

PCNSE Dumps

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 9.0

<https://www.certleader.com/PCNSE-dumps.html>



NEW QUESTION 1

- (Exam Topic 2)

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 2

- (Exam Topic 2)

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 3

- (Exam Topic 2)

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

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

Answer: D

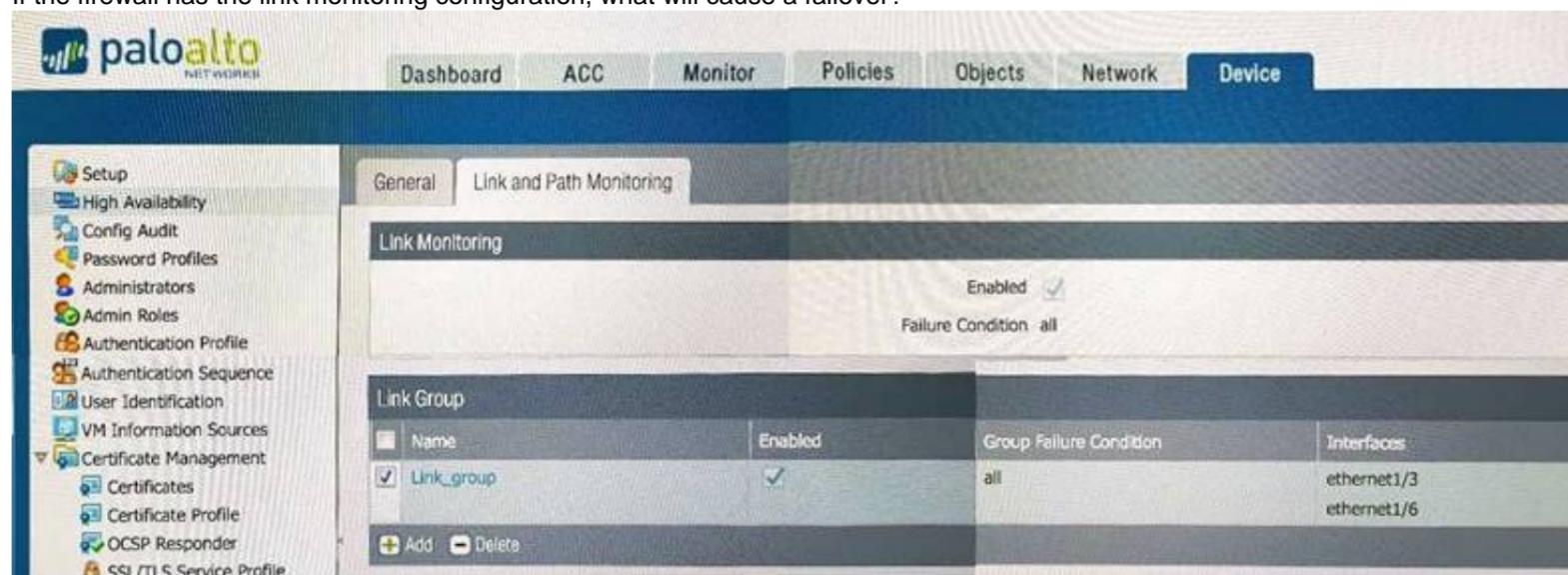
Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC>

NEW QUESTION 4

- (Exam Topic 2)

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



- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or Ethernet1/6 going down
- D. ethernet1/6 going down

Answer: A

NEW QUESTION 5

- (Exam Topic 2)

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

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

Answer: AC

NEW QUESTION 6

- (Exam Topic 2)

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 7

- (Exam Topic 2)

An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge. What is the expected verdict from WildFire?

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

Answer: A

Explanation:

Wildfire verdicts are as follow1-Begin2-Greyware3-Malicious4-Phishing https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-concepts/v

NEW QUESTION 8

- (Exam Topic 2)

What is exchanged through the HA2 link?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 9

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 2)

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

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC>

NEW QUESTION 10

- (Exam Topic 2)

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 as their accounting application and to scan this traffic for threats. Which option would achieve this result?

