# PCNSE.exam.70q

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

**PCNSE**

**Palo Alto Networks Certified Network Security Engineer**

**Exam A**

**QUESTION 1**

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 2**

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

A. The settings assigned to the template that is on top of the stack.
B. The administrator will be promoted to choose the settings for that chosen firewall.
C. All the settings configured in all templates.

D. Depending on the firewall location, Panorama decides with settings to send.

**Correct Answer:** A
**Section: (none)**
**Explanation**
**Explanation/Reference:**

**QUESTION 3**
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 4**
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 5**

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 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 form 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?

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**
A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port which it connects.

How would an administrator configure the interface to 1Gbps?

A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
B. set deviceconfig system speed-duplex 1Gbps-duplex
C. set deviceconfig system speed-duplex 1Gbps-full-duplex
D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

**Correct Answer:** C
**Section: (none)**
**Explanation**

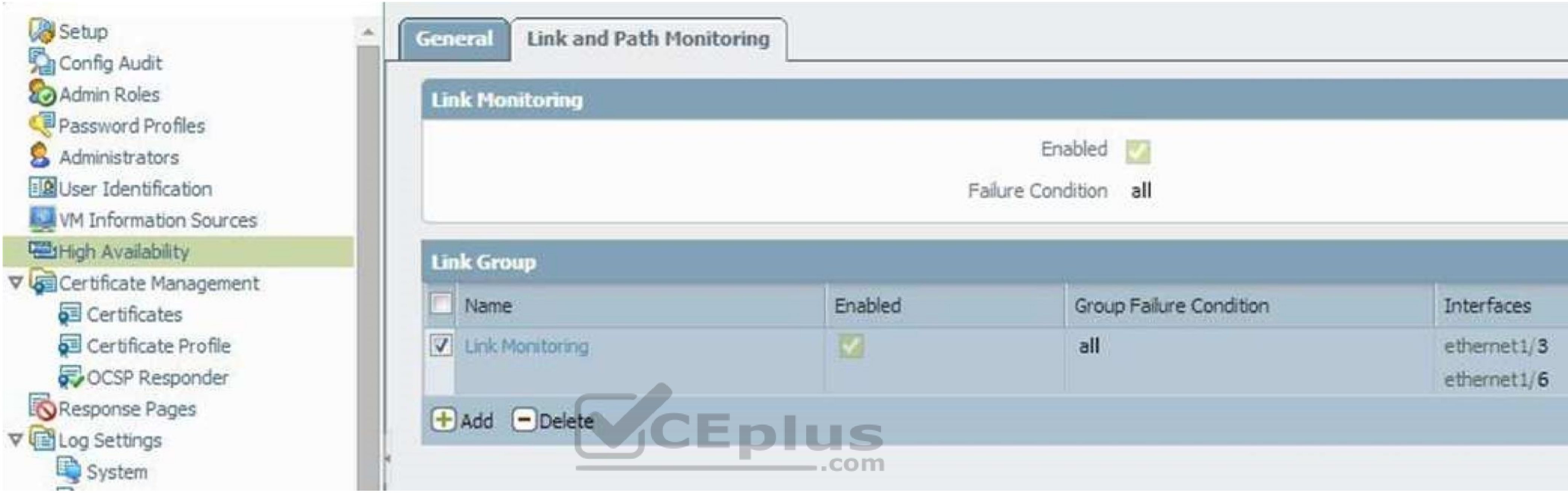
**Explanation/Reference:**
Reference: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034

**QUESTION 11**
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 we browsing access to the server.

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

A. application: web-browsing; service: application-default
B. application: web-browsing; service: service-https

C. application: ssl; service: any



**Link Monitoring**

Enabled ☑

Failure Condition all

**Link Group**

| □ | Name | Enabled | Group Failure Condition | Interfaces |
|---|---|---|---|---|
| ☑ | Link Monitoring | ☑ | all | ethernet1/3<br>ethernet1/6 |

D. application: web-browsing; service: (custom with destination TCP port 8080)

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 12**
If the firewall has the 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 13**
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. Redistribution of user mappings
C. Virtual Wire mode
D. Content inspection

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**
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 15**

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 16**

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 17**
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?

