Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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

NEW QUESTION 1
An administrator wants to create a No-NAT rule to exempt a flow from the default NAT rule. What is the best way to do this?

A. Create a Security policy rule to allow the traffic.
B. Create a new NAT rule with the correct parameters and leave the translation type as None
C. Create a static NAT rule with an application override.
D. Create a static NAT rule translating to the destination interface.

Answer: B

NEW QUESTION 2
Which object would an administrator create to enable access to all applications in the office-programs subcategory?

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

Answer: A

NEW QUESTION 3
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

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

Answer: C

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

NEW QUESTION 4
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 m a device group to which to push policy rules
D. You specify the location as pre can - or post-rules to push policy rules

Answer: C

NEW QUESTION 5
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 6
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-algorithm-detection

NEW QUESTION 7
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 8
Which rule type is appropriate for matching traffic both within and between the source and destination zones?

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

Answer: A

NEW QUESTION 9
Which dynamic update type includes updated anti-spyware signatures?

A. Applications and Threats
B. GlobalProtect Data File
C. Antivirus
D. PAN-DB

Answer: A

NEW QUESTION 10
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 10
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

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

Answer: A

Explanation:
To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletproof-isps#:~:text=A%20new%20built%2Din%20external,%2C%20illegal%2C%20and%20unethi cal%20content.

NEW QUESTION 13
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 16
Which solution is a viable option to capture user identification when Active Directory is not in use?

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

Answer: D

NEW QUESTION 19
An address object of type IP Wildcard Mask can be referenced in which part of the configuration?

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

Answer: A

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

NEW QUESTION 22
How is the hit count reset on a rule?

A. select a security policy rule, right click Hit Count > Reset
B. with a dataplane reboot
C. Device > Setup > Logging and Reporting Settings > Reset Hit Count
D. in the CLI, type command reset hitcount <POLICY-NAME>

Answer: A

NEW QUESTION 24
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 27
Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 30
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

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

Answer: D

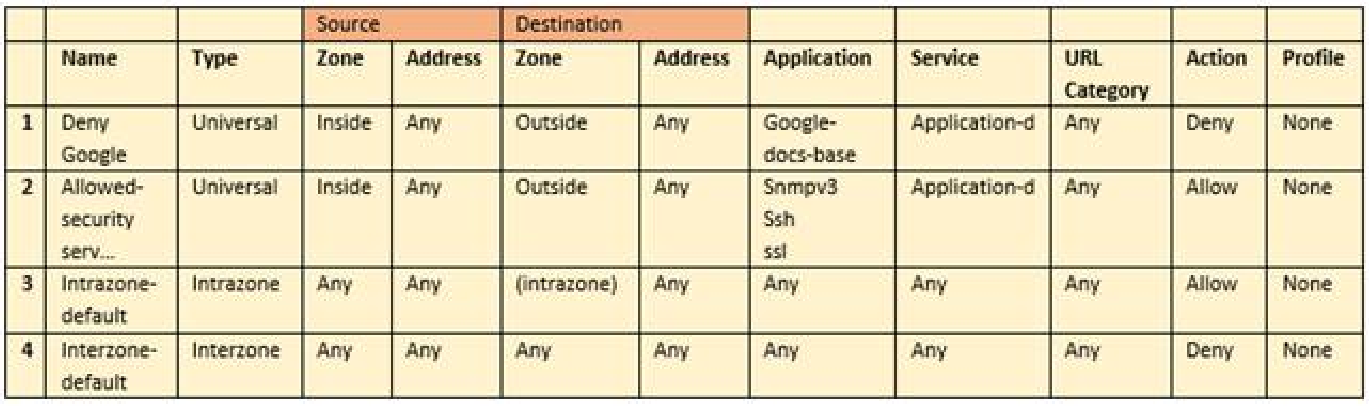
NEW QUESTION 34
Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

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 malvertizing.
? 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 39
Based on the security policy rules shown, ssh will be allowed on which port?



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

Answer: C

NEW QUESTION 43
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 48
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

Explanation:

Reference:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0ClQSCA0

NEW QUESTION 52
Which three types of authentication services can be used to authenticate user traffic flowing through the firewalls data plane? (Choose three)

A. TACACS
B. SAML2
C. SAML10
D. Kerberos
E. TACACS+

Answer: ABD

NEW QUESTION 54
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

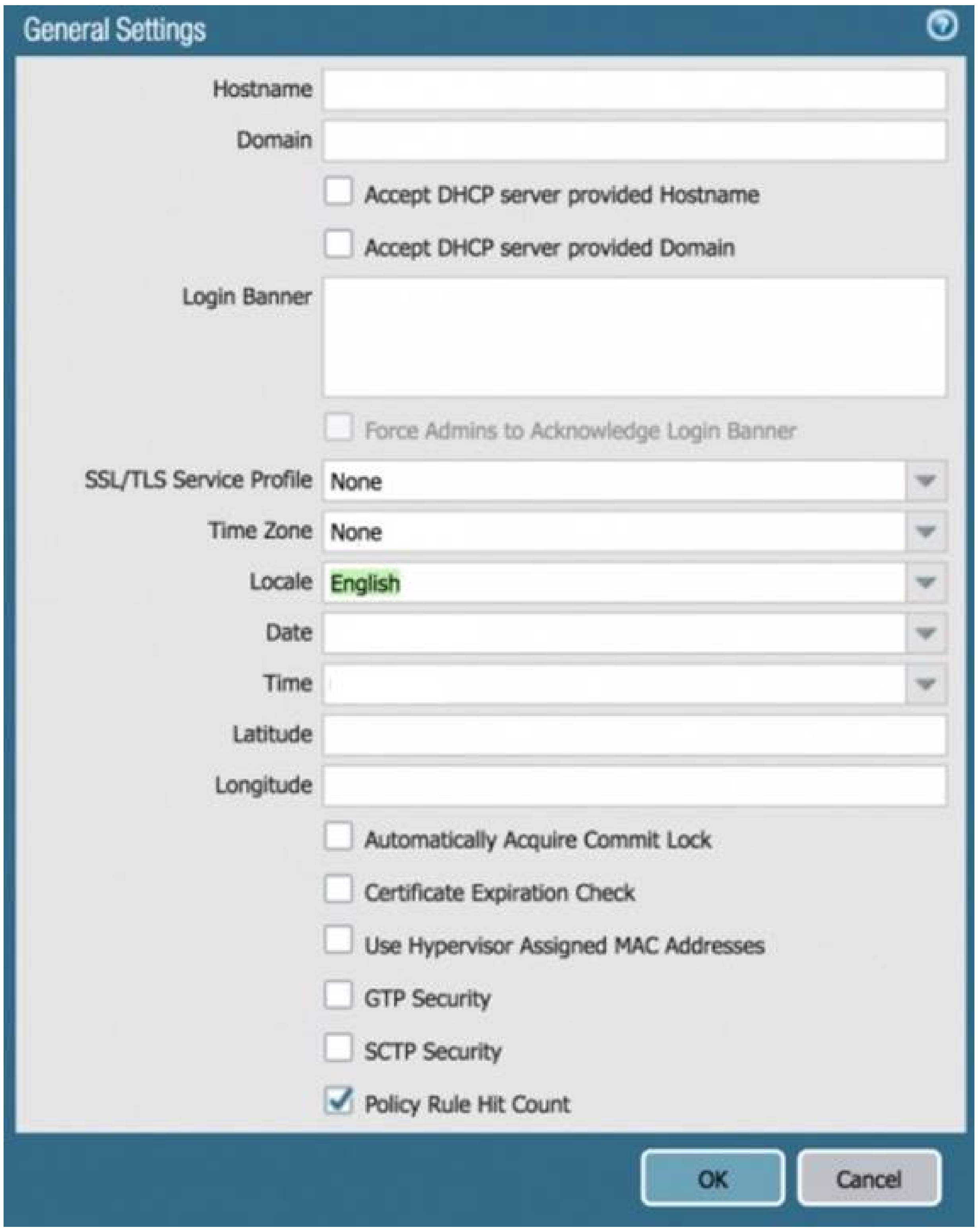
NEW QUESTION 59
Which profile should be used to obtain a verdict regarding analyzed files?

