Palo Alto Net.PCNSC.by.Fanto.28q

Number: PCNSC
Passing Score: 800
Time Limit: 120
File Version: 2.0

Exam Code: PCNSC

Exam Name: Palo Alto Networks Certified Network Security Consultant

Exam A

QUESTION 1
Which two types of security profiles are recommended to protect against known and unknown threats? (Choose two)

A. Antivirus
B. URL Filtering
C. Anti-Spyware
D. File Blocking

Correct Answer: A, C
Section:

QUESTION 2
Which of the following Palo Alto Networks features can help reduce the attack surface by limiting the number of applications allowed through the firewall?

A. URL Filtering
B. App-ID
C. User-ID
D. Content-ID

Correct Answer: B
Section:

QUESTION 3
In a multi-tenant environment, what feature allows you to assign different administrators to different tenants?

A. Admin Roles
B. Device Groups
C. Access Domains
D. Virtual Systems

Correct Answer: C
Section:

QUESTION 4
Which two log types are necessary to fully investigate a network intrusion? (Choose two)

A. URL Filtering log
B. Traffic log
C. Threat log
D. System log

Correct Answer: B, C

Section:

QUESTION 5
What configuration is necessary for Active/Active HA to synchronize sessions between peers?

A. Enable session synchronization under the HA settings
B. Use the same virtual IP address on both peers
C. Configure a floating IP address
D. Enable session preemption on both peers

Correct Answer: A
Section:

QUESTION 6
Which Palo Alto Networks feature allows you to create dynamic security policies based on the behavior of the devices in your network?

A. Behavioral Threat Detection
B. Cortex XDR
C. App-ID
D. Dynamic Address Groups

Correct Answer: D
Section:

QUESTION 7
How can you enforce a security policy based on the device type?

A. Use User-ID
B. Use Device-ID
C. Use App-ID
D. Use Content-ID

Correct Answer: B
Section:

QUESTION 8
Which CLI command is used to verify the high availability state of a Palo Alto Networks firewall?

A. show high-availability state
B. show ha state
C. show ha status
D. show high-availability status

Correct Answer: C
Section:

QUESTION 9

In Panorama, what is the correct order of precedence for security policies?

A. Device group pre-rules, shared pre-rules, local rules, device group post-rules, shared post-rules

B. Shared pre-rules, device group pre-rules, local rules, shared post-rules, device group post-rules

C. Shared pre-rules, device group pre-rules, local rules, device group post-rules, shared post-rules

D. Device group pre-rules, shared pre-rules, local rules, shared post-rules, device group post-rules

Correct Answer: C
Section:

QUESTION 10

A firewall that was previously connected lo a User-ID agent server now shows disconnected What is the likely cause?

A. The server has stopped listening on port 2010

B. The Domain Controller service account has been locked out

C. The agent is not running

D. The firewall was upgraded to a PAN-OS version that is not compatible with the agent version

Correct Answer: D
Section:
Explanation:

If a firewall that was previously connected to a User-ID agent server now shows disconnected, the likely cause is:
D . The firewall was upgraded to a PAN-OS version that is not compatible with the agent version
When a firewall is upgraded to a new version of PAN-OS, there can be compatibility issues with the existing User-ID agent if it is not updated accordingly. This can result in the firewall being unable to communicate with the User-ID agent, showing it as disconnected.
Palo Alto Networks - User-ID Agent Compatibility: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-agent

QUESTION 11

A customer's Palo Alto Networks NGFW currently has only one security policy allowing all traffic They have identified that this is a substantial security risk and have heard that the Expedition tool can help them extract security policies from an 'allow any' rule
What should the consultant say about Expedition?

A. Expedition cannot parse log files and therefore cannot be used for this purpose

B. By using the Machine Learning feature Expedition can parse the traffic log files related to the polcy and extract security rules for matching traffic

C. Live firewall traffic can be viewed on Expedition when connected to a firewall, and Expedition can automatically create and push policies to the firewall

D. The log files can be viewed on Expedition, and right-clicking a log entry gives the option to create security policy from the log entry.

