

## PCNSA Dumps

### Palo Alto Networks Certified Network Security Administrator

<https://www.certleader.com/PCNSA-dumps.html>



**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**

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 4**

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?

**No App Specified**  
These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks you convert these service only security policies to application based policies.

|   | Name           | Service             | Traffic (Bytes, 30 days) | App Usage    |           |                       | Compare | Modified     |
|---|----------------|---------------------|--------------------------|--------------|-----------|-----------------------|---------|--------------|
|   |                |                     |                          | Apps Allowed | Apps Seen | Days with No New Apps |         |              |
| 3 | egress-outside | application-default | 25.3G                    | any          | 8         | 8                     | Compare | 2019-06-2... |
| 1 | inside-portal  | any                 | 372.6M                   | any          | 9         | 8                     | Compare | 2019-06-2... |

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

D. Service

**Answer: C**

**NEW QUESTION 5**

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

| Name                        | Type      | Source |         | Destination |              | Application                       | Service             | Action |
|-----------------------------|-----------|--------|---------|-------------|--------------|-----------------------------------|---------------------|--------|
|                             |           | Zone   | Address | Zone        | Address      |                                   |                     |        |
| 1 inside-portal             | universal | inside | any     | outside     | 203.0.113.20 | any                               | any                 | Allow  |
| 2 internal-inside-dmz       | universal | inside | any     | dmz         | any          | ftp<br>ssh<br>ssl<br>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 6**

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 7**

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 8**

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 9**

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 10**

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 10**

Which Palo Alto networks security operating platform service protects cloud-based application such as Dropbox and salesforce by monitoring permissions and shared and scanning files for Sensitive information?

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

**Answer:** A

**NEW QUESTION 13**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The precedence is from the top down; First Match Wins: 1) Block list: Manually entered blocked URLs Objects - 2) Allow list: Manually entered allowed URLs Objects - 3) Custom URL Categories - 4) Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

**NEW QUESTION 18**

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

**Explanation:**

Explanation/Reference: Reference:

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

**NEW QUESTION 22**

Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

- A. outbound
- B. north south
- C. inbound
- D. east west

**Answer: D**

**NEW QUESTION 26**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**NEW QUESTION 28**

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 33**

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

|   |  |  |
|---|--|--|
| Device SN: 007251000154341<br>IP Protocol: udp<br>Log Action: global-logs<br>Generated Time: 2021/08/27 02:02:49<br>Receive Time: 2021/08/27 02:02:53<br>Tunnel Type: N/A   | Interface: ethernet1/4<br>NAT IP: 67.290.64.58<br>NAT Port: 26251<br>X-Forwarded-For IP: 0.0.0.0 | NAT IP: 8.8.4.4<br>NAT Port: 53  |
| <b>Details</b>  |  | <b>Flags</b>   |
| Threat Type: spyware<br>Threat ID/Name: Phishing:151.136.74.in-addr.arpa<br>ID: 109010001 (View in Threat Vault)<br>Category: dns-phishing<br>Content Version: AppThreat-0-0<br>Severity: low<br>Repeat Count: 2<br>File Name:<br>URL: 151.136.74.in-addr.arpa<br>Partial Hash: 0<br>Prap ID: 0<br>Source UUID:<br>Destination UUID:<br>Dynamic User Group:<br>Network Slice ID SST: 0<br>Network Slice ID SD:<br>App Category: networking<br>App Subcategory: infrastructure<br>App Technology: network-protocol<br>App Characteristic: used-by-malware-has-known-vulnerability-pervasive-use<br>App Container:<br>App Risk: 3 |  | Captive Portal: <input type="checkbox"/><br>Proxy Transaction: <input type="checkbox"/><br>Decrypted: <input type="checkbox"/><br>Packet Capture: <input type="checkbox"/><br>Client to Server: <input checked="" type="checkbox"/><br>Server to Client: <input type="checkbox"/><br>Tunnel Inspected: <input type="checkbox"/>  |
| <b>DeviceID</b>   |  | Source Device Category: Virtual Machine<br>Source Device Profile: VMware<br>Source Device Model:<br>Source Device Vendor: VMware, Inc.<br>Source Device OS Family:<br>Source Device OS Version:<br>Source Device Host: ubuntu-server<br>Source Device MAC: 00:50:56:a2:19:63<br>Destination Device Category:<br>Destination Device Profile:<br>Destination Device Model: |

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

**Answer: C**

**NEW QUESTION 38**

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 from the gambling URL category.

C. Add \*.powerball.com to the URL Filtering allow list.

D. Create a custom URL category, add \*.powerball.com to it and allow it in the Security Profile.

**Answer:** CD

**NEW QUESTION 40**

An administrator is implementing an exception to an external dynamic list by adding an entry to the list manually. The administrator wants to save the changes, but the OK button is grayed out.

What are two possible reasons the OK button is grayed out? (Choose two.)

A. The entry contains wildcards.

B. The entry is duplicated.

C. The entry doesn't match a list entry.

D. The entry matches a list entry.

**Answer:** BC

**NEW QUESTION 44**

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 49**

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 50**

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 54**

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

- A. GlobalProtect agent
- B. XML API
- C.

