

PaloAltoNetworks.PCNSA.v2024-11-18.q240

Exam Code:	PCNSA
Exam Name:	Palo Alto Networks Certified Network Security Administrator
Certification Provider:	Palo Alto Networks
Free Question Number:	240
Version:	v2024-11-18
# of views:	2302
# of Questions views:	2400
https://www.exam-tests.com/PCNSA-exam/PaloAltoNetworks.PCNSA.v2024-11-18.q240.html	

NEW QUESTION: 1

What are two differences between an implicit dependency and an explicit dependency in App-ID? (Choose two.)

- A. An implicit dependency requires the dependent application to be added in the security policy
- B. An explicit dependency does not require the dependent application to be added in the security policy
- C. An implicit dependency does not require the dependent application to be added in the security policy
- D. An explicit dependency requires the dependent application to be added in the security policy

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 2

Which two protocols are available on a Palo Alto Networks Firewall Interface Management Profile? (Choose two.)

- A. HTTPS
- B. RDP
- C. SSH
- D. SCP

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 3

Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

- A. security processing
- B. network processing
- C. data
- D. management

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 4

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

- A. after clicking Check New in the Dynamic Update window
- B. after connecting the firewall configuration
- C. after installing the update
- D. after downloading the update

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 5

Based on the screenshot what is the purpose of the group in User labelled "it"?

- A. Allows users in group "it" to access IT applications
- B. Allows users in group "DMZ" to access IT applications
- C. Allows "any" users to access servers in the DMZ zone
- D. Allows users to access IT applications on all ports

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

The PowerBall Lottery has reached an unusually high value this week. Your company has decided to raise morale by allowing employees to access the PowerBall Lottery website (www.powerball.com) for just this week. However, the company does not want employees to access any other websites also listed in the URL filtering "gambling" category.

Which method allows the employees to access the PowerBall Lottery website but without unblocking access to the "gambling" URL category?

- A. Create a custom URL category, add *.powerball.com to it and allow it in the Security Profile.
- B. Add *.powerball.com to the URL Filtering allow list.
- C. Add just the URL www.powerball.com to a Security policy allow rule.
- D. Manually remove powerball.com from the gambling URL category.

Answer: A,B ([LEAVE A REPLY](#))

NEW QUESTION: 7

What do dynamic user groups you to do?

- A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity
- B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity
- C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity
- D. create a dynamic list of firewall administrators

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 8

Which action related to App-ID updates will enable a security administrator to view the existing security policy rule that matches new application signatures?

- A. Review Policies
- B. Review Apps
- C. Pre-analyze
- D. Review App Matches

Answer: A ([LEAVE A REPLY](#))

References:

NEW QUESTION: 9

Based on the graphic, which statement accurately describes the output shown in the Server Monitoring panel?

- A. The User-ID agent is connected to a domain controller labeled lab-client.
- B. The host lab-client has been found by the User-ID agent.
- C. The host lab-client has been found by a domain controller.
- D. The User-ID agent is connected to the firewall labeled lab-client.

Answer: A ([LEAVE A REPLY](#))

lab-client is not a host, it is the name we are giving to the agent that is connecting to the specified domain controller (Active Directory).

NEW QUESTION: 10

Based on the screenshot what is the purpose of the included groups?

- A. They are used to map usernames to group names.
- B. They are only groups visible based on the firewall's credentials.
- C. They are groups that are imported from RADIUS authentication servers.
- D. They contain only the users you allow to manage the firewall.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 11

Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

- A. XML API
- B. log forwarding auto-tagging
- C. GlobalProtect agent
- D. User-ID Windows-based agent

Answer: A,D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profil>

NEW QUESTION: 12

Which license is required to use the Palo Alto Networks built-in IP address EDLs?

- A. DNS Security
- B. Threat Prevention
- C. WildFire
- D. SD-Wan

Answer: B ([LEAVE A REPLY](#))

An active Threat Prevention license is required to obtain Palo Alto Networks built-in EDLs. These built-in EDLs protect your network against malicious hosts.

NEW QUESTION: 13

Given the image, which two options are true about the Security policy rules. (Choose two.)

- A. In the Allow FTP to web server rule, FTP is allowed using App-ID
- B. The Allow Office Programs rule is using an Application Filter
- C. In the Allow Social Networking rule, allows all of Facebook's functions
- D. The Allow Office Programs rule is using an Application Group

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 14

Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

- A. global
- B. intrazone
- C. interzone
- D. universal

Answer: ([SHOW ANSWER](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>

NEW QUESTION: 15

Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH. web-browsing and SSL applications Which policy achieves the desired results?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 16

Arrange the correct order that the URL classifications are processed within the system.

Answer:

Explanation:

First - Block List

Second - Allow List

Third - Custom URL Categories

Fourth - External Dynamic Lists

Fifth - Downloaded PAN-DB Files

Sixth - PAN-DB Cloud

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

Which component is a building block in a Security policy rule?

- A. decryption profile
- B. destination interface
- C. timeout (min)
- D. application

Answer: (SHOW ANSWER)

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/building-blocks-in-a-security-policy-rule.html>

NEW QUESTION: 18

An administrator is updating Security policy to align with best practices.

Which Policy Optimizer feature is shown in the screenshot below?

- A. Rules without App Controls
- B. Rule Usage
- C. New App Viewer
- D. Unused Unused Apps

Answer: B (LEAVE A REPLY)

NEW QUESTION: 19

Which interface does not require a MAC or IP address?

- A. Virtual Wire
- B. Layer3
- C. Layer2
- D. Loopback

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 20

View the diagram. What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 21

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

- A. branch office traffic
- B. east-west traffic
- C. perimeter traffic
- D. north-south traffic

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 22

Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

- A. XML API
- B. log forwarding auto-tagging
- C. User-ID Windows-based agent
- D. GlobalProtect agent

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

Given the topology, which zone type should you configure for firewall interface E1/1?

- A. Tap
- B. Tunnel
- C. Virtual Wire

D. Layer3

Answer: A ([LEAVE A REPLY](#))

Tap - A Tap interface monitors traffic that is connected to a network switch's MIRROR/SPAN port.

NEW QUESTION: 24

An internal host wants to connect to servers of the internet through using source NAT.

Which policy is required to enable source NAT on the firewall?

- A. NAT policy with source zone and destination zone specified
- B. post-NAT policy with external source and any destination address
- C. NAT policy with no source or destination zone selected
- D. pre-NAT policy with external source and any destination address

Answer: A ([LEAVE A REPLY](#))

Explanation

NEW QUESTION: 25

Based on the security policy rules shown, ssh will be allowed on which port?

- A. 53
- B. 22
- C. 23
- D. 80

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 26

To what must an interface be assigned before it can process traffic?

- A. Security Protection
- B. Security policy
- C. Security Zone
- D. Security profile

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 27

Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

- A. Palo Alto Networks Bulletproof IP Addresses
- B. Palo Alto Networks C&C IP Addresses
- C. Palo Alto Networks Known Malicious IP Addresses
- D. Palo Alto Networks High-Risk IP Addresses

Answer: A ([LEAVE A REPLY](#))

To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.

NEW QUESTION: 28

An administrator is configuring a NAT rule

At a minimum, which three forms of information are required? (Choose three.)

- A. name
- B. destination interface
- C. destination address
- D. source zone
- E. destination zone

Answer: C,D,E ([LEAVE A REPLY](#))

NEW QUESTION: 29

An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

- A. Disable all logging
- B. Enable Log at Session Start
- C. Enable Log at Session End
- D. Enable Log at both Session Start and End

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 30

Match the Cyber-Attack Lifecycle stage to its correct description.

Answer:

Explanation

Reconnaissance - stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation - stage where the attacker will explore methods such as a root kit to establish

persistence Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.

Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION: 31

Which two statements apply to an Advanced Threat Prevention subscription? (Choose two.)

- A. Due to its more advanced signatures, it provides the ability to identify new threats.
- B. When it is active, a WildFire profile is no longer needed.
- C. It contains all the features already in a Threat Prevention subscription.
- D. It provides the ability to identify evasive and previously unseen command-and-control (C2) threats.

Answer: C,D ([LEAVE A REPLY](#))

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

- A. Untrust (any) to DMZ (1.1.1.100), web browsing - Allow
- B. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
- C. Untrust (any) to Untrust (1.1.1.100), web browsing - Allow
- D. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 33

Which definition describes the guiding principle of the zero-trust architecture?

- A. never trust, never connect
- B. always connect and verify
- C. never trust, always verify
- D. trust, but verify

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>

NEW QUESTION: 34

What must be considered with regards to content updates deployed from Panorama?

