



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

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

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

Answer: D

NEW QUESTION 2

Which option is part of the content inspection process?

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

Answer: C

NEW QUESTION 3

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
- E. CLI, API

Answer: D

Explanation:

<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 4

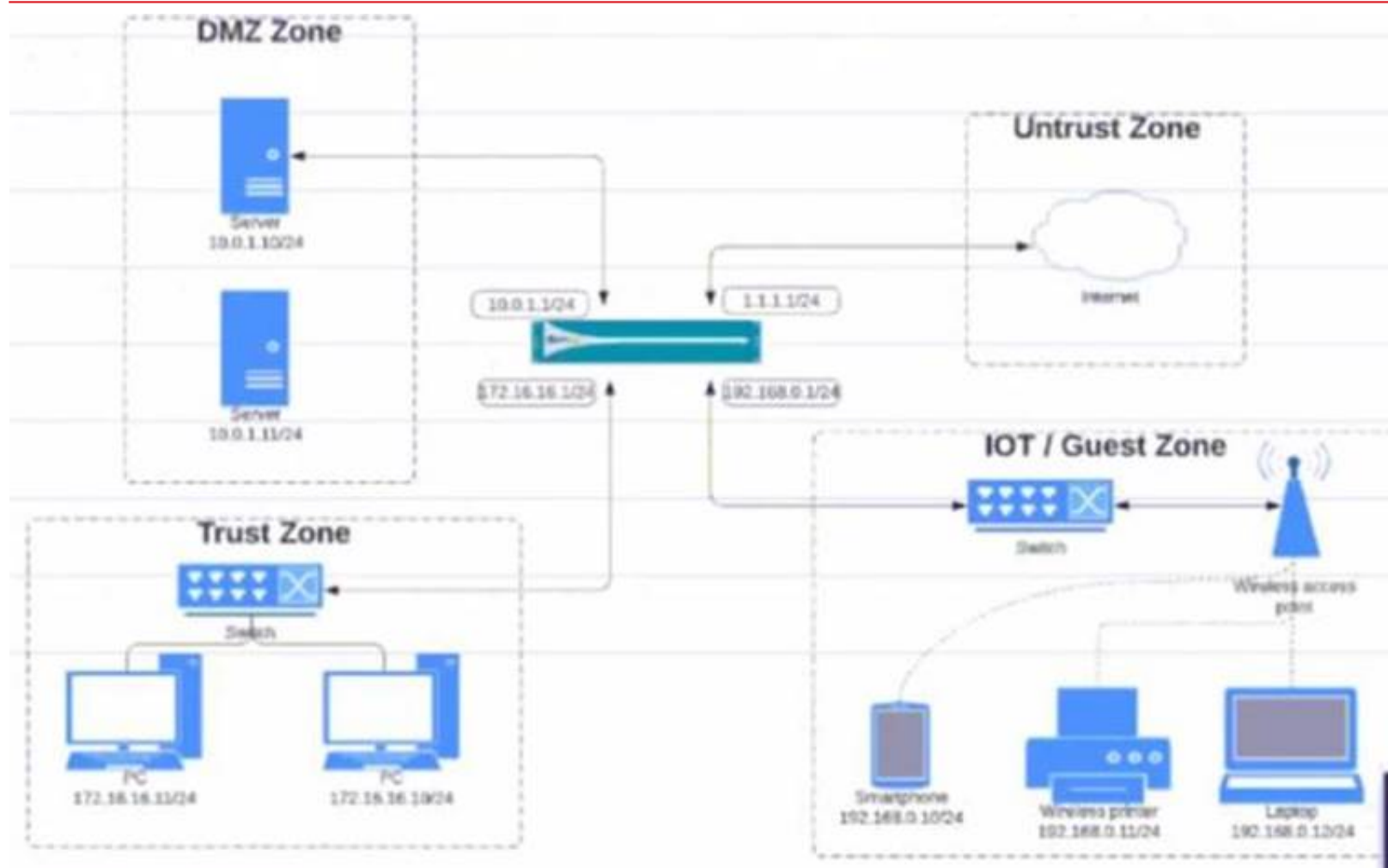
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

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

Answer: ACDEF

NEW QUESTION 5

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)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B)

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24
			Trust	192.168.0.0/24			Untrust	10.0.1.0/24

C)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

D)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24
			Trust	172.16.16.0/24			Untrust	192.168.0.0/24

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

Answer: C

NEW QUESTION 6

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

NEW QUESTION 7

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

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

Answer: AB

NEW QUESTION 8

In which profile should you configure the DNS Security feature?