User-ID Windows-based agent

- D. log forwarding auto-tagging

**Answer:** BC

**NEW QUESTION 55**

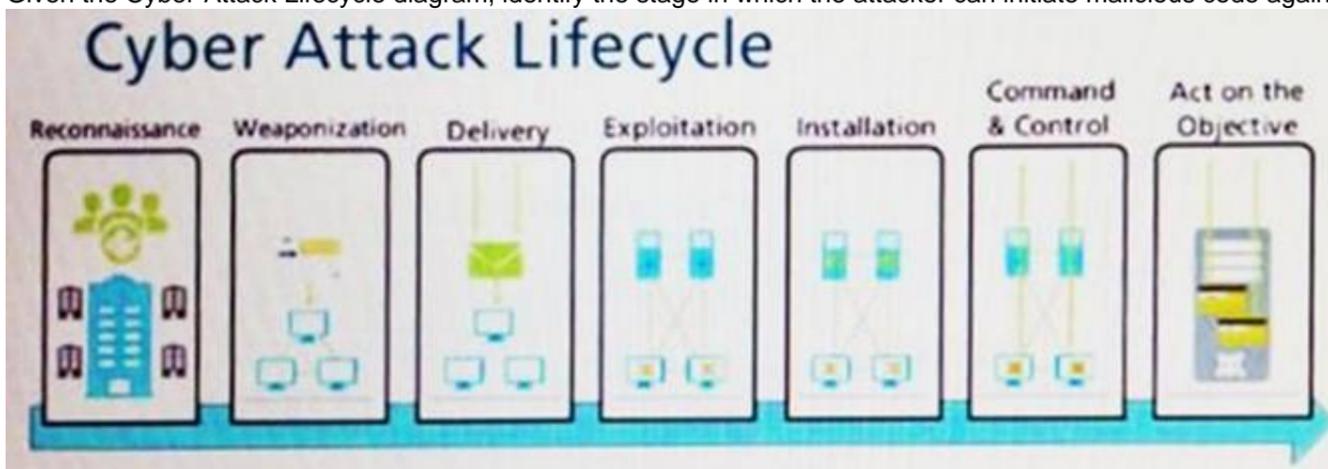
By default, which action is assigned to the interzone-default rule?

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

**Answer:** C

**NEW QUESTION 60**

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



- A.

Exploitation

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

**Answer:** A

**NEW QUESTION 61**

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 62**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 65**

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 70**

Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

- A. reconnaissance
- B. delivery
- C. exploitation
- D. installation

**Answer:** B

**Explanation:**

Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious links, or attachments and malvertising.

? Gain full visibility into all traffic, including SSL, and block high-risk applications.

Extend those protections to remote and mobile devices.

? Protect against perimeter breaches by blocking malicious or risky websites through URL filtering.

? Block known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti-malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking.

? Detect unknown malware and automatically deliver protections globally to thwart new attacks.

? Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.  
<https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle>

**NEW QUESTION 74**

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

- A. Mastered
- B. Not Mastered

**Answer: A**

**NEW QUESTION 77**

If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?

A)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: Application-Default  
Applications: SSH  
Action: Deny

B)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: SSH  
Applications: Any  
Action: Allow

C)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: SSH  
Applications: Any  
Action: Deny

D)

Source Zone: Trusted  
Destination Zone: DMZ  
Services: Application-Default  
Applications: SSH  
Action: Allow

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

**Answer: D**

**NEW QUESTION 80**

Which option lists the attributes that are selectable when setting up an Application filters?

- A. Category, Subcategory, Technology, and Characteristic
- B. Category, Subcategory, Technology, Risk, and Characteristic
- C. Name, Category, Technology, Risk, and Characteristic
- D. Category, Subcategory, Risk, Standard Ports, and Technology

**Answer: B**

**Explanation:**

Explanation/Reference: Reference:

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters>

**NEW QUESTION 81**

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

Security policy rules inspect but do not block traffic.

- A. Security Profile should be used only on allowed traffic.
- C. Security Profiles 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 82**

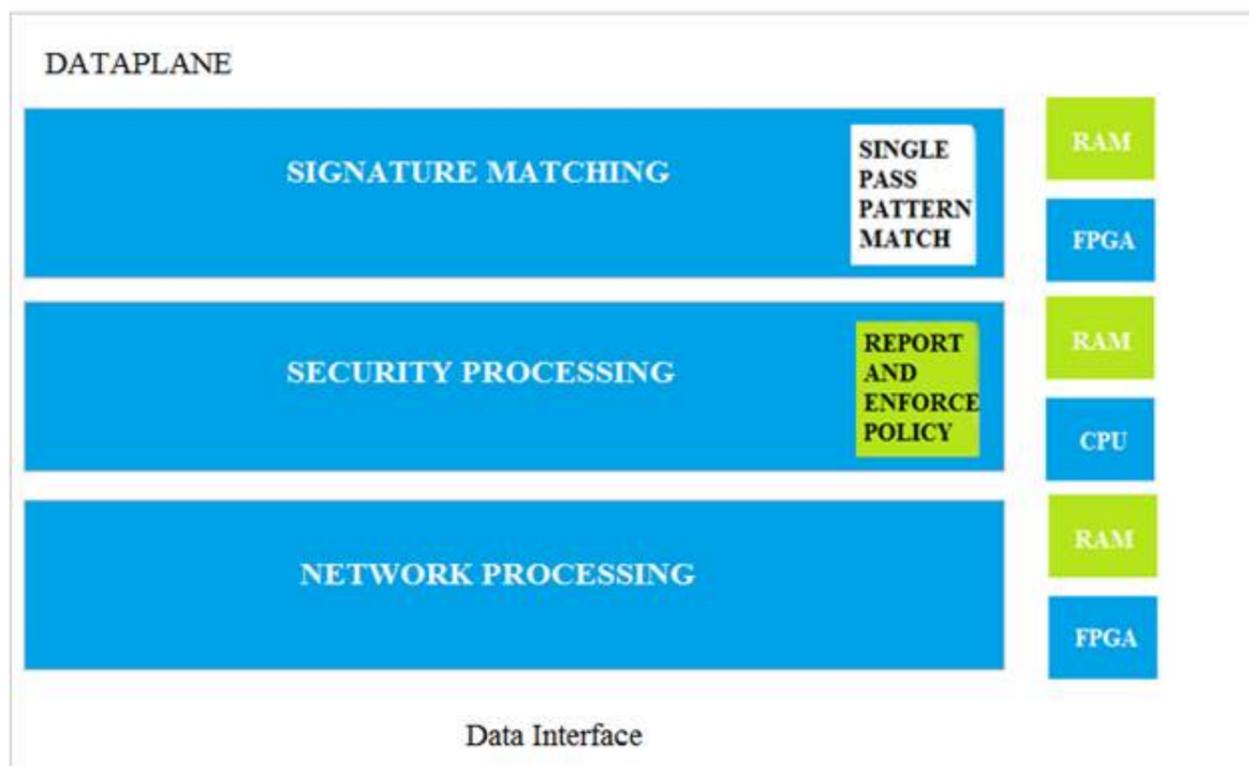
What is the main function of the Test Policy Match function?