- A. Create an Application Override policy and a custom threat signature for the application

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

Answer: D

NEW QUESTION 13

- (Exam Topic 2)

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg.txt. The firewall is currently running PAN-OS 10.0 and using a lab config. The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsyst-jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command: > request resort system. Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because

- A. Firewall must be in factory default state or have all private data deleted for bootstrapping
- B. The hostname is a required parameter, but it is missing in init-cfg.txt
- C. The USB must be formatted using the ext3 file system, FAT32 is not supported
- D. PANOS version must be 9.1.x at a minimum but the firewall is running 10.0.x
- E. The bootstrap.xml file is a required file but it is missing

Answer: C

NEW QUESTION 16

- (Exam Topic 2)

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-docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deploy>

NEW QUESTION 20

- (Exam Topic 2)

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

- A. 15,000
- B. 10,000
- C. 75,000
- D. 5,000

Answer: B

NEW QUESTION 24

- (Exam Topic 2)

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

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

Answer: AB

NEW QUESTION 28

- (Exam Topic 2)

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab. Which profile is the cause of the missing Policies tab?

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

Answer: A

NEW QUESTION 31

- (Exam Topic 2)

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: A

NEW QUESTION 34

- (Exam Topic 2)

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: D

Explanation:

"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy."

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#>

NEW QUESTION 35

- (Exam Topic 2)

On the NGFW, how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

- A. * 1. Select Device > Certificate Management > Certificates > Device > Certificates * 2. Import the certificate * 3 Select Import Private Key * 4 Click Generate to generate the new certificate
- B. * 1 Select Device > Certificates * 2 Select Certificate Profile * 3 Generate the certificate * 4 Select Block Private Key Export.
- C. * 1 Select Device > Certificates * 2 Select Certificate Profile * 3 Generate the certificate * 4 Select Block Private Key Export
- D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate * 3 Select Block Private Key Export * 4 Click Generate to generate the new certificate.

Answer: D

NEW QUESTION 37

- (Exam Topic 2)

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

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

Answer: BDE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra>

NEW QUESTION 40

- (Exam Topic 2)

The firewall identifies a popular application as an unknown-tcp.

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

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

Answer: AD

Explanation:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applic>

NEW QUESTION 41

- (Exam Topic 2)

Refer to the exhibit.

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	<input checked="" type="checkbox"/>		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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 20:59:38 2019 GMT	valid	RSA	
Forward_Trust	vsys1	CN = fwdtrust.la...	CN = sca.lab.local		<input checked="" type="checkbox"/>	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: B

NEW QUESTION 45

- (Exam Topic 2)

Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

- A. respond to changes in user behavior or potential threats using manual policy changes
- B. respond to changes in user behavior or potential threats without automatic policy changes
- C. respond to changes in user behavior and confirmed threats with manual policy changes
- D. respond to changes in user behavior or potential threats without manual policy changes

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:tex>

NEW QUESTION 50

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring>

“Before you can enable Decryption Mirroring, you must obtain and install a Decryption Port Mirror license. The license is free of charge and can be activated through the support portal as described in the following procedure. After you install the Decryption Port Mirror license and reboot the firewall, you can enable decryption port mirroring.”

NEW QUESTION 55

- (Exam Topic 2)

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

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

Answer: B

Explanation:

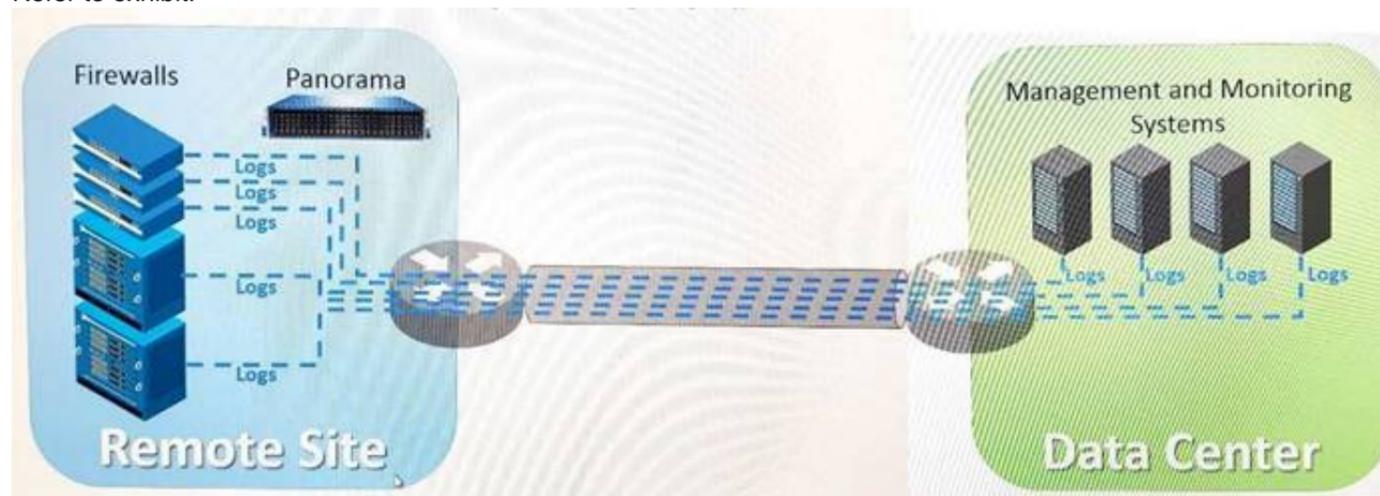
Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Overrid>
<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#>

NEW QUESTION 59

- (Exam Topic 2)

Refer to exhibit.



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

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

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

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and>
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"
"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

NEW QUESTION 63

- (Exam Topic 2)

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

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

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

Answer: A

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-update>

NEW QUESTION 67

- (Exam Topic 2)

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

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

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishi>

Reference:

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

NEW QUESTION 69

- (Exam Topic 2)

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: D

Explanation:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec>

NEW QUESTION 73

- (Exam Topic 2)

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

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

Answer: ABC

NEW QUESTION 76

- (Exam Topic 2)

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 81

- (Exam Topic 2)

A customer wants to set up a site-to-site VPN using tunnel interfaces? Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. Vpn-tunnel.1024
- B. vpn-tunne.1
- C. tunnel 1025
- D. tunne
- E. 1

Answer: CD

NEW QUESTION 82

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 83

- (Exam Topic 2)

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 88

- (Exam Topic 2)

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 91

- (Exam Topic 2)

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

Which priority is correct for the passive firewall?

- A. 99
- B. 1
- C. 255

Answer: D

Explanation:

Reference:

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5. (page 9)

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf page 315

NEW QUESTION 95

- (Exam Topic 1)

Which CLI command displays the physical media that are connected to ethernetl/8?

- A. > show system state filter-pretty sys.si.p8.stats
- B. > show interface ethernetl/8
- C. > show system state filter-pretty sys.sl.p8.phy
- D. > show system state filter-pretty sys.si.p8.med

Answer: D

NEW QUESTION 98

- (Exam Topic 1)

Refer to the exhibit.

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
Domain-Root-Cert	CN = demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 23 16:50:22 2021 GMT	valid	RSA	Trusted Root CA
Domain-Sub-CA	CN = sub.demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 23 16:52:26 2021 GMT	valid	RSA	
Forward-Trust	CN = fwdtrust.demo.local	CN = sub.demo.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jul 23 16:53:38 2021 GMT	valid	RSA	

Which certificate can be used as the Forward Trust certificate?

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

Answer: D

NEW QUESTION 100

- (Exam Topic 1)

An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices. The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed.

Which Panorama tool can help this organization?

- A. Config Audit
- B. Policy Optimizer
- C. Application Groups
- D. Test Policy Match

Answer: A

NEW QUESTION 104

- (Exam Topic 1)

A variable name must start with which symbol?

- A. \$
- B. &
- C. !
- D. #

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-tem>

NEW QUESTION 109

- (Exam Topic 1)

When setting up a security profile which three items can you use? (Choose three)

- A. Wildfire analysis
- B. anti-ransom ware
- C. antivirus
- D. URL filtering
- E. decryption profile

Answer: ACD

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

NEW QUESTION 114

- (Exam Topic 1)

In a firewall, which three decryption methods are valid? (Choose three)

- A. SSL Inbound Inspection
- B. SSL Outbound Proxyless Inspection
- C. SSL Inbound Proxy
- D. Decryption Mirror
- E. SSH Proxy

Answer: ADE

NEW QUESTION 117

- (Exam Topic 1)

PBF can address which two scenarios? (Select Two)

- A. forwarding all traffic by using source port 78249 to a specific egress interface
- B. providing application connectivity the primary circuit fails
- C. enabling the firewall to bypass Layer 7 inspection
- D. routing FTP to a backup ISP link to save bandwidth on the primary ISP link

Answer: AC

NEW QUESTION 121

- (Exam Topic 1)

When overriding a template configuration locally on a firewall, what should you consider?

