PCNSA.38q

Number: PCNSA
Passing Score: 800
Time Limit: 120 min

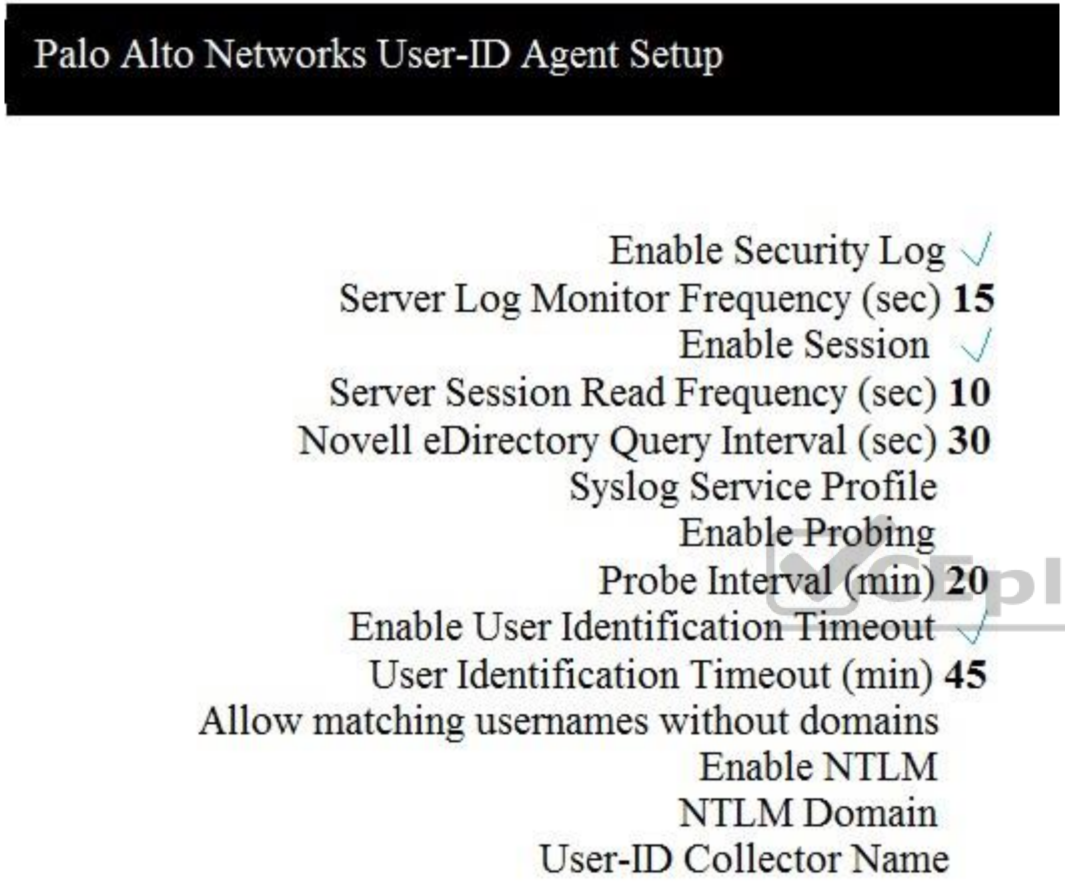
PCNSA

Palo Alto Networks Certified Network Security Administrator

Exam A

QUESTION 1

Which two configuration settings shown are not the default? (Choose two.)



