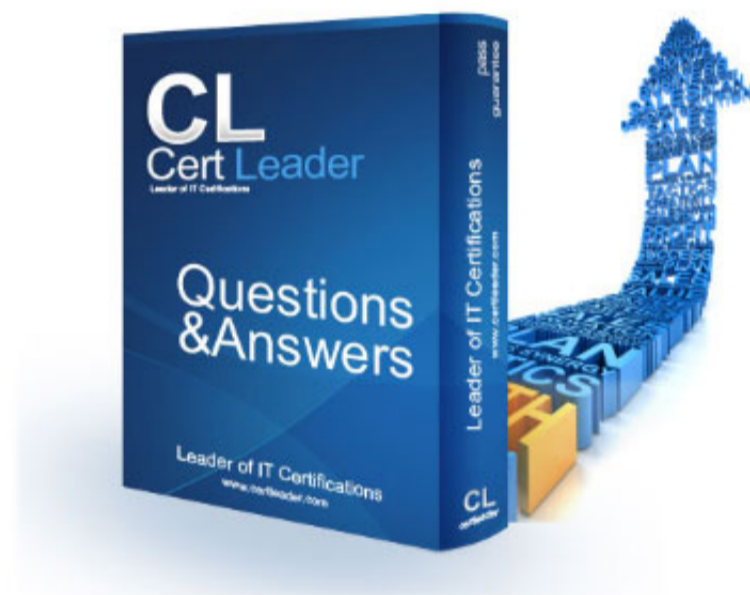


PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

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



NEW QUESTION 1

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 2

Which administrative management services can be configured to access a management interface?

- A. HTTP, CLI, SNMP, HTTPS
- B. HTTPS, SSH telnet SNMP
- C. SSH: telnet HTTP, HTTPS
- D. HTTPS, HTTP
- E. CLI, API

Answer: D

Explanation:

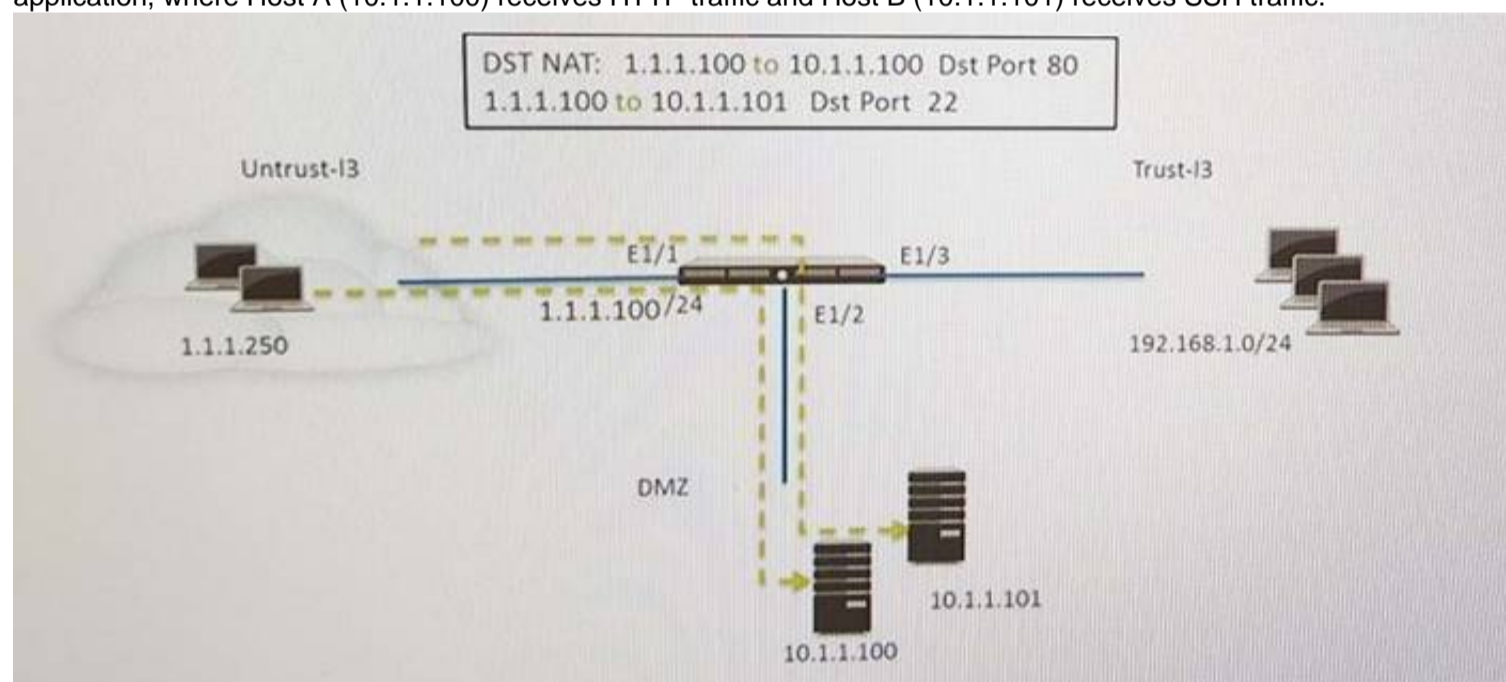
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces> You can use the following user interfaces to manage the Palo Alto Networks firewall:

