PCNSE.85q

Website: https://vceplus.com
VCE to PDF Converter: https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus

https://vceplus.com/

PCNSE

Palo Alto Networks Certified Network Security Engineer

Exam A

QUESTION 1
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

A. check
B. find
C. test
D. sim

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html

QUESTION 2
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.

Which two mandatory options are used to configure a VLAN interface? (Choose two.)

A. Virtual router
B. Security zone
C. ARP entries
D. Netflow Profile

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:
QUESTION 3
A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN configuration would adapt to changes when deployed to the future site?

A. Preconfigured GlobalProtect satellite
B. Preconfigured GlobalProtect client
C. Preconfigured IPsec tunnels
D. Preconfigured PPTP Tunnels

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair.

Which NGFW receives the configuration from Panorama?

A. The Passive firewall, which then synchronizes to the active firewall
B. The active firewall, which then synchronizes to the passive firewall
C. Both the active and passive firewalls, which then synchronize with each other
D. Both the active and passive firewalls independently, with no synchronization afterward

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

A. The settings assigned to the template that is on top of the stack.
B. The administrator will be promoted to choose the settings for that chosen firewall.
C. All the settings configured in all templates.
D. Depending on the firewall location, Panorama decides with settings to send.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Which method will dynamically register tags on the Palo Alto Networks NGFW?

A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
B. Restful API or the VMware API on the firewall or on the User-ID agent
C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynamically

QUESTION 7
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

A. Device>Setup>Services>AutoFocus
B. Device> Setup>Management >AutoFocus
C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
D. Device>Setup>WildFire>AutoFocus
E. Device>Setup> Management> Logging and Reporting Settings

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

QUESTION 8
An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

A. Security policy rule allowing SSL to the target server
B. Firewall connectivity to a CRL
C. Root certificate imported into the firewall with "Trust" enabled
D. Importation of a certificate from an HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

QUESTION 9
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)
B. Kernel Virtualization Module (KVM)
C. Boot Strap Virtualization Module (BSVM)
D. Microsoft Hyper-V

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

QUESTION 10
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?

A. web-browsing and 443
B. SSL and 80
C. SSL and 443
D. web-browsing and 80

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
A Security policy rule is configured with a Vulnerability Protection Profile and an action of 'Deny".

Which action will this cause configuration on the matched traffic?

A. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to "Deny".
B. The configuration will allow the matched session unless a vulnerability signature is detected. The "Deny" action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit.
D. The configuration is valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to "Deny."

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
What are two benefits of nested device groups in Panorama? (Choose two.)

A. Reuse of the existing Security policy rules and objects
B. Requires configuring both function and location for every device
C. All device groups inherit settings form the Shared group
D. Overwrites local firewall configuration

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
Which Captive Portal mode must be configured to support MFA authentication?

A. NTLM
B. Redirect
C. Single Sign-On
D. Transparent

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication

QUESTION 14
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects.

How would an administrator configure the interface to 1Gbps?

