

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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



NEW QUESTION 1

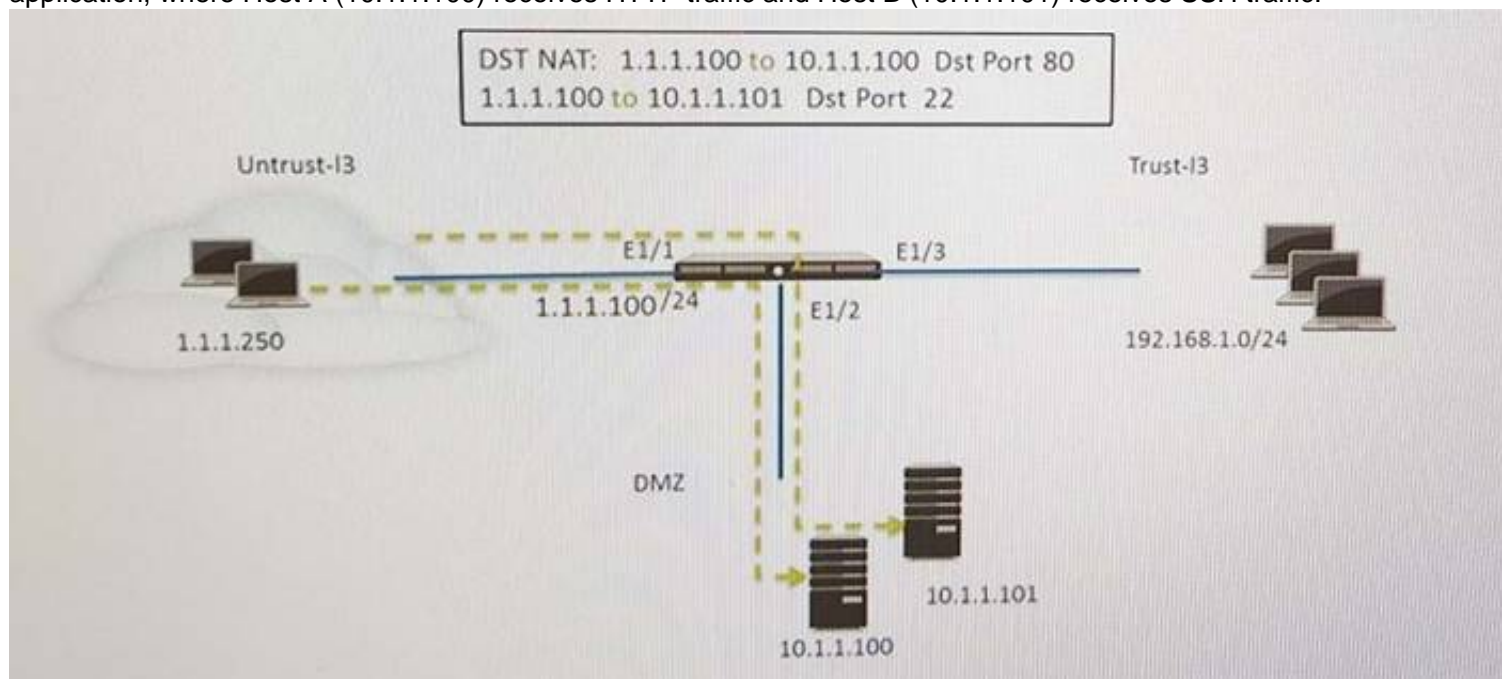
Which data flow direction is protected in a zero trust firewall deployment that is not protected in a perimeter-only firewall deployment?

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

Answer: D

NEW QUESTION 2

Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.)

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

Answer: AE

NEW QUESTION 3

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 4

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.