- Use the Web Interface to perform configuration and monitoring tasks with relative ease. This graphical interface allows you to access the firewall using HTTPS (recommended) or HTTP and it is the best way to perform administrative tasks.
- Use the Command Line Interface (CLI) to perform a series of tasks by entering commands in rapid succession over SSH (recommended), Telnet, or the console port. The CLI is a no-frills interface that supports two command modes, operational and configure, each with a distinct hierarchy of commands and statements. When you become familiar with the nesting structure and syntax of the commands, the CLI provides quick response times and administrative efficiency.
- Use the XML API to streamline your operations and integrate with existing, internally developed applications and repositories. The XML API is a web service implemented using HTTP/HTTPS requests and responses.
- Use Panorama to perform web-based management, reporting, and log collection for multiple firewalls.

The Panorama web interface resembles the firewall web interface but with additional functions for centralized management.

NEW QUESTION 3

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 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

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 6

Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

- A. Root
- B. Dynamic
- C. Role-based
- D. Superuser

Answer: C

NEW QUESTION 7

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

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

Answer: AB

NEW QUESTION 8

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

NEW QUESTION 9

Complete the statement. A security profile can block or allow traffic

- A. on unknown-tcp or unknown-udp traffic
- B. after it is matched by a security policy that allows traffic
- C. before it is matched by a security policy
- D. after it is matched by a security policy that allows or blocks traffic

Answer: B

Explanation:

Security profiles are objects added to policy rules that are configured with an action of allow.

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 10

Which security profile will provide the best protection against ICMP floods, based on individual combinations of a packet's source and destination IP address?

- A. DoS protection
- B. URL filtering
- C. packet buffering
- D. anti-spyware

Answer: A

NEW QUESTION 12

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 16

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 17

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 22

Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

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

Answer: BD

NEW QUESTION 26

Why does a company need an Antivirus profile?

- A. To prevent command-and-control traffic
- B. To protect against viruses, worms, and trojans
- C. To prevent known exploits
- D. To prevent access to malicious web content

Answer: B

NEW QUESTION 31

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

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

Answer: AD

NEW QUESTION 32

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

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

Answer: A

NEW QUESTION 37

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



- A. The User-ID agent is connected to a domain controller labeled lab-client.
- B. The host lab-client has been found by the User-ID agent.
- C. The host lab-client has been found by a domain controller.
- D. The User-ID agent is connected to the firewall labeled lab-client.

Answer: A

NEW QUESTION 42

Which license must an administrator acquire prior to downloading Antivirus updates for use with the firewall?

- A. URL filtering
- B. Antivirus
- C. WildFire
- D. Threat Prevention

Answer: D

NEW QUESTION 46

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

- A. XML API
- B. log forwarding auto-tagging
- C. GlobalProtect agent
- D. User-ID Windows-based agent

Answer: AD

Explanation:

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

NEW QUESTION 48

Which Security profile can you apply to protect against malware such as worms and Trojans?

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

Answer: B

NEW QUESTION 53

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

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

Answer: BCE

NEW QUESTION 55

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 60

Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

- A. QoS profile
- B. DoS Protection profile
- C. Zone Protection profile
- D. DoS Protection policy

Answer: BC

NEW QUESTION 65

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 67

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 72

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 77

An internal host wants to connect to servers of the internet through using source NAT. Which policy is required to enable source NAT on the firewall?

