PCNSE.prepaway.premium.exam.162q

Number: PCNSE
Passing Score: 800
Time Limit: 120 min
File Version: 7.0

PCNSE

Palo Alto Networks Certified Network Security Engineer

Version 7.0

Exam A

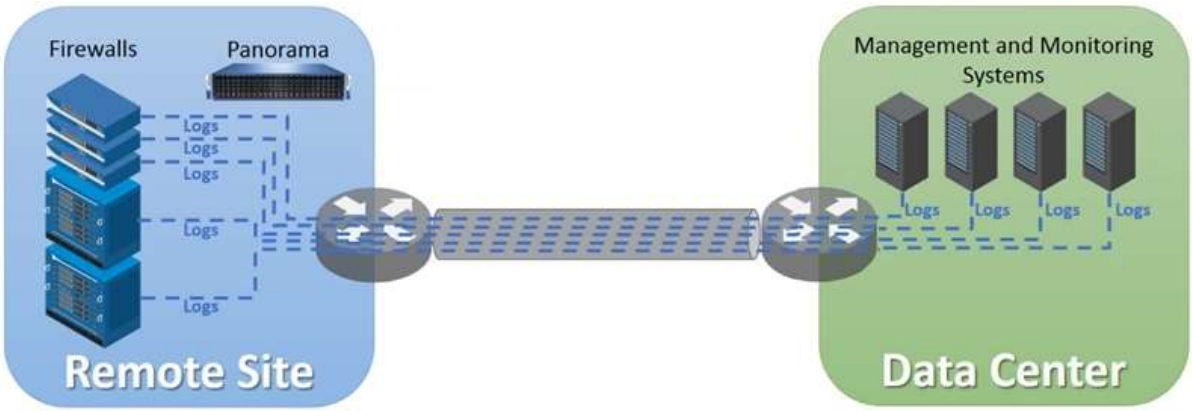
QUESTION 1
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

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
Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Configure log compression and optimization features on all remote firewalls.
D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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 4
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans.

Which Security Profile type will protect against worms and trojans?

A. Anti-Spyware
B. Instruction Prevention
C. File Blocking
D. Antivirus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles

QUESTION 5
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 6
An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

A. 0
B. 99
C. 1
D. 255

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/high-availability/device-priority-and-preemption

QUESTION 7
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?

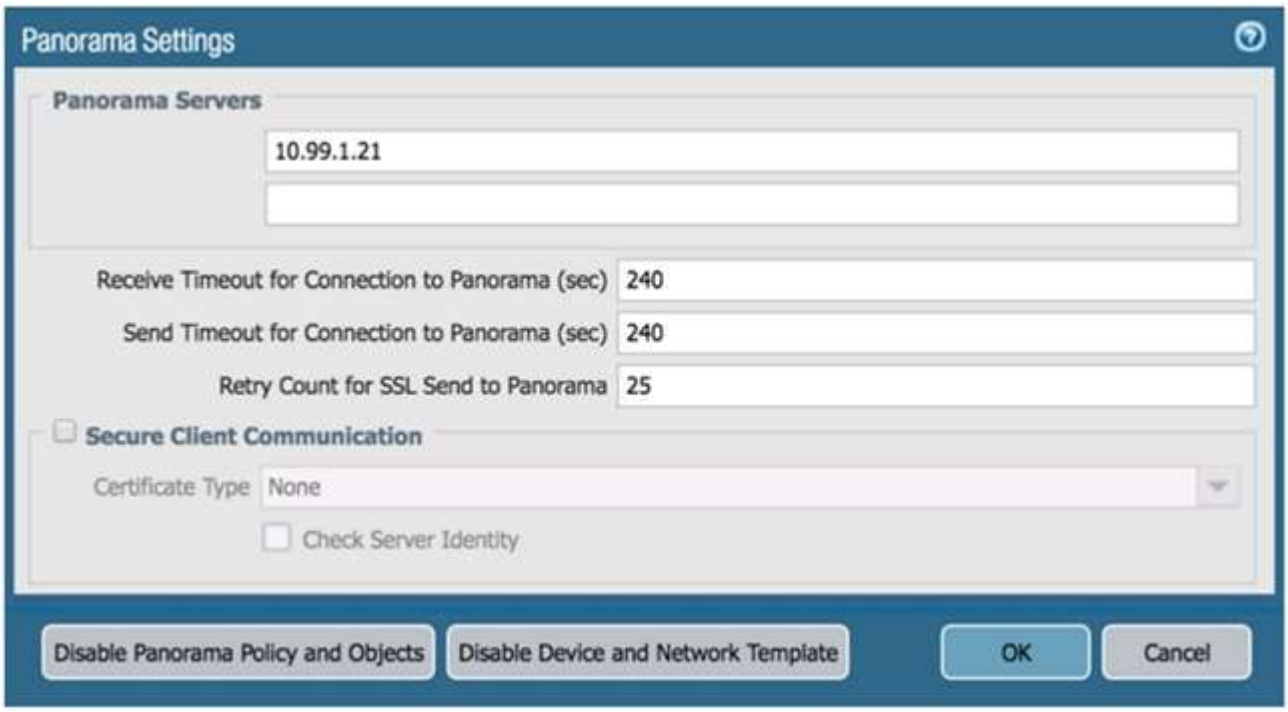
A. The passive firewall, which then synchronizes to the active firewall
B. The active firewall, which then synchronizes to the passive firewall
C. Both the active and passive firewalls, which then synchronize with each other
D. Both the active and passive firewalls independently, with no synchronization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

Correct Answer: C
Section: (none)
Explanation

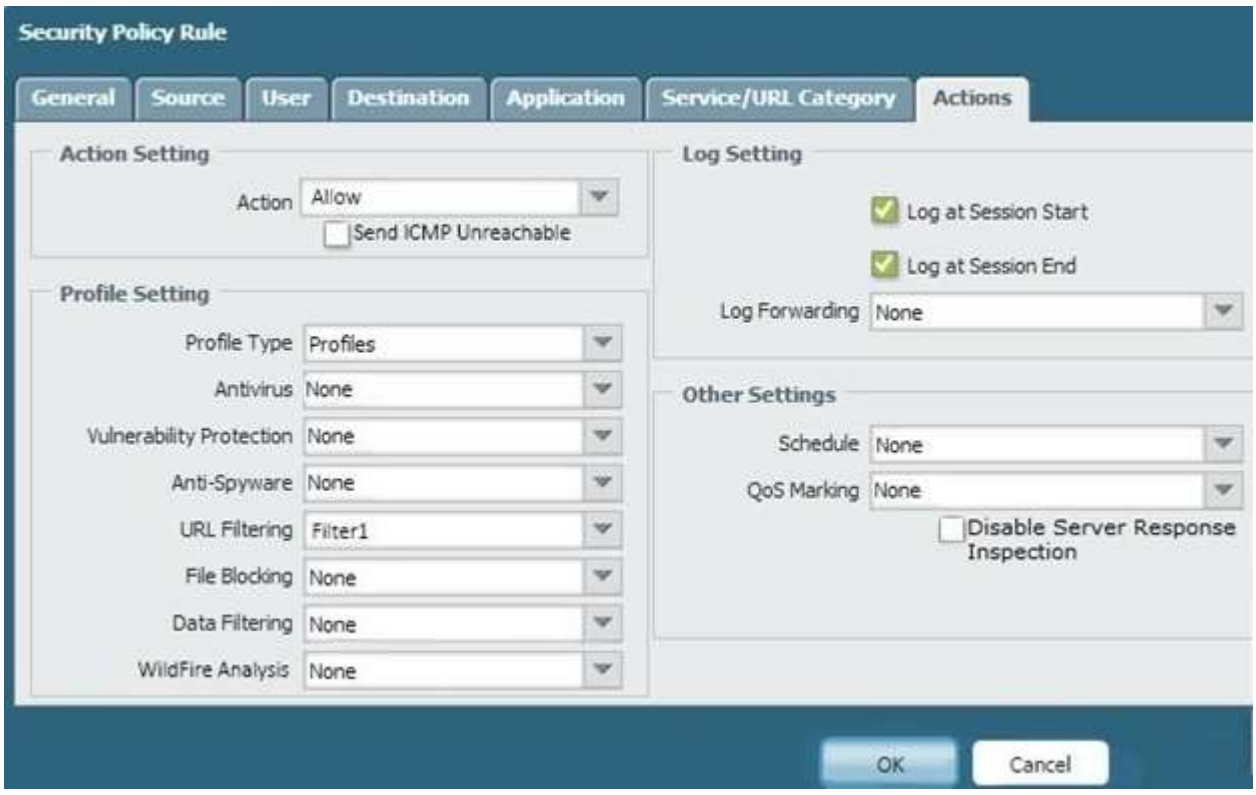
Explanation/Reference:

QUESTION 8
An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the firewall to Panorama?