- A. Only Panorama can revert the override
- B. Panorama will lose visibility into the overridden configuration
- C. Panorama will update the template with the overridden value
- D. The firewall template will show that it is out of sync within Panorama

Answer: B

NEW QUESTION 123

- (Exam Topic 1)

An internal system is not functioning The firewall administrator has determined that the incorrect egress interface is being used After looking at the configuration, the administrator believes that the firewall is not using a static route What are two reasons why the firewall might not use a static route"? (Choose two.)

- A. no install on the route
- B. duplicate static route
- C. path monitoring on the static route
- D. disabling of the static route

Answer: C

NEW QUESTION 125

- (Exam Topic 1)

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

Answer: D

NEW QUESTION 130

- (Exam Topic 1)

A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

- A. The firewall did not install the session
- B. The TCP connection terminated without identifying any application data
- C. The firewall dropped a TCP SYN packet
- D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 134

- (Exam Topic 1)

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three)

- A. Destination Zone
- B. App-ID
- C. Custom URL Category
- D. User-ID
- E. Source Interface

Answer: ADE

NEW QUESTION 139

- (Exam Topic 1)

Which configuration task is best for reducing load on the management plane?

- A. Disable logging on the default deny rule
- B. Enable session logging at start
- C. Disable pre-defined reports
- D. Set the URL filtering action to send alerts

Answer: A

NEW QUESTION 141

- (Exam Topic 1)

In a Panorama template which three types of objects are configurable? (Choose three)

- A. HIP objects
- B. QoS profiles
- C. interface management profiles
- D. certificate profiles
- E. security profiles

Answer: ACE

NEW QUESTION 144

- (Exam Topic 1)

Which Panorama objects restrict administrative access to specific device-groups?

- A. templates
- B. admin roles
- C. access domains
- D. authentication profiles

Answer: C

NEW QUESTION 148

- (Exam Topic 2)

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:

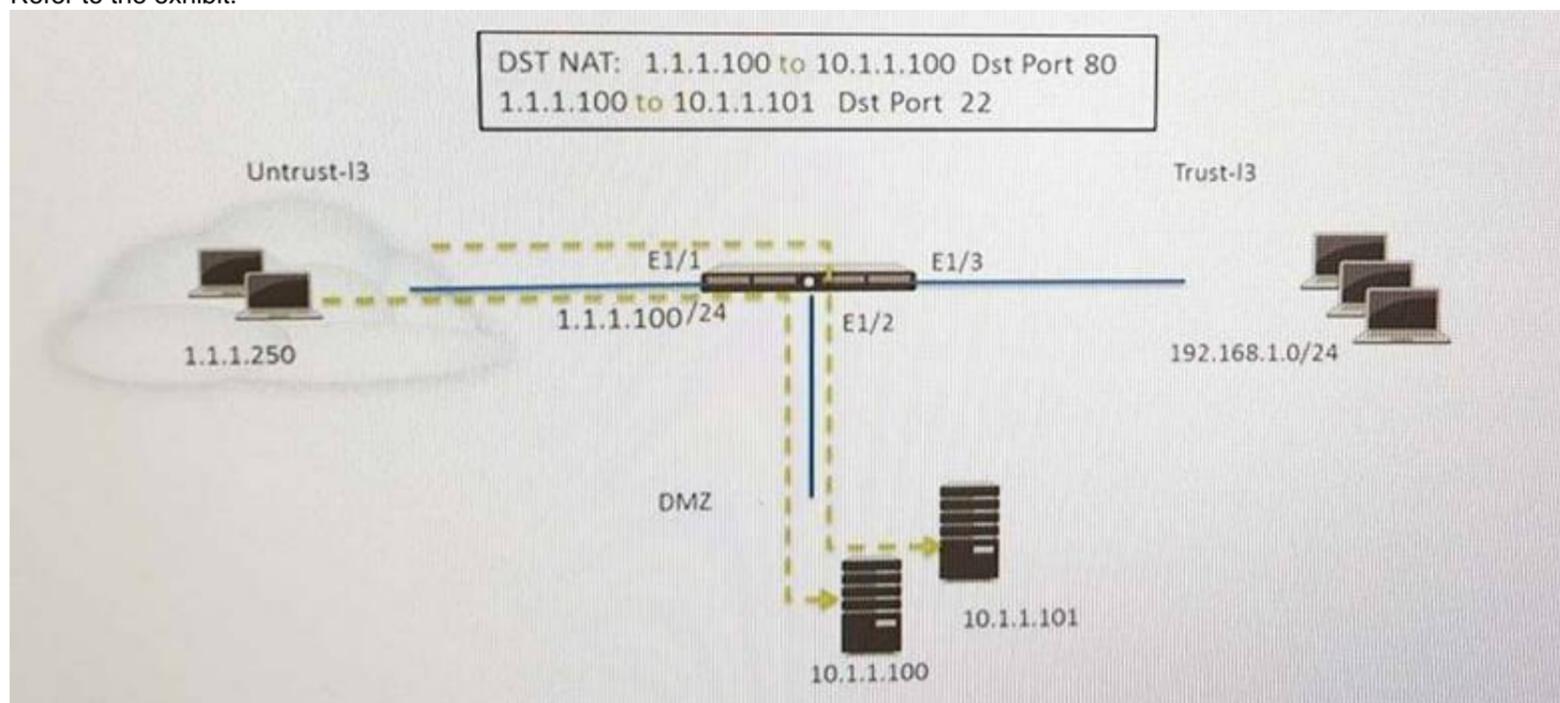
Reference:

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

NEW QUESTION 152

- (Exam Topic 2)

Refer to the exhibit.



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

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

- A. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing –Allow
- B. Untrust (Any) to DMZ (1.1.1.100), web-browsing –Allow
- C. Untrust (Any) to Untrust (10.1.1.1), web-browsing –Allow
- D. Untrust (Any) to Untrust (10.1.1.1), SSH -Allow
- E. Untrust (Any) to DMZ (1.1.1.100), SSH –Allow

Answer: BE

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat>

NEW QUESTION 155

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

If you check in the FW the default port for web-browsing is TCP 80, so you will need a custom app. admin@PA-LAB-01# show predefined application web-browsing web-browsing { category general-internet; subcategory internet-utility; technology browser-based; analysis 'Web browsing continues to evolve. Initially used to simply view HTML formatted information, web browsers have become the client, through which, users can access new applications that provide functionality far beyond simple information browsing. These applications include web mail, instant messaging, streaming media, web conferencing, blogs, file sharing and other social networking applications. Much of the plain web-browsing activities has effectively been overshadowed by all the other applications. } default { port tcp/80; } tunnel-applications http-proxy; risk 4; } [edit]

NEW QUESTION 158

- (Exam Topic 2)

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-profile-vulnerability-protection>

NEW QUESTION 161

- (Exam Topic 2)

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

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

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-m>

NEW QUESTION 162

- (Exam Topic 2)

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

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

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-aut>

NEW QUESTION 167

- (Exam Topic 2)

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: AC

Explanation:

Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

NEW QUESTION 172

- (Exam Topic 2)

An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

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

Answer: D

Explanation:

Palo Alto Networks Panorama 7.0 Administrator's Guide • 77 Manage Firewalls Manage Device Groups Add a Device Group Create a Device Group Hierarchy Create Objects for Use in Shared or Device Group Policy Revert to Inherited Object Values Manage Unused Shared Objects Manage Precedence of Inherited Objects Move or Clone a Policy Rule or Object to a Different Device Group Select a URL Filtering Vendor on Panorama Push a Policy Rule to a Subset of Firewalls Manage the Rule Hierarchy Add a Device Group After adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. ##### PAN-OS doesn't synchronize pushed rules across HA peers. ##### To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.

<https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pan>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

NEW QUESTION 175

- (Exam Topic 3)

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 178

- (Exam Topic 3)

Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

- A. Master
- B. Universal
- C. Shared
- D. Global

Answer: C

NEW QUESTION 182

- (Exam Topic 3)

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 186

- (Exam Topic 3)

Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

- A. X-Auth IPsec VPN
- B. GlobalProtect Apple IOS
- C. GlobalProtect SSL
- D. GlobalProtect Linux

Answer: A

Explanation:

(<http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/>)

NEW QUESTION 190

- (Exam Topic 3)

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/59>

NEW QUESTION 193

- (Exam Topic 3)

Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

- A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
- B. The devices are licensed and ready for deployment.
- C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
- D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
- E. The interface are pingable.