- A. URL Filtering Profile
- B. Anti-Spyware Profile
- C. Zone Protection Profile
- D. Antivirus Profile

Answer: B

NEW QUESTION 9

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

NEW QUESTION 10

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

Answer: BD

NEW QUESTION 10

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: D

Explanation:

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

NEW QUESTION 11

An administrator configured a Security policy rule with an Antivirus Security profile. The administrator did not change the action (or the profile. If a virus gets detected, how wilt the firewall handle the traffic?

- A. It allows the traffic because the profile was not set to explicitly deny the traffic.
- B. It drops the traffic because the profile was not set to explicitly allow the traffic.
- C. It uses the default action assigned to the virus signature.
- D. It allows the traffic but generates an entry in the Threat logs.

Answer: B

NEW QUESTION 15

The Palo Alto Networks NGFW was configured with a single virtual router named VR-1 What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

- A. Add zones attached to interfaces to the virtual router
- B. Add interfaces to the virtual router
- C. Enable the redistribution profile to redistribute connected routes

D. Add a static routes to route between the two interfaces

Answer: D

NEW QUESTION 17

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: ABC

Explanation:

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.

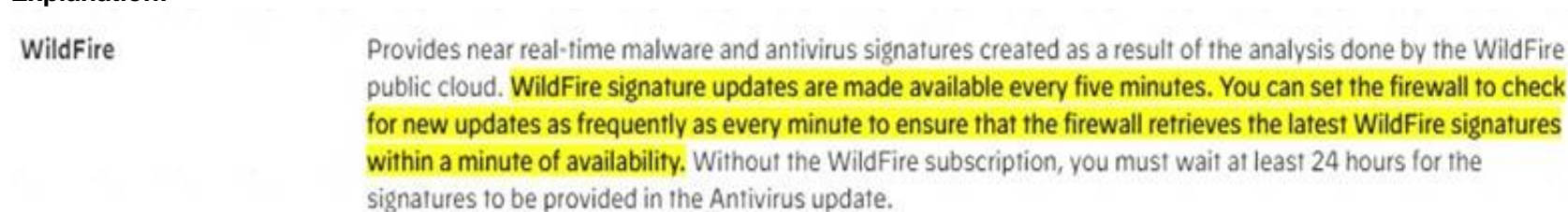
NEW QUESTION 21

What is the minimum frequency for which you can configure the firewall to check for new wildfire antivirus signatures?

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

Answer: B

Explanation:



NEW QUESTION 24

An administrator wants to create a NAT policy to allow multiple source IP addresses to be translated to the same public IP address. What is the most appropriate NAT policy to achieve this?

- A. Dynamic IP and Port
- B. Dynamic IP
- C. Static IP
- D. Destination

Answer: A

NEW QUESTION 29

Which two security profile types can be attached to a security policy? (Choose two.)

- A. antivirus
- B. DDoS protection
- C. threat
- D. vulnerability

Answer: AD

NEW QUESTION 32

Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?

- A. destination address
- B. source address
- C. destination zone
- D. source zone

Answer: B

NEW QUESTION 34


A Security Profile can block or allow traffic at which point?

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

Answer: A

NEW QUESTION 36

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



The screenshot shows the 'Server Monitoring' section of a network management interface. It includes tabs for 'User Mapping', 'Connection Security', 'User-ID Agents', 'Terminal Services Agents', 'Group Mapping Settings', and 'Captive Portal Settings'. The main area displays configuration for the 'lab.local' domain, including 'Kerberos Server Profile', 'Enable Security Log', 'Server Log Monitor Frequency (sec)', 'Enable Session', 'Server Session Read Frequency (sec)', 'Novell eDirectory Query Interval (sec)', 'Syslog Service Profile', 'Enable Probing', 'Prove Interval (min)', 'Enable User Identification Timeout', 'User Identification Timeout (min)', 'Allow matching usernames without domains', 'Enable NTLM', 'NTLM Domain', and 'User-ID Collector Name'. Below this is a 'Server Monitoring' table with columns: Name, Enabled, Type, Network Address, and Status.

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected

- 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

NEW QUESTION 39

Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

- A. Threat Prevention License
- B. Threat Implementation License
- C. Threat Environment License
- D. Threat Protection License

Answer: A

NEW QUESTION 44

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



The screenshot shows the 'Detailed Log View' section of a network management interface. It displays a log entry for a dropped DNS packet. The log is organized into three main sections: General, Source, and Destination. The General section includes Session ID, Action, Host ID, Application, Rule, Rule UUID, Device SN, IP Protocol, Log Action, Generated Time, Receive Time, and Tunnel Type. The Source section includes Source User, Source, Source DAG, Country, Port, Zone, Interface, NAT IP, NAT Port, and X-Forwarded-For IP. The Destination section includes Destination User, Destination, Destination DAG, Country, Port, Zone, Interface, NAT IP, and NAT Port. There is also a 'Flags' section at the bottom right.

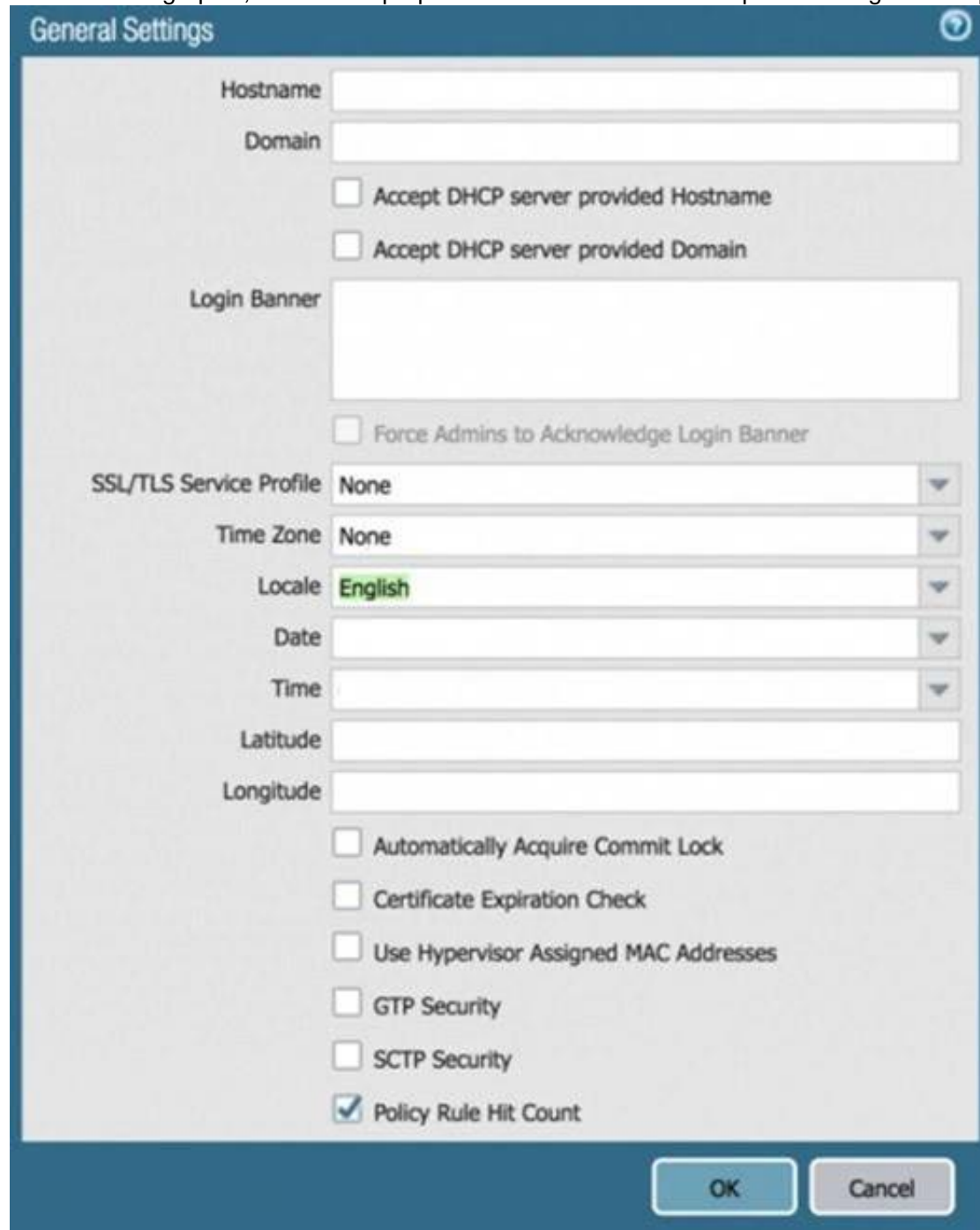
General	Source	Destination
Session ID: 781868	Source User:	Destination User:
Action: drop	Source: 192.168.101.25	Destination: 8.8.4.4
Host ID:	Source DAG:	Destination DAG:
Application: dns	Country: 192.168.0.0-192.168.255.255	Country: United States
Rule: Outbound DNS	Port: 46282	Port: 53
Rule UUID: ea9f3b96-e280-467c-aca5-0b1902857791	Zone: Servers	Zone: Internet
Device SN: 007251000156341	Interface: ethernet1/4	Interface: ethernet1/8
IP Protocol: udp	NAT IP: 67.190.64.58	NAT IP: 8.8.4.4
Log Action: global-logs	NAT Port: 26351	NAT Port: 53
Generated Time: 2021/08/27 02:02:49	X-Forwarded-For IP: 0.0.0.0	
Receive Time: 2021/08/27 02:02:53		
Tunnel Type: N/A		