- A. Content update schedulers need to be configured separately per device group.
- B. Panorama can only install up to five content versions of the same type for potential rollback scenarios.
- C. A PAN-OS upgrade resets all scheduler configurations for content updates.
- D. Panorama can only download one content update at a time for content updates of the same type.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 35

Which profile should be used to obtain a verdict regarding analyzed files?

- A. Content-ID

- B. WildFire analysis
- C. Advanced threat prevention
- D. Vulnerability profile

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 36

Which three onfiguration settings are required on a Palo Alto networks firewall management interface?

- A. default gateway
- B. IP address
- C. hostname
- D. auto-negotiation
- E. netmask

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 37

Refer to the exhibit.

Based on the network diagram provided, which two statements apply to traffic between the User and Server networks? (Choose two.)

- A. Traffic is permitted through the default intrazone "allow" rule.
- B. Traffic restrictions are possible by modifying intrazone rules.
- C. Traffic restrictions are not possible, because the networks are in the same zone.
- D. Traffic is permitted through the default interzone "allow" rule.

Answer: ([SHOW ANSWER](#)**)**

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITHCA0&lang=es>

NEW QUESTION: 38

Which three interface deployment methods can be used to block traffic flowing through the Palo Alto Networks firewall? (Choose three.)

- A. Layer 3
- B. Virtual Wire
- C. Layer 2
- D. HA
- E. Tap

Answer: A,B,D ([LEAVE A REPLY](#))

NEW QUESTION: 39

Which order of steps is the correct way to create a static route?

- A. 1) Enter the route and netmask
- 2) Enter the IP address for the specific next hop

- 3) Specify the outgoing interface for packets to use to go to the next hop
- 4) Add an IPv4 or IPv6 route by name

B. 1) Enter the route and netmask

- 2) Specify the outgoing interface for packets to use to go to the next hop
- 3) Enter the IP address for the specific next hop
- 4) Add an IPv4 or IPv6 route by name

C. 1) Enter the IP address for the specific next hop

- 2) Enter the route and netmask
- 3) Add an IPv4 or IPv6 route by name
- 4) Specify the outgoing interface for packets to use to go to the next hop

D. 1) Enter the IP address for the specific next hop

- 2) Add an IPv4 or IPv6 route by name
- 3) Enter the route and netmask
- 4) Specify the outgoing interface for packets to use to go to the next hop

Answer: A ([LEAVE A REPLY](#))

Enter the route and netmask

Enter the IP address for the specific next hop

Specify the outgoing interface for packets to use to go to the next hop Add an IPv4 or IPv6 route by name Comprehensive This is the correct order of steps to create a static route in a virtual router on the firewall. The first step is to enter the route and netmask for the destination network, such as 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address. The second step is to enter the IP address for the specific next hop, such as 192.168.56.1 or 2001:db8:49e:1::1. The third step is to specify the outgoing interface for packets to use to go to the next hop, such as ethernet1/1. The fourth step is to add an IPv4 or IPv6 route by name, such as route11. Reference:

Configure a Static Route - Palo Alto Networks

NEW QUESTION: 40

What allows a security administrator to preview the Security policy rules that match new application signatures?

- A.** Review Release Notes
- B.** Dynamic Updates-Review Policies
- C.** Dynamic Updates-Review App
- D.** Policy Optimizer-New App Viewer

Answer: B ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy-rules>

NEW QUESTION: 41

In the example security policy shown, which two websites would be blocked? (Choose two.)

- A.** LinkedIn

- B. YouTube
- C. Facebook
- D. Amazon

Answer: A,C ([LEAVE A REPLY](#))

NEW QUESTION: 42

An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.

Which Security profile should be used?

- A. Vulnerability protection
- B. Anti-spyware
- C. URL filtering
- D. Antivirus

Answer: A ([LEAVE A REPLY](#))

Vulnerability Protection profiles protect against threats entering the network. For example, Vulnerability Protection profiles help protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

<https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-vulnerability-protection>

NEW QUESTION: 43

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

- A. after downloading the update
- B. after installing the update
- C. after connecting the firewall configuration
- D. after clicking Check New in the Dynamic Update window

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH, web-browsing and SSL applications.

Which policy achieves the desired results?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 45

Choose the option that correctly completes this statement. A Security Profile can block or allow traffic _____.

- A. on either the data plane or the management plane.
- B. after it is matched by a security policy rule that allows traffic.
- C. before it is matched to a Security policy rule.
- D. after it is matched by a security policy rule that allows or blocks traffic.

Answer: B (LEAVE A REPLY)

After a packet has been allowed by the Security policy, Security Profiles are used to scan packets for threats, vulnerabilities, viruses, spyware, malicious URLs, data exfiltration, and exploitation software.

NEW QUESTION: 46

Drag and Drop Question

Place the following steps in the packet processing order of operations from first to last.

Select and Place:

Answer:

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam! BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:
<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

Match the Cyber-Attack Lifecycle stage to its correct description.

Answer:

NEW QUESTION: 48

The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop. The malware contacted a known command-and-control server, which caused the infected laptop to begin exfiltrating corporate data.

Which security profile feature could have been used to prevent the communication with the command-and- control server?

- A. Create a URL filtering profile and block the DNS Sinkhole URL category
- B. Create an antivirus profile and enable its DNS Sinkhole feature.
- C. Create an anti-spyware profile and enable DNS Sinkhole feature.
- D. Create a Data Filtering Profiles and enable its DNS Sinkhole feature.

Answer: (SHOW ANSWER)

NEW QUESTION: 49

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?

- A. Network Processing
- B. Signature Matching
- C. Security Matching
- D. Security Processing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 50

Which path is used to save and load a configuration with a Palo Alto Networks firewall?

- A. Device>Setup>Management
- B. Device>Setup>Interfaces
- C. Device>Setup>Operations
- D. Device>Setup>Services

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 51

What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

- A. Configure a URL Filtering profile.
- B. Plan for mobile-employee risk
- C. Implement a threat intel program.
- D. Rely on a DNS resolver.
- E. Train your staff to be security aware.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

An administrator would like to determine the default deny action for the application dns-over-https. Which action would yield the information?

- A. Check the action for the decoder in the antivirus profile
- B. Check the action for the Security policy matching that traffic
- C. View the application details in Objects > Applications
- D. View the application details in beacon paloaltonetworks.com

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 53

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

- A. TACACS+

- B. RADIUS
- C. LDAP
- D. SAML

Answer: C ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence>

NEW QUESTION: 54

What must you configure to enable the firewall to access multiple Authentication Profiles to authenticate a non-local account?

- A. authentication sequence
- B. LDAP server profile
- C. authentication server list
- D. authentication list profile

Answer: A ([LEAVE A REPLY](#))

Authentication Sequence Admin Roles for external administrator accounts can be assigned to an Authentication Sequence, which includes a sequence of one or more Authentication Profiles that are processed in a specific order. The firewall checks against each Authentication Profile within the Authentication Sequence until one Authentication Profile successfully authenticates the user.

NEW QUESTION: 55

Which action would an administrator take to ensure that a service object will be available only to the selected device group?

- A. create the service object in the specific template
- B. uncheck the shared option
- C. ensure that disable override is selected
- D. ensure that disable override is cleared

Answer: ([SHOW ANSWER](#)**)**

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups/crea>

NEW QUESTION: 56

The firewall sends employees an application block page when they try to access Youtube. Which Security policy rule is blocking the youtube application?

- A. Deny Google
- B. allowed-security services
- C. interzone-default
- D. intrazone-default

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 57

Match the network device with the correct User-ID technology.

Answer:

Explanation

Microsoft Exchange - Server monitoring

Linux authentication - syslog monitoring

Windows Client - client probing

Citrix client - Terminal Services agent

NEW QUESTION: 58

What are two valid selections within an Anti-Spyware profile? (Choose two.)

A. Default

B. Deny

C. Random early drop

D. Drop

Answer: A,D ([LEAVE A REPLY](#))

Deny is a policy action, random early drop is part of the inner workings of DoS protection

NEW QUESTION: 59

Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

A. internal-inside-dmz

B. inside-portal

C. intercone-default

D. egress outside

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 60

Based on the screenshot, what is the purpose of the Included Groups?

A. They are groups that are imported from RADIUS authentication servers.

B. They are the only groups visible based on the firewall's credentials.

C. They contain only the users you allow to manage the firewall.

D. They are used to map users to groups.

Answer: ([SHOW ANSWER](#)**)**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html>

NEW QUESTION: 61

Access to which feature requires the PAN-OS Filtering license?

