



Paloalto-Networks

Exam Questions PCNSE

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

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 2)

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

Which configuration will enable this HA scenario?

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

Answer: A

NEW QUESTION 2

- (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 3

- (Exam Topic 2)

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-inte>

NEW QUESTION 4

- (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. Replay
- C. Web Application
- D. DoS Protection

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#>

NEW QUESTION 5

- (Exam Topic 2)

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

Answer: A

NEW QUESTION 6

- (Exam Topic 2)

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

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

Answer:

AD

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#>

NEW QUESTION 7

- (Exam Topic 2)

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

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

Answer: AD

NEW QUESTION 8

- (Exam Topic 2)

To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations

Which one is the correct configuration?

- A. @Panorama
- B. #Pancrama
- C. &Panorama
- D. \$Panorama

Answer: D

NEW QUESTION 9

- (Exam Topic 2)

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>

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series>

NEW QUESTION 10

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 2)

How does Panorama prompt VMWare NSX to quarantine an infected VM?

- A. HTTP Server Profile
- B. Syslog Server Profile
- C. Email Server Profile
- D. SNMP Server Profile

Answer: A

NEW QUESTION 14

- (Exam Topic 2)

What is the purpose of the firewall decryption broker?

- A. Decrypt SSL traffic and 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 18

- (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 21

- (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 24

- (Exam Topic 2)

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

Answer: A

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0>

NEW QUESTION 26

- (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 28

- (Exam Topic 2)

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

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>

NEW QUESTION 31

- (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 35

- (Exam Topic 2)

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

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

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers>

NEW QUESTION 36

- (Exam Topic 2)

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: B

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFIcAK>

NEW QUESTION 38

- (Exam Topic 2)

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

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

Answer: C

Explanation:

System Resources (widget) Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or

Panorama). <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widg>

NEW QUESTION 43

- (Exam Topic 2)

Which administrative authentication method supports authorization by an external service?

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

Answer: C

NEW QUESTION 47

- (Exam Topic 2)

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

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

Answer: AD

Explanation:

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

NEW QUESTION 51

- (Exam Topic 2)

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

Answer: C

Explanation:

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalpr>

NEW QUESTION 56

- (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 57

- (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 traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

- A. Create a custom App-ID and enable scanning on the advanced tab.
- B. Create an Application Override policy.
- C. Create a custom App-ID and use the “ordered conditions” check box.
- D. Create an Application Override policy and custom threat signature for the application.

Answer: A

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRoCAK>

NEW QUESTION 58

- (Exam Topic 2)

At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?

- A. exploitation
- B. IP command and control
- C. delivery
- D. reconnaissance

Answer: D

NEW QUESTION 61

- (Exam Topic 2)

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. Wildfire update package
- B. User-ID agent
- C. Anti virus update package
- D. Application and Threats update package

Answer: D

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.

: <https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045>

NEW QUESTION 64

- (Exam Topic 2)

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

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

Answer: CD

Explanation:

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-update>

NEW QUESTION 66

- (Exam Topic 1)

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 70

- (Exam Topic 1)

Which statement accurately describes service routes and virtual systems?

- A. Virtual systems can only use one interface for all global service and service routes of the firewall
- B. The interface must be used for traffic to the required external services
- C. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall
- D. Virtual systems cannot have dedicated service routes configured: and virtual systems always use the global service and service route settings for the firewall

Answer: A

NEW QUESTION 72

- (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 76

- (Exam Topic 1)

During SSL decryption which three factors affect resource consumption1? (Choose three)

- A. TLS protocol version
- B. transaction size
- C. key exchange algorithm
- D. applications that use non-standard ports
- E. certificate issuer

Answer: ABC

Explanation:

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ss>

NEW QUESTION 80

- (Exam Topic 1)

Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

- A. PAN-OS integrated User-ID agent
- B. LDAP Server Profile configuration
- C. GlobalProtect
- D. Windows-based User-ID agent

Answer: A

NEW QUESTION 83

- (Exam Topic 1)

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

- A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
- B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
- C. Enterprise-Intermediate-CAi
- D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits [https //www example-website com/](https://www.example-website.com/) with a server certificate Common Name (CN) [www example-website com](https://www.example-website.com/) The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for [www example-website com](https://www.example-website.com/) was issued by which of the following?
- E. Enterprise-Untrusted-CA which is a self-signed CA
- F. Enterprise-Trusted-CA which is a self-signed CA
- G. Enterprise-Intermediate-CA which wa
- H. in turn, issued by Enterprise-Root-CA
- I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 84

- (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 85

- (Exam Topic 1)

A firewall should be advertising the static route 10.2.0.0/24 into OSPF. The configuration on the neighbor is correct but the route is not in the neighbor's routing table. Which two configurations should you check on the firewall? (Choose two.)