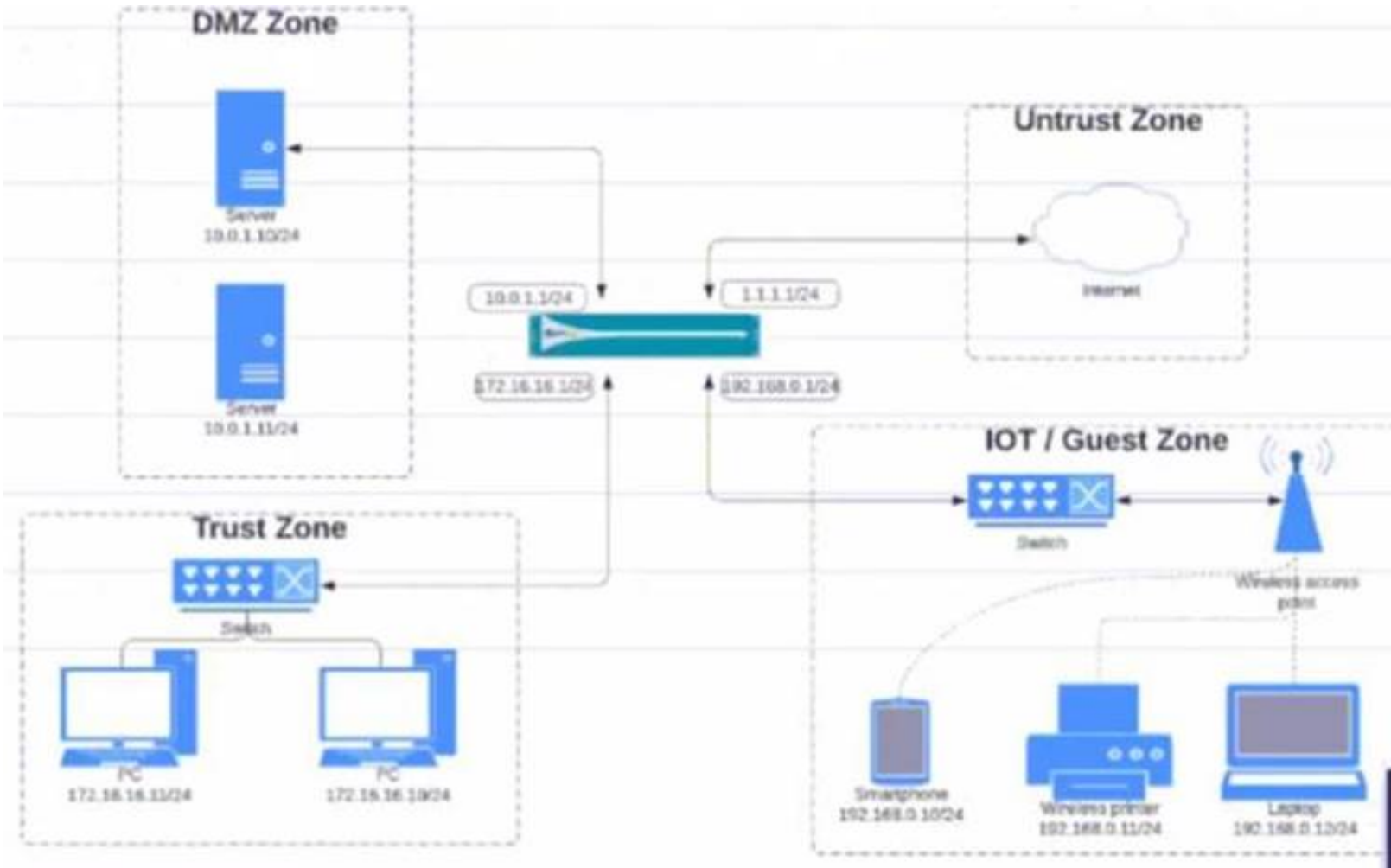
Why doesn't the administrator see the traffic?

- 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 5

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



Which policy achieves the desired results?

A)

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

B)

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

C)

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

D)

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

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

Answer: C

NEW QUESTION 6

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 7

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

- A. PAN-DB database
- B. DNS Security
- C. Custom URL categories
- D. URL external dynamic lists

Answer: A

NEW QUESTION 8

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

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

Answer: D

NEW QUESTION 9

Which administrator type utilizes predefined roles for a local administrator account?

- A. Superuser
- B. Role-based
- C. Dynamic
- D. Device administrator

Answer: C

NEW QUESTION 10

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

			Source		Destination						
	Name	Type	Zone	Address	Zone	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. intrazone-default
- B. Deny Google
- C. allowed-security services
- D. interzone-default

Answer: D

NEW QUESTION 10

The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet The firewall is configured with two zones;

- * 1. trust for internal networks
- * 2. untrust to the internet

Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)

- A. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application
- B. Create a deny rule at the top of the policy from trust to untrust with service application-default and select evasive as the application.
- C. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic.
- D. Create a deny rule at the top of the policy from trust to untrust with service application-default and add an application filter with the evasive characteristic

Answer: D

NEW QUESTION 11

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 14

A network administrator is required to use a dynamic routing protocol for network connectivity.

Which three dynamic routing protocols are supported by the NGFW Virtual Router for this purpose? (Choose three.)

- A. RIP
- B. OSPF
- C. IS-IS
- D. EIGRP
- E. BGP

Answer: ABE

NEW QUESTION 17

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

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

Answer: A

NEW QUESTION 18

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 21

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

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

Answer: B

Explanation:

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 23

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 25

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?

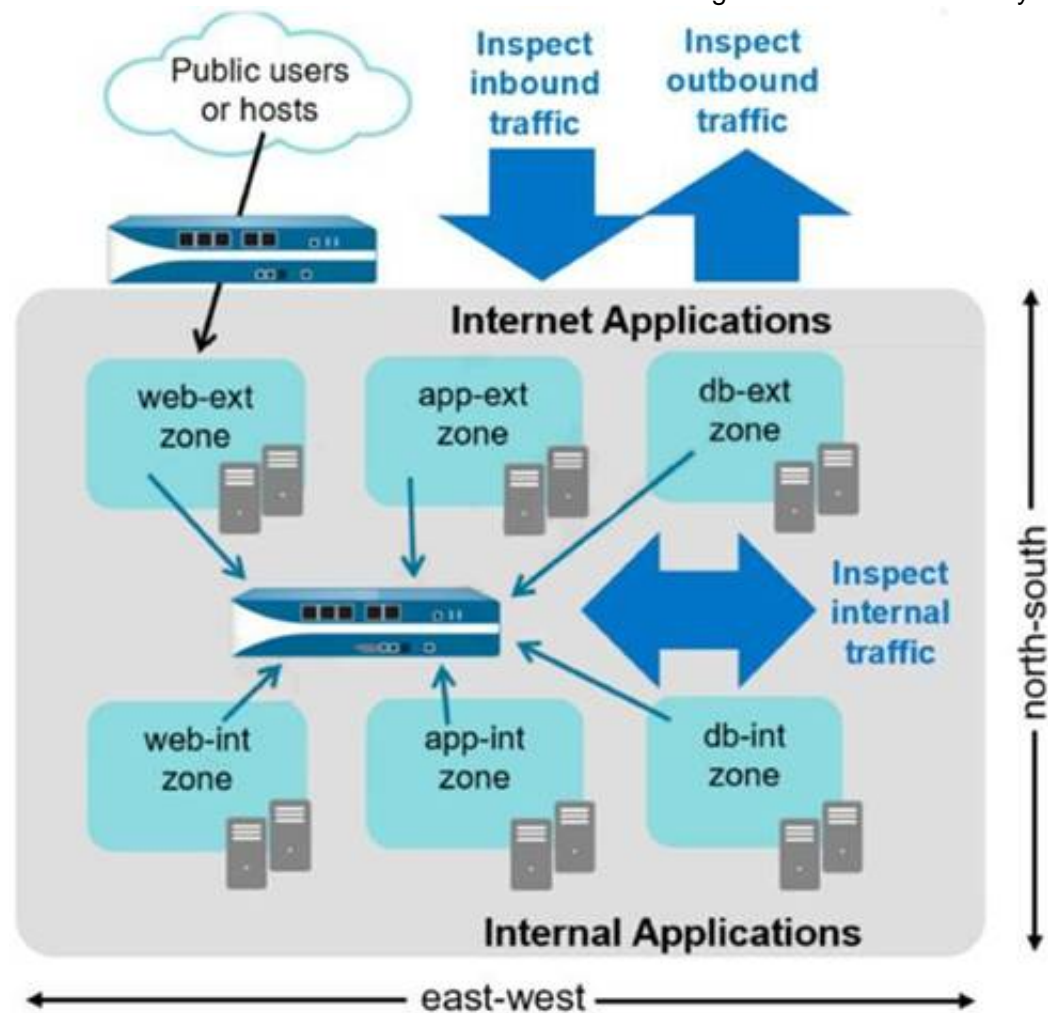
- A. Dynamic IP and Port

- B. Dynamic IP
- C. Static IP
- D. Destination

Answer: A

NEW QUESTION 26

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



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

Answer: D

NEW QUESTION 31

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 34

An administrator wants to prevent access to media content websites that are risky

Which two URL categories should be combined in a custom URL category to accomplish this goal? (Choose two)

- A. streaming-media
- B. high-risk
- C. recreation-and-hobbies
- D. known-risk

Answer: AC

NEW QUESTION 38

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

				Source				Destination		Risk Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

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

Answer: AD

Explanation:

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

NEW QUESTION 40

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 42

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?

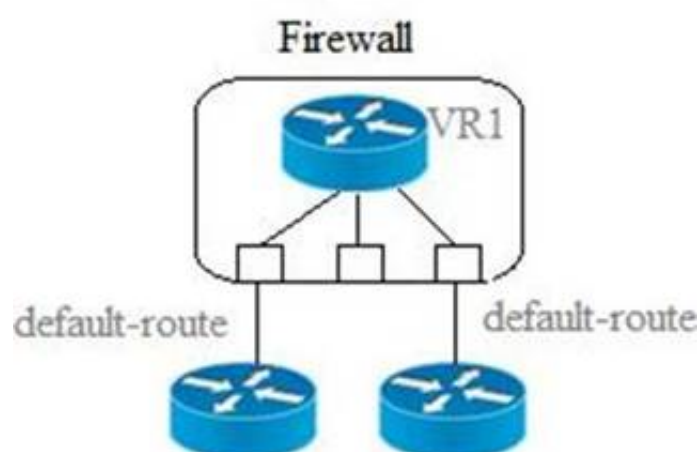
- A. Drop the traffic silently
- B. Perform the default deny action as defined in the App-ID database for the application
- C. Send a TCP reset packet to the client- and server-side devices
- D. Discard the session's packets and send a TCP reset packet to let the client know the session has been terminated

Answer: D

NEW QUESTION 47

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

Multiple Static Default Routes



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

Answer: CD

NEW QUESTION 48

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

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

Answer: C

NEW QUESTION 50

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 lookups 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 52

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

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

Answer: B

NEW QUESTION 57

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 62

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

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

Answer: B

NEW QUESTION 63

What is the maximum volume of concurrent administrative account sessions?

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

Answer: C

NEW QUESTION 66

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 67

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

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

D. security processing

Answer: A

NEW QUESTION 71

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 72

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 73

Which information is included in device state other than the local configuration?

- A. uncommitted changes
- B. audit logs to provide information of administrative account changes
- C. system logs to provide information of PAN-OS changes
- D. device group and template settings pushed from Panorama

Answer: D

NEW QUESTION 78

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 81

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 82

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 85

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 87

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

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 – 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 90

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

Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Step 1 – Select network tab

Step 2 – Select zones from the list of available items

Step 3 – Select Add

Step 4 – Specify Zone Name

Step 5 – Specify Zone Type

Step 6 – Assign interfaces as needed

NEW QUESTION 93

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 97

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. exclude
- B. continue
- C. hold
- D. override

Answer: D

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 98

An administrator would like to silently drop traffic from the internet to a ftp server. Which Security policy action should the administrator select?

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

Answer: D

NEW QUESTION 103

Palo Alto Networks firewall architecture accelerates content map minimizing latency using which two components'? (Choose two)

- A. Network Processing Engine
- B. Single Stream-based Engine
- C. Policy Engine
- D. Parallel Processing Hardware

Answer: B

NEW QUESTION 107

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

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

Answer: C

NEW QUESTION 111

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 115

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

Reconnaissance	Drag answer here	stage where the attacker has motivation for attacking a network to deface web property
Installation	Drag answer here	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	Drag answer here	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	Drag answer here	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reconnaissance – stage where the attacker scans for network vulnerabilities and services that can be exploited. Installation – stage where the attacker will explore methods such as a root kit to establish persistence Command and Control – stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
Act on the Objective – stage where an attacker has motivation for attacking a network to deface web property

NEW QUESTION 119

Identify the correct order to configure the PAN-OS integrated USER-ID agent.

- * 3. add the service account to monitor the server(s)
- * 2. define the address of the servers to be monitored on the firewall
- * 4. commit the configuration, and verify agent connection status
- * 1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

- A. 2-3-4-1
- B. 1-4-3-2
- C. 3-1-2-4
- D. 1-3-2-4

Answer: D

NEW QUESTION 120

An administrator is configuring a NAT rule

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

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

Answer: BDE

NEW QUESTION 123

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 125

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-users>

NEW QUESTION 126

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

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

Answer: D

Explanation:

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

NEW QUESTION 129

What is the main function of Policy Optimizer?

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

Answer: D

NEW QUESTION 131

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 135

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

NEW QUESTION 138

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

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

Answer: D

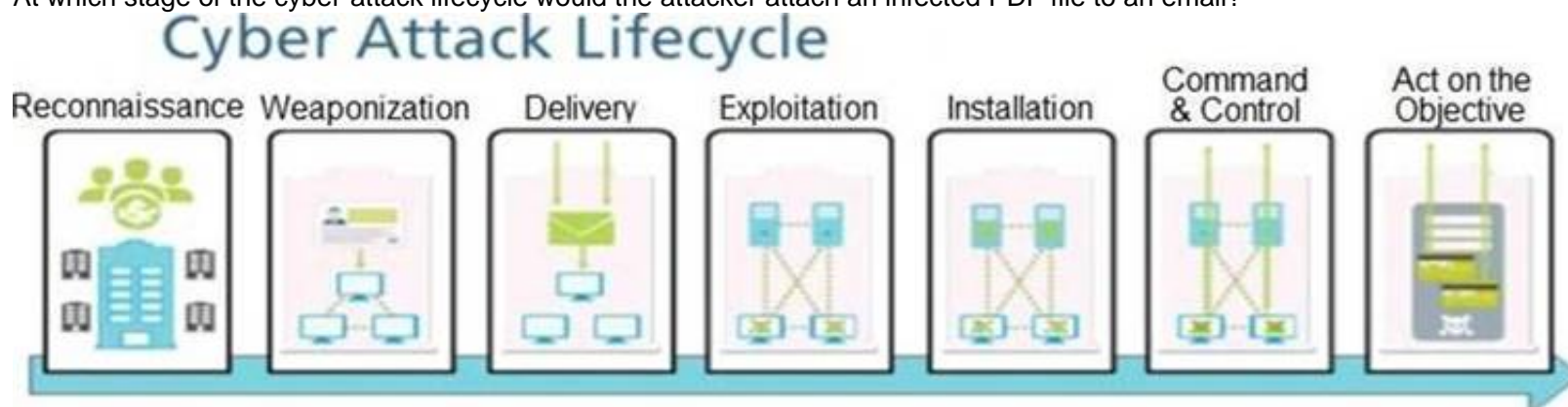
Explanation:

Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures

within a minute of availability.

NEW QUESTION 141

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



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

Answer: A

NEW QUESTION 146

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 150

According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

- A. by minute
- B. hourly
- C. daily
- D. weekly

Answer: C

NEW QUESTION 154

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

Answer: B

NEW QUESTION 155

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

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

Answer: C

NEW QUESTION 157

The PowerBall Lottery has reached a high payout amount and a company has decided to help employee morale by allowing employees to check the number, but doesn't want to unblock the gambling URL category.

Which two methods will allow the employees to get to the PowerBall Lottery site without the company unlocking the gambling URL category? (Choose two.)

- A. Add all the URLs from the gambling category except powerball.com to the block list and then set the action for the gambling category to allow.

- B. Manually remove powerball.com from the gambling URL category.
- C. Add *.powerball.com to the allow list
- D. Create a custom URL category called PowerBall and add *.powerball.com to the category and set the action to allow.

Answer: CD

NEW QUESTION 158

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-profi>

NEW QUESTION 161

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 165

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

NEW QUESTION 170

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

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

Answer: BCE

NEW QUESTION 174

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

NEW QUESTION 176

What are three factors that can be used in domain generation algorithms? (Choose three.)

- A. cryptographic keys
- B. time of day
- C. other unique values
- D. URL custom categories
- E. IP address

Answer: ABC

Explanation:

Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a

large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-a>

NEW QUESTION 178

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 183

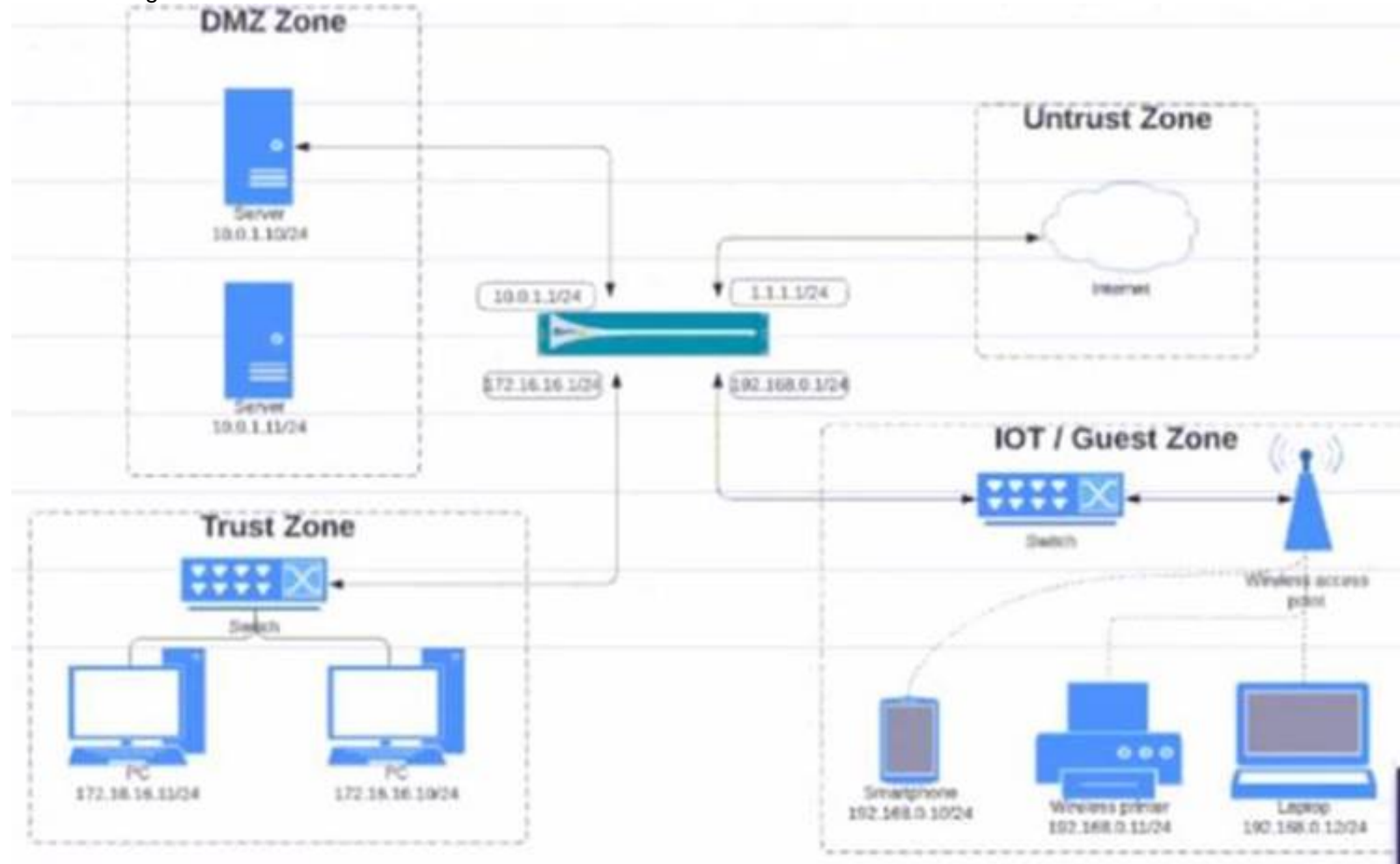
A network administrator created an intrazone Security policy rule on the firewall. The source zones were set to IT. Finance, and HR. Which two types of traffic will the rule apply to? (Choose two)

- A. traffic between zone IT and zone Finance
- B. traffic between zone Finance and zone HR
- C. traffic within zone IT
- D. traffic within zone HR

Answer: CD

NEW QUESTION 184

View the diagram.



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

A)

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

B)

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/
			Trust	192.168.0.0/24			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 A
- B. Option B
- C. Option C
- D. Option D

Answer: C

NEW QUESTION 188

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 sameURL then which choice would be the last to block access to the URL?

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

Answer: D

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 Cached: URLs learned from External Dynamic Lists (EDLs) - 5) Pre-Defined Categories: PAN-DB or Brightcloud categories.

NEW QUESTION 191

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

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

Answer: B

NEW QUESTION 194

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

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

Answer: B

NEW QUESTION 199

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

Answer Area

First	Drag answer here	PAN-DB Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	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 200

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

NEW QUESTION 201

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

TYPE	FROM ZONE	TO ZONE	INGRESS IF	SOURCE	NAT APPLIED	EGRESS IF	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	5.8K	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 205

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

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

Answer: BD

NEW QUESTION 208

.....

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