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

Answer: A

Explanation:
? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic1.
? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis1.
? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination2. WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware3. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats34.
? The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational5.
? Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.
? Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.
Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.
References:
1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto
Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks
: [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION 60
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration
option?



General Settings

Hostname

Domain

□ Accept DHCP server provided Hostname

□ Accept DHCP server provided Domain

Login Banner

□ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: None

Locale: English

Date

Time

Latitude

Longitude

□ Automatically Acquire Commit Lock

□ Certificate Expiration Check

□ Use Hypervisor Assigned MAC Addresses

□ GTP Security

□ SCTP Security

☑ Policy Rule Hit Count

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

Answer: C

Explanation:
Reference:https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000 0ClFGCA0

NEW QUESTION 63

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 65
The CFO found a malware infected USB drive in the parking lot, which when inserted infected their corporate laptop the malware contacted a known command-and-control server which exfiltrating corporate data.
Which Security profile feature could have been used to prevent the communications with the command-and-control server?

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

Answer: C

NEW QUESTION 67

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

A. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 69
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 72
What must be configured before setting up Credential Phishing Prevention?

A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat- prevention/prevent-credential-phishing/set-up-credential-phishing-prevention

NEW QUESTION 75
Which interface type can use virtual routers and routing protocols?

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

Answer: B

NEW QUESTION 79
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 84
Which path in PAN-OS 10.0 displays the list of port-based security policy rules?

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

Answer: A

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

NEW QUESTION 85
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 86
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 91
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 94
By default, what is the maximum number of templates that can be added to a template stack?

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

Answer: B

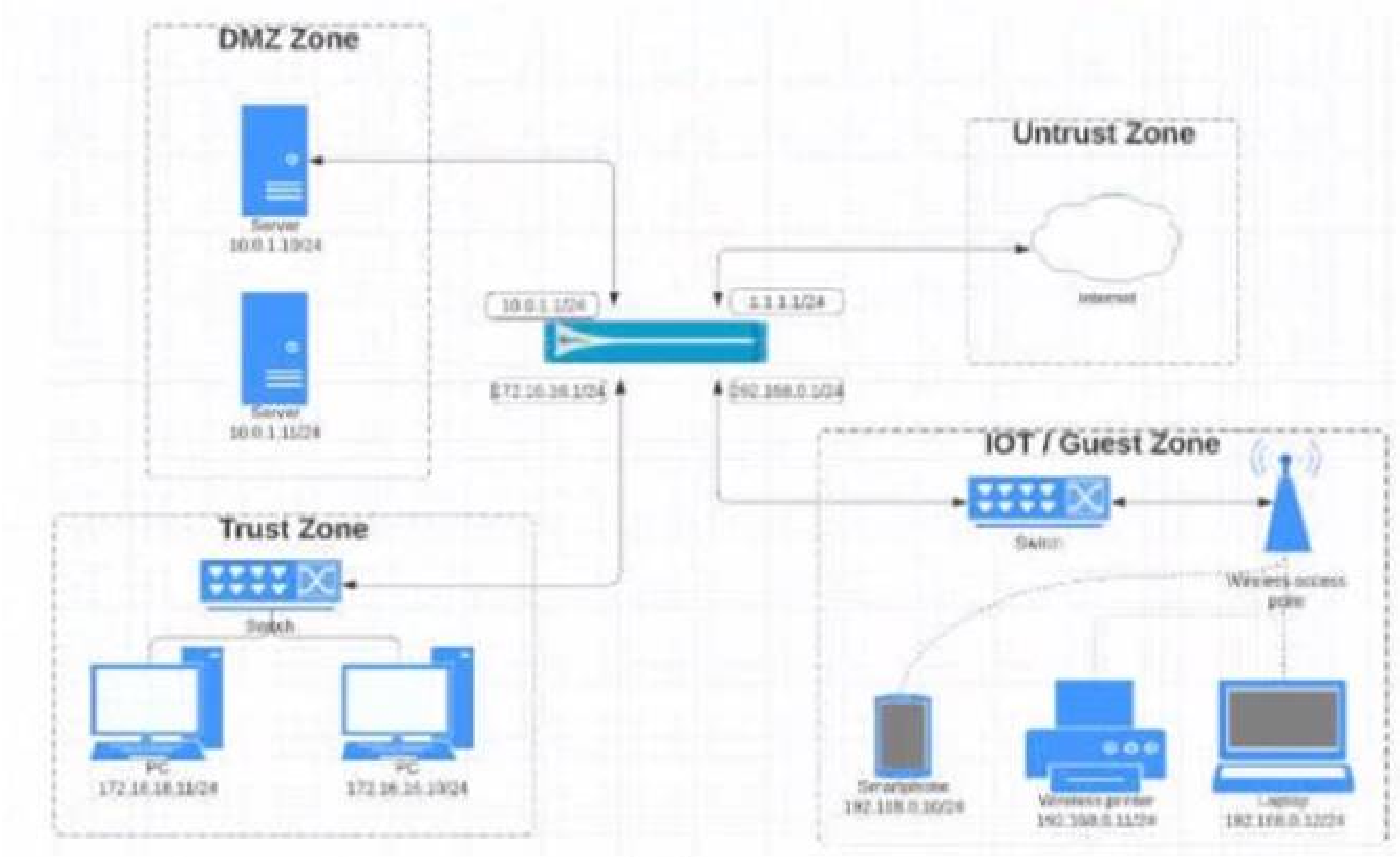
Explanation:
By default, the maximum number of templates that can be added to a template stack is 8. This is the recommended limit for performance reasons, as adding more templates may result in sluggish responses on the user interface. However, starting from PAN-OS 8.1.10 and 9.0.4, you can use a debug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