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 exported form the firewalls and manually imported into Panorama.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 18**
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 19**

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 20**

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**

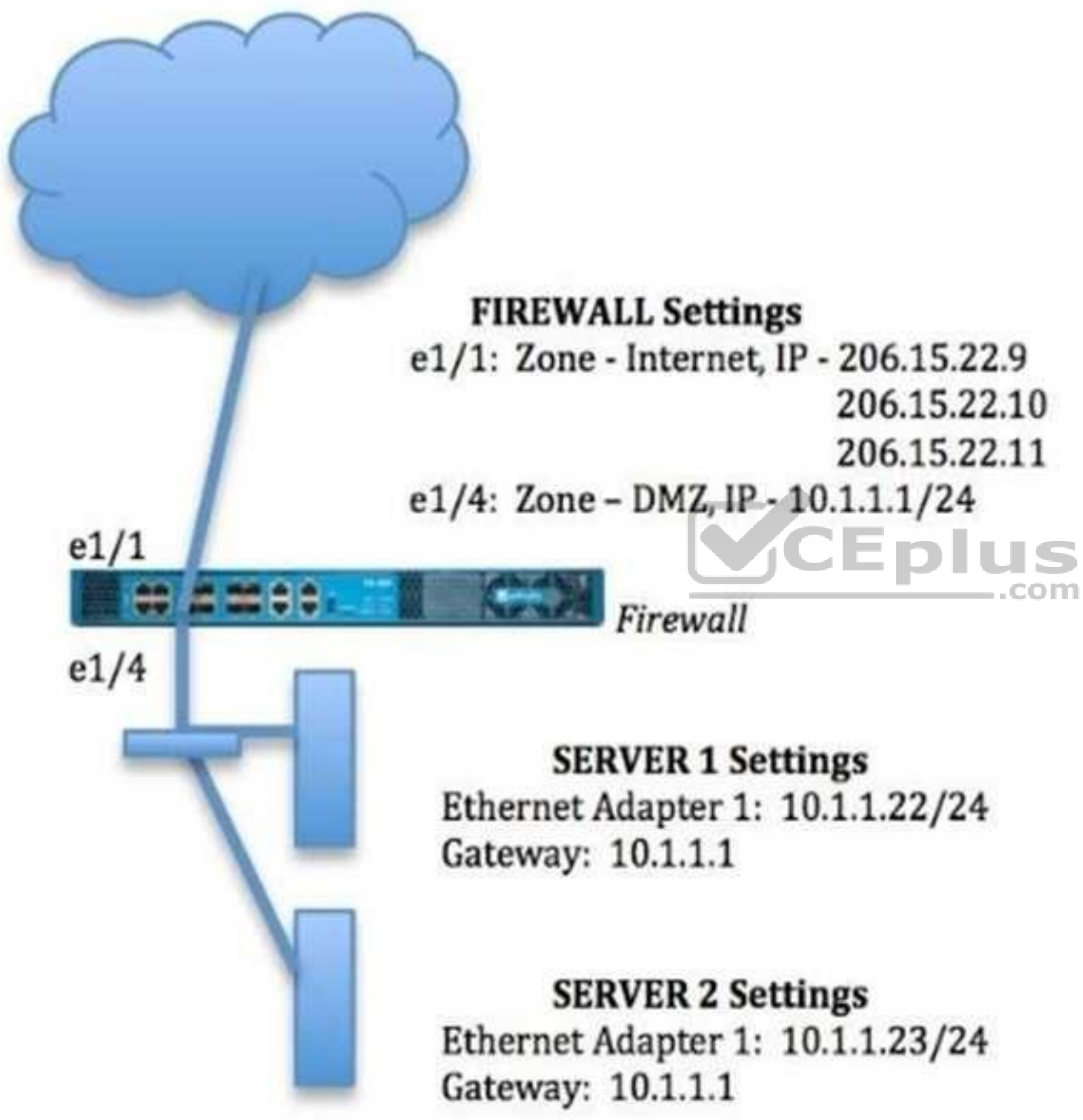
**Explanation/Reference:**

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

**QUESTION 21**

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?