A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex

C. set deviceconfig system speed-duplex 1Gbps-full-duplex

D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

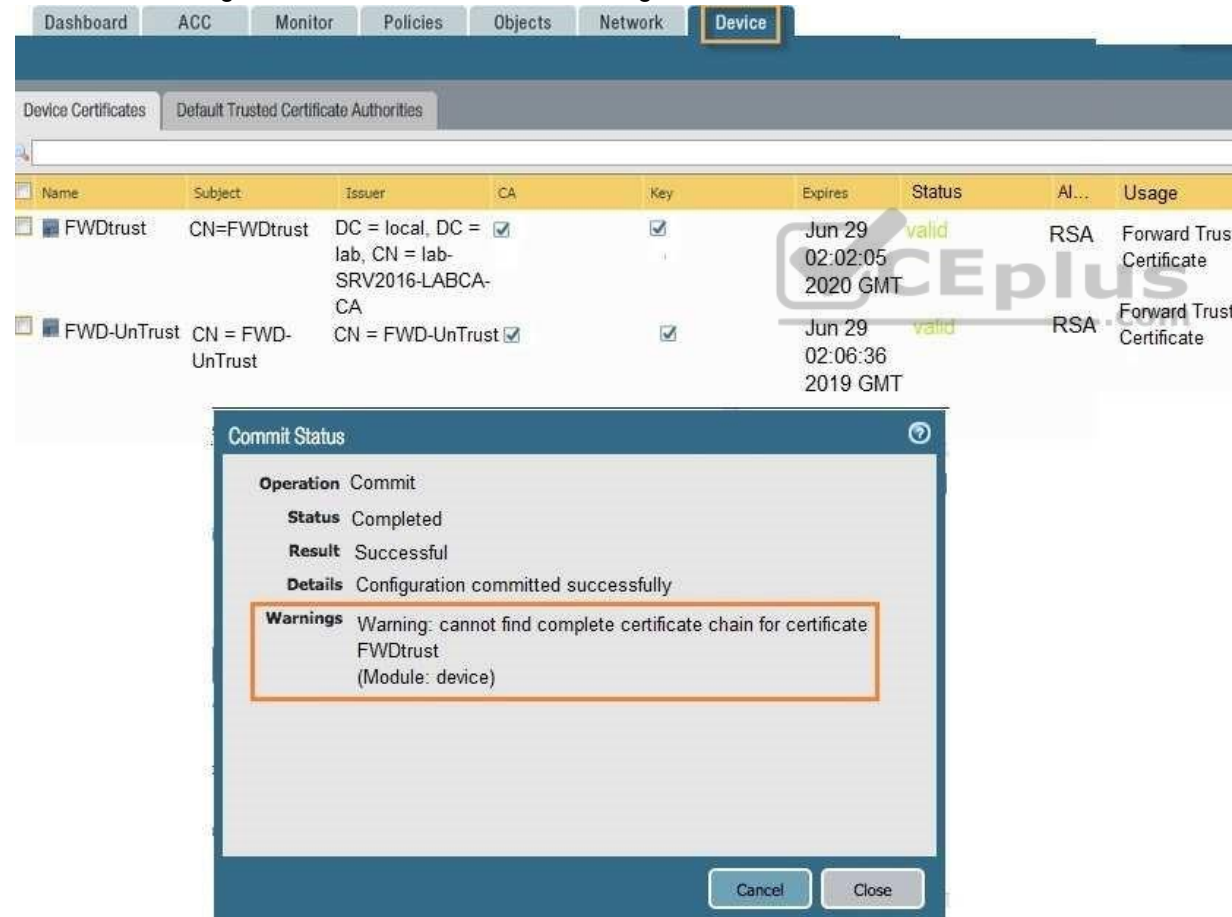**Correct Answer:** C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034

QUESTION 15
Based on the image, what caused the commit warning?

A. The CA certificate for FWDtrust has not been imported into the firewall.
B. The FWDtrust certificate has not been flagged as Trusted Root CA.
C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
D. The FWDtrust certificate does not have a certificate chain.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

A. Use the debug dataplane packet-diag set capture stage firewall file command.
B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
C. Use the debug dataplane packet-diag set capture stage management file command.
D. Use the tcpdump command.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390

QUESTION 17
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications.
QoS natively integrates with which feature to provide service quality?

A. Port Inspection
B. Certificate revocation
C. Content-ID
D. App-ID

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#idaed4e749-80b44641-a37c-c741aba562e9

QUESTION 18
Which three settings are defined within the Templates object of Panorama? (Choose three.)

A. Setup
B. Virtual Routers
C. Interfaces
D. Security
E. Application Override

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
A customer has an application that is being identified as unknown-tcp for one of their custom PostgreSQL database connections.

Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

A. Application Override policy.
B. Security policy to identify the custom application.
C. Custom application.
D. Custom Service object.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 20
What are the differences between using a service versus using an application for Security Policy match?

A. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an "application" allows the firewall to take immediate action if the port being used is a member of the application standard port list.

B. There are no differences between "service" or "application". Use of an "application" simplifies configuration by allowing use of a friendly application name instead of port numbers.

C. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used

D. Use of a "service" enables the firewall to take action after enough packets allow for App-ID identification

Correct Answer: A
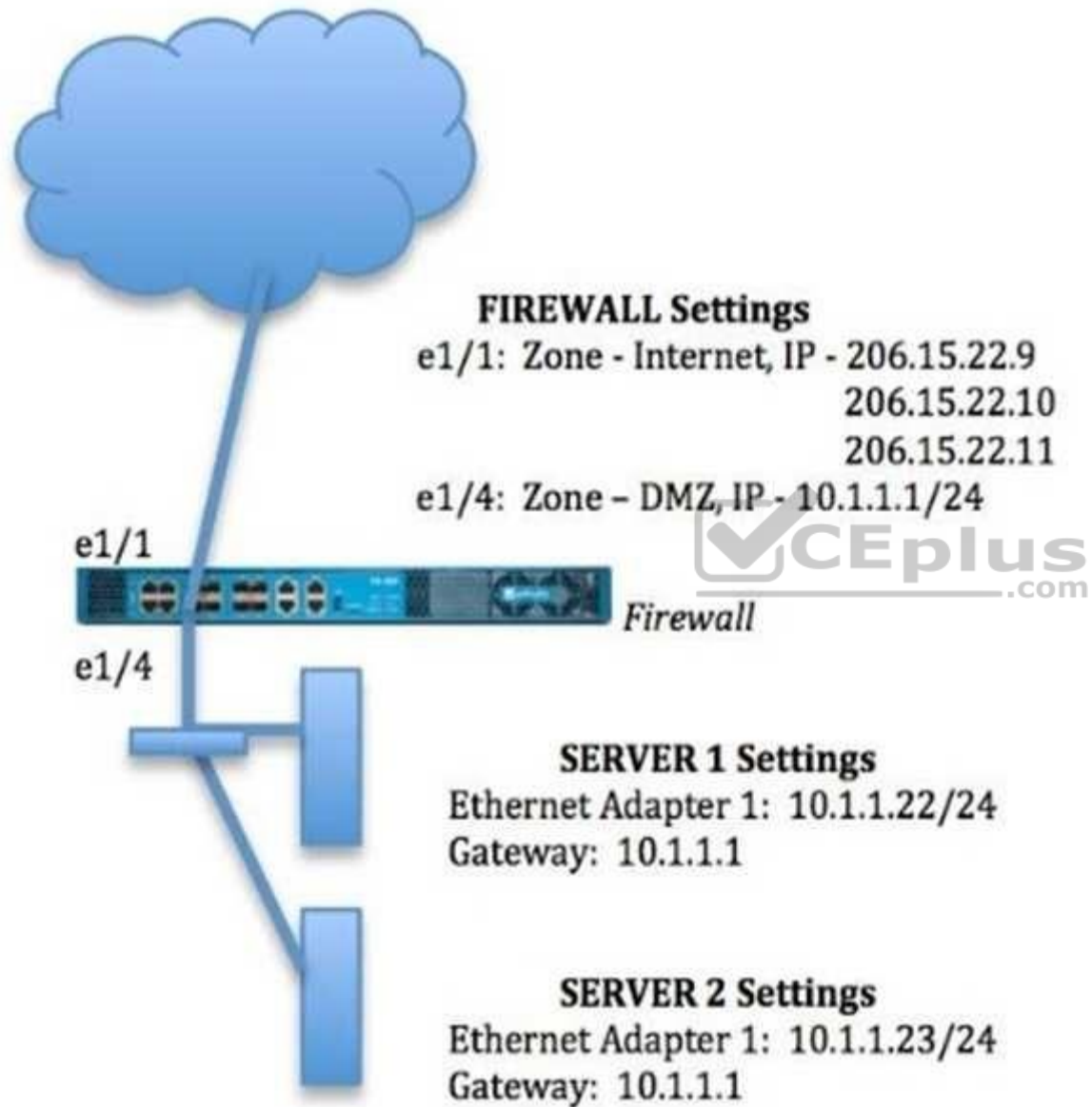**Section: (none)**
Explanation

Explanation/Reference:

QUESTION 21
An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?

FIREWALL Settings
e1/1: Zone - Internet, IP - 206.15.22.9
                                     206.15.22.10
                                     206.15.22.11
e1/4: Zone – DMZ, IP - 10.1.1.1/24

SERVER 1 Settings
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1

SERVER 2 Settings
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

D.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port:80/TCP

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW.
The update contains an application that matches the same traffic signatures as the custom application.

Which application should be used to identify traffic traversing the NGFW?

A. Custom application
B. System logs show an application error and neither signature is used.
C. Downloaded application
D. Custom and downloaded application signature files are merged and both are used

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which event will happen if an administrator uses an Application Override Policy?

A. Threat-ID processing time is decreased.
B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
C. The application name assigned to the traffic by the security rule is written to the Traffic log.
D. App-ID processing time is increased.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

QUESTION 24
A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

A. Enable packet buffer protection on the Zone Protection Profile.
B. Apply an Anti-Spyware Profile with DNS sinkholing.
C. Use the DNS App-ID with application-default.
D. Apply a classified DoS Protection Profile.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 25
If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?