NEW QUESTION 99
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

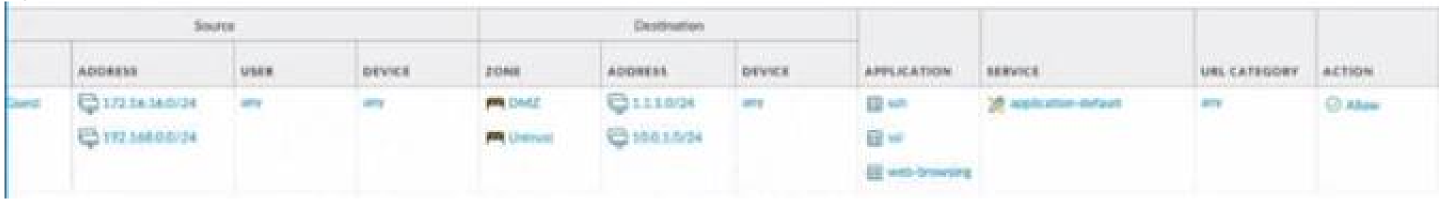
Answer: D

NEW QUESTION 104
View the diagram.



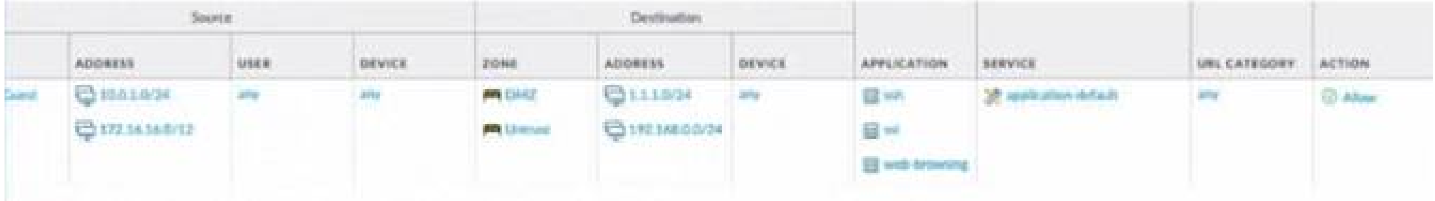
What is the most restrictive yet fully functional rule to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A)



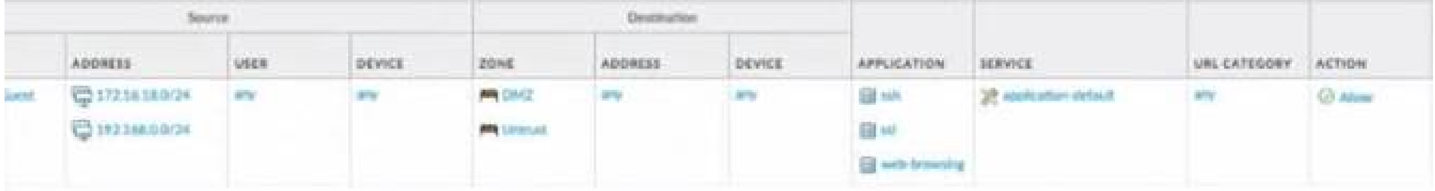
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default	any	Allow

B)



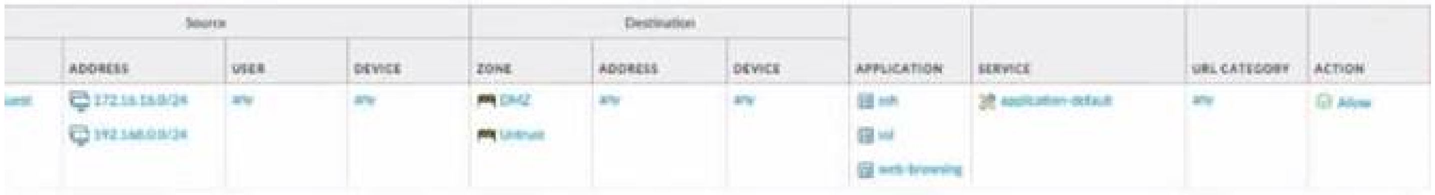
Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
Guest	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default	any	Allow

C)



Source				Destination						
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION
uest	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

D)



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

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

Option D

D.

Answer: C

NEW QUESTION 108

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) server1.

? An Anti-Spyware security profile consists of four tabs: Signature Policies, Signature Exceptions, Machine Learning Policies, and Inline Cloud Analysis1.

? 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 responses1.

? 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 profile1.
? 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 analysis1.
? 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/SMTPS traffic, or IMAP/IMAPS traffic1.
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

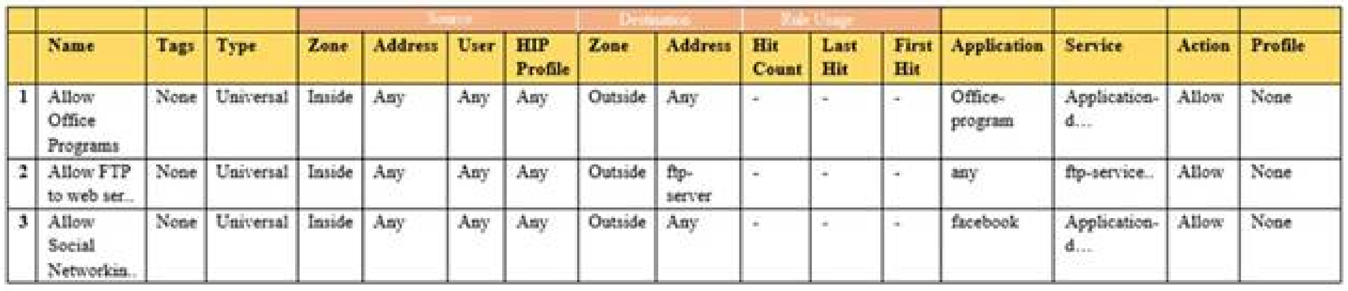
NEW QUESTION 110
In which section of the PAN-OS GUI does an administrator configure URL Filtering profiles?