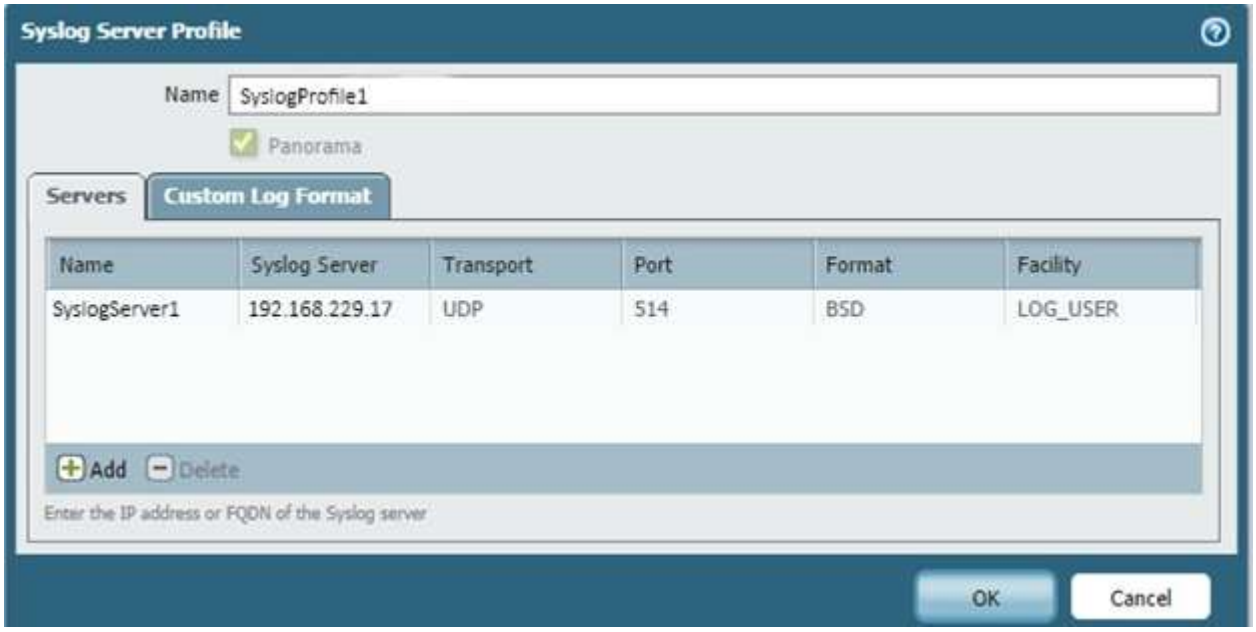
A.



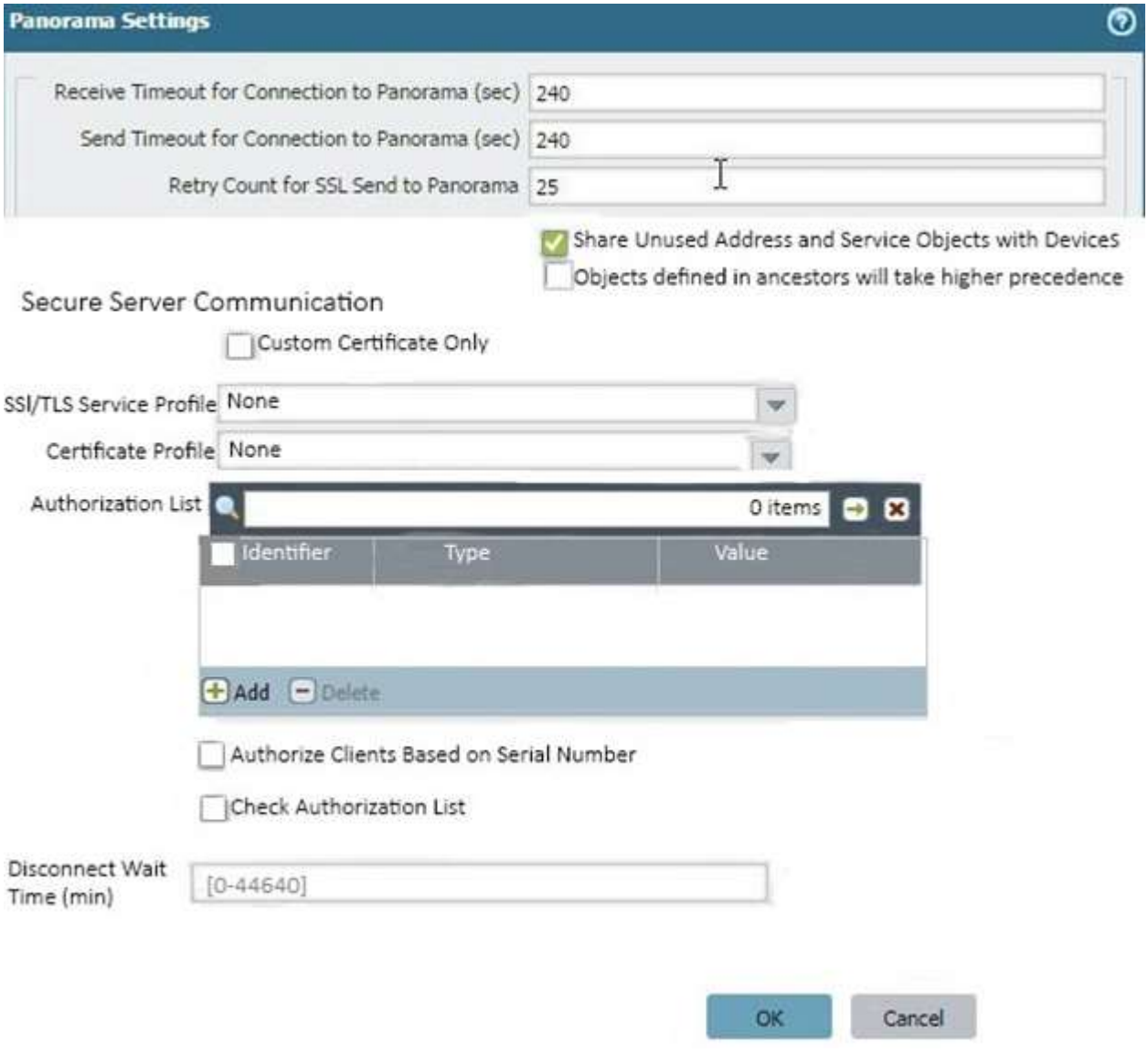
B.



C.



D.



Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

A. To enable Gateway authentication to the Portal
B. To enable Portal authentication to the Gateway
C. To enable user authentication to the Portal
D. To enable client machine authentication to the Portal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.
Reference https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/globalprotect/network-globalprotect-portals

QUESTION 10
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 11
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 *ready-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 12
How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

A. Configure the option for “Threshold”.
B. Disable automatic updates during weekdays.
C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update.
D. Automatically “download and install” but with the “disable new applications” option used.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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 14
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 15
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 16
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

A. XML API
B. Port Mapping
C. Client Probing
D. Server Monitoring

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent

Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/user-id-concepts/group-mapping#id93306080-fd9b-4f1b-96a6-4bfe1c8e69df

QUESTION 17
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 18
Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

A. Security policy
B. Decryption policy
C. Authentication policy
D. Application Override policy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 20
A user’s traffic traversing a Palo Alto Networks NGFW sometimes can reach http://www.company.com. At other times the session times out. The NGFW has been configured with a PBF rule that the user’s traffic matches when it goes to http://www.company.com.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.
B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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 22
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 23
An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required.

Which interface type would support this business requirement?

A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable we browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to thins server on tcp/8080?

A. application: web-browsing; service: application-default
B. application: web-browsing; service: service-https
C. application: ssl; service: any
D. application: web-browsing; service: (custom with destination TCP port 8080)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
If the firewall has the following link monitoring configuration, what will cause a failover?

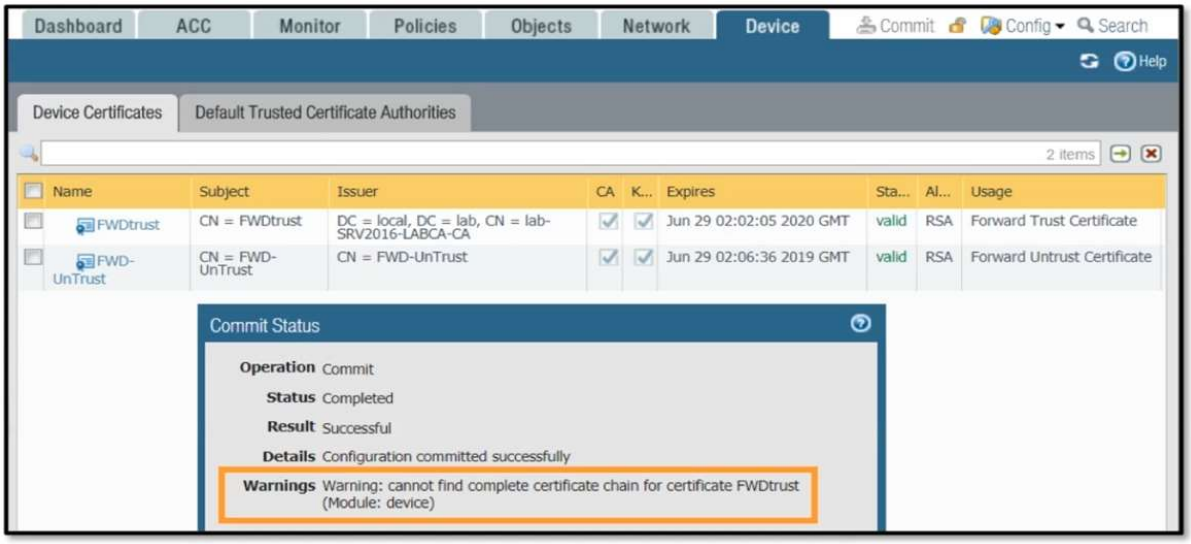
A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/3 going down

C. ethernet1/3 or ethernet1/6 going down
D. ethernet1/6 going down

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
In 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 28
Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

A. Okta
B. DUO
C. RADIUS
D. PingID

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 30
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#idaed4e749-80b4-4641-a37c-c741aba562e9

QUESTION 31
A session in the Traffic log is reporting the application as “incomplete.”

What does “incomplete” mean?

