



Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

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

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

Answer: C

Explanation:

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 4

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

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

Answer: AD

Explanation:

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

NEW QUESTION 5

What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

- A. Configure an authentication policy
- B. Configure an authentication sequence
- C. Configure an authentication profile
- D. Isolate the management interface on a dedicated management VLAN

Answer: C

NEW QUESTION 6

An administrator would like to block access to a web server, while also preserving

resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

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

Answer: AC

NEW QUESTION 7

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

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

Answer: B

NEW QUESTION 8

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 9

What is an advantage for using application tags?

- A. They are helpful during the creation of new zones
- B. They help with the design of IP address allocations in DHCP.
- C. They help content updates automate policy updates
- D. They help with the creation of interfaces

Answer: C

NEW QUESTION 10

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 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 15

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

- A. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 18

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 22

What allows a security administrator to preview the Security policy rules that match new application signatures?

- A. Review Release Notes
- B. Dynamic Updates-Review Policies
- C. Dynamic Updates-Review App
- D. Policy Optimizer-New App Viewer

Answer: B

Explanation:

<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 23

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

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

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

Answer: C

NEW QUESTION 27

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

- A)
- Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Deny
- B)
- Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Allow
- C)
- Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Deny
- D)

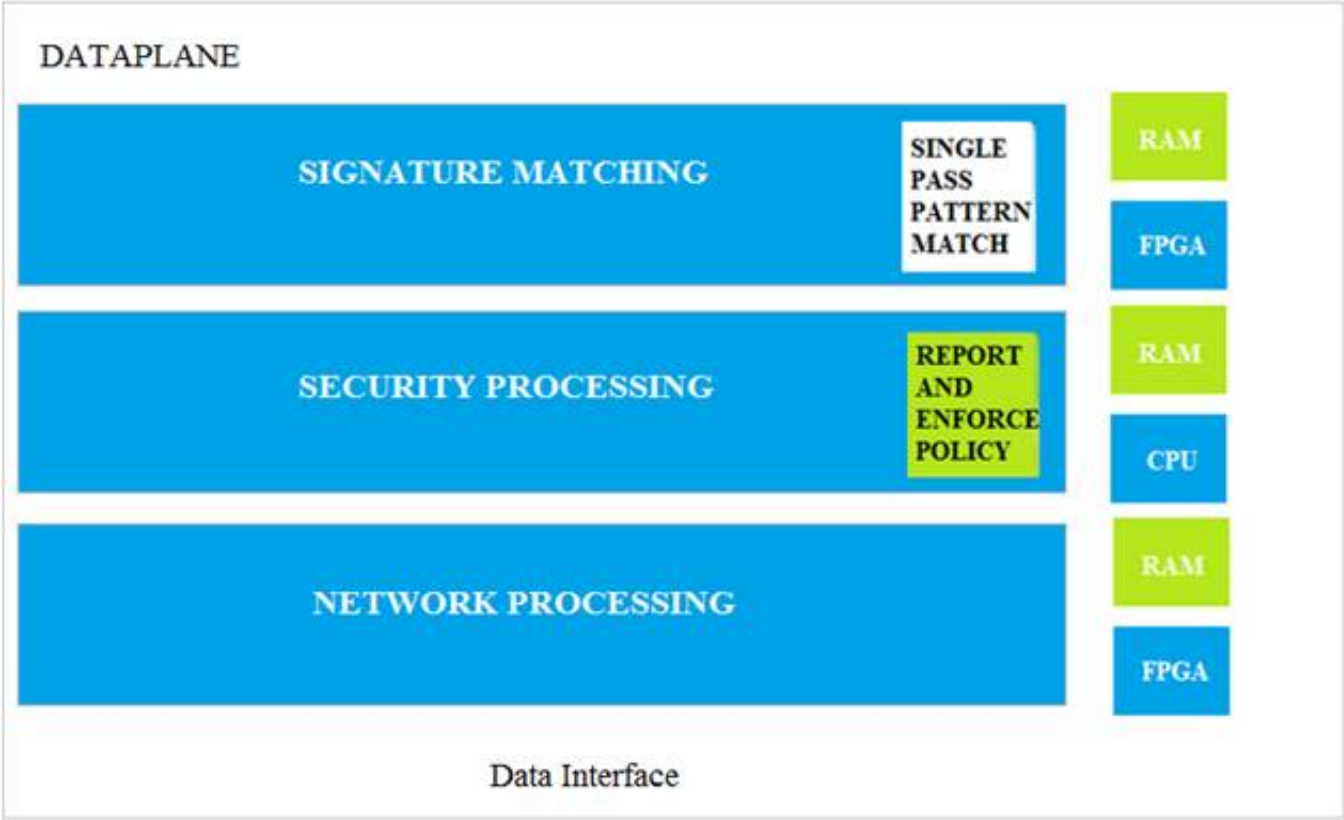
Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow

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

Answer: D

NEW QUESTION 30

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



- A. Signature Matching
- B. Network Processing
- C. Security Processing
- D. Security Matching

Answer: A

NEW QUESTION 34

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 36

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

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

Answer: A

NEW QUESTION 38

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 42

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

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

Answer: B

NEW QUESTION 46

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

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

Answer: A

Explanation:

? A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic¹.
? There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis¹.
? The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination². WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware³. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats⁴.
? 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 49

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

OK

Cancel

- 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 0CIFGCA0>

NEW QUESTION 51

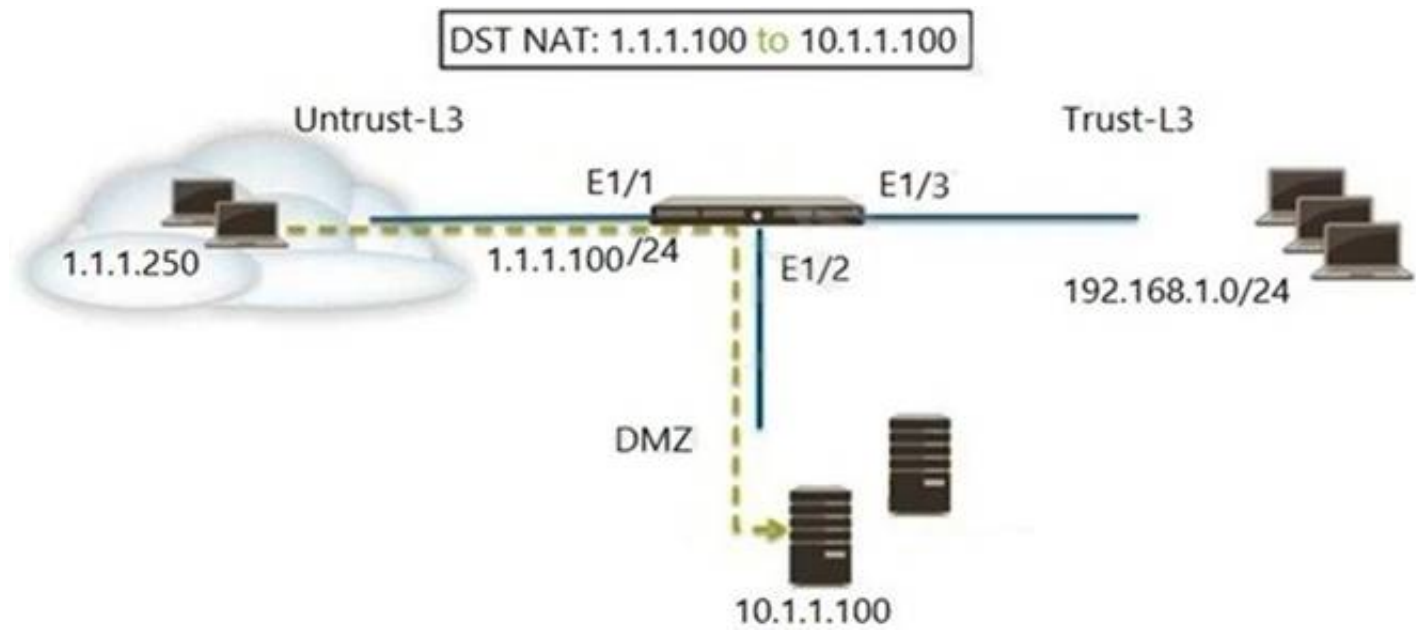
An administrator has configured a Security policy where the matching condition includes a single application and the action is deny
 If the application s default deny action is reset-both what action does the firewall take*?

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

Answer: A

NEW QUESTION 55

Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 59

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. Mastered
- B. Not Mastered

Answer: A

NEW QUESTION 62

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

The screenshot shows the User-ID Agent configuration and monitoring panel. The configuration section includes the following settings:

- Domain's DNS Name: lab.local
- Kerberos Server Profile: lab-kerberos
- Enable Security Log: ☒
- Server Log Monitor Frequency (sec): 2
- Enable Session: ☒
- Server Session Read Frequency (sec): 10
- Novell eDirectory Query Interval (sec): 30
- Syslog Service Profile: ☒
- Enable Probing: ☒
- Prove 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:

The Server Monitoring section shows a table with the following data:

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected

- 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 64

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 68

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 69

What action will inform end users when their access to Internet content is being restricted?

- A. Create a custom 'URL Category' object with notifications enabled.
- B. Publish monitoring data for Security policy deny logs.
- C. Ensure that the 'site access' setting for all URL sites is set to 'alert'.
- D. Enable 'Response Pages' on the interface providing Internet access.

Answer: D

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/device/device-response-pages.html>

NEW QUESTION 74

Which URL Filtering profile action would you set to allow users the option to access a site only if they provide a URL admin password?

- A. override
- B. authorization
- C. authentication
- D. continue

Answer: B

Explanation:

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

NEW QUESTION 75

DRAG DROP

Match the network device with the correct User-ID technology.

Answer Area

Microsoft Exchange	Drag answer here	syslog monitoring
Linux authentication	Drag answer here	Terminal Services agent
Windows clients	Drag answer here	server monitoring
Citrix client	Drag answer here	client probing

Answer:

Answer Area

Microsoft Exchange	server monitoring	syslog monitoring
Linux authentication	syslog monitoring	Terminal Services agent
Windows clients	client probing	server monitoring
Citrix client	Terminal Services agent	client probing

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Microsoft Exchange – Server monitoring
Linux authentication – syslog monitoring
Windows Client – client probing
Citrix client – Terminal Services agent

NEW QUESTION 79

When creating a custom URL category object, which is a valid type?

- A. domain match
B. host names
C. wildcard
D. category match

Answer: D

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-custom-objects-url-category.html>

NEW QUESTION 82

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 84

Which three configuration settings are required on a Palo Alto networks firewall management interface?

- A. default gateway
B. netmask
C. IP address
D. hostname
E. auto-negotiation

Answer: ABC

Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK>

NEW QUESTION 85

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

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

Answer: D

Explanation:

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

NEW QUESTION 88

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 92

Which type of administrator account cannot be used to authenticate user traffic flowing through the firewall's data plane?

- A. Kerberos user
- B. SAML user
- C. local database user
- D. local user

Answer: B

NEW QUESTION 97

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

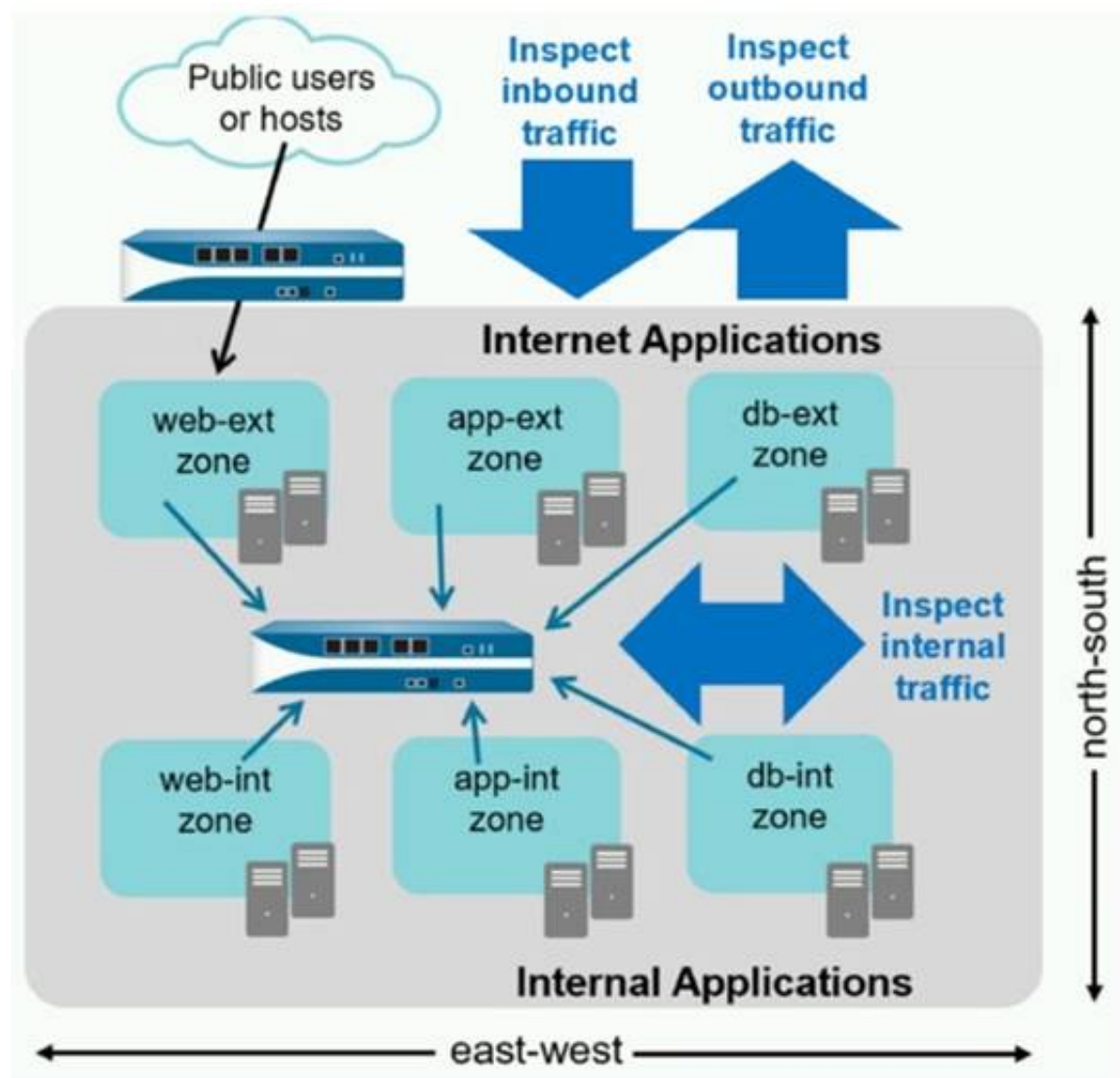
Explanation:

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 100

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 102

Which type of address object is www.paloaltonetworks.com?

- A. IP range
- B. IP netmask
- C. named address
- D. FQDN

Answer: D

Explanation:

NEW QUESTION 107

What is the purpose of the automated commit recovery feature?

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

Answer: C

Explanation:

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

NEW QUESTION 112

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

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

Answer: A

NEW QUESTION 113

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 117

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 121

Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.

Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

- A. antivirus profile applied to outbound security policies
- B. data filtering profile applied to inbound security policies
- C. data filtering profile applied to outbound security policies
- D. vulnerability profile applied to inbound security policies

Answer: C

Explanation:

NEW QUESTION 126

An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.

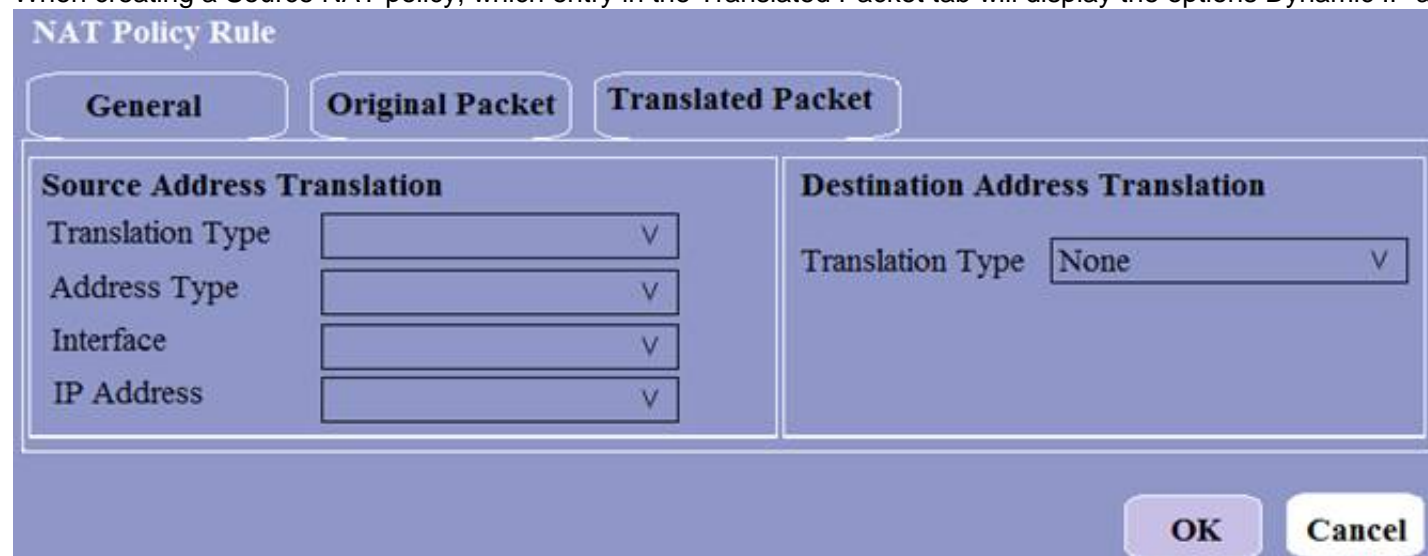
Which Security profile should be used?

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

Answer: C

NEW QUESTION 128

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?



The screenshot shows the 'NAT Policy Rule' configuration window with the 'Translated Packet' tab selected. It contains two main sections: 'Source Address Translation' and 'Destination Address Translation'. The 'Source Address Translation' section has four dropdown menus: 'Translation Type', 'Address Type', 'Interface', and 'IP Address'. The 'Destination Address Translation' section has one dropdown menu: 'Translation Type', which is currently set to 'None'. At the bottom right are 'OK' and 'Cancel' buttons.

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

Answer: A

NEW QUESTION 131

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

Answer: A

NEW QUESTION 134

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

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

Answer: B

NEW QUESTION 138

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

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

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

Answer: A

NEW QUESTION 141

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

Explanation:

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC>

NEW QUESTION 146

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

Explanation:

Reference:<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types.html>

NEW QUESTION 151

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

Explanation:

Reference:<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000000CIVHCA0>

NEW QUESTION 152

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

- A. authentication
- B. decryption
- C application override
- C. NAT

Answer: AB

Explanation:

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

NEW QUESTION 156

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

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

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

Answer: D

NEW QUESTION 158

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 159

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 164

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

D. 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

Answer: AD

NEW QUESTION 169

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 174

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 178

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 181

Which prevention technique will prevent attacks based on packet count?

- A. zone protection profile
- B. URL filtering profile
- C. antivirus profile
- D. vulnerability profile

Answer: A

NEW QUESTION 185

Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

- A. User identification
- B. Filtration protection
- C. Vulnerability protection
- D. Antivirus
- E. Application identification
- F. Anti-spyware

Answer: ACDEF

NEW QUESTION 187

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 189

.....

Relate Links

100% Pass Your PCNSA Exam with ExamBible Prep Materials

<https://www.exambible.com/PCNSA-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>