



Paloalto-Networks

Exam Questions PCNSE

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

NEW QUESTION 1

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

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

Answer: AB

NEW QUESTION 2

What is the purpose of the firewall decryption broker?

- A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
- B. Force decryption of previously unknown cipher suites
- C. Inspection traffic within IPsec tunnel
- D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 3

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 4

In the following image from Panorama, why are some values shown in red?

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

- A. sg2 session count is the lowest compared to the other managed devices.
- B. us3 has a logging rate that deviates from the administrator-configured thresholds.
- C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
- D. sg2 has misconfigured session thresholds.

Answer: C

NEW QUESTION 5

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

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

Answer: AC

NEW QUESTION 6

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

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

Answer: B

NEW QUESTION 7

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

- A. Virtual router
- B. Security zone
- C. ARP entries
- D. Netflow Profile

Answer: AB

Explanation:

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

NEW QUESTION 8

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.pdf (page 9)

NEW QUESTION 9

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: C

NEW QUESTION 10

To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

Answer: B

Explanation:

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

NEW QUESTION 10

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM- Series firewalls? (Choose two.)

- A. Red Hat Enterprise Virtualization (RHEV)
- B. Kernel Virtualization Module (KVM)
- C. Boot Strap Virtualization Module (BSVM)
- D. Microsoft Hyper-V

Answer: BD

Explanation:

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

NEW QUESTION 14

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.
How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

- A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question:.
- B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question:.

- C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
- D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Answer: C

NEW QUESTION 17

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 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 web browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to this 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: A

NEW QUESTION 22

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

NEW QUESTION 27

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Answer: D

Explanation:

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

NEW QUESTION 28

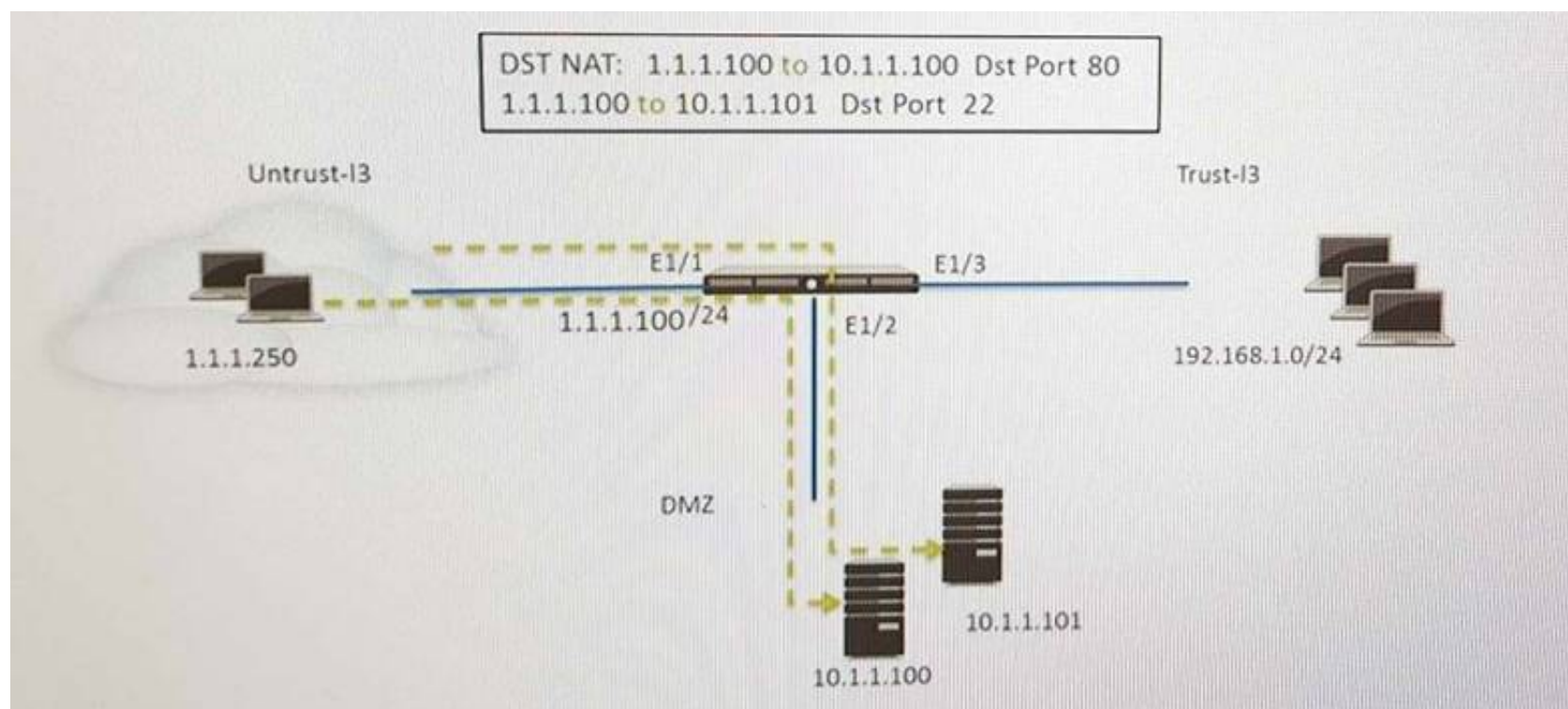
A session in the Traffic log is reporting the application as “incomplete.” What does “incomplete” mean?

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

Answer: B

NEW QUESTION 32

Refer to the exhibit.



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

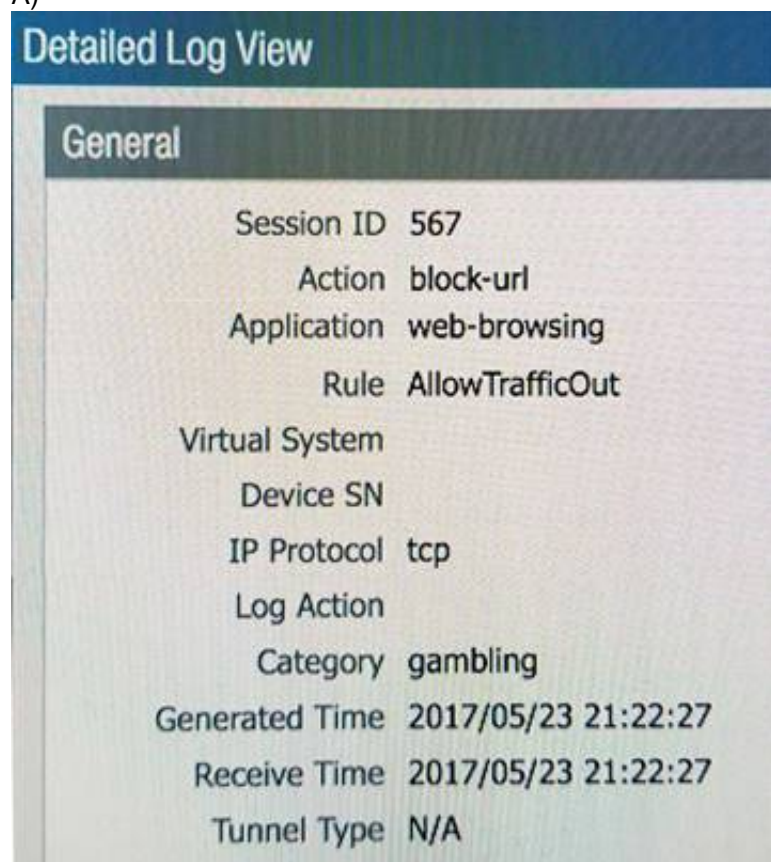
- A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
- D. Untrust (Any) to DMZ (10.1.1.1), ssh -Allow
- E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Answer: CD

NEW QUESTION 34

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
 Which configuration change should the administrator make?

