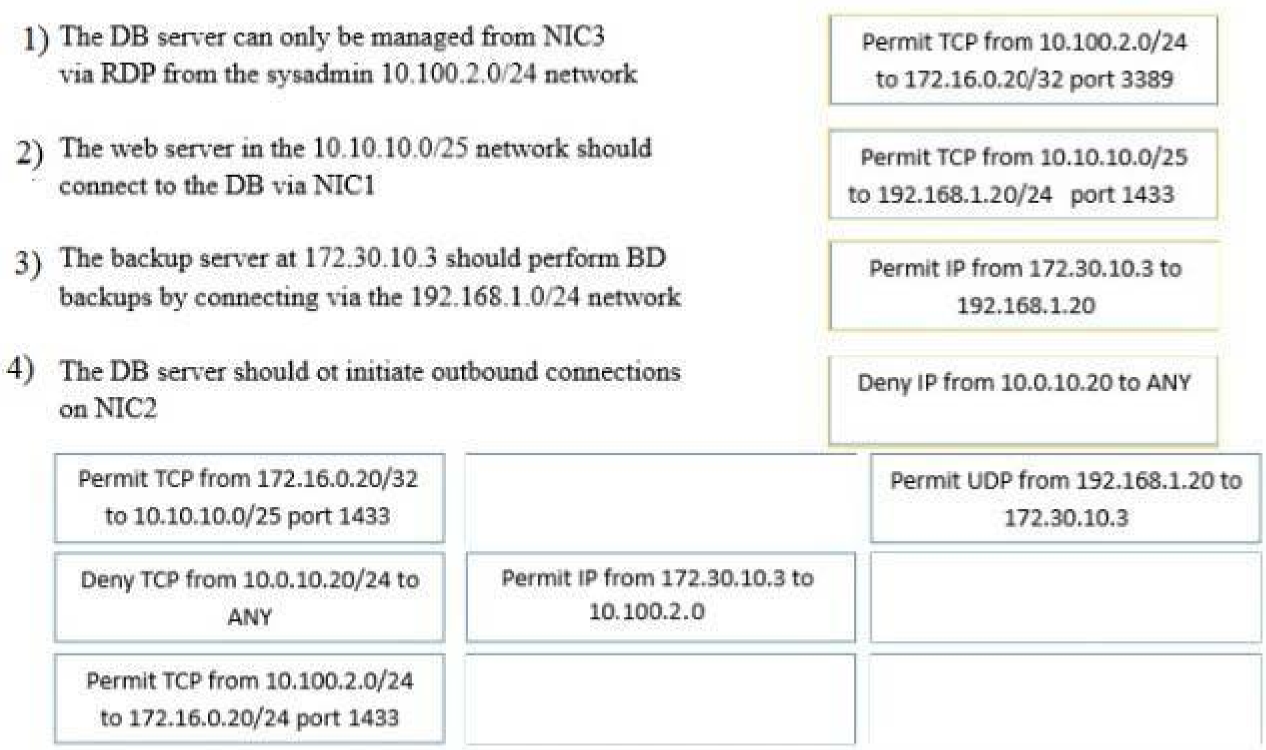
2) The web server in the 10.10.10.0/25 network should connect to the DB via NIC1

3) The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network

4) The DB server should ot initiate outbound connections on NIC2

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1433	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389	Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Permit IP from 172.30.10.3 to 10.100.2.0	Permit TCP from 10.10.10.0/25 to 192.168.1.20/24 port 1433
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1433	Permit IP from 172.30.10.3 to 192.168.1.20	Deny IP from 10.0.10.20 to ANY

Correct Answer:



1) The DB server can only be managed from NIC3 via RDP from the sysadmin 10.100.2.0/24 network	Permit TCP from 10.100.2.0/24 to 172.16.0.20/32 port 3389
2) The web server in the 10.10.10.0/25 network should connect to the DB via NIC1	Permit TCP from 10.10.10.0/25 to 192.168.1.20/24 port 1433
3) The backup server at 172.30.10.3 should perform BD backups by connecting via the 192.168.1.0/24 network	Permit IP from 172.30.10.3 to 192.168.1.20
4) The DB server should ot initiate outbound connections on NIC2	Deny IP from 10.0.10.20 to ANY

Permit TCP from 172.16.0.20/32 to 10.10.10.0/25 port 1433		Permit UDP from 192.168.1.20 to 172.30.10.3
Deny TCP from 10.0.10.20/24 to ANY	Permit IP from 172.30.10.3 to 10.100.2.0	
Permit TCP from 10.100.2.0/24 to 172.16.0.20/24 port 1433		

Question #5*Topic 1*

A security administrator is hardening a TrustedSolaris server that processes sensitive data. The data owner has established the following security requirements:
✑ The data is for internal consumption only and shall not be distributed to outside individuals
✑ The systems administrator should not have access to the data processed by the server
✑ The integrity of the kernel image is maintained
Which of the following host-based security controls BEST enforce the data owner's requirements? (Choose three.)