A. Policies
B. Network
C. Objects
D. Device

Answer: C

Explanation:
An administrator can configure URL Filtering profiles in the Objects section of the PAN-OS GUI. A URL Filtering profile is a collection of URL filtering controls that you can apply to individual Security policy rules that allow access to the internet1. You can set site access for URL categories, allow or disallow user credential submissions, enable safe search enforcement, and various other settings1.
To create a URL Filtering profile, go to Objects > Security Profiles > URL Filtering and click Add. You can then specify the profile name, description, and settings for each URL category and action2. Youcan also configure other options such as User Credential Detection, HTTP Header Insertion, and URL Filtering Inline ML2. After creating the profile, you can attach it to a Security policy rule that allows web traffic2.

NEW QUESTION 115
Given the image, which two options are true about the Security policy rules. (Choose two.)



				Source				Destination		Rule 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 119
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 123
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 125
An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

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

Answer: BD

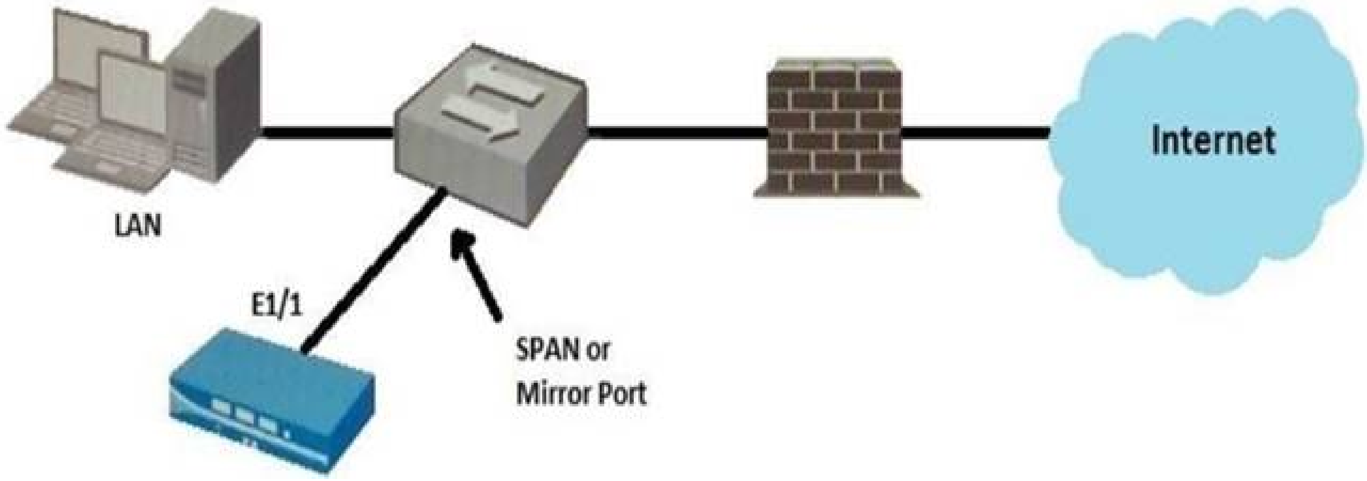
NEW QUESTION 128
According to the best practices for mission critical devices, what is the recommended interval for antivirus updates?

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

Answer: C

Explanation:
Reference:https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-mission- critical.html

NEW QUESTION 130
Given the topology, which zone type should you configure for firewall interface E1/1?



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

Answer: A

NEW QUESTION 135
An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.
Which Security profile should be used?

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

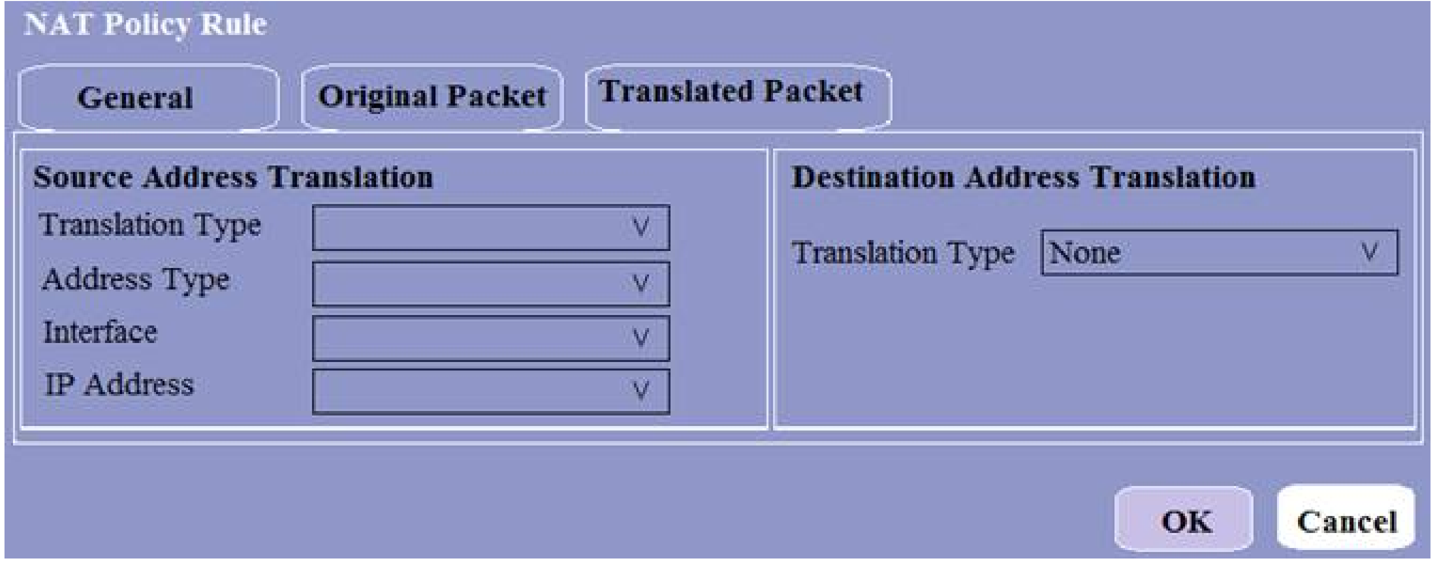
Answer: C

NEW QUESTION 136
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 139
When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?