Palo Alto Networks User-ID Agent Setup

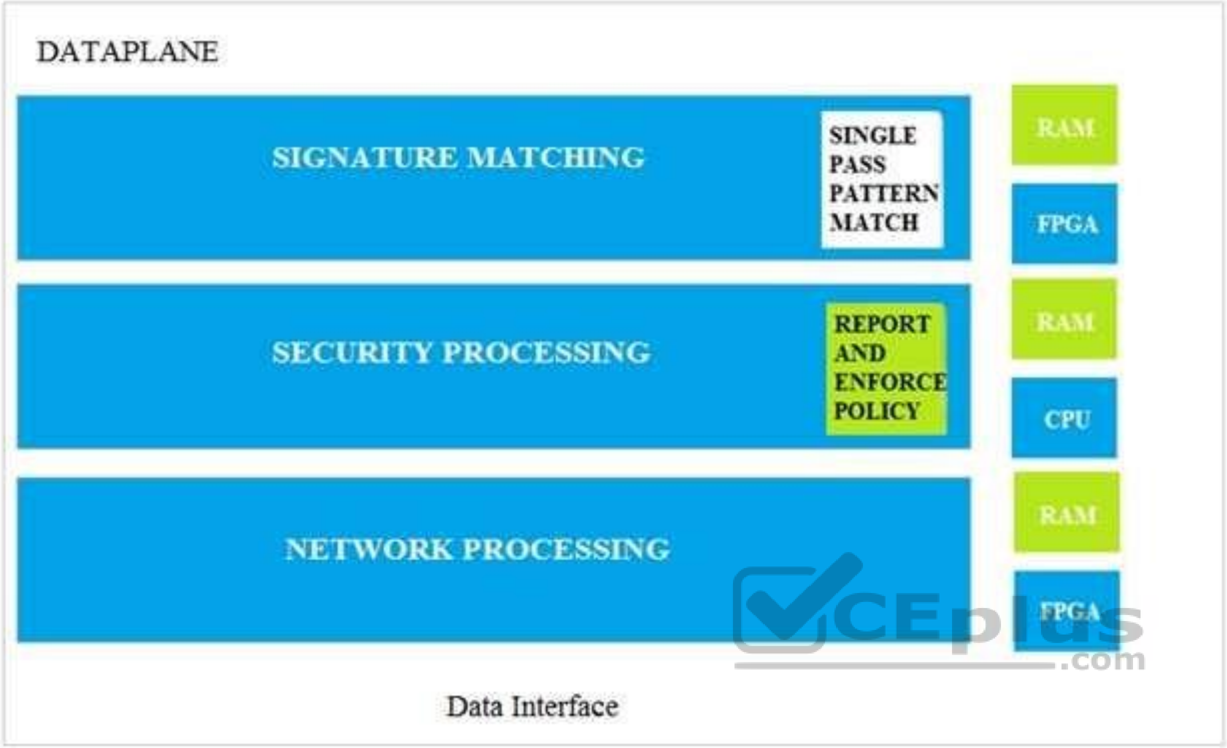
Enable Security Log	✓
Server Log Monitor Frequency (sec)	**15**
Enable Session	✓
Server Session Read Frequency (sec)	**10**
Novell eDirectory Query Interval (sec)	**30**
Syslog Service Profile	
Enable Probing	
Probe Interval (min)	**20**
Enable User Identification Timeout	✓
User Identification Timeout (min)	**45**
Allow matching usernames without domains	
Enable NTLM	
NTLM Domain	
User-ID Collector Name	

A. Enable Security Log
B. Server Log Monitor Frequency (sec)
C. Enable Session
D. Enable Probing

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/enable-servermonitoring

QUESTION 2
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching
B. Network Processing
C. Security Processing
D. Security Matching

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which option shows the attributes that are selectable when setting up application filters?

A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters

QUESTION 4
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List
B. Custom URL Categories
C. PAN-DB URL Categories
D. Allow List