- 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 Vulnerability Protection profile action.
- D. It was blocked by the Security policy action.

Answer: B

NEW QUESTION 45

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



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

Answer: C

NEW QUESTION 46

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: AD

Explanation:

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

NEW QUESTION 47

Which file is used to save the running configuration with a Palo Alto Networks firewall?

- A. running-config.xml
- B. run-config.xml
- C. running-configuration.xml
- D. run-configuratin.xml

Answer: A

NEW QUESTION 49

What are three differences between security policies and security profiles? (Choose three.)

- A. Security policies are attached to security profiles
- B. Security profiles are attached to security policies
- C. Security profiles should only be used on allowed traffic
- D. Security profiles are used to block traffic by themselves
- E. Security policies can block or allow traffic

Answer: BCE

NEW QUESTION 50

How often does WildFire release dynamic updates?

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

Answer: A

NEW QUESTION 54

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

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

Answer: B

NEW QUESTION 56

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

Answer: CD

NEW QUESTION 58

Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

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

Answer: B

NEW QUESTION 60

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.

Why doesn't the administrator see the traffic?

- A. Logging on the interzone-default policy is disabled.
- B. Traffic is being denied on the interzone-default policy.
- C. The Log Forwarding profile is not configured on the policy.
- D. The interzone-default policy is disabled by default.

Answer: A

NEW QUESTION 64

Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's data plane?

- A. Kerberos user
- B. SAML user
- C. local database user
- D. local user

Answer: B

NEW QUESTION 66

How do you reset the hit count on a security policy rule?

- A. First disable and then re-enable the rule.
- B. Reboot the data-plane.
- C. Select a Security policy rule, and then select Hit Count > Reset.
- D. Type the CLI command reset hitcount <POLICY-NAME>.

Answer: C

NEW QUESTION 67

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

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

Answer: D

NEW QUESTION 70

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

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

Answer: B

NEW QUESTION 75

An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?