A)



B)

URL Filtering Profile

Name: Filter1
Description:

Overrides Categories URL Filtering Settings User Credential Detection

65 items

Category	Site Access	User Credential Submission
<input type="checkbox"/> educational-institutions	allow	allow
<input type="checkbox"/> entertainment-and-arts	allow	allow
<input type="checkbox"/> extremism	allow	allow
<input type="checkbox"/> financial-services	allow	allow
<input checked="" type="checkbox"/> gambling	allow	block
<input type="checkbox"/> games	alert	allow
<input type="checkbox"/> government	allow	allow
<input type="checkbox"/> hacking	block	allow
<input type="checkbox"/> health-and-medicine	continue	allow
<input type="checkbox"/> home-and-garden	override	allow
<input type="checkbox"/> hunting-and-fishing	allow	allow

* Indicates a custom URL category, + indicates external dynamic list
[Check URL Category](#)

C)

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: www.megamillions.com

Rule Type: universal (default)

Description:

D)

URL Filtering Profile

Name: Filter1
Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow List: www.megamillions.com

Block List:

Action: continue

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com" will match "www.example.com/test" but not match "www.example.com.hk"

OK

E)

URL Filtering Profile

Name: Filter1
Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow List: www.megamillions.com

Block List:

Action: block

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

Answer: B

NEW QUESTION 37

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: ADE

NEW QUESTION 39

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

How quickly will the firewall receive back a verdict?

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

Answer: D

NEW QUESTION 40

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

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

Answer: A

NEW QUESTION 41

Which Palo Alto Networks VM-Series firewall is valid?

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

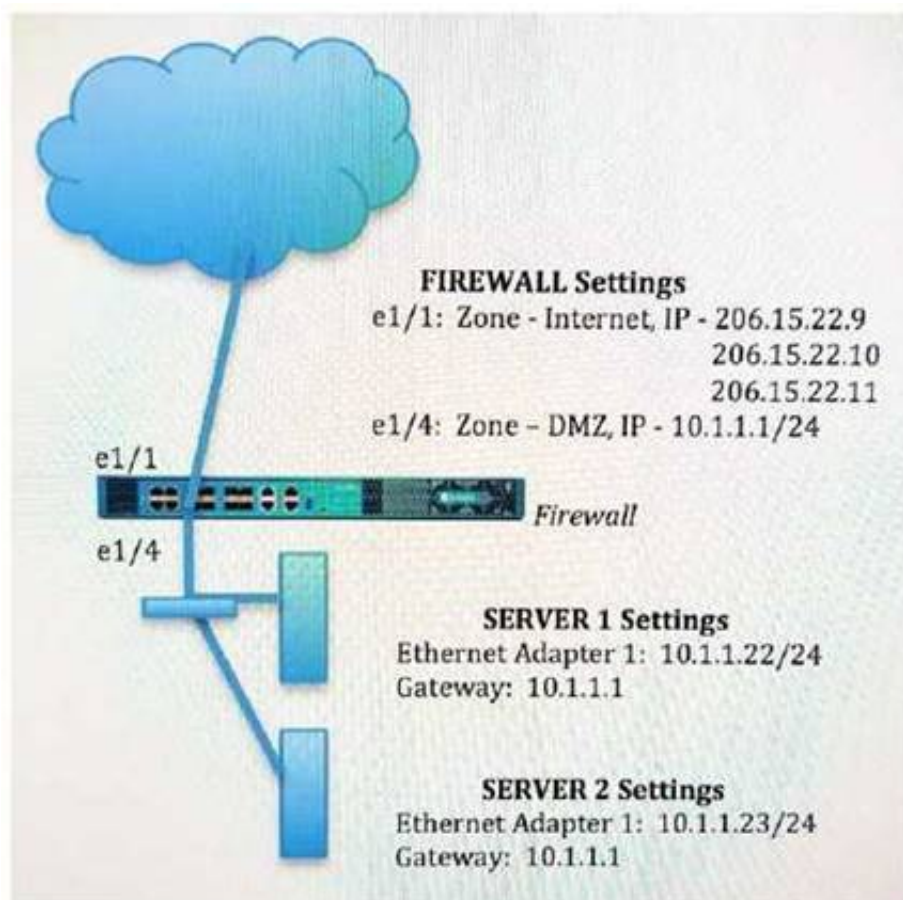
Answer: C

Explanation:

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

NEW QUESTION 46

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22



Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?