- 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 83**

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 86**

You must configure which firewall feature to enable a data-plane interface to submit DNS queries on behalf of the control plane?

- A. Admin Role profile
- B. virtual router
- C. DNS proxy
- D. service route

**Answer:** A

**NEW QUESTION 88**

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

**NEW QUESTION 91**

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 will 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 95**

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

**Explanation:**

Reference:

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

**NEW QUESTION 100**

What does an application filter help you to do?

- A. It dynamically provides application statistics based on network, threat, and blocked activity,
- B. It dynamically filters applications based on critical, high, medium, low or informational severity.
- C. It dynamically groups applications based on application attributes such as category and subcategory.
- D. It dynamically shapes defined application traffic based on active sessions and bandwidth usage.

**Answer:** C

**NEW QUESTION 102**

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 105**

A server-admin in the USERS-zone requires SSH-access to all possible servers in all current and future Public Cloud environments. All other required connections have already been enabled between the USERS- and the OUTSIDE-zone. What configuration-changes should the Firewall-admin make?

- A. Create a custom-service-object called SERVICE-SSH for destination-port-TCP-22. Create a security-rule between zone USERS and OUTSIDE to allow traffic from any source IP-address to any destination IP-address for SERVICE-SSH
- B. Create a security-rule that allows traffic from zone USERS to OUTSIDE to allow traffic from any source IP-address to any destination IP-address for application SSH
- C. In addition to option a, a custom-service-object called SERVICE-SSH-RETURN that contains source-port-TCP-22 should be create
- D. A second security-rule is required that allows traffic from zone OUTSIDE to USERS for SERVICE-SSH-RETURN for any source- IP-address to any destination-IP-address
- E. In addition to option c, an additional rule from zone OUTSIDE to USERS for application SSH from any source-IP-address to any destination-IP-address is required to allow the return-traffic from the SSH-servers to reach the server-admin

**Answer:** B

**NEW QUESTION 106**

Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?

- A. Management

- B. High Availability
- C. Aggregate
- D. Aggregation

**Answer: C**

**NEW QUESTION 108**

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 111**

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 389

**Answer: B**

**Explanation:**

? 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 112**

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 exfiltrated corporate data.

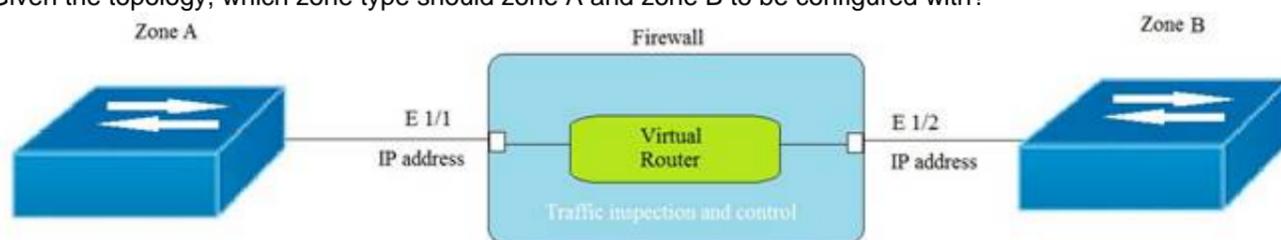
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

- 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 114**

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



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

**Answer: A**

**NEW QUESTION 119**

DRAG DROP

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

| Operational Task             | Answer Area |        |
|------------------------------|-------------|--------|
| Security profile enforcement |             | first  |
| decryption                   |             | second |
| zone protection              |             | third  |
| App-ID                       |             | fourth |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**NEW QUESTION 123**

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. pattern based application identification
- B. application override policy match
- C. session application identified
- D. application changed from content inspection

**Answer:** AB

**Explanation:**

Reference:<http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

**NEW QUESTION 124**

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

**Explanation:**

Reference:

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

**NEW QUESTION 126**

The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop. Which security profile feature could have been used to prevent the communication with the CnC server?

- A. Create an anti-spyware profile and enable DNS Sinkhole
- B. Create an antivirus profile and enable DNS Sinkhole
- C. Create a URL filtering profile and block the DNS Sinkhole category
- D. Create a security policy and enable DNS Sinkhole

**Answer:** A

**Explanation:**

**NEW QUESTION 130**

What is the correct process for creating a custom URL category?

- A. Objects > Security Profiles > URL Category > Add
- B. Objects > Custom Objects > URL Filtering > Add
- C. Objects > Security Profiles > URL Filtering > Add
- D. Objects > Custom Objects > URL Category > Add

**Answer:** D

**Explanation:**

**NEW QUESTION 131**

Which User Credential Detection method should be applied within a URL Filtering Security profile to check for the submission of a valid corporate username and the associated password?

- A. Domain Credential
- B. IP User
- C. Group Mapping
- D. Valid Username Detected Log Severity

**Answer: C**

**NEW QUESTION 135**

Which interface type can use virtual routers and routing protocols?

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

**Answer: B**

**NEW QUESTION 136**

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 141**

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**

**Explanation:**

Reference:<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 142**

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 144**

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

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

**Answer: BCE**

**NEW QUESTION 149**

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?

default

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

**Answer:** C

**NEW QUESTION 154**

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 155**

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

**Explanation:**

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

**NEW QUESTION 156**

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

**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 159**

Which Security profile must be added to Security policies to enable DNS Signatures to be checked?