NAT Policy Rule

General | Original Packet | Translated Packet

Source Address Translation

Translation Type
Address Type
Interface
IP Address

Destination Address Translation

Translation Type: None

OK | Cancel

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

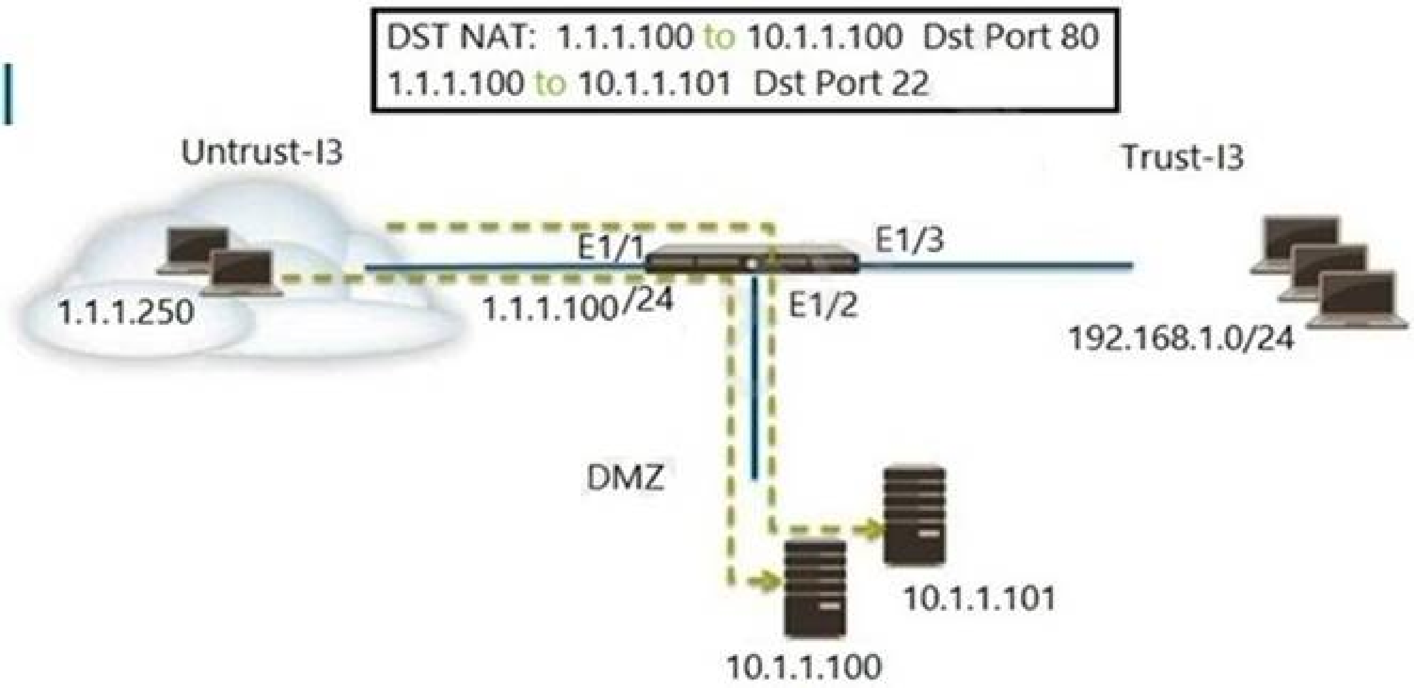
Answer: A

NEW QUESTION 140
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 141
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

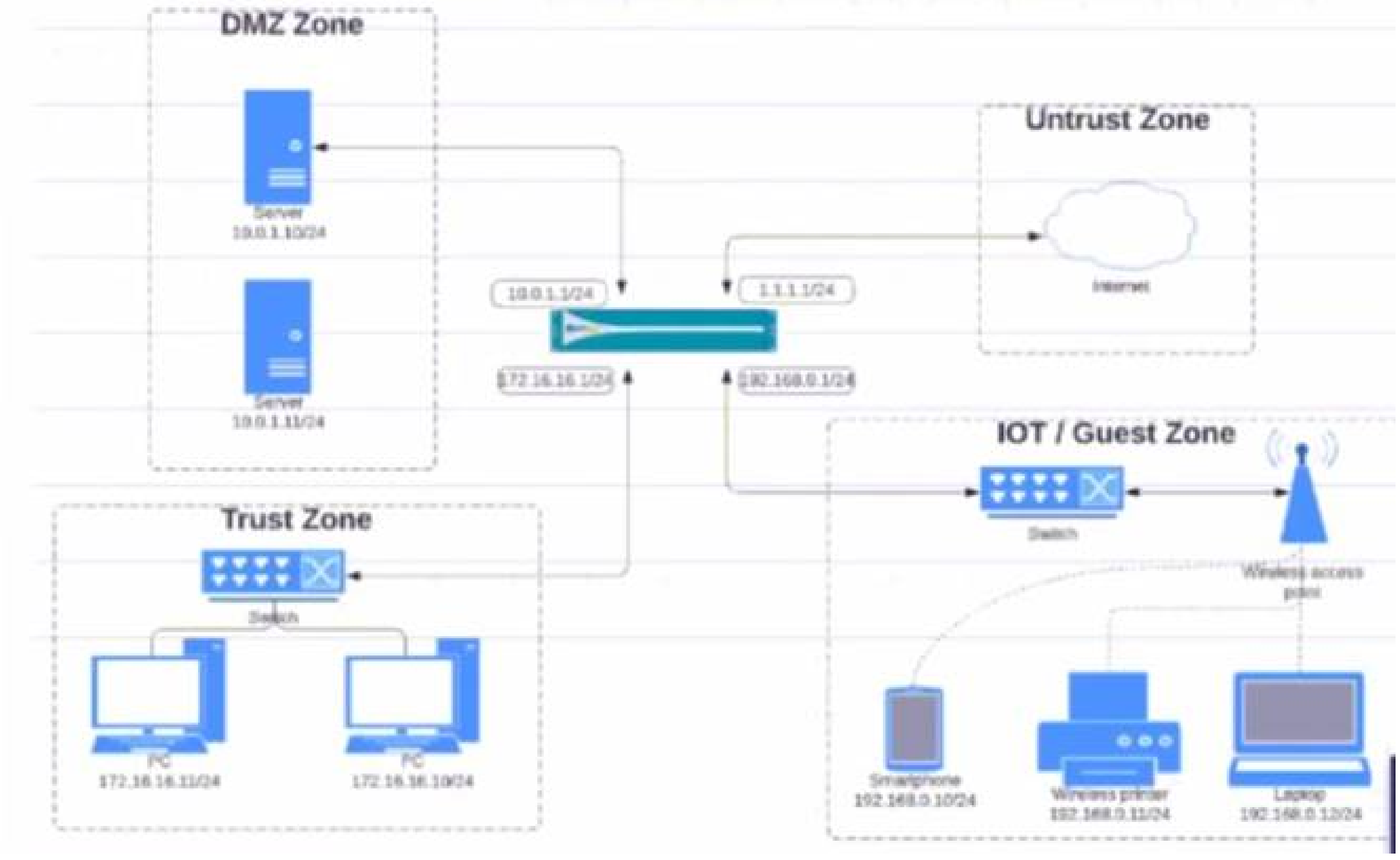
Answer: AE

NEW QUESTION 143
Why should a company have a File Blocking profile that is attached to a Security policy?