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

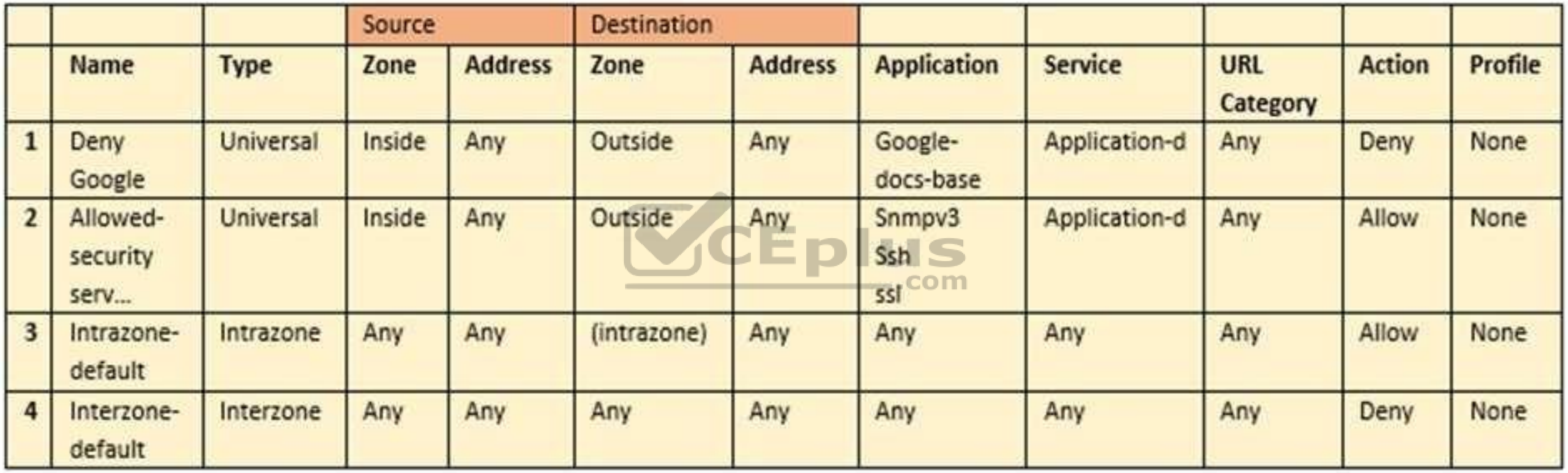
QUESTION 5
Which statement is true regarding a Best Practice Assessment?

A. The BPA tool can be run only on firewalls
B. It provides a percentage of adoption for each assessment area
C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networksassessment-and-review-tools

QUESTION 6
Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?



			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. intrazone-default
B. Deny Google
C. allowed-security services
D. interzone-default

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which interface does **not** require a MAC or IP address?

A. Virtual Wire
B. Layer3
C. Layer2
D. Loopback

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified
B. Rule Usage Filter >Hit Count > Unused in 30 days
C. Rule Usage Filter > Unused Apps
D. Rule Usage Filter > Hit Count > Unused in 90 days