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

**Answer:** D

**NEW QUESTION 161**

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 164**

DRAG DROP

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

|                       | Answer Area          |  |
|-----------------------|----------------------|--|
| reconnaissance        | <input type="text"/> | stage that reveals the attacker's motivation                 |
| installation          | <input type="text"/> | stage where the attacker scans for network exploited         |
| command and control   | <input type="text"/> | stage where the attacker will explore methods of persistence |
| act on the objectives | <input type="text"/> | stage where the attacker has access to a system              |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

|                       | Answer Area  |  |
|-----------------------|--|--|
| reconnaissance        | <input type="text" value="reconnaissance"/>        | stage that reveals the attacker's motivation                 |
| installation          | <input type="text" value="installation"/>          | stage where the attacker scans for network exploited         |
| command and control   | <input type="text" value="command and control"/>   | stage where the attacker will explore methods of persistence |
| act on the objectives | <input type="text" value="act on the objectives"/> | stage where the attacker has access to a system              |

**NEW QUESTION 166**

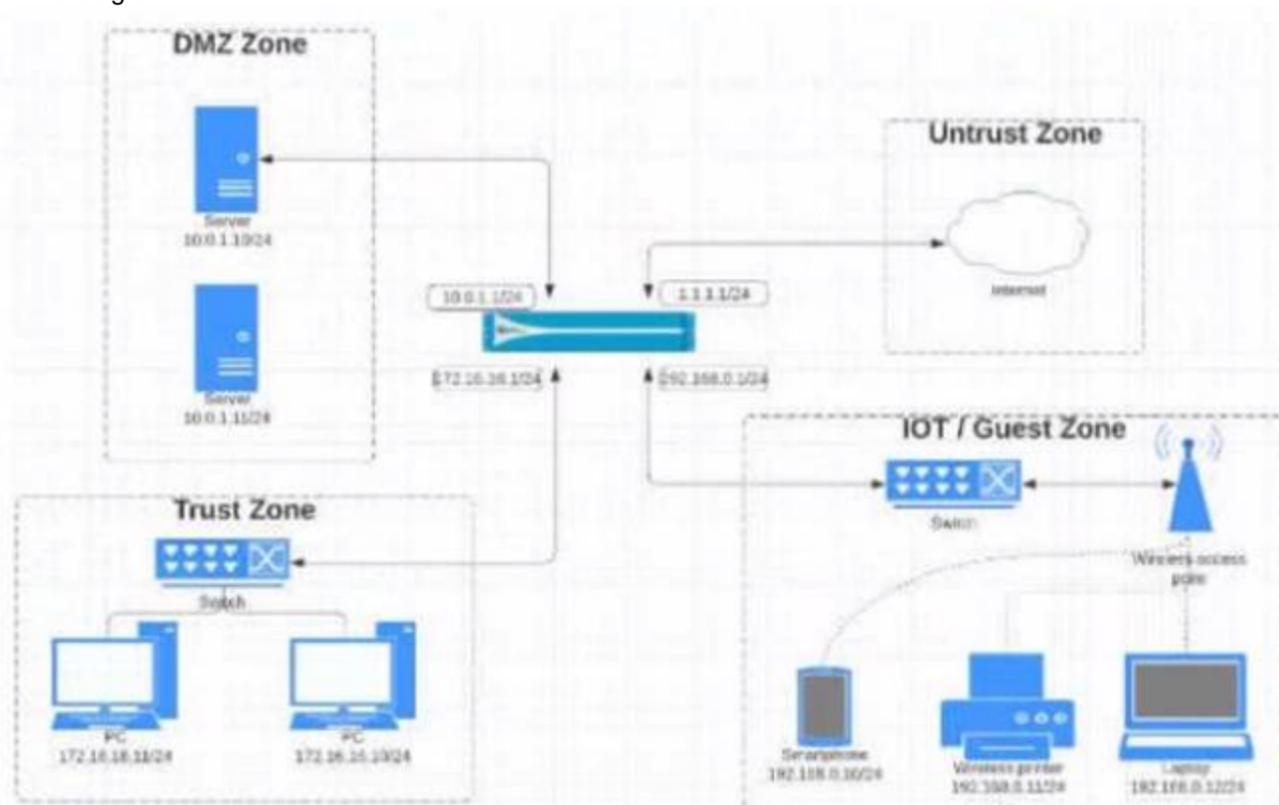
An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration. Why doesn't the administrator see the traffic?

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

Answer: D

**NEW QUESTION 171**

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)

|        | Source         |      |        | Destination |            |        | APPLICATION  | SERVICE             | URL CATEGORY | ACTION |
|--------|----------------|------|--------|-------------|------------|--------|--------------|---------------------|--------------|--------|
|        | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS    | DEVICE |              |                     |              |        |
| Source | 172.16.16.0/24 | any  | any    | DMZ         | 1.1.1.0/24 | any    | ssh          | application-default | any          | Allow  |
|        | 192.168.0.0/24 |      |        | Untrust     | 100.1.0/24 |        | ssh          |                     |              |        |
|        |                |      |        |             |            |        | web-browsing |                     |              |        |

B)

|        | Source         |      |        | Destination |                |        | APPLICATION  | SERVICE             | URL CATEGORY | ACTION |
|--------|----------------|------|--------|-------------|----------------|--------|--------------|---------------------|--------------|--------|
|        | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS        | DEVICE |              |                     |              |        |
| Source | 10.0.1.0/24    | any  | any    | DMZ         | 1.1.1.0/24     | any    | ssh          | application-default | any          | Allow  |
|        | 172.16.16.0/12 |      |        | Untrust     | 192.168.0.0/24 |        | ssh          |                     |              |        |
|        |                |      |        |             |                |        | web-browsing |                     |              |        |

C)

|        | Source         |      |        | Destination |         |        | APPLICATION  | SERVICE             | URL CATEGORY | ACTION |
|--------|----------------|------|--------|-------------|---------|--------|--------------|---------------------|--------------|--------|
|        | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS | DEVICE |              |                     |              |        |
| Source | 172.16.16.0/24 | any  | any    | DMZ         | any     | any    | ssh          | application-default | any          | Allow  |
|        | 192.168.0.0/24 |      |        | Untrust     |         |        | ssh          |                     |              |        |
|        |                |      |        |             |         |        | web-browsing |                     |              |        |

D)

|        | Source         |      |        | Destination |         |        | APPLICATION  | SERVICE             | URL CATEGORY | ACTION |
|--------|----------------|------|--------|-------------|---------|--------|--------------|---------------------|--------------|--------|
|        | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS | DEVICE |              |                     |              |        |
| Source | 172.16.16.0/24 | any  | any    | DMZ         | any     | any    | ssh          | application-default | any          | Allow  |
|        | 192.168.0.0/24 |      |        | Untrust     |         |        | ssh          |                     |              |        |
|        |                |      |        |             |         |        | web-browsing |                     |              |        |

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

**Answer: C**

**NEW QUESTION 176**

Within an Anti-Spyware security profile, which tab is used to enable machine learning based engines?