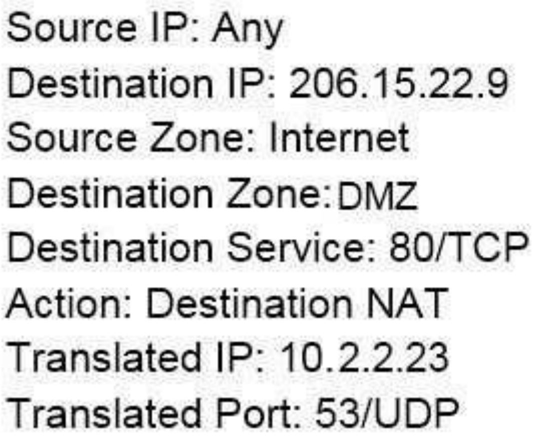


**FIREWALL Settings**
e1/1: Zone - Internet, IP - 206.15.22.9
206.15.22.10
206.15.22.11
e1/4: Zone – DMZ, IP - 10.1.1.1/24

**SERVER 1 Settings**
Ethernet Adapter 1: 10.1.1.22/24
Gateway: 10.1.1.1

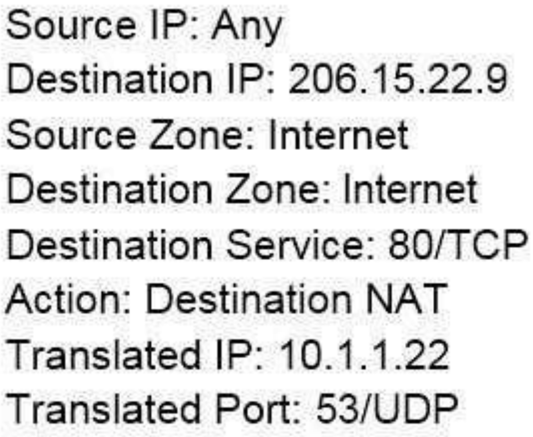
**SERVER 2 Settings**
Ethernet Adapter 1: 10.1.1.23/24
Gateway: 10.1.1.1

A.



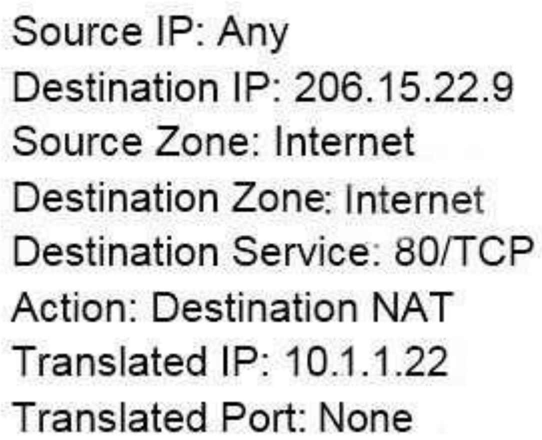
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B.



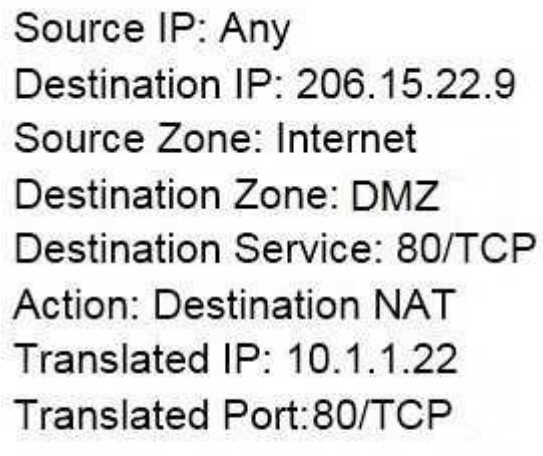
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C.



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

D.



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

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

**Correct Answer:** C

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
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:**