- A. Within the redistribution profile ensure that Redist is selected
- B. In the redistribution profile check that the source type is set to "ospf"
- C. In the OSFP configuration ensure that the correct redistribution profile is selected in the OSPF Export Rules section
- D. Ensure that the OSPF neighbor state is "2-Way"

Answer: AC

NEW QUESTION 87

- (Exam Topic 1)

What are two characteristic types that can be defined for a variable? (Choose two.)

- A. zone
- B. FQDN
- C. path group
- D. IP netmask

Answer: BD

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-tem>

NEW QUESTION 90

- (Exam Topic 1)

In a security-first network, what is the recommended threshold value for content updates to be dynamically updated?

- A. 1 to 4 hours
- B. 6 to 12 hours
- C. 24 hours
- D. 36 hours

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-thr>

NEW QUESTION 92

- (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 94

- (Exam Topic 1)

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world. Panorama will manage the firewalls.

The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure. The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration.

Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. variables
- B. template stacks
- C. collector groups
- D. virtual systems

Answer: C

NEW QUESTION 99

- (Exam Topic 1)

An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls.

The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls. If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the

configuration does not appear what is the root cause?

- A. Panorama has no connection to Palo Alto Networks update servers
- B. Panorama does not have valid licenses to push the dynamic updates
- C. No service route is configured on the firewalls to Palo Alto Networks update servers
- D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed

Answer: D

NEW QUESTION 100

- (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 104

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 107

- (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 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: 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 108

- (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 109

- (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 110

- (Exam Topic 2)

An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

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

Answer: B

Explanation:

<https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-t>

NEW QUESTION 112

- (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 I 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 113

- (Exam Topic 3)

Which two events trigger the operation of automatic commit recovery? (Choose two.)

- A. when an aggregate Ethernet interface component fails
- B. when Panorama pushes a configuration
- C. when a firewall HA pair fails over
- D. when a firewall performs a local commit

Answer: BD

NEW QUESTION 118

- (Exam Topic 3)

Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

- A. ms.log
- B. traffic.log
- C. system.log
- D. dp-monitor.log
- E. authd.log

Answer: CE

NEW QUESTION 121

- (Exam Topic 3)

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 124

- (Exam Topic 3)

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

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

Answer: ACE

NEW QUESTION 129

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 132

- (Exam Topic 3)

Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

- A. VM-100
- B. VM-200
- C. VM-1000-HV
- D. VM-300

Answer: C

NEW QUESTION 133

- (Exam Topic 3)

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 137

- (Exam Topic 3)

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

Which Link Type setting will correct the error?

- A. Set 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 141

- (Exam Topic 3)

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

Which security Profile type will prevent these behaviors?

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

Answer: D

NEW QUESTION 145

- (Exam Topic 3)

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 indecating 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 150

- (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 155

- (Exam Topic 3)

Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

- A. link requirements
- B. the name of the ISP
- C. IP Addresses
- D. branch and hub locations

Answer: ACD

NEW QUESTION 159

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 163

- (Exam Topic 3)

In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall. Which authentication method must be used?

- A. LDAP
- B. Kerberos
- C. Certification based authentication
- D. RADIUS with Vendor-Specific Attributes

Answer: D

NEW QUESTION 168

- (Exam Topic 3)

Click the Exhibit button below,

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

Which is the next hop IP address for the HTTPS traffic from Will's PC?

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

Answer: C

NEW QUESTION 173

- (Exam Topic 3)

People are having intermittent quality issues during a live meeting via web application.

- A. Use QoS profile to define QoS Classes
- B. Use QoS Classes to define QoS Profile
- C. Use QoS Profile to define QoS Classes and a QoS Policy
- D. Use QoS Classes to define QoS Profile and a QoS Policy

Answer: C

NEW QUESTION 176

- (Exam Topic 3)

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 181

- (Exam Topic 3)

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-os/newfeaturesguide/wildfire-features/wildfire-grayw>

NEW QUESTION 182

- (Exam Topic 3)

A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information.

Users outside the company are in the "Untrust-L3" zone

The web server physically resides in the "Trust-L3" zone.

Web server public IP address: 23.54.6.10

Web server private IP address: 192.168.1.10

Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two)

- A. Untrust-L3 for both Source and Destination zone
- B. Destination IP of 192.168.1.10
- C. Untrust-L3 for Source Zone and Trust-L3 for Destination Zone
- D. Destination IP of 23.54.6.10

Answer: CD

NEW QUESTION 186

- (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 189

.....

Relate Links

100% Pass Your PCNSE Exam with ExamBible Prep Materials

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

Contact us

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

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