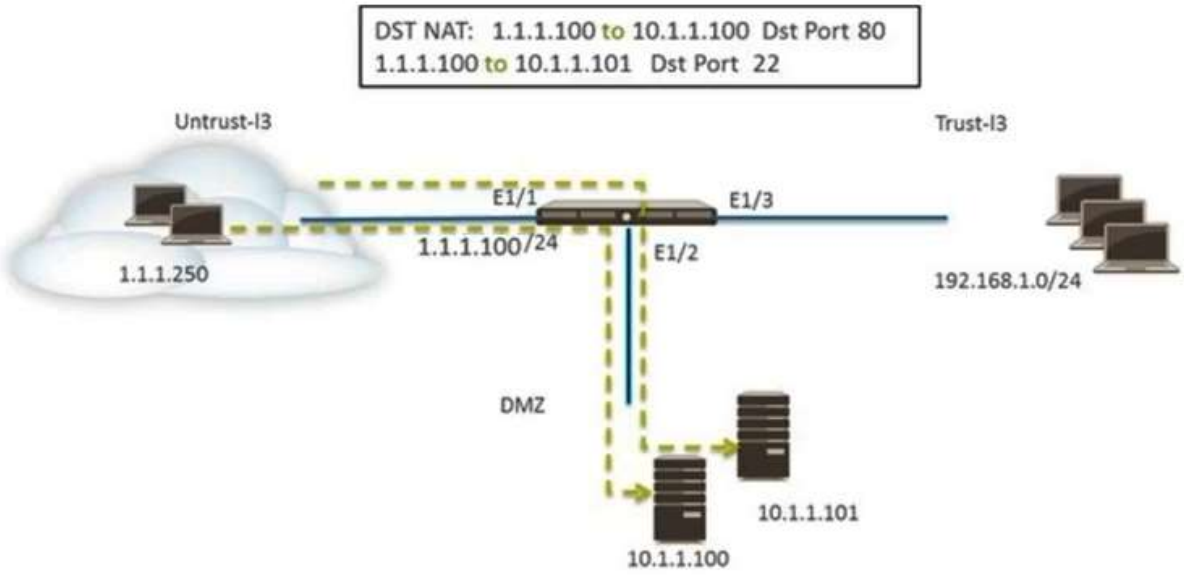
A. The three-way TCP handshake was observed, but the application could not be identified.
B. The three-way TCP handshake did not complete.
C. The traffic is coming across UDP, and the application could not be identified.
D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

Which two Security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing - Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh - Allow
C. Untrust (Any) to DMZ (10.1.1.100), web-browsing - Allow
D. Untrust (Any) to DMZ (10.1.1.100), ssh - Allow
E. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing - Allow

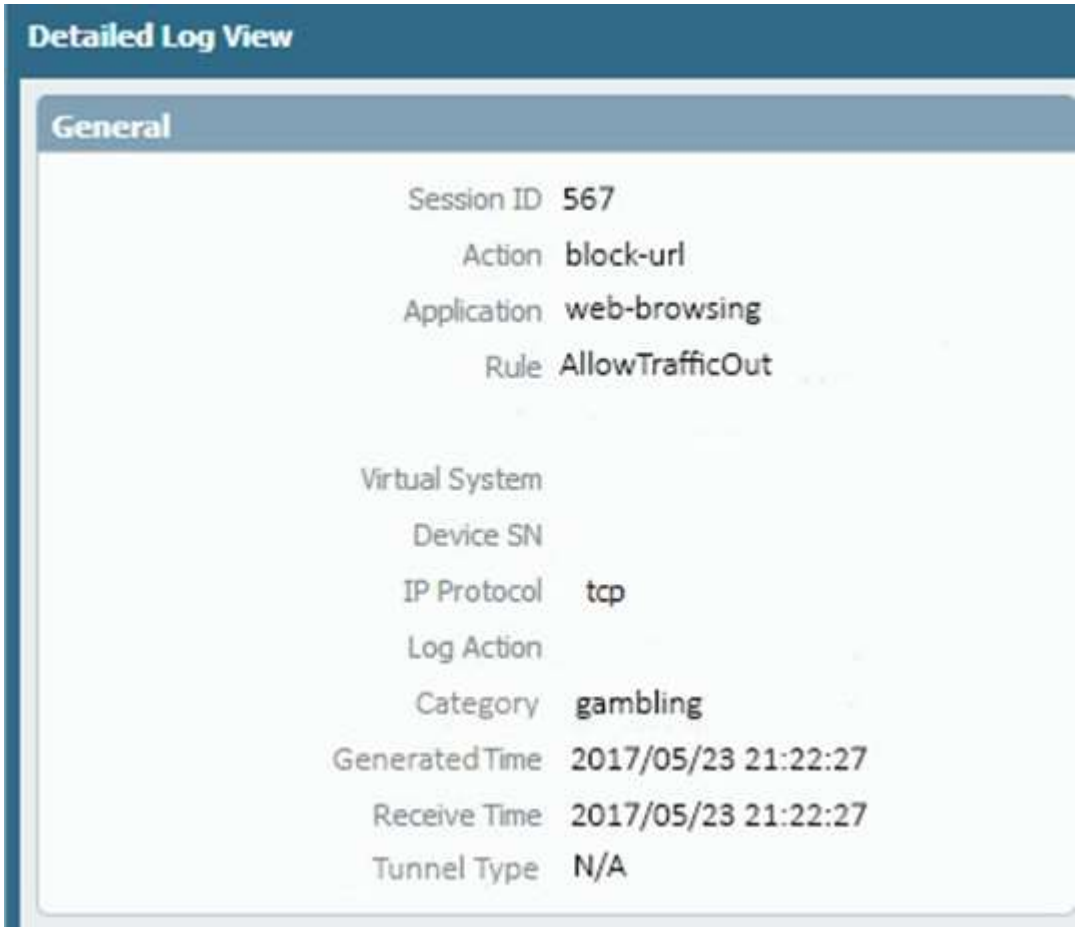
Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

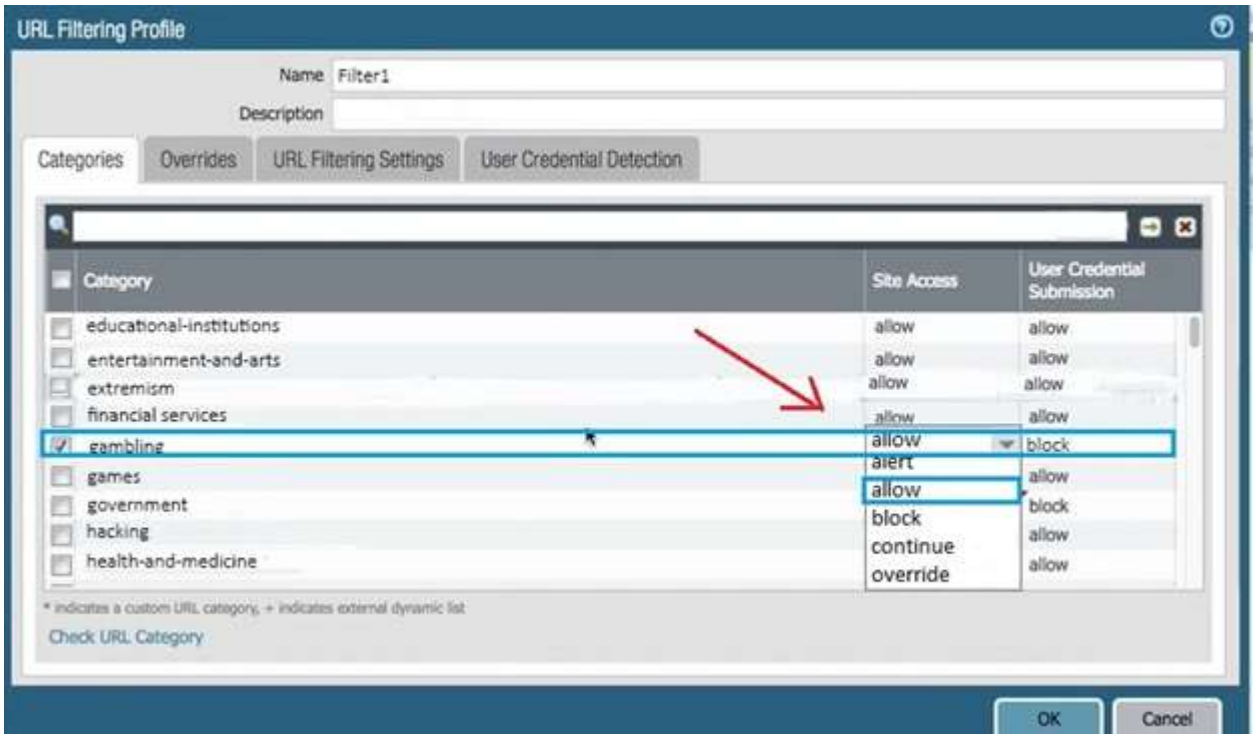
QUESTION 33
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.

Which configuration change should the administrator make?

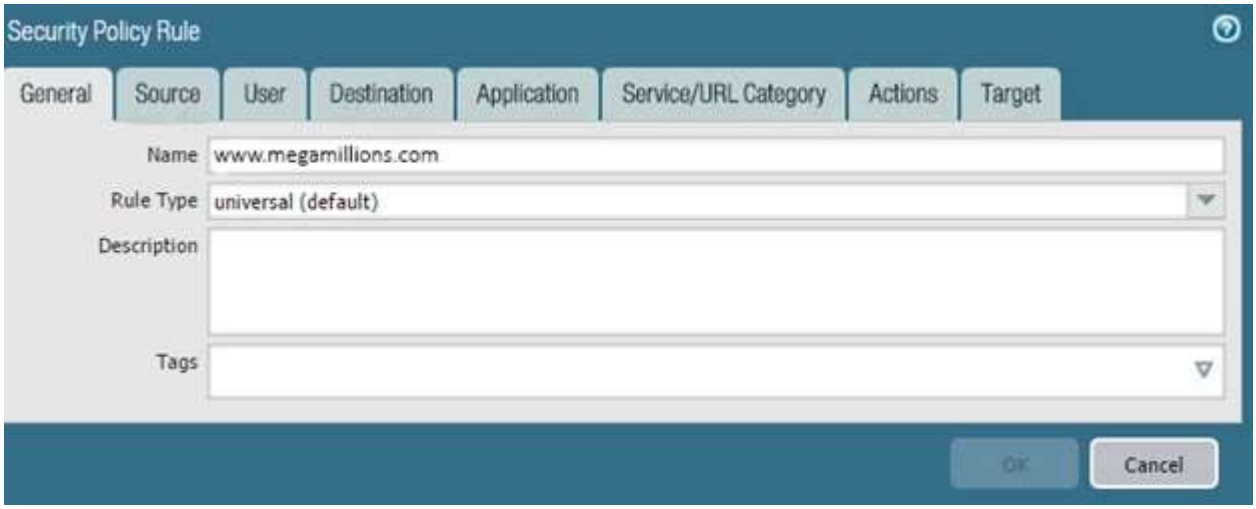
A.



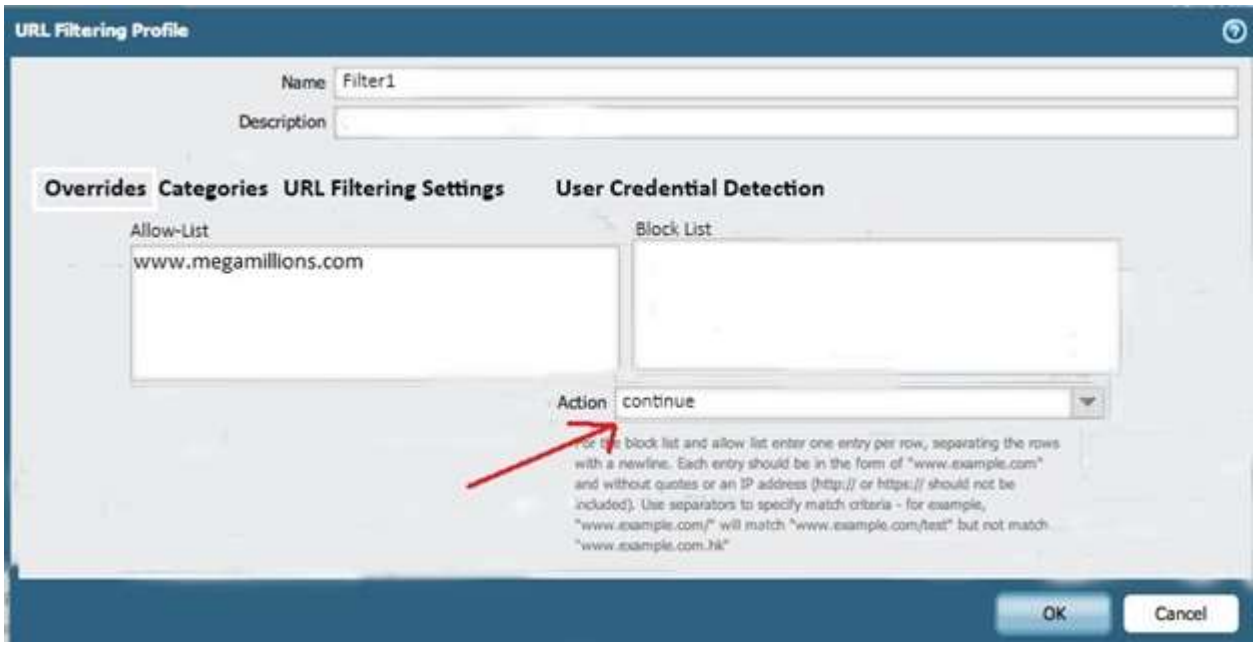
B.



C.



D.



E.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 36
An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab.

Which profile is the cause of the missing Policies tab?

A. Admin Role
B. WebUI
C. Authentication
D. Authorization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

A. WildFire updates
B. NAT
C. NTP
D. antivirus
E. file blocking

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama.

Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs into Panorama.
B. A CLI command will forward the pre-existing logs to Panorama.
C. Use the ACC to consolidate pre-existing logs.
D. The log database will need to exported form the firewalls and manually imported into Panorama.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

A. More than 15 minutes
B. 5 minutes
C. 10 to 15 minutes
D. 5 to 10 minutes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
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 41
Which Palo Alto Networks VM-Series firewall is valid?

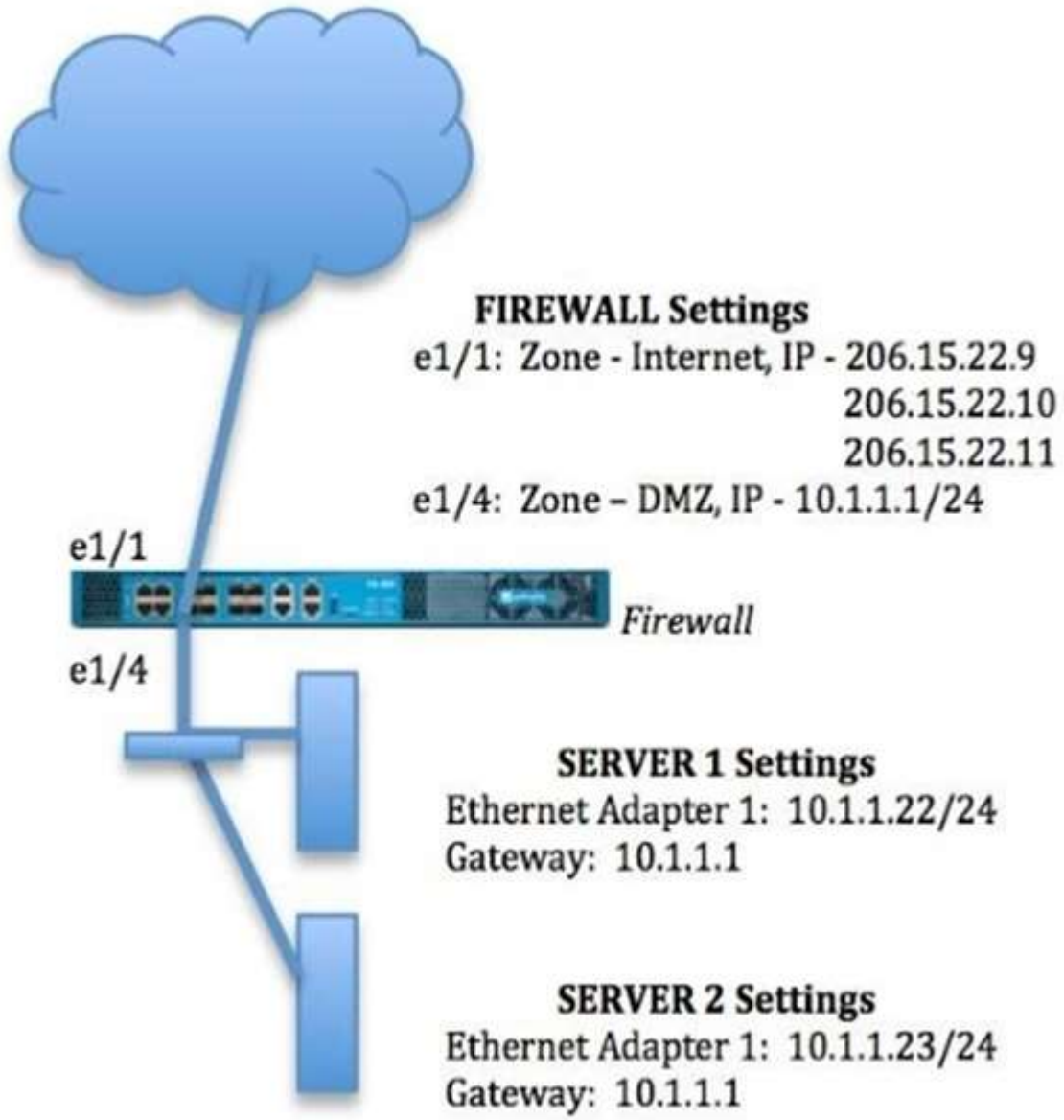
A. VM-25
B. VM-800
C. VM-50
D. VM-400

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 42
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?



A.

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

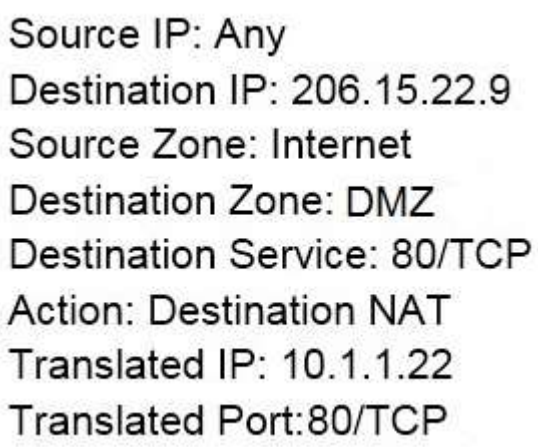
B.

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.



Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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 44
Starting with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

A. GlobalProtect
B. System
C. Authentication
D. Configuration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/

enhanced-logging-for-globalprotect.html

QUESTION 45
Refer to the exhibit.

```
######################
admin@Lab33-111-PA-3060(active)> show routing fib

id      destination           nexthop            flags  interface          mtu
------------------------------------------------------------------------------
47      0.0.0.0/0             10.46.40.1         ug     ethernet1/3        1500
46      10.46.40.0/23         0.0.0.0            u      ethernet1/3        1500
45      10.46.41.111/32       0.0.0.0            uh     ethernet1/3        1500
70      10.46.41.113/32       10.46.40.1         ug     ethernet1/3        1500
51      192.168.111.0/24      0.0.0.0            u      ethernet1/6        1500
50      192.168.111.2/32      0.0.0.0            uh     ethernet1/6        1500
------------------------------------------------------------------------------
######################

admin@Lab33-111-PA-3060(active)> show virtual-wire all

total virtual-wire shown :           1
flags :    m - multicast firewalling
           p - link state pass-through
           s - vlan sub-interface
           i - ip+vlan sub-interface
           t - tenant sub-interface

name               interface1        interface2        flags   allowed-tags
------------------------------------------------------------------------------
VW-1               ethernet1/7       ethernet1/5       p

######################
```

Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

A. ethernet1/6
B. ethernet1/3
C. ethernet1/7
D. ethernet1/5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which three authentication services can an administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

A. Kerberos
B. PAP
C. SAML

D. TACACS+
E. RADIUS
F. LDAP

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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 48
Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

A. Deny application facebook-chat before allowing application facebook
B. Deny application facebook on top
C. Allow application facebook on top
D. Allow application facebook before denying application facebook-chat

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673

QUESTION 49
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 50
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 51
An administrator has users accessing network resources through Citrix XenApp 7.x.

Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

A. Client Probing
B. Terminal Services agent
C. GlobalProtect
D. Syslog Monitoring

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 web-browsing 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 53
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 54
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 55
In a virtual router, which object contains all potential routes?

A. MIB
B. RIB
C. SIP
D. FIB

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/virtual-routers

QUESTION 56
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 57
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
C. Forward_Trust
D. Domain-Root-Cert

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

A. Configure a Decryption Profile and select SSL/TLS services.
B. Set up SSL/TLS under **Policies > Service/URL Category>Service**.
C. Set up Security policy rule to allow SSL communication.
D. Configure an SSL/TLS Profile.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-ssltls-service-profile

QUESTION 59
Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

A. ACC
B. System Logs
C. App Scope
D. Session Browser

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which protection feature is available only in a Zone Protection Profile?

A. SYN Flood Protection using SYN Flood Cookies
B. ICMP Flood Protection
C. Port Scan Protection
D. UDP Flood Protections

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which CLI command can be used to export the tcpdump capture?

A. scp export tcpdump from mgmt.pcap to <username@host:path>
B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
D. download mgmt-pcap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415

QUESTION 62
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 63
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 64
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 65
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. Pattern based application identification
B. Application override policy match
C. Application changed from content inspection
D. Session application identified.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

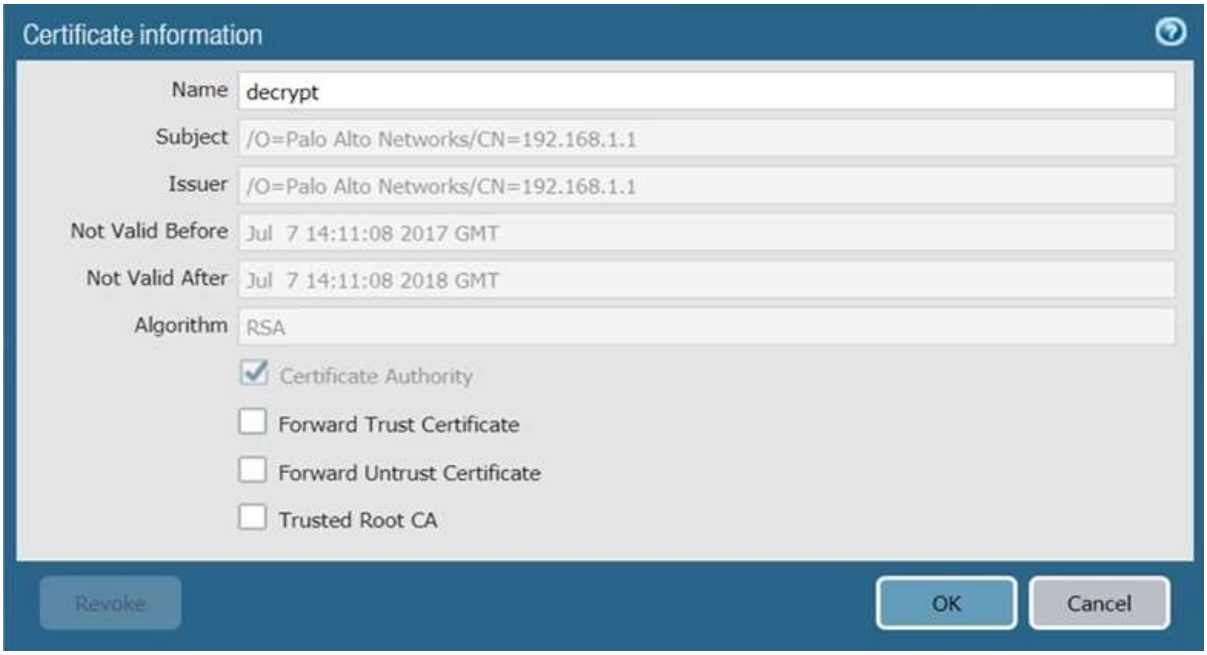
QUESTION 66
Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

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 67
The certificate information displayed in the following image is for which type of certificate?



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 68
Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

A. Disable SNMP on the management interface.
B. Application override of SSL application.
C. Disable logging at session start in Security policies.
D. Disable predefined reports.
E. Reduce the traffic being decrypted by the firewall.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which feature must you configure to prevent users from 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 70
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-firewall-configurations

QUESTION 71
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 a custom threat signature for the application.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

A. View the System logs and look for the error messages about BGP.
B. Perform a traffic pcap on the NGFW to see any BGP problems.
C. View the Runtime Stats and look for problems with BGP configuration.
D. View the ACC tab to isolate routing issues.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router.

Which two options enable the administrator to troubleshoot this issue? (Choose two.)

A. View Runtime Stats in the virtual router.
B. View System logs.
C. Add a redistribution profile to forward as BGP updates.
D. Perform a traffic pcap at the routing stage.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which three firewall states are valid? (Choose three.)

A. Active
B. Functional
C. Pending
D. Passive
E. Suspended

Correct Answer: ADE

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

QUESTION 76
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 77
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.

Which interface type and license feature are necessary to meet the requirement?

A. Decryption Mirror interface with the Threat Analysis license
B. Virtual Wire interface with the Decryption Port Export license
C. Tap interface with the Decryption Port Mirror license
D. Decryption Mirror interface with the associated Decryption Port Mirror license

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring

QUESTION 78
When is the content inspection performed in the packet flow process?

A. after the application has been identified
B. before session lookup
C. before the packet forwarding process
D. after the SSL Proxy re-encrypts the packet

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

QUESTION 79
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 80
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection

QUESTION 81
Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

A. Descendant objects will take precedence over other descendant objects.
B. Descendant objects will take precedence over ancestor objects.
C. Ancestor objects will have precedence over descendant objects.
D. Ancestor objects will have precedence over other ancestor objects.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 82
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.

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 83
What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

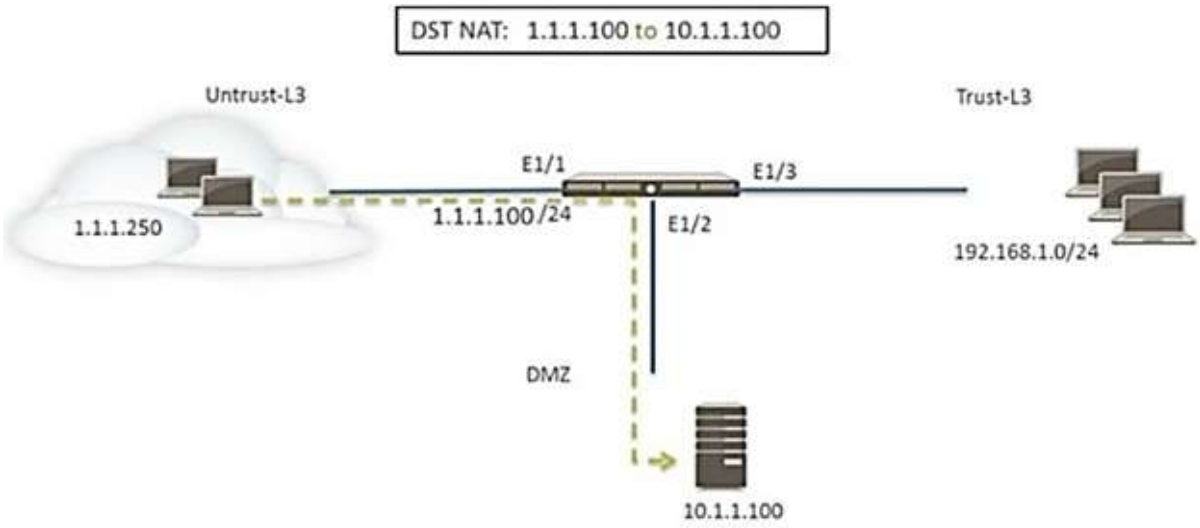
```
admin@Lab33-111-PA-3060(active)> show clock

Thu Jun  8 12:49:55 PDT 2017
#####################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
#####################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
#####################
admin@Lab33-111-PA-3060(active)> show routing fib
id      destination           nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
47      0.0.0.0/0             10.46.40.1         ug     ethernet1/3        1500
67      10.10.20.0/24         0.0.0.0            u      ethernet1/7        1500
66      10.10.20.111/32       0.0.0.0            uh     ethernet1/7        1500
46      10.46.40.0/23         0.0.0.0            u      ethernet1/3        1500
49      10.46.44.0/23         0.0.0.0            u      ethernet1/5        1500
45      10.46.41.111/32       0.0.0.0            uh     ethernet1/3        1500
70      10.46.41.113/32       10.46.40.1         ug     ethernet1/3        1500
48      10.46.45.111/32       0.0.0.0            uh     ethernet1/5        1500
51      192.168.111.0/24      0.0.0.0            u      ethernet1/6        1500
50      192.168.111.2/32      0.0.0.0            uh     ethernet1/6        1500
--------------------------------------------------------------------------------
```

A. ethernet1/7
B. ethernet1/5
C. ethernet1/6
D. ethernet1/3

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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 85
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-http; 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-https; action: allow
   Rule #2: application: ssl; service: application-default; action: allow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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 87
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.

Which solution in PAN-OS® software would help in this case?

A. application override
B. Virtual Wire mode
C. content inspection
D. redistribution of user mappings

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network

QUESTION 88
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-on-kvm/use-an-iso-file-to-deploy-the-vm-series-firewall

QUESTION 89
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 90
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 91
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 92
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 93
The firewall identifies a popular application as an unknown-tcp.

Which two options are available to identify the application? (Choose two.)

A. Create a custom application.
B. Create a custom object for the custom application server to identify the custom application.
C. Submit an Apple-ID request to Palo Alto Networks.
D. Create a Security policy to identify the custom application.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/use-application-objects-in-policy/create-a-custom-application

QUESTION 94
If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

A. TLS Bidirectional Inspection
B. SSL Inbound Inspection
C. SSH Forward Proxy
D. SMTP Inbound Decryption

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 95
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-and-policy-rules/dos-protection-profiles

QUESTION 96
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

A. Verify AutoFocus status using the 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 97
Which CLI command enables an administrator to check the CPU utilization of the dataplane?

A. `show running resource-monitor`
B. `debug data-plane dp-cpu`
C. `show system resources`
D. `debug running resources`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which DoS protection mechanism detects and prevents session exhaustion attacks?

A. Packet Based Attack Protection
B. Flood Protection

C. Resource Protection
D. TCP Port Scan Protection

Correct Answer: C
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-and-policy-rules/dos-protection-profiles

QUESTION 99
Which two subscriptions are available when configuring Panorama to push dynamic updates to connected devices? (Choose two.)

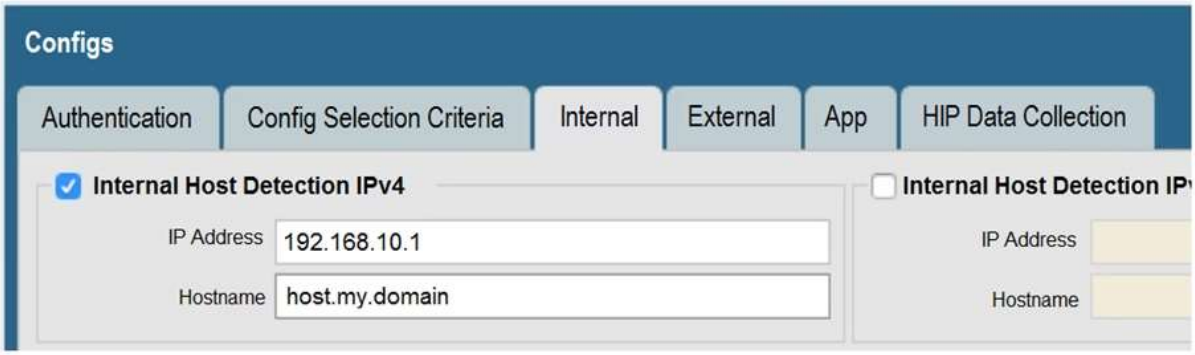
A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus

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 100
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-client-authentication-configurations/define-the-globalprotect-agent-configurations

QUESTION 101
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 102
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 103
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 104
A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation.

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

A. ae.8
B. aggregate.1
C. ae.1
D. aggregate.8

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which three authentication factors does PAN-OS® software support for MFA? (Choose three.)

A. Push
B. Pull
C. Okta Adaptive
D. Voice
E. SMS

Correct Answer: ADE
Section: (none)
Explanation

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

QUESTION 106
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor.

When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. Replay
C. Web Application
D. DoS Protection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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 is reachable using a Destination NAT policy in the Palo Alto Networks firewall.

A. Zone Pair:
Source Zone: Internet
Destination Zone: Internet

Rule Type:
'intrazone'

B. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ

Rule Type:
'interzone' or 'universal'

C. Zone Pair:
Source Zone: Internet
Destination Zone: Internet

Rule Type:
'intrazone' or 'universal'

D. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ

Rule Type:
'intrazone'

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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 109
Which log file can be used to identify SSL decryption failures?

A. Traffic
B. ACC
C. Configuration
D. Threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
A customer wants to set up a site-to-site VPN using tunnel interfaces.

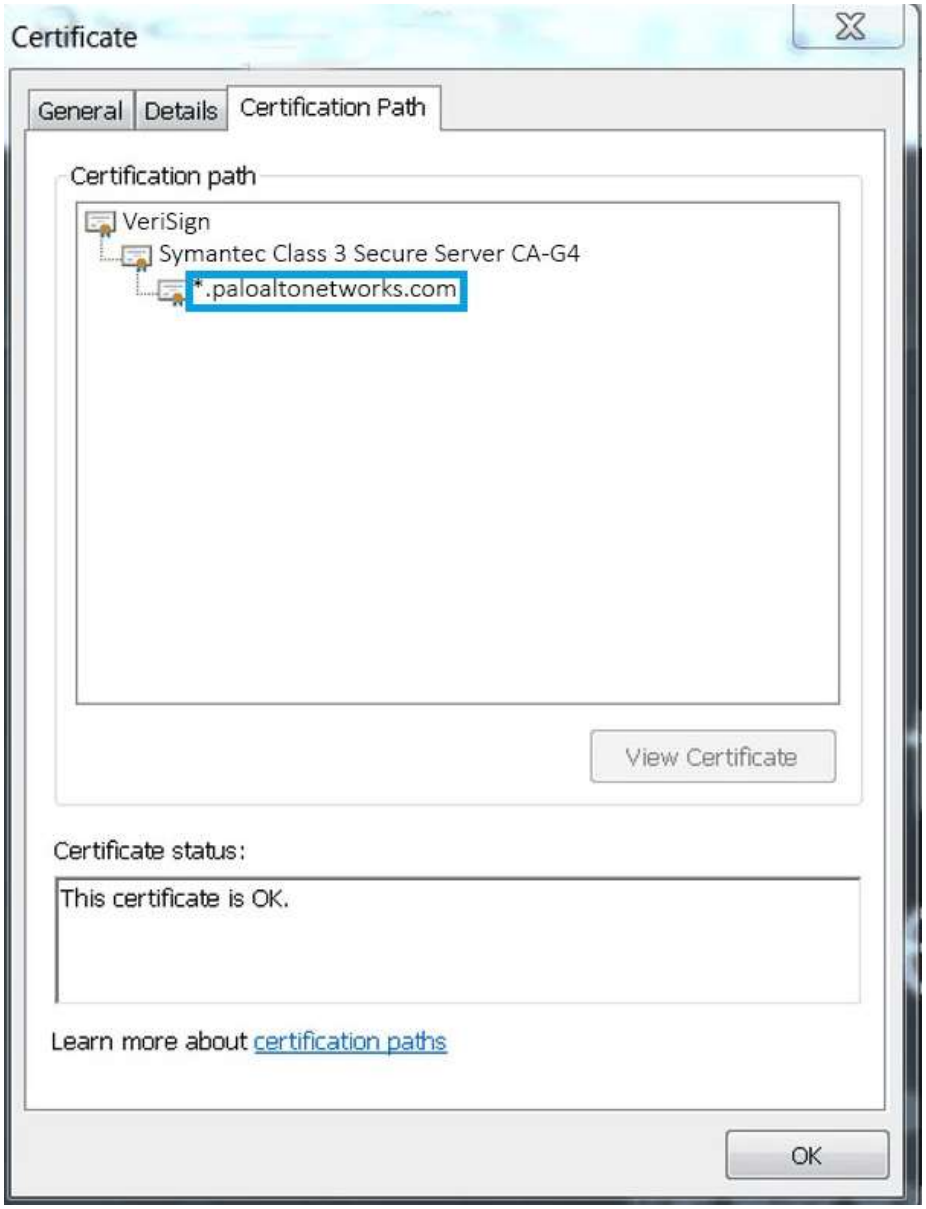
Which two formats are correct for naming tunnel interfaces? (Choose two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Based on the following image, what is the correct path of root, intermediate, and end-user certificate?



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 112
An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet.

Which configuration will enable the firewall to download and install application updates automatically?

A. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
B. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
C. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the update servers goes out of the interface acting as your Internet connection.
D. Configure a Security policy rule to allow all traffic to and from the update servers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
A company wants to install a NGFW firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to 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 114
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall
B. Domain Controller to User-ID agent
C. User-ID agent to Panorama
D. firewall to firewall

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

A. System Utilization log
B. System log
C. Resources widget
D. CPU Utilization widget

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
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 117
Which two features does PAN-OS® software use to identify applications? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.1.0. The firewall is not a part of an HA pair.

What needs to be updated first?

A. Applications and Threats
B. XML Agent
C. WildFire
D. PAN-OS® Upgrade Agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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 120
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two.)

A. HA1 IP Address
B. Master Key
C. Zone Protection Profile
D. Network Interface Type

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge.

What is the expected verdict from WildFire?

A. Malware
B. Grayware
C. Phishing
D. Spyware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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 123
Which operation will impact the 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 124
Which User-ID method maps IP addresses to usernames for users connecting through a web proxy that has already authenticated the user?

A. syslog listening
B. server monitoring
C. client probing
D. port mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
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 126
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

A. At-boot
B. Pre-logon
C. User-logon (Always on)
D. On-demand

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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 128
Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)

A. Role Based
B. Custom Panorama Admin

C. Device Group
D. Dynamic
E. Template Admin

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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 130
Which is the maximum number of samples that can be submitted to WildFire per day, based on a WildFire subscription?

A. 10,000
B. 15,000
C. 7,500
D. 5,000

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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 132
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 133
Which logs enable a firewall administrator to determine whether a session was decrypted?

A. Traffic
B. Security Policy
C. Decryption
D. Correlated Event

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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 135
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 136
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-ha-firewall-pair-to-pan-os-80

QUESTION 137
A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.

Which Security Profile type will prevent these behaviors?

A. Anti-Spyware
B. WildFire
C. Vulnerability Protection
D. Antivirus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles

QUESTION 138
What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations

QUESTION 139
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

A. CRL
B. CRT
C. OCSP
D. Cert-Validation-Profile
E. SSL/TLS Service Profile

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/certificate-management/set-up-verification-for-certificate-revocation-status

QUESTION 140
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 141
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

A. .dll
B. .exe
C. .fon
D. .apk
E. .pdf
F. .jar

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
C. The firewalls do not use floating IPs in active/active HA.
D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/floating-ip-address-and-virtual-mac-address

QUESTION 143
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4_1/split-tunnel-for-public-applications

QUESTION 144
How does Panorama prompt VMWare NSX to quarantine an infected VM?

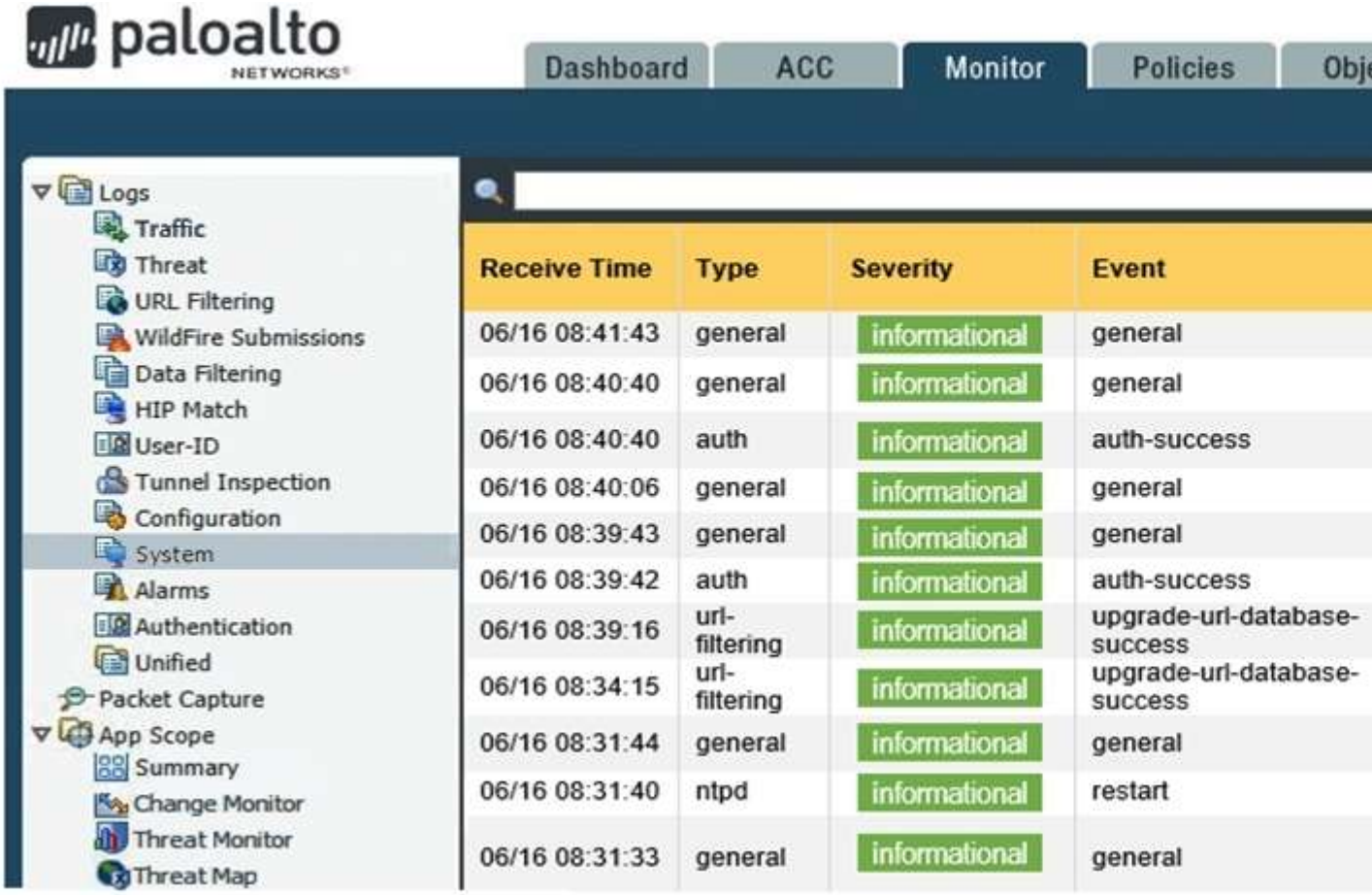
A. HTTP Server Profile
B. Syslog Server Profile
C. Email Server Profile
D. SNMP Server Profile

Correct Answer: A
Section: (none)
Explanation

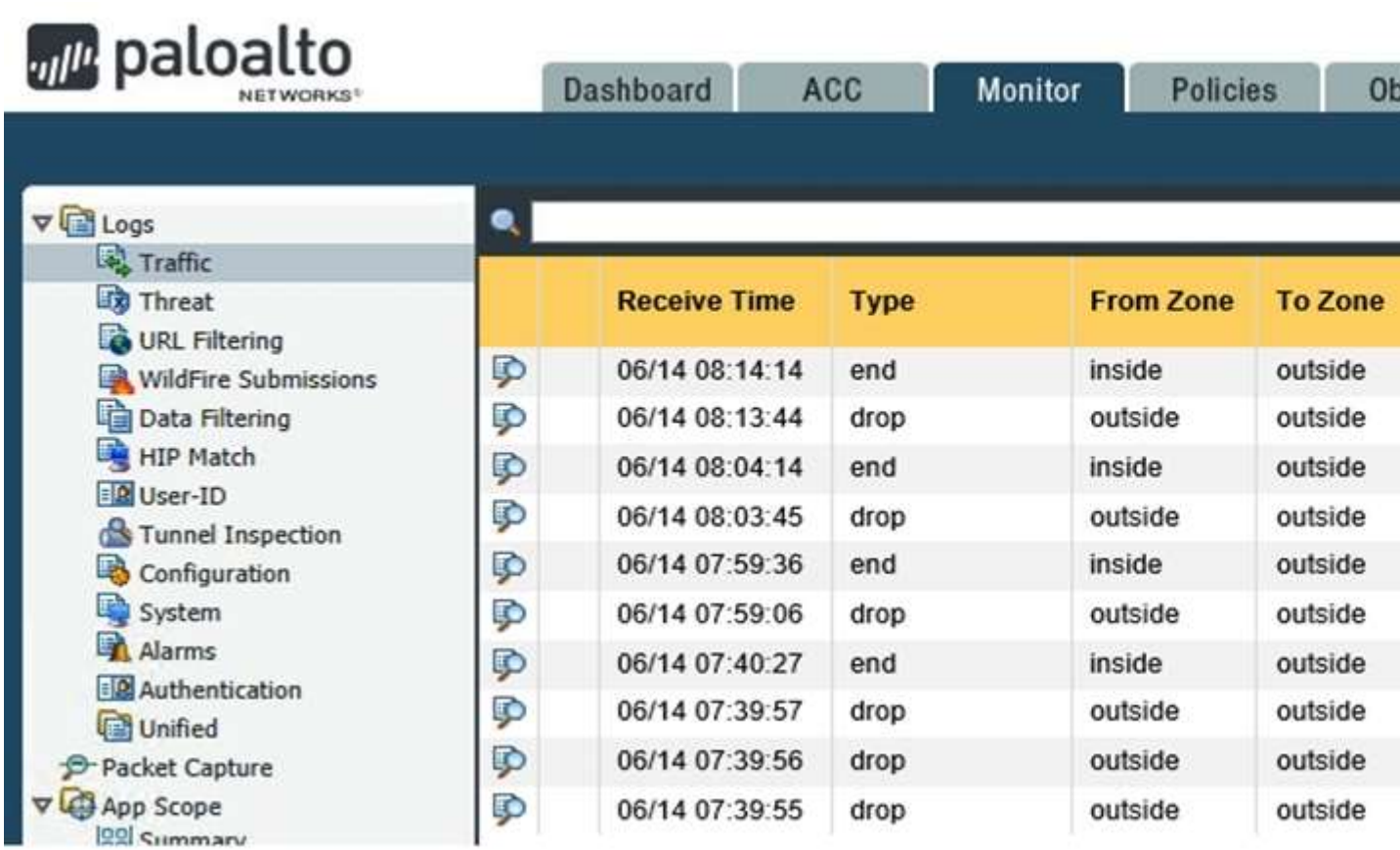
Explanation/Reference:
Reference: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected-guests

QUESTION 145
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.