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

Answer: C

NEW QUESTION 77

During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

- A. check now
- B. review policies
- C. test policy match
- D. download

Answer: B

NEW QUESTION 79

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

NEW QUESTION 82

Which firewall feature do you need to configure to query Palo Alto Networks service updates over a data-plane interface instead of the management interface?

- A. Data redistribution
- B. Dynamic updates
- C. SNMP setup
- D. Service route

Answer: D

NEW QUESTION 83

Which the app-ID application will you need to allow in your security policy to use facebook-chat?

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

Answer: BD

NEW QUESTION 87

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

Answer: B

NEW QUESTION 90

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

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

Answer: ABD

NEW QUESTION 95

Which tab would an administrator click to create an address object?

- A. Device
- B. Policies
- C. Monitor
- D. Objects

Answer: D

NEW QUESTION 99

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 on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
- C. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected
- D. 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

Answer: B

NEW QUESTION 102

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. export named configuration snapshot
- D. save candidate config

Answer: A

Explanation:

Export Named Configuration Snapshot This option exports the current running configuration, a candidate configuration snapshot, or a previously imported configuration (candidate or running). The firewall exports the configuration as an XML file with the specified name. You can save the snapshot in any network location. These exports often are used as backups. These XML files also can be used as templates for building other firewall configurations.

NEW QUESTION 106

Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic. Which statement accurately describes how the firewall will apply an action to matching traffic?

- A. If it is an allowed rule, then the Security Profile action is applied last
- B. If it is a block rule then the Security policy rule action is applied last
- C. If it is an allow rule then the Security policy rule is applied last
- D. If it is a block rule then Security Profile action is applied last

Answer: A

NEW QUESTION 111

An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

- A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory
- B. Create an Application Group and add business-systems to it
- C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
- D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office

Answer: A

Explanation:

An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html>

NEW QUESTION 115

Which prevention technique will prevent attacks based on packet count?

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

Answer: A

NEW QUESTION 116

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

Explanation:

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

NEW QUESTION 120

An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

Answer: AC

NEW QUESTION 122

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Disable automatic updates during weekdays
- B. Automatically “download and install” but with the “disable new applications” option used
- C. Automatically “download only” and then install Applications and Threats later, after the administrator approves the update
- D. Configure the option for “Threshold”

Answer: D

NEW QUESTION 127

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

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

Answer: C

NEW QUESTION 130

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

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

NEW QUESTION 135

After making multiple changes to the candidate configuration of a firewall, the administrator would like to start over with a candidate configuration that matches the running configuration.

Which command in Device > Setup > Operations would provide the most operationally efficient way to accomplish this?

- A. Import named config snapshot
- B. Load named configuration snapshot
- C. Revert to running configuration
- D. Revert to last saved configuration

Answer: C

NEW QUESTION 139

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 downloading the update
- D. after installing the update

Answer: A

NEW QUESTION 140

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

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

Answer: BDE

NEW QUESTION 141

You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server. Which Security Profile when applied to outbound Security policy rules detects and prevents this threat from establishing a command-and-control connection?

- A. Antivirus Profile
- B. Data Filtering Profile
- C. Vulnerability Protection Profile
- D. Anti-Spyware Profile

Answer: D

Explanation:

Anti-Spyware Security Profiles block spyware on compromised hosts from trying to communicate with external command-and-control (C2) servers, thus enabling you to detect malicious traffic leaving the network from infected clients.

NEW QUESTION 146

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

Explanation:

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

NEW QUESTION 151

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

NEW QUESTION 154

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: D

Explanation:

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

NEW QUESTION 158

Which DNS Query action is recommended for traffic that is allowed by Security policy and matches Palo Alto Networks Content DNS Signatures?

- A. block
- B. sinkhole
- C. alert
- D. allow

Answer: B

Explanation:

To enable DNS sinkholing for domain queries using DNS security, you must activate your DNS Security subscription, create (or modify) an Anti-Spyware policy to reference the DNS Security service, configure the log severity and policy settings for each DNS signature category, and then attach the profile to a security policy rule.
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security>

NEW QUESTION 161

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

- A. on the App Dependency tab in the Commit Status window
- B. on the Policy Optimizer's Rule Usage page
- C. on the Application tab in the Security Policy Rule creation window
- D. on the Objects > Applications browser pages

Answer: AC

NEW QUESTION 166

Which URL profiling action does not generate a log entry when a user attempts to access that URL?

