- **Vendor: CompTIA**
- **Exam Code: SY0-501**
- **Exam Name: CompTIA Security+ Certification Exam**
- **New Updated Questions from Braindump2go (Updated in July/2020)**

QUESTION 1214
A local coffee shop runs a small WiFi hotspot for its customers that utilizes WPA2-PSK. The coffee shop would like to stay current with security trends and wants to implement WPA3 to make its WiFi even more secure. Which of the following technologies should the coffee shop use in place of PSK?

A. WEP
B. EAP
C. WPS
D. SAE

Answer: D

QUESTION 1215
An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.
B. It provides insurance in case of a data breach.
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance.
E. It assures customers that the organization meets security standards.

Answer: E

QUESTION 1216
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?

A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules.
C. Emulate the malware in a heavily monitored DMZ segment.
D. Apply network blacklisting rules for the adversary domain.

Answer: BA

QUESTION 1217
An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one

implementing the changes. Which of the following is this an example of?

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

Answer: C

QUESTION 1218
An organization just experienced a major cyberattack incident. The attack was well coordinated, sophisticated, and highly skilled. Which of the following targeted the organization?

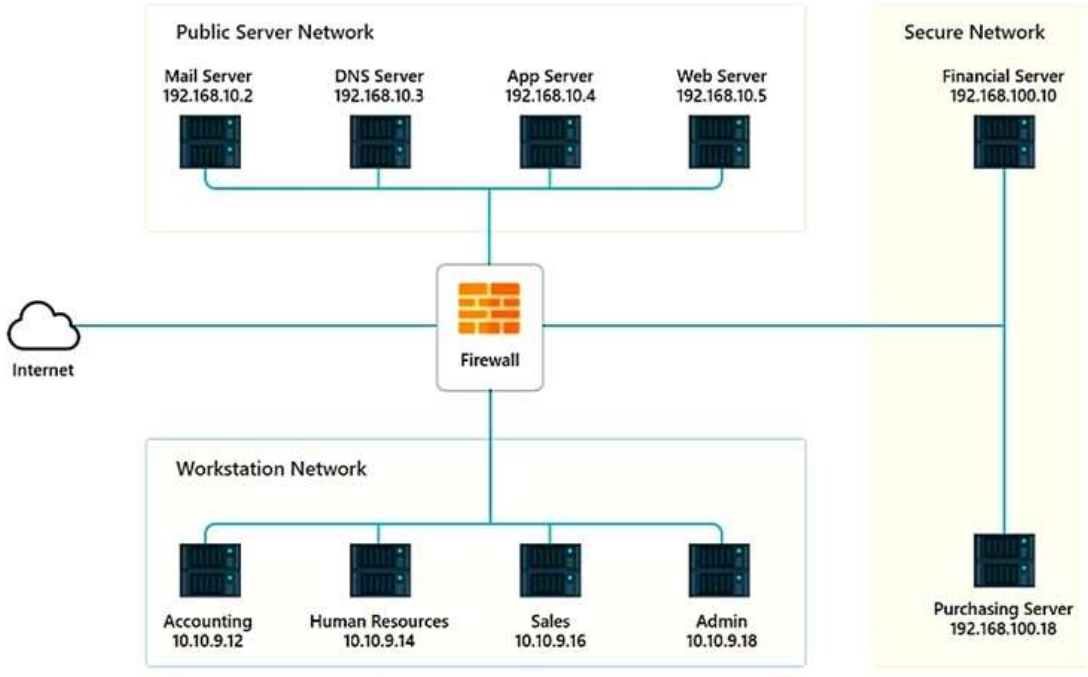
A. Shadow IT
B. An insider threat
C. A hacktivist
D. An advanced persistent threat