- A. NAT policy with source zone and destination zone specified
- B. post-NAT policy with external source and any destination address
- C. NAT policy with no source of destination zone selected
- D. pre-NAT policy with external source and any destination address

Answer: A

NEW QUESTION 81

Which type of security policy rule will match traffic that flows between the Outside zone and inside zone, but would not match traffic that flows within the zones?

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

Answer: C

NEW QUESTION 85

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

NEW QUESTION 89

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

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

Answer: C

NEW QUESTION 92

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 93

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



Rule Name	Action	Source	Destination	Service	Log	Comment
1. Allow HTTP	Allow	any	any	HTTP	Yes	
2. Allow HTTPS	Allow	any	any	HTTPS	Yes	
3. Allow SSH	Allow	any	any	SSH	Yes	
4. Allow Telnet	Allow	any	any	Telnet	Yes	
5. Allow FTP	Allow	any	any	FTP	Yes	
6. Allow SMTP	Allow	any	any	SMTP	Yes	
7. Allow POP3	Allow	any	any	POP3	Yes	
8. Allow IMAP	Allow	any	any	IMAP	Yes	
9. Allow DNS	Allow	any	any	DNS	Yes	
10. Allow NTP	Allow	any	any	NTP	Yes	
11. Allow SNMP	Allow	any	any	SNMP	Yes	
12. Allow RDP	Allow	any	any	RDP	Yes	
13. Allow VNC	Allow	any	any	VNC	Yes	
14. Allow SMB	Allow	any	any	SMB	Yes	
15. Allow NFS	Allow	any	any	NFS	Yes	
16. Allow CIFS	Allow	any	any	CIFS	Yes	
17. Allow LDAP	Allow	any	any	LDAP	Yes	
18. Allow Kerberos	Allow	any	any	Kerberos	Yes	
19. Allow SFTP	Allow	any	any	SFTP	Yes	
20. Allow SCP	Allow	any	any	SCP	Yes	
21. Allow Ssh	Allow	any	any	Ssh	Yes	
22. Allow Ssh	Allow	any	any	Ssh	Yes	
23. Allow Ssh	Allow	any	any	Ssh	Yes	
24. Allow Ssh	Allow	any	any	Ssh	Yes	
25. Allow Ssh	Allow	any	any	Ssh	Yes	
26. Allow Ssh	Allow	any	any	Ssh	Yes	
27. Allow Ssh	Allow	any	any	Ssh	Yes	
28. Allow Ssh	Allow	any	any	Ssh	Yes	
29. Allow Ssh	Allow	any	any	Ssh	Yes	
30. Allow Ssh	Allow	any	any	Ssh	Yes	

- 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

NEW QUESTION 96

Which statement is true regarding a Best Practice Assessment?

- A. The BPA tool can be run only on firewalls
- B. 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 99

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

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

Answer: D

NEW QUESTION 103

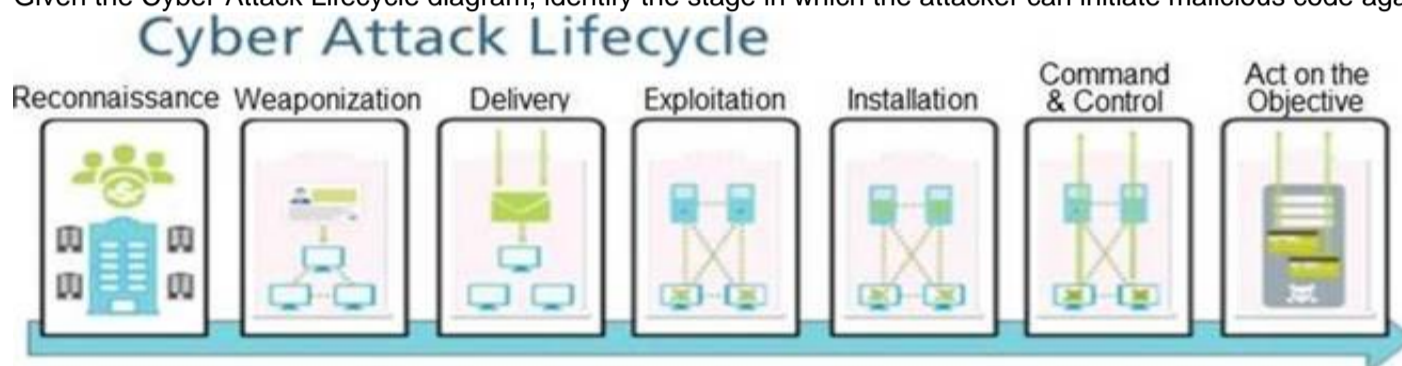
Why should a company have a File Blocking profile that is attached to a Security policy?