- A. Override
- B. Allow
- C. Block
- D. Continue

Answer: B

NEW QUESTION 169

What is the main function of Policy Optimizer?

- A. reduce load on the management plane by highlighting combinable security rules
- B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
- C. eliminate "Log at Session Start" security rules
- D. convert port-based security rules to application-based security rules

Answer: D

NEW QUESTION 170

Which object would an administrator create to enable access to all applications in the office-programs subcategory?

- A. application filter
- B. URL category
- C. HIP profile
- D. application group

Answer: A

NEW QUESTION 175

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

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

Answer: A

NEW QUESTION 179

What is the purpose of the automated commit recovery feature?

- A. It reverts the Panorama configuration.
- B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.
- C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.
- D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

Answer: C

NEW QUESTION 181

What can be achieved by selecting a policy target prior to pushing policy rules from Panorama?

- A. Doing so limits the templates that receive the policy rules
- B. Doing so provides audit information prior to making changes for selected policy rules
- C. You can specify the firewalls in a device group to which to push policy rules
- D. You specify the location as pre or post-rules to push policy rules

Answer: C

NEW QUESTION 184

In a security policy what is the quickest way to reset all policy rule hit counters to zero?

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

Answer: C

NEW QUESTION 186

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 with a URL Filtering profile that references the site access setting of continue to NO-FILES
- 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 that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile

Answer: B

NEW QUESTION 188

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

Palo Alto Networks User-ID Agent Setup

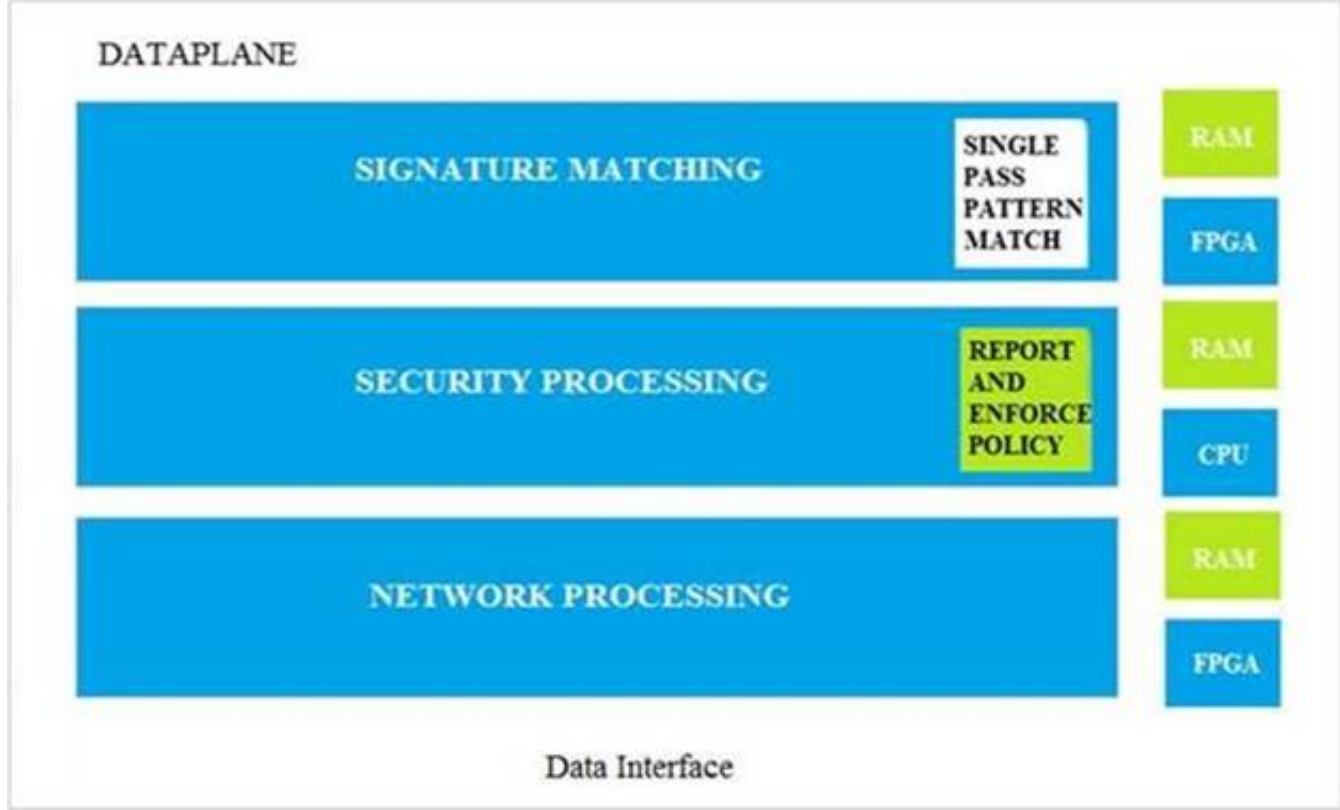
Enable Security Log ✓
Server Log Monitor Frequency (sec) **15**
Enable Session ✓
Server Session Read Frequency (sec) **10**
Novell eDirectory Query Interval (sec) **30**
Syslog Service Profile
Enable Probing
Probe Interval (min) **20**
Enable User Identification Timeout ✓
User Identification Timeout (min) **45**
Allow matching usernames without domains
Enable NTLM
NTLM Domain
User-ID Collector Name