A. Mapping to the IP address of the logged-in user.
B. First four letters of the username matching any valid corporate username.
C. Using the same user's corporate username and password.
D. Matching any valid corporate username.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/credential-phishing-prevention

QUESTION 26

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all webbrowsing traffic from any to any zone.

What must the administrator configure so that the PAN-OS® software can be upgraded?

A. Security policy rule
B. CRL
C. Service route
D. Scheduler

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

Which feature prevents the submission of corporate login information into website forms?

A. Data filtering
B. User-ID
C. File blocking
D. Credential phishing prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance

QUESTION 28
Which option is part of the content inspection process?

A. Packet forwarding process
B. SSL Proxy re-encrypt
C. IPsec tunnel encryption
D. Packet egress process

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

A. Create a decryption rule matching the encrypted BitTorrent traffic with action "No-Decrypt," and place the rule at the top of the Decryption policy.
B. Create a Security policy rule that matches application "encrypted BitTorrent" and place the rule at the top of the Security policy.
C. Disable the exclude cache option for the firewall.
D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Refer to the exhibit.

Which certificates can be used as a Forward Trust certificate?

A. Certificate from Default Trust Certificate Authorities
B. Domain Sub-CA

	Device Certificates	Default Trusted Certificate Authorities						
	Name	Location	Subject	Issuer	CA	Key	Expires	Status	Algo
☐	Domain-Root-Cert	vsys1	DC=local, DC=lab, CN=lab-DEMO-2008R2-CA	DC=local, DC=lab, CN=lab-DEMO-2008R2-CA	✓		Nov1 00:34:47 2021 GMT	valid	RSA
☐	Domain Sub-CA	vsys1	CN=sca.lab.local	DC=local, DC=lab, CN=lab-DEMO-2008R2-CA	✓	✓	Jun 6 20:59:38 2019 GMT	valid	RSA
☐	Forward_Trust	vsys1	CN=fwdtrust.la..	CN=sca.lab.local		✓	Jun 6 21:09:49 GMT	valid	RSA

C. Forward_Trust
D. Domain-Root-Cert

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 31
An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.

Which configuration setting or step will allow the firewall to get automatic application signature updates?

A. A scheduler will need to be configured for application signatures.
B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
C. A Threat Prevention license will need to be installed.
D. A service route will need to be configured.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

QUESTION 32
Which three options are supported in HA Lite? (Choose three.)

A. Virtual link
B. Active/passive deployment
C. Synchronization of IPsec security associations
D. Configuration synchronization
E. Session synchronization

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite

QUESTION 33
Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

A. debug system details
B. show session info
C. show system info
D. show system details

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful-Commands/ta-p/56511

QUESTION 34
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

A. Session Browser
B. Application Command Center
C. TCP Dump
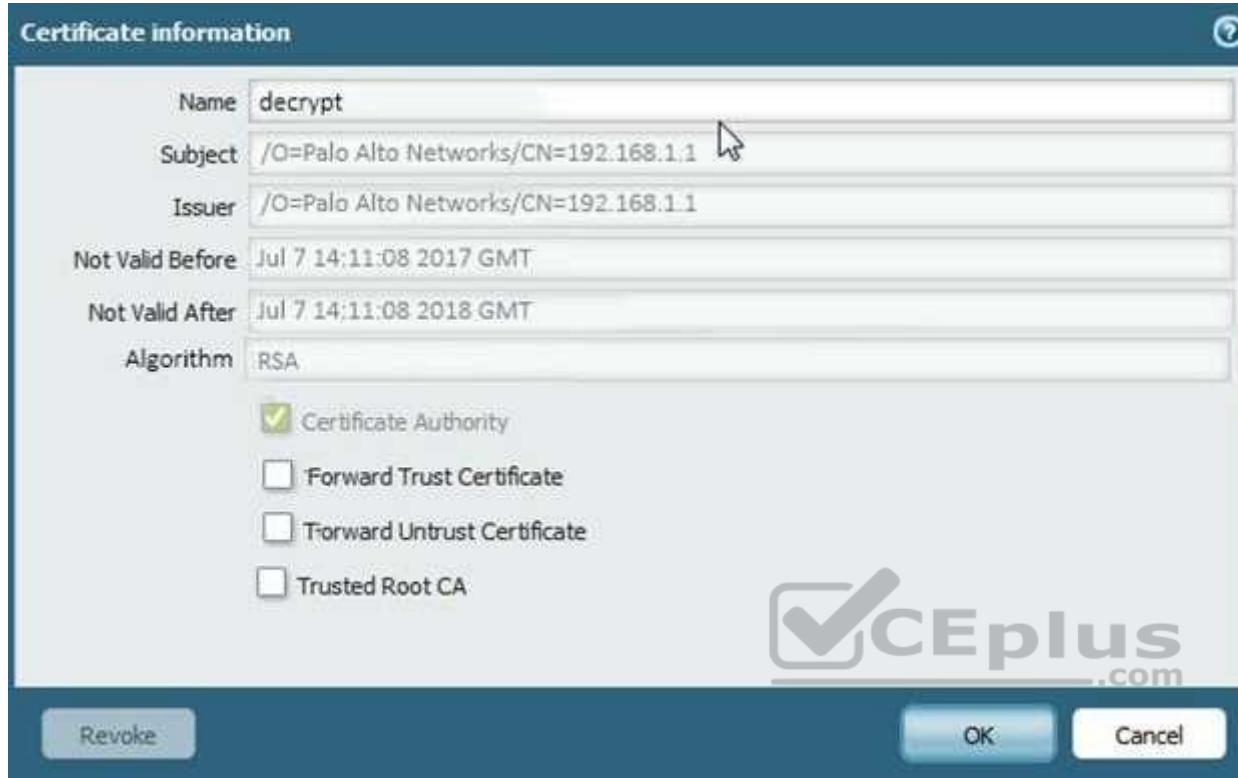D. Packet Capture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342

