Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

https://www.2passeasy.com/dumps/PCNSA/

NEW QUESTION 1
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 Object to define Security policies
D. As an attribute to define an application filter
E. As a global filter in the Application Command Center (ACC)

Answer: ABD

Explanation:

NEW QUESTION 2
Which operations are allowed when working with App-ID application tags?

A. Predefined tags may be deleted.
B. Predefined tags may be augmented by custom tags.
C. Predefined tags may be modified.
D. Predefined tags may be updated by WildFire dynamic updates.

Answer: B

NEW QUESTION 3
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

A. URL traffic
B. vulnerability protection
C. anti-spyware
D. antivirus

Answer: C

Explanation:

NEW QUESTION 4
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 5
Which attribute can a dynamic address group use as a filtering condition to determine its membership?

A. tag
B. wildcard mask
C. IP address
D. subnet mask

Answer: A

Explanation:
Dynamic Address Groups: A dynamic address group populates its members dynamically using looks ups for tags and tag-based filters. Dynamic address groups are very useful if you have an extensive virtual infrastructure where changes in virtual machine location/IP address are frequent. For example, you have a sophisticated failover setup or provision new virtual machines frequently and would like to apply policy to traffic from or to the new machine without modifying the configuration/rules on the firewall. https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects- address-groups

NEW QUESTION 6
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

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list.html

NEW QUESTION 7
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List
B. Custom URL Categories
C. PAN-DB URL Categories
D. Allow List

Answer: AD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

NEW QUESTION 8
DRAG DROP
Arrange the correct order that the URL classifications are processed within the system.

Answer:

Answer Area

First	Block List	PAN-DB Cloud
Second	Allow Lists	External Dynamic Lists
Third	Custom URL Categories	Custom URL Categories
Fourth	External Dynamic Lists	Block List
Fifth	Downloaded PAN-DB File	Downloaded PAN-DB File
Sixth	PAN-DB Cloud	Allow Lists

A. Mastered
B. Not Mastered

Answer: A

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 9
Based on the show security policy rule would match all FTP traffic from the inside zone to the outside zone?

	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	Action
1	inside-portal	universal	inside	any	outside	203.0.113.20	any	any	Allow
2	internal-inside-dmz	universal	inside	any	dmz	any	ftp / ssh / ssl / web-browsing	application-default	Allow
3	egress-outside	universal	inside	any	outside	any	any	application-default	Allow
4	egress-outside-content-id	universal	inside	any	outside	any	any	application-default	Allow
5	danger-simulated-traffic	universal	danger	any	danger	any	any	application-default	Allow
6	intrazone-default	intrazone	any	any	(intrazone)	any	any	any	Allow
7	intrazone-default	intrazone	any	any	any	any	any	any	Deny

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

Answer: B

NEW QUESTION 10
When creating a Panorama administrator type of Device Group and Template Admin, which two things must you create first? (Choose two.)

A. password profile
B.

                                    access domain
C. admin rote
D. server profile

Answer: CD

NEW QUESTION 10
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer: C

Explanation:
 https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html

NEW QUESTION 11
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

A. HIP profile
B. Application group
C. URL category
D. Application filter

Answer: C

NEW QUESTION 14
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

Explanation:
 References:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new- app-ids-introduced- incontent-releases/review-new-app-id-impact-on- existing-policy-rules

NEW QUESTION 17
What do you configure if you want to set up a group of objects based on their ports alone?

A. Application groups

B. Service groups
C. Address groups
D. Custom objects

Answer: B

NEW QUESTION 20
Which built-in IP address EDL would be useful for preventing traffic from IP addresses that are verified as unsafe based on WildFire analysis Unit 42 research and data gathered from telemetry?

A.

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

Answer: D

Explanation:
? Palo Alto Networks Known Malicious IP Addresses
—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry (Share ThreatIntelligence with Palo Alto Networks). Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/built-in-edls

NEW QUESTION 21
An administrator configured a Security policy rule where the matching condition includes a single application and the action is set to deny. What deny action will the firewall perform?

A. Drop the traffic silently
B. Perform the default deny action as defined in the App-ID database for the application
C. Send a TCP reset packet to the client- and server-side devices
D.

                                          Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated

Answer: D

NEW QUESTION 26
Which action results in the firewall blocking network traffic with out notifying the sender?

A. Drop
B. Deny
C. Reset Server
D. Reset Client

Answer: B

NEW QUESTION 27
Which two settings allow you to restrict access to the management interface? (Choose two)

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 32
What are two valid selections within an Antivirus profile? (Choose two.)

A. deny
B. drop
C. default
D. block-ip

Answer: BC

NEW QUESTION 37
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

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamicupdates

NEW QUESTION 38
DRAG DROP
Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Threat Intelligence Cloud	Next-Generation Firewall	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Threat Intelligence Cloud	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Advanced Endpoint Protection	Inspects processes and files to prevent known and unknown exploits.

NEW QUESTION 41
In a security policy what is the quickest way to rest 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 43
Which type security policy rule would match traffic flowing between the inside zone and outside zone within the inside zone and within the outside zone?

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

Answer: B

NEW QUESTION 45
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: D

Explanation:
 Explanation Explanation/Reference: Reference:
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer- panorama/manage- locks-forrestricting-configuration-changes.html

NEW QUESTION 47

Which two statements are correct about App-ID content updates? (Choose two.)

A. Updated application content may change how security policy rules are enforced
B. After an application content update, new applications must be manually classified prior to use
C. Existing security policy rules are not affected by application content updates
D. After an application content update, new applications are automatically identified and classified

Answer: AD

NEW QUESTION 51
An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

A. Security policy rule
B. ACC global filter
C. external dynamic list
D. NAT address pool

Answer: A

Explanation:
 You can use an address object of type IP Wildcard Mask only in a Security policy rule.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects- addresses
IP Wildcard Mask—Enter an IP wildcard address in the format of an IPv4 address followed by a slash and a mask (which must begin with a zero); for example, 10.182.1.1/0.127.248.0. In the wildcard mask, a zero (0) bit indicates that the bit being compared must match the bit in the IP address that is covered by the 0. A one (1) bit in the mask is a wildcard bit, meaning the bit being compared need not match the bit in the IP address that is covered by the 1. Convert the IP address and the wildcard mask to binary. To illustrate the matching: on binary snippet 0011, a wildcard mask of 1010 results in four matches (0001, 0011, 1001, and 1011).

NEW QUESTION 56
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 60
What is the main function of the Test Policy Match function?

A. verify that policy rules from Expedition are valid
B. confirm that rules meet or exceed the Best Practice Assessment recommendations
C. confirm that policy rules in the configuration are allowing/denying the correct traffic
D. ensure that policy rules are not shadowing other policy rules

Answer: D

NEW QUESTION 62
What are three valid ways to map an IP address to a username? (Choose three.)

A. using the XML API
B. DHCP Relay logs

C. a user connecting into a GlobalProtect gateway using a GlobalProtect Agent
D. usernames inserted inside HTTP Headers
E. WildFire verdict reports

Answer: ACD

NEW QUESTION 63
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

Explanation:
? 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 threats34.
? 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 67
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny
If the application s default deny action is reset-both what action does the firewall take*?

A. It sends a TCP reset to the client-side and server-side devices
B. It silently drops the traffic and sends an ICMP unreachable code
C. It silently drops the traffic
D. It sends a TCP reset to the server-side device

Answer: A

NEW QUESTION 72
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 exfiltrating corporate data.
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

A. Create a Data Filtering Profile and enable its DNS sinkhole feature.
B. Create an Antivirus Profile and enable its DNS sinkhole feature.
C. Create an Anti-Spyware Profile and enable its DNS sinkhole feature.
D. Create a URL Filtering Profile and block the DNS sinkhole URL category.

Answer: C

NEW QUESTION 73
What are the requirements for using Palo Alto Networks EDL Hosting Sen/ice?