- A. Inline Cloud Analysis
- B. Signature Exceptions
- C. Machine Learning Policies
- D. Signature Policies

**Answer: A**

**Explanation:**

? An Anti-Spyware security profile is a set of rules that defines how the firewall detects and prevents spyware from compromising hosts on the network. Spyware is a type of malware that collects information from the infected system, such as keystrokes, browsing history, or personal data, and sends it to an external command-and-control (C2) server<sup>1</sup>.

? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis<sup>1</sup>.

? The Signature Policies tab allows you to configure the actions and log settings for each spyware signature category, such as adware, botnet, keylogger, phishing, or worm. You can also enable DNS Security to block malicious DNS queries and responses<sup>1</sup>.

? The Signature Exceptions tab allows you to create exceptions for specific spyware signatures that you want to override the default action or log settings. For example, you can allow a signature that is normally blocked by the profile, or block a signature that is normally alerted by the profile<sup>1</sup>.

? The Machine Learning Policies tab allows you to configure the actions and log settings for machine learning based signatures that detect unknown spyware variants. You can also enable WildFire Analysis to submit unknown files to the cloud for further analysis<sup>1</sup>.

? The Inline Cloud Analysis tab allows you to enable machine learning based engines that detect unknown spyware variants in real time. These engines use cloud-based models to analyze the behavior and characteristics of network traffic and identify malicious patterns. You can enable inline cloud analysis for HTTP/HTTPS traffic, SMTP/SMTSP traffic, or IMAP/IMAPS traffic<sup>1</sup>.

Therefore, the tab that is used to enable machine learning based engines is the Inline Cloud Analysis tab. References:

1: Security Profile: Anti-Spyware - Palo Alto Networks

**NEW QUESTION 177**

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 178**

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:**

**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 179**

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 184**

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**

Which objects would be useful for combining several services that are often defined together?

- A. shared service objects
- B. service groups
- C. application groups
- D. application filters

**Answer:** B

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-services.html>

**NEW QUESTION 189**

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 194**

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 196**

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

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

**Answer: A**

**NEW QUESTION 199**

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 203**

Which 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: C**

**Explanation:**

**NEW QUESTION 208**

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

|   | Name                     | Type      | Source |         | Destination |         | Application      | Service       | URL Category | Action | Profile |
|---|--------------------------|-----------|--------|---------|-------------|---------|------------------|---------------|--------------|--------|---------|
|   |                          |           | Zone   | Address | Zone        | Address |                  |               |              |        |         |
| 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. intrazone-default

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

**Answer: D**

**NEW QUESTION 212**

Which statement is true regarding a Best Practice Assessment?

- The BPA tool can be run only on firewalls
- A:** It provides a percentage of adoption for each assessment data
- C. The assessment, guided by an experienced sales engineer, 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: C**

**NEW QUESTION 217**

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

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

**Answer: C**

**NEW QUESTION 219**

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 220**

Which type of address object is "10 5 1 1/0 127 248 2"?

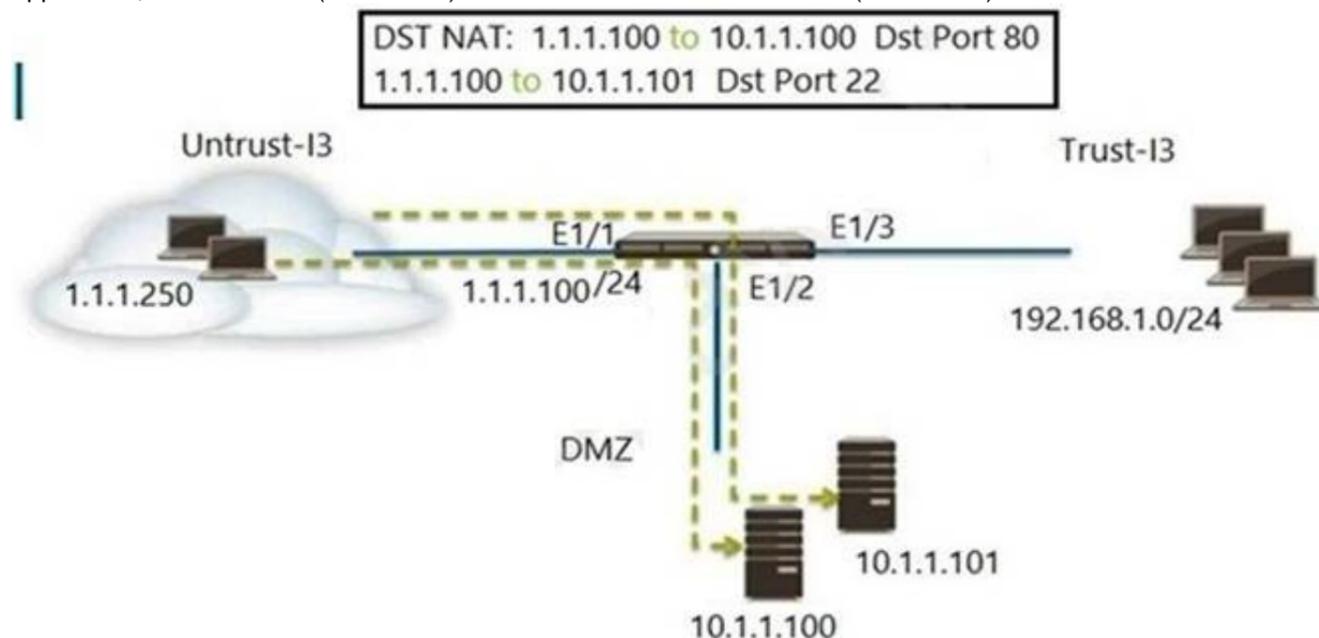
- A. IP subnet
- B. IP wildcard mask
- C. IP netmask
- D. IP range

**Answer: B**

**NEW QUESTION 221**

FILL IN THE BLANK

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

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

D. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

Answer: AE

**NEW QUESTION 224**

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 analyze file types
- D. To block uploading and downloading of any type of files

Answer: A

**NEW QUESTION 226**

Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP-to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.