A. PAN-DB database

B. DNS Security

C. Custom URL categories

D. URL external dynamic lists

Answer: A ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html>

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPASS.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 62

You receive notification about new malware that infects hosts through malicious files transferred by FTP.

Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

- A. URL Filtering profile applied to inbound Security policy rules.
- B. Data Filtering profile applied to outbound Security policy rules.
- C. Antivirus profile applied to inbound Security policy rules.
- D. Vulnerability Protection profile applied to outbound Security policy rules.

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 63

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

- A. branch office traffic
- B. east-west traffic
- C. perimeter traffic
- D. north-south traffic

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 64

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. Before deploying content updates, always check content release version compatibility.
- B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- C. Content updates for firewall A/A HA pairs need a defined master device.

D. After deploying content updates, perform a commit and push to Panorama.

Answer: D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama.html>

NEW QUESTION: 65

Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

- A.** authorization
- B.** continue
- C.** authentication
- D.** override

Answer: D ([LEAVE A REPLY](#))

OVERRIDE -The user will see a response page indicating that a password is required to allow access to websites in the given category. With this option, the security administrator or help-desk person would provide a password granting temporary access to all websites in the given category. A log entry is generated in the URL Filtering log. The Override webpage doesn't display properly on client systems configured to use a proxy server.

NEW QUESTION: 66

Selecting the option to revert firewall changes will replace what settings?

- A.** the candidate configuration with settings from the running configuration
- B.** dynamic update scheduler settings
- C.** the running configuration with settings from the candidate configuration
- D.** the device state with settings from another configuration

Answer: D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration-backups/revert-firewall-configuration-changes.html>

NEW QUESTION: 67

In the example security policy shown, which two websites would be blocked? (Choose two.)

- A.** LinkedIn
- B.** YouTube
- C.** Amazon
- D.** Facebook

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 68

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

- A. At the CLI enter the command reset rules and press Enter
- B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule
- C. Reboot the firewall
- D. Use the Reset Rule Hit Counter > All Rules option

Answer: D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/policies/policies-security/creating-and-managing-policies>

NEW QUESTION: 69

What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)

- A. It uses techniques such as DGA, DNS tunneling detection and machine learning.
- B. It requires a valid Threat Prevention license.
- C. It enables users to access real-time protections using advanced predictive analytics.
- D. It requires a valid URL Filtering license.
- E. It requires an active subscription to a third-party DNS Security service.

Answer: A,B,C ([LEAVE A REPLY](#))

DNS Security subscription enables users to access real-time protections using advanced predictive analytics.

When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real-time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

NEW QUESTION: 70

An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone. The administrator does not want to allow traffic between the DMZ and LAN zones.

Which Security policy rule type should they use?

- A. default
- B. universal
- C. intrazone
- D. interzone

Answer: C ([LEAVE A REPLY](#))

Intrazone: A security policy allowing traffic between the same zone, this applies the rule to all matching traffic within the specified source zones (cannot specify a destination zone for intrazone rules).

For example, if setting the source zone to A and B, the rule would apply to all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>

NEW QUESTION: 71

When creating a custom URL category object, which is a valid type?

- A. host names
- B. domain match
- C. category match
- D. wildcard

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 72

What is the maximum volume of concurrent administrative account sessions?

- A. 10
- B. 1
- C. Unlimited
- D. 2

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 73

Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

- A. save named configuration snapshot
- B. export device state
- C. save candidate config
- D. export named configuration snapshot

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 74

Arrange the correct order that the URL classifications are processed within the system.

Answer:

Explanation

First - Block List

Second - Allow List

Third - Custom URL Categories

Fourth - External Dynamic Lists

Fifth - Downloaded PAN-DB Files

Sixth - PAN-DB Cloud

NEW QUESTION: 75

Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?

- A. NAT Target Tab
- B. NAT Active/Active HA Binding Tab
- C. NAT Translated Packet Tab
- D. NAT Policies General Tab

Answer: ([SHOW ANSWER](#))

The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them. This reduces the complexity and duplication of managing NAT policies across multiple firewalls¹.

Reference: NAT Target Tab, NAT Policy Overview, NPTv6 Overview, Updated Certifications for PAN-OS 10.1.

NEW QUESTION: 76

Which two components are utilized within the Single-Pass Parallel Processing architecture on a Palo Alto Networks Firewall? (Choose two.)

- A. Layer-ID
- B. User-ID
- C. QoS-ID
- D. App-ID

Answer: ([SHOW ANSWER](#))

Explanation/Reference: <http://www.firewall.cx/networking-topics/firewalls/palo-alto-firewalls/1152-palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html>

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 77

Four configuration choices are listed, and each could be used to block access to a specific URL. If you configured each choice to block the same URL then which choice would be the last to block access to the URL?

- A. Custom URL category in Security Policy rule.
- B. PAN-DB URL category in URL Filtering Profile.
- C. EDL in URL Filtering Profile.
- D. Custom URL category in URL Filtering Profile.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 78

Which two firewall components enable you to configure SYN flood protection thresholds?
(Choose two.)

- A. QoS profile
- B. DoS Protection profile
- C. Zone Protection profile
- D. DoS Protection policy

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 79

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

- A. branch office traffic
- B. east-west traffic
- C. north-south traffic
- D. perimeter traffic

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 80

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Answer:

Explanation:

Threat Intelligence Cloud - Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.

Next-Generation Firewall - Identifies and inspects all traffic to block known threats

Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

NEW QUESTION: 81

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can run malicious code against a targeted machine.

- A. Reconnaissance

- B. Installation
- C. Exploitation
- D. Act on Objective

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 82

Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?

- A. allowed-security services
- B. Deny Google
- C. intrazone-default
- D. interzone-default

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 83

Which statement is true about Panorama managed devices?

- A. Panorama automatically removes local configuration locks after a commit from Panorama.
- B. Local configuration locks prohibit Security policy changes for a Panorama managed device.
- C. Security policy rules configured on local firewalls always take precedence.
- D. Local configuration locks can be manually unlocked from Panorama.

Answer: ([SHOW ANSWER](#))

When a user has a configuration lock, it is not possible to perform a commit or push a policy from Panorama. If the administrator is not available to remove the lock, a device WebGUI or CLI command can be used by a superuser to force the removal of the configuration lock.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CltACAS>

NEW QUESTION: 84

Match the cyber-attack lifecycle stage to its correct description.

Answer:

NEW QUESTION: 85

Which profile should be used to obtain a verdict regarding analyzed files?

- A. WildFire analysis
- B. Vulnerability profile
- C. Content-ID
- D. Advanced threat prevention

Answer: A ([LEAVE A REPLY](#))

A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.

There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis¹.

The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination². WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware³. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats⁴.

The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational⁵.

Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.

Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.

Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.

References:

1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION: 86

Which two statements are true for the DNS Security service introduced in PAN-OS version 10.0? (Choose two.)

- A. It is automatically enabled and configured.
- B. It eliminates the need for dynamic DNS updates.
- C. It removes the 100K limit for DNS entries for the downloaded DNS updates.
- D. It functions like PAN-DB and requires activation through the app portal.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 87

Within the WildFire Analysis profile, which three items are configurable? (Choose three.)

- A. FileType
- B. Direction
- C. Service

D. Application

E. Objects

Answer: A,B,D (LEAVE A REPLY)

Use a WildFire Analysis profile to specify for WildFire file analysis to be performed locally on the WildFire appliance or in the WildFire cloud. You can specify traffic to be forwarded to the public cloud or private cloud based on file type, application, or the transmission direction of the file (upload or download). After creating a WildFire analysis profile, adding the profile to a policy (PoliciesSecurity) further allows you apply the profile settings to any traffic matched to that policy (for example, a URL category defined in the policy).

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/objects/objects-security-profiles-wildfire-analysis>

NEW QUESTION: 88

Where in Panorama Would Zone Protection profiles be configured?

A. Shared

B. Templates

C. Device Groups

D. Panorama tab

Answer: B (LEAVE A REPLY)

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewall>

NEW QUESTION: 89

Match the cyber-attack lifecycle stage to its correct description.

Answer:

NEW QUESTION: 90

How can a complete overview of the logs be displayed to an administrator who has permission in the system to view them?

A. Select the unified log entry in the side menu.

B. Modify the number of columns visible on the page

C. Modify the number of logs visible on each page.

D. Select the system logs entry in the side menu.

Answer: A (LEAVE A REPLY)

The best way to view a complete overview of the logs is to select the unified log entry in the side menu. The unified log is a single view that displays all the logs generated by the firewall, such as traffic, threat, URL filtering, data filtering, and WildFire logs¹. The unified log allows the administrator to filter, sort, and export the logs based on various criteria, such as time range, severity, source, destination, application, or action¹.