- A. SELinux
- B. DLP
- C. HIDS
- D. Host-based firewall
- E. Measured boot
- F. Data encryption
- G. Watermarking

Correct Answer: *CEF*

Question #6*Topic 1*

An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

- A. Secure storage policies
- B. Browser security updates
- [✓ C. Input validation]
- D. Web application firewall
- E. Secure coding standards
- [✓ F. Database activity monitoring]

Correct Answer: *CF*

Question #7*Topic 1*

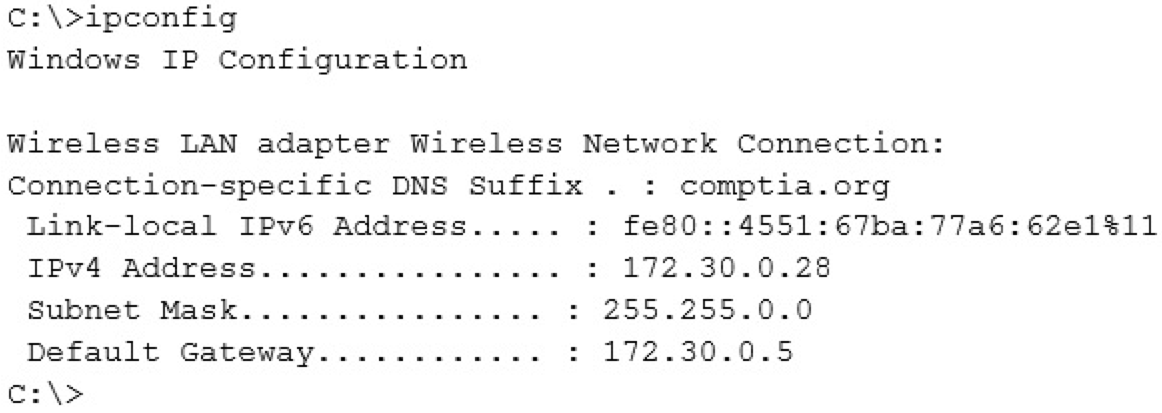
A company has entered into a business agreement with a business partner for managed human resources services. The Chief Information Security Officer (CISO) has been asked to provide documentation that is required to set up a business-to-business VPN between the two organizations. Which of the following is required in this scenario?

- A. ISA
- B. BIA
- C. SLA
- D. RA A

Correct Answer: *Explanation*

Question #8*Topic 1*

Given the following output from a local PC:



```
C:\>ipconfig
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : comptia.org
 Link-local IPv6 Address..... : fe80::4551:67ba:77a6:62e1%11
 IPv4 Address............... : 172.30.0.28
 Subnet Mask................ : 255.255.0.0
 Default Gateway............ : 172.30.0.5
C:\>
```

Which of the following ACLs on a stateful host-based firewall would allow the PC to serve an intranet website?

- A. Allow 172.30.0.28:80 -> ANY
- B. Allow 172.30.0.28:80 -> 172.30.0.0/16
- C. Allow 172.30.0.28:80 -> 172.30.0.28:443
- D. Allow 172.30.0.28:80 -> 172.30.0.28:53

Correct Answer: *B*

Question #9*Topic 1*

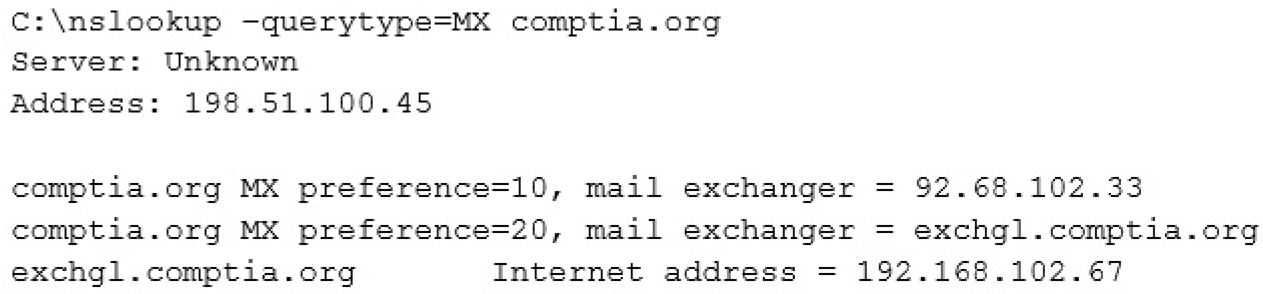
A penetration tester has been contracted to conduct a physical assessment of a site. Which of the following is the MOST plausible method of social engineering to be conducted during this engagement?

- A. Randomly calling customer employees and posing as a help desk technician requiring user password to resolve issues
- B. Posing as a copier service technician and indicating the equipment had "phoned home" to alert the technician for a service call
- C. Simulating an illness while at a client location for a sales call and then recovering once listening devices are installed
- D. Obtaining fake government credentials and impersonating law enforcement to gain access to a company facility

Correct Answer: *A*

Question #10*Topic 1*

A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:



```
C:\nslookup -querytype=MX comptia.org
Server: Unknown
Address: 198.51.100.45

comptia.org MX preference=10, mail exchanger = 92.68.102.33
comptia.org MX preference=20, mail exchanger = exchgl.comptia.org
exchgl.comptia.org       Internet address = 192.168.102.67
```

Which of the following should the penetration tester conclude about the command output?

- A. The public/private views on the Comptia.org DNS servers are misconfigured
- [✓ B. Comptia.org is running an older mail server, which may be vulnerable to exploits]
- C. The DNS SPF records have not been updated for Comptia.org
- D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack

Correct Answer: *B*