**QUESTION 23**
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

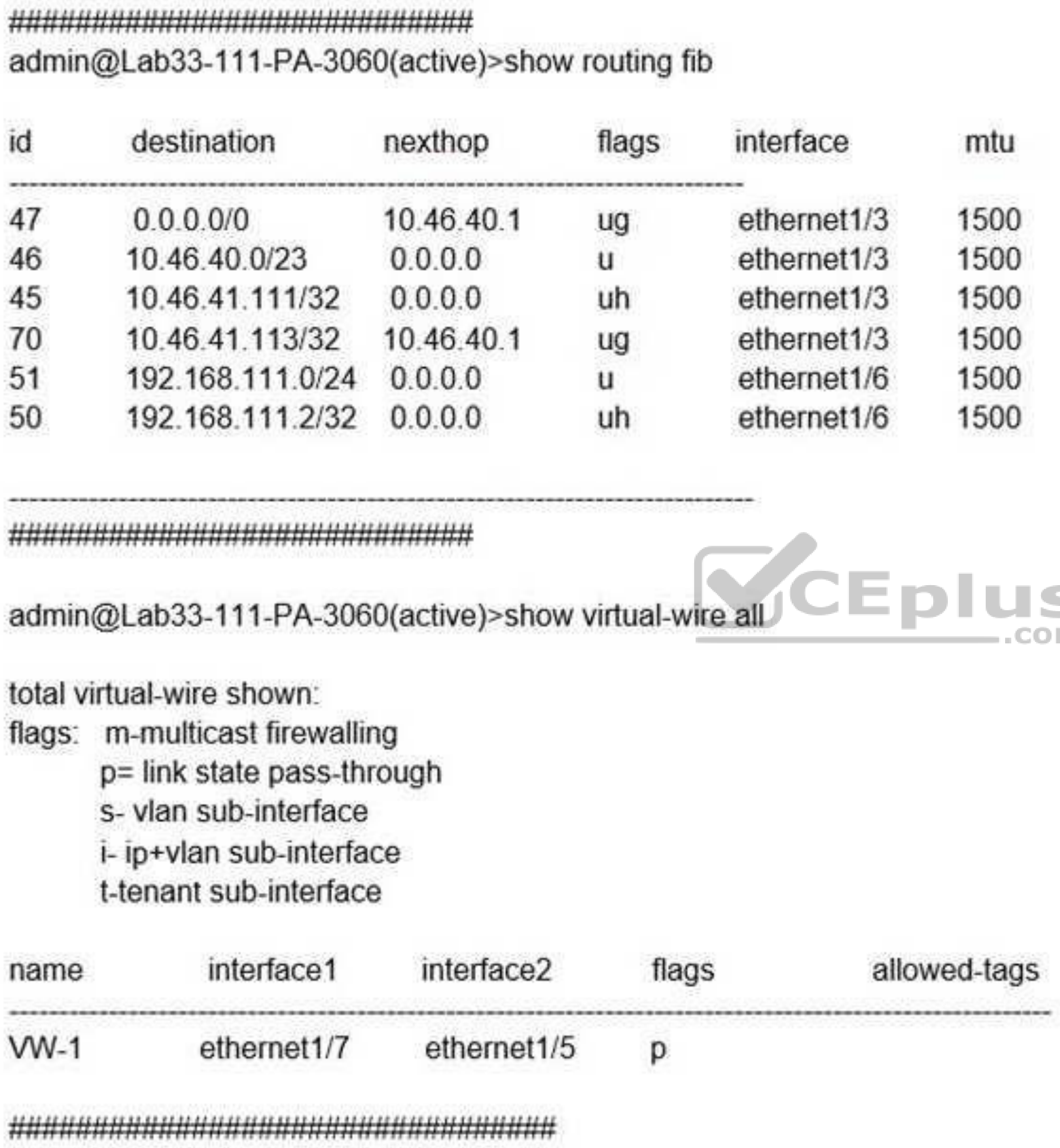
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar

**Correct Answer:** DEF
**Section: (none)**
**Explanation**
**Explanation/Reference:**

Reference: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

**QUESTION 24**

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:
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 25**
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 26**
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-amp-Tricks-How-to-Create-an-Application-Override/ta-p/65513