Answer: BC

NEW QUESTION 194

- (Exam Topic 3)

The IT department has received complaints about VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter. Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

- A. QoS Statistics
- B. Applications Report
- C. Application Command Center (ACC)
- D. QoS Log

Answer: A

NEW QUESTION 198

- (Exam Topic 3)

A network engineer has received a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.

Which CLI command will help identify the issue?

- A. test routing fib virtual-router vr1
- B. show routing route type static destination 98.139.183.24
- C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
- D. show routing interface

Answer: C

NEW QUESTION 199

- (Exam Topic 3)

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

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

Answer: ABF

NEW QUESTION 203

- (Exam Topic 3)

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/deter)

NEW QUESTION 207

- (Exam Topic 3)

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 208

- (Exam Topic 3)

Which three log-forwarding destinations require a server profile to be configured? (Choose three)

- A. SNMP Trap
- B. Email
- C. RADIUS
- D. Kerberos
- E. Panorama
- F. Syslog

Answer: ABF

NEW QUESTION 212

- (Exam Topic 3)

When performing the "ping" test shown in this CLI output:

```

name      id      vsys zone      forwarding      tag      address
-----
ethernet1/1 16      1      untrust      vsrcm-ethernet1/2 0      N/A
ethernet1/2 17      1      untrust      vsrcm-ethernet1/1 0      N/A
ethernet1/3 18      1      trust        vsrcm-ethernet1/3 0      10.46.72.93/24
ethernet1/4 20      1      DMZ          vsrcm-ethernet1/4 0      10.30.0.93/24
ethernet1/7 22      1      Trust        vsrcm-ethernet1/7 0      N/A
ethernet1/11 26      1      Trust        vsrcm-ethernet1/11 0      N/A
ethernet1/15 30      2      L3-Trust-V2   vsrcm-ethernet1/15 0      N/A
ethernet1/18 31      0      Trust        vsrcm-ethernet1/18 0      N/A
wan1       48      1      L3-Trust      vsrcm-ethernet1/48 0      192.168.93.1/24
dedicated-ha1 5       0      HA            vsrcm-ethernet1/5 0      1.1.1.1/30
dedicated-ha2 6       0      HA            vsrcm-ethernet1/6 0      2.2.2.1/30

Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:90:0b:34:4c:82

Ip address: 10.46.64.94
Netmask: 255.255.254.0
Default gateway: 10.46.64.1
Ipv6 address: unknown
Ipv6 link local address: unknown
Ipv6 default gateway: unknown

> ping host 8.8.8.8
  
```

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 215

- (Exam Topic 3)

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 217

- (Exam Topic 3)

YouTube videos are consuming too much bandwidth on the network, causing delays in mission-critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:

- * ethernet1/1, Zone: Untrust (Internet-facing)
- * ethernet1/2, Zone: Trust (client-facing)

A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.

Which setting for class 6 with throttle YouTube traffic?

- A. Outbound profile with Guaranteed Ingress
- B. Outbound profile with Maximum Ingress
- C. Inbound profile with Guaranteed Egress
- D. Inbound profile with Maximum Egress

Answer: D

NEW QUESTION 220

- (Exam Topic 3)

Panorama provides which two SD_WAN functions? (Choose two.)

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

Answer: CD

NEW QUESTION 223

- (Exam Topic 3)

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 227

- (Exam Topic 3)

A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.

What can be done to simplify the NAT policy?

- A. Configure ECMP to handle matching NAT traffic
- B. Configure a NAT Policy rule with Dynamic IP and Port
- C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
- D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi-directional option

Answer: C

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples>

NEW QUESTION 230

- (Exam Topic 3)

Palo Alto Networks maintains a dynamic database of malicious domains.

Which two Security Platform components use this database to prevent threats? (Choose two)

- A. Brute-force signatures
- B. BrightCloud Url Filtering
- C. PAN-DB URL Filtering
- D. DNS-based command-and-control signatures

Answer: CD

NEW QUESTION 234

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSE Exam with Our Prep Materials Via below:

<https://www.certleader.com/PCNSE-dumps.html>