



Paloalto-Networks

Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 8.0

NEW QUESTION 1

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

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

Answer: AB

NEW QUESTION 2

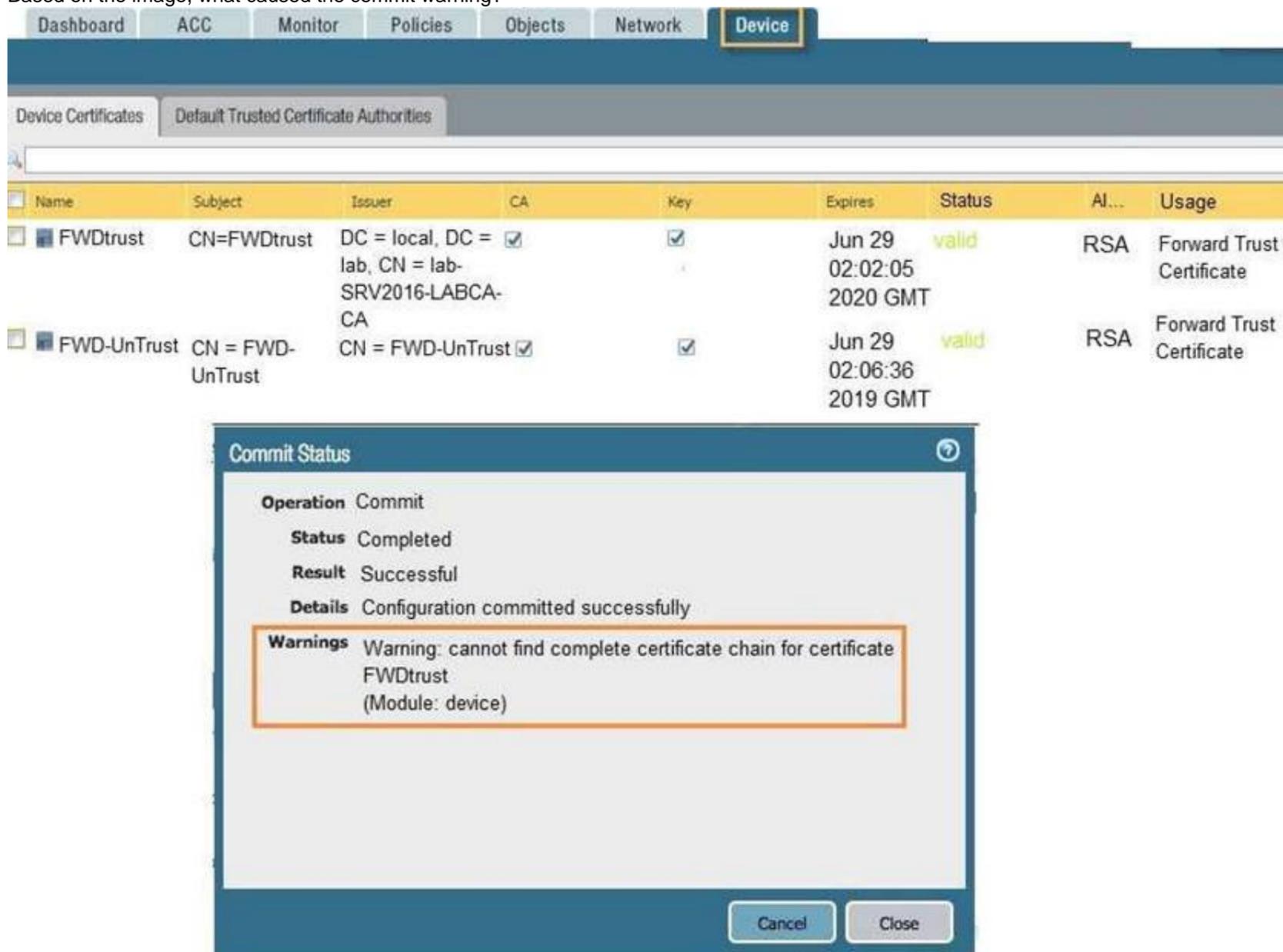
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category

Answer: ABC

NEW QUESTION 3

Based on the image, what caused the commit warning?



The screenshot shows the Palo Alto Networks GUI with the 'Device' tab selected. Under 'Device Certificates', there are two certificates listed:

Name	Subject	Issuer	CA	Key	Expires	Status	Al...	Usage
FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

Below the table, a 'Commit Status' dialog box is open, showing the following details:

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Configuration committed successfully
- Warnings:** Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

- 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.

Answer: D

NEW QUESTION 4

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

Answer: A

NEW QUESTION 5

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

Answer: AC

NEW QUESTION 6

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

Answer: B

NEW QUESTION 7

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

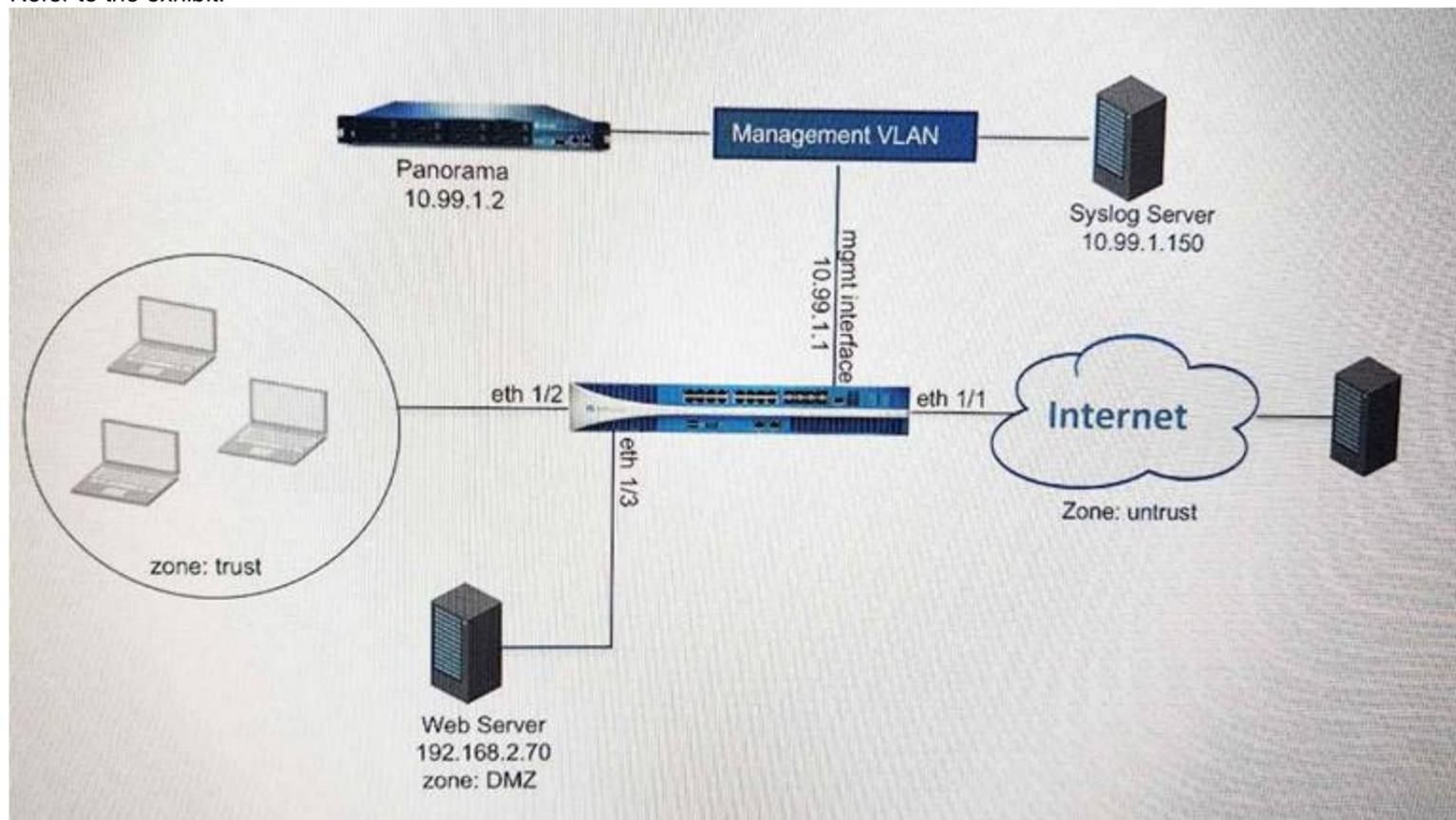
Answer: AB

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d>

NEW QUESTION 8

Refer to the exhibit.



An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side.

Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

A)

Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Secure Client Communication

Certificate Type None

Check Server Identity

B)

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action Allow

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None

Profile Setting

Profile Type Profiles

Antivirus None

Vulnerability Protection None

Anti-Spyware None

URL Filtering Filter1

File Blocking None

Data Filtering None

WildFire Analysis None

Other Settings

Schedule None

QoS Marking None

Disable Server Response Inspection

OK Cancel

C)

Syslog Server Profile

Name SyslogProfile1

Servers Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

+ Add - Delete

D)

Panorama Settings

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

Share Unused Address and Service Objects with Devices

Objects defined in ancestors will take higher precedence

Secure Server Communication

Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

Identifier	Type	Value
0 items		

Authorize Clients Based on Serial Number

Check Authorization List

Connect Wait Time (min) [0 - 44640]

OK

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

Answer: D

NEW 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

Answer: C

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/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

NEW QUESTION 10

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

Answer: D

Explanation:

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

NEW QUESTION 10

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.

Answer: A

NEW QUESTION 14

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

Answer: BD

Explanation:

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

NEW QUESTION 15

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

Answer: B

NEW QUESTION 17

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 to 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.

Answer: C

NEW QUESTION 22

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 from the Shared group
- D. Overwrites local firewall configuration

Answer: BC

NEW 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

Answer: C

NEW QUESTION 26

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

Answer: B

Explanation:

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

NEW QUESTION 27

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. Redistribution of user mappings
- C. Virtual Wire mode
- D. Content inspection

Answer: B

NEW QUESTION 30

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.

Answer: D

Explanation:

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

NEW QUESTION 34

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

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and-users>

NEW QUESTION 37

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.

Answer: B

NEW QUESTION 42

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

Answer: ABC

NEW QUESTION 46

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. DoS Protection
- C. Web Application

D. Replay

Answer: A

NEW QUESTION 47

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. src
- D. apk
- E. pdf
- F. jar

Answer: DEF

Explanation:

Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

NEW QUESTION 51

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 53

If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 58

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.

Answer: D

NEW QUESTION 62

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

Answer: A

NEW QUESTION 63

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

Answer: B

Explanation:

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

NEW QUESTION 64

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.

Answer: CDE

NEW QUESTION 65

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.

Answer: D

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewall-configurations

NEW QUESTION 70

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

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. TLS Bidirectional proxy
- D. SSL Outbound Inspection

Answer: A

NEW QUESTION 75

An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are from 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.

Answer: A

NEW QUESTION 79

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.

Answer: CD

NEW QUESTION 81

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.

Answer: AB

NEW QUESTION 86

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

Answer: A

Explanation:

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

NEW QUESTION 87

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

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

NEW QUESTION 89

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.

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management>

NEW QUESTION 94

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:
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
```

#####

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?

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

Answer: D

NEW QUESTION 97

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.

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html>

NEW QUESTION 98

Which feature can be configured on VM-Series firewalls?

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

Answer: D

NEW QUESTION 103

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

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links>

NEW QUESTION 104

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. 5-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Protocol
- B. 7-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Source User, URL Category and Source Security Zone.
- C. 6-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Protocol and Source Security Zone
- D. 9-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application and URL Category

Answer: A

NEW QUESTION 109

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

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

Answer: C

NEW QUESTION 111

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

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

Answer: C

NEW QUESTION 114

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 e1/1.
- 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. DNS settings for the firewall to use for resolution
- B. scheduler for timed downloads of PAN-OS software
- C. static route pointing application PaloAlto-updates to the update servers
- D. Security policy rule allowing PaloAlto-updates as the application

Answer: D

NEW QUESTION 118

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. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interface destined for the update servers goes out of the interface acting as your internet connection.
- B. Configure a security policy rule to allow all traffic to and from the update servers.
- C. Download and install application updates cannot be done automatically if the MGT port cannot reach the internet.
- D. 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.

Answer: B

NEW QUESTION 119

An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

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

Answer: B

NEW QUESTION 121

Which operation will impact the performance of the management plane?

- A. WildFire Submissions
- B. DoS Protection
- C. decrypting SSL Sessions
- D. Generating a SaaS Application Report.

Answer: C

NEW QUESTION 125

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

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

Answer: A

NEW QUESTION 127

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

Answer: C

NEW QUESTION 128

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

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

D. System Utilization log

Answer: C

NEW QUESTION 133

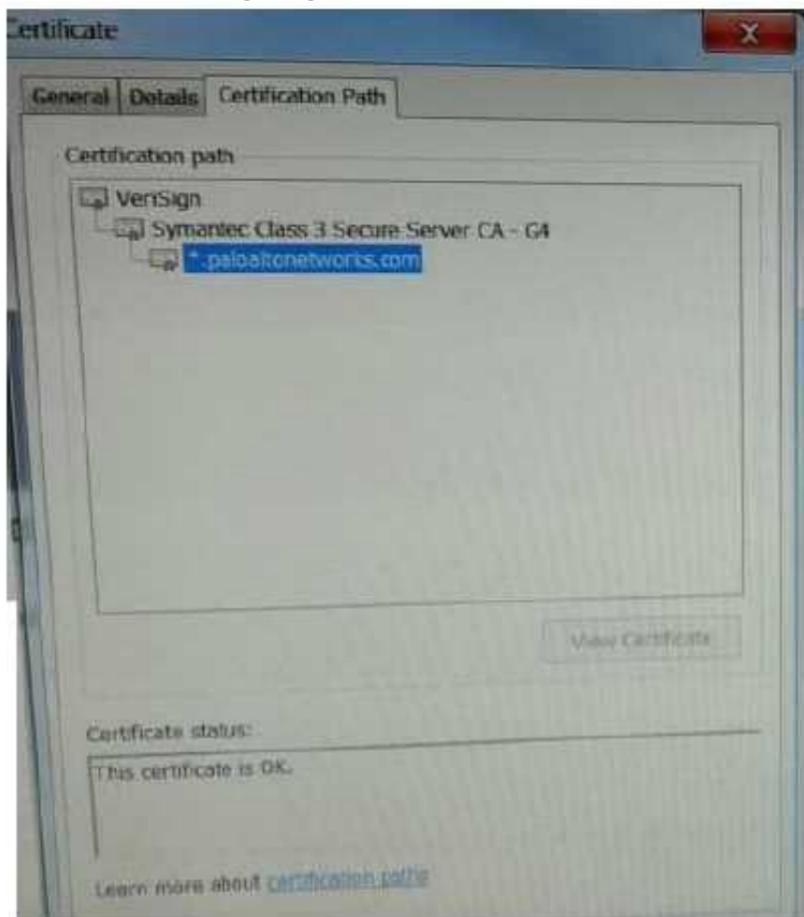
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

- A. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group E.Template Admin

Answer: DE

NEW QUESTION 137

Based on the following image,



what is the correct path of root, intermediate, and end-user certificate?

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

Answer: D

NEW QUESTION 138

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.

Virtual Router - OSPF - Area						
Area ID		0.0.0.0				
Type	Range	Interface	Virtual Link			
<input type="checkbox"/>		Enable	Passive	Link Type	Metric	Priority
<input type="checkbox"/>	tunnel.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1
<input type="checkbox"/>	ethernet1/21	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1

Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp

F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 141

A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk. What action will bring the VPN up and allow traffic to start passing between the sites?

- A. Change the Site-B IKE Gateway profile version to match Site-A,
- B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
- C. Enable NAT Traversal on the Site-A IKE Gateway profile.
- D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

NEW QUESTION 143

A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.

Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

- A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
- B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
- C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
- D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
- E. Download and install PAN-OS 8.0.4 directly on each firewall.
- F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

Answer: ACF

NEW QUESTION 146

A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

- A. Panorama virtual appliance on ESX(i) only
- B. M-500
- C. M-100 with Panorama installed
- D. M-100

Answer: BC

Explanation:

(<https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181>)

NEW QUESTION 149

Which two mechanisms help prevent a split brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

- A. Configure the management interface as HA3 Backup
- B. Configure Ethernet 1/1 as HA1 Backup
- C. Configure Ethernet 1/1 as HA2 Backup
- D. Configure the management interface as HA2 Backup
- E. Configure the management interface as HA1 Backup
- F. Configure ethernet1/1 as HA3 Backup

Answer: BE

NEW QUESTION 150

How is the Forward Untrust Certificate used?

- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
- D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 153

Which command can be used to validate a Captive Portal policy?

- A. eval captive-portal policy <criteria>
- B. request cp-policy-eval <criteria>
- C. test cp-policy-match <criteria>
- D. debug cp-policy <criteria>

Answer: C

NEW QUESTION 158

A company has a pair of Palo Alto Networks firewalls configured as an Active/Passive High Availability (HA) pair. What allows the firewall administrator to determine the last date a failover event occurred?

- A. From the CLI issue use the show System log
- B. Apply the filter subtype eq ha to the System log
- C. Apply the filter subtype eq ha to the configuration log
- D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 160

A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled. Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment?

- A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
- B. File Blocking profiles applied to outbound security policies with action set to alert
- C. Vulnerability Protection profiles applied to outbound security policies with action set to block
- D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

NEW QUESTION 164

How does Panorama handle incoming logs when it reaches the maximum storage capacity?

- A. Panorama discards incoming logs when storage capacity full.
- B. Panorama stops accepting logs until licenses for additional storage space are applied
- C. Panorama stops accepting logs until a reboot to clean storage space.
- D. Panorama automatically deletes older logs to create space for new ones.

Answer: D

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/determine-panorama-log-storage-requirements)

NEW QUESTION 169

Only two Trust to Untrust rules have been created in the Security policy Rule1 allows google-base Rule2 allows youtube-base

The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to access <https://www.youtube.com> in a web browser, they get an error indicating that the server cannot be found. Which action will allow youtube.com display in the browser correctly?

- A. Add SSL App-ID to Rule1
- B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
- C. Add the DNS App-ID to Rule2
- D. Add the Web-browsing App-ID to Rule2

Answer: C

NEW QUESTION 173

Which three options are available when creating a security profile? (Choose three)

- A. Anti-Malware
- B. File Blocking
- C. Url Filtering
- D. IDS/IPS
- E. Threat Prevention
- F. Antivirus

Answer: ABF

NEW QUESTION 175

Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

- A. Vulnerability Object
- B. DoS Protection Profile
- C. Data Filtering Profile
- D. Zone Protection Profile

Answer: BD

NEW QUESTION 176

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine. Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

- A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
- B. Wait until an official Application signature is provided from Palo Alto Networks.
- C. Modify the session timer settings on the closest referenced application to meet the needs of the in-house application
- D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 177

A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible from the Monitor tab. What could cause this condition?

- A. The firewall does not have an active WildFire subscription.
- B. The engineer's account does not have permission to view WildFire Submissions.
- C. A policy is blocking WildFire Submission traffic.
- D. Though WildFire is working, there are currently no WildFire Submissions log entries.

Answer: B

NEW QUESTION 182

Click the Exhibit button below,

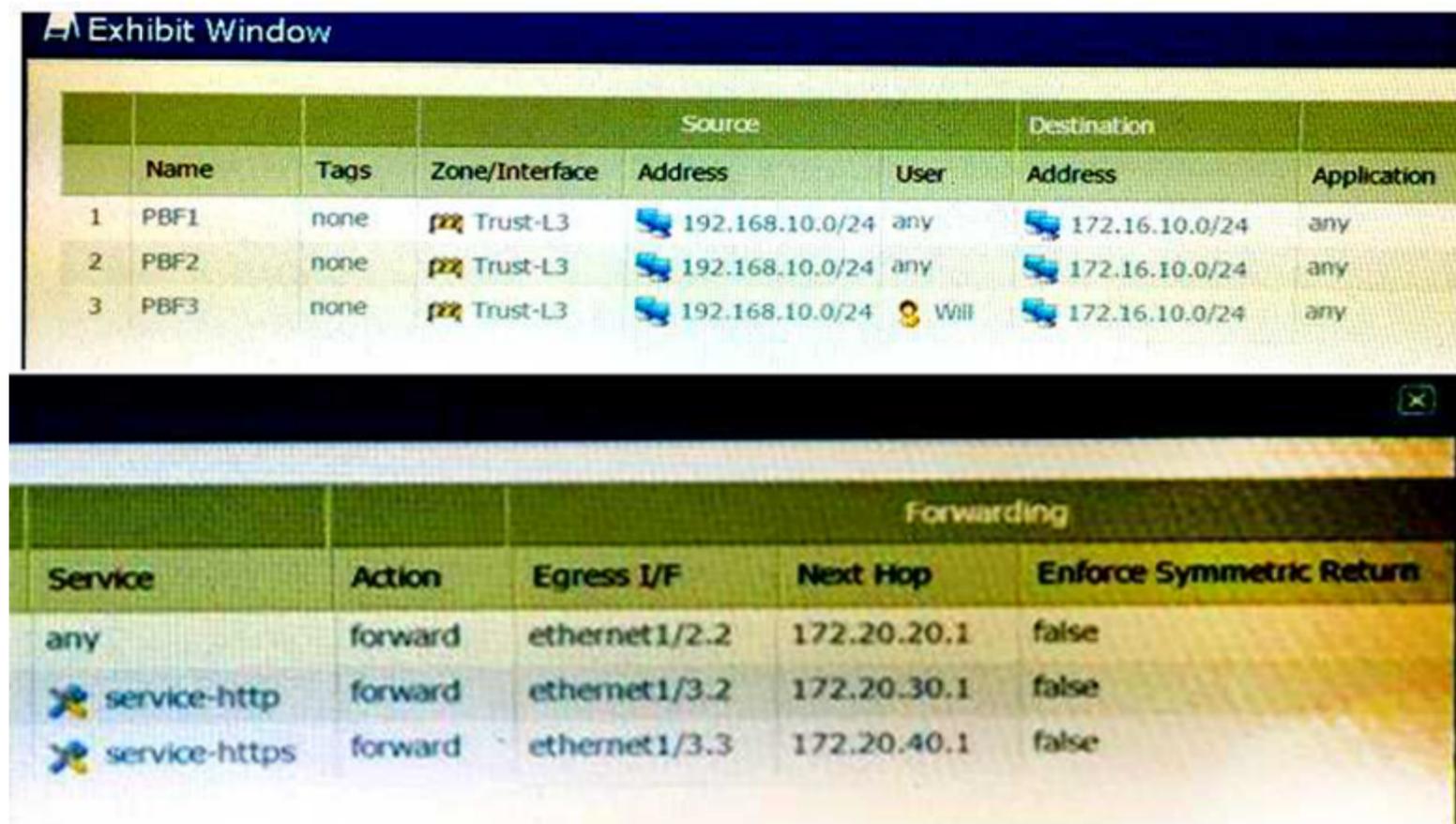


Exhibit Window							
		Source			Destination		
	Name	Tags	Zone/Interface	Address	User	Address	Application
1	PBF1	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
2	PBF2	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
3	PBF3	none	Trust-L3	192.168.10.0/24	Will	172.16.10.0/24	any

Forwarding				
Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return
any	forward	ethernet1/2.2	172.20.20.1	false
service-http	forward	ethernet1/3.2	172.20.30.1	false
service-https	forward	ethernet1/3.3	172.20.40.1	false

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20. Which is the next hop IP address for the HTTPS traffic from Will's PC?

- A. 172.20.30.1
- B. 172.20.40.1
- C. 172.20.20.1
- D. 172.20.10.1

Answer: C

NEW QUESTION 183

What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

- A. Clean
- B. Benign
- C. Adware
- D. Suspicious
- E. Grayware
- F. Malware

Answer: BEF

Explanation:

[https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK \"https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict\"/os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict](https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK \)

NEW QUESTION 185

What can missing SSL packets when performing a packet capture on dataplane interfaces?

- A. The packets are hardware offloaded to the offloaded processor on the dataplane
- B. The missing packets are offloaded to the management plane CPU
- C. The packets are not captured because they are encrypted
- D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 190

A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.
- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 191

The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalProtect Portal?

- A. Server Certificate
- B. Client Certificate
- C. Authentication Profile
- D. Certificate Profile

Answer: A

Explanation:

(<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351>)

NEW QUESTION 193

Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)

- A. Virtual Wire
- B. Loopback
- C. Layer 3
- D. Tunnel

Answer: BC

NEW QUESTION 198

After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

- A. A Server Profile has not been configured for logging to this Panorama device.
- B. Panorama is not licensed to receive logs from this particular firewall.
- C. The firewall is not licensed for logging to this Panorama device.
- D. None of the firewall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 203

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing. All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface. Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag
- C. Layer 2 interface type with a VLAN assigned
- D. Layer 3 subinterface type with specified tag

Answer: D

NEW QUESTION 204

Firewall administrators cannot authenticate to a firewall GUI.

Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

- A. ms log
- B. authd log
- C. System log
- D. Traffic log
- E. dp-monitor .log

Answer:

BC

NEW QUESTION 205

A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.

Which configuration setting needs to be modified?

- A. Service route
- B. Default route
- C. Management profile
- D. Authentication profile

Answer: A

NEW QUESTION 206

Which URL Filtering Security Profile action tags the URL Filtering category to the URL Filtering log?

- A. Log
- B. Alert
- C. Allow
- D. Default

Answer: B

NEW QUESTION 211

Which three rule types are available when defining policies in Panorama? (Choose three.)

- A. Pre Rules
- B. Post Rules
- C. Default Rules
- D. Stealth Rules
- E. Clean Up Rules

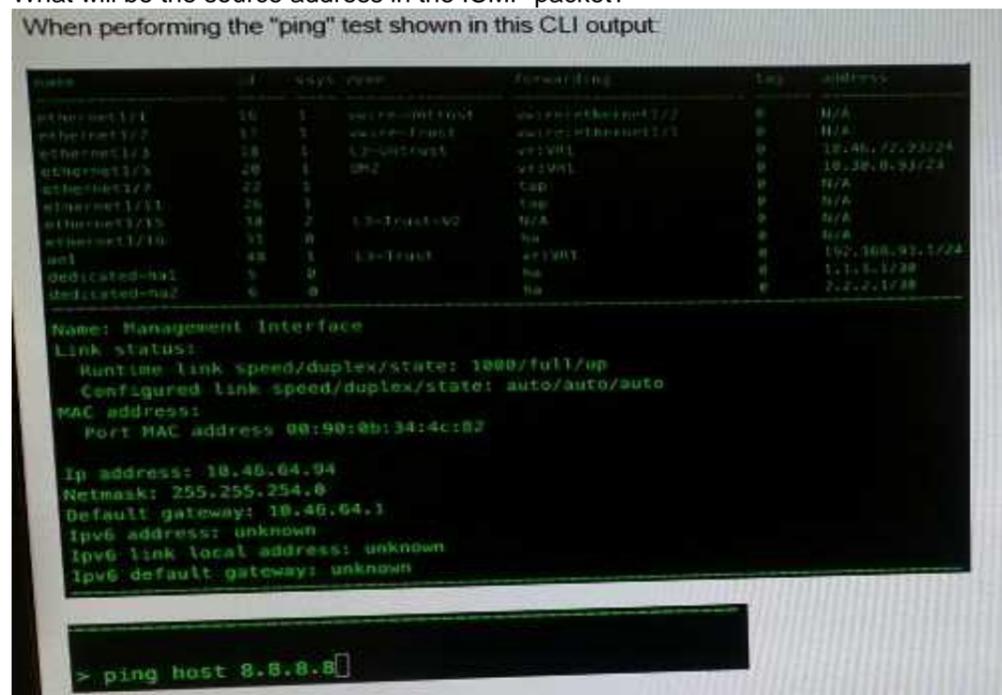
Answer: ABC

Explanation:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defining-policies-on-panorama>
<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defining-policies-on-panorama>

NEW QUESTION 215

What will be the source address in the ICMP packet?



- A. 10.30.0.93
- B. 10.46.72.93
- C. 10.46.64.94
- D. 192.168.93.1

Answer: C

NEW QUESTION 216

Which CLI command displays the current management plane memory utilization?

- A. > debug management-server show

- B. > show running resource-monitor
- C. > show system info
- D. > show system resources

Answer: D

Explanation:

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux." <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

NEW QUESTION 221

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

- A. Enable support for non-standard syslog messages under device management
- B. Check the custom-format check box in the syslog server profile
- C. Select a non-standard syslog server profile
- D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 223

A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.

What should be done first?

- A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
- B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
- C. remove the device from the Collector Group
- D. Revert to a previous configuration

Answer: C

NEW QUESTION 228

Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

- A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
- B. Enable User-ID on the zone object for the destination zone
- C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
- D. Enable User-ID on the zone object for the source zone
- E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 229

An administrator is configuring an IPsec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:

```
less mp-log ikemgr.log:
2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:52:33 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====> Due to
timeout.
2014-08-05 03:52:33 [INFO]: <====> PHASE-1 SA DELETED <====>
<====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====>
2014-08-05 03:53:54 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====> Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====>
```

What could be the cause of this problem?

- A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
- C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

Answer: C

NEW QUESTION 231

.....

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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

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

Answer: AB

NEW QUESTION 2

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

Answer: ABC

NEW QUESTION 3

Based on the image, what caused the commit warning?

The screenshot shows the Palo Alto Networks GUI with the 'Device' tab selected. Under 'Device Certificates', there are two certificates listed:

Name	Subject	Issuer	CA	Key	Expires	Status	Al...	Usage
FWDtrust	CN=FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Trust Certificate

Below the table, a 'Commit Status' dialog box is open, showing the following details:

- Operation:** Commit
- Status:** Completed
- Result:** Successful
- Details:** Configuration committed successfully
- Warnings:** Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

- 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.

Answer: D

NEW QUESTION 4

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

Answer: A

NEW QUESTION 5

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

Answer: AC

NEW QUESTION 6

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

Answer: B

NEW QUESTION 7

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

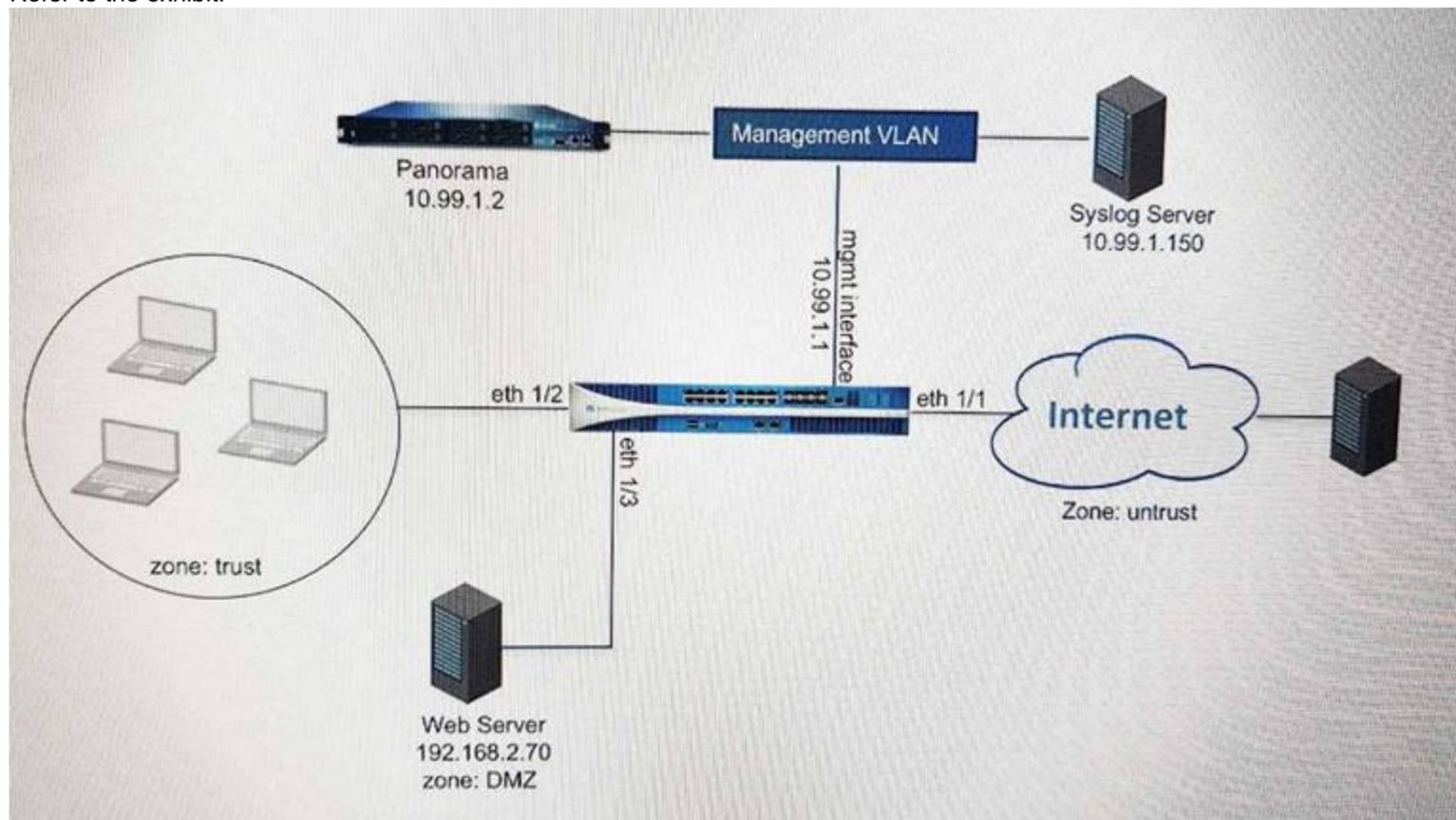
Answer: AB

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd-8064499f5b9d>

NEW QUESTION 8

Refer to the exhibit.



An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side. Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?

A)

Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Secure Client Communication

Certificate Type None

Check Server Identity

B)

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action Allow

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding None

Profile Setting

Profile Type Profiles

Antivirus None

Vulnerability Protection None

Anti-Spyware None

URL Filtering Filter1

File Blocking None

Data Filtering None

WildFire Analysis None

Other Settings

Schedule None

QoS Marking None

Disable Server Response Inspection

OK Cancel

C)

Syslog Server Profile

Name SyslogProfile1

Servers Custom Log Format

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

+ Add - Delete

D)

Panorama Settings

Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

Share Unused Address and Service Objects with Devices

Objects defined in ancestors will take higher precedence

Secure Server Communication

Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

Identifier	Type	Value
0 items		

Authorize Clients Based on Serial Number

Check Authorization List

Connect Wait Time (min) [0 - 44640]

OK

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

Answer: D

NEW 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

Answer: C

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/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

NEW QUESTION 10

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

Answer: D

Explanation:

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

NEW QUESTION 10

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.

Answer: A

NEW QUESTION 14

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

Answer: BD

Explanation:

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

NEW QUESTION 15

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

Answer: B

NEW QUESTION 17

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 to 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.

Answer: C

NEW QUESTION 22

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 from the Shared group
- D. Overwrites local firewall configuration

Answer: BC

NEW 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

Answer: C

NEW QUESTION 26

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

Answer: B

Explanation:

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

NEW QUESTION 27

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. Redistribution of user mappings
- C. Virtual Wire mode
- D. Content inspection

Answer: B

NEW QUESTION 30

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.

Answer: D

Explanation:

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

NEW QUESTION 34

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

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and-users>

NEW QUESTION 37

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.

Answer: B

NEW QUESTION 42

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

Answer: ABC

NEW QUESTION 46

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. DoS Protection
- C. Web Application

D. Replay

Answer: A

NEW QUESTION 47

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. src
- D. apk
- E. pdf
- F. jar

Answer: DEF

Explanation:

Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

NEW QUESTION 51

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 53

If the firewall is configured for credential phishing prevention using the “Domain Credential Filter” method, which login will be detected as credential theft?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 58

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.

Answer: D

NEW QUESTION 62

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

Answer: A

NEW QUESTION 63

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

Answer: B

Explanation:

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

NEW QUESTION 64

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.

Answer: CDE

NEW QUESTION 65

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.

Answer: D

Explanation:

Reference:

https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewall-configurations

NEW QUESTION 70

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

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. TLS Bidirectional proxy
- D. SSL Outbound Inspection

Answer: A

NEW QUESTION 75

An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are from 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.

Answer: A

NEW QUESTION 79

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.

Answer: CD

NEW QUESTION 81

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.

Answer: AB

NEW QUESTION 86

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

Answer: A

Explanation:

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

NEW QUESTION 87

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

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

NEW QUESTION 89

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.

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management>

NEW QUESTION 94

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:
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	

#####

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?

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

Answer: D

NEW QUESTION 97

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.

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html>

NEW QUESTION 98

Which feature can be configured on VM-Series firewalls?

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

Answer: D

NEW QUESTION 103

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

Answer: A

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links>

NEW QUESTION 104

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. 5-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Protocol
- B. 7-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Source User, URL Category and Source Security Zone.
- C. 6-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Protocol and Source Security Zone
- D. 9-tuple matchSource IP Address, Destination IP Address, Source Port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application and URL Category

Answer: A

NEW QUESTION 109

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

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

Answer: C

NEW QUESTION 111

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

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

Answer: C

NEW QUESTION 114

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 e1/1.
- 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. DNS settings for the firewall to use for resolution
- B. scheduler for timed downloads of PAN-OS software
- C. static route pointing application PaloAlto-updates to the update servers
- D. Security policy rule allowing PaloAlto-updates as the application

Answer: D

NEW QUESTION 118

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. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interface destined for the update servers goes out of the interface acting as your internet connection.
- B. Configure a security policy rule to allow all traffic to and from the update servers.
- C. Download and install application updates cannot be done automatically if the MGT port cannot reach the internet.
- D. 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.

Answer: B

NEW QUESTION 119

An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

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

Answer: B

NEW QUESTION 121

Which operation will impact the performance of the management plane?

- A. WildFire Submissions
- B. DoS Protection
- C. decrypting SSL Sessions
- D. Generating a SaaS Application Report.

Answer: C

NEW QUESTION 125

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

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

Answer: A

NEW QUESTION 127

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

Answer: C

NEW QUESTION 128

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

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

D. System Utilization log

Answer: C

NEW QUESTION 133

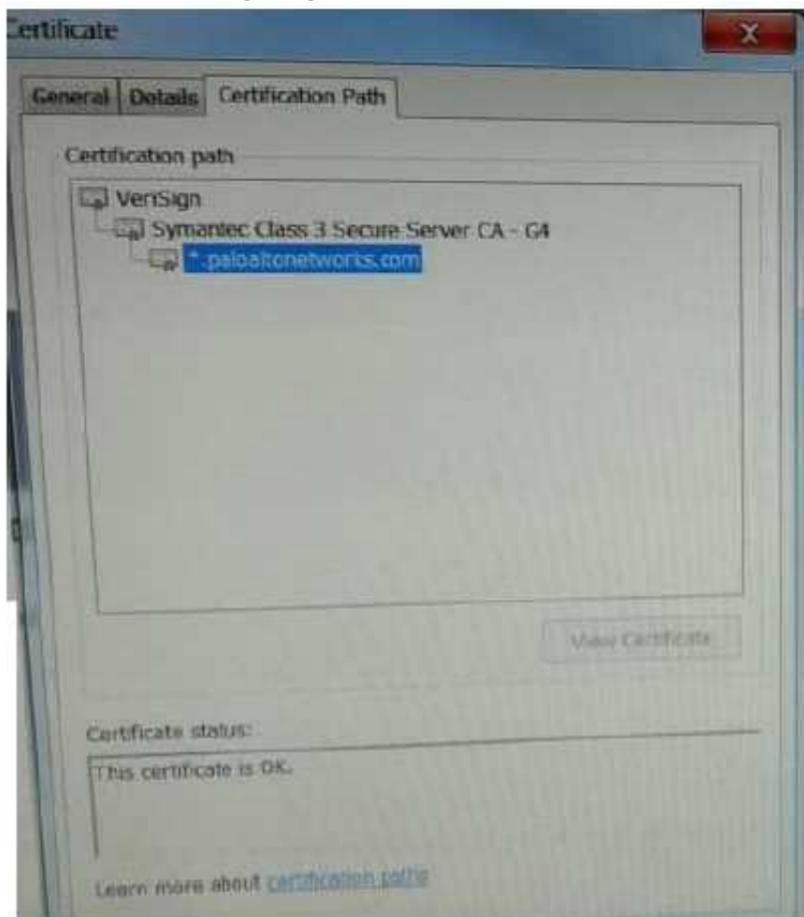
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

- A. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group E.Template Admin

Answer: DE

NEW QUESTION 137

Based on the following image,



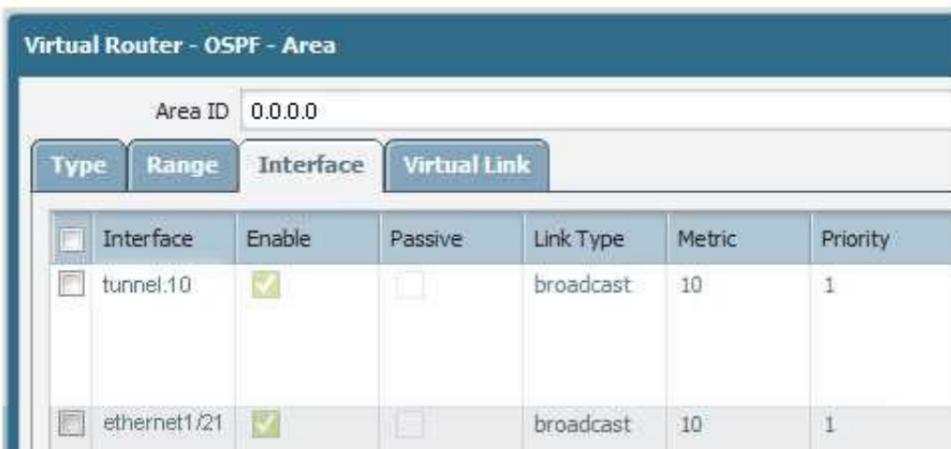
what is the correct path of root, intermediate, and end-user certificate?

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

Answer: D

NEW QUESTION 138

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.



Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp

F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 141

A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk. What action will bring the VPN up and allow traffic to start passing between the sites?

- A. Change the Site-B IKE Gateway profile version to match Site-A,
- B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
- C. Enable NAT Traversal on the Site-A IKE Gateway profile.
- D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

NEW QUESTION 143

A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.

Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

- A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
- B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
- C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
- D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
- E. Download and install PAN-OS 8.0.4 directly on each firewall.
- F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

Answer: ACF

NEW QUESTION 146

A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

- A. Panorama virtual appliance on ESX(i) only
- B. M-500
- C. M-100 with Panorama installed
- D. M-100

Answer: BC

Explanation:

(<https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181>)

NEW QUESTION 149

Which two mechanisms help prevent a split brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

- A. Configure the management interface as HA3 Backup
- B. Configure Ethernet 1/1 as HA1 Backup
- C. Configure Ethernet 1/1 as HA2 Backup
- D. Configure the management interface as HA2 Backup
- E. Configure the management interface as HA1 Backup
- F. Configure ethernet1/1 as HA3 Backup

Answer: BE

NEW QUESTION 150

How is the Forward Untrust Certificate used?

- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has been decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
- D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 153

Which command can be used to validate a Captive Portal policy?

- A. eval captive-portal policy <criteria>
- B. request cp-policy-eval <criteria>
- C. test cp-policy-match <criteria>
- D. debug cp-policy <criteria>

Answer: C

NEW QUESTION 158

A company has a pair of Palo Alto Networks firewalls configured as an Active/Passive High Availability (HA) pair. What allows the firewall administrator to determine the last date a failover event occurred?

- A. From the CLI issue use the show System log
- B. Apply the filter subtype eq ha to the System log
- C. Apply the filter subtype eq ha to the configuration log
- D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 160

A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled. Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment?

- A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
- B. File Blocking profiles applied to outbound security policies with action set to alert
- C. Vulnerability Protection profiles applied to outbound security policies with action set to block
- D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

NEW QUESTION 164

How does Panorama handle incoming logs when it reaches the maximum storage capacity?

- A. Panorama discards incoming logs when storage capacity full.
- B. Panorama stops accepting logs until licenses for additional storage space are applied
- C. Panorama stops accepting logs until a reboot to clean storage space.
- D. Panorama automatically deletes older logs to create space for new ones.

Answer: D

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/determine-panorama-log-storage-requirements)

NEW QUESTION 169

Only two Trust to Untrust rules have been created in the Security policy Rule1 allows google-base Rule2 allows youtube-base

The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to access <https://www.youtube.com> in a web browser, they get an error indicating that the server cannot be found. Which action will allow youtube.com display in the browser correctly?

- A. Add SSL App-ID to Rule1
- B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
- C. Add the DNS App-ID to Rule2
- D. Add the Web-browsing App-ID to Rule2

Answer: C

NEW QUESTION 173

Which three options are available when creating a security profile? (Choose three)

- A. Anti-Malware
- B. File Blocking
- C. Url Filtering
- D. IDS/IPS
- E. Threat Prevention
- F. Antivirus

Answer: ABF

NEW QUESTION 175

Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

- A. Vulnerability Object
- B. DoS Protection Profile
- C. Data Filtering Profile
- D. Zone Protection Profile

Answer: BD

NEW QUESTION 176

Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.

Which method should company.com use to immediately address this traffic on a Palo Alto Networks device?

- A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.
- B. Wait until an official Application signature is provided from Palo Alto Networks.
- C. Modify the session timer settings on the closest referenced application to meet the needs of the in-house application
- D. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic

Answer: D

NEW QUESTION 177

A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible from the Monitor tab. What could cause this condition?

- A. The firewall does not have an active WildFire subscription.
- B. The engineer's account does not have permission to view WildFire Submissions.
- C. A policy is blocking WildFire Submission traffic.
- D. Though WildFire is working, there are currently no WildFire Submissions log entries.

Answer: B

NEW QUESTION 182

Click the Exhibit button below,

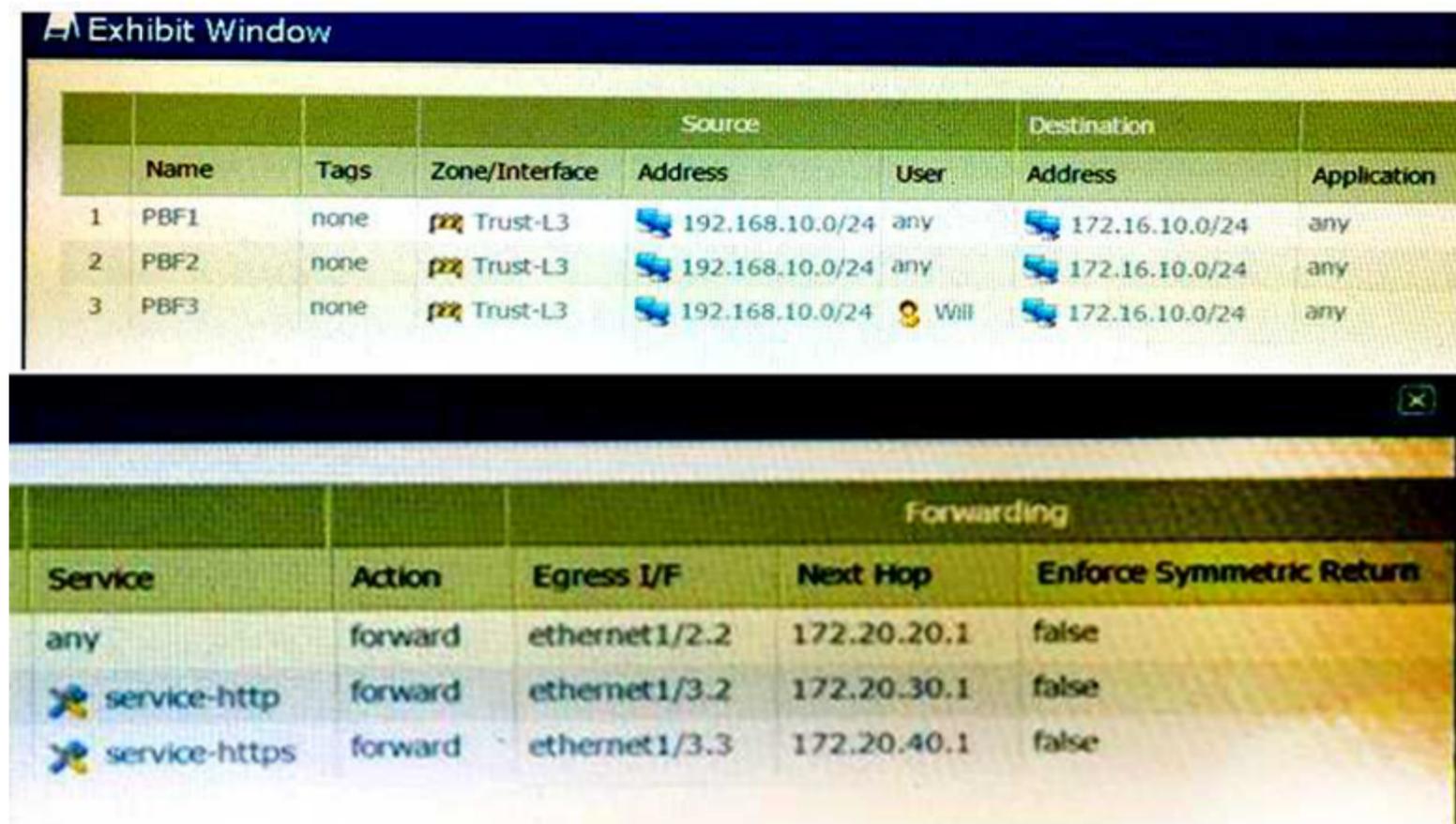


Exhibit Window							
		Source			Destination		
	Name	Tags	Zone/Interface	Address	User	Address	Application
1	PBF1	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
2	PBF2	none	Trust-L3	192.168.10.0/24	any	172.16.10.0/24	any
3	PBF3	none	Trust-L3	192.168.10.0/24	Will	172.16.10.0/24	any

Forwarding				
Service	Action	Egress I/F	Next Hop	Enforce Symmetric Return
any	forward	ethernet1/2.2	172.20.20.1	false
service-http	forward	ethernet1/3.2	172.20.30.1	false
service-https	forward	ethernet1/3.3	172.20.40.1	false

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20. Which is the next hop IP address for the HTTPS traffic from Will's PC?

- A. 172.20.30.1
- B. 172.20.40.1
- C. 172.20.20.1
- D. 172.20.10.1

Answer: C

NEW QUESTION 183

What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

- A. Clean
- B. Benign
- C. Adware
- D. Suspicious
- E. Grayware
- F. Malware

Answer: BEF

Explanation:

[https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK \"https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict\"/os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict](https://www.paloaltonetworks.com/documentation/70/pan-HYPERLINK \)

NEW QUESTION 185

What can missing SSL packets when performing a packet capture on dataplane interfaces?

- A. The packets are hardware offloaded to the offloaded processor on the dataplane
- B. The missing packets are offloaded to the management plane CPU
- C. The packets are not captured because they are encrypted
- D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 190

A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.
- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 191

The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalProtect Portal?

- A. Server Certificate
- B. Client Certificate
- C. Authentication Profile
- D. Certificate Profile

Answer: A

Explanation:

(<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351>)

NEW QUESTION 193

Which two interface types can be used when configuring GlobalProtect Portal?(Choose two)

- A. Virtual Wire
- B. Loopback
- C. Layer 3
- D. Tunnel

Answer: BC

NEW QUESTION 198

After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

- A. A Server Profile has not been configured for logging to this Panorama device.
- B. Panorama is not licensed to receive logs from this particular firewall.
- C. The firewall is not licensed for logging to this Panorama device.
- D. None of the firewall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 203

A network design calls for a "router on a stick" implementation with a PA-5060 performing inter-VLAN routing. All VLAN-tagged traffic will be forwarded to the PA-5060 through a single dot1q trunk interface. Which interface type and configuration setting will support this design?

- A. Trunk interface type with specified tag
- B. Layer 3 interface type with specified tag
- C. Layer 2 interface type with a VLAN assigned
- D. Layer 3 subinterface type with specified tag

Answer: D

NEW QUESTION 204

Firewall administrators cannot authenticate to a firewall GUI.

Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

- A. ms log
- B. authd log
- C. System log
- D. Traffic log
- E. dp-monitor .log

Answer:

- B. > show running resource-monitor
- C. > show system info
- D. > show system resources

Answer: D

Explanation:

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux." <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59364>

NEW QUESTION 221

How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

- A. Enable support for non-standard syslog messages under device management
- B. Check the custom-format check box in the syslog server profile
- C. Select a non-standard syslog server profile
- D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 223

A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.

What should be done first?

- A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
- B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
- C. remove the device from the Collector Group
- D. Revert to a previous configuration

Answer: C

NEW QUESTION 228

Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

- A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
- B. Enable User-ID on the zone object for the destination zone
- C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
- D. Enable User-ID on the zone object for the source zone
- E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 229

An administrator is configuring an IPsec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:

```
less mp-log ikemgr.log:
2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:52:33 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====> Due to
timeout.
2014-08-05 03:52:33 [INFO]: <====> PHASE-1 SA DELETED <====>
<====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f22f4e15:0000000000000000 <====>
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====>
<====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====>
2014-08-05 03:53:54 [PROTO_NOTIFY]: <====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====>
<====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:33351420a9a1aa47:0000000000000000 <====> Due to
timeout.
2014-08-05 03:53:54 [INFO]: <====> PHASE-1 SA DELETED <====>
```

What could be the cause of this problem?

- A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
- B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
- C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
- D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

Answer: C

NEW QUESTION 231

.....

Relate Links

100% Pass Your PCNSE Exam with ExamBible Prep Materials

<https://www.exambible.com/PCNSE-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>