A. any supported Palo Alto Networks firewall or Prisma Access firewall
B. an additional subscription free of charge
C. a firewall device running with a minimum version of PAN-OS 10.1
D. an additional paid subscription

Answer: A

NEW QUESTION 76
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.
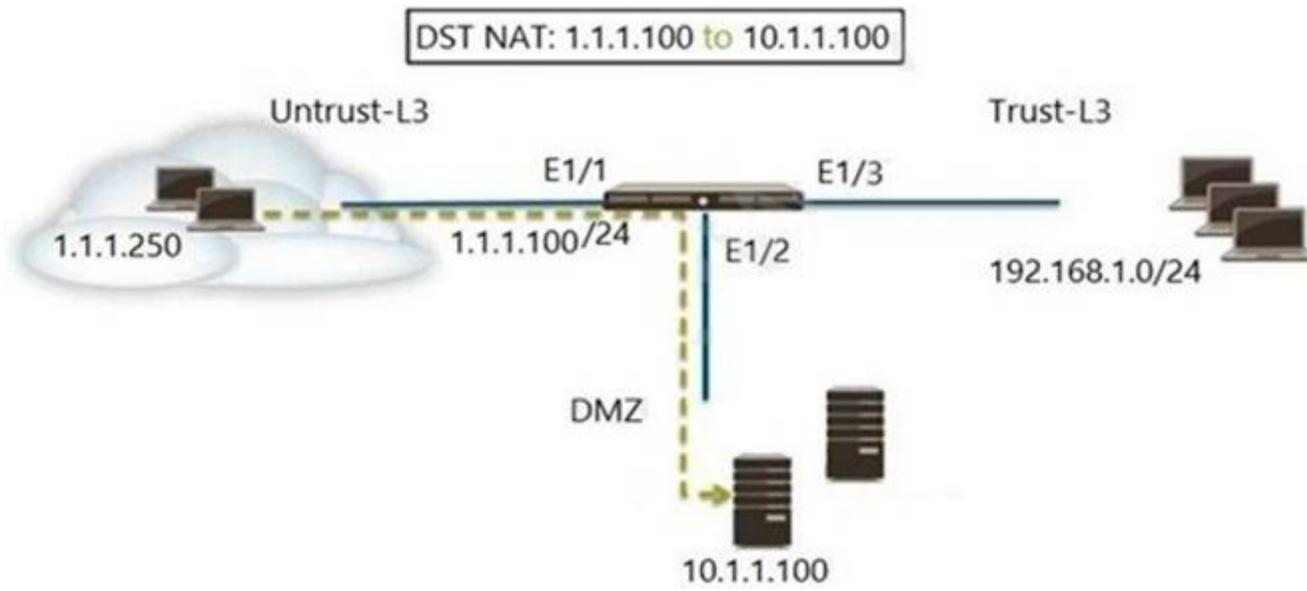
Which Security policy rule will allow traffic to flow to the web server?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

NEW QUESTION 81
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 of destination zone selected
D. pre-NAT policy with external source and any destination address

Answer: A

NEW QUESTION 86
DRAG DROP
Place the steps in the correct packet-processing order of operations.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 91
Based on the security policy rules shown, ssh will be allowed on which port?

	Name	Type	Source Zone	Source Address	Destination Zone	Destination Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

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

Answer: C

Explanation:

NEW QUESTION 92
Given the detailed log information above, what was the result of the firewall traffic inspection?
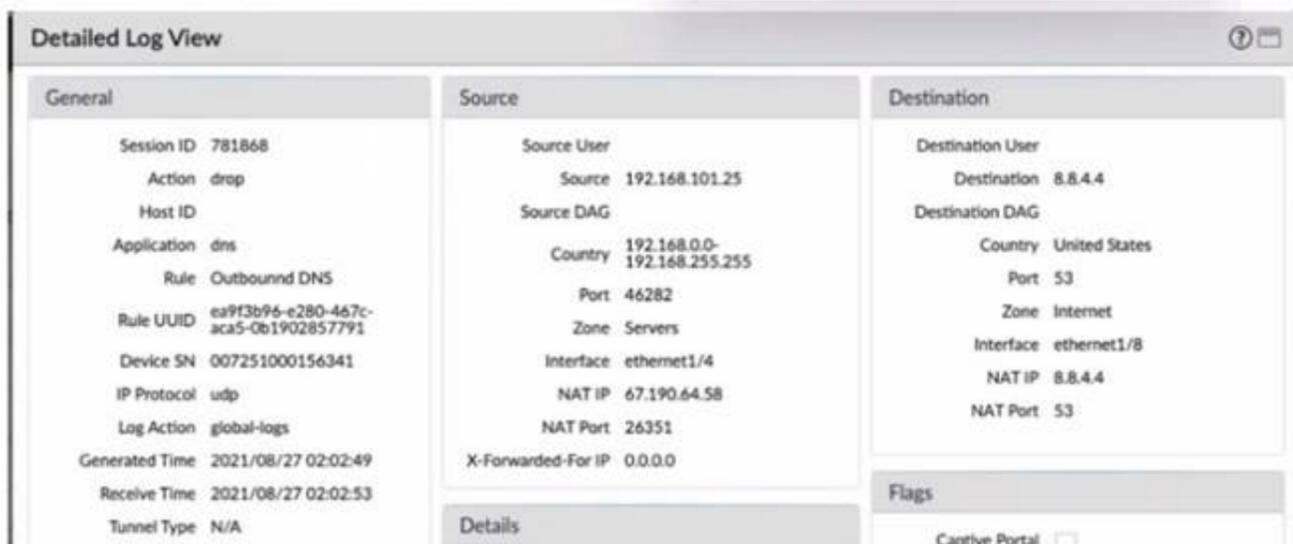
A. It was blocked by the Anti-Virus Security profile action.
B. It was blocked by the Anti-Spyware Profile action.
C. It was blocked by the Vulnerability Protection profile action.
D. It was blocked by the Security policy action.

Answer: B

NEW QUESTION 94
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 98
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

Explanation:

Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering- concepts/url- filteringprofile-actions.html

NEW QUESTION 101
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

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id- features/policy- optimizer.html

NEW QUESTION 102
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

Explanation:

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 106
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

NEW QUESTION 109
An administrator needs to allow users to use only certain email applications.
How should the administrator configure the firewall to restrict users to specific email applications?

A. Create an application filter and filter it on the collaboration category, email subcategory.
B. Create an application group and add the email applications to it.
C. Create an application filter and filter it on the collaboration category.
D. Create an application group and add the email category to it.

Answer: B

NEW QUESTION 112
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: ABC

Explanation:

Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

NEW QUESTION 113
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 117
What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 120
Which two DNS policy actions in the anti-spyware security profile can prevent hacking attacks through DNS queries to malicious domains? (Choose two.)

A. Deny
B. Sinkhole
C. Override
D. Block

Answer: BD

Explanation:
? A DNS policy action is a setting in an Anti-Spyware security profile that defines
how the firewall handles DNS queries to malicious domains. A malicious domain is a domain name that is associated with a known threat, such as malware, phishing, or botnet1.
? There are four possible DNS policy actions: alert, allow, block, and sinkhole1.
? The alert action logs the DNS query and allows it to proceed to the intended destination. This action does not prevent hacking attacks, but only notifies the administrator of the potential threat1.
? The allow action allows the DNS query to proceed to the intended destination without logging it. This action does not prevent hacking attacks, but only bypasses the DNS security inspection2.
? The block action blocks the DNS query and sends a response to the client with an NXDOMAIN (non-existent domain) error code. This action prevents hacking attacks by preventing the client from resolving the malicious domain1.
? The sinkhole action redirects the DNS query to a predefined IP address (the sinkhole IP address) that is under the control of the administrator. This action prevents hacking attacks by isolating the client from the malicious domain and allowing the administrator to monitor and remediate the infected host1.
? The override action is not a valid DNS policy action, but a setting in an Anti- Spyware security profile that allows the administrator to create exceptions for specific spyware signatures that they want to override the default action or log settings3.
Therefore, the two DNS policy actions that can prevent hacking attacks through DNS queries to malicious domains are block and sinkhole.
                                References:
1: Enable DNS Security - Palo Alto Networks 2: How To Disable the DNS Security Feature from an Anti-Spyware Profile - Palo Alto Networks 3: Security Profile: Anti-Spyware - Palo Alto Networks

NEW QUESTION 123
An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

                        Security policy = drop, Gambling category in URL profile = allow
A:
B. Security policy = den
C. Gambling category in URL profile = block
D. Security policy = allow, Gambling category in URL profile = alert
E. Security policy = allo
F. Gambling category in URL profile = allow

Answer: C

NEW QUESTION 127
                        Which Security profile would you apply to identify infected hosts on the protected network uwall user database?