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

Answer: BC

NEW QUESTION 189

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



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

Answer: A

NEW QUESTION 190

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

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

Answer: BCE

NEW QUESTION 193

Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed.
Security Policy: Source Zone: Internal to DMZ Zone services “Application defaults”, and action = Allow

- A. Destination IP: 192.168.1.123/24
- B. Application = ‘Telnet’
- C. Log Forwarding
- D. USER-ID = ‘Allow users in Trusted’

Answer: B

NEW QUESTION 195

A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

- A. Rule Usage Filter > No App Specified
- B. Rule Usage Filter >Hit Count > Unused in 30 days
- C. Rule Usage Filter > Unused Apps
- D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer: D

NEW QUESTION 200

Place the steps in the correct packet-processing order of operations.

Operational Task	Answer Area
Security profile enforcement	<div></div> first
decryption	<div></div> second
zone protection	<div></div> third
App-ID	<div></div> fourth

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, application, table Description automatically generated with medium confidence

NEW QUESTION 202

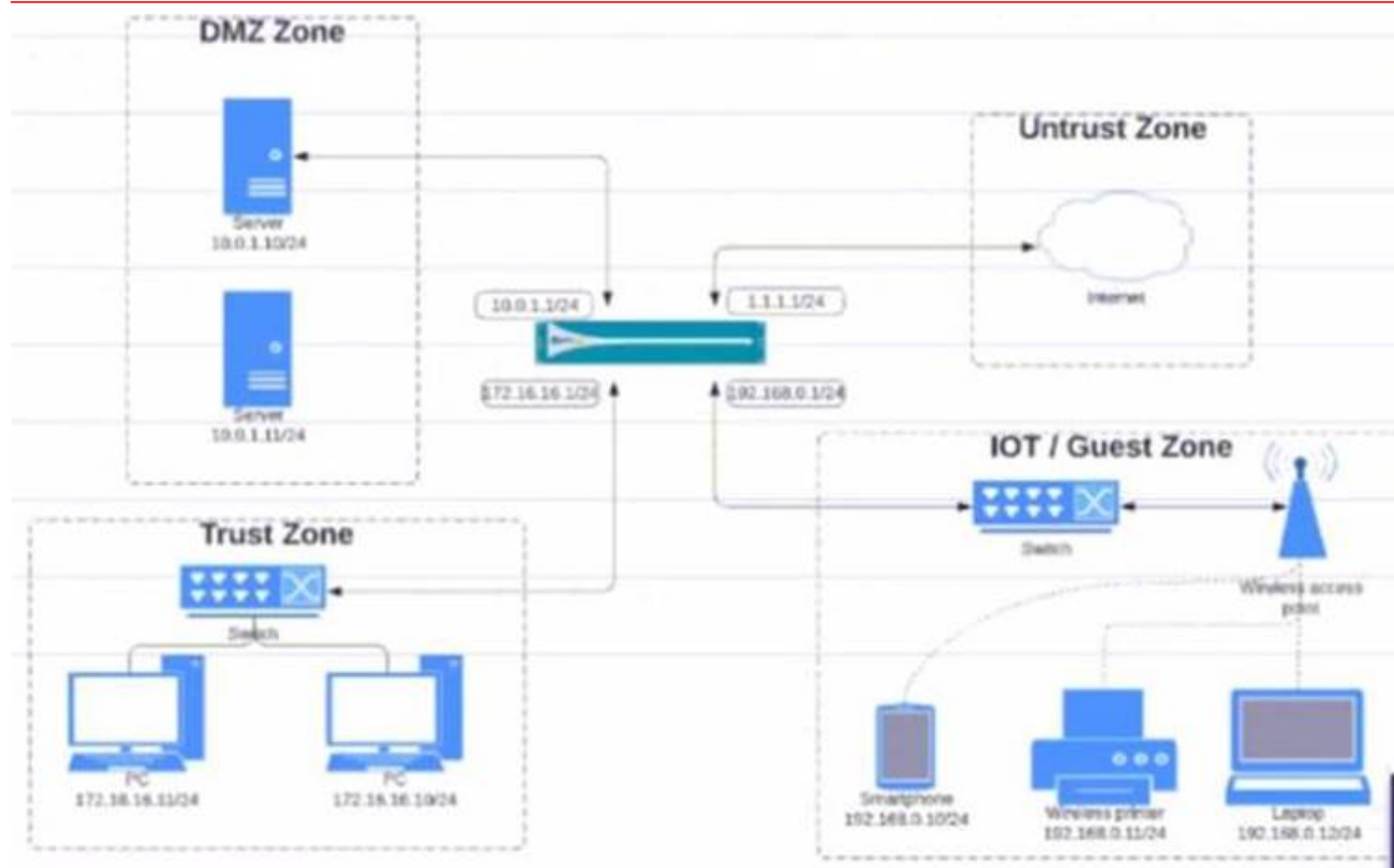
An administrator is trying to enforce policy on some (but not all) of the entries in an external dynamic list. What is the maximum number of entries that they can be exclude?

- A. 50
- B. 100
- C. 200
- D. 1,000

Answer: B

NEW QUESTION 206

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)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B)

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24
			Trust	192.168.0.0/24			Untrust	10.0.1.0/24

C)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

D)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24
			Trust	172.16.16.0/24			Untrust	192.168.0.0/24

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

Answer: C

NEW QUESTION 209

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. anti-spyware

- B. URL filtering
- C. vulnerability protection
- D. file blocking

Answer: C

NEW QUESTION 211

Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?

- A. override
- B. allow
- C. block
- D. continue

Answer: B

NEW QUESTION 212

Which security policy rule would be needed to match traffic that passes between the Outside zone and Inside zone, but does not match traffic that passes within the zones?

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

Answer: B

NEW QUESTION 215

You need to allow users to access the office–suite application of their choice. How should you configure the firewall to allow access to any office-suite application?

- A. Create an Application Group and add Office 365, Evernote Google Docs and Libre Office
- B. Create an Application Group and add business-systems to it.
- C. Create an Application Filter and name it Office Programs, then filter it on the office programs subcategory.
- D. Create an Application Filter and name it Office Programs then filter on the business-systems category.

Answer: C

NEW QUESTION 219

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

Explanation:

To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletpro>

NEW QUESTION 220

.....

Relate Links

100% Pass Your PCNSA Exam with ExamBible Prep Materials

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

Contact us

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

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