- 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 107

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 108

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 113

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 117

Which Security policy action will message a user's browser that their web session has been terminated?

- A. Reset server

- B. Deny
- C. Drop
- D. Reset client

Answer: B

NEW QUESTION 122

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

- A. password profile
- B. access domain
- C. admin role
- D. server profile

Answer: CD

NEW QUESTION 125

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-po>

NEW QUESTION 130

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 132

When HTTPS for management and GlobalProtect are enabled on the same interface, which TCP port is used for management access?

- A. 80
- B. 8443
- C. 4443
- D. 443

Answer: C

NEW QUESTION 137

Which statement is true regarding NAT rules?

- A. Static NAT rules have precedence over other forms of NAT.
- B. Translation of the IP address and port occurs before security processing.
- C. NAT rules are processed in order from top to bottom.
- D. Firewall supports NAT on Layer 3 interfaces only.

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overvie>

NEW QUESTION 138

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 141

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 143

Match each rule type with its example

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.

Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.

Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B and from zone B to zone A, but not traffic within zones A or B.

Answer Area

Universal

Intrazone

Interzone

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	
Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.	
Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B from zone B to zone A, but not traffic within zones A or B.	

Answer Area	
Create a policy with source zones A and B and destination zone A and B. The rule would apply to traffic from zone A to zone B from zone B to zone A, but not traffic within zones A or B.	Universal
Create a policy with source zones A and B. The rule will apply all traffic within zone A and all traffic within zone B, but not to traffic between zones A and B.	Intrazone
Create a policy with source zones A and B and destination zone A and B. The rule should apply to all traffic within zone A, all traffic within zone B, all traffic from zone A to zone B, and all traffic from zone B to zone A.	Interzone

NEW QUESTION 144

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

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

Answer: A

NEW QUESTION 147

Which statement is true about Panorama managed devices?

- A. Panorama automatically removes local configuration locks after a commit from Panorama
- B. Local configuration locks prohibit Security policy changes for a Panorama managed device
- C. Security policy rules configured on local firewalls always take precedence
- D. Local configuration locks can be manually unlocked from Panorama

Answer: D

NEW QUESTION 148

Which two matching criteria are used when creating a Security policy involving NAT? (Choose two.)

- A. Post-NAT address
- B. Post-NAT zone
- C. Pre-NAT zone
- D. Pre-NAT address

Answer: BD

NEW QUESTION 150

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

NEW QUESTION 155

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 159

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 161

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 164

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 166

In a File Blocking profile, which two actions should be taken to allow file types that support critical apps? (Choose two.)

- A. Clone and edit the Strict profile.
- B. Use URL filtering to limit categories in which users can transfer files.
- C. Set the action to Continue.
- D. Edit the Strict profile.

Answer: AD

NEW QUESTION 168

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

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

Answer: C

NEW QUESTION 172

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 177

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

- A. Application groups
- B. Service groups
- C. Address groups
- D. Custom objects

Answer: B

NEW QUESTION 179

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 181

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-in-content-releases/review-new-app-id-impact-on-existing-policy-rules>

