PCCET Q&As

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Pass Palo Alto Networks PCCET Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pccet.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which technique changes protocols at random during a session?

A. use of non-standard ports

B. port hopping

C. hiding within SSL encryption

D. tunneling within commonly used services

Correct Answer: B

Port hopping, in which ports and protocols are randomly changed during a session.

QUESTION 2

Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

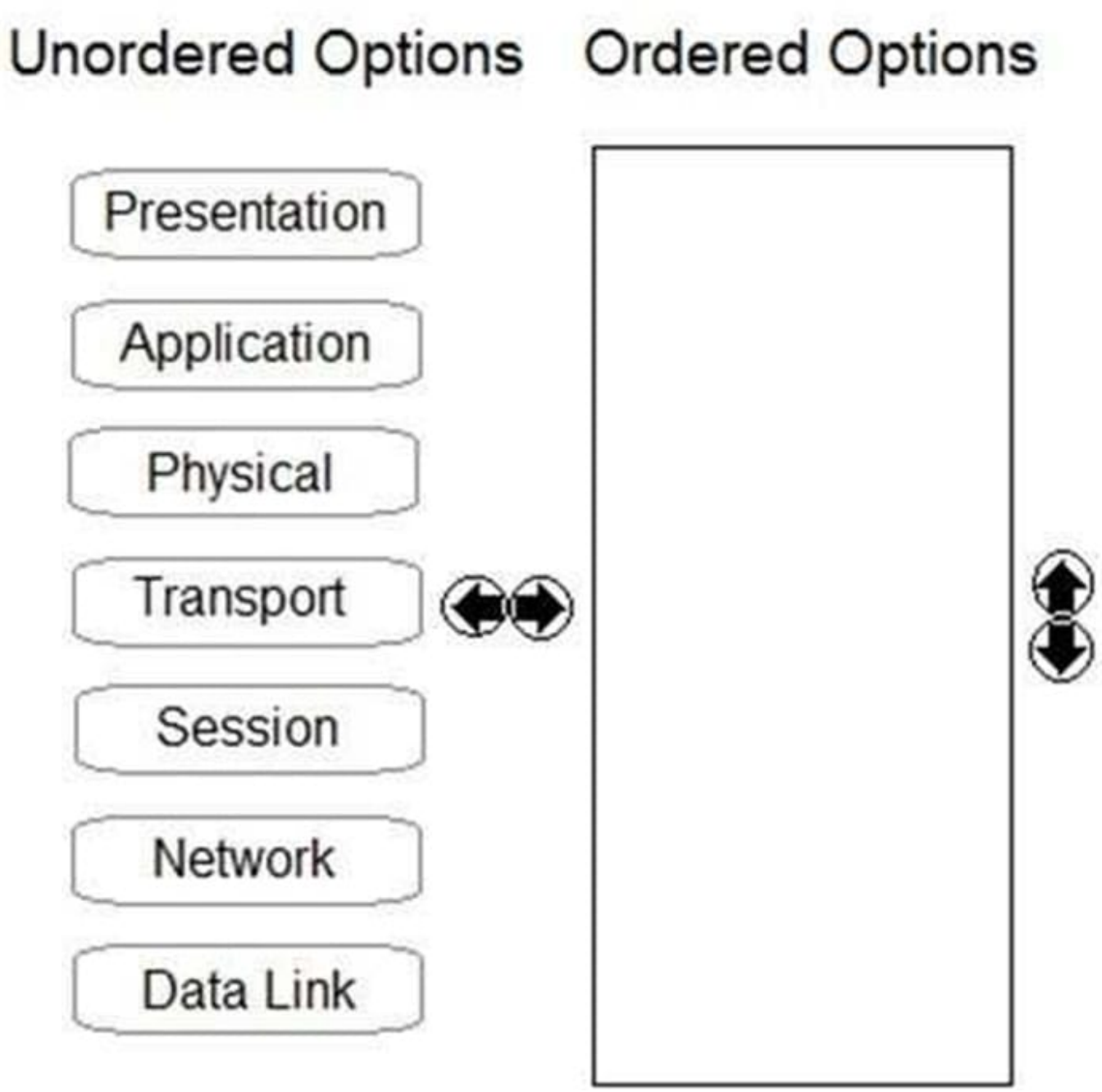
Correct Answer: D

QUESTION 3

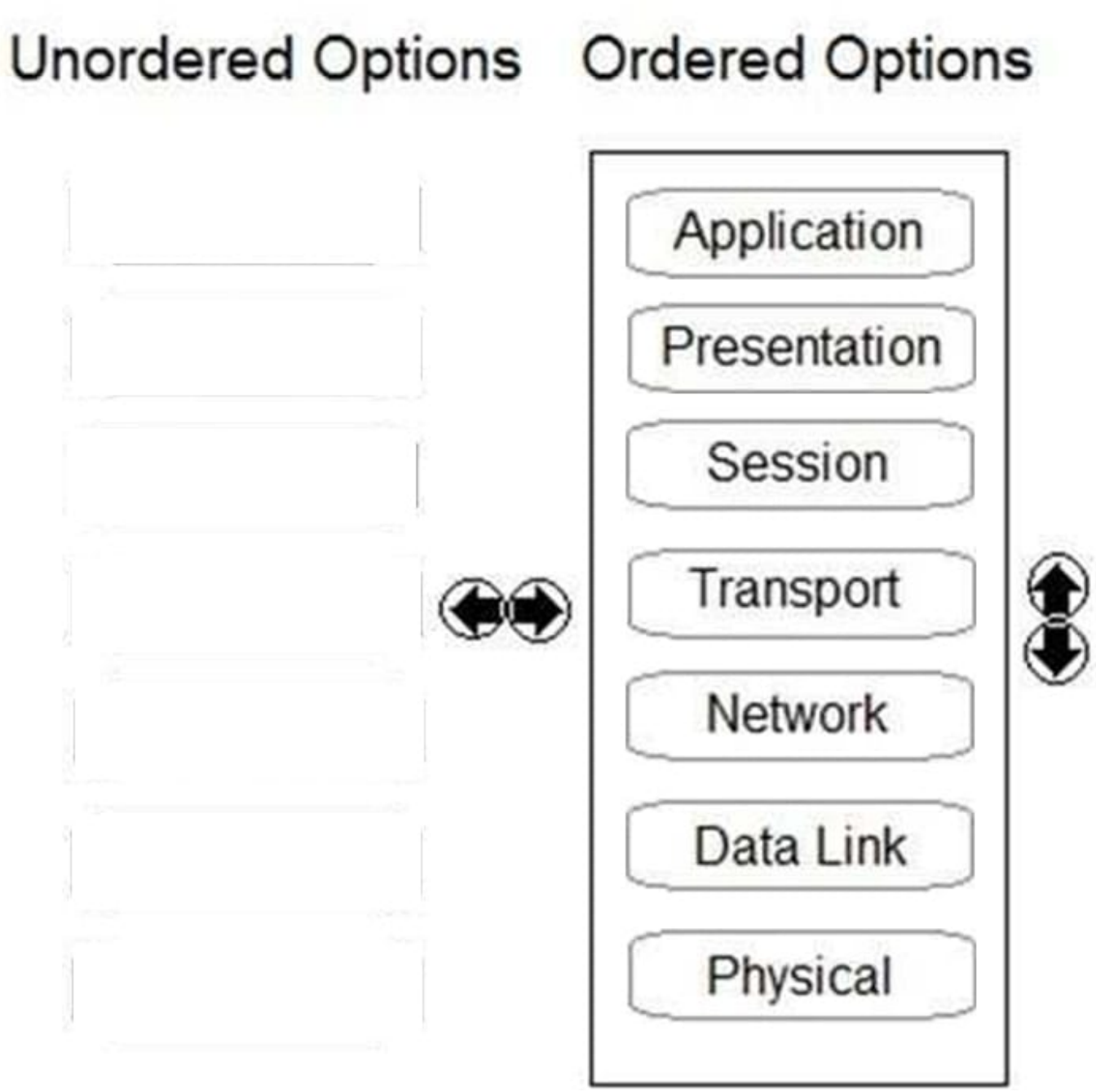
DRAG DROP

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Select and Place:



Correct Answer:



QUESTION 4

Which activities do local organization security policies cover for a SaaS application?

A. how the data is backed up in one or more locations

B. how the application can be used

C. how the application processes the data

D. how the application can transit the Internet

Correct Answer: B

QUESTION 5

In a traditional data center what is one result of sequential traffic analysis?

A. simplifies security policy management

B. reduces network latency

C. causes security policies to be complex

D. improves security policy application ID enforcement

Correct Answer: C

Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying