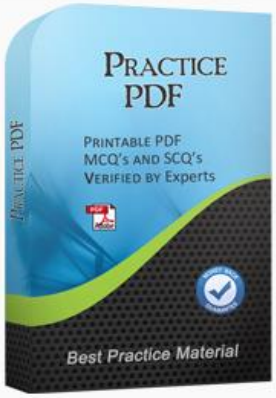
Actual4Cert

Actual4Cert

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

http://www.actual4cert.com/

We are a test cert center to provide the best and valid study material for all of you, and aim to help you pass.

Exam : **PCNSA**

Title : Palo Alto Networks Certified Network Security Administrator

Vendor : Palo Alto Networks

Version : DEMO

NO.1 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
Answer: B

NO.2 The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?
A. Add zones attached to interfaces to the virtual router
B. Add interfaces to the virtual router
C. Enable the redistribution profile to redistribute connected routes
D. Add a static routes to route between the two interfaces
Answer: D

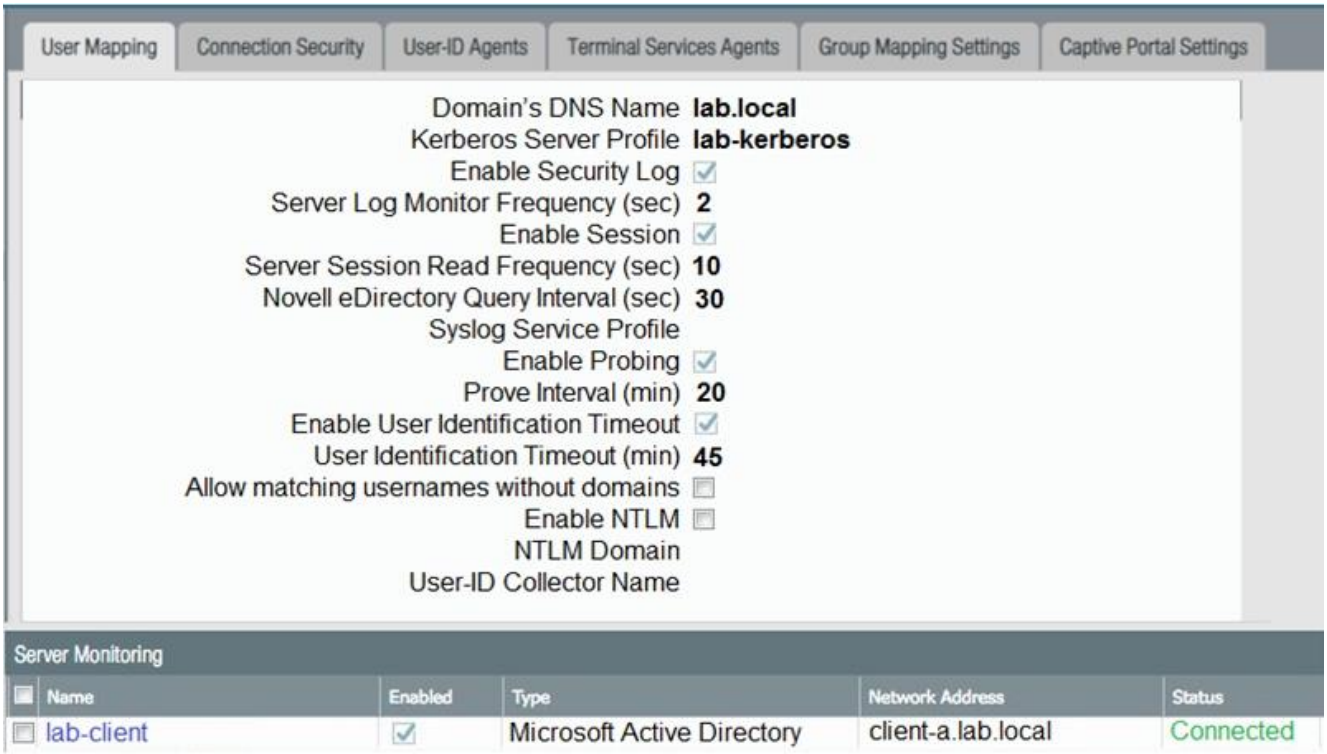
NO.3 Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?
A. block
B. sinkhole
C. alert
D. allow
Answer: B
Explanation:
To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security

NO.4 What must be configured before setting up Credential Phishing Prevention?
A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID
Answer: B
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up

NO.5 Which order of steps is the correct way to create a static route?
A. 1) Enter the route and netmask
2) Enter the IP address for the specific next hop

3) Specify the outgoing interface for packets to use to go to the next hop
4) Add an IPv4 or IPv6 route by name
B. 1) Enter the route and netmask
2) Specify the outgoing interface for packets to use to go to the next hop
3) Enter the IP address for the specific next hop
4) Add an IPv4 or IPv6 route by name
C. 1) Enter the IP address for the specific next hop
2) Enter the route and netmask
3) Add an IPv4 or IPv6 route by name
4) Specify the outgoing interface for packets to use to go to the next hop
D. 1) Enter the IP address for the specific next hop
2) Add an IPv4 or IPv6 route by name
3) Enter the route and netmask
4) Specify the outgoing interface for packets to use to go to the next hop
Answer: A
* Enter the route and netmask
* Enter the IP address for the specific next hop
* Specify the outgoing interface for packets to use to go to the next hop
* Add an IPv4 or IPv6 route by name Comprehensive Explanation: This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or
2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11. References:
* Configure a Static Route - Palo Alto Networks

NO.6 Based on the graphic which statement accurately describes the output shown in the server monitoring panel?



A. The User-ID agent is connected to a domain controller labeled lab-client.
B. The host lab-client has been found by the User-ID agent.
C. The host lab-client has been found by a domain controller.
D. The User-ID agent is connected to the firewall labeled lab-client.
Answer: A

NO.7 Which security profile should be used to classify malicious web content?
A. URL Filtering
B. Antivirus
C. Web Content
D. Vulnerability Protection
Answer: A
Explanation:
URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups. References: URL Filtering, Set Up a Basic Security Policy, Updated Certifications for PAN-OS 10.1

NO.8 Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?
A. URL filtering
B. Antivirus

C. WildFire
D. Threat Prevention
Answer: D

NO.9 What do dynamic user groups you to do?
A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
D. create a dynamic list of firewall administrators
Answer: C
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text

NO.10 Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location.
What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?
A. save named configuration snapshot
B. export device state
C. export named configuration snapshot
D. save candidate config
Answer: C
Explanation:
The Revert, Save, and Load operations all work with firewall co nfigurations local to the firewall. The Export operations transfer configurations as XML-formatted files from the firewall to the host running the web interface browser. From your local machine, you can save the files as configuration backups. The Import operations transfer XML configuration files from the host running the web interface browser to the firewall.
The XML file can be loaded as the candidate configuration or even be committed to becoming the running configuration. [Palo Alto Networks]

NO.11 Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?
A. Inline Cloud Analysis
B. Signature Exceptions
C. Machine Learning Policies
D. Signature Policies
Answer: A
Explanation:
* An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and

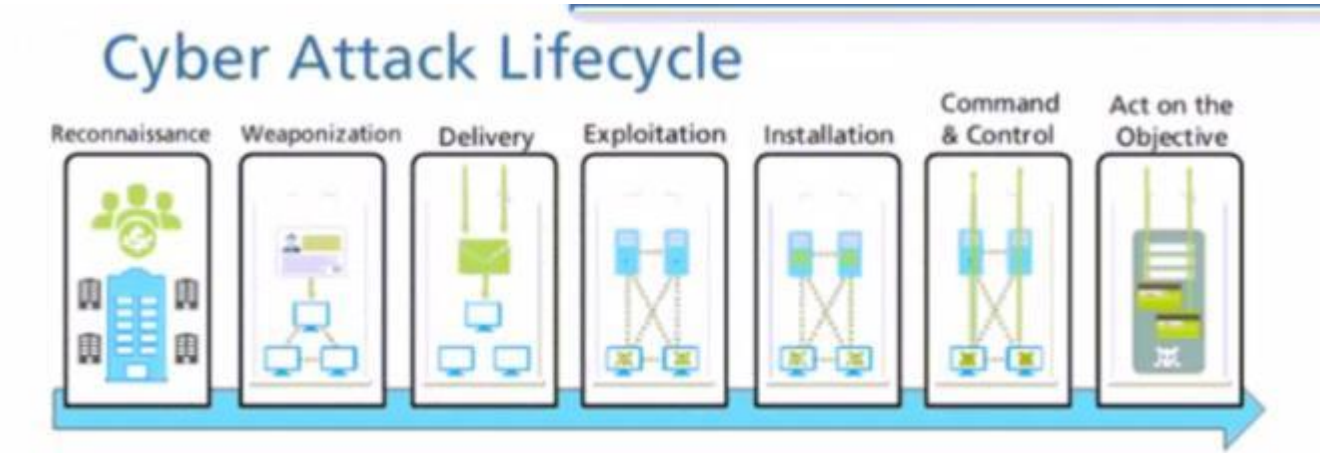
sends it to an external command-and-control (C2) server1.
* An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.
* The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses1.
* The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile1.
* The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis1.
* The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTPS traffic, or IMAP/IMAPS traffic1.
Therefore, the tab that is used to enable machine learning based engines is the Inline Cloud Analysis tab.
References:
1: Security Profile: Anti-Spyware - Palo Alto Networks

NO.12 Which two security profile types can be attached to a security policy? (Choose two.)
A. antivirus
B. DDoS protection
C. threat
D. vulnerability
Answer: A D

NO.13 When creating a custom URL category object, which is a valid type?
A. domain match
B. host names
C. wildcard
D. category match
Answer: D

NO.14 An administrator wants to prevent access to media content websites that are risky Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)
A. streaming-media
B. high-risk
C. recreation-and-hobbies
D. known-risk
Answer: A C

NO.15 At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



A. delivery
B. command and control
C. explotation
D. reinsurance
E. installation
Answer: A

NO.16 How often does WildFire release dynamic updates?
A. every 5 minutes
B. every 15 minutes
C. every 60 minutes
D. every 30 minutes
Answer: A

NO.17 According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?
A. by minute
B. hourly
C. daily
D. weekly
Answer: C

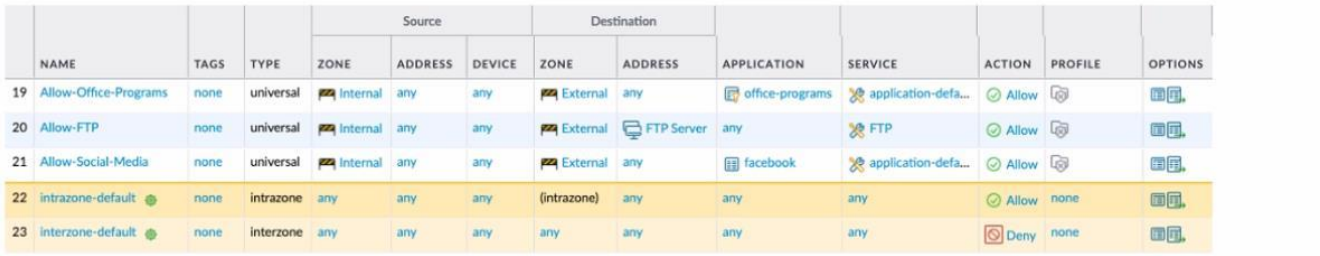
NO.18 Based on the screenshot what is the purpose of the included groups?

			Source			Destination				
	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.
B. They are used to map usernames to group names.
C. They contain only the users you allow to manage the firewall.
D. They are groups that are imported from RADIUS authentication servers.
Answer: B

NO.19 Based on the image provided, which two statements apply to the Security policy rules?

(Choose two.)



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source DEVICE	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

A. The Allow-Office-Programs rule is using an application filter.
B. The Allow-Office-Programs rule is using an application group.
C. The Allow-Social-Media rule allows all Facebook functions.
D. In the Allow-FTP policy, FTP is allowed using App-ID.
Answer: A C

NO.20 Which Security profile can you apply to protect against malware such as worms and Trojans?
A. data filtering
B. antivirus
C. vulnerability protection
D. anti-spyware
Answer: B

NO.21 An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how wilt the firewall handle the traffic?
A. It allows the traffic because the profile was not set to explicitly deny the traffic.
B. It drops the traffic because the profile was not set to explicitly allow the traffic.
C. It uses the default action assigned to the virus signature.
D. It allows the traffic but generates an entry in the Threat logs.
Answer: B

NO.22 An administrator would like to determine the default deny action for the application dns-over-https Which action would yield the information?
A. View the application details in beacon paloaltonetworks.com
B. Check the action for the Security policy matching that traffic
C. Check the action for the decoder in the antivirus profile
D. View the application details in Objects > Applications
Answer: D

NO.23 All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone.
Complete the empty field in the Security policy using an application object to permit only this type of access.
Source Zone: Internal -
Destination Zone: DMZ Zone -

Application: _____
Service: application-default -
Action: allow
A. Application = "any"
B. Application = "web-browsing"
C. Application = "ssl"
D. Application = "http"
Answer: B

NO.24 When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP port is used for management access?
A. 80
B. 8443
C. 4443
D. 443
Answer: C

NO.25 Which action results in the firewall blocking network traffic with out notifying the sender?
A. Drop
B. Deny
C. Reset Server
D. Reset Client
Answer: B

NO.26 What are the two main reasons a custom application is created? (Choose two.)
A. To correctly identify an internal application in the traffic log
B. To change the default categorization of an application
C. To visually group similar applications
D. To reduce unidentified traffic on a network
Answer: A D
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-c

NO.27 What are three ways application characteristics are used? (Choose three.)
A. As an attribute to define an application group
B. As a setting to define a new custom application
C. As an Object to define Security policies
D. As an attribute to define an application filter
E. As a global filter in the Application Command Center (ACC)
Answer: A B D

NO.28 Assume that traffic matches a Security policy rule but the attached Security Profiles is

configured to block matching traffic Which statement accurately describes how the firewall will apply an action to matching traffic?

A. If it is an allowed rule, then the Security Profile action is applied last

B. If it is a block rule then the Security policy rule action is applied last

C. If it is an allow rule then the Security policy rule is applied last

D. If it is a block rule then Security Profile action is applied last

Answer: A

NO.29 An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

A. Disable all logging

B. Enable Log at Session End

C. Enable Log at Session Start

D. Enable Log at both Session Start and End

Answer: B

NO.30 Which feature must be configured to enable a data plane interface to submit DNS queries originated from the firewall on behalf of the control plane?

A. Service route

B. Admin role profile

C. DNS proxy

D. Virtual router

Answer: A

Explanation:

By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Netw orks services such as soft ware, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to th e service on a server is aservice route.

[Palo Alto Networks]

PAN-OS 10 -> Device -> Setup -> Services -> Service Features -> Service Route Configuration

NO.31 What are three configurable interface types for a data-plane ethernet interface? (Choose three.)

A. Layer 3

B. HSCI

C. VWire

D. Layer 2

E. Management

Answer: A C D

Explanation:

Three configurable interface types for a data-plane ethernet interface are Layer 3, VWire, and Layer 2. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface1.
VWire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.
Layer 2: A layer 2 interface allows the firewall to act as a switch and forward traffic based on MAC addresses. The firewall can send and receive traffic from a layer 2 interface and apply security policies and inspect the traffic based on the source and destination zones of the interface3.
References: Ethernet Interface Types, Virtual Wire Interfaces, Layer 2 Interfaces, Layer 3 Interfaces, [Certifications - Palo Alto Networks], [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NO.32 When is the content inspection performed in the packet flow process?
A. after the application has been identified
B. after the SSL Proxy re-encrypts the packet
C. before the packet forwarding process
D. before session lookup
Answer: A

NO.33 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
Answer: A

NO.34 An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.
Why doesn't the administrator see the traffic?
A. Traffic is being denied on the interzone-default policy.
B. The Log Forwarding profile is not configured on the policy.
C. The interzone-default policy is disabled by default
D. Logging on the interzone-default policy is disabled
Answer: D

NO.35 Which tab would an administrator click to create an address object?
A. Device
B. Policies
C. Monitor
D. Objects

Answer: D