Modifying the number of columns visible on the page or the number of logs visible on each page does not provide a complete overview of the logs, but only changes the display settings of the

current log view. Selecting the system logs entry in the side menu does not show all the logs generated by the firewall, but only shows the logs related to system events, such as configuration changes, system alerts, or HA status2.

References:

1: View Logs - Palo Alto Networks 2: View and Manage Logs - Palo Alto Networks

NEW QUESTION: 91

If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

- A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL
- B. Configure a frequency schedule to clear group mapping cache
- C. Configure a Primary Employee ID number for user-based Security policies
- D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or

Answer: A ([LEAVE A REPLY](#))

If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups>

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPASS.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 92

An administrator would like to silently drop traffic from the internet to a ftp server.

Which Security policy action should the administrator select?

- A. Drop
- B. Reset-server
- C. Deny
- D. Block

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 93

Which two App-ID applications will need to be allowed to use facebook-chat? (Choose two.)

- A. facebook
- B. facebook-chat
- C. facebook-base
- D. facebook-email

Answer: ([SHOW ANSWER](#))

Explanation/Reference: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIV0CAK>

NEW QUESTION: 94

All users from the internal zone must be allowed only HTTP access to a server in the DMZ zone. Complete the empty field in the Security policy using an application object to permit only this type of access.

Source Zone: Internal

Destination Zone: DMZ Zone

Application: _____

Service: application-default

Action: allow

- A. Application = "any"
- B. Application = "web-browsing"
- C. Application = "ssl"
- D. Application = "http"

Answer: B ([LEAVE A REPLY](#))

http is not an application but service, the web-browsing can be http/https.

NEW QUESTION: 95

Based on the security policy rules shown, ssh will be allowed on which port?

- A. same port as ssl and snmpv3
- B. any port
- C. the default port
- D. only ephemeral ports

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 96

Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

- A. Policies> Security> Rule Usage> No App Specified
- B. Policies> Security> Rule Usage> Port only specified
- C. Policies> Security> Rule Usage> Port-based Rules
- D. Policies> Security> Rule Usage> Unused Apps

Answer: A ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html>

NEW QUESTION: 97

Based on the screenshot, what is the purpose of the group in User labelled "it"?

- A. Allow users in group "DMZ" to access IT applications.
- B. Allows "any" users to access servers in the DMZ zone.
- C. Allows users to access IT applications on all ports.
- D. Allow users in group "it" to access IT applications.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 98

An administrator wants to prevent hacking attacks through DNS queries to malicious domains. Which two DNS policy actions can the administrator choose in the Anti-Spyware Security Profile? (Choose two.)

- A. block
- B. override
- C. deny
- D. sinkhole

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 99

What is considered best practice with regards to committing configuration changes?

- A. Wait until all running and pending jobs are finished before committing.
- B. Export configuration after each single configuration change performed.
- C. Validate configuration changes prior to committing.
- D. Disable the automatic commit feature that prioritizes content database installations before committing.

Answer: C ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-cli-quick-start/use-the-cli/commit-configuration-changes> As a best practice, validate configuration changes prior to committing so that you can fix any errors that will cause a commit failure, thereby ensuring that the commit will succeed. This is particularly useful in environments with a strict change window.

NEW QUESTION: 100

Review the screenshot below. Based on the information it contains, which protocol decoder will detect a machine-learning match, create a Threat log entry, and permit the traffic?

- A. smb
- B. imap
- C. ftp
- D. http2

Answer: ([SHOW ANSWER](#))

According to the screenshot, only imap, pop3 and smtp have a default (alert) action, which generates an alert for each application traffic flow. The alert is saved in the threat log.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles>

NEW QUESTION: 101

Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

- A. Route with highest metric is actively used
- B. Path monitoring determines if route is useable
- C. Route with lowest metric is actively used
- D. Path monitoring does not determine if route is useable

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 102

Which type of address object is www.paloaltonetworks.com?

- A. IP range
- B. FQDN
- C. named address
- D. IP netmask

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 103

What do you configure if you want to set up a group of objects based on their ports alone?

- A. address groups
- B. custom objects
- C. application groups
- D. service groups

Answer: ([SHOW ANSWER](#))

Service = layer 4, Application = layer 7

NEW QUESTION: 104

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. After deploying content updates, perform a commit and push to Panorama.
- B. Content updates for firewall A/A HA pairs need a defined master device.
- C. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- D. Before deploying content updates, always check content release version compatibility.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 105

Given the screenshot what two types of route is the administrator configuring? (Choose two)

- A. OSPF
- B. static route
- C. default route
- D. BGP

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 106

What action will inform end users when their access to Internet content is being restricted?

- A. Enable 'Response Pages' on the interface providing Internet access.
- B. Create a custom 'URL Category' object with notifications enabled.
- C. Publish monitoring data for Security policy deny logs.
- D. Ensure that the 'site access' setting for all URL sites is set to 'alert'.

Answer: A ([LEAVE A REPLY](#))

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPASS.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 107

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

- A. Role-based
- B. Multi-Factor Authentication
- C. Dynamic
- D. SAML

Answer: ([SHOW ANSWER](#)**)**

Explanation/Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html>

NEW QUESTION: 108

Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

- A. Apps Allowed
- B. Name
- C. Apps Seen

D. Service

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 109

Where does a user assign a tag group to a policy rule in the policy creation window?

A. Application tab

B. General tab

C. Actions tab

D. Usage tab

Answer: B ([LEAVE A REPLY](#))

A user can assign a tag group to a policy rule in the policy creation window by selecting the General tab. A tag group is a collection of tags that can be used to identify and filter policy rules based on different criteria, such as function, location, or priority. A user can create a tag group on Panorama and assign it to a policy rule to apply the same set of tags to multiple firewalls or device groups¹. To assign a tag group to a policy rule, the user needs to:

Select the General tab in the policy creation window.

Click the Tag Group drop-down menu and select the tag group that the user wants to assign to the policy rule.

Click OK to save the changes. The policy rule will inherit the tags from the tag group and display them in the Tag column.

NEW QUESTION: 110

When creating an address object, which option is available to select from the Type drop-down menu?

A. IP Address Class

B. IPv4 Address

C. IP Netmask

D. IPv6 Address

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 111

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.

A. Reconnaissance

B. Installation

C. Act on Objective

D. Exploitation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 112

Given the screenshot what two types of route is the administrator configuring? (Choose two)

- A. BGP
- B. default route
- C. OSPF
- D. static route

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 113

Which two actions are needed for an administrator to get real-time WildFire signatures? (Choose two.)

- A. Obtain a Threat Prevention subscription.
- B. Enable Dynamic Updates.
- C. Move within the WildFire public cloud region.
- D. Obtain a WildFire subscription.

Answer: ([SHOW ANSWER](#)**)**

<https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-100/wildfire-real->

NEW QUESTION: 114

Which statement is true regarding NAT rules?

- A. Static NAT rules have precedence over other forms of NAT.
- B. Translation of the IP address and port occurs before security processing.
- C. NAT rules are processed in order from top to bottom.
- D. Firewall supports NAT on Layer 3 interfaces only.

Answer: C ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview>

NEW QUESTION: 115

Which type of profile must be applied to the Security policy rule to protect against buffer overflows, illegal code execution, and other attempts to exploit system flaws?

- A. URL filtering
- B. vulnerability protection
- C. file blocking
- D. anti-spyware

Answer: B ([LEAVE A REPLY](#))

Vulnerability Protection Security Profiles protect against threats entering the network. For example, Vulnerability Protection Security Profiles protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. The default Vulnerability Protection Security Profile protects clients and servers from all known critical-, high-, and medium-severity threats. You also can create exceptions that enable you to change the response to a specific signature.

NEW QUESTION: 116

Match the cyber-attack lifecycle stage to its correct description.

Answer:

NEW QUESTION: 117

Which Palo Alto network security operating platform component provides consolidated policy creation and centralized management?

- A. Prisma SaaS
- B. AutoFocus
- C. GlobalProtect
- D. Panorama

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 118

In which threat profile object would you configure the DNS Security service?

- A. Antivirus
- B. URL Filtering
- C. WildFire
- D. Anti-Spyware

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 119

Given the detailed log information above, what was the result of the firewall traffic inspection?

- A. It was blocked by the Anti-Virus Security profile action.
- B. It was blocked by the Anti-Spyware Profile action.
- C. It was blocked by the Security policy action.
- D. It was blocked by the Vulnerability Protection profile action.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 120

Which three statement describe the operation of Security Policy rules or Security Profiles?
(Choose three)

- A. Security Policy rules are attached to Security Profiles.
- B. Security Profile should be used only on allowed traffic.
- C. Security policy rules inspect but do not block traffic.
- D. Security Profile are attached to security policy rules.
- E. Security Policy rules can block or allow traffic.