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

Answer: A

NEW QUESTION 128
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 131
Which protocol used to map username to user groups when user-ID is configured?

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

Answer: D

NEW QUESTION 135
Which action results in the firewall blocking network traffic without notifying the sender?

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

Answer: C

NEW QUESTION 139

Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

A. GlobalProtect
B. AutoFocus
C. Aperture
D. Panorama

Answer: A

Explanation:
 GlobalProtect: GlobalProtect safeguards your mobile workforce by inspecting all traffic using your next-generation firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud.

NEW QUESTION 144
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?

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

Answer: D

Explanation:

NEW QUESTION 146
Which service protects cloud-based applications such as Dropbox and Salesforce by administering permissions and scanning files for sensitive information?

A. Aperture
B. AutoFocus
C. Parisma SaaS
D. GlobalProtect

Answer: C

NEW QUESTION 148
By default, what is the maximum number of templates that can be added to a template stack?

A. 6
B. 8
C. 10
D. 12

Answer: B

Explanation:
By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug command to increase the maximum number of templates per stack to 16. This command requires a commit operation to take effect.
A template stack is a collection of templates that you can use to push common settings to multiple firewalls or Panorama managed collectors. A template contains the network and device settings that you want to share across devices, such as interfaces, zones, virtual routers, DNS, NTP, and login banners. You can create multiple templates for different device groups or locations and add them to a template stack in a hierarchical order. The settings in the lower templates override the settings in the higher templates if there are any conflicts. You can then assign a template stack to one or more devices and push the configuration changes.

NEW QUESTION 150
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)

A. Option A
B. Option B
C. Option C

D.   Option D

Answer: C

NEW QUESTION 155
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 159
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

Explanation:

NEW QUESTION 164
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?

A. Increase the backup capacity for configuration backups per firewall
B. Increase the per-firewall capacity for address and service objects
C. Reduce the configuration and session synchronization time between HA pairs
D. Reduce the number of objects pushed to a firewall

Answer: D

NEW QUESTION 169
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 172
What in the minimum frequency for which you can configure the firewall too 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:

WildFire   Provides near real-time malware and antivirus signatures created as a result of the analysis done by the WildFire public cloud. **WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability.** Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.

NEW QUESTION 177
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 182
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

Explanation:
Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/enable-automated-commit-recovery.html

NEW QUESTION 185
An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?

A. Eleven rules use the "Infrastructure* tag.
B. The view Rulebase as Groups is checked.
C. There are seven Security policy rules on this firewall.
D. Highlight Unused Rules is checked.

Answer: B

Explanation:

NEW QUESTION 188
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

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

Answer: A

NEW QUESTION 190
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, HTT
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 194
An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.
Which object should the administrator use as a match condition in the Security policy?

A. the Content Delivery Networks URL category
B. the Online Storage and Backup URL category
C. an application group containing all of the file-sharing App-IDs reported in the traffic logs
D. an application filter for applications whose subcategory is file-sharing

Answer: D

NEW QUESTION 198
What is a function of application tags?

A. creation of new zones
B. application prioritization
C. automated referenced applications in a policy

D. IP address allocations in DHCP

Answer: C

NEW QUESTION 199
DRAG DROP
Place the following steps in the packet processing order of operations from first to last.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 203
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 204
Which action can be set in a URL Filtering Security profile to provide users temporary access to all websites in a given category using a provided password?