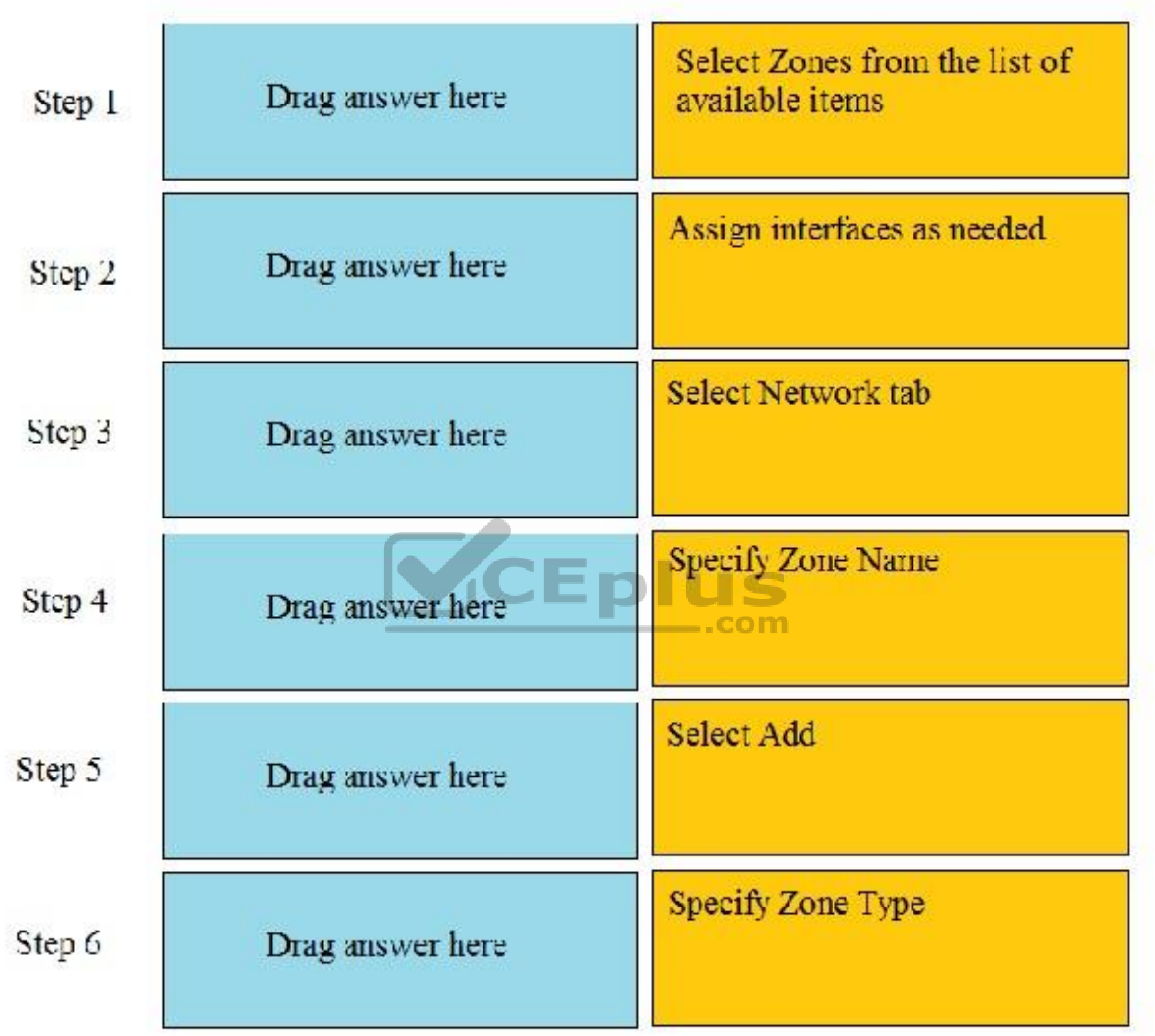
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
DRAG DROP

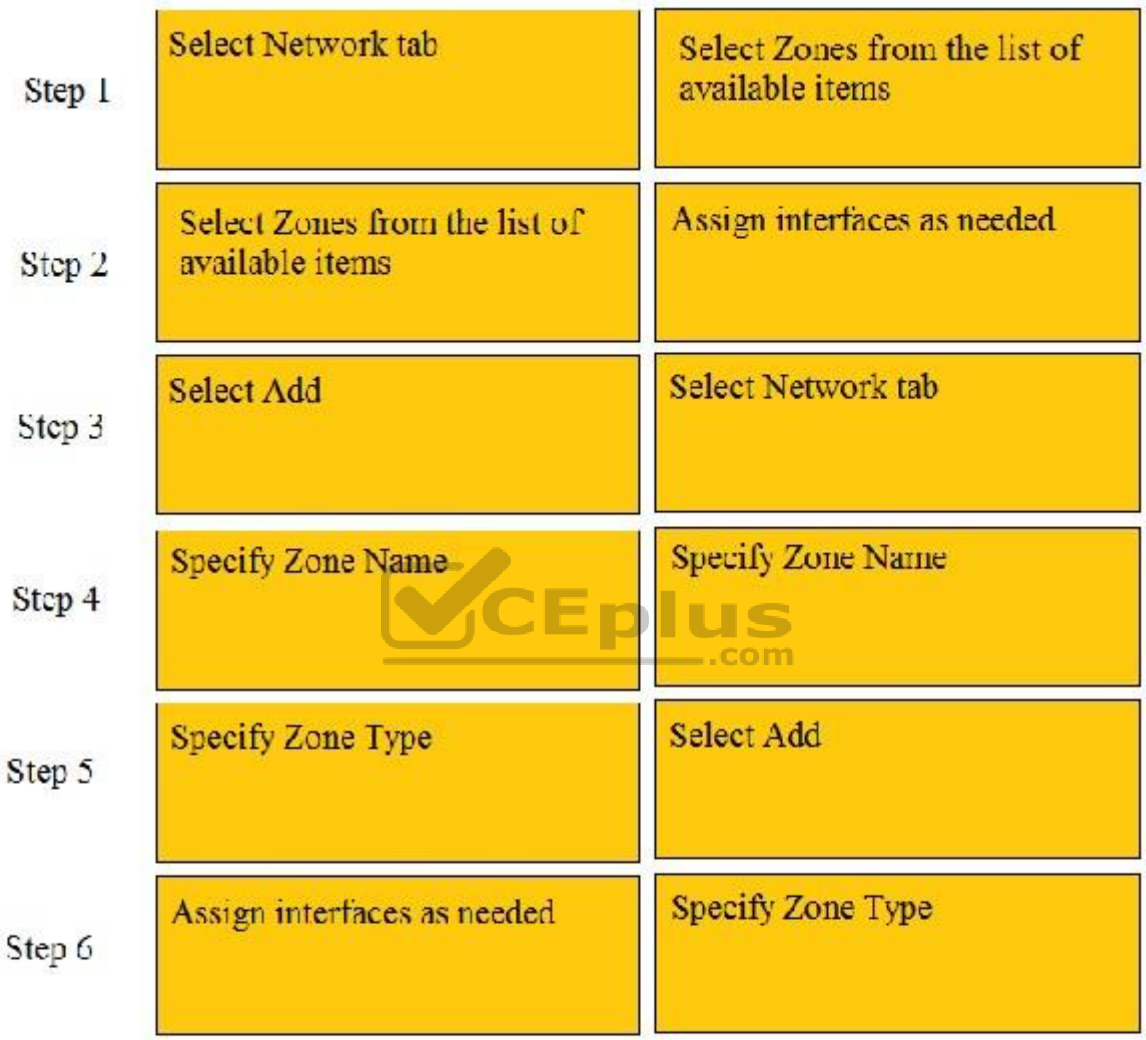
Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Select and Place:



Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

Correct Answer:



Step 1	Select Network tab	Select Zones from the list of available items
Step 2	Select Zones from the list of available items	Assign interfaces as needed
Step 3	Select Add	Select Network tab
Step 4	Specify Zone Name	Specify Zone Name
Step 5	Specify Zone Type	Select Add
Step 6	Assign interfaces as needed	Specify Zone Type

Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

A. An implicit dependency does not require the dependent application to be added in the security policy
B. An implicit dependency requires the dependent application to be added in the security policy
C. An explicit dependency does not require the dependent application to be added in the security policy
D. An explicit dependency requires the dependent application to be added in the security policy

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.
What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. At the CLI enter the command reset rules and press Enter
B. Highlight a rule and use the **Reset Rule Hit Counter > Selected Rules** for each rule
C. Reboot the firewall
D. Use the **Reset Rule Hit Counter > All Rules** option

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/policies/policies-security/creating-and-managing-policies

QUESTION 12

Which two App-ID applications will need to be allowed to use Facebook-chat? (Choose two.)

A. facebook
B. facebook-chat
C. facebook-base

D. facebook-email

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV0CAK

QUESTION 13
In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

A. Weaponization
B. Reconnaissance
C. Installation
D. Command and Control
E. Exploitation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Identify the correct order to configure the PAN-OS integrated USER-ID agent.

