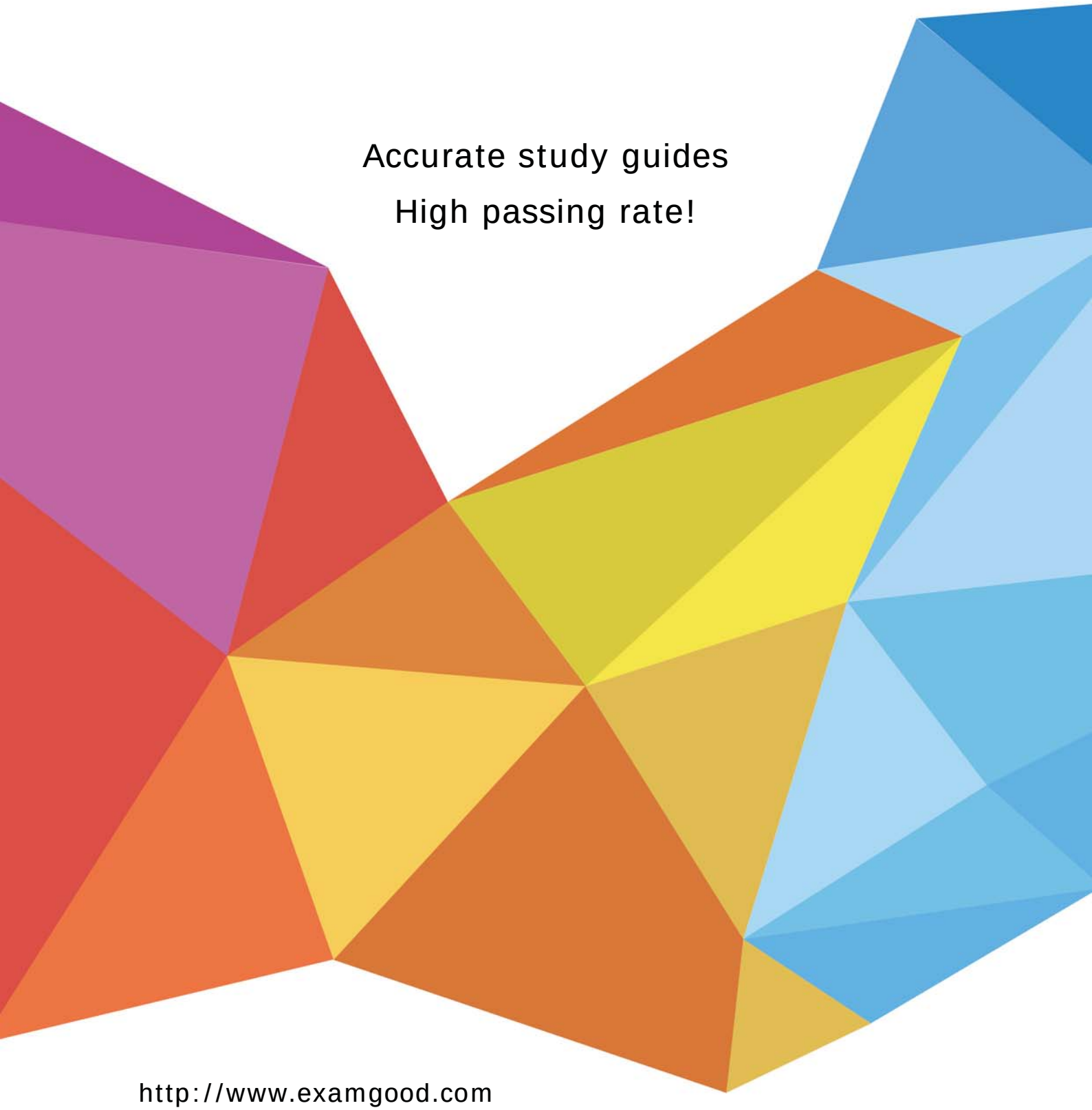
EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!



Accurate study guides

High passing rate!

