



Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1

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 2

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

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

Answer: A

NEW QUESTION 3

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

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

Answer: AB

NEW QUESTION 4

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 5

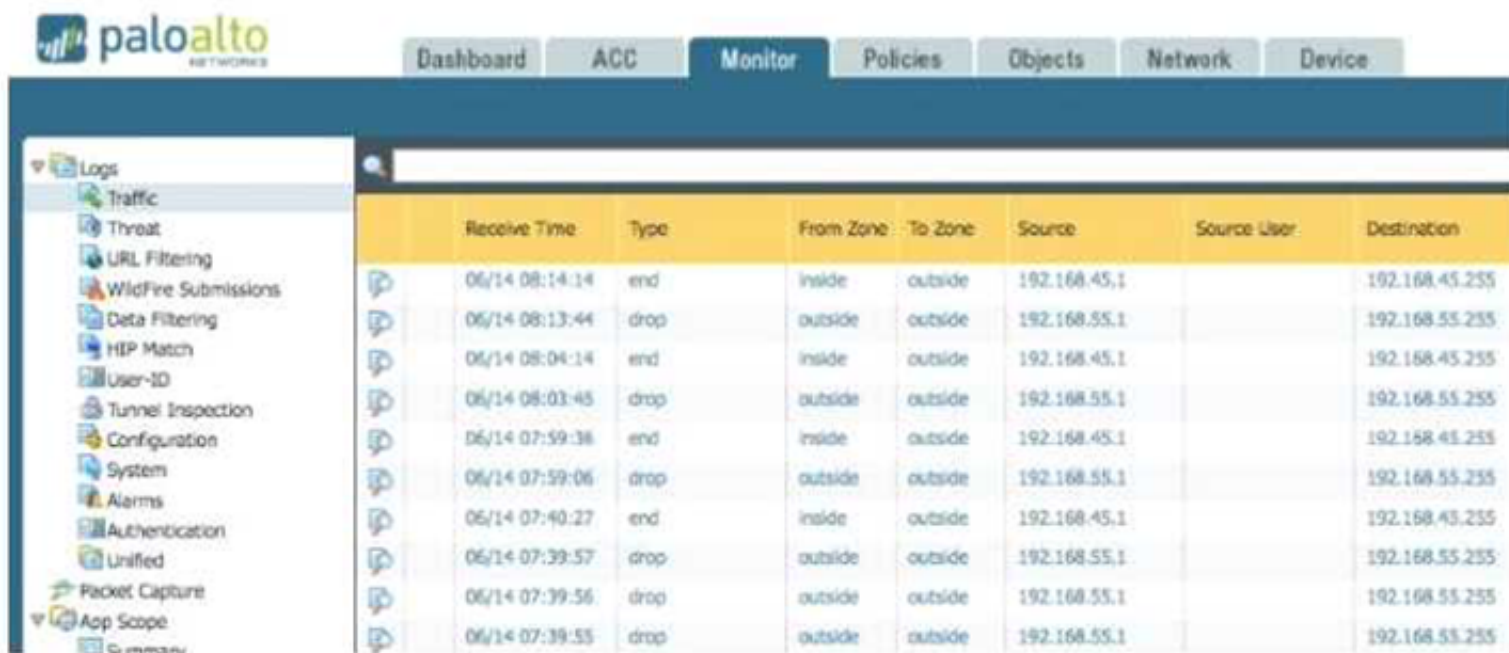
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A



Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	Informational	general		User admin accessed Monitor tab
06/16 08:40:40	general	Informational	general		User admin logged in via Web from 192.168.55.1 using https
06/16 08:40:40	auth	Informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	Informational	general		LOGIN ON tty1 BY admin
06/16 08:39:43	general	Informational	general		User admin logged in via CLI from Console
06/16 08:39:42	auth	Informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	Informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntpd	Informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	Informational	general		Commit job succeeded. Completion time=2017/06/16 08:31:33. JobId=29. User=admin

B

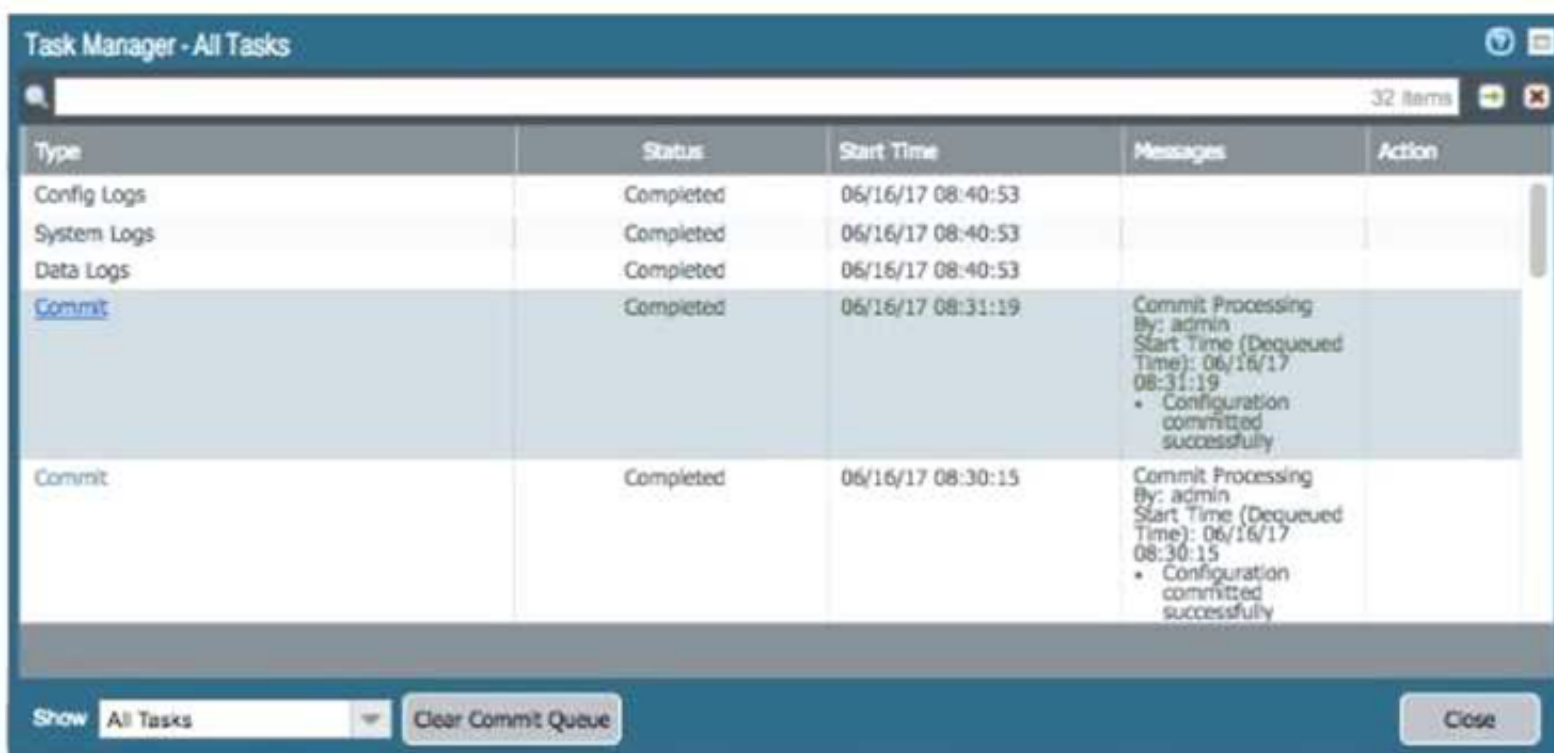


Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:38	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C

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

D



Type	Status	Start Time	Messages	Action
Config Logs	Completed	06/16/17 08:40:53		
System Logs	Completed	06/16/17 08:40:53		
Data Logs	Completed	06/16/17 08:40:53		
Commit	Completed	06/16/17 08:31:19	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:31:19 • Configuration committed successfully	
Commit	Completed	06/16/17 08:30:15	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:30:15 • Configuration committed successfully	

- A. Exhibit A
 B. Exhibit B
 C. Exhibit C
 D. Exhibit D

Answer: AD

NEW QUESTION 6

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

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

Answer: AD

NEW QUESTION 7

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

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

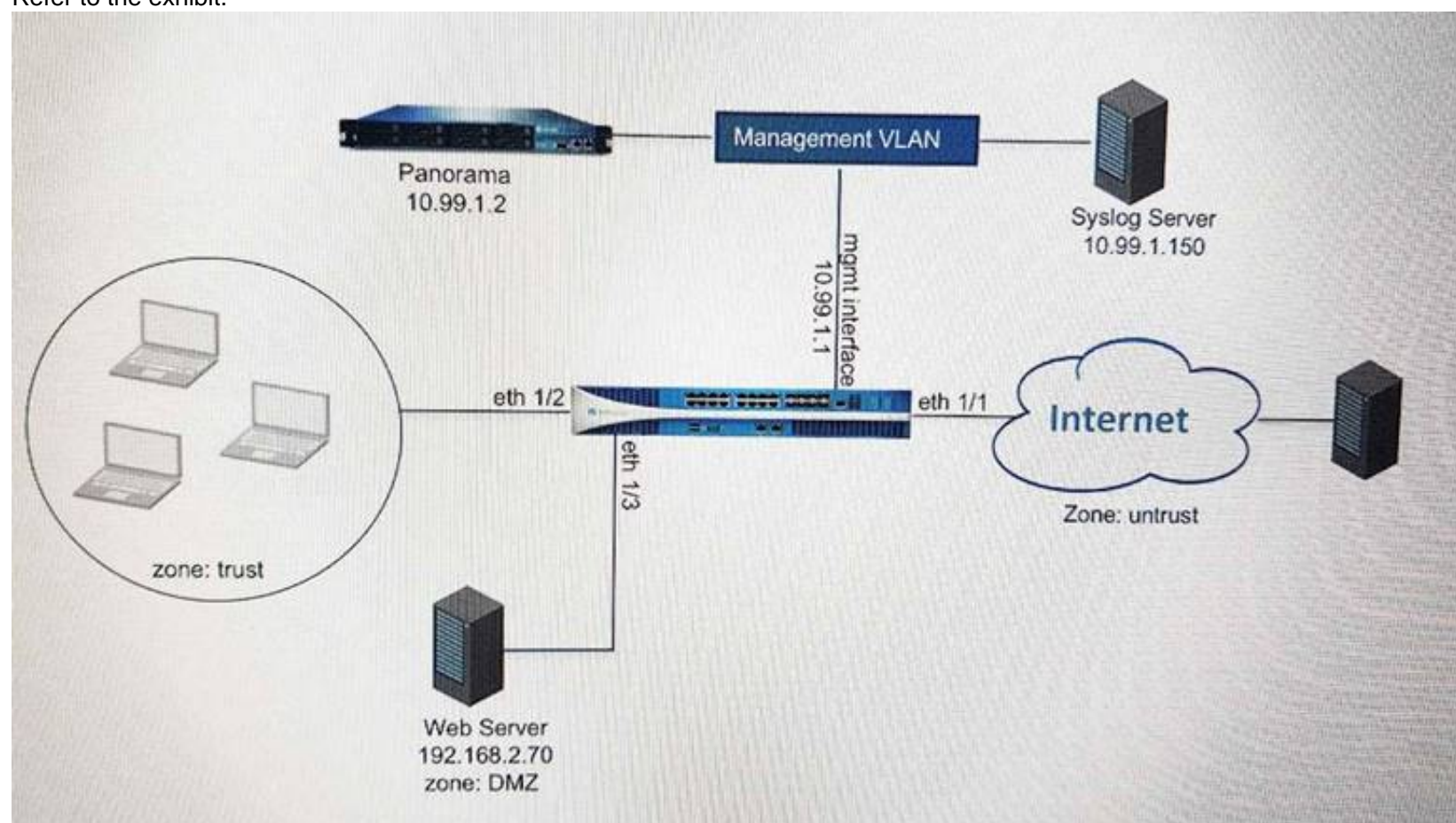
- A. Preconfigured GlobalProtect satellite
 B. Preconfigured GlobalProtect client

- C. Preconfigured IPsec tunnels
- D. Preconfigured PPTP Tunnels

Answer: A

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

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

Log Setting

☒ Log at Session Start

☒ Log at Session End

Log Forwarding

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
------------	------	-------

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Connect Wait Time (min) [0 - 44640]

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

Answer: D

NEW QUESTION 9

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

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

Answer: A

Explanation:

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts>

NEW QUESTION 10

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

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

Answer: C

NEW QUESTION 10

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

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

Answer: B

Explanation:

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

NEW QUESTION 15

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 19

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 21

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 22

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

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

Answer: BD

NEW QUESTION 26

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

How quickly will the firewall receive back a verdict?

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

Answer: D

NEW QUESTION 31

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 32

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-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

NEW QUESTION 33

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 34

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

Answer: B

NEW QUESTION 39

In a virtual router, which object contains all potential routes?

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

Answer: B

Explanation:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev%2520B.pdf&usg=AOvVaw0H9qgaJK0ol2xjlJBNo1Km

NEW QUESTION 41

Refer to the exhibit.

Device Certificates									
Default Trusted Certificate Authorities									
1 item									
Name	Location	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
Domain-Root-Cert	vsys1	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	✓		Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate
Domain-Sub-CA	vsys1	CN = sca.lab.local	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	✓	✓	Jun 6 20:59:38 2019 GMT	valid	RSA	
Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local		✓	Jun 6 21:09:49 2018 GMT	valid	RSA	

Which certificates can be used as a Forwarded Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward_Trust
- D. Domain-Root-Cert

Answer: A

NEW QUESTION 42

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 44

During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

Answer: BD

NEW QUESTION 45

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 48

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 50

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

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

Answer: A

Explanation:

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

NEW QUESTION 53

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 58

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

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

Answer: BC

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload>

NEW QUESTION 59

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

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

Answer: ABC

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/create-a-decryption-profile>

NEW QUESTION 60

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 65

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

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

Answer: BD

Explanation:

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

NEW QUESTION 66

Which DoS protection mechanism detects and prevents session exhaustion attacks?

- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles>

NEW QUESTION 70

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

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

Answer: B

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssh-proxy>

NEW QUESTION 72

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

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

Answer: A

NEW QUESTION 75

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: [https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS- Upgrade/ta-p/111045](https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045)

NEW QUESTION 77

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

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

Answer: CD

NEW QUESTION 78

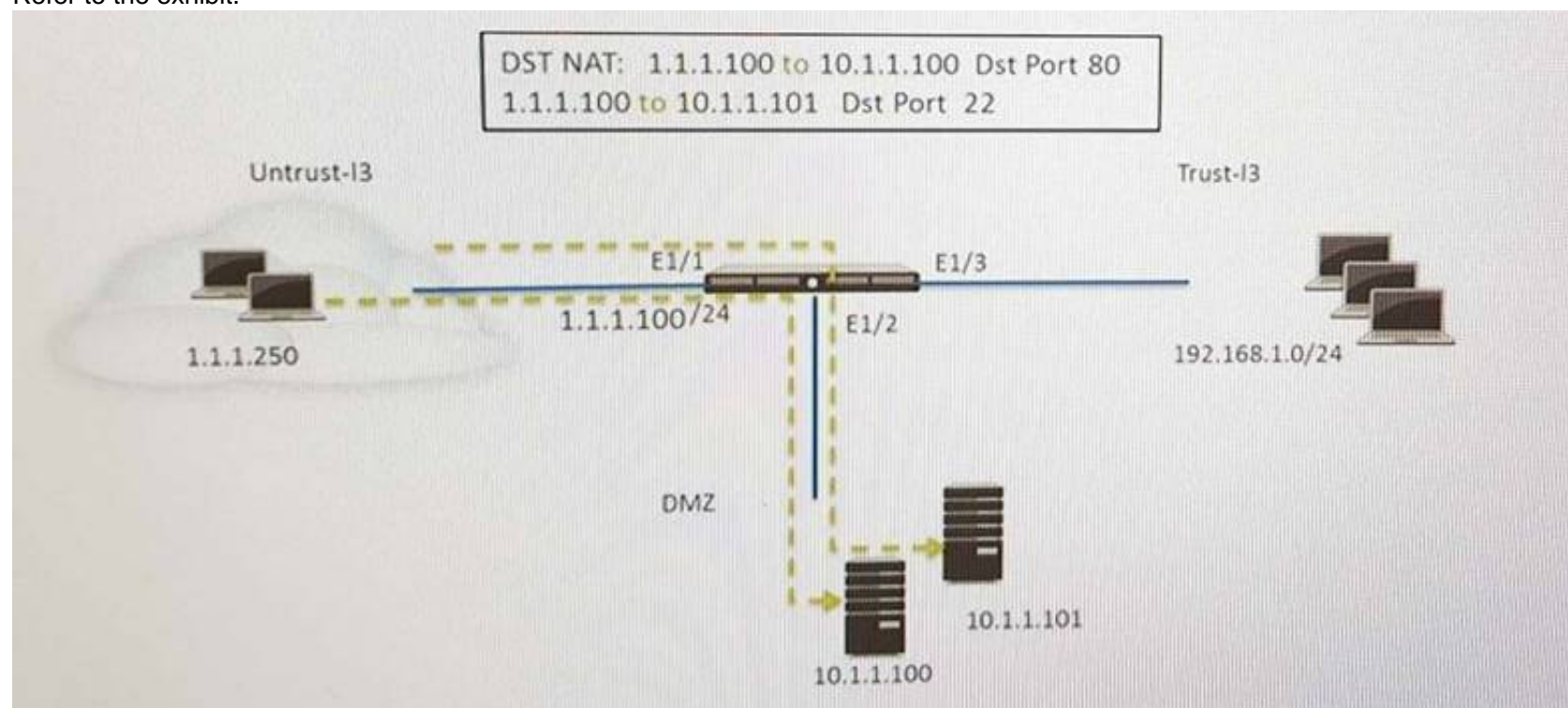
Which four NGFW multi-factor authentication factors are supported by PAN-OS? (Choose four.)

- A. User logon
- B. Short message service
- C. Push
- D. SSH key
- E. One-Time Password
- F. Voice

Answer: BCEF

NEW QUESTION 82

Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic. Which two security policy rules will accomplish this configuration? (Choose two)

- A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
- B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
- C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
- D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 84

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 87

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

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

Answer: CD

NEW QUESTION 89

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

- A. Select download-and-install.
- B. Select download-and-install, with "Disable new apps in content update" selected.
- C. Select download-only.

D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 93

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"/>	Interface	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 tunnel to p2p
- B. Set tunnel to p2mp
- C. Set Ethernet 1/1 to p2p
- D. Set Ethernet 1/1 to p2mp
- E. Set Ethernet 1/1 to p2p
- F. Set Ethernet 1/1 to p2mp

Answer: A

NEW QUESTION 94

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

Answer: BCD

Explanation:

(<https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069>)

NEW QUESTION 96

A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.

What should be done next?

- A. Click the simple-critical rule and then click the Action drop-down list.
- B. Click the Exceptions tab and then click show all signatures.
- C. View the default actions displayed in the Action column.
- D. Click the Rules tab and then look for rules with "default" in the Action column.

Answer: B

NEW QUESTION 101

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 104

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 105

Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

- A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.
- B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.
- C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
- D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

Answer: C

NEW QUESTION 110

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 114

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

- A. test panoramas-connect 10.10.10.5
- B. show panoramas-status
- C. show arp all | match 10.10.10.5
- D. topdump filter "host 10.10.10.5
- E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 116

Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

- A. Certificate revocation list
- B. Trusted root certificate
- C. Machine certificate
- D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 121

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 126

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 128

Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

- A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
- B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
- C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.

- D. Enter the command `logger-mode enable` then enter Y to confirm the change to Log Collector mode.
- E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION 130

A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

- A. Blocked Activity
- B. Bandwidth Activity
- C. Threat Activity
- D. Network Activity

Answer: D

NEW QUESTION 134

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 137

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting, it is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

- A. DHCP has been set to Auto.
- B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
- C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
- D. DNS has not been properly configured on the firewall

Answer: B

NEW QUESTION 138

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 140

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

- A. The two devices must share a routable floating IP address
- B. The two devices may be different models within the PA-5000 series
- C. The HA1 IP address from each peer must be on a different subnet
- D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 145

Which three options does the WF-500 appliance support for local analysis? (Choose three)

- A. E-mail links
- B. APK files
- C. jar files
- D. PNG files
- E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 149

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 153

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 157

Which option is an IPv6 routing protocol?

- A. RIPv3
- B. OSPFv3
- C. OSPv3
- D. BGP NG

Answer: B

NEW QUESTION 158

Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

- A. Microsoft Active Directory
- B. Microsoft Terminal Services
- C. Aerohive Wireless Access Point
- D. Palo Alto Networks Captive Portal

Answer: B

NEW QUESTION 163

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.

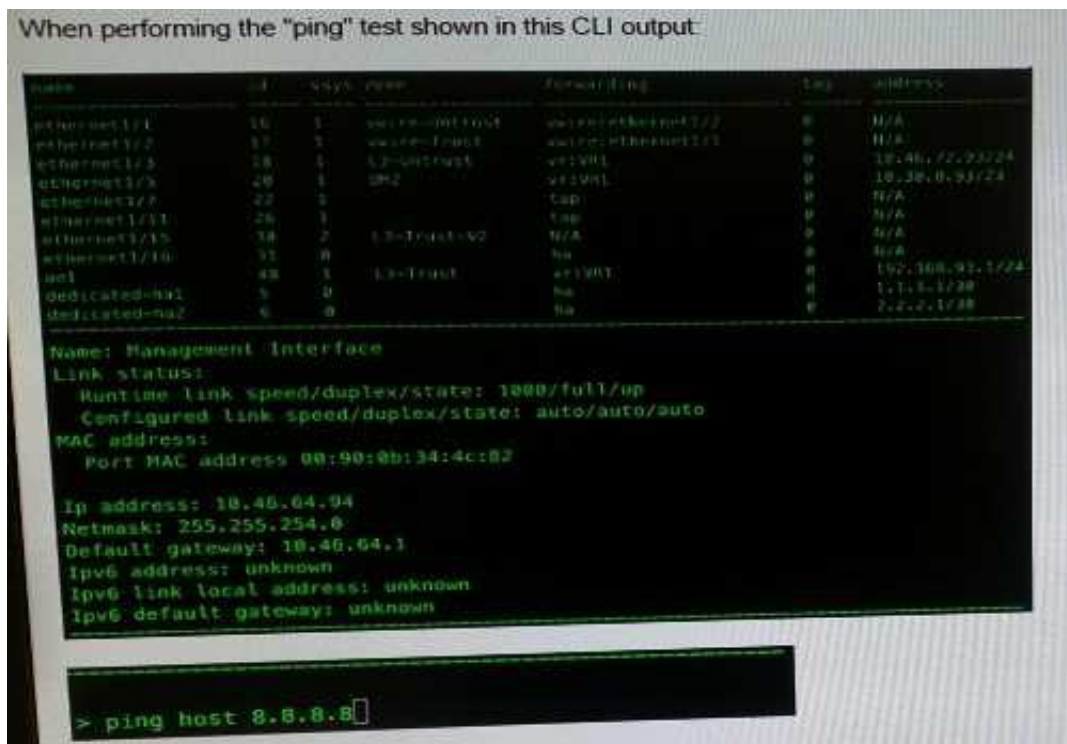
Which configuration setting needs to be modified?

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

Answer: A

NEW QUESTION 164

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 166

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

- A. BGP not sure
- B. OSPFv3
- C. RIP
- D. Static Route

Answer: BD

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-OSPF-or-BGP-with/ta-p/62773>

NEW QUESTION 169

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 174

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinkhole enabled, generating a traffic log.

What will be the destination IP Address in that log entry?

- A. The IP Address of sinkhole.paloaltonetworks.com
- B. The IP Address of the command-and-control server
- C. The IP Address specified in the sinkhole configuration
- D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864>

NEW QUESTION 178

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 179

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 182

.....

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

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 2

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

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

Answer: A

NEW QUESTION 3

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

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

Answer: AB

NEW QUESTION 4

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 5

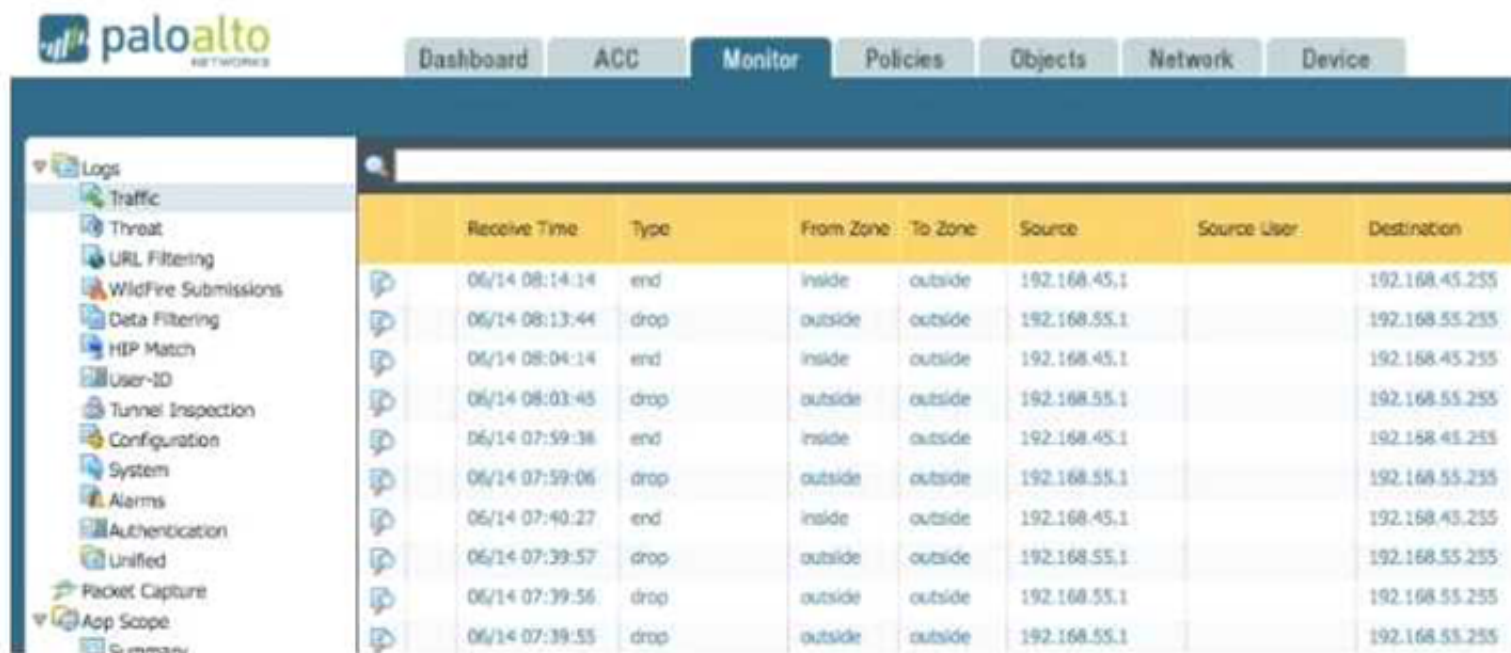
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A



Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	Informational	general		User admin accessed Monitor tab
06/16 08:40:40	general	Informational	general		User admin logged in via Web from 192.168.55.1 using https
06/16 08:40:40	auth	Informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	Informational	general		LOGIN ON tty1 BY admin
06/16 08:39:43	general	Informational	general		User admin logged in via CLI from Console
06/16 08:39:42	auth	Informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	Informational	upgrade-uri-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	Informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntpd	Informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	Informational	general		Commit job succeeded. Completion time=2017/06/16 08:31:33. JobId=29. User=admin

B

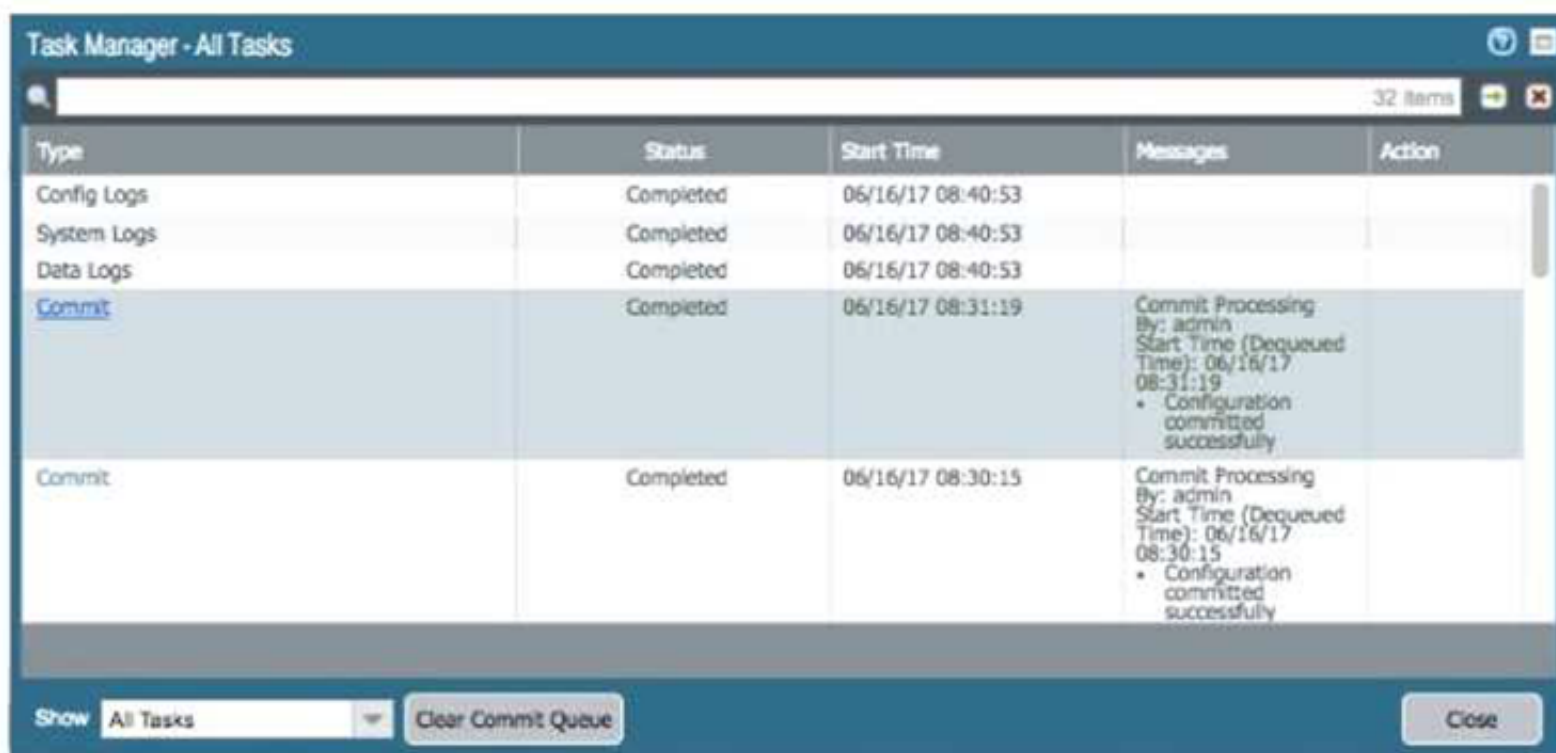


Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:38	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C

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

D



Type	Status	Start Time	Messages	Action
Config Logs	Completed	06/16/17 08:40:53		
System Logs	Completed	06/16/17 08:40:53		
Data Logs	Completed	06/16/17 08:40:53		
Commit	Completed	06/16/17 08:31:19	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:31:19 • Configuration committed successfully	
Commit	Completed	06/16/17 08:30:15	Commit Processing By: admin Start Time (Dequeued Time): 06/16/17 08:30:15 • Configuration committed successfully	

- A. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

Answer: AD

NEW QUESTION 6

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

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

Answer: AD

NEW QUESTION 7

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

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

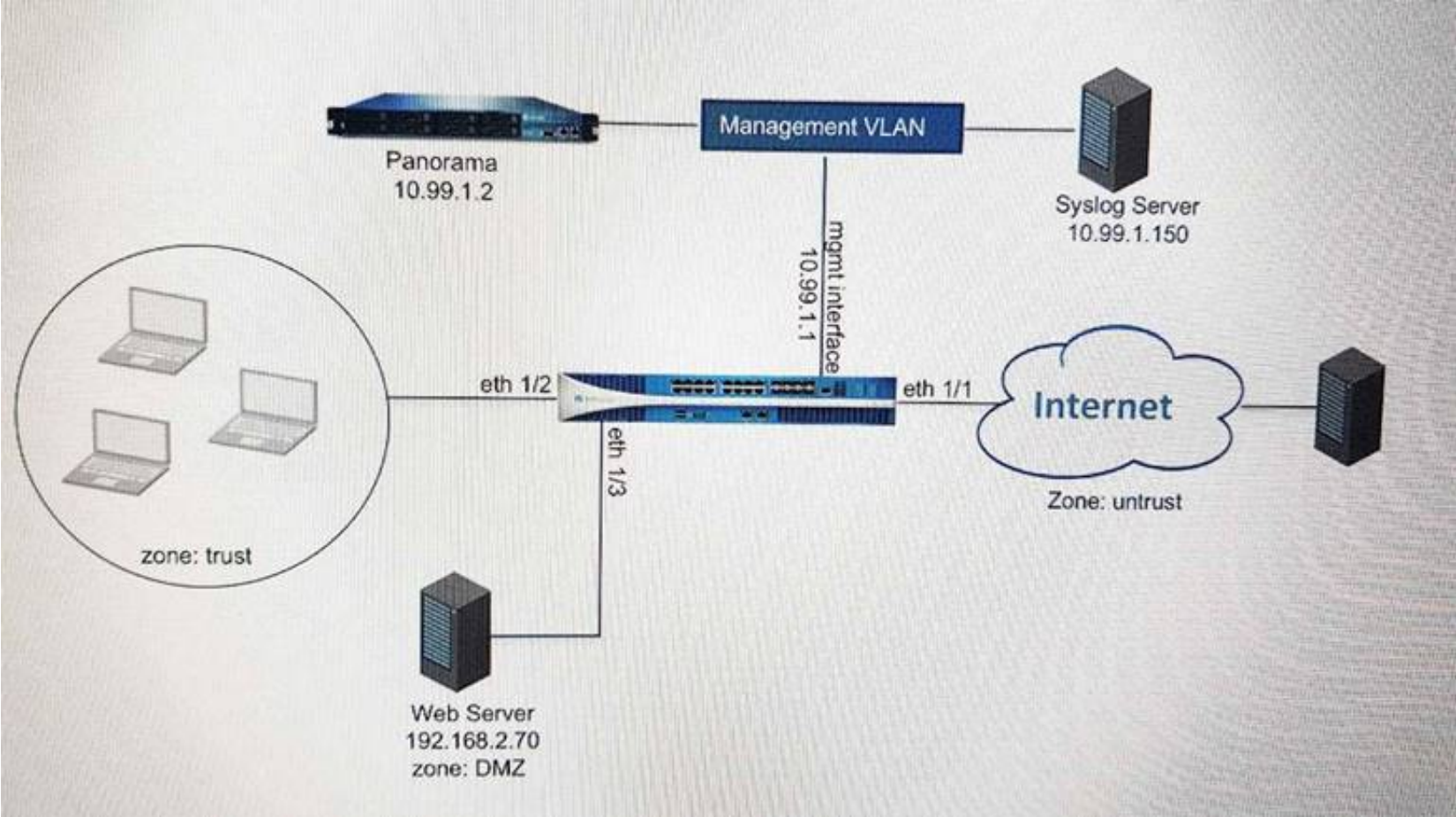
- A. Preconfigured GlobalProtect satellite
- B. Preconfigured GlobalProtect client

- C. Preconfigured IPsec tunnels
- D. Preconfigured PPTP Tunnels

Answer: A

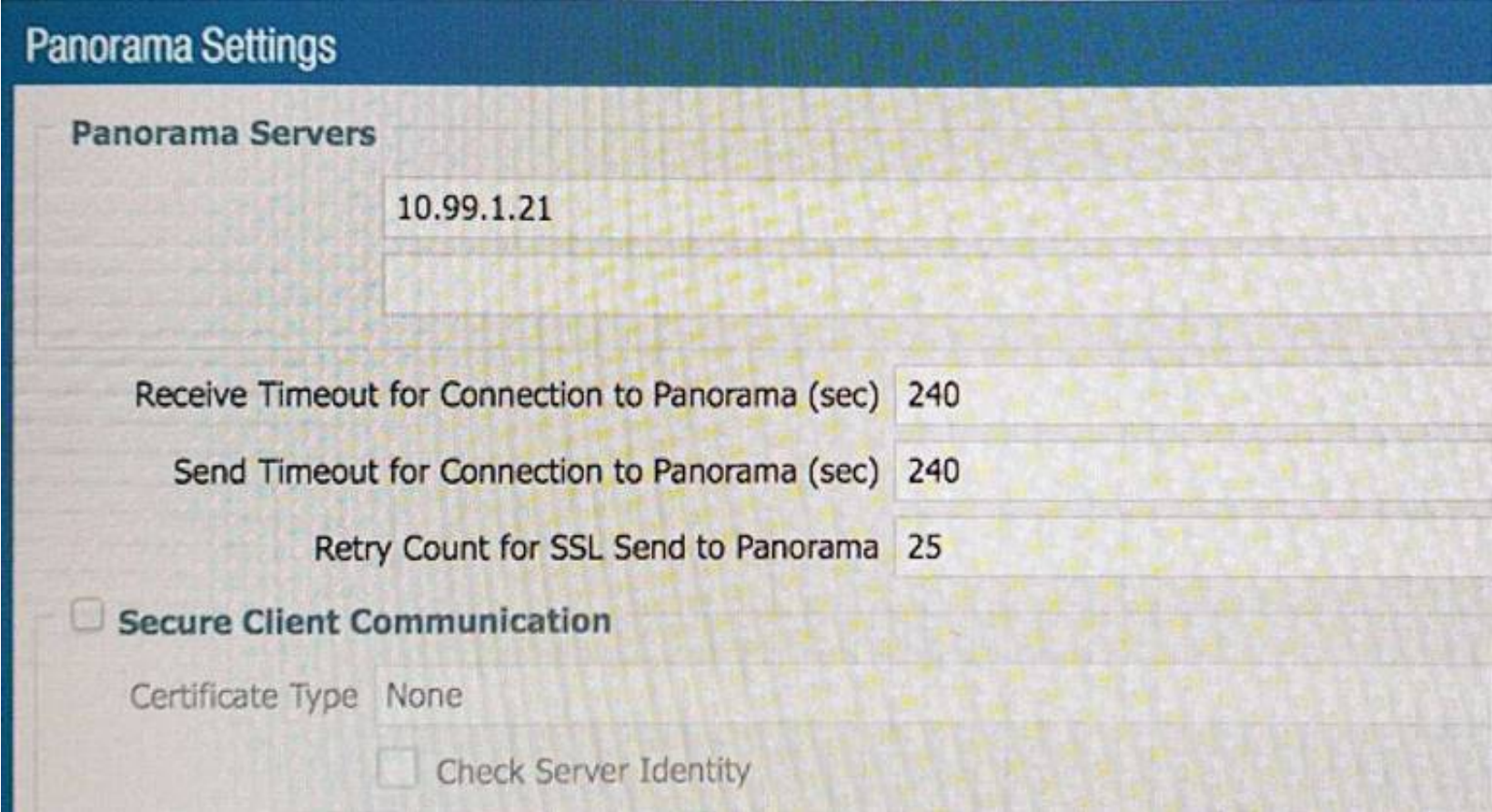
NEW QUESTION 8

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)



B)

Security Policy Rule

General

Source

User

Destination

Application

Service/URL Category

Actions

Action Setting

Action

Allow

☐ Send ICMP Unreachable

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

Log Setting

☒ Log at Session Start

☒ Log at Session End

Log Forwarding

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
------------	------	-------

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Connect Wait Time (min) [0 - 44640]

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

Answer: D

NEW QUESTION 9

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

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

Answer: A

Explanation:

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts>

NEW QUESTION 10

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

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

Answer: C

NEW QUESTION 10

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

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

Answer: B

Explanation:

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

NEW QUESTION 15

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 19

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 21

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 22

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

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

Answer: BD

NEW QUESTION 26

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

How quickly will the firewall receive back a verdict?

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

Answer: D

NEW QUESTION 31

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 32

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-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

NEW QUESTION 33

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 34

An administrator has users accessing network resources through Citrix XenApp 7 x. Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

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

Answer: B

NEW QUESTION 39

In a virtual router, which object contains all potential routes?

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

Answer: B

Explanation:

Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk&url=https%3A%2F%2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tkb%2F487%2F1%2FRoute%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-%2520Rev%2520B.pdf&usg=AOvVaw0H9qgaJK0ol2xjlJBNo1Km

NEW QUESTION 41

Refer to the exhibit.

Device Certificates									
Default Trusted Certificate Authorities									
1 item									
Name	Location	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
Domain-Root-Cert	vsys1	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	✓		Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate
Domain-Sub-CA	vsys1	CN = sca.lab.local	DC = local, DC = lab, CN = lab-DEMO-2008R2-CA	✓	✓	Jun 6 20:59:38 2019 GMT	valid	RSA	
Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local		✓	Jun 6 21:09:49 2018 GMT	valid	RSA	

Which certificates can be used as a Forwarded Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward_Trust
- D. Domain-Root-Cert

Answer: A

NEW QUESTION 42

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 44

During the packet flow process, which two processes are performed in application identification? (Choose two.)

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

Answer: BD

NEW QUESTION 45

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 48

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 50

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that sessions are being decrypted?

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

Answer: A

Explanation:

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

NEW QUESTION 53

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 58

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

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

Answer: BC

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload>

NEW QUESTION 59

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

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

Answer: ABC

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/create-a-decryption-profile>

NEW QUESTION 60

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 65

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

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

Answer: BD

Explanation:

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

NEW QUESTION 66

Which DoS protection mechanism detects and prevents session exhaustion attacks?

- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

Answer: C

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles>

NEW QUESTION 70

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

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

Answer: B

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssh-proxy>

NEW QUESTION 72

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

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

Answer: A

NEW QUESTION 75

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS software?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: [https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS- Upgrade/ta-p/111045](https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045)

NEW QUESTION 77

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

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

Answer: CD

NEW QUESTION 78

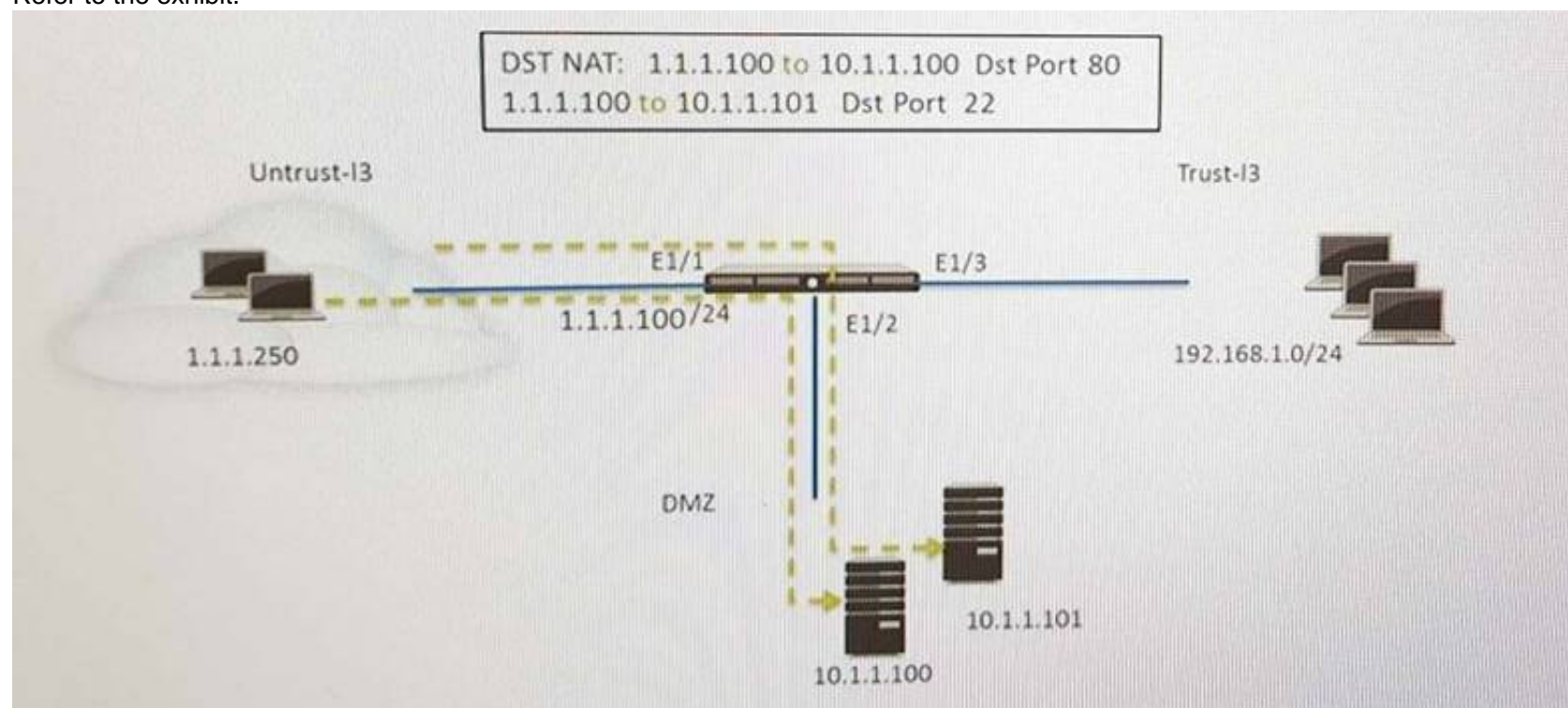
Which four NGFW multi-factor authentication factors are supported by PAN-OSS? (Choose four.)

- A. User logon
- B. Short message service
- C. Push
- D. SSH key
- E. One-Time Password
- F. Voice

Answer: BCEF

NEW QUESTION 82

Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) received HTTP traffic and host B(10.1.1.101) receives SSH traffic. Which two security policy rules will accomplish this configuration? (Choose two)

- A. Untrust (Any) to Untrust (10.1.1.1) Ssh-Allow
- B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
- C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
- D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 84

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 87

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

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

Answer: CD

NEW QUESTION 89

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

- A. Select download-and-install.
- B. Select download-and-install, with "Disable new apps in content update" selected.
- C. Select download-only.

D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 93

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 ID0.0.0.0

TypeRangeInterfaceVirtual Link

<input type="checkbox"/>	Interface	Enable	Passive	Link Type	Metric	Priority
<input type="checkbox"/>	tunnel.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	broadcast	10	1
<input type="checkbox"/>						
<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 tunnel to p2p
- B. Set tunnel to p2mp
- C. Set Ethernet 1/1 to p2mp
- D. Set Ethernet 1/1 to p2p
- E. Set Ethernet 1/1 to p2mp
- F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 94

Which three fields can be included in a pcap filter? (Choose three)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

Answer: BCD

Explanation:

(<https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069>)

NEW QUESTION 96

A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.

What should be done next?

- A. Click the simple-critical rule and then click the Action drop-down list.
- B. Click the Exceptions tab and then click show all signatures.
- C. View the default actions displayed in the Action column.
- D. Click the Rules tab and then look for rules with "default" in the Action column.

Answer: B

NEW QUESTION 101

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 104

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 105

Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

- A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.
- B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.
- C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
- D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

Answer: C

NEW QUESTION 110

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 114

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

- A. test panoramas-connect 10.10.10.5
- B. show panoramas-status
- C. show arp all | match 10.10.10.5
- D. topdump filter "host 10.10.10.5
- E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 116

Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

- A. Certificate revocation list
- B. Trusted root certificate
- C. Machine certificate
- D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 121

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 126

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 128

Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

- A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
- B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
- C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.

- D. Enter the command `logger-mode enable` then enter Y to confirm the change to Log Collector mode.
- E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:

(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION 130

A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

- A. Blocked Activity
- B. Bandwidth Activity
- C. Threat Activity
- D. Network Activity

Answer: D

NEW QUESTION 134

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 137

A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting, it is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

- A. DHCP has been set to Auto.
- B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
- C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
- D. DNS has not been properly configured on the firewall

Answer: B

NEW QUESTION 138

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 140

A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

- A. The two devices must share a routable floating IP address
- B. The two devices may be different models within the PA-5000 series
- C. The HA1 IP address from each peer must be on a different subnet
- D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 145

Which three options does the WF-500 appliance support for local analysis? (Choose three)

- A. E-mail links
- B. APK files
- C. jar files
- D. PNG files
- E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 149

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 153

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 157

Which option is an IPv6 routing protocol?

- A. RIPv3
- B. OSPFv3
- C. OSPv3
- D. BGP NG

Answer: B

NEW QUESTION 158

Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

- A. Microsoft Active Directory
- B. Microsoft Terminal Services
- C. Aerohive Wireless Access Point
- D. Palo Alto Networks Captive Portal

Answer: B

NEW QUESTION 163

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.

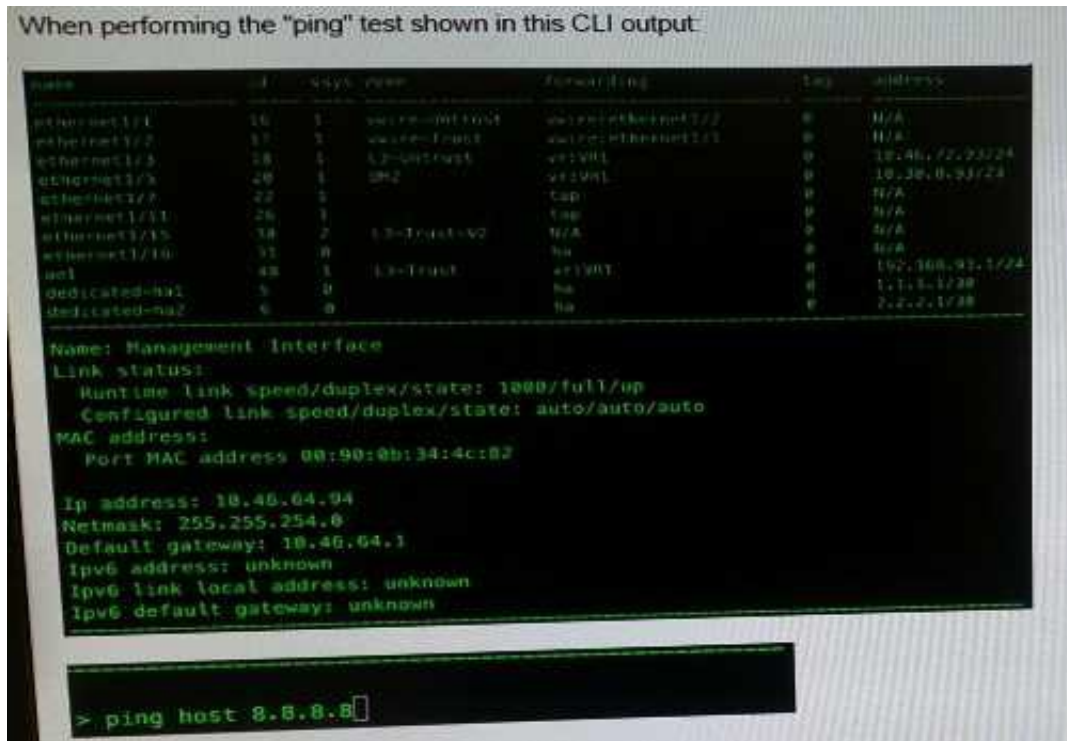
Which configuration setting needs to be modified?

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

Answer: A

NEW QUESTION 164

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 166

A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

- A. BGP not sure
- B. OSPFv3
- C. RIP
- D. Static Route

Answer: BD

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-OSPF-or-BGP-with/ta-p/62773>

NEW QUESTION 169

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 174

When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinkhole enabled, generating a traffic log.

What will be the destination IP Address in that log entry?

- A. The IP Address of sinkhole.paloaltonetworks.com
- B. The IP Address of the command-and-control server
- C. The IP Address specified in the sinkhole configuration
- D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864>

NEW QUESTION 178

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 179

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 182

.....

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/>