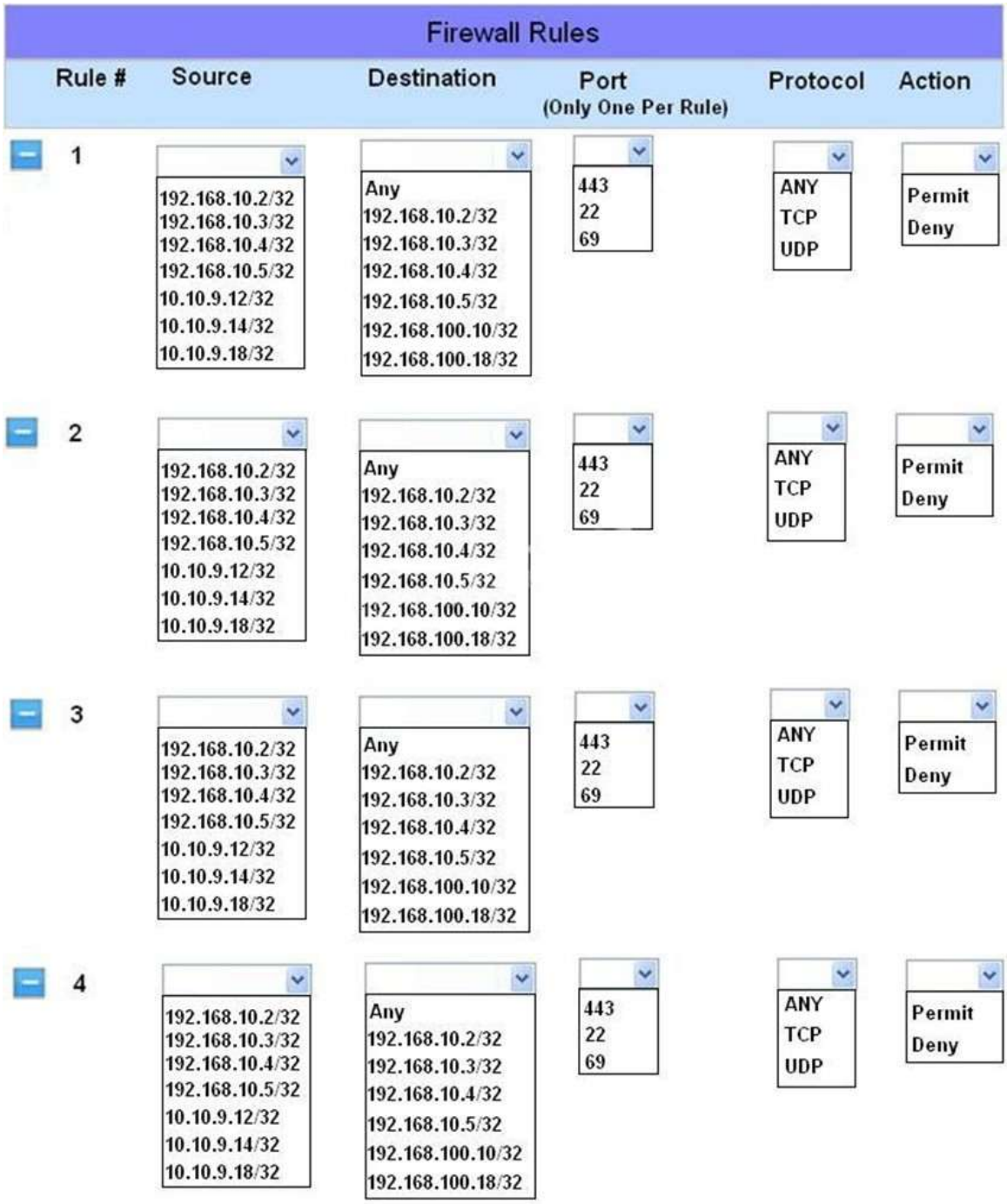
Answer: D

QUESTION 1219
Hotspot Question
The security administration has installed a new firewall which implements an implicit DENY policy by default.
INSTRUCTIONS
Click on the firewall and configure it to allow ONLY the following communication:
- The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
- The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port.
- The Admin workstation should ONLY be able to access the server on the secure network over the default TFTP port.