Answer: B,D,E ([LEAVE A REPLY](#))

NEW QUESTION: 121

Which Security profile should be applied in order to protect against illegal code execution?

- A. Vulnerability Protection profile on allowed traffic
- B. Antivirus profile on allowed traffic
- C. Antivirus profile on denied traffic
- D. Vulnerability Protection profile on denied traffic

Answer: A (LEAVE A REPLY)

The Security profile that should be applied in order to protect against illegal code execution is the Vulnerability Protection profile on allowed traffic. The Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. The firewall can block or alert on traffic that matches a specific threat signature or a group of threats. The Vulnerability Protection profile can prevent illegal code execution by detecting and blocking attempts to exploit buffer overflows, format string vulnerabilities, or other code injection techniques¹. To apply the Vulnerability Protection profile on allowed traffic, you need to:

Create or modify a Vulnerability Protection profile on the firewall or Panorama and configure the rules and exceptions for the threats that you want to protect against².

Attach the Vulnerability Protection profile to a Security policy rule that allows traffic that you want to scan for vulnerabilities³.

Commit the changes to the firewall or Panorama and the managed firewalls.

References: Vulnerability Protection Profile, Create a Vulnerability Protection Profile, Attach a Vulnerability Protection Profile to a Security Policy Rule, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPASS.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122

Which action results in the firewall blocking network traffic without notifying the sender?

- A. Reset Client
- B. No notification
- C. Drop
- D. Deny

Answer: C (LEAVE A REPLY)

NEW QUESTION: 123

By default, which action is assigned to the interzone-default rule?

- A. Reset-server
- B. Deny
- C. Reset-client
- D. Allow

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 124

Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

- A. The traffic was denied by URL filtering.
- B. The web session was unsuccessfully decrypted.
- C. The traffic was denied by security profile.
- D. The web session was decrypted.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 125

A Panorama administrator would like to create an address object for the DNS server located in the New York City office, but does not want this object added to the other Panorama managed firewalls.

Which configuration action should the administrator take when creating the address object?

- A. Tag the address object with the New York Office tag.
- B. Ensure that Disable Override is cleared.
- C. Ensure that the Shared option is checked.
- D. Ensure that the Shared option is cleared.

Answer: ([SHOW ANSWER](#))

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/manage-unused-shared-objects>

NEW QUESTION: 126

Starting with PAN_OS version 9.1 which new type of object is supported for use within the user field of a security policy rule?

- A. remote username
- B. dynamic user group
- C. local username
- D. static user group

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 127

A network administrator creates an intrazone security policy rule on a NGFW. The source zones are set to IT.

Finance, and HR.

To which two types of traffic will the rule apply? (Choose two.)

- A. Within zone HR
- B. Within zone IT
- C. Between zone IT and zone HR
- D. Between zone IT and zone Finance

Answer: (SHOW ANSWER)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITHCA0>

NEW QUESTION: 128

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.

- A. Installation
- B. Reconnaissance
- C. Act on Objective
- D. Exploitation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 129

Drag and Drop Question

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Select and Place:

Answer:

NEW QUESTION: 130

Based on the network diagram provided, which two statements apply to traffic between the User and Server networks? (Choose two.)

- A. Traffic is permitted through the default intrazone "allow" rule.
- B. Traffic restrictions are possible by modifying intrazone rules.
- C. Traffic restrictions are not possible, because the networks are in the same zone.
- D. Traffic is permitted through the default interzone "allow" rule.

Answer: A,B (LEAVE A REPLY)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITHCA0&lang=es>

NEW QUESTION: 131

If using group mapping with Active Directory Universal Groups, what must you do when configuring the User-ID?

- A. Create an LDAP Server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL

- B. Configure a frequency schedule to clear group mapping cache
- C. Configure a Primary Employee ID number for user-based Security policies
- D. Create a RADIUS Server profile to connect to the domain controllers using LDAPS on port 636 or

Answer: ([SHOW ANSWER](#))

If you have Universal Groups, create an LDAP server profile to connect to the root domain of the Global Catalog server on port 3268 or 3269 for SSL, then create another LDAP server profile to connect to the root domain controllers on port 389. This helps ensure that users and group information is available for all domains and subdomains.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups>

NEW QUESTION: 132

Based on the security policy rules shown, ssh will be allowed on which port?

- A. 53
- B. 80
- C. 22
- D. 23

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 133

What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

- A. LDAP server profile
- B. authentication list profile
- C. authentication sequence
- D. authentication server list

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 134

When a security rule is configured as Intrazone, which field cannot be changed?

- A. Actions
- B. Source Zone
- C. Application
- D. Destination Zone

Answer: ([SHOW ANSWER](#))

When a security rule is configured as Intrazone, the destination zone field cannot be changed. This is because an intrazone rule applies to traffic that originates and terminates in the same zone. The destination zone is automatically set to the same value as the source zone and cannot be modified¹. An intrazone rule allows you to control and inspect traffic within a zone, such as applying security profiles or logging options². Reference: What are Universal, Intrazone and Interzone Rules?, Security Policy, Updated Certifications for PAN-OS 10.1, Palo Alto Networks

Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 135

Based on the security policy rules shown, ssh will be allowed on which port?

- A. only ephemeral ports
- B. the default port
- C. any port
- D. same port as ssl and snmpv3

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 136

Which solution is a viable option to capture user identification when Active Directory is not in use?

- A. Authentication Portal
- B. Cloud Identity Engine
- C. Directory Sync Service
- D. group mapping

Answer: A ([LEAVE A REPLY](#))

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 137

Which two statements are true for the DNS security service introduced in PAN-OS version 10.0?

- A. IT is automatically enabled and configured.
- B. IT eliminates the need for dynamic DNS updates.
- C. It functions like PAN-DB and requires activation through the app portal.
- D. It removes the 100K limit for DNS entries for the downloaded DNS updates.

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 138

Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

- A. engress outside
- B. inside-portal

C. internal-inside-dmz

D. intercone-default

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 139

Your company occupies one floor in a single building. You have two Active Directory domain controllers on a single network. The firewall's management plane is only slightly utilized.

Which User-ID agent is sufficient in your network?

A. Windows-based agent deployed on each domain controller

B. PAN-OS integrated agent deployed on the firewall

C. Citrix terminal server agent deployed on the network

D. Windows-based agent deployed on the internal network a domain member

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-user-mapping.html>

NEW QUESTION: 140

Which action should be taken to identify threats that have been detected by using inline cloud analysis?

A. Filter Threat logs by Type

B. Filter Threat logs by Action

C. Filter Threat logs by Application

D. Filter Threat logs by Threat Category

Answer: B ([LEAVE A REPLY](#))

To identify threats detected by inline cloud analysis, you should filter the Threat logs by Action.

This helps in pinpointing the specific actions taken by the firewall in response to detected threats, allowing for a more focused analysis of how threats were handled.

NEW QUESTION: 141

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

A. east-west traffic

B. branch office traffic

C. perimeter traffic

D. north-south traffic

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 142

Which policy set should be used to ensure that a policy is applied just before the default security rules?

- A. Shared post-rulebase
- B. Local firewall policy
- C. Parent device-group post-rulebase
- D. Child device-group post-rulebase

Answer: A ([LEAVE A REPLY](#))

Order:

Shared pre-rules

Device group pre-rules

Local firewall rules

Device group post-rules

Shared post-rules

Intrazone-default

Interzone-default

NEW QUESTION: 143

Which Security profile should be applied in order to protect against illegal code execution?

- A. Vulnerability Protection profile on allowed traffic
- B. Antivirus profile on allowed traffic
- C. Antivirus profile on denied traffic
- D. Vulnerability Protection profile on denied traffic

Answer: A ([LEAVE A REPLY](#))

The Security profile that should be applied in order to protect against illegal code execution is the Vulnerability Protection profile on allowed traffic. The Vulnerability Protection profile defines the actions that the firewall takes to protect against exploits and vulnerabilities in applications and protocols. The firewall can block or alert on traffic that matches a specific threat signature or a group of threats. The Vulnerability Protection profile can prevent illegal code execution by detecting and blocking attempts to exploit buffer overflows, format string vulnerabilities, or other code injection techniques¹. To apply the Vulnerability Protection profile on allowed traffic, you need to:

Create or modify a Vulnerability Protection profile on the firewall or Panorama and configure the rules and exceptions for the threats that you want to protect against².