A. Mastered
B. Not Mastered

**Answer:** A

Explanation:
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 208
Given the topology, which zone type should you configure for firewall interface E1/1?
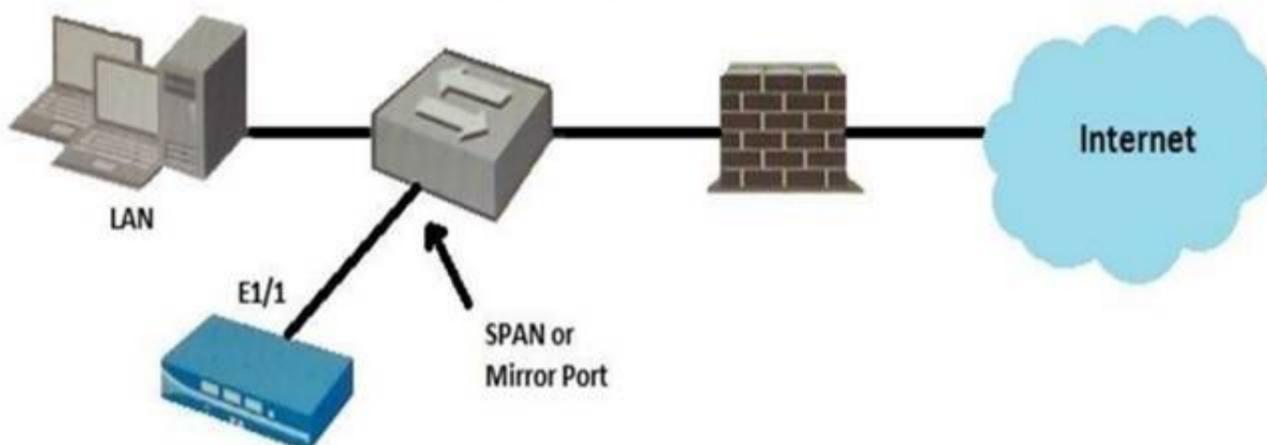

A. Tap
B. Tunnel

C. Virtual Wire
D. Layer3

Answer: A

NEW QUESTION 209
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)
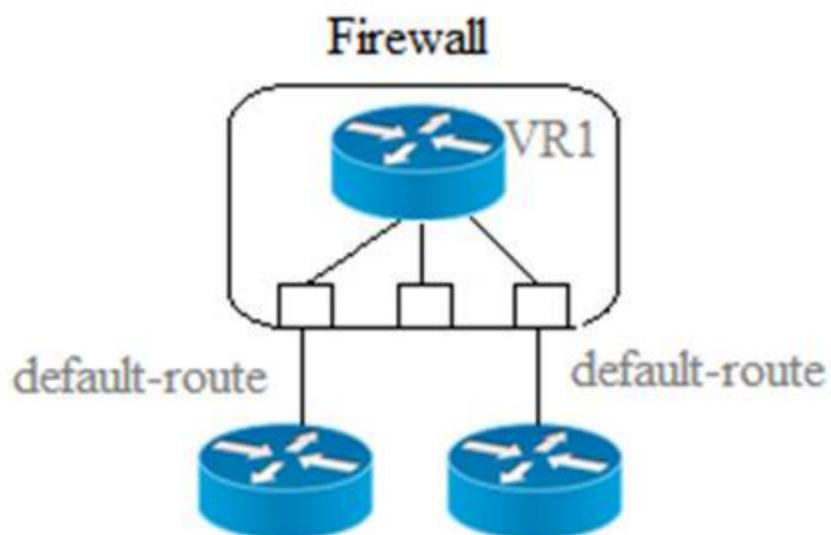
Path monitoring does not determine if route is useable
A: Route with highest metric is actively used
B
C. Path monitoring determines if route is useable
D. Route with lowest metric is actively used

Answer: CD

NEW QUESTION 211
Selecting the option to revert firewall changes will replace what settings?