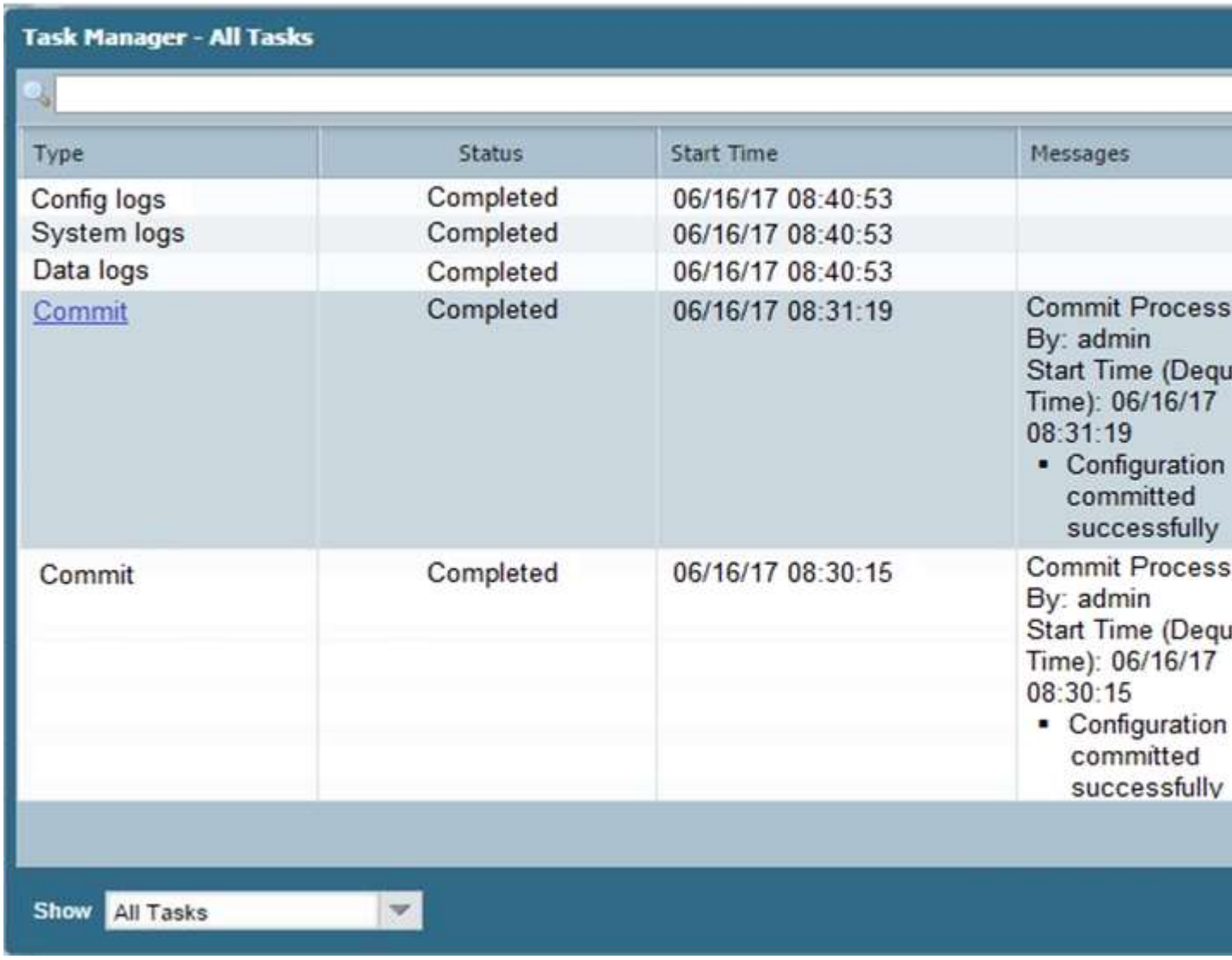


B.



C.

D.



Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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 147
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 per 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-network-security/configure-packet-buffer-protection

QUESTION 148
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 149
SAML SLO is supported for which two firewall features? (Choose two.)

A. GlobalProtect Portal
B. CaptivePortal
C. WebUI
D. CLI

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 150
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 151
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 152
In the following image from Panorama, why are some values shown in red?

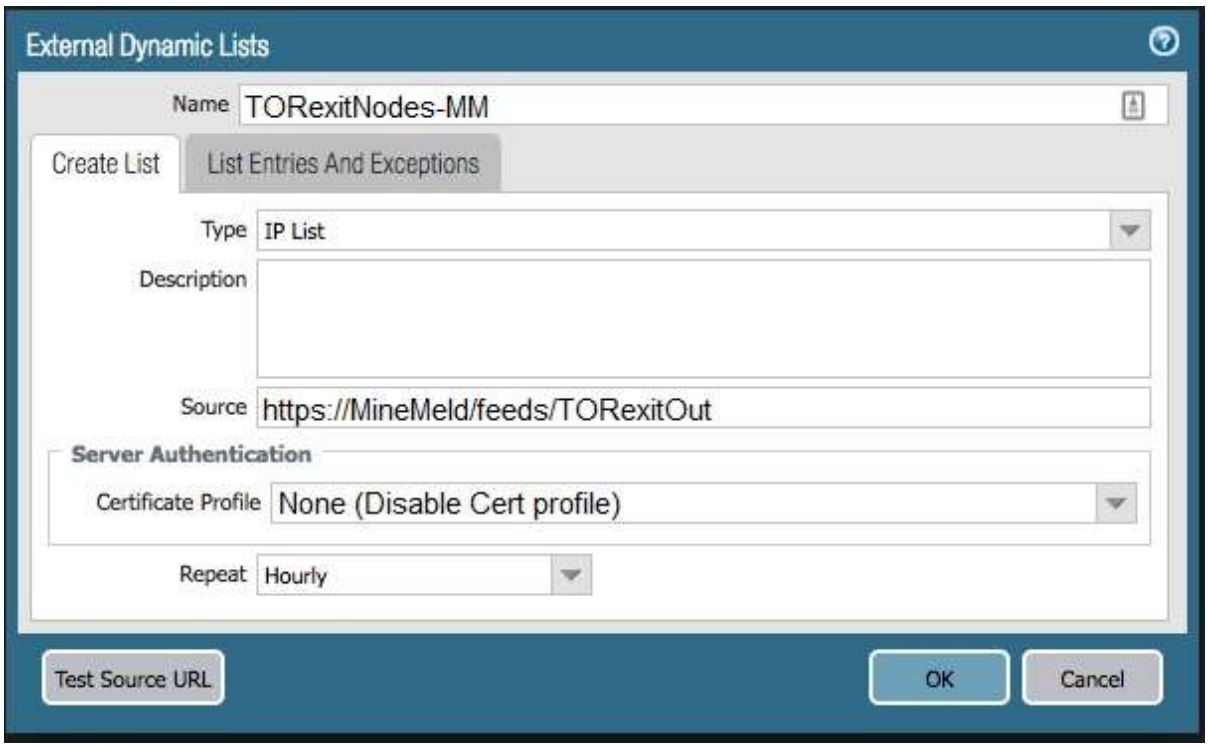
Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

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 153
The firewall is not downloading IP addresses from MineMeld. Based on the image, what most likely is wrong?



A. A Certificate Profile that contains the client certificate needs to be selected.
B. The source address supports only files hosted with an ftp://<address/file>.
C. External Dynamic Lists do not support SSL connections.
D. A Certificate Profile that contains the CA certificate needs to be selected.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://live.paloaltonetworks.com/t5/MineMeld-Articles/Connecting-PAN-OS-to-MineMeld-using-External-Dynamic-Lists/ta-p/190414

QUESTION 154
Which three split tunnel methods are supported by a GlobalProtect Gateway? (Choose three.)

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

QUESTION 155
Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two.)

A. Successful GlobalProtect Deployed Activity
B. GlobalProtect Deployment Activity
C. Successful GlobalProtect Connection Activity
D. GlobalProtect Quarantine Activity

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html

QUESTION 156
Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

A. log forwarding auto-tagging
B. XML API
C. GlobalProtect agent
D. User-ID Windows-based agent

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html

QUESTION 157
SD-WAN is designed to support which two network topology types? (Choose two.)

A. point-to-point

B. hub-and-spoke
C. full-mesh
D. ring

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which option describes the operation of the automatic commit recovery feature?

A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html

QUESTION 159
Which three items are important considerations during SD-WAN configuration planning? (Choose three.)

A. branch and hub locations
B. link requirements
C. the name of the ISP
D. IP Addresses

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration

QUESTION 160
Starting with PAN-OS version 9.1, application dependency information is now reported in which two new locations? (Choose two.)

A. on the **App Dependency** tab in the **Commit Status** window
B. on the Policy Optimizer's **Rule Usage** page
C. on the **Application** tab in the **Security Policy Rule** creation window
D. on the **Objects > Applications** browser pages

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies

QUESTION 161
Which two events trigger the operation of automatic commit recovery? (Choose two.)

A. when an aggregate Ethernet interface component fails
B. when Panorama pushes a configuration
C. when a firewall performs a local commit
D. when a firewall HA pair fails over

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html

QUESTION 162
Panorama provides which two SD-WAN functions? (Choose two.)

A. network monitoring
B. control plane
C. data plane
D. physical network links

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference: