

PCNSE

Number: PCNSE
Passing Score: 800
Time Limit: 120 min
File Version: 1

PCNSE



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/>

Exam A

QUESTION 1

Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?



<https://vceplus.com/>

- A. check
- B. find
- C. test
- D. sim



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html>

QUESTION 2

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.

Which two mandatory options are used to configure a VLAN interface? (Choose two.)

- A. Virtual router
- B. Security zone
- C. ARP entries
- D. Netflow Profile

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans.

Which Security Profile type will protect against worms and trojans?

- A. Anti-Spyware
- B. Instruction Prevention
- C. File Blocking
- D. Antivirus

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles>

QUESTION 4

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

- A. 0
- B. 99
- C. 1
- D. 255

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/high-availability/device-priority-and-preemption>

QUESTION 5

An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

- A. The passive firewall, which then synchronizes to the active firewall
- B. The active firewall, which then synchronizes to the passive firewall
- C. Both the active and passive firewalls, which then synchronize with each other
- D. Both the active and passive firewalls independently, with no synchronization afterward

Correct Answer: C

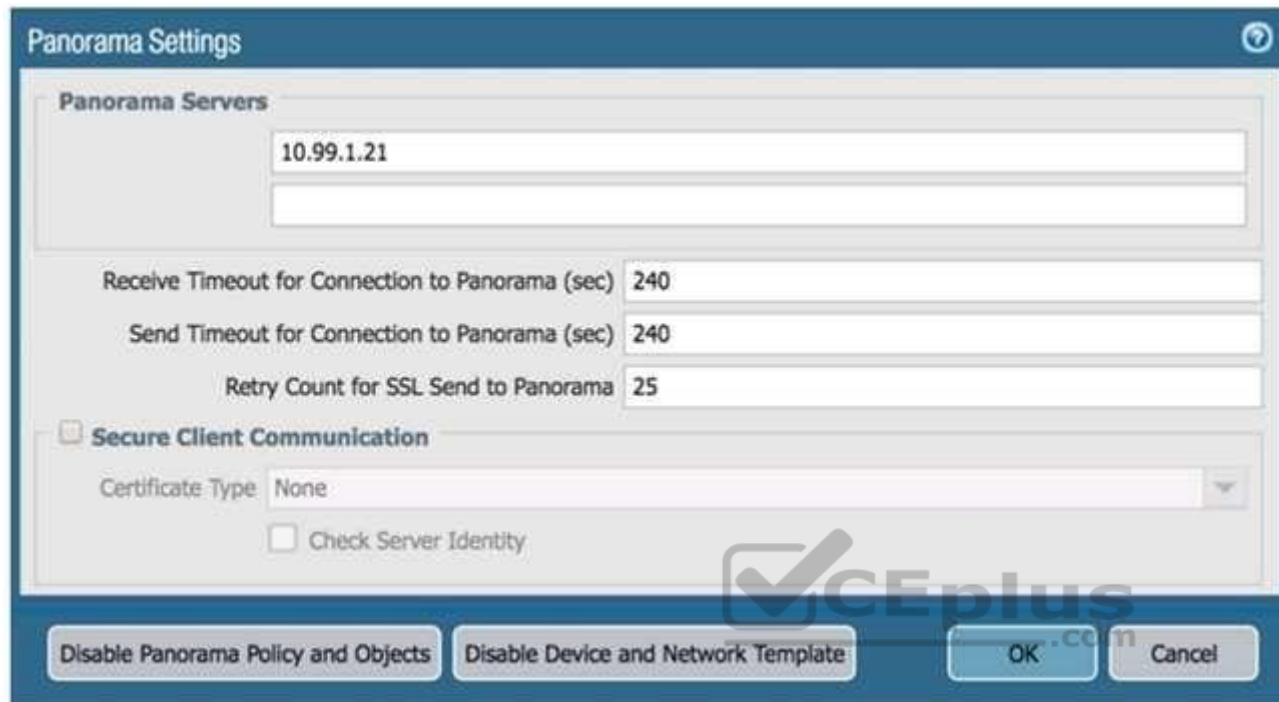
Section: (none)

Explanation

Explanation/Reference:**QUESTION 6**

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall. Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the firewall to Panorama?

A.



The image shows a 'Panorama Settings' dialog box with a blue title bar and a question mark icon in the top right corner. The dialog is divided into two main sections. The first section, 'Panorama Servers', contains a text field with the IP address '10.99.1.21' and an empty text field below it. The second section contains three labeled text fields: 'Receive Timeout for Connection to Panorama (sec)' with the value '240', 'Send Timeout for Connection to Panorama (sec)' with the value '240', and 'Retry Count for SSL Send to Panorama' with the value '25'. Below these is a section titled 'Secure Client Communication' with a checkbox that is currently unchecked. Under this checkbox, there is a 'Certificate Type' dropdown menu set to 'None' and an unchecked checkbox labeled 'Check Server Identity'. At the bottom of the dialog, there are four buttons: 'Disable Panorama Policy and Objects', 'Disable Device and Network Template', 'OK', and 'Cancel'. A large, semi-transparent 'VCEplus.com' watermark is overlaid across the center of the dialog box.

Panorama Settings

Panorama Servers

10.99.1.21

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

☐ **Secure Client Communication**

Certificate Type: None

☐ Check Server Identity

Disable Panorama Policy and Objects Disable Device and Network Template OK Cancel

B.

Security Policy Rule

General Source User Destination Application Service/URL Category **Actions**

Action Setting

Action: ☐ Send ICMP Unreachable

Profile Setting

Profile Type:
Antivirus:
Vulnerability Protection:
Anti-Spyware:
URL Filtering:
File Blocking:
Data Filtering:
WildFire Analysis:

Log Setting

☒ Log at Session Start
☒ Log at Session End
Log Forwarding:

Other Settings

Schedule:
QoS Marking:
☐ Disable Server Response Inspection

OK Cancel

C.



Syslog Server Profile

Name: SyslogProfile1

☒ Panorama

Servers **Custom Log Format**

Name	Syslog Server	Transport	Port	Format	Facility
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

 Add  Delete

Enter the IP address or FQDN of the Syslog server

OK Cancel

D.

Panorama Settings

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

☒ Share Unused Address and Service Objects with Devices

☐ Objects defined in ancestors will take higher precedence

Secure Server Communication

☐ Custom Certificate Only

SSL/TLS Service Profile None

Certificate Profile None

Authorization List

Identifier	Type	Value
0 items		

+ Add - Delete

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

Disconnect Wait Time (min) [0-44640]

OK Cancel

E.

Correct Answer: D

Section: (none)



Explanation

Explanation/Reference:

QUESTION 7

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

QUESTION 8

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 *ready-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:

<https://vceplus.com/>

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

QUESTION 9

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

- 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 10

To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>

QUESTION 11

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

- A. Red Hat Enterprise Virtualization (RHEV)

- B. Kernel Virtualization Module (KVM)
- C. Boot Strap Virtualization Module (BSVM)
- D. Microsoft Hyper-V

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

QUESTION 12

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 13

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 14

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 15

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 16

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?

- 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 17

A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable web browsing access to the server.



<https://vceplus.com/>

Which application and service need to be configured to allow only cleartext web-browsing traffic to this server on tcp/8080?

- A. application: web-browsing; service: application-default
- B. application: web-browsing; service: service-https
- C. application: ssl; service: any
- D. application: web-browsing; service: (custom with destination TCP port 8080)

Correct Answer: A

Section: (none)

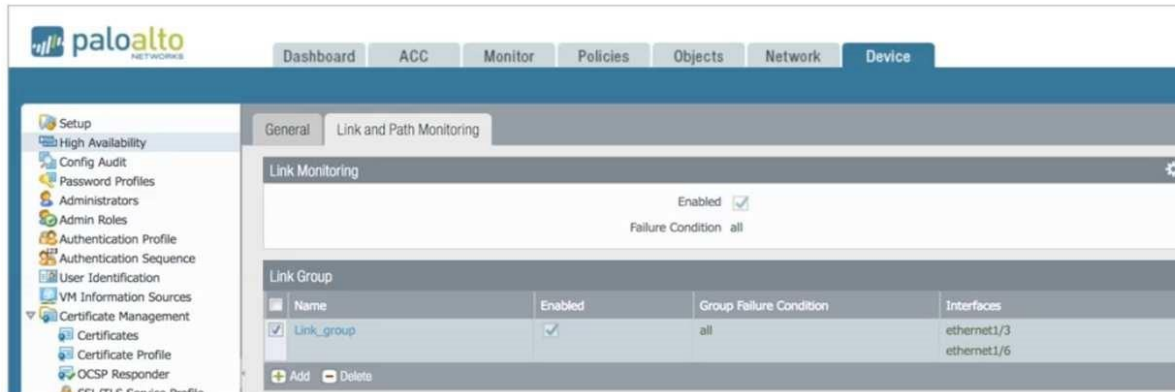
Explanation

<https://vceplus.com/>

Explanation/Reference:

QUESTION 18

If the firewall has the following link monitoring configuration, what will cause a failover?



- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or ethernet1/6 going down
- D. ethernet1/6 going down

Correct Answer: A

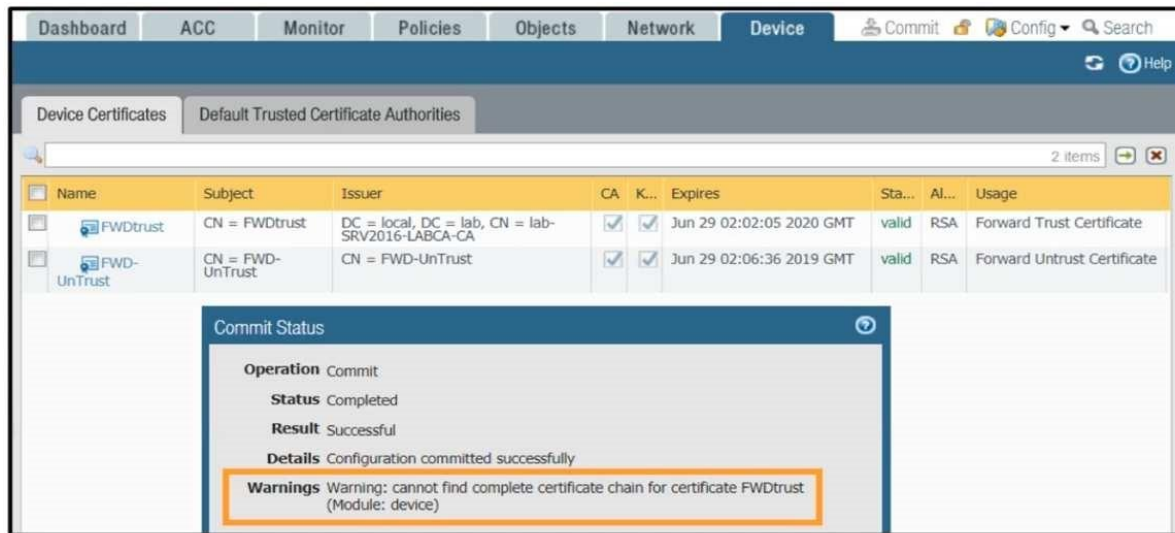
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

In the image, what caused the commit warning?



- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

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

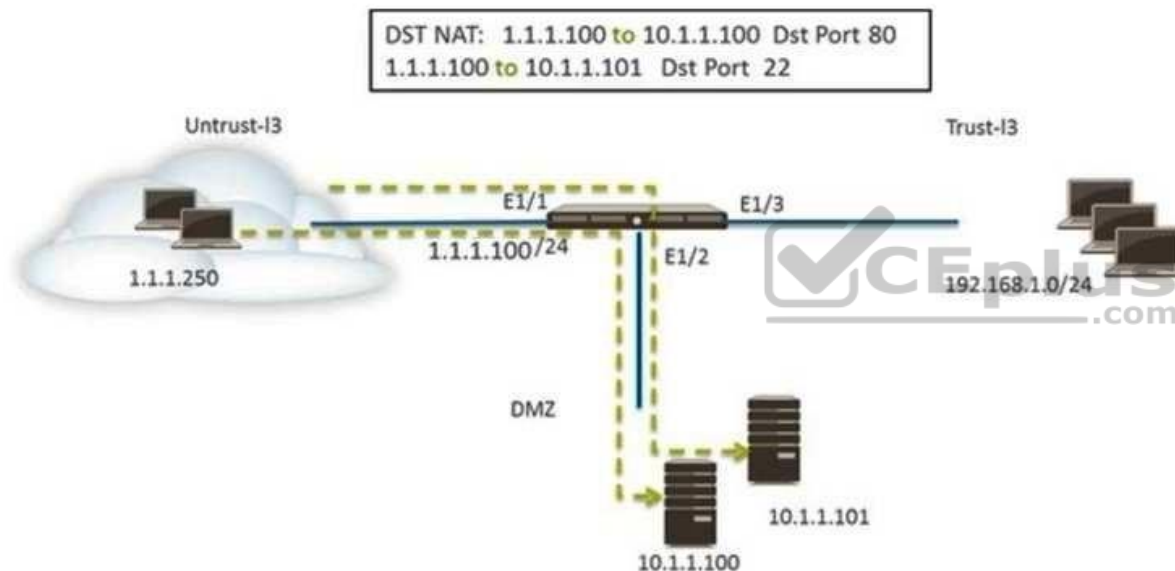
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

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 (10.1.1.1), web-browsing - Allow
- B. Untrust (Any) to Untrust (10.1.1.1), 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 22

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: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

A customer has an application that is being identified as unknown-tcp 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 24

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 25

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 26

Which Palo Alto Networks VM-Series firewall is valid?

- A. VM-25
- B. VM-800
- C. VM-50
- D. VM-400

Correct Answer: C

Section: (none)

Explanation

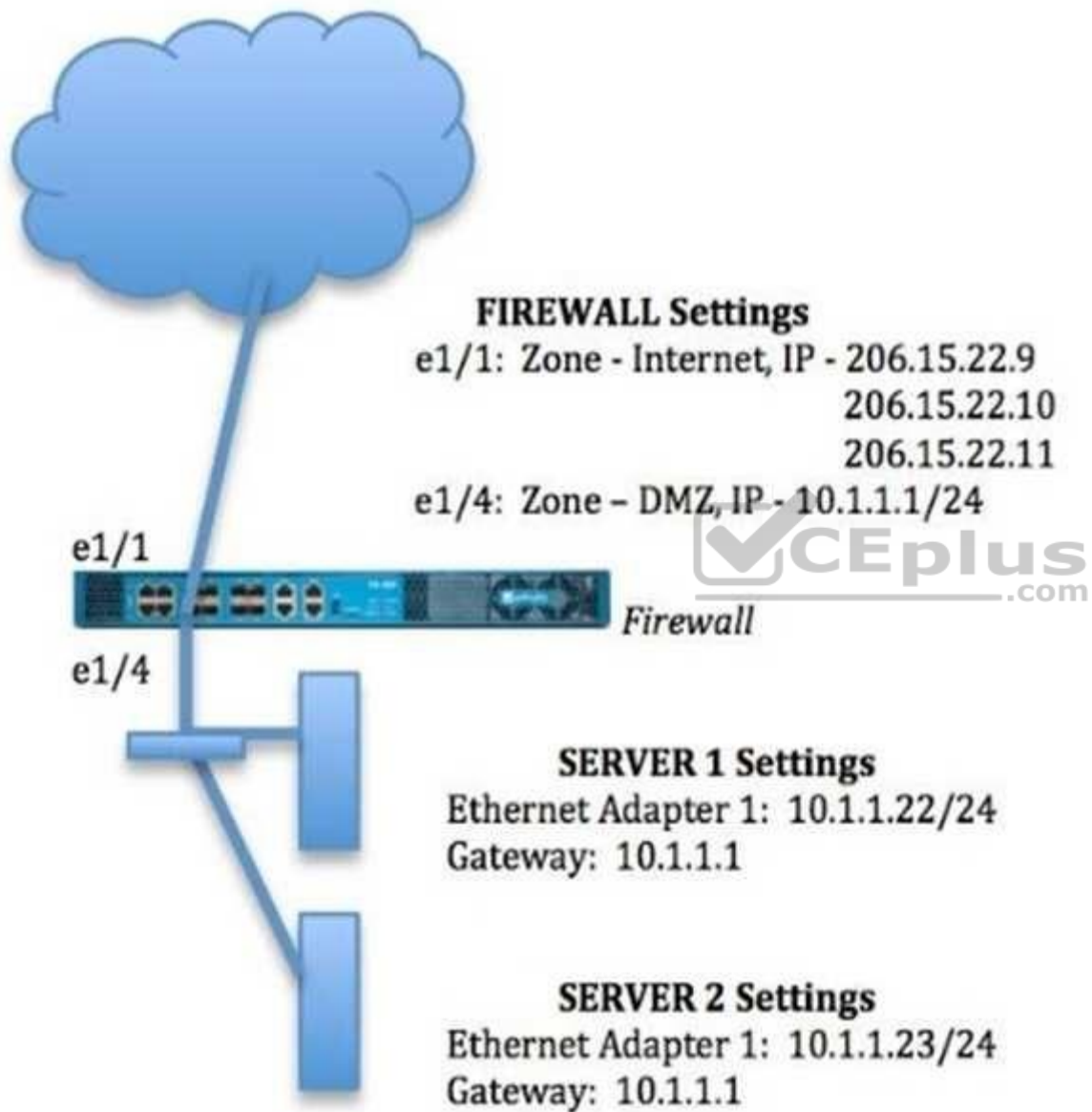
Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

QUESTION 27

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?



Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP



A.

B.



Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP



C.

D.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 28

An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW. The update contains an application that matches the same traffic signatures as the custom application.

Which application should be used to identify traffic traversing the NGFW?

- A. Custom application
- B. System logs show an application error and neither signature is used.
- C. Downloaded application
- D. Custom and downloaded application signature files are merged and both are used

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

<https://vceplus.com/>

QUESTION 29

Starting with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

- A. GlobalProtect
- B. System
- C. Authentication
- D. Configuration

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html>

QUESTION 30

Refer to the exhibit.



#####

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 : 1

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 ethernet1/7 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 31

Which three authentication services can an 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 32

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 33

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 34

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 35

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 36

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 37

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

- A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
- B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
- C. Disable the exclude cache option for the firewall.
- D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

- A. Configure a Decryption Profile and select SSL/TLS services.
- B. Set up SSL/TLS under **Policies > Service/URL Category>Service**.
- C. Set up Security policy rule to allow SSL communication.
- D. Configure an SSL/TLS Profile.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-ssl/tls-service-profile>

QUESTION 39

Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

- A. ACC
- B. System Logs
- C. App Scope
- D. Session Browser

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

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 41

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 42

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 43

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 44

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)

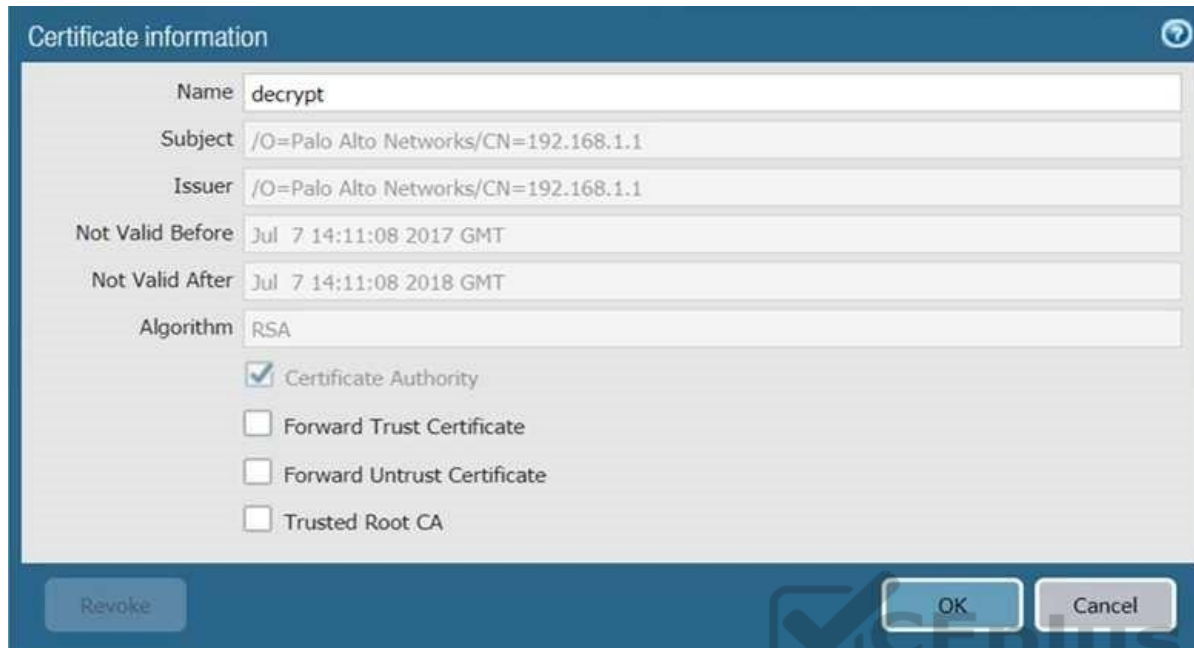
Explanation

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 45

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:

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 are four checkboxes:

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

At the bottom are three buttons: 'Revoke', 'OK', and 'Cancel'.

- 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 46

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 47

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 48

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 49

Which virtual router feature determines if a specific destination IP address is reachable?

- A. Heartbeat Monitoring
- B. Failover
- C. Path Monitoring
- D. Ping-Path

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf>

QUESTION 50

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

QUESTION 51

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 52

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 53

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 54

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
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	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

A. ethernet1/7

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

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-http; 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-https; action: allow Rule
#2: application: ssl; service: application-default; action: allow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

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

- A. The firewall is in multi-vsyz 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 57

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 58

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 59

The firewall identifies a popular application as an unknown-tcp.

Which two options are available to identify the application? (Choose two.)

- A. Create a custom application.
- B. Create a custom object for the custom application server to identify the custom application.
- C. Submit an Apple-ID request to Palo Alto Networks.
- D. Create a Security policy to identify the custom application.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/use-application-objects-in-policy/create-a-custom-application>

QUESTION 60

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

QUESTION 61

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

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.
- B. Add a Vulnerability Protection Profile to block the attack.
- C. Add QoS Profiles to throttle incoming requests.
- D. Add a DoS Protection Profile with defined session count.

Correct Answer: D

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-andpolicy-rules/dos-protection-profiles>

QUESTION 62

Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

- A. Verify AutoFocus status using the CLI “test” command.
- B. Check the WebUI Dashboard AutoFocus widget.
- C. Check for WildFire forwarding logs.
- D. Check the license.



<https://vceplus.com/>

E. Verify AutoFocus is enabled below Device Management tab.

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>

QUESTION 63

What is exchanged through the HA2 link?

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

Correct Answer: C

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 64

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

<https://vceplus.com/>

- 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 65

A customer wants to set up a site-to-site VPN using tunnel interfaces.

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

- A. tunnel.1
- B. vpn-tunnel.1
- C. tunnel.1025
- D. vpn-tunnel.1024



Correct Answer: AC

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 NGFW firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to 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

Which two features does PAN-OS® software use to identify applications? (Choose two.)

- A. transaction characteristics
- B. session number
- C. port number

D. application layer payload

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

An administrator wants to upgrade an NGFW from PAN-OS® 7.1.2 to PAN-OS® 8.1.0. 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 70

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two.)

- A. HA1 IP Address
- B. Master Key
- C. Zone Protection Profile
- D. Network Interface Type

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:



QUESTION 71

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

What is the expected verdict from WildFire?

- A. Malware
- B. Grayware
- C. Phishing
- D. 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 the 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

Which User-ID method maps IP addresses to usernames for users connecting through a web proxy that has already authenticated the user?

- A. syslog listening
- B. server monitoring
- C. client probing
- D. port mapping

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 75

Which feature can provide NGFWs with User-ID mapping information?

- A. Web Captcha
- B. Native 802.1q authentication
- C. GlobalProtect
- D. Native 802.1x authentication

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)

- A. Role Based
- B. Custom Panorama Admin
- C. Device Group
- D. Dynamic
- E. Template Admin

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

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 78

Which logs enable a firewall administrator to determine whether a session was decrypted?

- A. Traffic
- B. Security Policy
- C. Decryption
- D. Correlated Event

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

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 80

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 81

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing, and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS® software?

- A. Antivirus update package.
- B. Applications and Threats update package.
- C. User-ID agent.
- D. WildFire update package.

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-an-ha-firewall-pair-to-pan-os-80>

QUESTION 82

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>

QUESTION 83

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons>

QUESTION 84

In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

- A. sg2 session count is the lowest compared to the other managed devices.
- B. us3 has a logging rate that deviates from the administrator-configured thresholds.
- C. uk3 has a logging rate that deviates from the seven-day calculated baseline.

<https://vceplus.com/>

D. sg2 has misconfigured session thresholds.

Correct Answer: C

Section: (none)

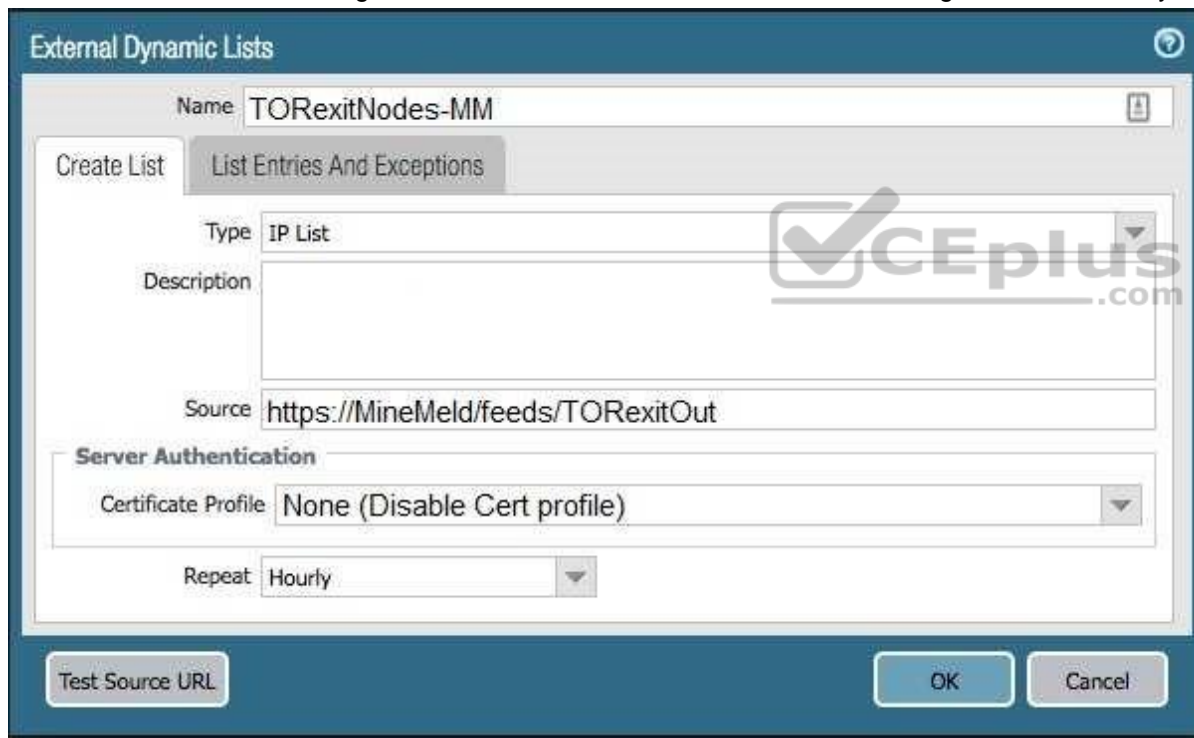
Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/panorama-features/device-monitoring-through-panorama>

QUESTION 85

The firewall is not downloading IP addresses from MineMeld. Based on the image, what most likely is wrong?



A. A Certificate Profile that contains the client certificate needs to be selected.

B. The source address supports only files hosted with an ftp://<address/file>.

- C. External Dynamic Lists do not support SSL connections.
- D. A Certificate Profile that contains the CA certificate needs to be selected.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://live.paloaltonetworks.com/t5/MineMeld-Articles/Connecting-PAN-OS-to-MineMeld-using-External-Dynamic-Lists/ta-p/190414>

QUESTION 86

Which three split tunnel methods are supported by a GlobalProtect Gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category



Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features/split-tunnel-for-public-applications>

QUESTION 87

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html>

QUESTION 88

SD-WAN is designed to support which two network topology types? (Choose two.)

- A. point-to-point
- B. hub-and-spoke
- C. full-mesh
- D. ring

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 89

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
- B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
- C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
- D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

QUESTION 90

Which two events trigger the operation of automatic commit recovery? (Choose two.)

- A. when an aggregate Ethernet interface component fails
- B. when Panorama pushes a configuration
- C. when a firewall performs a local commit
- D. when a firewall HA pair fails over

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

QUESTION 91

Panorama provides which two SD-WAN functions? (Choose two.)

- A. network monitoring
- B. control plane
- C. data plane
- D. physical network links

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

<https://vceplus.com/>