QUESTION 35
The certificate information displayed in the following image is for which type of certificate?

Certificate information

Name	decrypt
Subject	/O=Palo Alto Networks/CN=192.168.1.1
Issuer	/O=Palo Alto Networks/CN=192.168.1.1
Not Valid Before	Jul 7 14:11:08 2017 GMT
Not Valid After	Jul 7 14:11:08 2018 GMT
Algorithm	RSA

☑ Certificate Authority

☐ Forward Trust Certificate

☐ Forward Untrust Certificate

☐ Trusted Root CA

Revoke   OK   Cancel

A. Forward Trust certificate
B. Self-Signed Root CA certificate
C. Web Server certificate
D. Public CA signed certificate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 36
Which feature must you configure to prevent users form accidentally submitting their corporate credentials to a phishing website?

A. URL Filtering profile
B. Zone Protection profile
C. Anti-Spyware profile
D. Vulnerability Protection profile

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing

QUESTION 37
How can a candidate or running configuration be copied to a host external from Panorama?

A. Commit a running configuration.
B. Save a configuration snapshot.
C. Save a candidate configuration.
D. Export a named configuration snapshot.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewallconfigurations

QUESTION 38
If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect traffic when users browse to HTTP(S) websites?

A. SSL Forward Proxy
B. SSL Inbound Inspection
C. TLS Bidirectional proxy
D. SSL Outbound Inspection
Correct Answer: B

Explanation/Reference:

QUESTION 39
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

A. Create a custom App-ID and enable scanning on the advanced tab.
B. Create an Application Override policy.
C. Create a custom App-ID and use the "ordered conditions" check box.
D. Create an Application Override policy and custom threat signature for the application.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which virtual router feature determines if a specific destination IP address is reachable?

A. Heartbeat Monitoring
B. Failover
C. Path Monitoring
D. Ping-Path

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf

QUESTION 41

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port.

Which log entry can the administrator use to verify that sessions are being decrypted?

A. In the details of the Traffic log entries
B. Decryption log
C. Data Filtering log
D. In the details of the Threat log entries

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719

QUESTION 42
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

https://vceplus.com/.

How would the administrator establish the chain of trust?

A. Use custom certificates
B. Enable LDAP or RADIUS integration
C. Set up multi-factor authentication
D. Configure strong password authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment

QUESTION 43
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.

Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443?

A. Rule #1: application: web-browsing; service: application-default; action: allow
   Rule #2: application: ssl; service: application-default; action: allow
B. Rule #1: application: web-browsing; service: service-https; action: allow Rule
   #2: application: ssl; service: application-default; action: allow
C. Rule # 1: application: ssl; service: application-default; action: allow
   Rule #2: application: web-browsing; service: application-default; action: allow
D. Rule #1: application: web-browsing; service: service-http; action: allow Rule
   #2: application: ssl; service: application-default; action: allow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys mode.
B. The traffic is offloaded.
C. The traffic does not match the packet capture filter.
D. The firewall's DP CPU is higher than 50%.