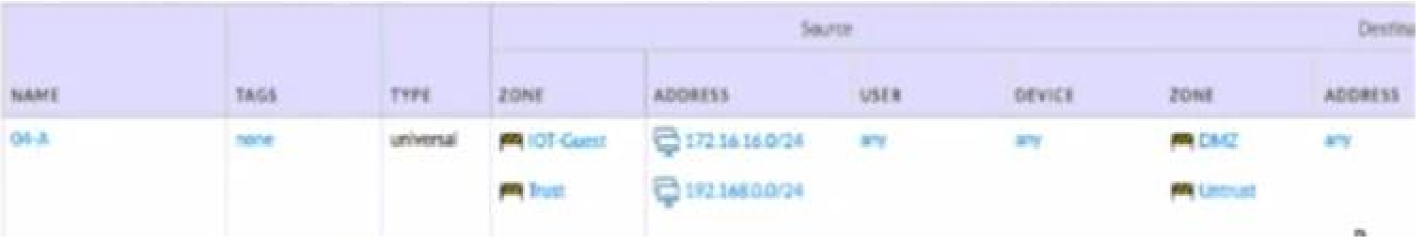
A. To block uploading and downloading of specific types of files
B. To detonate files in a sandbox environment
C. To analyze file types
D. To block uploading and downloading of any type of files

Answer: A

NEW QUESTION 145
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

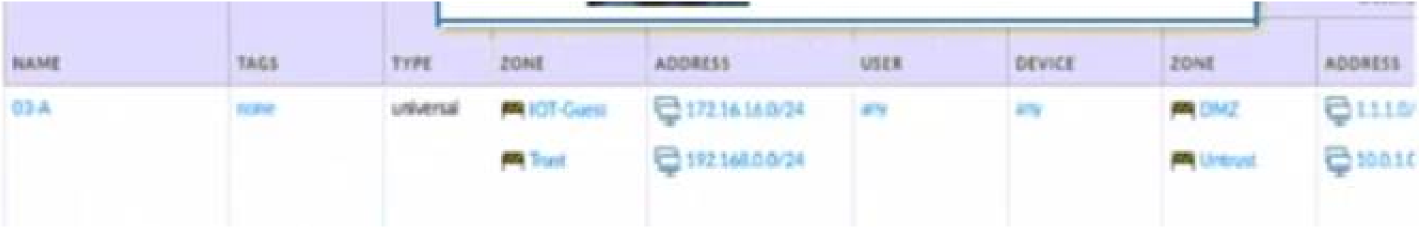


Which policy achieves the desired results?
A)



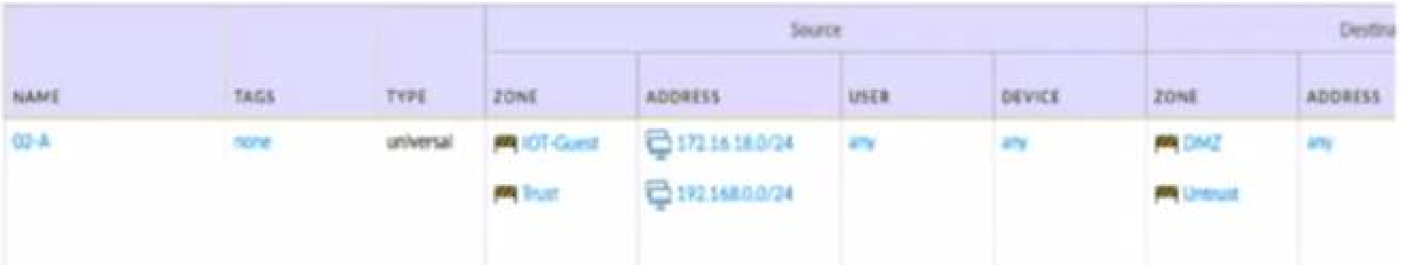
			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any

B)



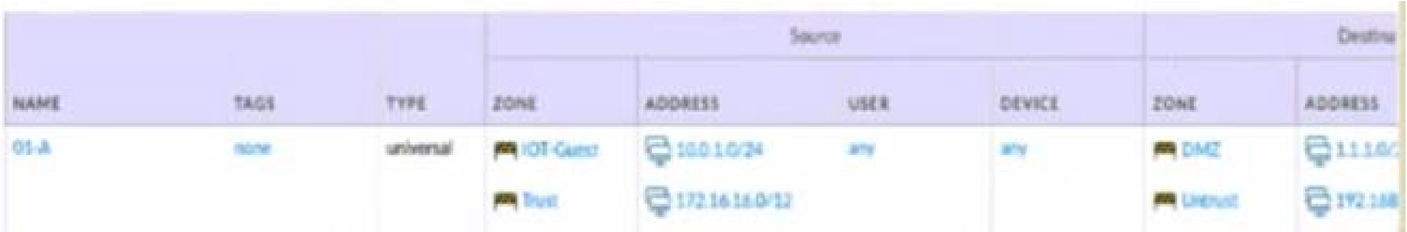
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/ 10.0.1.0

C)



			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any

D)



			Source				Destina	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/ 192.168

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

Answer: C

NEW QUESTION 147
How often does WildFire release dynamic updates?

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

Answer: A

NEW QUESTION 151
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.co
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 polic
F. Set the policy action to Deny.

Answer: CD

NEW QUESTION 156
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 158
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

Explanation:

NEW QUESTION 161
Which type firewall configuration contains in-progress configuration changes?

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

Answer: C

NEW QUESTION 162
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. Mastered
B. Not Mastered

Answer: A

NEW QUESTION 165
What must be considered with regards to content updates deployed from Panorama?

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

Answer: D

Explanation:

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

NEW QUESTION 167
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 171
Which statement is true regarding a Prevention Posture Assessment?