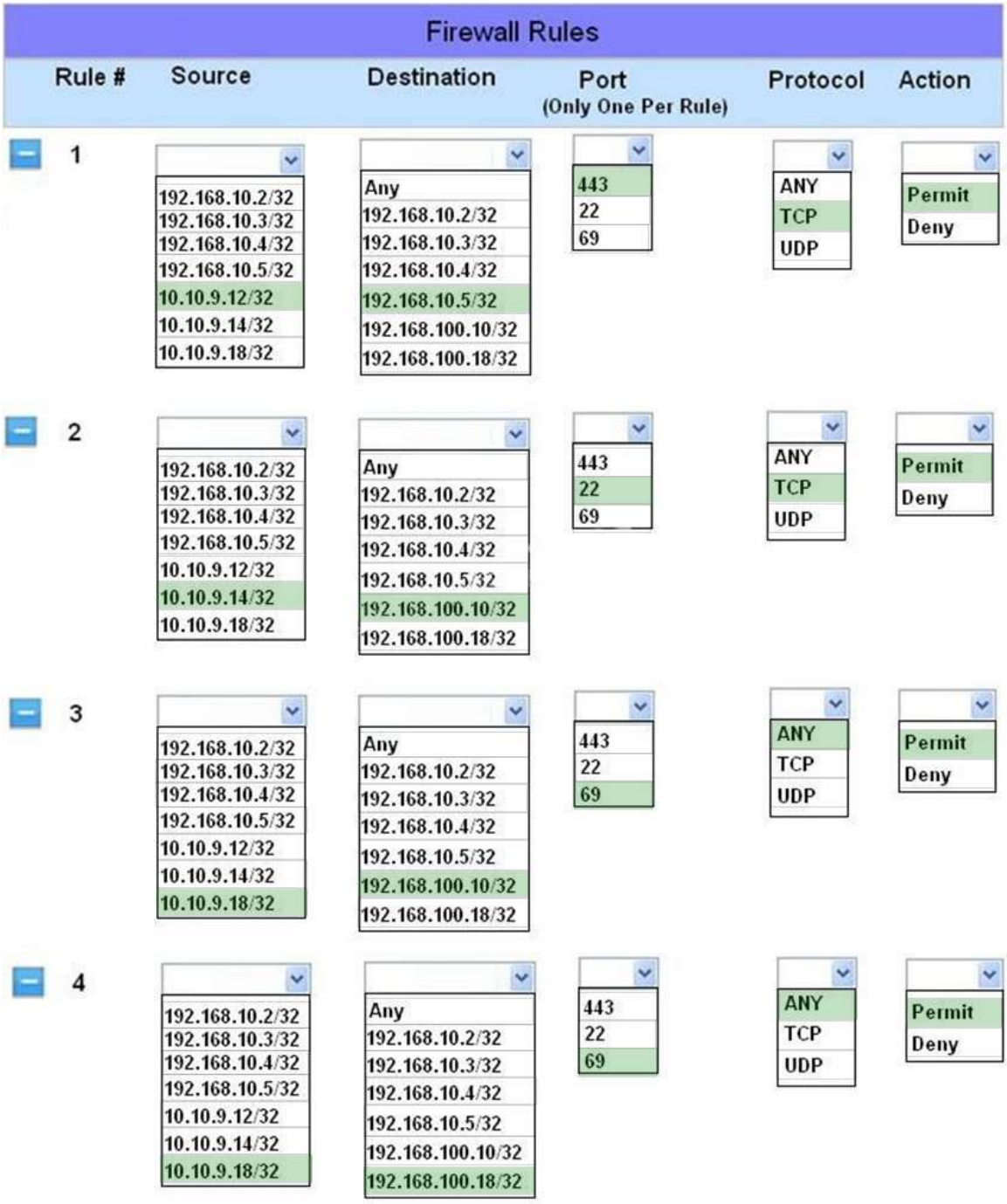
The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram




Firewall Rules
Rule #
Source
Destination
Port
(Only One Per Rule)
Protocol
Action
1
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
2
3
4

Answer:


Firewall Rules
Rule #
Source
Destination
Port
(Only One Per Rule)
Protocol
Action
1
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
2
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
3
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny
4
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
10.10.9.12/32
10.10.9.14/32
10.10.9.18/32
Any
192.168.10.2/32
192.168.10.3/32
192.168.10.4/32
192.168.10.5/32
192.168.100.10/32
192.168.100.18/32
443
22
69
ANY
TCP
UDP
Permit
Deny