Correct Answer: B
Section:
Explanation:

The Expedition tool can help the customer extract security policies from an 'allow any' rule by using its Machine Learning feature:
B . By using the Machine Learning feature, Expedition can parse the traffic log files related to the policy and extract security rules for matching traffic
Expedition can analyze traffic log files and apply machine learning algorithms to suggest security policies that match the observed traffic patterns. This helps in creating a more secure and granular policy set from a broad 'allow any' rule.
Palo Alto Networks - Expedition Documentation: https://live.paloaltonetworks.com/t5/expedition-migration-tool/ct-p/migration_tool
Palo Alto Networks - Using Machine Learning in Expedition: https://live.paloaltonetworks.com/t5/expedition-articles/expedition-machine-learning-overview/ta-p/260401

QUESTION 12

In an environment using User-ID, what role does the User-ID agent play?

A. It assigns IP addresses to users

B. It maps user identities to IP addresses

C. It inspects traffic for malicious content

D. It enforces security policies based on IP addresses

Correct Answer: B
Section:

QUESTION 13
What is the purpose of the WildFire Analysis Profile in a security policy?

A. To specify which files are sent to WildFire for analysis

B. To configure the WildFire subscription settings

C. To enable WildFire to analyze all network traffic

D. To define the action to be taken on files analyzed by WildFire

Correct Answer: A
Section:

QUESTION 14
A customer has deployed a GlobalProtect portal and gateway as its remote-access VPN solution for its fleet of Windows 10 laptops
The customer wants to use Host information Profile (HIP) data collected at the GlobalProtect gateway throughout its enterprise as an additional means of policy enforcement
What additional licensing must the customer purchase?

A. DNS Security on the perimeter firewall

B. GlobalProtect license for each firewall that will use HIP data to enforce policy

C. WildFire license

D. GlobalProtect license for the gateway firewall

Correct Answer: B
Section:
Explanation:
To utilize Host Information Profile (HIP) data collected at the GlobalProtect gateway for policy enforcement throughout the enterprise, the customer needs to purchase a GlobalProtect license for each firewall that will use HIP data to enforce policy. The GlobalProtect license enables the firewall to collect and use HIP data to create policies based on the security posture of the endpoints.
Palo Alto Networks - GlobalProtect Licensing: https://docs.paloaltonetworks.com/globalprotect/10-0/globalprotect-admin/globalprotect-licenses

QUESTION 15
Your customer has asked you to set up tunnel monitoring on an IPsec VPN tunnel between two offices What three steps are needed to set up tunnel monitoring? (Choose three)