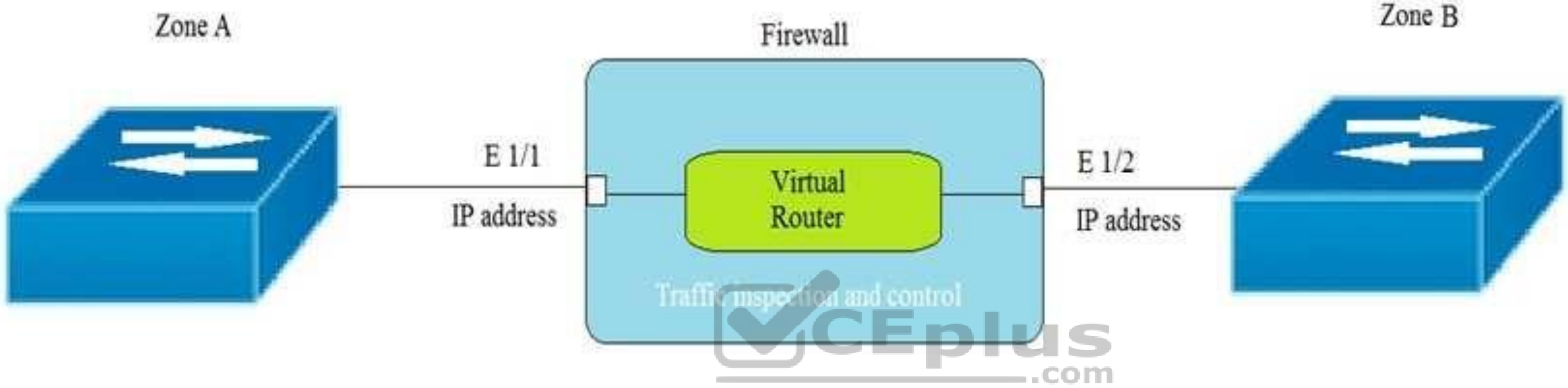
3. add the service account to monitor the server(s)
2. define the address of the servers to be monitored on the firewall
4. commit the configuration, and verify agent connection status
1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

A. 2-3-4-1
B. 1-4-3-2
C. 3-1-2-4
D. 1-3-2-4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Given the topology, which zone type should zone A and zone B to be configured with?



A. Layer3
B. Tap
C. Layer2
D. Virtual Wire

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

A. domain controller
B. TACACS+
C. LDAP
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Layer 2
B. Tap
C. Layer 3
D. Virtual Wire

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18

Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

A. Root
B. Dynamic
C. Role-based
D. Superuser

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser
B. Role-based
C. Dynamic
D. Device administrator

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-cli-quick-start/get-started-with-the-cli/give-administrators-access-to-the-cli/administrativeprivileges?PageSpeed=noscript

QUESTION 20

The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.

Which security profile feature could have been used to prevent the communication with the CnC server?

A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-security-profiles-anti-spyware-profile

QUESTION 21
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

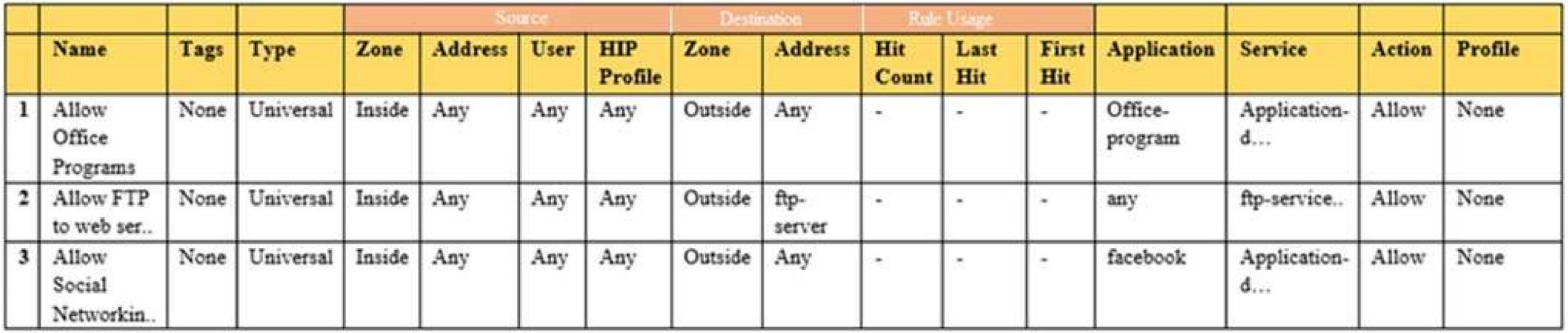
A. Active Directory monitoring
B. Windows session monitoring
C. Windows client probing
D. domain controller monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
What are three differences between security policies and security profiles? (Choose three.)