NEW QUESTION 183

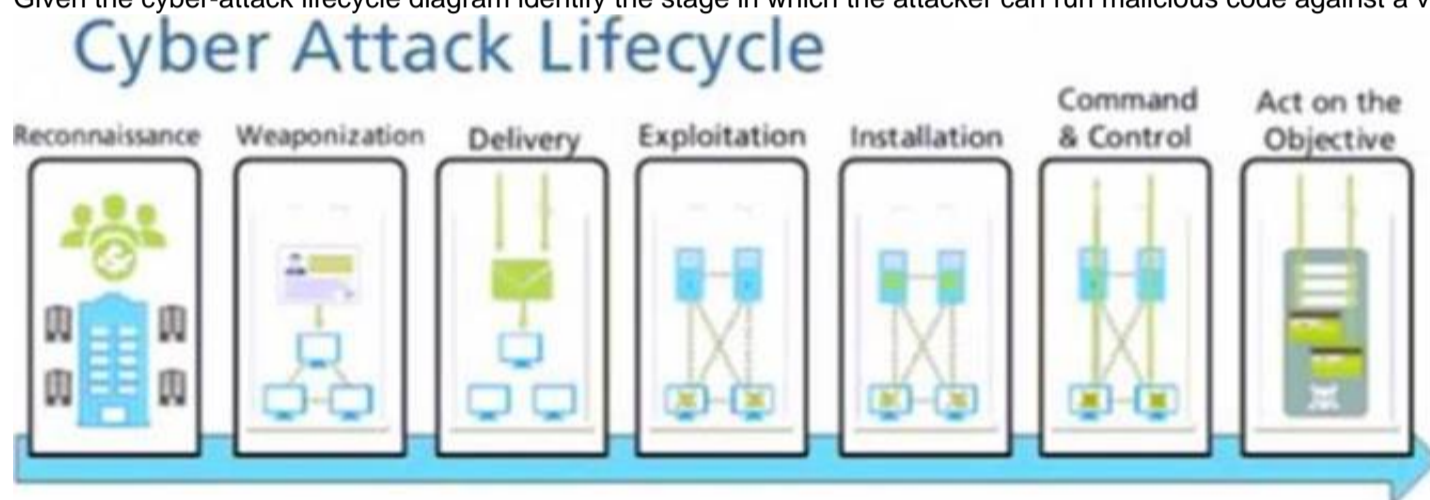
An administrator is troubleshooting an issue with traffic that matches the intrazone-default rule, which is set to default configuration. What should the administrator do?

- A. change the logging action on the rule
- B. review the System Log
- C. refresh the Traffic Log
- D. tune your Traffic Log filter to include the dates

Answer: A

NEW QUESTION 186

Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



- A. Exploitation
- B. Installation
- C. Reconnaissance
- D. Act on the Objective

Answer: A

NEW QUESTION 190

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 195

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 200

What is the purpose of the automated commit recovery feature?

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

Answer: C

NEW QUESTION 203

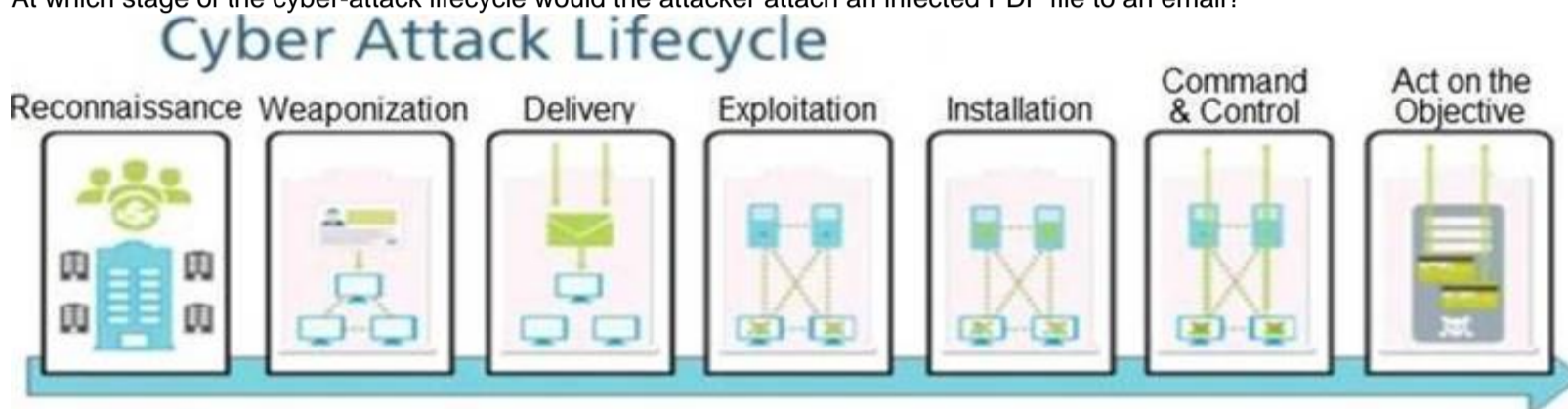
To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