A. Create a monitoring profile

B. Add an IP address to each tunnel interface

C. Restart each IPsec tunnel

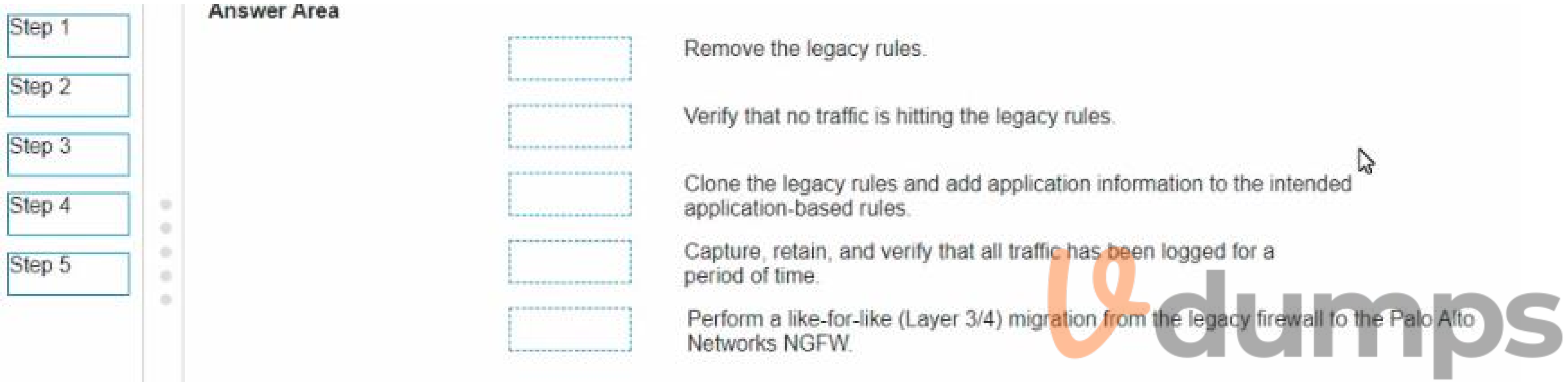
D. Restart each IKE gateway

E. Enable tunnel monitoring on each IPsec tunnel

Correct Answer: A, B, E
Section:
Explanation:
To set up tunnel monitoring on an IPsec VPN tunnel between two offices, the following steps are needed:
A . Create a monitoring profile: This profile defines the criteria for monitoring, such as the IP address to ping and the failure condition.
B . Add an IP address to each tunnel interface: Tunnel monitoring requires an IP address on each tunnel interface to send and receive monitoring pings.
E . Enable tunnel monitoring on each IPsec tunnel: This step activates the monitoring profile on the IPsec tunnel, ensuring that the tunnel is actively monitored and can trigger alerts or failover mechanisms if the tunnel goes down.
These steps ensure that the tunnel is properly monitored, allowing for proactive detection and response to connectivity issues.
Palo Alto Networks - Configuring IPsec Tunnel Monitoring: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/vpns/site-to-site-vpn/configure-ipsec-tunnel-monitoring

QUESTION 16
DRAG DROP
Match the App-ID adoption task with its order in the process.

Select and Place:

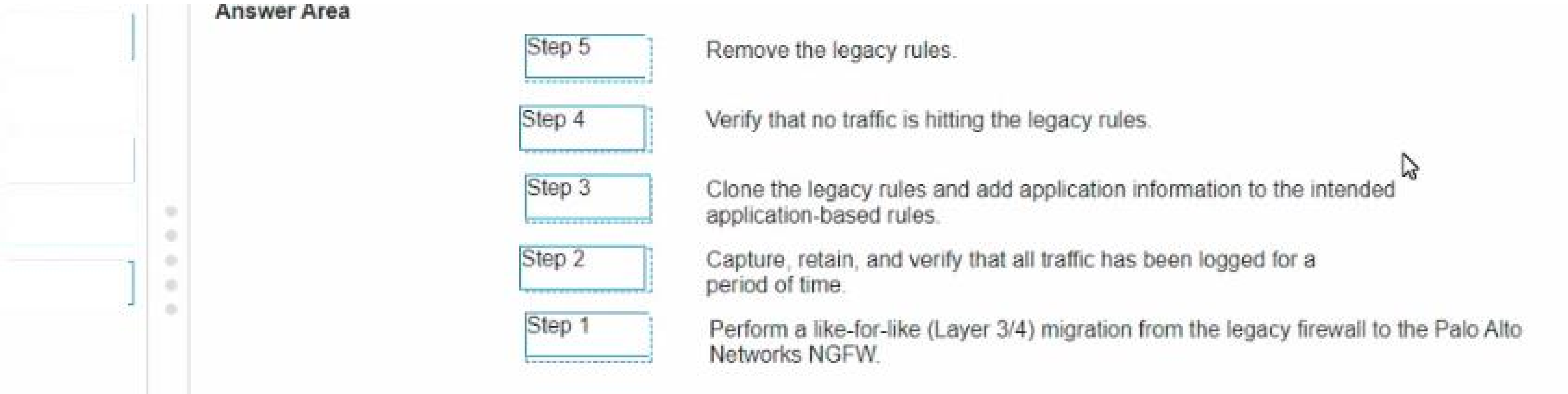


Step 1
Step 2
Step 3
Step 4
Step 5

Answer Area

Remove the legacy rules.
Verify that no traffic is hitting the legacy rules.
Clone the legacy rules and add application information to the intended application-based rules.
Capture, retain, and verify that all traffic has been logged for a period of time.
Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.

Correct Answer:



Answer Area

Step 5 Remove the legacy rules.
Step 4 Verify that no traffic is hitting the legacy rules.
Step 3 Clone the legacy rules and add application information to the intended application-based rules.
Step 2 Capture, retain, and verify that all traffic has been logged for a period of time.
Step 1 Perform a like-for-like (Layer 3/4) migration from the legacy firewall to the Palo Alto Networks NGFW.