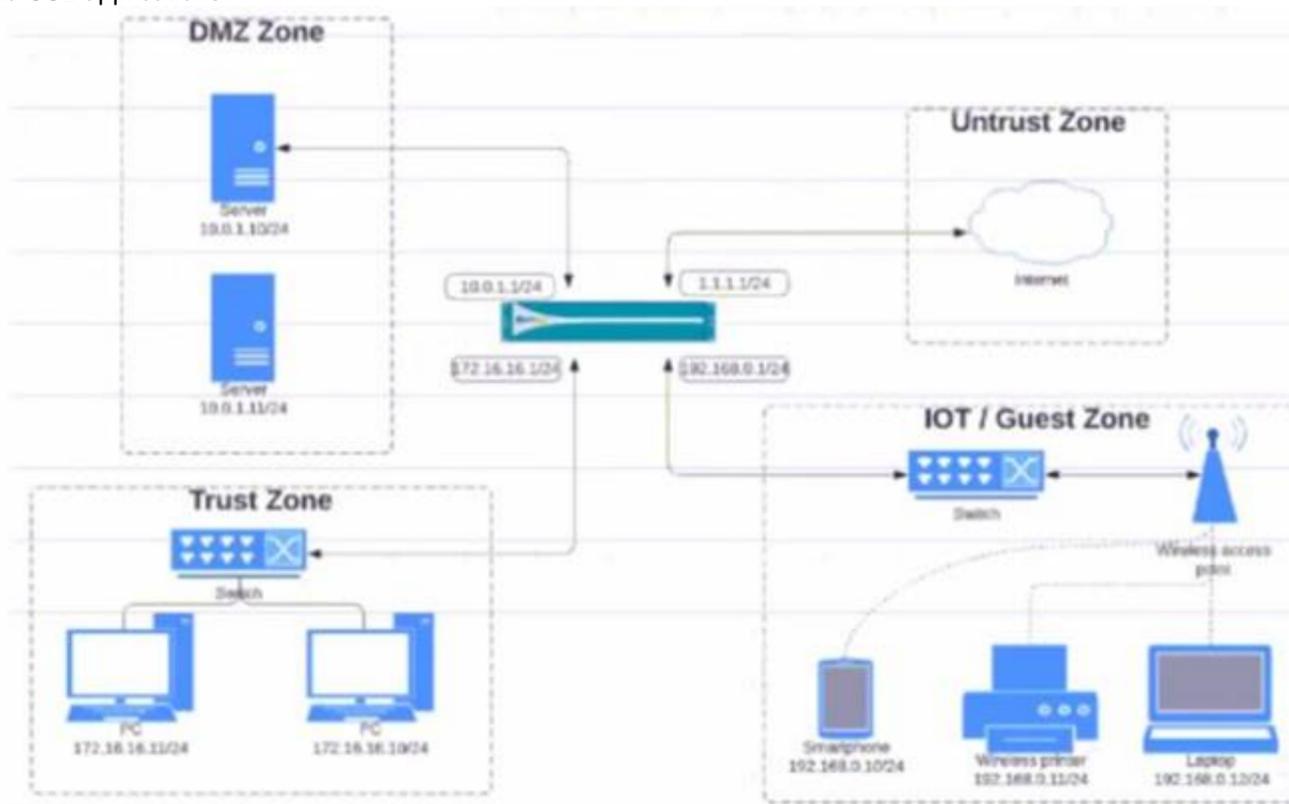
Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

- A. syslog
- B. RADIUS
- C. UID redistribution
- D. XFF headers

Answer: A

**NEW QUESTION 229**

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     | 192.168.0/24   |      |        | Untrust |             |  |

B)

| NAME | TAGS | TYPE      | Source    |                |      |        |         | Destination |  |
|------|------|-----------|-----------|----------------|------|--------|---------|-------------|--|
|      |      |           | ZONE      | ADDRESS        | USER | DEVICE | ZONE    | ADDRESS     |  |
| 03-A | none | universal | IOT-Guest | 172.16.16.0/24 | any  | any    | DMZ     | 1.1.1.0/    |  |
|      |      |           | Trust     | 192.168.0/24   |      |        | Untrust | 10.0.1.0    |  |

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 231**

An administrator would like to override the default deny action for a given application and instead would like to block the traffic and send the ICMP code "communication with the destination is administratively prohibited"  
Which security policy action causes this?

- A. Drop
- B. Drop, send ICMP Unreachable
- C. Reset both
- D. Reset server

**Answer: B**

**NEW QUESTION 234**

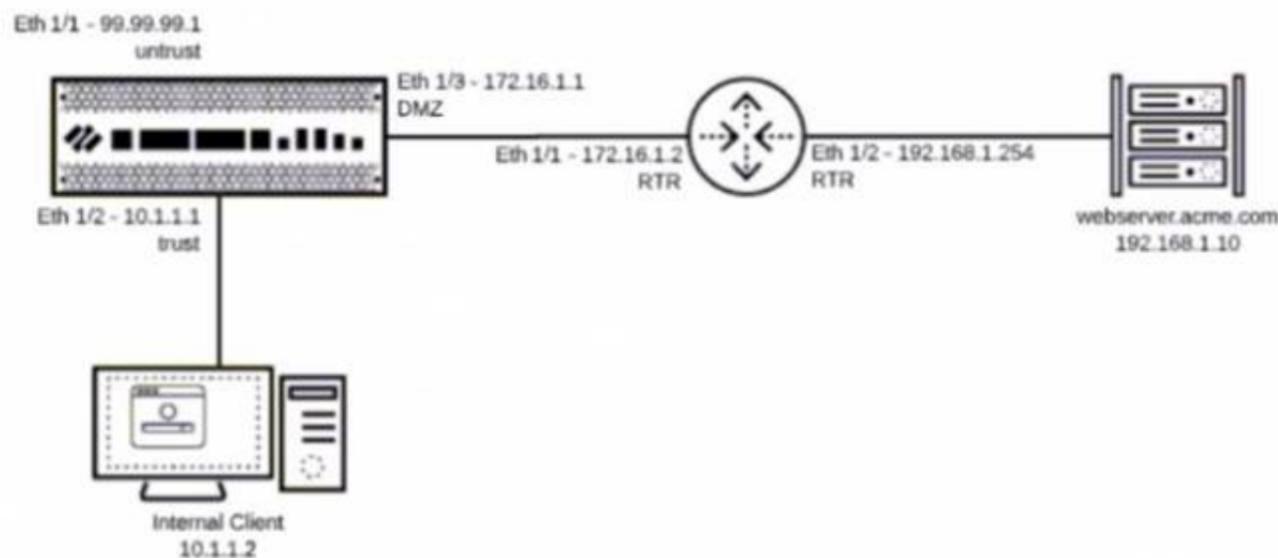
A website is unexpectedly allowed due to miscategorization.  
What are two ways to resolve this issue for a proper response? (Choose two.)

- A. Identify the URL category being assigned to the website. Edit the active URL Filtering profile and update that category's site access settings to block.
- B. Create a URL category and assign the affected URL. Update the active URL Filtering profile site access setting for the custom URL category to block.
- C. Review the categorization of the website on <https://urlfiltering.paloaltonetworks.com>
- D. Submit for "request change", identifying the appropriate categorization, and wait for confirmation before testing again.
- E. Create a URL category and assign the affected URL. Add a Security policy with a URL category qualifier of the custom URL category below the original policy.
- F. Set the policy action to Deny.

**Answer: CD**

**NEW QUESTION 237**

You have been tasked to configure access to a new web server located in the DMZ  
Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10.1.1.0/24 network to 192.168.1.0/24?



- A. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 192.168.1.10
- B. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2
- C. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 172.16.1.2
- D. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 192.168.1.254

**Answer: C**

**NEW QUESTION 238**

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**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection.html>

example, 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 241**

Which type firewall configuration contains in-progress configuration changes?

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

**Answer: C**

**NEW QUESTION 242**

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

- A. authentication
- B. decryption
- C. application override
- D. 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 246**

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 249**

How many zones can an interface be assigned with a Palo Alto Networks firewall?

- A. two
- B. three
- C. four
- D. one

**Answer: D**

**NEW QUESTION 254**

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

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

**Answer: D**

**Explanation:**

Reference:

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

**NEW QUESTION 259**

How frequently can wildfire updates be made available to firewalls?

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

**Answer:** D

**NEW QUESTION 261**

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

**NEW QUESTION 262**

The NetSec Manager asked to create a new firewall Local Administrator profile with customized privileges named NewAdmin. This new administrator has to authenticate without inserting any username or password to access the WebUI.

What steps should the administrator follow to create the New\_Admin Administrator profile?

- A.
  - \* 1. Select the "Use only client certificate authentication" check box.
  - \* 2. Set Role to Role Based.
  - \* 3. Issue to the Client a Certificate with Common Name = NewAdmin
- B.
  - \* 1. Select the "Use only client certificate authentication" check box.
  - \* 2. Set Role to Dynamic.
  - \* 3. Issue to the Client a Certificate with Certificate Name = NewAdmin
- C.
  - \* 1. Set the Authentication profile to Local.
  - \* 2. Select the "Use only client certificate authentication" check box.
  - \* 3. Set Role to Role Based.
- D.
  - \* 1. Select the "Use only client certificate authentication" check box.
  - \* 2. Set Role to Dynamic.
  - \* 3. Issue to the Client a Certificate with Common Name = New Admin

A.

**Answer:** B

**NEW QUESTION 267**

Which three filter columns are available when setting up an Application Filter? (Choose three.)

- A. Parent App
- B. Category
- C. Risk
- D. Standard Ports
- E. Subcategory

**Answer:** BCE

**Explanation:**

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-application-filters>

**NEW QUESTION 272**

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

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the->

[windows-user-id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html](#)

**NEW QUESTION 277**

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**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 281**

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 282**

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

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

**Answer:** A

**NEW QUESTION 285**

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 286**

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 288**

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 292**

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**

**Explanation:**

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 logs<sup>1</sup>. 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 action<sup>1</sup>.

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 status<sup>2</sup>.

References:

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

**NEW QUESTION 295**

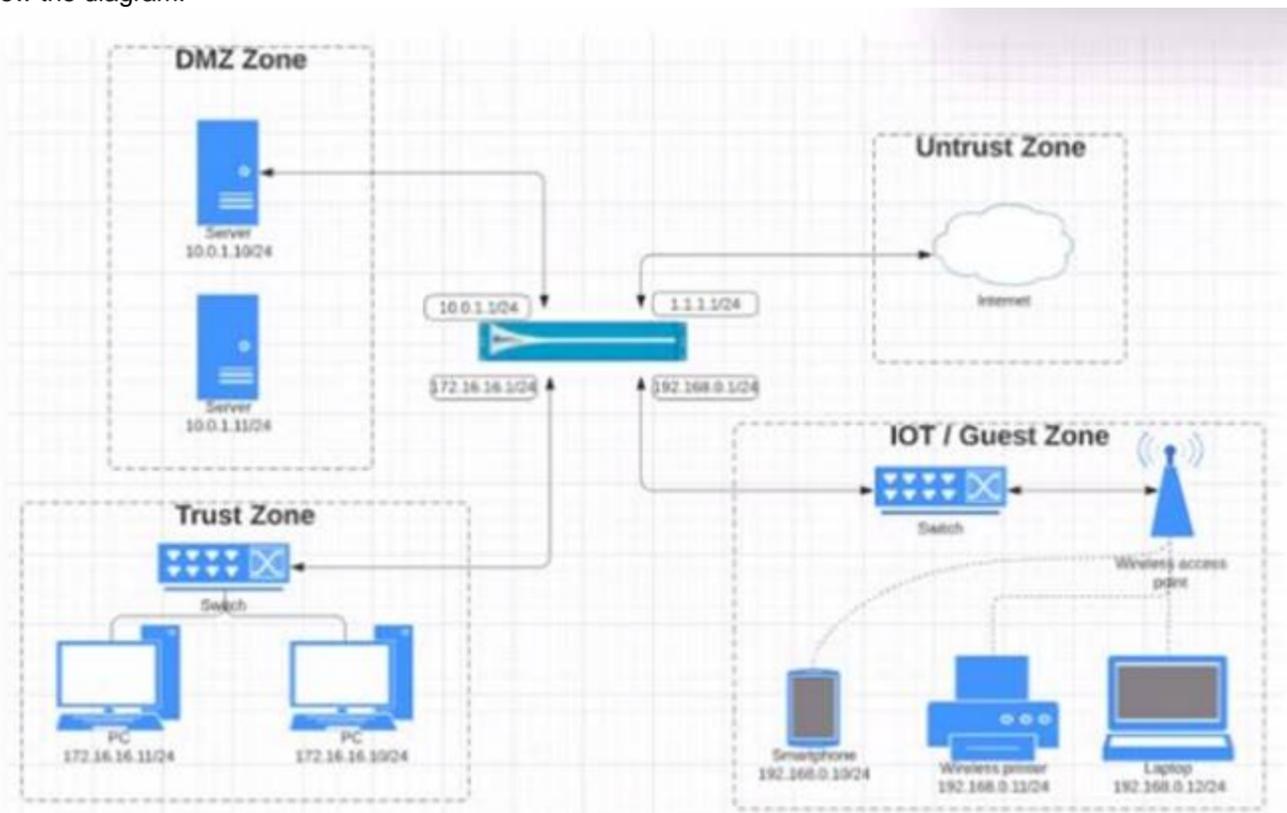
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration. What should the administrator do?

