



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.



PCNSC MCQs
PCNSC TestPrep
PCNSC Study Guide
PCNSC Practice Test
PCNSC Exam Questions



Palo-Alto

PCNSC

Palo Alto Networks Certified Network Security Consultant



Question: 1

A session in the Traffic log is reporting the application as "incomplete"

What does "incomplete" mean?

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

Answer: A

Question: 2

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

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

Answer: A,B,C

Question: 3

What is exchanged through the HA2 link?

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

Answer: C

Question: 4

An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewalls use layer 3 interface to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

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

Answer: C

Question: 5

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

Answer: B

Question: 6

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

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

Answer: D

Question: 7

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

- A. Restful API or the VMware API on the firewall or on the User-ID agent or the ready-only domain controller
- B. XML API or the VMware API on the firewall on the User-ID agent or the CLI
- C. Restful API or the VMware API on the firewall or on the User-ID Agent
- D. XML- API or lite VM Monitoring agent on the NGFW or on the User-ID agent

Answer: D

Question: 8

An administrator logs in to the Palo Alto Networks NGFW and reports and reports that the WebUI is missing the policies tab.

Which profile is the cause of the missing policies tab?

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

Answer: B

Question: 9

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

- A. credential submission prevention
- B. file blocking
- C. User-ID
- D. data filtering

Answer: A

Question: 10

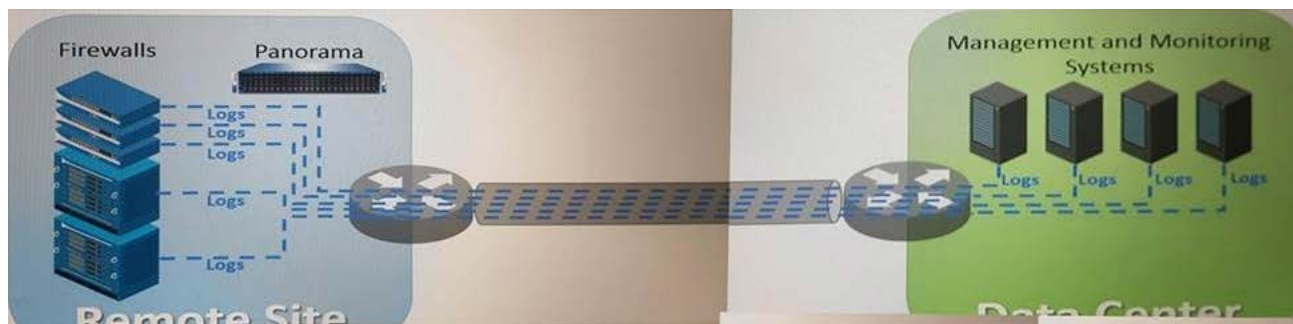
Which CLI command enables an administrator to view detail about the firewall including uptime, PAN -OS® version, and serial number?

- A. debug system details
- B. Show systemdetail
- C. Show system info
- D. Show session info

Answer: C

Question: 11

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



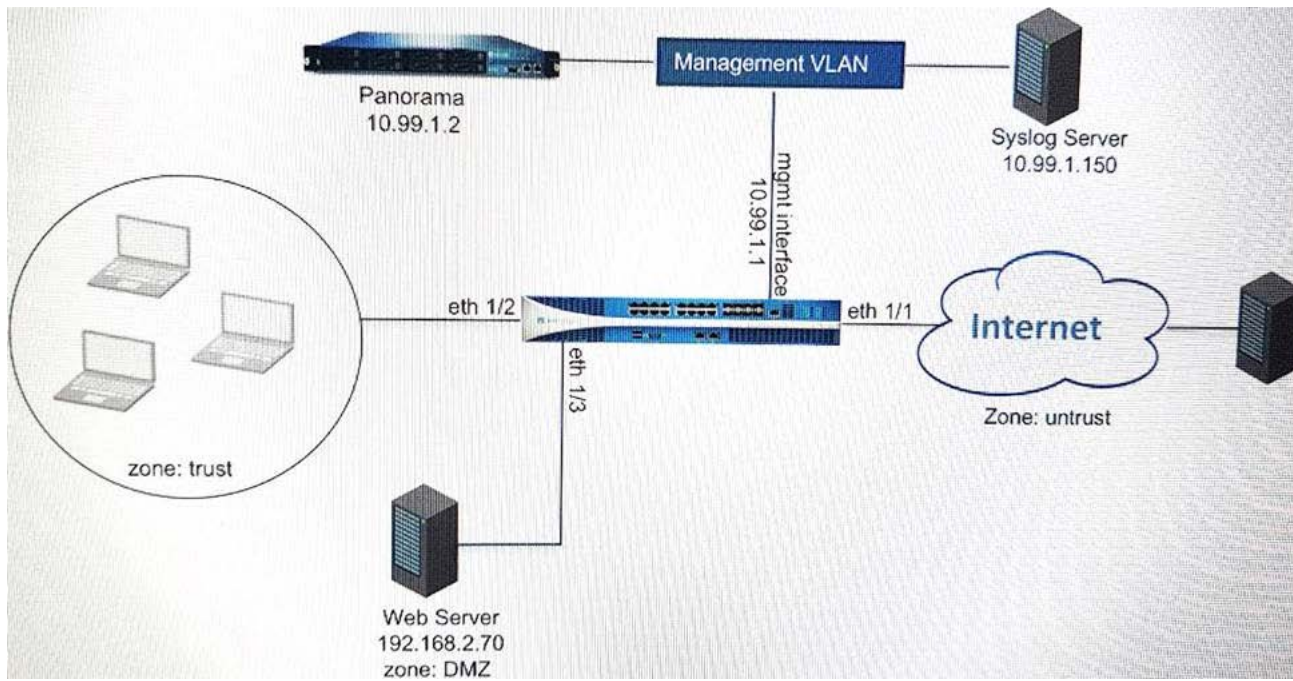
How could the Palo Alto Networks NOFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

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

Answer: A

Question: 12

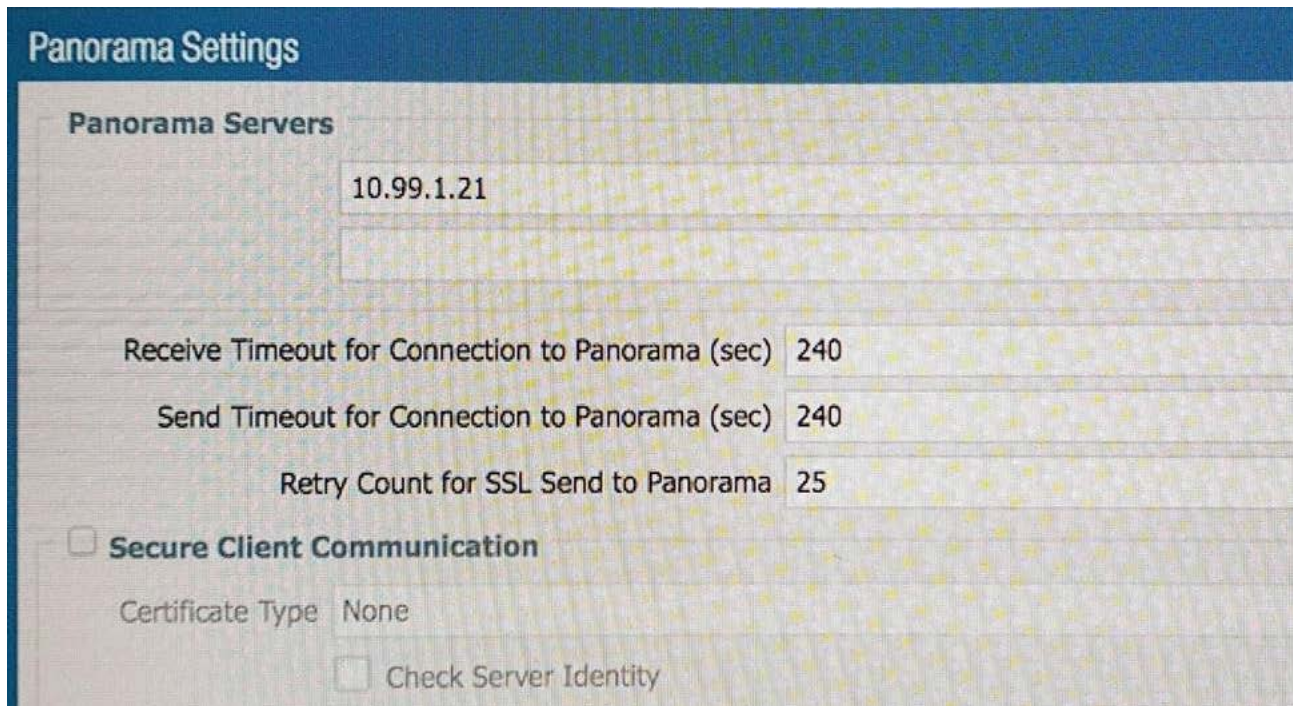
Refer to the exhibit.



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

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 | Can

C)

Syslog Server Profile

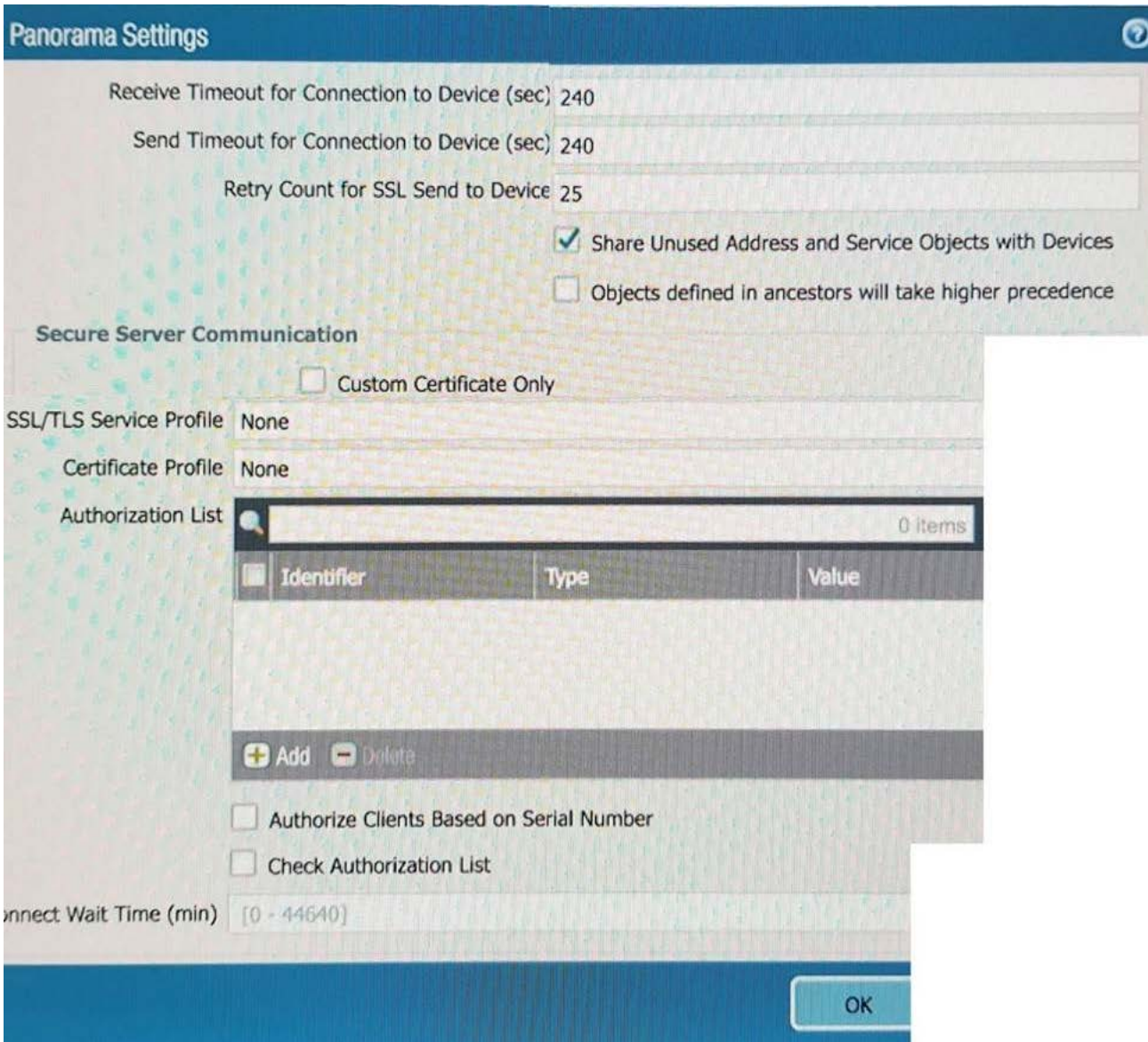
Name: SyslogProfile1

Servers | Custom Log Format

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

+ Add - Delete

D)



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

Answer: D

Question: 13

An administrator has left a firewall to used default port for all management services.

Which three function performed by the dataplane? (Choose three.)

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

Answer: A,C,D

Question: 14

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch it connect.

How would an administrator configure the interface to 10Gbps?

- A. set deviceconfig system speed-duplex 10Gbps-full-duplex
- B. set deviceconfig interface speed-duplex 10Gbps--full-duplex
- C. set deviceconfig interface speed-duplex 10Gbps--half-duplex
- D. set deviceconfig system speed-duplex 10Gbps--half-duplex.

Answer: D

Question: 15

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

Which Security Profile type will prevent these behaviors?

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

Answer: D

Question: 16

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

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

Answer: B

Question: 17

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

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward now proxy
- D. SMTP inbound Decryption

Answer: C

Question: 18

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

Answer: A,B,D

Question: 19

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

Answer: B

Question: 20

Which administrative authentication method supports authorization by an external service?

- A. RADIUS
- B. SSH keys
- C. Certification
- D. LDAP

Answer: A

Question: 21

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

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

Answer: A,B,D

Question: 22

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

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

Answer: C

Question: 23

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

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

- A. custom application
- B. Custom and downloaded application signature files are merged and are used
- C. System logs show an application errors and signature is used.
- D. downloaded application

Answer: A

Question: 24

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

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

- A. preconfigured GlobalProtcet satellite
- B. preconfigured GlobalProtcet client
- C. preconfigured iPsec tunnels
- D. preconfigured PPTP Tunnels

Answer: A

Question: 25

What will be the egress interface if the trafficâs ingress interface is Ethernet 1/6 sourcing form 192.168.11.3 and to the destination 10.46.41.113.during the.

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

```
Thu Jun 8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules
```

```
test-pbf {  
  action {  
    forward {  
      egress-interface ethernet1/5;  
    }  
  }  
  from {  
    zone L3-Trust;  
  }  
  enforce-symmetric-return {  
    enabled no;  
  }  
  source 192.168.111.3;  
  destination 10.46.41.113;  
  source-user any;  
  destination any;  
  source any;  
  schedule schedule-nbf;
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-p
```

```
schedule-pbf {  
  schedule-type {  
    recurring {  
      daily 16:00-21:00;  
    }  
  }  
}
```

```
#####
```

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

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

id	destination	nexthop	flags	interface
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6

- A. ethernet 1/6
- B. ethernet 1/5
- C. ethernet 1/3
- D. ethernet 1/7

Answer: C

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.