A)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

D)

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

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

Answer: D

NEW QUESTION 50

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 55

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

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

Answer: A

Explanation:

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

NEW QUESTION 57

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

Answer: A

NEW QUESTION 58

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN- OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

- A. Security policy rule
- B. CRL
- C. Service route
- D. Scheduler

Answer: A

NEW QUESTION 63

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt
- C. IPsec tunnel encryption
- D. Packet egress process

Answer: A

NEW QUESTION 67

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=AOvVaw0H9qgaJK0oI2xjIJBNo1Km

NEW QUESTION 69

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

- A. ACC

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

Answer: D

NEW QUESTION 71

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

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

Answer: A

NEW QUESTION 75

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 77

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 80

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

- A. Session Browser
- B. Application Command Center
- C. TCP Dump
- D. Packet Capture

Answer: B

Explanation:

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

NEW QUESTION 83

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 88

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 93

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router. Which two options would help the administrator troubleshoot this issue? (Choose two.)

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

Answer: CD

NEW QUESTION 97

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>

NEW QUESTION 99

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 101

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

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

Answer: D

Explanation:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network>

NEW QUESTION 104

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 107

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

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

Answer: A

NEW QUESTION 112

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 117

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 119

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

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

Answer: A

NEW QUESTION 122

A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

- A. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
- B. Repeat forevery additional VLANand use a VLAN ID of 0 for untagged traffi
- C. Assign each interface/subinterface to a unique zone.
- D. Create V-Wire objects with two V-Wire sub interface and assign only a single VLAN ID to the "Tag Allowed field one of the V-Wire object Repeat for every additional VLAN and use a VIAN ID of 0 for untagged traffi
- E. Assign each interface/subinterfaceto a unique zone.
- F. Create V-Wire objects with two V-Wire interfaces and define a range "0- 4096" in the 'Tag Allowed filed of the V-Wire object.
- G. Create Layer 3 sub interfaces that are each assigned to a single VLAN ID and a common virtual route
- H. The physical Layer 3interface would handle untagged traffi
- I. Assign each interface /subinterface to a unique zon
- J. Do not assign any interface anIP address

Answer: C

NEW QUESTION 124

Which logs enable a firewall administrator to determine whether a session was decrypted?

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

Answer: B

NEW QUESTION 127

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 131

Which User-ID method maps IP address to usernames for users connecting through a web proxy that has already authenticated the user?

- A. Client Probing
- B. Port mapping
- C. Server monitoring
- D. Syslog listening

Answer: D

NEW QUESTION 132

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

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

Answer: A

NEW QUESTION 136

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 139

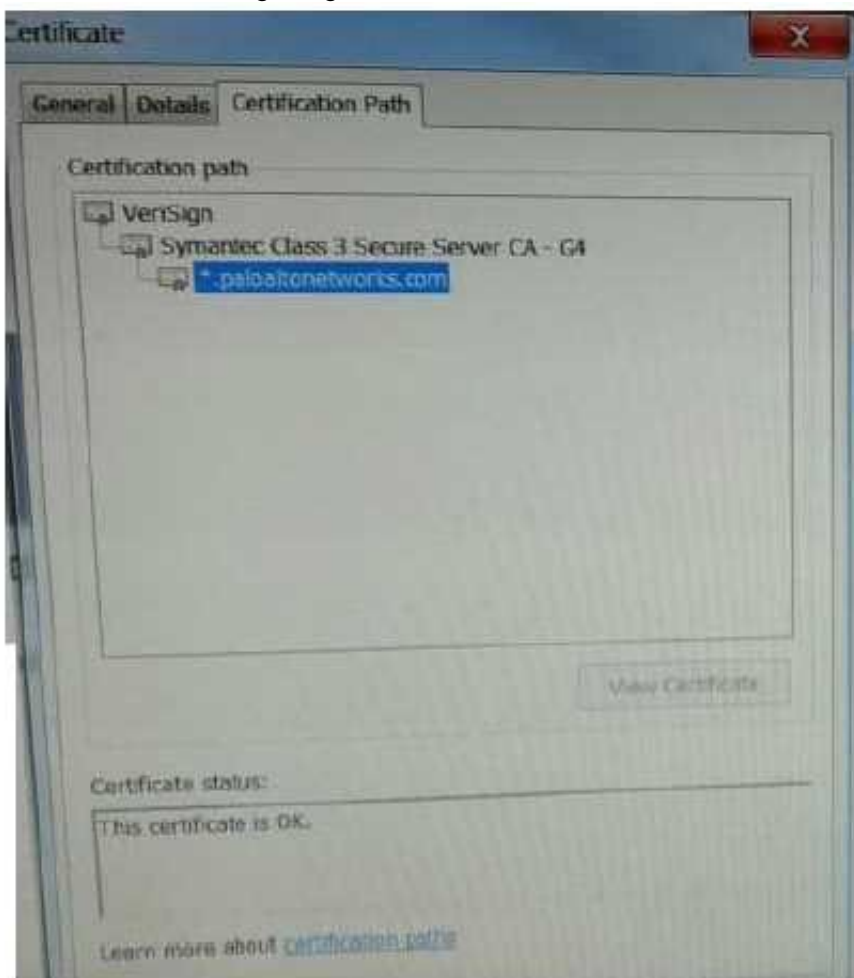
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