**QUESTION 27**
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?

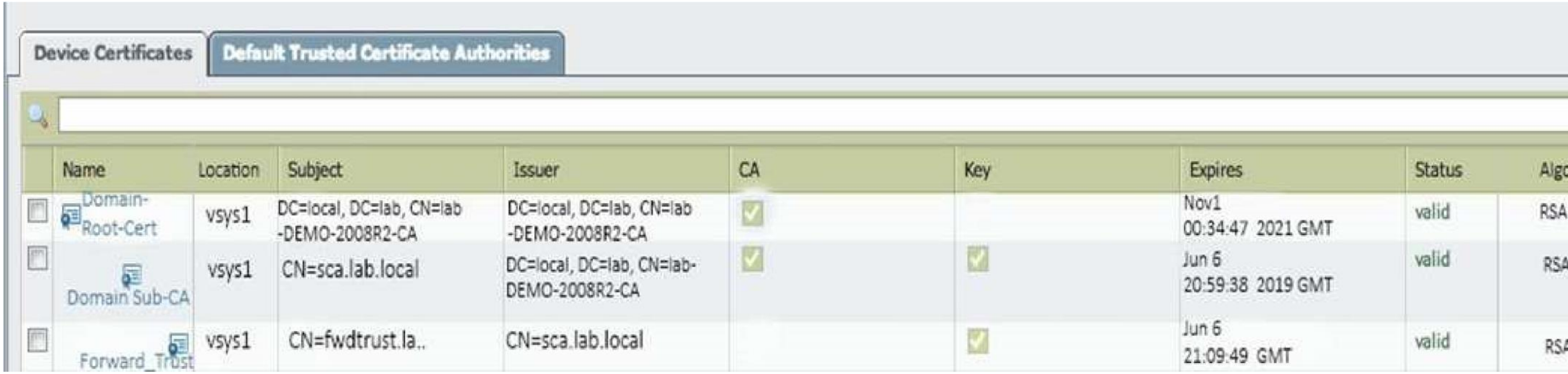
A. Create a decryption rule matching the encrypted BitTorrent traffic with action “No-Decrypt,” and place the rule at the top of the Decryption policy.
B. Create a Security policy rule that matches application “encrypted BitTorrent” and place the rule at the top of the Security policy.
C. Disable the 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 28**
Refer to the exhibit.
Which certificates can be used as a Forward Trust certificate?

A. Certificate from Default Trust Certificate Authorities
B. Domain Sub-CA
C. Forward_Trust
D. Domain-Root-Cert



Device Certificates | Default Trusted Certificate Authorities

| | Name | Location | Subject | Issuer | CA | Key | Expires | Status | Algo |
|---|---|---|---|---|---|---|---|---|---|
| □ | Domain-Root-Cert | vsys1 | DC=local, DC=lab, CN=lab -DEMO-2008R2-CA | DC=local, DC=lab, CN=lab -DEMO-2008R2-CA | ✓ | | Nov1 00:34:47 2021 GMT | valid | RSA |
| □ | Domain Sub-CA | vsys1 | CN=sca.lab.local | DC=local, DC=lab, CN=lab-DEMO-2008R2-CA | ✓ | ✓ | Jun 6 20:59:38 2019 GMT | valid | RSA |
| □ | Forward_Trust | vsys1 | CN=fwdtrust.la.. | CN=sca.lab.local | | ✓ | Jun 6 21:09:49 GMT | valid | RSA |

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 29**
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 Polices > 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-ssltls-service-profile

**QUESTION 30**
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 31**
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 32**
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 33**
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 34**
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 35**
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 36**
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?

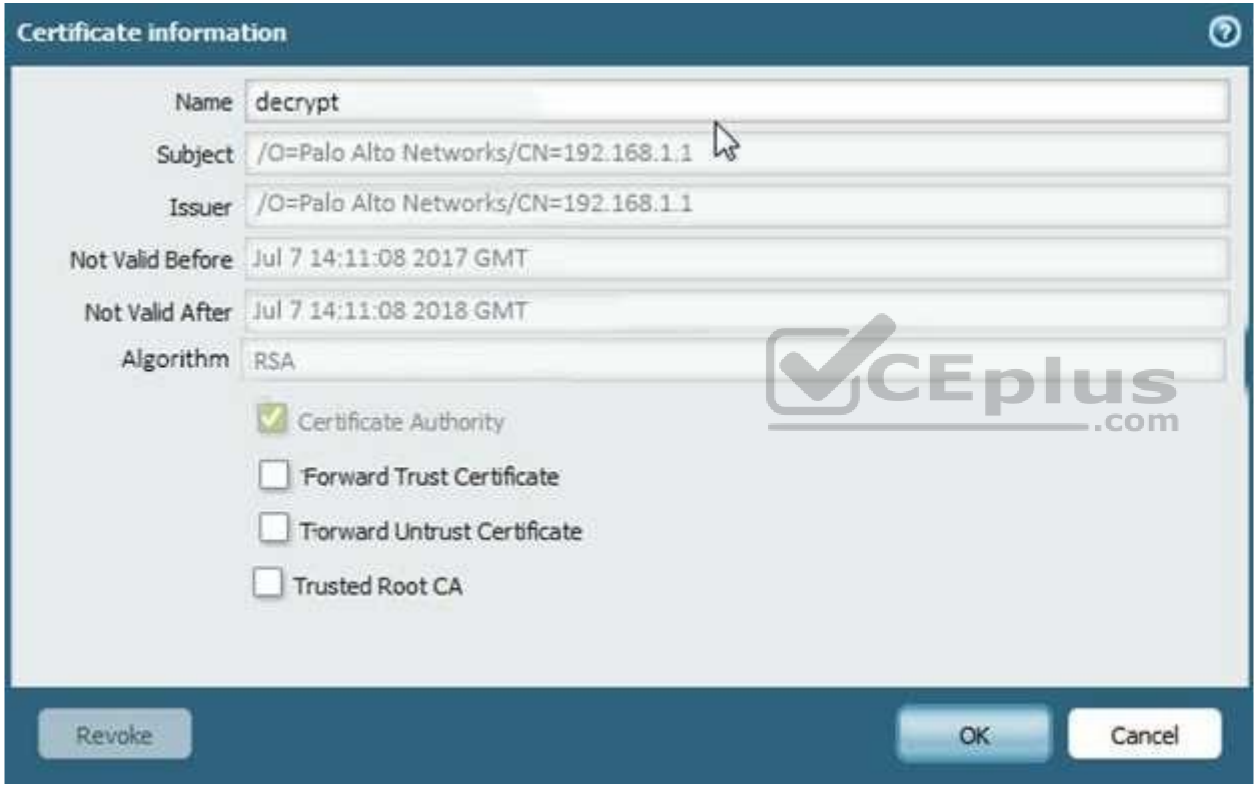
A. Session Browser
B. Application Command Center
C. TCP Dump
D. Packet Capture

**Correct Answer:** B

**Section: (none)**
**Explanation**

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

**QUESTION 37**
The certificate information displayed in the following image is for which type of certificate?



Certificate information

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

☑ Certificate Authority
☐ Forward Trust Certificate
☐ Forward Untrust Certificate
☐ Trusted Root CA

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 38**
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 39**
Which feature must you configure to prevent users form 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 40**

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 41**
If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto networks NGFW to inspect 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 42**
An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are form 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 43**
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 44**
Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

A. The firewall is in multi-vsys 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 45**
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 46**
An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in "the cloud"). Bootstrapping is the most expedient way to perform this task.

Which option describes deployment of a bootstrap package in an on-premise virtual environment?

A. Use config-drive on a USB stick.
B. Use an S3 bucket with an ISO.
C. Create and attach a virtual hard disk (VHD).
D. Use a virtual CD-ROM with an ISO.

**Correct Answer:** D
**Section: (none)**
**Explanation**
**Explanation/Reference:**
Reference: https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-onkvm/use-an-iso-file-to-deploy-the-vm-series-firewall

**QUESTION 47**

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 48**

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 49**

Which feature can be configured on VM-Series firewalls?
A. aggregate interfaces
B. machine learning
C. multiple virtual systems
D. GlobalProtect

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 50**
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 51**
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 52**
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 53**
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 54**
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 55**
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 56**
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 57**
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 58**
Which data flow describes redistribution of user mappings?

A. User-ID agent to firewall
B. Domain Controller to User-ID agent
C. User-ID agent to Panorama
D. firewall to firewall

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 59**
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 60**
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 61**
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 62**
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 63**
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 64**
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 65**
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 66**
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 67**
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-hafirewall-pair-to-pan-os-80

**QUESTION 68**
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 69**
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 70**
Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

A. GlobalProtect version 4.0 with PAN-OS 8.1
B. GlobalProtect version 4.1 with PAN-OS 8.1
C. GlobalProtect version 4.1 with PAN-OS 8.0
D. GlobalProtect version 4.0 with PAN-OS 8.0

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Reference: https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4_1/split-tunnelfor-public-applications