Correct Answer: BC
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

QUESTION 46
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in "the cloud"). Bootstrapping is the most expedient way to perform this task.

Which option describes deployment of a bootstrap package in an on-premise virtual environment?

A. Use config-drive on a USB stick.
B. Use an S3 bucket with an ISO.
C. Create and attach a virtual hard disk (VHD).
D. Use a virtual CD-ROM with an ISO.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-onkvm/use-an-iso-file-to-deploy-the-vm-series-firewall

QUESTION 47
Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a "No Decrypt" action? (Choose two.)

A. Block sessions with expired certificates
B. Block sessions with client authentication
C. Block sessions with unsupported cipher suites
D. Block sessions with untrusted issuers
E. Block credential phishing

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traffic-to-decrypt/create-a-decryption-profile

QUESTION 48
Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

A. port mapping
B. server monitoring
C. client probing
D. XFF headers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users

QUESTION 49
Which feature can be configured on VM-Series firewalls?

A. aggregate interfaces
B. machine learning
C. multiple virtual systems
D. GlobalProtect

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
In High Availability, which information is transferred via the HA data link?

A. session information
B. heartbeats
C. HA state information
D. User-ID information

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links

QUESTION 51
A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.
B. Add a Vulnerability Protection Profile to block the attack.
C. Add QoS Profiles to throttle incoming requests.
D. Add a DoS Protection Profile with defined session count.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-andpolicy-rules/dos-protection-profiles

QUESTION 52
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

A. Verify AutoFocus status using CLI "test" command.
B. Check the WebUI Dashboard AutoFocus widget.
C. Check for WildFire forwarding logs.
D. Check the license
E. Verify AutoFocus is enabled below Device Management tab.

Correct Answer: DE

Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

QUESTION 53

Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

QUESTION 54

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.

D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-clientauthentication-configurations/define-the-globalprotect-agent-configurations

QUESTION 55
Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

A. TACACS+
B. Kerberos
C. PAP
D. LDAP
E. SAML
F. RADIUS

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
What is exchanged through the HA2 link?

A. hello heartbeats
B. User-ID information
C. session synchronization
D. HA state information

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links

QUESTION 57
Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

A. Both SSH keys and SSL certificates must be generated.
B. No prerequisites are required.
C. SSH keys must be manually generated.
D. SSL certificates must be generated.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy

QUESTION 58
Which Zone Pair and Rule Type will allow a successful connection for a user on the Internet zone to a web server hosted on the DMZ zone? The web server

Zone Pair:
Source Zone: Internet
Destination Zone: Internet

Rule Type:
'intrazone'

is reachable using a Destination NAT policy in the Palo Alto Networks firewall. A.

Zone Pair:
Source Zone: Internet
Destination Zone: DMZ

Rule Type:
'interzone' or 'universal'

Zone Pair:
Source Zone: Internet
Destination Zone: Internet

Rule Type:
'intrazone' or 'universal'

Zone Pair:
Source Zone: Internet
Destination Zone: DMZ

Rule Type:
'intrazone'

B.

C.

D.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
An administrator has configured a QoS policy rule and a QoS Profile that limits the maximum allowable bandwidth for the YouTube application. However, YouTube is consuming more than the maximum bandwidth allotment configured.
Which configuration step needs to be configured to enable QoS?

A. Enable QoS interface
B. Enable QoS in the Interface Management Profile
C. Enable QoS Data Filtering Profile
D. Enable QoS monitor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
A customer wants to set up a site-to-site VPN using tunnel interfaces.

Which two formats are correct for naming tunnel interfaces? (Choose two.)