- A. domain controller
- B. TACACS+
- C. LDAP
- D. RADIUS

Answer: C

NEW QUESTION 205

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



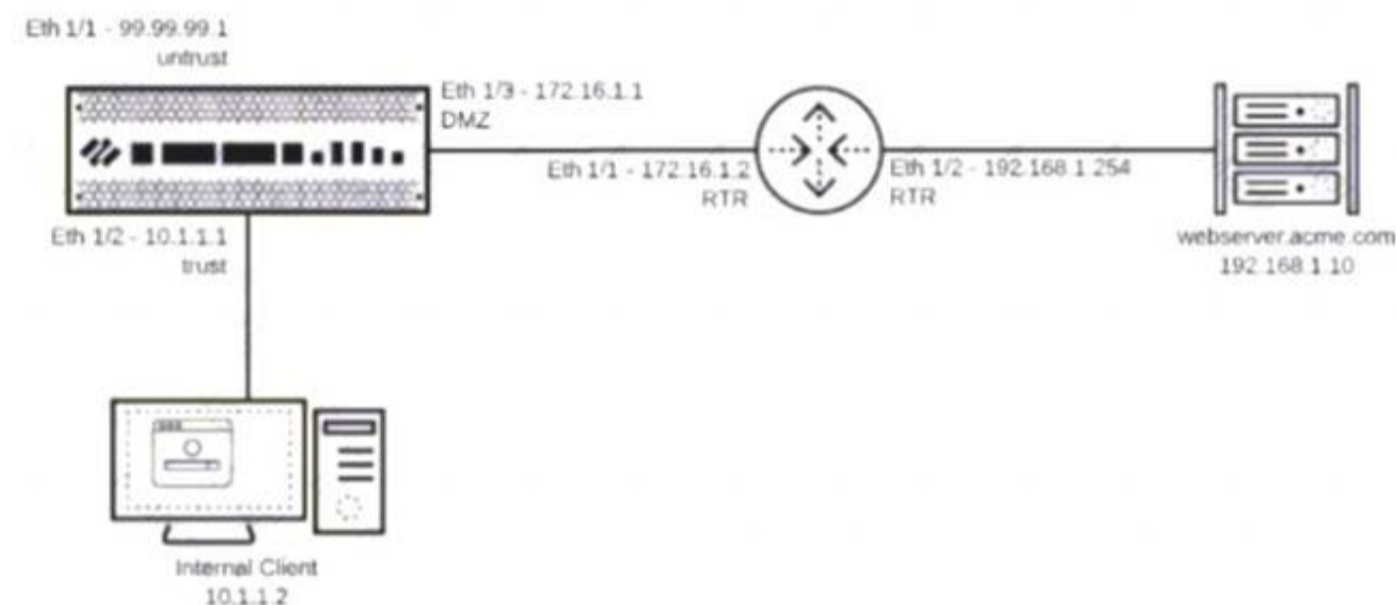
- A. delivery
- B. command and control
- C. exploitation
- D. reinsurance
- E. installation

Answer: A

NEW QUESTION 207

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 208

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 212

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

- A. enabling the Content-ID filter
- B. administrative management services
- C. restricting HTTP and telnet using App-ID
- D. permitted IP addresses

Answer: AC

NEW QUESTION 217

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

Palo Alto Networks User-ID Agent Setup

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

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

Answer: BC

NEW QUESTION 218

An administrator would like to apply a more restrictive Security profile to traffic for file sharing applications. The administrator does not want to update the Security policy or object when new applications are released.

Which object should the administrator use as a match condition in the Security policy?

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

Answer: D

NEW QUESTION 219

Which interface does not require a MAC or IP address?

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

Answer: A

NEW QUESTION 224

Access to which feature requires PAN-OS Filtering licens?

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

Answer: A

NEW QUESTION 226

An administrator needs to allow users to use only certain email applications.

How should the administrator configure the firewall to restrict users to specific email applications?

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

Answer: B

NEW QUESTION 231

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

<input type="checkbox"/>	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 232

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

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

Answer: A

Explanation:

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

NEW QUESTION 236

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 241

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

NEW QUESTION 242

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 245

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 247

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

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

Answer: C

NEW QUESTION 249

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 254

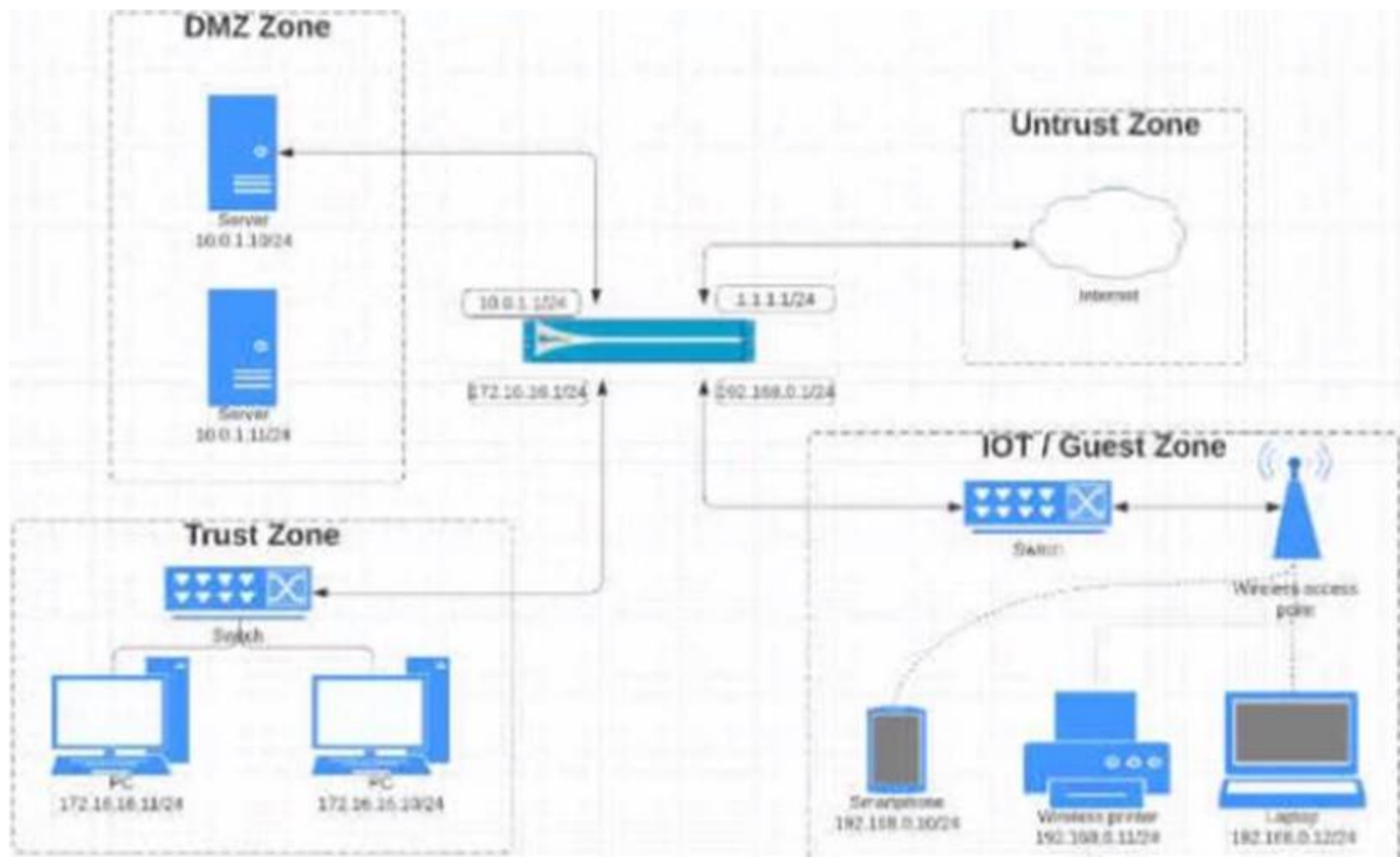
Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

- A. SAML
- B. Multi-Factor Authentication
- C. Role-based
- D. Dynamic

Answer: C

NEW QUESTION 257

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				
Guest	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	10.0.1.0/24		ssh telnet web-browsing			

B)

Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
Guest	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 telnet web-browsing			

C)

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

D)

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

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

Answer: C

NEW QUESTION 261

An administrator wishes to follow best practices for logging traffic that traverses the firewall Which log setting is correct?

- A. Disable all logging
B. Enable Log at Session End
C. Enable Log at Session Start
D. Enable Log at both Session Start and End

Answer: B

NEW QUESTION 262

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 264

.....

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>