A. Security policies are attached to security profiles
B. Security profiles are attached to security policies
C. Security profiles should only be used on allowed traffic
D. Security profiles are used to block traffic by themselves
E. Security policies can block or allow traffic



				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23

Given the image, which two options are true about the Security policy rules. (Choose two.)

A. The Allow Office Programs rule is using an Application Filter
B. In the Allow FTP to web server rule, FTP is allowed using App-ID
C. The Allow Office Programs rule is using an Application Group
D. In the Allow Social Networking rule, allows all of Facebook’s functions

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

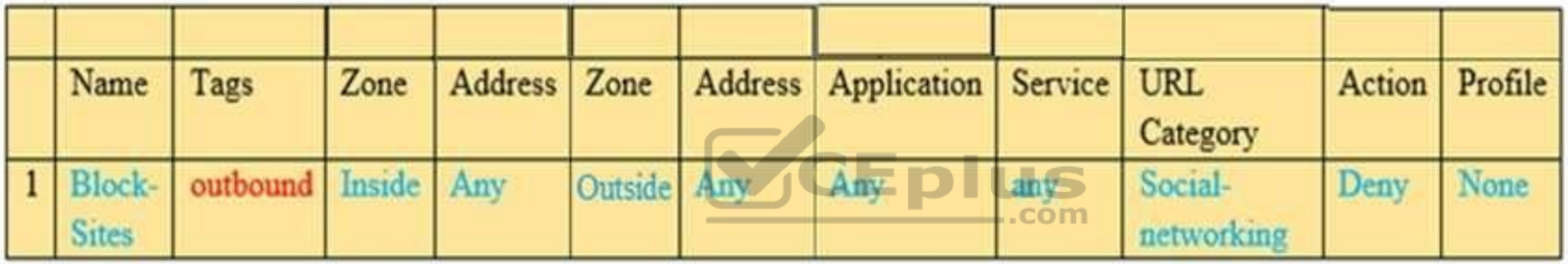
QUESTION 24

Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

A. global
B. intrazone
C. interzone
D. universal

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

QUESTION 25
In the example security policy shown, which two websites would be blocked? (Choose two.)



	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

A. LinkedIn
B. Facebook
C. YouTube
D. Amazon

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26

Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

A. GlobalProtect
B. Panorama
C. Aperture
D. AutoFocus

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which statement is true regarding a Prevention Posture Assessment?

A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networksassessment-and-review-tools

QUESTION 28
The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn’t want to unblock the gambling URL category.
Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.

B. Manually remove powerball.com from the gambling URL category.
C. Add *.powerball.com to the allow list
D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 29
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Panorama
D. GlobalProtect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.
Which security profile components will detect and prevent this threat after the firewall`s signature database has been updated?

A. antivirus profile applied to outbound security policies
B. data filtering profile applied to inbound security policies
C. data filtering profile applied to outbound security policies
D. vulnerability profile applied to inbound security policies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

Which update option is **not** available to administrators?

A. New Spyware Notifications
B. New URLs
C. New Application Signatures
D. New Malicious Domains E. New Antivirus Signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be created. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source-IP-address to any destination-Ip-address
D. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which interface type can use virtual routers and routing protocols?

A. Tap
B. Layer3
C. Virtual Wire
D. Layer2

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Which URL profiling action does not generate a log entry when a user attempts to access that URL?

A. Override
B. Allow
C. Block
D. Continue

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

QUESTION 35
An internal host wants to connect to servers of the internet through using source NAT.
Which policy is required to enable source NAT on the firewall?

A. NAT policy with source zone and destination zone specified
B. post-NAT policy with external source and any destination address
C. NAT policy with no source of destination zone selected

D. pre-NAT policy with external source and any destination address

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet`s source and destination IP address?

A. DoS protection
B. URL filtering
C. packet bufferingD. anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

A. Layer-ID
B. User-ID
C. QoS-ID
D. App-ID

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.firewall.cx/networking-topics/firewalls/palo-alto-firewalls/1152-palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html

QUESTION 38

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

A. **Device>Setup>Services**

B. **Device>Setup>Management**

C. **Device>Setup>Operations**

D. **Device>Setup>Interfaces**

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: