

PCNSE.exam.79q

Number: PCNSE
Passing Score: 800
Time Limit: 120 min



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

PCNSE

Palo Alto Networks Certified Network Security Engineer

Exam A

QUESTION 1

Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMWare API on the firewall or on the User-ID agent or the read-only domain controller (RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML-API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynamically>

QUESTION 2

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?



<https://vceplus.com/>

- A. Configure the option for "Threshold".
- B. Disable automatic updates during weekdays.
- C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update.
- D. Automatically "download and install" but with the "disable new applications" option used.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

- A. Security policy
- B. Decryption policy
- C. Authentication policy
- D. Application Override policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

A Security policy rule is configured with a Vulnerability Protection Profile and an action of 'Deny'.

Which action will this cause configuration on the matched traffic?

- A. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to “Deny”.
- B. The configuration will allow the matched session unless a vulnerability signature is detected. The “Deny” action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
- C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit.
- D. The configuration is valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to “Deny.”

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>.

How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

- A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.
- B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
- C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
- D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

What are two benefits of nested device groups in Panorama? (Choose two.)

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group

D. Overwrites local firewall configuration

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Which Captive Portal mode must be configured to support MFA authentication?

- A. NTLM
- B. Redirect
- C. Single Sign-On
- D. Transparent

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

QUESTION 9

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required.

Which interface type would support this business requirement?



<https://vceplus.com/>

- A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ

- B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
- C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

- A. Okta
- B. DUO
- C. RADIUS
- D. PingID

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 11

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

- A. Use the debug dataplane packet-diag set capture stage firewall file command.
- B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
- C. Use the debug dataplane packet-diag set capture stage management file command.
- D. Use the tcpdump command.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390>

QUESTION 12

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#idaed4e749-80b44641-a37c-c741aba562e9>

QUESTION 13

A session in the Traffic log is reporting the application as “incomplete.”

What does “incomplete” mean?

- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Correct Answer: B

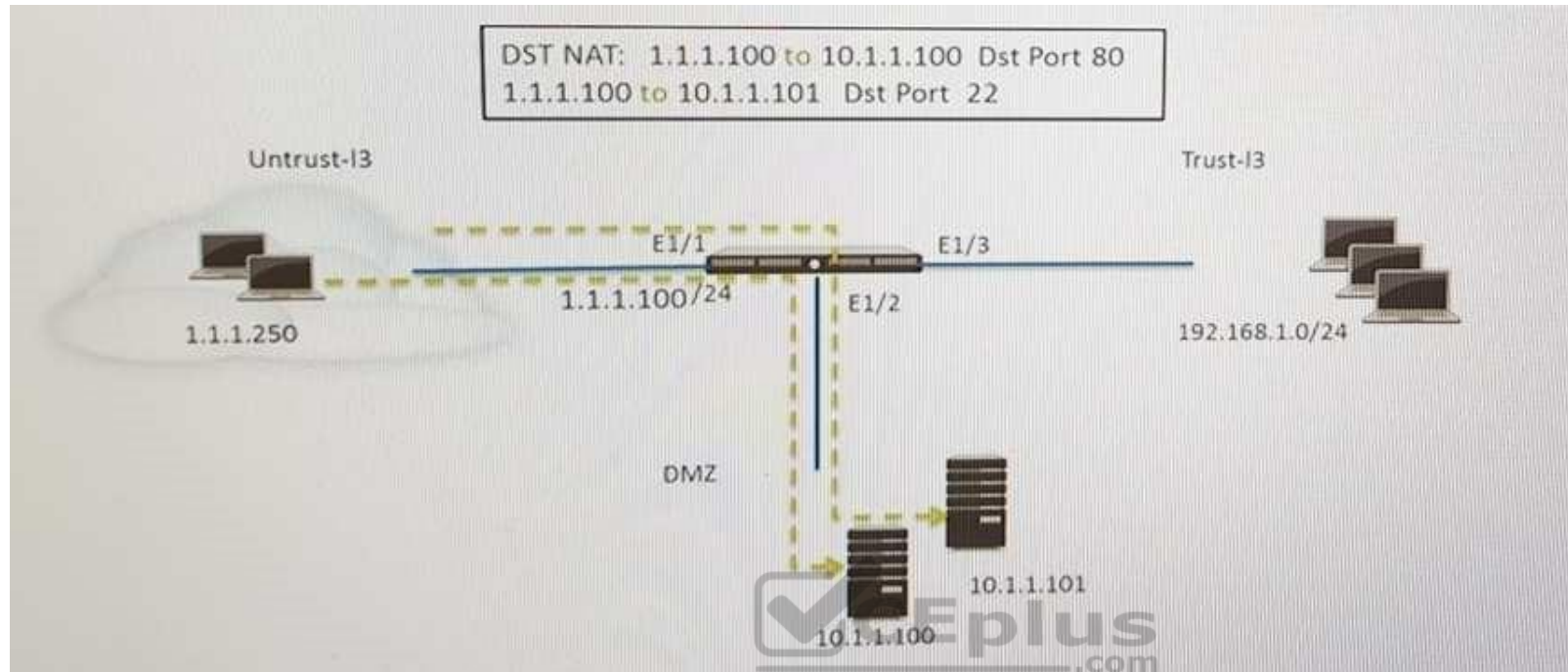
Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

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 Untrust (10.1.1.100), web-browsing -Allow
- B. Untrust (Any) to Untrust (10.1.1.101), ssh -Allow
- C. Untrust (Any) to DMZ (10.1.1.100), web-browsing -Allow
- D. Untrust (Any) to DMZ (10.1.1.100), ssh -Allow
- E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Correct Answer: CD

Section: (none)

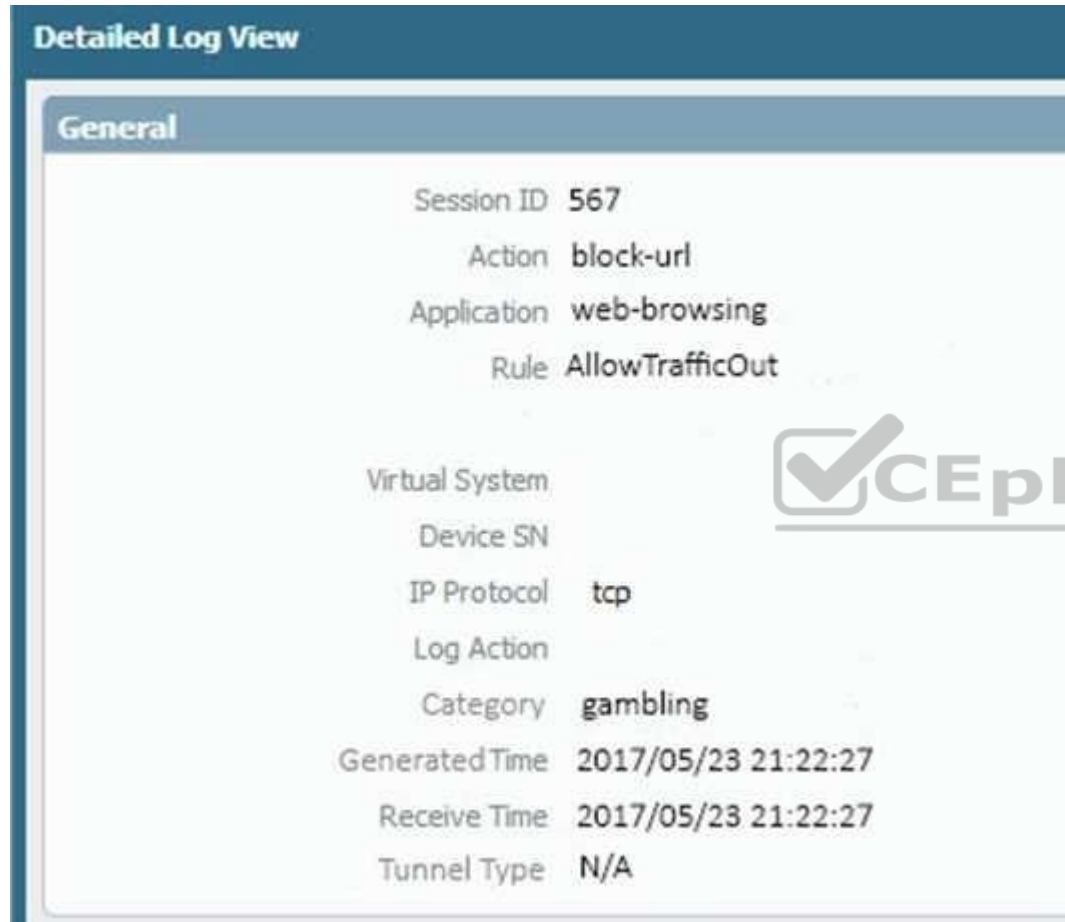
Explanation

Explanation/Reference:

QUESTION 15

An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.

Which configuration change should the administrator make? A.



URL Filtering Profile

Name: Filter1

Description:

Categories | Overrides | URL Filtering Settings | User Credential Detection

Category	Site Access	User Credential Submission
<input type="checkbox"/> educational-institutions	allow	allow
<input type="checkbox"/> entertainment-and-arts	allow	allow
<input type="checkbox"/> extremism	allow	allow
<input type="checkbox"/> financial services	allow	allow
<input checked="" type="checkbox"/> gambling	allow	block
<input type="checkbox"/> games	allow	allow
<input type="checkbox"/> government	allow	allow
<input type="checkbox"/> hacking	block	block
<input type="checkbox"/> health-and-medicine	continue	allow
	override	allow

* indicates a custom URL category; + indicates external dynamic list

Check URL Category

OK Cancel

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions | Target

Name: www.megamillions.com

Rule Type: universal (default)

Description:

Tags:

OK Cancel

B. C.

URL Filtering Profile

Name:

Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow-List:

Block List:

Action:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

D.

URL Filtering Profile

Name:

Description:

Overrides Categories URL Filtering Settings User Credential Detection

Allow-List:

Block List:

Action:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

E.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which three settings are defined within the Templates object of Panorama? (Choose three.)

- A. Setup
- B. Virtual Routers
- C. Interfaces
- D. Security
- E. Application Override

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections.

Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 18

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab.

Which profile is the cause of the missing Policies tab?

- A. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

- A. WildFire updates
- B. NAT
- C. NTP
- D. antivirus
- E. File blocking

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama.

Which action would enable the firewalls to send their pre-existing logs to Panorama?



<https://vceplus.com/>

- A. Use the import option to pull logs into Panorama.
- B. A CLI command will forward the pre-existing logs to Panorama.
- C. Use the ACC to consolidate pre-existing logs.
- D. The log database will need to be exported from the firewalls and manually imported into Panorama.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A Palo Alto Networks NGFW just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 22

What are the differences between using a service versus using an application for Security Policy match?

- A. Use of a “service” enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an “application” allows the firewall to take immediate action if the port being used is a member of the application standard port list.
- B. There are no differences between “service” or “application”. Use of an “application” simplifies configuration by allowing use of a friendly application name instead of port numbers.
- C. Use of a “service” enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an “application” allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used
- D. Use of a “service” enables the firewall to take action after enough packets allow for App-ID identification

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Refer to the exhibit.



<https://vceplus.com/>



#####

admin@Lab33-111-PA-3060(active)>show routing fib

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6	1500
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6	1500

#####

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:

flags: m-multicast firewalling
 p= link state pass-through
 s- vlan sub-interface
 i- ip+vlan sub-interface
 t-tenant sub-interface

name	interface1	interface2	flags	allowed-tags
VW-1	ethernet1/7	ethernet1/5	p	

#####

Which will be the egress interface if the traffic's ingress interface is ethernet 1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

- A. ethernet1/6
- B. ethernet1/3
- C. ethernet1/7
- D. ethernet1/5

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

Which three authentication services can administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

- A. Kerberos
- B. PAP
- C. SAML
- D. TACACS+
- E. RADIUS
- F. LDAP



Correct Answer: ACF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which event will happen if an administrator uses an Application Override Policy?

- A. Threat-ID processing time is decreased.
- B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
- C. The application name assigned to the traffic by the security rule is written to the Traffic log.
- D. App-ID processing time is increased.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

QUESTION 26

Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

- A. Deny application facebook-chat before allowing application facebook
- B. Deny application facebook on top
- C. Allow application facebook on top
- D. Allow application facebook before denying application facebook-chat

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673>

QUESTION 27

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?

- A. Mapping to the IP address of the logged-in user.
- B. First four letters of the username matching any valid corporate username.
- C. Using the same user's corporate username and password.
- D. Matching any valid corporate username.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/credential-phishing-prevention>

QUESTION 29

An administrator has users accessing network resources through Citrix XenApp 7 x.

Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

- A. Client Probing
- B. Terminal Services agent
- C. GlobalProtect
- D. Syslog Monitoring



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web browsing traffic from any to any zone.

What must the administrator configure so that the PAN-OS® software can be upgraded?

- A. Security policy rule
- B. CRL
- C. Service route
- D. Scheduler

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which feature prevents the submission of corporate login information into website forms?



- A. Data filtering
- B. User-ID
- C. File blocking
- D. Credential phishing prevention

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance>

QUESTION 32

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt C. IPsec tunnel encryption
- D. Packet egress process

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Which protection feature is available only in a Zone Protection Profile?

- A. SYN Flood Protection using SYN Flood Cookies
- B. ICMP Flood Protection
- C. Port Scan Protection
- D. UDP Flood Protections

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 34

Which CLI command can be used to export the tcpdump capture?

- A. scp export tcpdump from mgmt.pcap to <username@host:path>
- B. scp extract mgmt-pcap from mgmt.pcap to <username@host:path>
- C. scp export mgmt-pcap from mgmt.pcap to <username@host:path>
- D. download mgmt.-pcap

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415>

QUESTION 35

An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.

Which configuration setting or step will allow the firewall to get automatic application signature updates?

- A. A scheduler will need to be configured for application signatures.
- B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
- C. A Threat Prevention license will need to be installed.
- D. A service route will need to be configured.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list.

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates>

QUESTION 36

Which three options are supported in HA Lite? (Choose three.)

- A. Virtual link
- B. Active/passive deployment
- C. Synchronization of IPsec security associations
- D. Configuration synchronization
- E. Session synchronization

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite>

QUESTION 37

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

- A. debug system details
- B. show session info
- C. show system info
- D. show system details

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful-Commands/ta-p/56511>

QUESTION 38

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. Application changed from content inspection
- D. Session application identified.



Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

- A. Session Browser
- B. Application Command Center
- C. TCP Dump
- D. Packet Capture

Correct Answer: B

Section: (none)

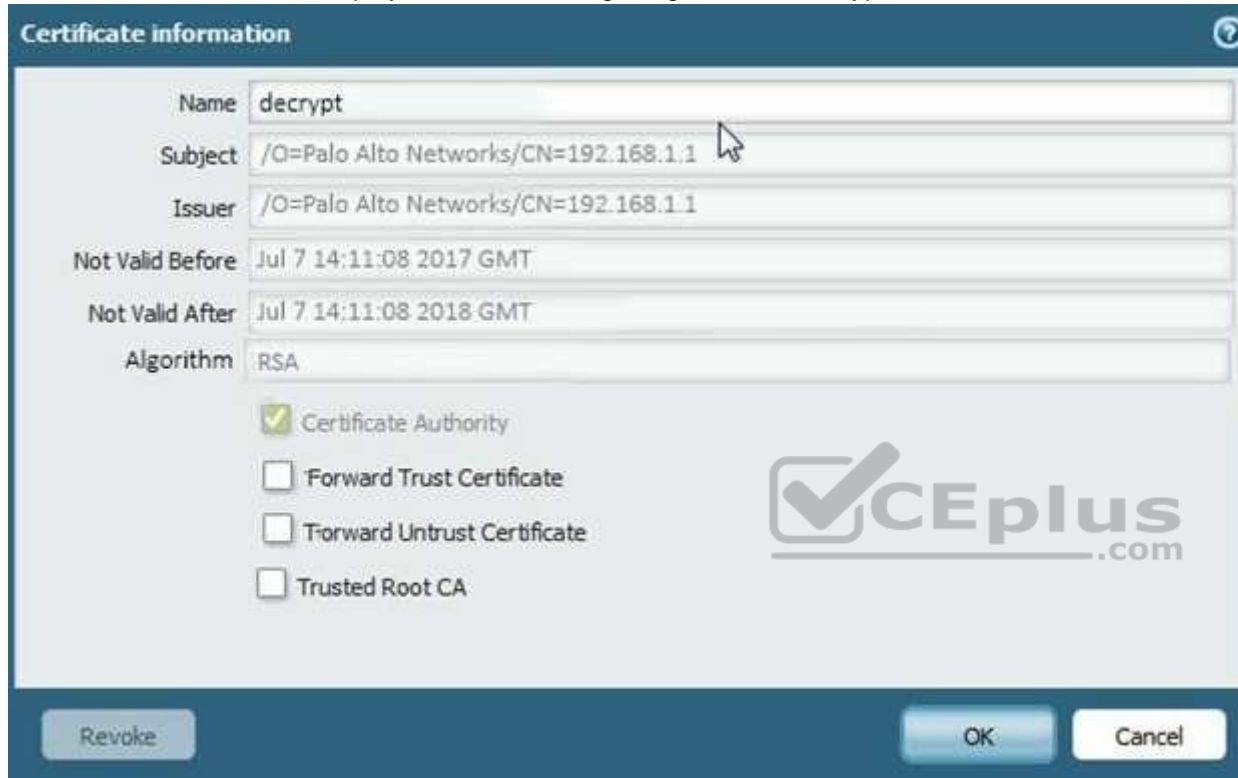
Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Management-Articles/Tips-and-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342>

QUESTION 40

The certificate information displayed in the following image is for which type of certificate?



The image shows a 'Certificate information' dialog box with the following fields and options:

Field	Value
Name	decrypt
Subject	/O=Palo Alto Networks/CN=192.168.1.1
Issuer	/O=Palo Alto Networks/CN=192.168.1.1
Not Valid Before	Jul 7 14:11:08 2017 GMT
Not Valid After	Jul 7 14:11:08 2018 GMT
Algorithm	RSA

Below the fields, there are four checkboxes:

- ☒ Certificate Authority
- ☐ Forward Trust Certificate
- ☐ Forward Untrust Certificate
- ☐ Trusted Root CA

At the bottom, there are three buttons: 'Revoke', 'OK', and 'Cancel'. A large 'CEplus.com' watermark is visible in the background of the dialog box.

- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

- A. Disable SNMP on the management interface.
- B. Application override of SSL application.
- C. Disable logging at session start in Security policies.
- D. Disable predefined reports.
- E. Reduce the traffic being decrypted by the firewall.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing> **QUESTION 43**

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewallconfigurations

QUESTION 44

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect traffic when users browse to HTTP(S) websites?



- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. TLS Bidirectional proxy
- D. SSL Outbound Inspection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

- A. Create a custom App-ID and enable scanning on the advanced tab.
- B. Create an Application Override policy.
- C. Create a custom App-ID and use the “ordered conditions” check box.
- D. Create an Application Override policy and custom threat signature for the application.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router.

Which two options enable the administrator to troubleshoot this issue? (Choose two.)

- A. View Runtime Stats in the virtual router.
- B. View System logs.
- C. Add a redistribution profile to forward as BGP updates.
- D. Perform a traffic pcap at the routing stage.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port.

Which log entry can the administrator use to verify that sessions are being decrypted?

- A. In the details of the Traffic log entries
- B. Decryption log
- C. Data Filtering log
- D. In the details of the Threat log entries

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719>

QUESTION 49

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

QUESTION 50

Which processing order will be enabled when a Panorama administrator selects the setting “Objects defined in ancestors will take higher precedence?”

- A. Descendant objects will take precedence over other descendant objects.
- B. Descendant objects will take precedence over ancestor objects.
- C. Ancestor objects will have precedence over descendant objects.
- D. Ancestor objects will have precedence over other ancestor objects.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-setup-management>

QUESTION 51

An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

How would the administrator establish the chain of trust?

- A. Use custom certificates
- B. Enable LDAP or RADIUS integration
- C. Set up multi-factor authentication
- D. Configure strong password authentication

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment

QUESTION 52

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

```
admin@Lab33-111-PA-3060(active)> show clock
```

```
Thu Jun  8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)> show routing fib
```

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
40	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	1500

- A. ethernet1/7
- B. ethernet1/5
- C. ethernet1/6
- D. ethernet1/3

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443?

- A. Rule #1: application: web-browsing; service: application-default; action: allow
Rule #2: application: ssl; service: application-default; action: allow
- B. Rule #1: application: web-browsing; service: service-https; action: allow Rule
#2: application: ssl; service: application-default; action: allow
- C. Rule # 1: application: ssl; service: application-default; action: allow
Rule #2: application: web-browsing; service: application-default; action: allow
- D. Rule #1: application: web-browsing; service: service-http; action: allow Rule
#2: application: ssl; service: application-default; action: allow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

- A. The firewall is in multi-vsyt mode.

- B. The traffic is offloaded.
- C. The traffic does not match the packet capture filter.
- D. The firewall's DP CPU is higher than 50%.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload>

QUESTION 55

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.

Which solution in PAN-OS® software would help in this case?

- A. application override
- B. Virtual Wire mode
- C. content inspection
- D. redistribution of user mappings



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network>

QUESTION 56

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a “No Decrypt” action? (Choose two.)

- A. Block sessions with expired certificates
- B. Block sessions with client authentication
- C. Block sessions with unsupported cipher suites
- D. Block sessions with untrusted issuers
- E. Block credential phishing

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traffic-to-decrypt/create-a-decryption-profile>

QUESTION 57

Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

- A. port mapping
- B. server monitoring
- C. client probing
- D. XFF headers

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users>

QUESTION 58

In High Availability, which information is transferred via the HA data link?

- A. session information
- B. heartbeats
- C. HA state information
- D. User-ID information

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

QUESTION 59

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

- A. `show running resource-monitor`
- B. `debug data-plane dp-cpu` C. `show system resources`
- D. `debug running resources`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

Which DoS protection mechanism detects and prevents session exhaustion attacks?



- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

QUESTION 61

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?



- A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
- B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
- C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
- D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-clientauthentication-configurations/define-the-globalprotect-agent-configurations>

QUESTION 62

Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

- A. TACACS+
- B. Kerberos
- C. PAP
- D. LDAP
- E. SAML
- F. RADIUS

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 63

Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

- A. Both SSH keys and SSL certificates must be generated.
- B. No prerequisites are required.
- C. SSH keys must be manually generated.
- D. SSL certificates must be generated.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy>

QUESTION 64

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation.

Which two formats are correct for naming aggregate interfaces? (Choose two.)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor.

When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

- A. Zone Protection

- B. Replay
- C. Web Application
- D. DoS Protection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet.

Which configuration will enable the firewall to download and install application updates automatically?

- A. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
- B. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
- C. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the update servers goes out of the interface acting as your Internet connection.
- D. Configure a Security policy rule to allow all traffic to and from the update servers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

A company wants to install a PA-3060 firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and assign untagged (native) traffic to its own zone.

Which option differentiates multiple VLANs into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of "0-4096" in the "Tag Allowed" field of the V-Wire object.
- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the "Tag Allowed" field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

- C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
- D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System Utilization log
- B. System log
- C. Resources widget
- D. CPU Utilization widget



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

Which four NGFW multi-factor authentication factors are supported by PAN-OS®? (Choose four.)

- A. Short message service
- B. Push
- C. User logon
- D. Voice
- E. SSH key
- F. One-Time Password

Correct Answer: ABDF

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

QUESTION 70

An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.0.2. The firewall is not a part of an HA pair.

What needs to be updated first?

- A. Applications and Threats
- B. XML Agent
- C. WildFire
- D. PAN-OS® Upgrade Agent

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 71

An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware monitors behavior without the user's knowledge.

What is the expected verdict from WildFire?

- A. Malware
- B. Grayware
- C. PhishingD. Spyware

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

When configuring the firewall for packet capture, what are the valid stage types?

- A. receive, management, transmit, and non-syn
- B. receive, management, transmit, and drop
- C. receive, firewall, send, and non-syn
- D. receive, firewall, transmit, and drop

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which operation will impact performance of the management plane?

- A. DoS protection
- B. WildFire submissions
- C. generating a SaaS Application report
- D. decrypting SSL sessions

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

- A. 6-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol, and Source Security Zone
- B. 5-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Protocol
- C. 7-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, URL Category, and Source Security Zone
- D. 9-tuple match:
Source IP Address, Destination IP Address, Source port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

- A. ingress processing errors
- B. rule match with action “deny”
- C. rule match with action “allow”
- D. equal-cost multipath

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 76

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- Firewall has internet connectivity through e 1/1.
 - Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
 - Service route is configured, sourcing update traffic from e1/1.
 - A communication error appears in the System logs when updates are performed.
- Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. Static route pointing application PaloAlto-updates to the update servers
- B. Security policy rule allowing PaloAlto-updates as the application
- C. Scheduler for timed downloads of PAN-OS software
- D. DNS settings for the firewall to use for resolution

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Add an Anti-Spyware Profile to block attacking IP address
- B. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- C. Add QoS Profiles to throttle incoming requests
- D. Add a tuned DoS Protection Profile

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 78

Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

- A. .dll
- B. .exe
- C. .fon
- D. .apk
- E. .pdf
- F. .jar

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

An administrator has been asked to configure active/active HA for a pair of Palo Alto Networks NGFWs. The firewall use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

- A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
- B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
- C. The firewalls do not use floating IPs in active/active HA.
- D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/floating-ip-address-and-virtual-mac-address>



<https://vceplus.com/>