- A. Mastered
- B. Not Mastered

**Answer: A**

**NEW QUESTION 298**

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 |         |        |     | APPLICATION         | SERVICE |
|------|------|-----------|-----------|----------------|------|--------|-------------|---------|--------|-----|---------------------|---------|
|      |      |           | ZONE      | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS | DEVICE |     |                     |         |
| 10-A | None | universal | IOT-Guest | 172.16.16.0/24 | any  | any    | DMZ         | any     | any    | ssh | application-default |         |
|      |      |           | Trust     | 192.168.0.0/24 |      |        | Untrust     |         |        | ssh | web-browsing        |         |

B)

| NAME | TAGS | TYPE      | Source |                |      |        | Destination |             |        | APPLICATION | SERVICE             |
|------|------|-----------|--------|----------------|------|--------|-------------|-------------|--------|-------------|---------------------|
|      |      |           | ZONE   | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS     | DEVICE |             |                     |
| 00-A | None | universal | DMZ    | 172.16.18.0/24 | any  | any    | DMZ         | 1.1.1.0/24  | any    | web         | application-default |
|      |      |           | Trust  | 172.16.0.0/24  |      |        | Untrust     | 10.0.1.0/24 |        |             |                     |

C)

| NAME | TAGS | TYPE      | Source |                |      |        | Destination |               |        | APPLICATION | SERVICE             |
|------|------|-----------|--------|----------------|------|--------|-------------|---------------|--------|-------------|---------------------|
|      |      |           | ZONE   | ADDRESS        | USER | DEVICE | ZONE        | ADDRESS       | DEVICE |             |                     |
| 00-A | None | universal | DMZ    | 10.0.1.0/24    | any  | any    | DMZ         | 1.1.1.0/24    | any    | web         | application-default |
|      |      |           | Trust  | 172.16.16.0/12 |      |        | Untrust     | 172.16.0.0/24 |        |             |                     |

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 299**

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 300**

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**

**Explanation:**

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/enable-dnssecurity.html>

**NEW QUESTION 304**

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**

**Explanation:**

**NEW QUESTION 305**

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 on the Application tab in the Security Policy Rule creation window
- C. on the Objects > Applications browser pages

**Answer: AC**

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies.html>

**NEW QUESTION 310**

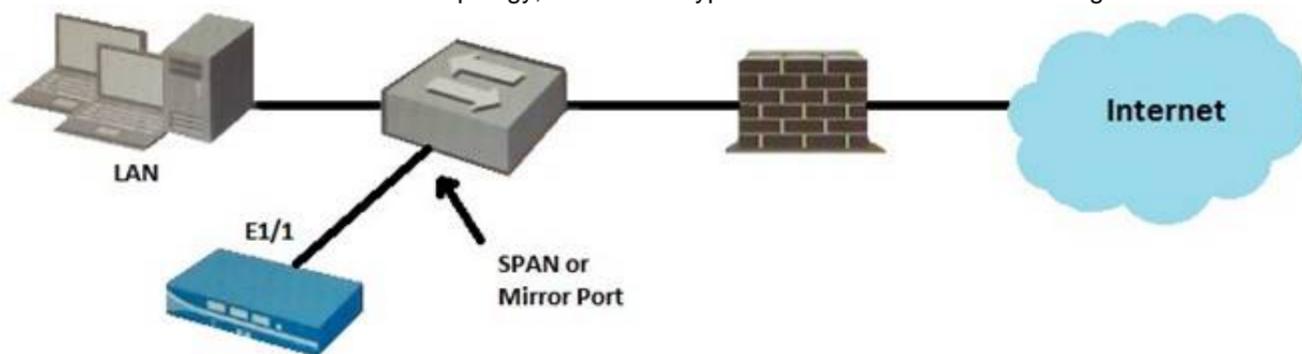
An administrator is reviewing another administrator's Security policy log settings. Which log setting configuration is consistent with best practices for normal traffic?

- A. Log at Session Start and Log at Session End both enabled
- B. Log at Session Start disabled Log at Session End enabled
- C. Log at Session Start enabled Log at Session End disabled
- D. Log at Session Start and Log at Session End both disabled

**Answer: B**

**NEW QUESTION 315**

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



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

**Answer: A**

**NEW QUESTION 320**

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**

**NEW QUESTION 321**

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

| Name       | Type      | Source |         |      | Destination |         | Application |
|------------|-----------|--------|---------|------|-------------|---------|-------------|
|            |           | Zone   | Address | User | Zone        | Address |             |
| 1 allow-it | universal | inside | any     | it   | dmz         | any     | it-tools    |

Allows users to access IT applications on all ports

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

**Answer: D**

**NEW QUESTION 326**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your PCNSA Exam with Our Prep Materials Via below:**

<https://www.certleader.com/PCNSA-dumps.html>