Attach the Vulnerability Protection profile to a Security policy rule that allows traffic that you want to scan for vulnerabilities³.

Commit the changes to the firewall or Panorama and the managed firewalls.

NEW QUESTION: 144

Which Security profile generates an alert based on a threshold when the action is set to Alert?

- A. Vulnerability Protection
- B. Antivirus

C. DoS protection

D. Anti-Spyware

Answer: C ([LEAVE A REPLY](#))

DoS Protection profiles set thresholds that protect against new session IP flood attacks and provide resource protection (maximum concurrent session limits for specified endpoints and resources). DoS Protection profiles protect specific devices (classified profiles) and groups of devices (aggregate profiles) against SYN, UDP, ICMP, ICMPv6, and Other IP flood attacks. Configuring Flood Protection thresholds in a DoS Protection profile is similar to configuring Flood Protection in a Zone Protection profile, but Zone Protection profiles protect entire ingress zones, while DoS protection profiles and policy rules are granular and targeted, and can even be classified to a single device (IP address). The firewall measures the aggregate number of connections-per-second (CPS) to a group of devices (aggregate profile) or measures the CPS to individual devices (classified profile).

NEW QUESTION: 145

Given the topology, which zone type should interface E1/1 be configured with?

A. Tunnel

B. Virtual Wire

C. Layer3

D. Tap

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 146

Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

A. Route with lowest metric is actively used

B. Route with highest metric is actively used

C. Path monitoring does not determine if route is useable

D. Path monitoring determines if route is useable

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 147

The administrator profile "SYS01 Admin" is configured with authentication profile "Authentication Sequence SYS01," and the authentication sequence SYS01 has a profile list with four authentication profiles:

* Auth Profile LDAP

* Auth Profile Radius

* Auth Profile Local

* Auth Profile TACACS

After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the "SYS01 Admin" username and password.

What is the "SYS01 Admin" login capability after the outage?

- A. Auth KO because RADIUS server lost user and password for SYS01 Admin
- B. Auth KO because LDAP server is not reachable
- C. Auth OK because of the Auth Profile Local
- D. Auth OK because of the Auth Profile TACACS -

Answer: ([SHOW ANSWER](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-an-authentication-profile-a>

NEW QUESTION: 148

Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

- A. Name
- B. Apps Allowed
- C. Apps Seen
- D. Service

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 149

Which statement best describes the use of Policy Optimizer?

- A. Policy Optimizer can display which Security policies have not been used in the last 90 days
- B. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove
- C. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
- D. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 150

Which two firewall components enable you to configure SYN flood protection thresholds?

(Choose two.)

- A. QoS profile
- B. DoS Protection profile
- C. Zone Protection profile
- D. DoS Protection policy

Answer: B,C ([LEAVE A REPLY](#))

Explanation

Explanation/Reference:

Reference:

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

NEW QUESTION: 151

Which statement is true about Panorama managed devices?

- A. Panorama automatically removes local configuration locks after a commit from Panorama.
- B. Local configuration locks prohibit Security policy changes for a Panorama managed device.
- C. Security policy rules configured on local firewalls always take precedence.
- D. Local configuration locks can be manually unlocked from Panorama.

Answer: A ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/manage-locks-for-restricting-configuration-changes.html>

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam! BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:
<https://www.braindumpsPASS.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 152

Which statement is true regarding a Best Practice Assessment?

- A. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
- B. The BPA tool can be run only on firewalls
- C. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
- D. It provides a percentage of adoption for each assessment data

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 153

What is a function of application tags?

- A. IP address allocations in DHCP
- B. application prioritization
- C. automated referenced applications in a policy
- D. creation of new zones

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 154

The Administrator profile "PCNSA Admin" is configured with an Authentication profile "Authentication Sequence PCNSA".

The Authentication Sequence PCNSA has a profile list with four Authentication profiles:

Auth Profile LDAP

Auth Profile Radius

Auth Profile Local

Auth Profile TACACS

After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the "PCNSA Admin" username and password.

Which option describes the "PCNSA Admin" login capabilities after the outage?

- A. Auth KO because LDAP server is not reachable
- B. Auth OK because of the Auth Profile TACACS
- C. Auth KO because RADIUS server lost user and password for PCNSA Admin
- D. Auth OK because of the Auth Profile Local

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 155

Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

- A. The host lab-client has been found by the User-ID agent.
- B. The User-ID agent is connected to the firewall labeled lab-client.
- C. The host lab-client has been found by a domain controller.
- D. The User-ID agent is connected to a domain controller labeled lab-client.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 156

Match each rule type with its example

Answer:

NEW QUESTION: 157

Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

- A. It defines the CA certificate used to verify the client's browser.
- B. It defines the firewall's global SSL/TLS timeout values.
- C. It defines the SSUTLS encryption strength used to protect the management interface.
- D. It defines the certificate to send to the client's browser from the management interface.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 158

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

- A. anti-spyware profile applied to outbound security policies

- B. antivirus profile applied to outbound security policies
- C. URL filtering profile applied to outbound security policies
- D. vulnerability protection profile applied to outbound security policies

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 159

Which object would an administrator create to block access to all high-risk applications?

- A. HIP profile
- B. Vulnerability Protection profile
- C. application group
- D. application filter

Answer: D ([LEAVE A REPLY](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKECA0>

NEW QUESTION: 160

Your company occupies one floor in a single building you have two active directory domain controllers on a single networks the firewall s management plane is only slightly utilized.

Which user-ID agent sufficient in your network?

- A. PAN-OS integrated agent deployed on the firewall
- B. Windows-based agent deployed on the internal network a domain member
- C. Citrix terminal server agent deployed on the network
- D. Windows-based agent deployed on each domain controller

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 161

What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

- A. every 30 minutes
- B. every 5 minutes
- C. once every 24 hours
- D. every 1 minute

Answer: ([SHOW ANSWER](#))

Explanation

Firewalls with an active WildFire WildFire signatures every five minutes. If you do not have a WildFire subscription, are made available within 24-48 hours as part of the antivirus update for firewalls with an active Threat Prevention license.

<https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-concepts/wildfire-sign>

NEW QUESTION: 162

Which security profile should be used to classify malicious web content?

- A. URL Filtering
- B. Antivirus
- C. Web Content
- D. Vulnerability Protection

Answer: A ([LEAVE A REPLY](#))

URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups. References: URL Filtering, Set Up a Basic Security Policy, Updated Certifications for PAN-OS 10.1

NEW QUESTION: 163

Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website.

How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?

- A. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile
- B. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES
- C. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate Data Filtering profile
- D. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 164

When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?

- A. Address Type
- B. Interface
- C. Translation Type
- D. IP Address

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 165

When configuring a security policy, what is a best practice for User-ID?

- A. Use only one method for mapping IP addresses to usernames.
- B. Allow the User-ID agent in zones where agents are not monitoring services.
- C. Limit User-ID to users registered in an Active Directory server.
- D. Deny WMI traffic from the User-ID agent to any external zone.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 166

Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Answer:

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam! BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:
<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 167

Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

- A. Root
- B. Dynamic
- C. Role-based
- D. Superuser

Answer: B ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types#id8b324bf1-eac8-40e1-82d5-6f82ff761fa9>

NEW QUESTION: 168

Which statement is true regarding a Best Practice Assessment?

- A. It runs only on firewalls.
- B. It shows how current configuration compares to Palo Alto Networks recommendations.
- C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.

Answer: B ([LEAVE A REPLY](#))

Best Practice Assessment (BPA) Tool -The BPA for next-generation firewalls and Panorama evaluates a device's configuration by measuring the adoption of capabilities, validating whether the policies adhere to best practices, and providing recommendations and instructions for how to remediate failed best practice checks.

The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories. The results include trending data, which shows the rate of security improvement as you adopt new capabilities, fix gaps, and progress toward a Zero-Trust network.

The BPA component performs more than 200 security checks on a firewall or Panorama configuration and provides a pass/fail score for each check. Each check is a best practice identified by Palo Alto Networks security experts. If a check returns a failing score, the tool provides the justification for the failing score and how to fix the issue.

<https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools>

NEW QUESTION: 169

Match the cyber-attack lifecycle stage to its correct description.

Answer:

NEW QUESTION: 170

In order to protect users against exploit kits that exploit a vulnerability and then automatically download malicious payloads, which Security profile should be configured?

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

Answer: C ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/security-profiles>

NEW QUESTION: 171

Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

- A. engress outside
- B. internal-inside-dmz
- C. intercone-default
- D. inside-portal

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 172

The External zone type is used to pass traffic between which type of objects?

- A. virtual routers

- B. virtual systems
- C. Layer 3 interfaces
- D. Layer 2 interfaces

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 173

Which three configuration settings are required on a Palo Alto networks firewall management interface?