A. tunnel.1
B. vpn-tunnel.1
C. tunnel.1025
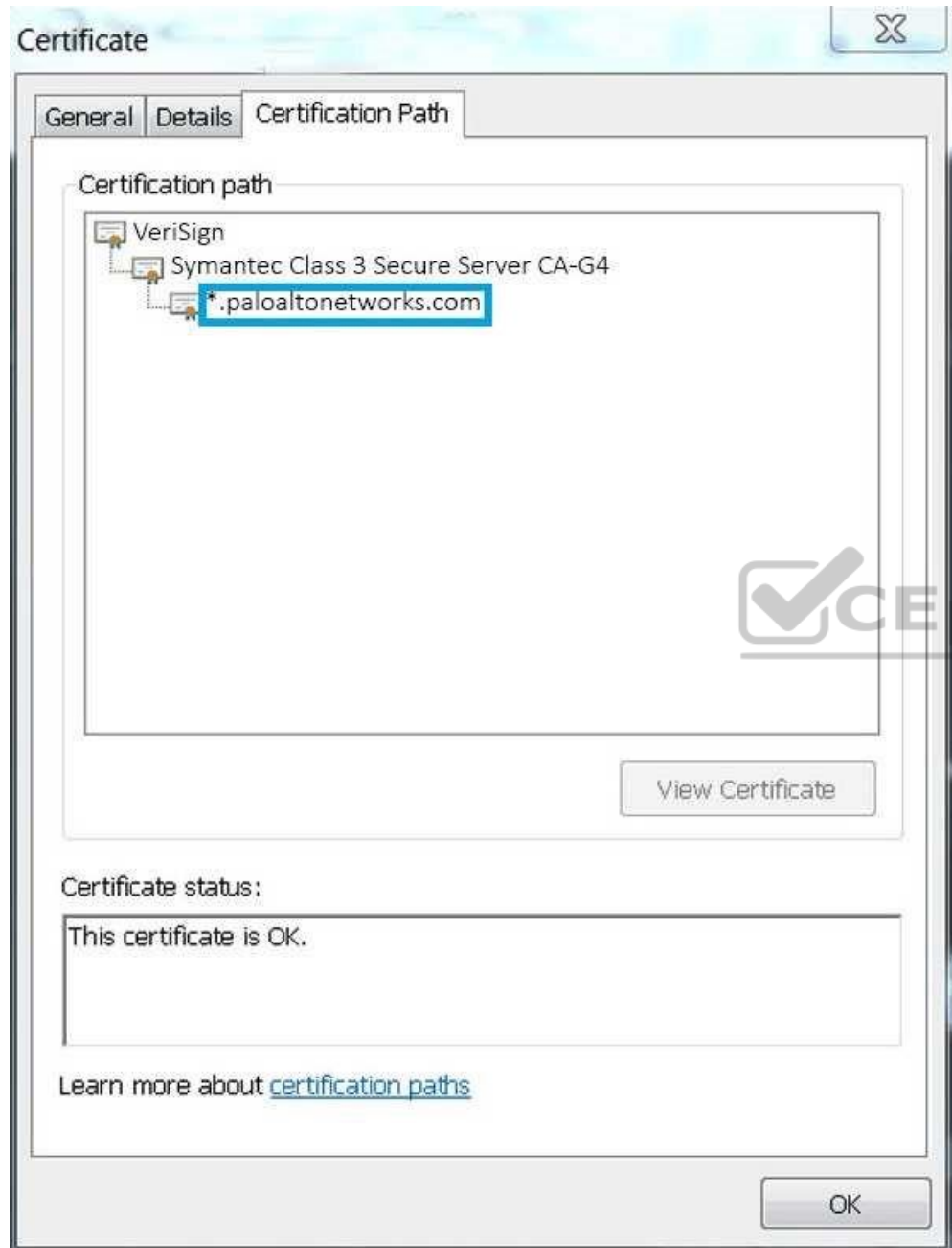D. vpn-tunnel.1024

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
QUESTION 61
Based on the following image, what is the correct path of root, intermediate, and end-user certificate?

Certificate

General | Details | **Certification Path**

Certification path

- VeriSign
  - Symantec Class 3 Secure Server CA-G4
    - *.paloaltonetworks.com

[View Certificate]

Certificate status:

This certificate is OK.

Learn more about certification paths

[OK]

A. Palo Alto Networks > Symantec > VeriSign
B. VeriSign > Symantec > Palo Alto Networks
C. Symantec > VeriSign > Palo Alto Networks
D. VeriSign > Palo Alto Networks > Symantec

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and assign untagged (native) traffic to its own zone.

Which option differentiates multiple VLANs into separate zones?

A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096" in the "Tag Allowed" field of the V-Wire object.
B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the "Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which four NGFW multi-factor authentication factors are supported by PAN-OS®? (Choose four.)

A. Short message service
B. Push
C. User logon

D. Voice
E. SSH key
F. One-Time Password

Correct Answer: ABDF
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication

QUESTION 64
Which two features does PAN-OS® software use to identify applications? (Choose two.)

A. transaction characteristics
B. session number
C. pot number
D. application layer payload

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

A. Load configuration version
B. Save candidate config
C. Export device state
D. Load named configuration snapshot

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 66
When configuring the firewall for packet capture, what are the valid stage types?