Section:
Explanation:
Palo Alto Networks - App-ID Best Practices: https://docs.paloaltonetworks.com/best-practices
Palo Alto Networks - Migration from Legacy Firewalls: https://docs.paloaltonetworks.com/migration

QUESTION 17
In preparation for a cutover event, what two processes or procedures should be verified? (Choose two)

A. auditing
B. change management requirements

C. roles and responsibilities

D. logging and reporting

Correct Answer: B, C
Section:
Explanation:
For any cutover event, especially when dealing with network security infrastructure like Palo Alto Networks firewalls, it is critical to ensure that:
Change Management Requirements (B): This involves verifying that all planned changes have been approved, documented, and communicated to all relevant stakeholders. The change management process ensures that any modifications are controlled, predictable, and include a rollback plan in case of issues.
Reference: Palo Alto Networks Best Practices for Change Management Documentation.
Roles and Responsibilities (C): Clearly defined roles and responsibilities ensure that everyone involved knows their specific tasks during the cutover. This reduces confusion, ensures accountability, and helps in the smooth execution of the cutover plan. It includes defining who is responsible for specific tasks, who needs to be notified, and who has the authority to make decisions. Reference: Palo Alto Networks Operational Best Practices Documentation.

QUESTION 18
What is the default port used by the Terminal Services agent to communicate with a firewall?

A. 5007

B. 5009

C. 443

D. 636

Correct Answer: A
Section:
Explanation:
The default port used by the Terminal Services agent to communicate with a Palo Alto Networks firewall is 5007. The Terminal Services agent (TS agent) integrates with Microsoft Terminal Services to associate user information with sessions, enabling User-ID to accurately map user identities to security policies.
Reference: Palo Alto Networks Terminal Services Agent Documentation.

QUESTION 19
What command can you use to check the status of GlobalProtect clients connected to the firewall?

A. show globalprotect status

B. show globalprotect gateway

C. show globalprotect current-user

D. show globalprotect statistics

Correct Answer: B
Section:

QUESTION 20
Which feature allows you to use multiple links simultaneously to balance the load in a Palo Alto Networks firewall?

A. High Availability

B. Aggregate Ethernet

C. Virtual Wire

D. ECMP (Equal-Cost Multi-Path)

Correct Answer: D
Section:

QUESTION 21
Which two conditions must be met for a firewall to successfully forward traffic to a syslog server? (Choose two)

A. The syslog server must be defined in the Device > Server Profiles > Syslog section
B. A syslog forwarding profile must be created and applied to the appropriate security policies
C. The firewall must be in Virtual Wire mode
D. The syslog server must be reachable over a secure connection

Correct Answer: A, B
Section:

QUESTION 22
What type of NAT rule is required to translate an internal server's private IP address to a public IP address for external access?

A. Source NAT
B. Destination NAT
C. Dynamic NAT
D. Bidirectional NAT

Correct Answer: B
Section:

QUESTION 23
Which Panorama operational mode is necessary to manage a large number of firewalls and also act as a log collector?

A. Management Only
B. Log Collector Only
C. Management and Log Collector
D. Dedicated Log Collector

Correct Answer: C
Section:

QUESTION 24
In an HA (High Availability) setup, what is the purpose of the HA3 link?

A. Synchronize session state information
B. Synchronize configuration changes
C. Exchange heartbeats between the devices
D. Transmit HA control traffic

Correct Answer: A
Section:

QUESTION 25
Which of the following must be enabled to use Threat Prevention features such as Anti-Virus and Anti-Spyware on a firewall?

A. Security Profiles
B. WildFire Subscription
C. URL Filtering
D. GlobalProtect Subscription

Correct Answer: A
Section:

QUESTION 26
When creating a custom application signature, which field allows you to specify the layer 7 protocol details to match?

A. Application ID
B. Signature ID
C. Pattern Match
D. Protocol Decoder

Correct Answer: C
Section:

QUESTION 27
Which license is required to use the Cortex XDR Managed Threat Hunting service?

A. Cortex Data Lake license
B. WildFire license
C. Cortex XDR Pro per TB license
D. Threat Prevention license

Correct Answer: C
Section:

QUESTION 28
Which touting configuration should you recommend lo a customer who wishes lo actively use multiple pathways to the same destination?

A. OSPF
B. ECMP
C. BGP
D. RIPv2

Correct Answer: B
Section:
Explanation:
For a customer who wishes to actively use multiple pathways to the same destination, the recommended routing configuration is:
B . ECMP (Equal-Cost Multi-Path)
ECMP allows the use of multiple paths to the same destination with equal cost metrics, enabling load balancing and redundancy. It is suitable for scenarios where multiple pathways are desired for traffic distribution and fault

tolerance.
Palo Alto Networks - ECMP Overview: https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-networking-admin/ecmp
Palo Alto Networks - Configuring ECMP: https://knowledgebase.paloaltonetworks.com