- A. default gateway
- B. netmask
- C. IP address
- D. hostname
- E. auto-negotiation

Answer: A,B,C ([LEAVE A REPLY](#))

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

NEW QUESTION: 174

Which statement is true regarding a Prevention Posture Assessment?

- A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
- B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
- C. It provides a percentage of adoption for each assessment area
- D. It performs over 200 security checks on Panorama/firewall for the assessment

Answer: B ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools>

NEW QUESTION: 175

Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

- A. User identification
- B. Filtration protection
- C. Vulnerability protection
- D. Antivirus
- E. Application identification
- F. Anti-spyware

Answer: A,C,D,E,F ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 176

Given the topology, which zone type should zone A and zone B to be configured with?

- A. Virtual Wire
- B. Layer3
- C. Tap
- D. Layer2

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 177

Match each rule type with its example

Answer:

NEW QUESTION: 178

For the firewall to use Active Directory to authenticate users, which Server Profile is required in the Authentication Profile?

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

Answer: ([SHOW ANSWER](#)**)**

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence>

NEW QUESTION: 179

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. Content updates for firewall A/A HA pairs need a defined master device.
- B. After deploying content updates, perform a commit and push to Panorama.
- C. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- D. Before deploying content updates, always check content release version compatibility.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 180

Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

- A. data
- B. control
- C. security processing
- D. network processing

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 181

Based on the graphic, which statement accurately describes the output shown in the Server Monitoring panel?

- A. The User-ID agent is connected to the firewall labeled lab-client.
- B. The host lab-client has been found by a domain controller.
- C. The User-ID agent is connected to a domain controller labeled lab-client.
- D. The host lab-client has been found by the User-ID agent.

Answer: B ([LEAVE A REPLY](#))

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam! BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:
<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 182

Which administrative management services can be configured to access a management interface?

- A. HTTP, CLI, SNMP, HTTPS
- B. HTTPS, SSH telnet SNMP
- C. SSH: telnet HTTP, HTTPS
- D. HTTPS, HTTP. CLI, API

Answer: D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces> You can use the following user interfaces to manage the Palo Alto Networks firewall: Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.

Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency. Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.

Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls. The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION: 183

To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

- A. TACACS+
- B. domain controller
- C. LDAP
- D. RADIUS

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 184

Given the topology, which zone type should zone A and zone B to be configured with?

- A. Layer3
- B. Tap
- C. Layer2
- D. Virtual Wire

Answer: A ([LEAVE A REPLY](#))

Using IP address is layer 3. Mac address is layer 2.

NEW QUESTION: 185

What are three ways application characteristics are used? (Choose three.)

- A. As an attribute to define an application group
- B. As a setting to define a new custom application
- C. As an attribute to define an application filter
- D. As an Object to define Security policies
- E. As a global filter in the Application Command Center (ACC)

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 186

Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

- A. global
- B. intrazone
- C. interzone
- D. universal

Answer: ([SHOW ANSWER](#)**)**

Explanation

References: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>

NEW QUESTION: 187

Which feature must be configured to enable a data plane interface to submit DNS queries originated from the firewall on behalf of the control plane?

- A. Service route
- B. Admin role profile
- C. DNS proxy
- D. Virtual router

Answer: A ([LEAVE A REPLY](#))

By default, the firewall uses the management (MGT) interface to access external services, such as DNS servers, external authentication servers, Palo Alto Networks services such as software, URL updates, licenses, and AutoFocus. An alternative to using the MGT interface is configuring a data port (a standard interface) to access these services. The path from the interface to the service on a server is a service route. [Palo Alto Networks] PAN-OS 10 -> Device -> Setup -> Services -> Service Features -> Service Route Configuration

NEW QUESTION: 188

What does an administrator use to validate whether a session is matching an expected NAT policy?

- A. config audit
- B. test command
- C. system log
- D. threat log

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 189

Which two configuration settings shown are not the default? (Choose two.)

- A. Server Log Monitor Frequency (sec)
- B. Enable Probing
- C. Enable Security Log
- D. Enable Session

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 190

An administrator needs to create a Security policy rule that matches DNS traffic within the LAN zone, and also needs to match DNS traffic within the DMZ zone.

The administrator does not want to allow traffic between the DMZ and LAN zones.

Which Security policy rule type should they use?

- A. default

- B. universal
- C. intrazone
- D. interzone

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 191

Arrange the correct order that the URL classifications are processed within the system.

Answer:

Explanation

First - Block List

Second - Allow List

Third - Custom URL Categories

Fourth - External Dynamic Lists

Fifth - Downloaded PAN-DB Files

Sixth - PAN-DB Cloud

NEW QUESTION: 192

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Answer:

NEW QUESTION: 193

Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

- A. Citrix terminal server deployed on the internal network
- B. PAN-OS integrated agent deployed on the internal network
- C. Windows-based agent deployed on each of the WAN Links
- D. Windows-based agent deployed on the internal network

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 194

An administrator is investigating a log entry for a session that is allowed and has the end reason of aged-out. Which two fields could help in determining if this is normal? (Choose two.)

- A. Packets sent/received
- B. IP Protocol
- C. Action
- D. Decrypted

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 195

Match the Cyber-Attack Lifecycle stage to its correct description.

Answer:

Explanation

Reconnaissance - stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation - stage where the attacker will explore methods such as a root kit to establish

persistence Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.

Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION: 196

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

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

Answer: A (LEAVE A REPLY)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 197

Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

- A. The traffic was denied by security profile.
- B. The traffic was denied by URL filtering.
- C. The web session was decrypted.
- D. The web session was unsuccessfully decrypted.

Answer: (SHOW ANSWER)

NEW QUESTION: 198

Match the Cyber-Attack Lifecycle stage to its correct description.

Answer:

Explanation

Reconnaissance - stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation - stage where the attacker will explore methods such as a root kit to establish persistence

Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.

Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION: 199

Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

- A. domain controller monitoring
- B. Windows session monitoring
- C. Windows client probing
- D. Active Directory monitoring

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 200

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Answer:

NEW QUESTION: 201

Complete the statement. A security profile can block or allow traffic.

- A. before it is evaluated by a security policy
- B. on unknown-tcp or unknown-udp traffic
- C. after it is evaluated by a security policy that allows traffic
- D. after it is evaluated by a security policy that allows or blocks traffic

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 202

You receive notification about new malware that is being used to attack hosts. The malware exploits a software bug in common application.

Which Security Profile detects and blocks access to this threat after you update the firewall's threat signature database?

- A. Data Filtering Profile applied to outbound Security policy rules
- B. Antivirus Profile applied to outbound Security policy rules
- C. Data Filtering Profile applied to inbound Security policy rules
- D. Vulnerability Protection Profile applied to inbound Security policy rules

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 203

Which Palo Alto Networks service protects cloud-based applications such as Dropbox and Salesforce by monitoring permissions and shares and scanning files for sensitive information?

- A. Prisma SaaS
- B. AutoFocus
- C. Panorama
- D. GlobalProtect

Answer: A ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 204

In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

- A. Installation
- B. Weaponization
- C. Exploitation
- D. Command and Control
- E. Reconnaissance

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 205

What are three valid information sources that can be used when tagging users to dynamic user groups? (Choose three.)

- A. DNS Security service
- B. Firewall logs
- C. Custom API scripts
- D. Biometric scanning results from iOS devices
- E. Security Information and Event Management Systems (SIEMS), such as Splunk

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 206

What two authentication methods on the Palo Alto Networks firewalls support authentication and authorization for role-based access control? (Choose two.)

- A. SAML
- B. TACACS+
- C. LDAP
- D. Kerberos

Answer: A,B ([LEAVE A REPLY](#))

Reference:

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server.

The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML

server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

NEW QUESTION: 207

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 (1.1.1.100), ssh - Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- C. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
- D. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow
- E. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 208

Which Security policy set should be used to ensure that a policy is applied first?

- A. Child device-group pre-rulebase
- B. Shared pre-rulebase
- C. Parent device-group pre-rulebase
- D. Local firewall policy

Answer: B ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/defining-polic>

NEW QUESTION: 209

What is used to monitor Security policy applications and usage?

- A. Security profile
- B. App-ID
- C. Policy-based forwarding
- D. Policy Optimizer

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 210

Why should a company have a File Blocking profile that is attached to a Security policy?

- A. To block uploading and downloading of specific types of files
- B. To detonate files in a sandbox environment
- C. To block uploading and downloading of any type of files
- D. To analyze file types

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 211

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Answer:

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam! BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:
<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 212

Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.