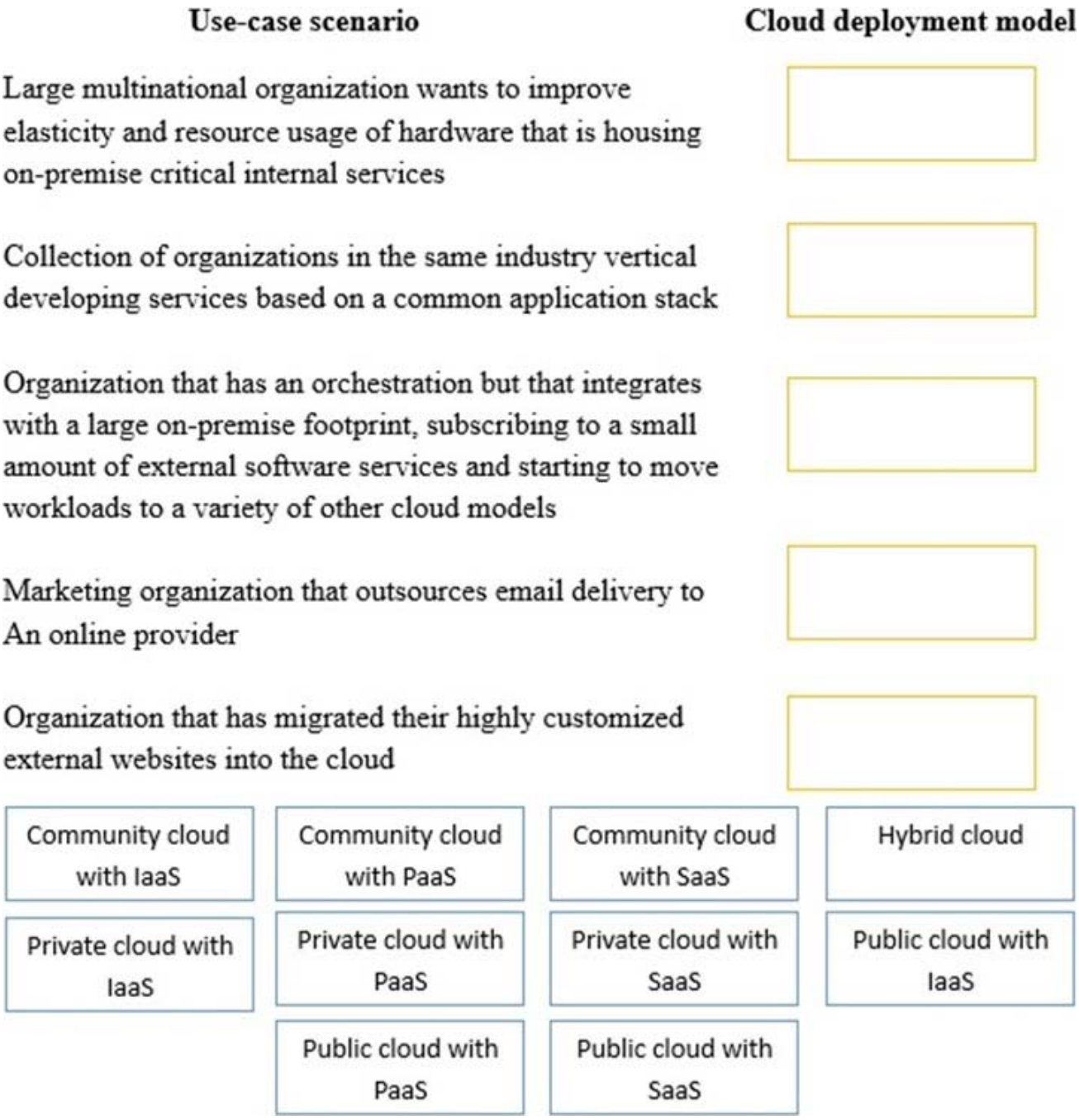
Exam : **CAS-003**

Title : CompTIA Advanced Security Practitioner (CASP)