A. The running configuration with settings from the candidate configuration
B. The candidate configuration with settings from the running configuration
C. The device state with settings from another configuration
D. Dynamic update scheduler settings

Answer: A

NEW QUESTION 215
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: BD

NEW QUESTION 219
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?
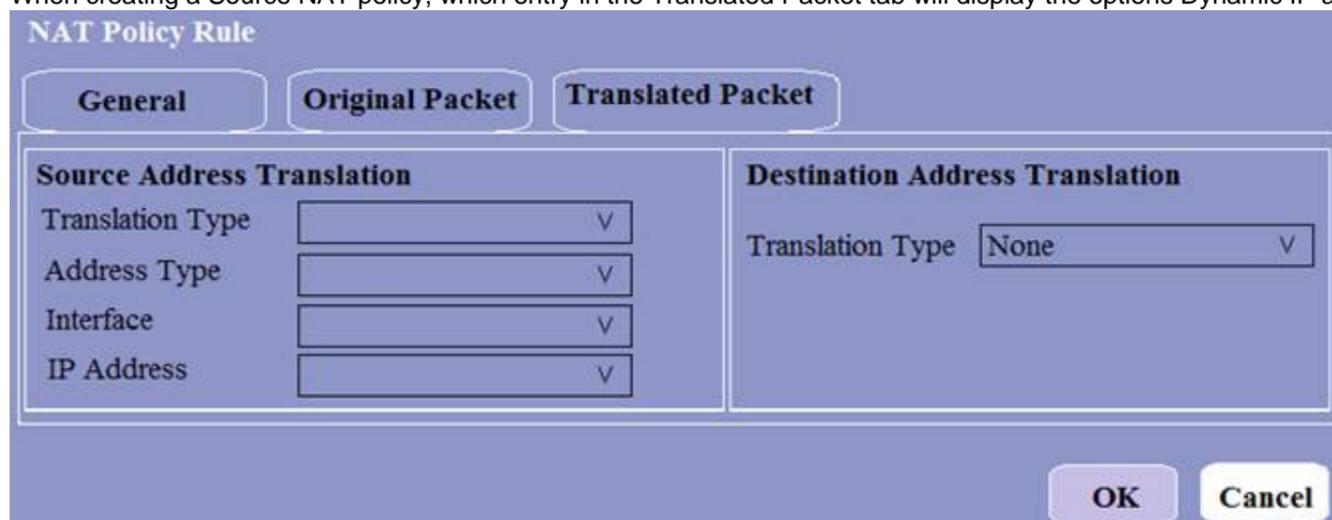
A. Translation Type
B. Interface
C. Address Type
D. IP Address

Answer: A

NEW QUESTION 220
A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

A. Windows-based agent on a domain controller
B. Captive Portal
C. Citrix terminal server with adequate data-plane resources
D. PAN-OS integrated agent

Answer: A

NEW QUESTION 224
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 225
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-profile-actions

NEW QUESTION 229
An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.
Which type of single unified engine will get this result?

A. User-ID
B. App-ID
C. Security Processing Engine
D. Content-ID

Answer: A

NEW QUESTION 232
Where within the firewall GUI can all existing tags be viewed?

A. Network > Tags
B. Monitor > Tags
C. Objects > Tags
D. Policies > Tags

Answer: C

NEW QUESTION 234
Which type firewall configuration contains in-progress configuration changes?

A. backup
B. running
C. candidate
D. committed

Answer: C

NEW QUESTION 239

URL categories can be used as match criteria on which two policy types? (Choose two.)

A. authentication
B. decryptionC application override
C. NAT

Answer: AB

Explanation:

Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html

NEW QUESTION 243
Which rule type is appropriate for matching traffic occurring within a specified zone?

A. Interzone
B. Universal
C. Intrazone
D. Shadowed

Answer: C

NEW QUESTION 248
Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	Internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

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

Answer: D

NEW QUESTION 249
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 251
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

Explanation:

Reference: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 253
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?

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

Answer: B

NEW QUESTION 254
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 259

Which interface type requires no routing or switching but applies Security or NAT policy rules before passing allowed traffic?