- A. Exploitation
- B. Act on the Objective
- C. Reconnaissance
- D. Installation

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 213

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.

- A. Exploitation
- B. Act on Objective
- C. Reconnaissance
- D. Installation

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 214

In the example security policy shown, which two websites fcked? (Choose two.)

- A. Amazon
- B. Facebook
- C. YouTube
- D. LinkedIn

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 215

Given the topology, which zone type should you configure for firewall interface E1/1?

- A. Tap
- B. Tunnel
- C. Virtual Wire
- D. Layer3

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

NEW QUESTION: 216

When an ethernet interface is configured with an IPv4 address, which type of zone is it a member of?

- A. Layer 3
- B. Tunnel
- C. Virtual Wire
- D. Tap

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 217

What Policy Optimizer policy view differ from the Security policy do?

- A. It shows rules that are missing Security profile configurations.
- B. It indicates rules with App-ID that are not configured as port-based.
- C. It shows rules with the same Source Zones and Destination Zones.
- D. It indicates that a broader rule matching the criteria is configured above a more specific rule.

Answer: B ([LEAVE A REPLY](#))

Policy Optimizer policy view differs from the Security policy view in several ways. One of them is that it indicates rules with App-ID that are not configured as port-based. These are rules that have the application set to "any" instead of a specific application or group of applications. These rules are overly permissive and can introduce security gaps, as they allow any application traffic on the specified ports. Policy Optimizer helps you convert these rules to application-based rules that follow the principle of least privilege access¹². You can use Policy Optimizer to discover and convert port-based rules to application-based rules, and also to remove unused applications, eliminate unused rules, and discover new applications that match your policy criteria³. Reference:

Policy Optimizer Best Practices - Palo Alto Networks

Manage: Policy Optimizer - Palo Alto Networks | TechDocs

Why use Security Policy Optimizer and what are the benefits?

NEW QUESTION: 218

Order the steps needed to create a new security zone with a Palo Alto Networks firewall.

Answer:

Explanation

Step 1 - Select network tab

Step 2 - Select zones from the list of available items

Step 3 - Select Add

Step 4 - Specify Zone Name

Step 5 - Specify Zone Type

Step 6 - Assign interfaces as needed

NEW QUESTION: 219

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 (1.1.1.100), web-browsing - Allow
- B. Untrust (Any) to DMZ (10.1.1.100. 10.1.1.101), ssh, 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: A,E ([LEAVE A REPLY](#))

NEW QUESTION: 220

Match each rule type with its example

Answer:

NEW QUESTION: 221

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

- A. delivery
- B. reinsurance
- C. installation
- D. exploitation
- E. command and control

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 222

At which point in the App-ID update process can you determine if an existing policy rule is affected by an App-ID update?

- A. after clicking Check Now in the Dynamic Update window
- B. after committing the firewall configuration
- C. after installing the update
- D. after downloading the update

Answer: D ([LEAVE A REPLY](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamic-updates>

NEW QUESTION: 223

Which prevention technique will prevent attacks based on packet count?

- A. zone protection profile
- B. vulnerability profile
- C. URL filtering profile
- D. antivirus profile

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 224

What is the best-practice approach to logging traffic that traverses the firewall?

- A. Enable both log at session start and log at session end.
- B. Enable log at session start only.
- C. Enable log at session end only.
- D. Disable all logging options.

Answer: C ([LEAVE A REPLY](#))

The best-practice approach to logging traffic that traverses the firewall is to enable log at session end only.

This option allows the firewall to generate a log entry only when a session ends, which reduces the load on the firewall and the log storage. The log entry contains information such as the source and destination IP addresses, ports, zones, application, user, bytes, packets, and duration of the session. The log at session end option also provides more accurate information about the session, such as the final application and user, the total bytes and packets, and the session end reason¹. To enable log at session end only, you need to:

Create or modify a Security policy rule that matches the traffic that you want to log.

Select the Actions tab in the policy rule and check the Log at Session End option.

Commit the changes to the firewall or Panorama and the managed firewalls.

References: View and Manage Logs, Log at Session End, Certifications - Palo Alto Networks, [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)] or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

NEW QUESTION: 225

When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?

- A. IP Address
- B. Translation Type
- C. Interface
- D. Address Type

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 226

Within a WildFire Analysis Profile, what match criteria can be defined to forward samples for analysis?

- A. Application Category
- B. Source
- C. File Size
- D. Direction

Answer: (SHOW ANSWER)

A WildFire Analysis Profile allows you to specify which files or email links to forward for WildFire analysis based on the application, file type, and transmission direction (upload or download) of the traffic. The direction match criteria determines whether the file or email link was sent from the source zone to the destination zone (upload) or from the destination zone to the source zone (download). You can also select both directions to forward files or email links regardless of the direction of the traffic. References: Security Profile:

Wildfire Analysis, Objects > Security Profiles > WildFire Analysis

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpsPass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 227

Based on the screenshot what is the purpose of the included groups?

- A. They are only groups visible based on the firewall's credentials.
- B. They are used to map usernames to group names.
- C. They contain only the users you allow to manage the firewall.
- D. They are groups that are imported from RADIUS authentication servers.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html>

NEW QUESTION: 228

Match the network device with the correct User-ID technology.

Answer:

NEW QUESTION: 229

How often does WildFire release dynamic updates?

- A. every 30 minutes
- B. every 60 minutes
- C. every 5 minutes
- D. every 15 minutes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 230

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server. Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

- A. antivirus profile applied to outbound security policies
- B. data filtering profile applied to inbound security policies
- C. data filtering profile applied to outbound security policies
- D. vulnerability profile applied to inbound security policies

Answer: A ([LEAVE A REPLY](#))

Antivirus: Includes new and updated antivirus signatures, including WildFire signatures and automatically generated command-and-control (C2) signatures. WildFire signatures detect malware seen first by firewalls from around the world. You must have a Threat Prevention subscription to get these updates.

New antivirus signatures are published daily.

NEW QUESTION: 231

Place the following steps in the packet processing order of operations from first to last.

Answer:

NEW QUESTION: 232

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 (1.1.1.100), ssh - Allow
- B. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
- C. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
- D. Untrust (Any)to DMZ (10.1.1.100. 10.1.1.101), ssh, web-browsing-Allow
- E. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 233

Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Answer:

NEW QUESTION: 234

A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp_base. On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp_chat and SuperApp_download, which will be deployed in 30 days.

Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

- A. All traffic matching the SuperApp_chat, and SuperApp_download is denied because it no longer matches the SuperApp-base application
- B. No impact because the apps were automatically downloaded and installed
- C. No impact because the firewall automatically adds the rules to the App-ID interface
- D. All traffic matching the SuperApp_base, SuperApp_chat, and SuperApp_download is denied until the security administrator approves the applications

Answer: A ([LEAVE A REPLY](#))

Explanation

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-r>

NEW QUESTION: 235

Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Answer:

NEW QUESTION: 236

An administrator is updating Security policy to align with best practices.

Which Policy Optimizer feature is shown in the screenshot below?

- A. Unused Unused Apps
- B. Rule Usage
- C. New App Viewer
- D. Rules without App Controls

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 237

An internal host wants to connect to servers of the internet through using source NAT.

Which policy is required to enable source NAT on the firewall?

- A. NAT policy with no source of destination zone selected
- B. NAT policy with source zone and destination zone specified
- C. post-NAT policy with external source and any destination address
- D. pre-NAT policy with external source and any destination address

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 238

In the example security policy shown, which two websites would be blocked? (Choose two.)

- A. LinkedIn
- B. YouTube
- C. Amazon
- D. Facebook

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 239

Complete the statement. A security profile can block or allow traffic.

- A. on unknown-tcp or unknown-udp traffic
- B. after it is evaluated by a security policy that allows traffic
- C. before it is evaluated by a security policy
- D. after it is evaluated by a security policy that allows or blocks traffic

Answer: B ([LEAVE A REPLY](#))

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.

NEW QUESTION: 240

Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

- A. It defines the firewall's global SSL/TLS timeout values.
- B. It defines the CA certificate used to verify the client's browser.
- C. It defines the SSUTLS encryption strength used to protect the management interface.
- D. It defines the certificate to send to the client's browser from the management interface.

Answer: ([SHOW ANSWER](#))

Valid PCNSA Dumps shared by BraindumpsPass.com for Helping Passing PCNSA Exam!

BraindumpsPass.com now offer the **newest PCNSA exam dumps**, the BraindumpsPass.com PCNSA exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com PCNSA dumps with Test Engine here:

<https://www.braindumpspass.com/Palo-Alto-Networks/PCNSA-practice-exam-dumps.html> (360

Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)