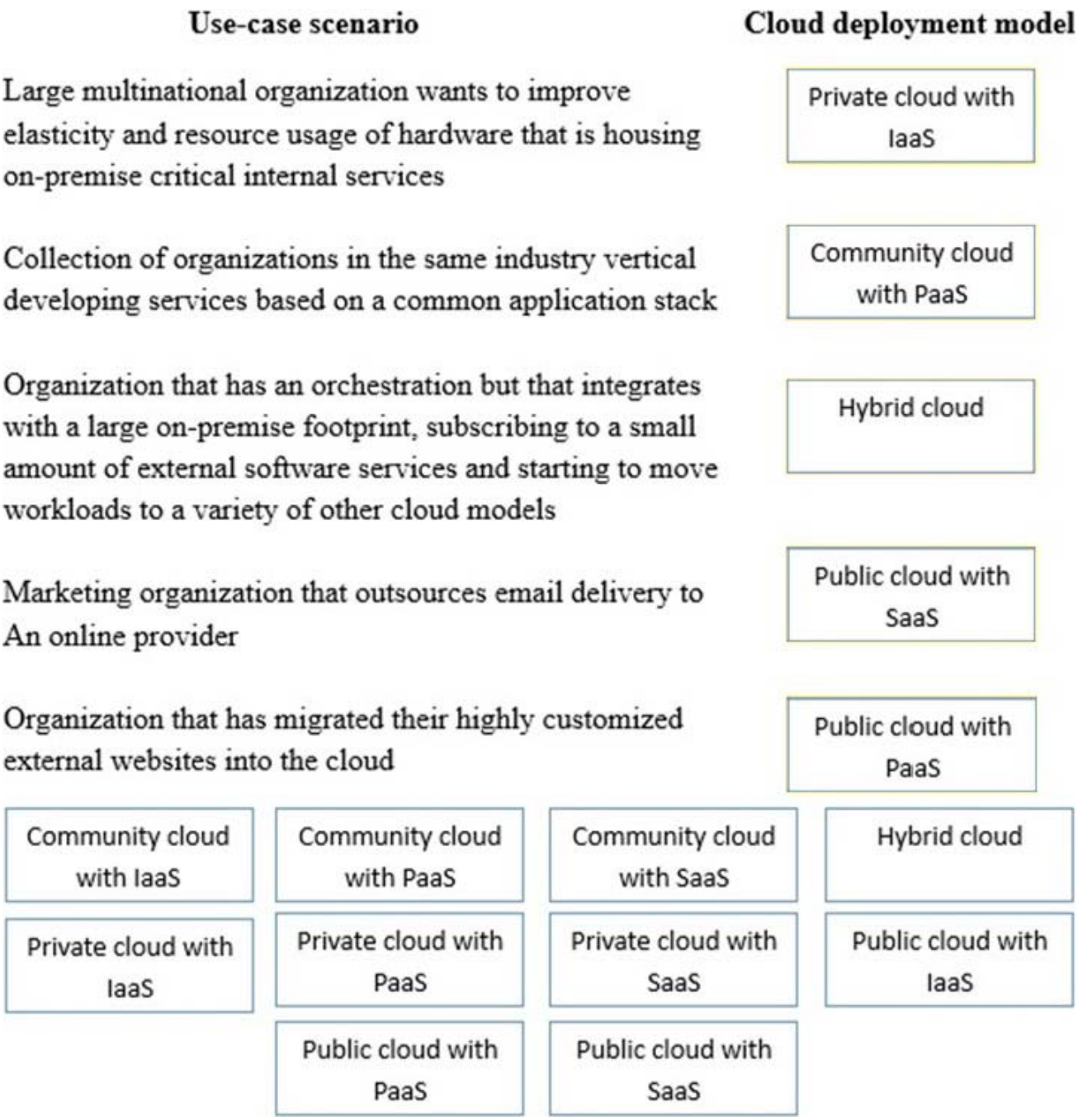
Version : DEMO

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.



Answer:



2.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.

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

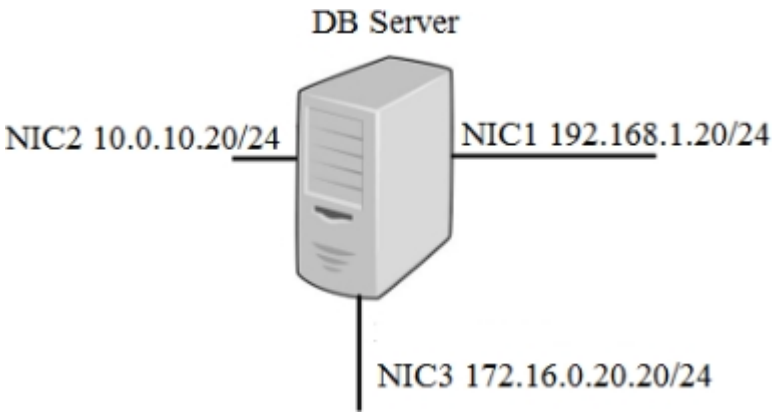
Answer:

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

Kerberos	oAuth
OTP	SAML

3.A company's Chief Operating Officer (COO) is concerned about the potential for competitors to infer proprietary information gathered from employees' social media accounts.
Which of the following methods should the company use to gauge its own social media threat level without targeting individual employees?
A. Utilize insider threat consultants to provide expertise.
B. Require that employees divulge social media accounts.
C. Leverage Big Data analytical algorithms.
D. Perform social engineering tests to evaluate employee awareness.
Answer: A

4.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.



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

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 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

5.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
Answer: CEF