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

Answer: A

NEW QUESTION 264
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. local username
B. dynamic user group
C. remote username
D. static user group

Answer: B

NEW QUESTION 265
View the diagram.
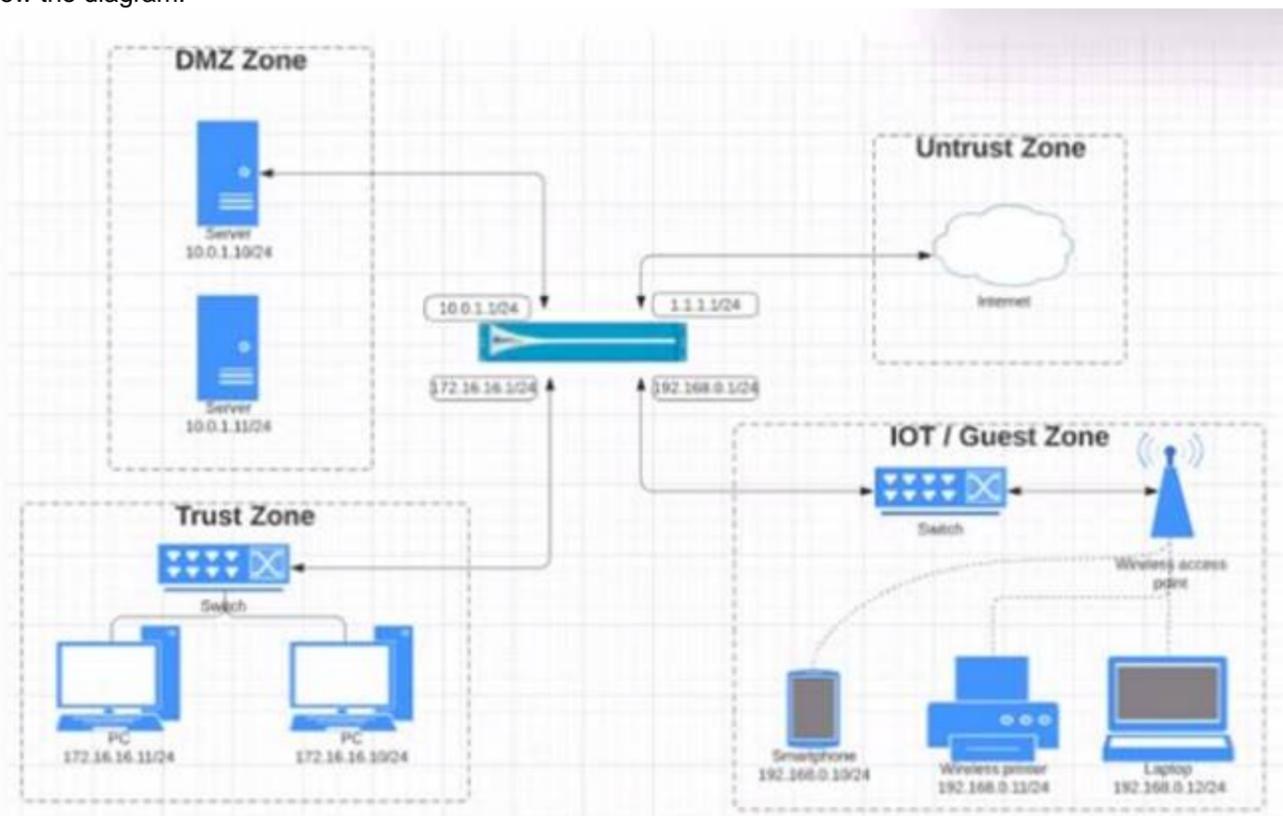
What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?
A)

        B)

C)

D)

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		

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

Answer: C

NEW QUESTION 267
Files are sent to the WildFire cloud service via the WildFire Analysis Profile. How are these files used?

A. WildFire signature updates
B. Malware analysis
C. Domain Generation Algorithm (DGA) learning
D. Spyware analysis

Answer: B

NEW QUESTION 270
What can be used as match criteria for creating a dynamic address group?

A. Usernames
B. IP addresses
C. Tags
D. MAC addresses

Answer: C

NEW QUESTION 275
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 279
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 282
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 284
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the
PCNSA Product From:

https://www.2passeasy.com/dumps/PCNSA/

Money Back Guarantee

PCNSA Practice Exam Features:

* PCNSA Questions and Answers Updated Frequently

* PCNSA Practice Questions Verified by Expert Senior Certified Staff

* PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year