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

Answer: B

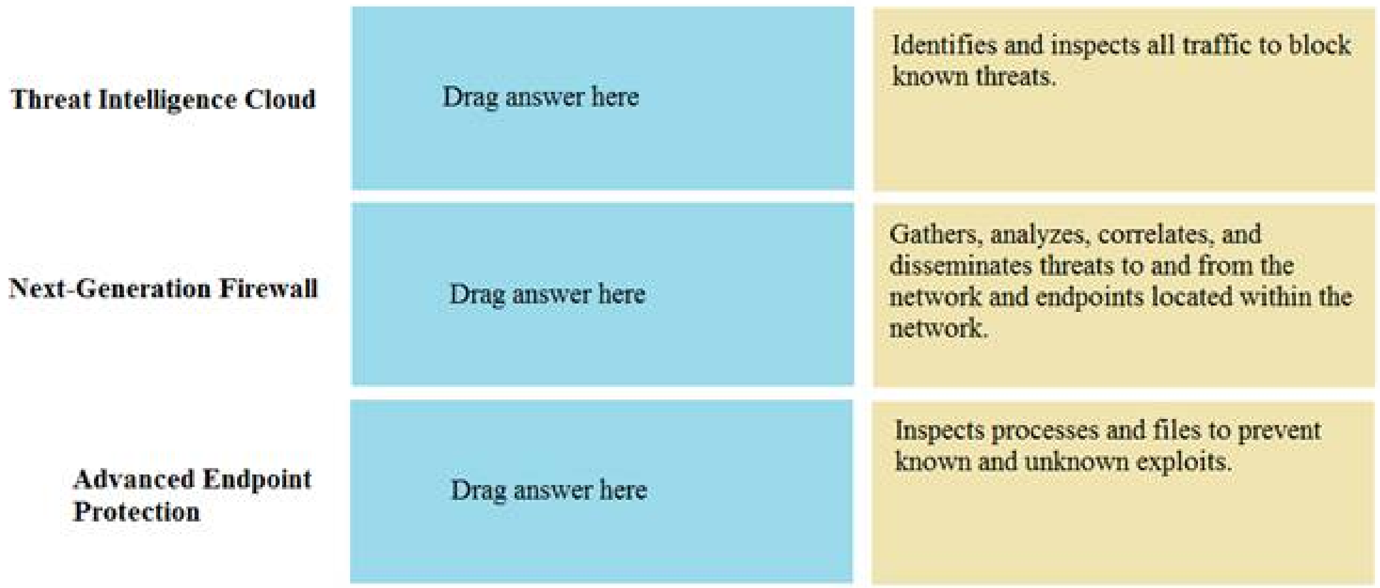
NEW QUESTION 175
Which three filter columns are available when setting up an Application Filter? (Choose three.)

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 178
DRAG DROP
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 182
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.

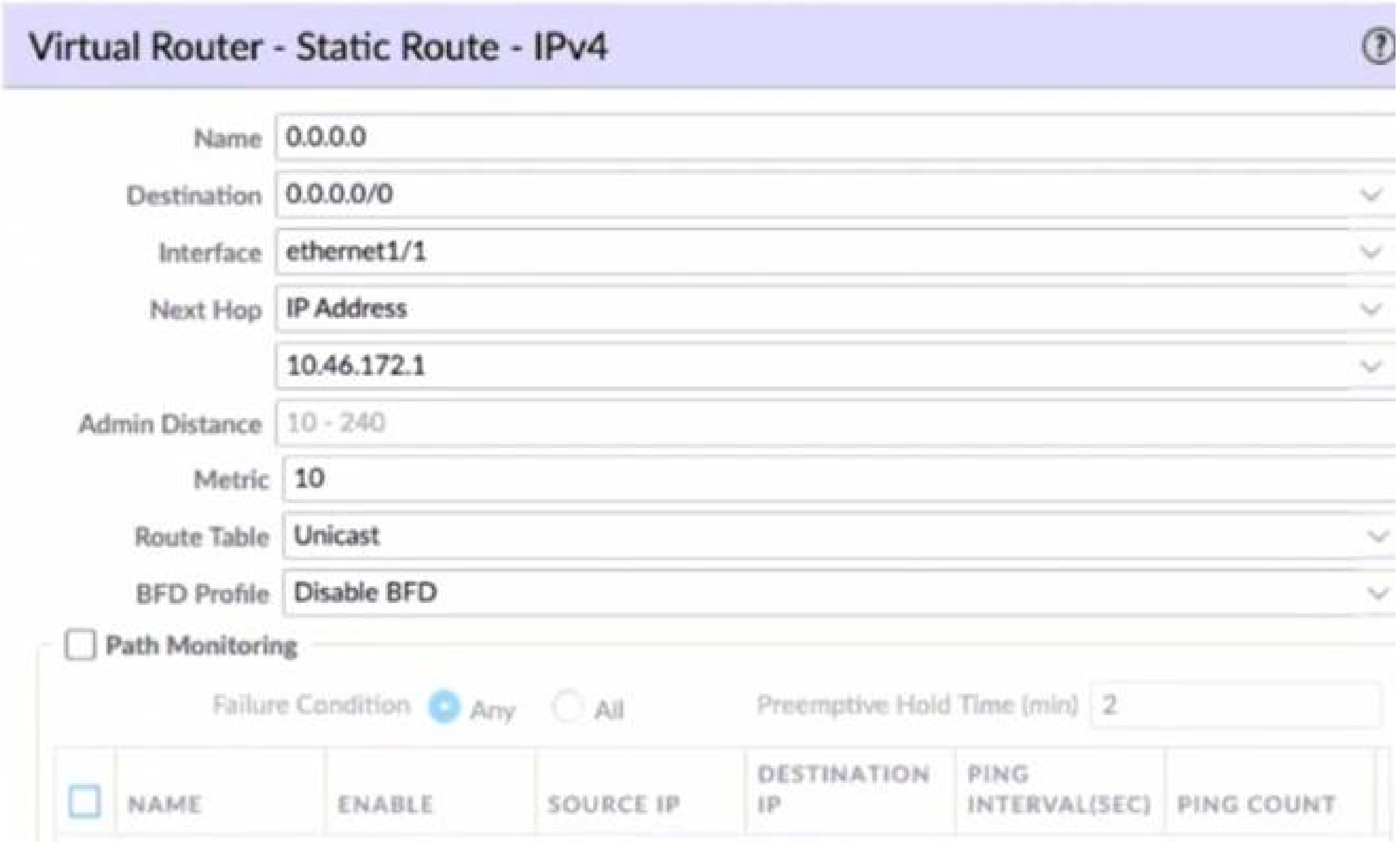
Answer: AB

NEW QUESTION 183
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 188
Given the screenshot what two types of route is the administrator configuring? (Choose two)


Virtual Router - Static Route - IPv4

Name	0.0.0.0
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address
	10.46.172.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

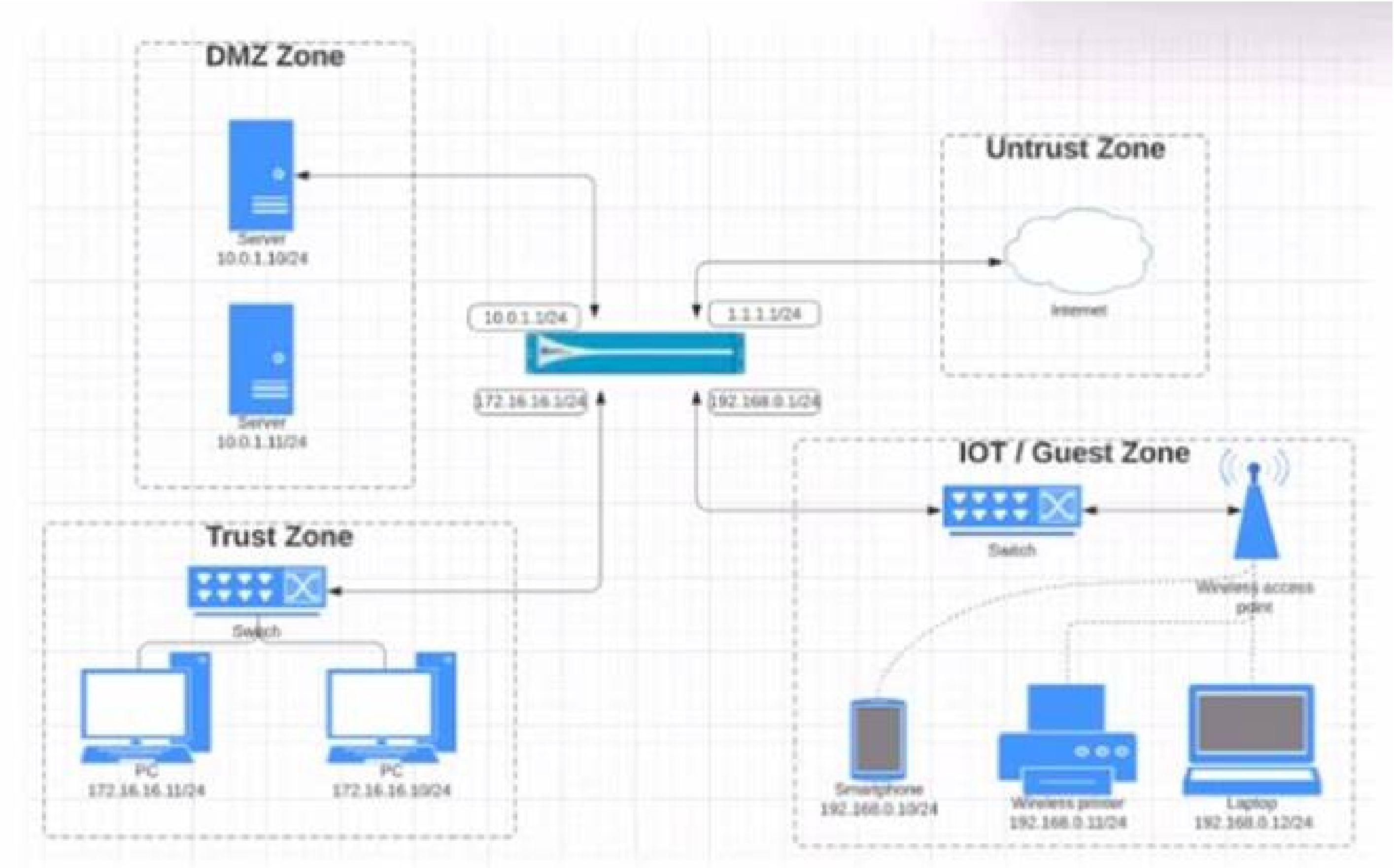
Failure Condition ● Any ○ All Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

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

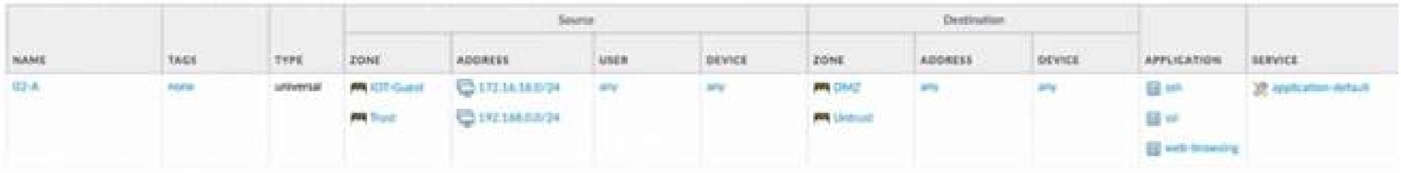
Answer: A

NEW QUESTION 191
View the diagram.



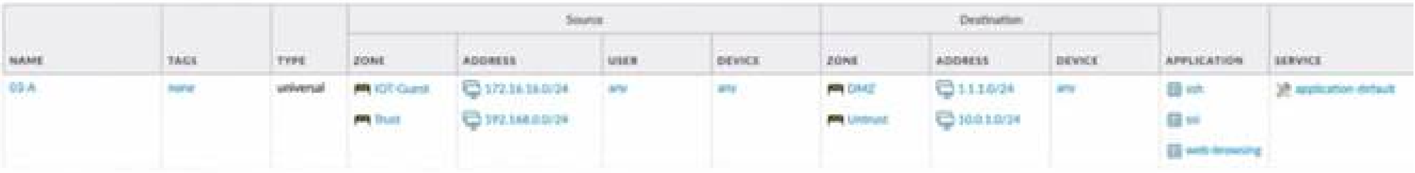
What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/lnternet zones from each of the lOT/Guest and Trust Zones?

A)



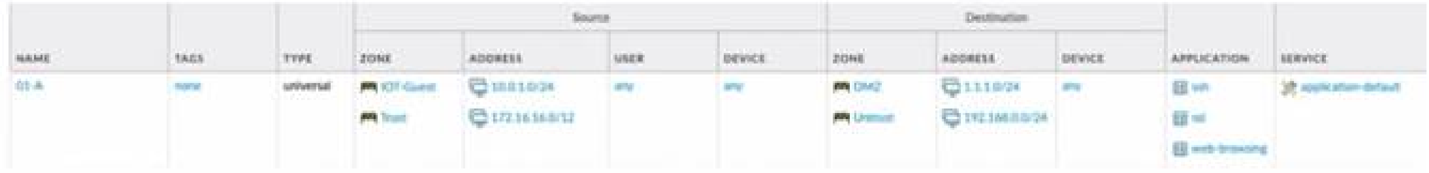
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

B)



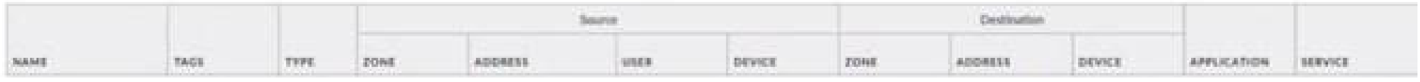
			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	application-default

C)



			Source				Destination				
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default

D)



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

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

Answer: C

NEW QUESTION 196

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 198
What can be used as match criteria for creating a dynamic address group?

A. Usernames
B. IP addresses

C. Tags
D. MAC addresses

Answer: C

NEW QUESTION 201
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 202
An administrator is reviewing another administrator s Security policy log settings Which log setting configuration is consistent with best practices tor 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 205
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 210
......