A. receive, management, transmit, and non-syn
B. receive, management, transmit, and drop
C. receive, firewall, send, and non-syn
D. receive, firewall, transmit, and drop

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Which operation will impact performance of the management plane?

A. DoS protection
B. WildFire submissions
C. generating a SaaS Application report
D. decrypting SSL sessions

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

A. 6-tuple match:
    Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone
B. 5-tuple match:
    Source IP Address, Destination IP Address, Source port, Destination Port, Protocol
C. 7-tuple match:
    Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone

D. 9-tuple match:
   Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which feature can provide NGFWs with User-ID mapping information?

A. Web Captcha
B. Native 802.1q authentication
C. GlobalProtect
D. Native 802.1x authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content IDs to traffic?

A. Select download-and-install
B. Select download-only
C. Select download-and-install, with "Disable new apps in content update" selected
D. Select disable application updates and select "Install only Threat updates"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71

In which two types of deployment is active/active HA configuration supported? (Choose two.)

A. Layer 3 mode
B. TAP mode
C. Virtual Wire mode
D. Layer 2 mode

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

A. ingress processing errors
B. rule match with action "deny"
C. rule match with action "allow"
D. equal-cost multipath

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
▪ Firewall has internet connectivity through e 1/1.
▪ Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
▪ Service route is configured, sourcing update traffic from e1/1.
▪ A communication error appears in the System logs when updates are performed. ▪
Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

A. Static route pointing application PaloAlto-updates to the update servers
B. Security policy rule allowing PaloAlto-updates as the application
C. Scheduler for timed downloads of PAN-OS software
D. DNS settings for the firewall to use for resolution

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

A. Add an Anti-Spyware Profile to block attacking IP address
B. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
C. Add QoS Profiles to throttle incoming requests
D. Add a tuned DoS Protection Profile

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing, and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS® software?

A. Antivirus update package.
B. Applications and Threats update package.
C. User-ID agent.
D. WildFire update package.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-an-hafirewall-pair-to-pan-os-80

QUESTION 76
Which administrative authentication method supports authorization by an external service?

A. Certificates
B. LDAP
C. RADIUS
D. SSH keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-authentication

QUESTION 77
How does Panorama prompt VMWare NSX to quarantine an infected VM?

A. HTTP Server Profile
B. Syslog Server Profile
C. Email Server Profile
D. SNMP Server Profile
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantineinfected-guests

QUESTION 78

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.) A.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
	06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 07:59:36	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
	06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
	06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

05/23 20:49:30	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:49:29	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex
05/23 20:47:24	port	informational	link-change	ethernet1/1	Port ethernet1/1: Up 10Gb/s-full duplex
05/23 20:47:22	port	informational	link-change	MGT	Port MGT: Up Unknown
05/23 20:47:18	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:47:17	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex

B. C.

D.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.

Correct Answer: AD
Section: (none)
Explanation
Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-decryption-profile

QUESTION 80
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

A. Enable and configure the Packet Buffer protection thresholds.
   Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholds Enable Interface
   Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.
   Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.
   Enable Packet Buffer Protection pre egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet
   Buffer Limits. Enable Zone Buffer Protection per zone.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/configure-zone-protection-to-increase-networksecurity/configure-packet-buffer-protection

QUESTION 81
What is the purpose of the firewall decryption broker?

A. decrypt SSL traffic and then send it as cleartext to a security chain of inspection tools.
B. force decryption of previously unknown cipher suites
C. reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools.
D. inspect traffic within IPsec tunnels

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/decryption-features/decryption-broker

QUESTION 82
What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

A. Rule Usage Hit counter will not be reset
B. Highlight Unused Rules will highlight all rules.
C. Highlight Unused Rules will highlight zero rules.
D. Rule Usage Hit counter will reset.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which is not a valid reason for receiving a decrypt-cert-validation error?

A. Unsupported HSM
B. Unknown certificate status
C. Client authentication
D. Untrusted issuer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons

QUESTION 84
In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. sg2 session count is the lowest compared to the other managed devices.

B. us3 has a logging rate that deviates from the administrator-configured thresholds.

C. uk3 has a logging rate that deviates from the seven-day calculated baseline.

D. sg2 has misconfigured session thresholds.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/panorama-features/device-monitoring-through-panorama

QUESTION 85
Which three split tunnel methods are supported by a GlobalProtect Gateway?

A. video streaming application

B. Client Application Process

C. Destination Domain

D. Source Domain

E. Destination user/group

F. URL Category

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features/split-tunnel-for-public-applications