Answer: AB

NEW QUESTION 141

Based on the following image,



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

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

Answer: D

NEW QUESTION 144

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

Answer: A

NEW QUESTION 148

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

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

Answer: D

NEW QUESTION 151

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

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

Answer: BE

NEW QUESTION 154

Click the Exhibit button



An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company. What would be the administrator's next step?

- A. Right-Click on the bittorrent link and select Value from the context menu

- B. Create a global filter for bittorrent traffic and then view Traffic logs.
- C. Create local filter for bittorrent traffic and then view Traffic logs.
- D. Click on the bittorrent application link to view network activity

Answer: D

NEW QUESTION 156

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 160

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 162

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

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

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

Answer: C

NEW QUESTION 164

A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and port.

Which option when enabled with the correction threshold would mitigate this attack without dropping legitimate traffic to other hosts inside the network?

- A. Zone Protection Policy with UDP Flood Protection
- B. QoS Policy to throttle traffic below maximum limit
- C. Security Policy rule to deny traffic to the IP address and port that is under attack
- D. Classified DoS Protection Policy using destination IP only with a Protect action

Answer: D

NEW QUESTION 168

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 169

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 172

A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.

Given the following zone information:

- DMZ zone: DMZ-L3
- Public zone: Untrust-L3
- Guest zone: Guest-L3
- Web server zone: Trust-L3
- Public IP address (Untrust-L3): 1.1.1.1
- Private IP address (Trust-L3): 192.168.1.50

What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

- A. Untrust-L3
- B. DMZ-L3
- C. Guest-L3
- D. Trust-L3

Answer: A

NEW QUESTION 175

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

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

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

Answer: D

NEW QUESTION 179

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 180

What are three valid method of user mapping? (Choose three)

- A. Syslog
- B. XML API
- C. 802.1X
- D. WildFire
- E. Server Monitoring

Answer: ABE

NEW QUESTION 181

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

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

Answer: BEF

Explanation:

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

NEW QUESTION 183

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

- A. From the CLI, issue the show counter global filter pcap yes command.
- B. From the CLI, issue the show counter global filter packet-filter yes command.

- C. From the GUI, select show global counters under the monitor tab.
- D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 184

Which interface configuration will accept specific VLAN IDs?

- A. Tab Mode
- B. Subinterface
- C. Access Interface
- D. Trunk Interface

Answer: B

NEW QUESTION 188

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 193

Support for which authentication method was added in PAN-OS 8.0?

- A. RADIUS
- B. LDAP
- C. Diameter
- D. TACACS+

Answer: D

Explanation:

<https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1>

NEW QUESTION 194

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 198

Which option is an IPv6 routing protocol?

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

Answer: B

NEW QUESTION 201

Firewall administrators cannot authenticate to a firewall GUI.

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

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

Answer: BC

NEW QUESTION 205

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

Which configuration setting needs to be modified?

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

Answer: A

NEW QUESTION 210

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

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

Answer: B

Explanation:

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions>

NEW QUESTION 215

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>"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>"palo

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

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

NEW QUESTION 219

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

NEW QUESTION 222

Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.

How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

- A. Enable on Site-A only
- B. Enable on Site-B only
- C. Enable on Site-B only with passive mode
- D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 225

Which field is optional when creating a new Security Policy rule?

- A. Name
- B. Description
- C. Source Zone
- D. Destination Zone

E. Action

Answer: B

NEW QUESTION 226

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCNSE Practice Exam Features:

- * PCNSE Questions and Answers Updated Frequently
- * PCNSE Practice Questions Verified by Expert Senior Certified Staff
- * PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCNSE Practice Test Here](#)