ITEM CONSTRUCTION FORM

NOTE: Please save this Word document with this name format – aa_bb_FirstLast *(aa is the 2 digit number of the module, bb is the 2 digit number of the unit, and FirstLast is your First Name and Last Name – example: 01_04_JamesGaidry)*

Name: Anna Schorr

_____

E-mail: _____aschorr@cloudsecurityalliance.org

_____

Module #: __3_____ *(Refer to Module Outline)*

Unit #: ____3.2____ *(Refer to Module Outline)*

Testing Concept: (One sentence describing what is being tested)

concept understanding

_____

Stem:

Because SDP architectures completely hide an organization's infrastructure from the internet, malicious actors can't attack what they cannot discover or see. The three main technologies that enable the hiding of architecture in an SDP are:

Options:

A. (Always make A the correct answer)
_____
1. Default drop-all firewall
2. Single packet authorization (SPA)
3. Separate data and control plane
4. Port Knocking

_____

Key:

A

Justification:

A. (Why is A the correct answer)

_____

Default drop-all firewall enables hiding of infrastructure in SDP architecture

SDP-mandates that protected resources are completely hidden from requesting entities and made visible only after they have been authenticated and authorized. Chiefly, SDP accomplishes this by limiting entities to required applications, applying granular access controls at the element level, and employing policy-driven authorization to expand or restrict an entity's privileges.

_____

B. (Why is B the correct answer)

_____

Single packet authorization (SPA) enables hiding of infrastructure in SDP architecture

C. (Why is C the correct answer)

_____

Separate data and control plane enables hiding of infrastructure in SDP architecture

D. (Why is D the incorrect answer)

_____

In the past, infrastructure hiding has partially been achieved through port knocking. It doesn't enable hiding of infrastructure in SDP architecture

Reference(s): (*Provide references to enable independent review. Include the publication title, publication year, author and page.)*

_____This question is directly from Module 3, 3.2 The Principles of Least Privilege and Need To Know

_____