Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 8.0

https://www.2passeasy.com/dumps/PCNSE/

NEW QUESTION 1
What is the purpose of the firewall decryption broker?

A. Decrypt SSL traffic a then send it as cleartext to a security chain of inspection tools
B. Force decryption of previously unknown cipher suites
C. Inspection traffic within IPsec tunnel
D. Reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools

Answer: A

NEW QUESTION 2
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

Answer: C

NEW QUESTION 3
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

Answer: A

NEW QUESTION 4
Which administrative authentication method supports authorization by an external service?

A. Certificates
B. LDAP
C. RADIUS
D. SSH keys

Answer: C

NEW QUESTION 5
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.

Answer: A

NEW QUESTION 6
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
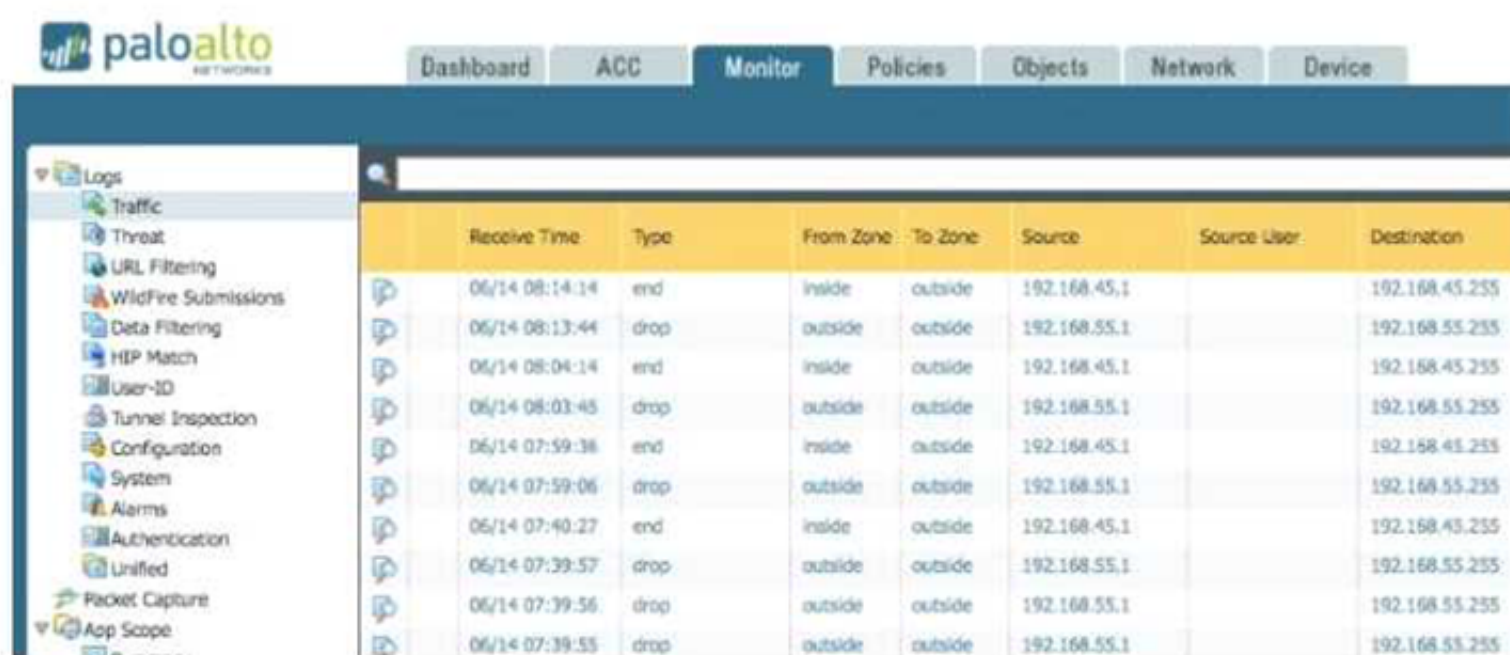
Answer: B

NEW QUESTION 7
An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A

B

C

05/23 20:49:30	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:49:29	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex
05/23 20:47:24	port	informational	link-change	ethernet1/1	Port ethernet1/1: Up 10Gb/s-full duplex
05/23 20:47:22	port	informational	link-change	MGT	Port MGT: Up Unknown
05/23 20:47:18	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:47:17	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex

D

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D

Answer: AD

NEW QUESTION 8
Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy? (Choose two.)

A. Create a no-decrypt Decryption Policy rule.
B. Configure an EDL to pull IP addresses of known sites resolved from a CRL.
C. Create a Dynamic Address Group for untrusted sites
D. Create a Security Policy rule with vulnerability Security Profile attached.
E. Enable the "Block sessions with untrusted issuers" setting.

Answer: AD

NEW QUESTION 9
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. 99
B. 1
C. 255

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.pdf (page 9)

NEW QUESTION 10
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

Answer: C

NEW QUESTION 10
Refer to the exhibit.
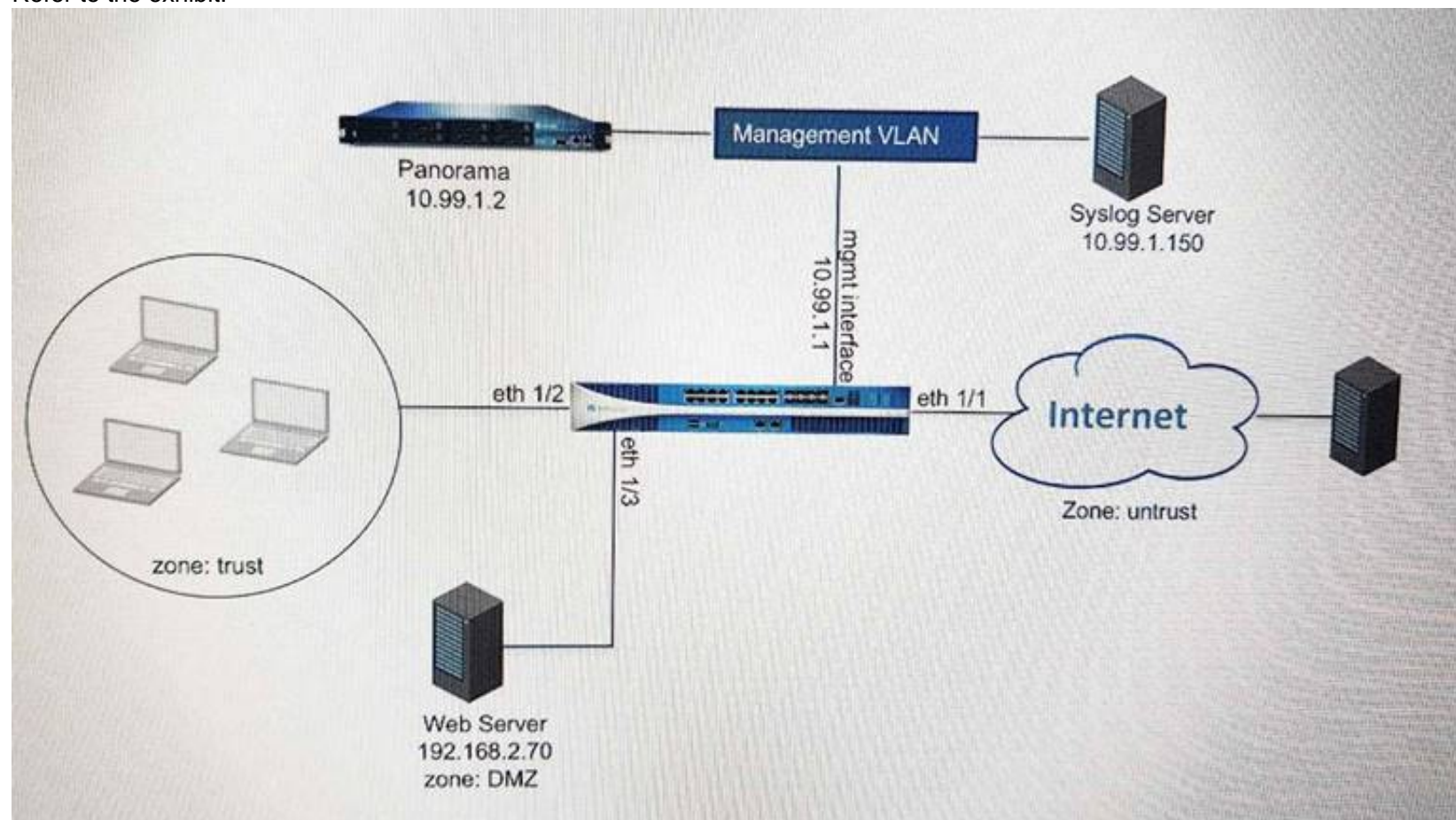
An administrator cannot see any of the Traffic logs from the Palo Alto Networks NGFW on Panorama. The configuration problem seems to be on the firewall side.
Where is the best place on the Palo Alto Networks NGFW to check whether the configuration is correct?
A)

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

B)

Security Policy Rule

General	Source	User	Destination	Application	Service/URL Category	Actions

Action Setting

Action Allow ▼

☐ Send ICMP Unreachable

Profile Setting

Profile Type	Profiles ▼
Antivirus	None ▼
Vulnerability Protection	None ▼
Anti-Spyware	None ▼
URL Filtering	Filter1 ▼
File Blocking	None ▼
Data Filtering	None ▼
WildFire Analysis	None ▼

Log Setting

☑ Log at Session Start
☑ Log at Session End

Log Forwarding None ▼

Other Settings

Schedule	None ▼
QoS Marking	None ▼

☐ Disable Server Response Inspection

OK   Can

C)

Syslog Server Profile

Name SyslogProfile1

Servers	Custom Log Format

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

➕ Add ➖ Delete

D)

Panorama Settings

Receive Timeout for Connection to Device (sec)	240
Send Timeout for Connection to Device (sec)	240
Retry Count for SSL Send to Device	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	🔍	0 items

| ☐ | Identifier | Type | Value |

➕ Add ➖ Delete

☐ Authorize Clients Based on Serial Number

☐ Check Authorization List

| onnect Wait Time (min) | [0 - 44640] |

OK

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

Answer: D

NEW QUESTION 14
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

Answer: C

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/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals

NEW QUESTION 18
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

Answer: B

Explanation:

Reference: https://www.paloaHYPERLINK
"https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence"ltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

NEW QUESTION 20
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

Answer: BD

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

NEW QUESTION 21
Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x- enabled wireless network device that has no native integration with PAN-OS® software?

A. XML API
B. Port Mapping
C. Client Probing
D. Server Monitoring

Answer: A

Explanation:
Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a
third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/user-id-concepts

NEW QUESTION 25
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

Answer: C

NEW QUESTION 29
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 invali
B. The Profile Settings section will be grayed out when the Action is set to "Deny".
C. The configuration will allow the matched session unless a vulnerability signature is detecte
D. The "Deny" action will supersede theper-severity defined actions defined in the associated Vulnerability Protection Profile.
E. The configuration is invali
F. It will cause the firewall to skip this Security policy rul
G. A warning will be displayed during a commit.
H. The configuration is vali
I. It will cause the firewall to deny the matched session
J. Any configured Security Profiles have no effect ifthe Security policy rule action is set to "Deny."

Answer: B

NEW QUESTION 32
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.

Answer: C

NEW QUESTION 36
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

Answer: BC

NEW QUESTION 41
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 EIGRPprotocols)
D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Answer: C

NEW QUESTION 42
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

Answer: B

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

NEW QUESTION 43
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
D. application: web-browsing; service: (custom with destination TCP port 8080)

Answer: A

NEW QUESTION 47
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

Answer: C

NEW QUESTION 48
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.

Answer: B
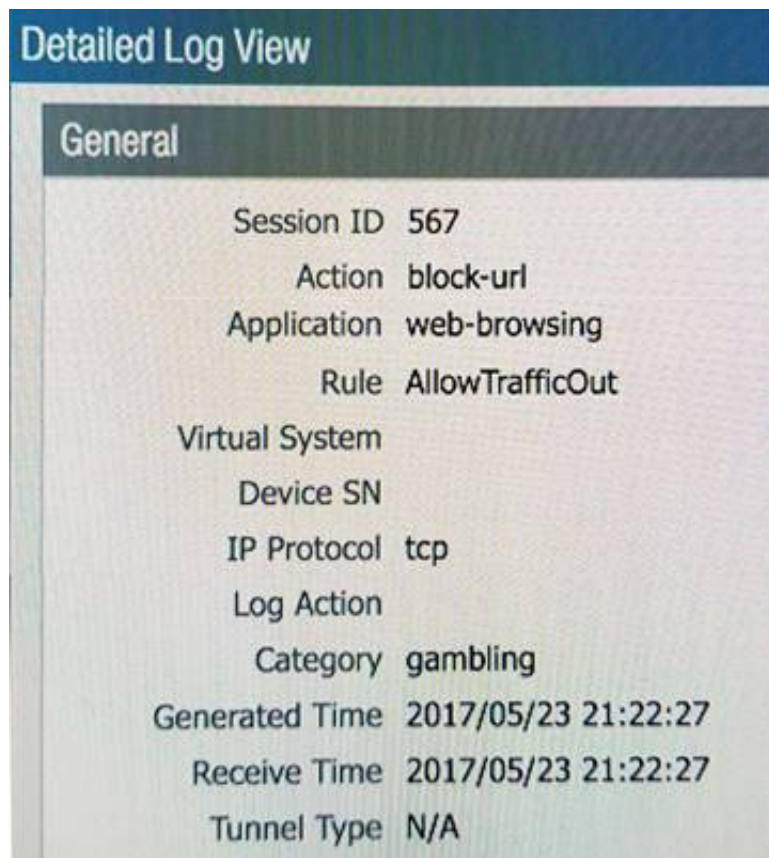
NEW QUESTION 52
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image. Which configuration change should the administrator make?
A)

Detailed Log View

General

Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A

B)

URL Filtering Profile

Name Filter1
Description

Overrides | Categories | URL Filtering Settings | User Credential Detection

65 items

Category	Site Access	User Credential Submission
educational-institutions	allow	allow
entertainment-and-arts	allow	allow
extremism	allow	allow
financial-services	allow	allow
✓ gambling	allow	block
games	alert	allow
government	allow	allow
hacking	block	allow
health-and-medicine	continue	allow
home-and-garden	override	allow
hunting-and-fishing	allow	allow

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

Check URL Category

C)

Security Policy Rule

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

Name www.megamillions.com
Rule Type universal (default)
Description

D)

URL Filtering Profile

Name Filter1

Description

Overrides | Categories | URL Filtering Settings | User Credential Detection

Allow List www.megamillions.com

Block List

Action continue

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

OK

E)

URL Filtering Profile

Name Filter1

Description

Overrides | Categories | URL Filtering Settings | User Credential Detection
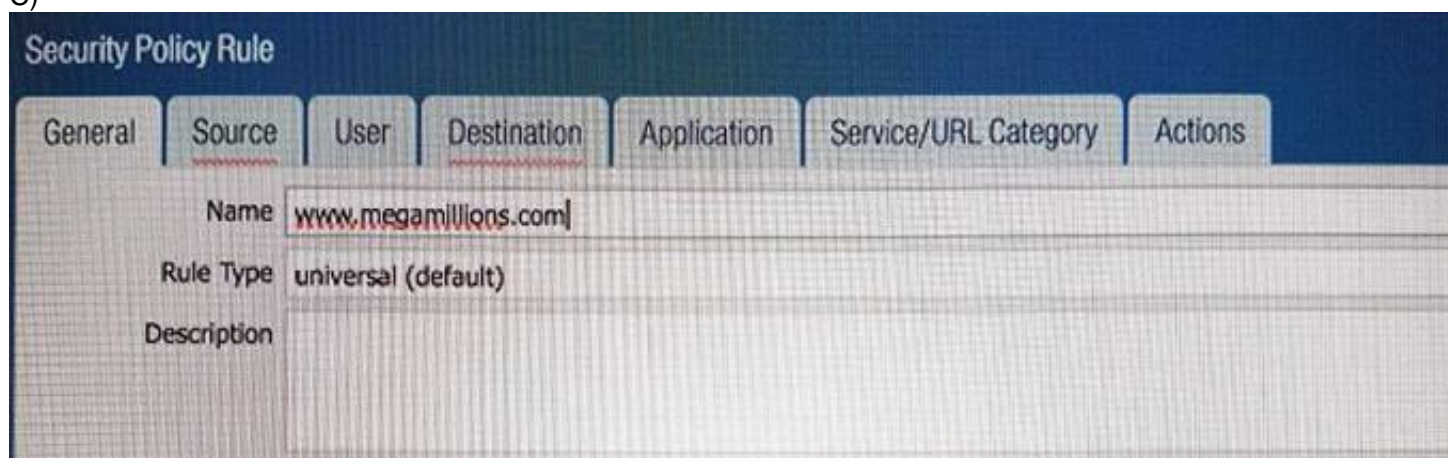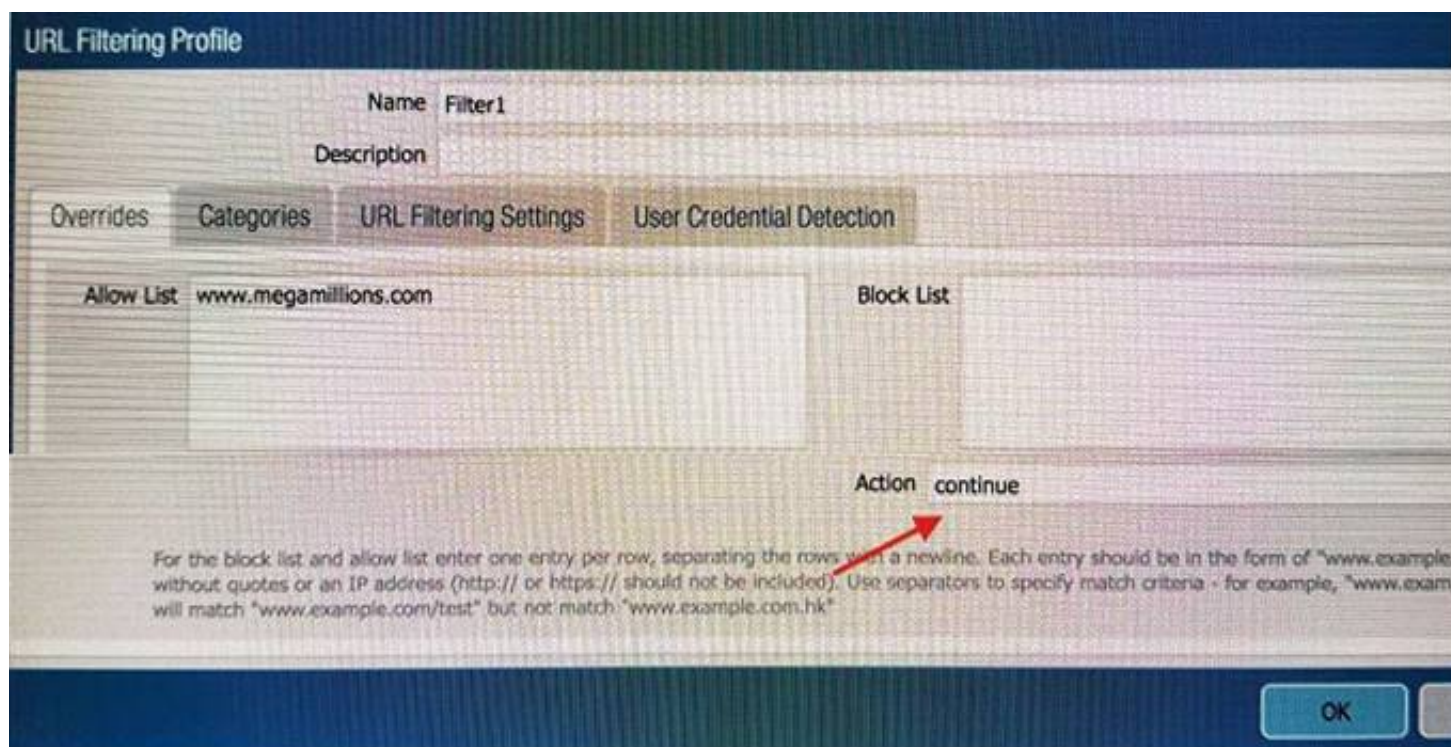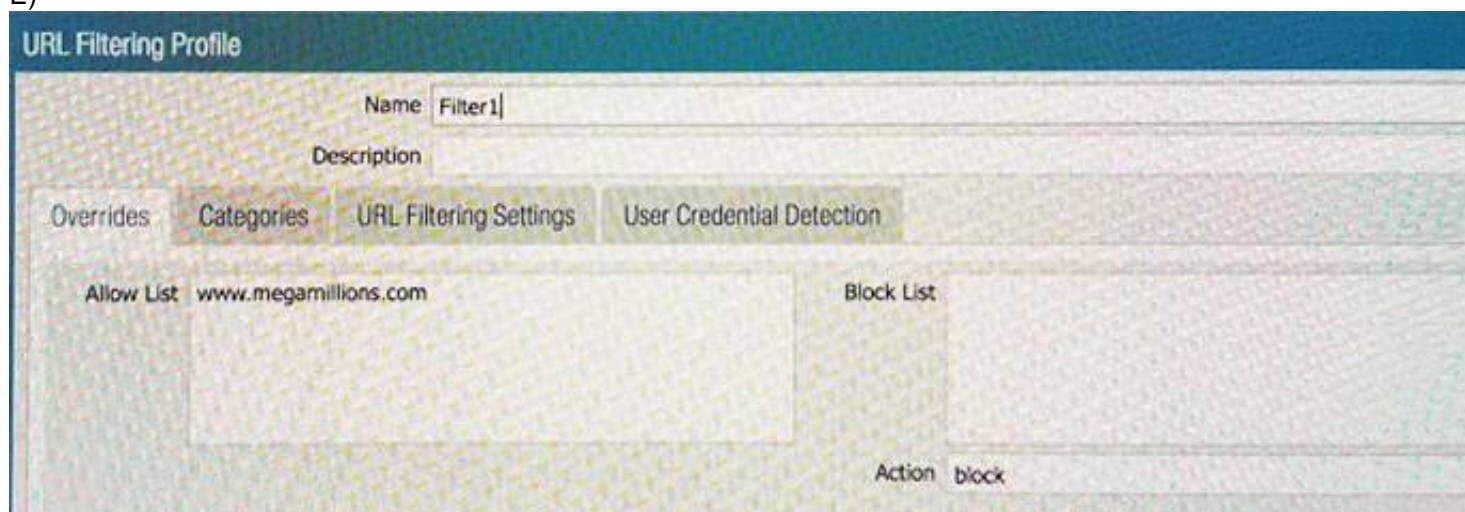
Allow List www.megamillions.com

Block List

Action block

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

Answer: B

NEW QUESTION 53
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

Answer: ADE

NEW QUESTION 55
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.
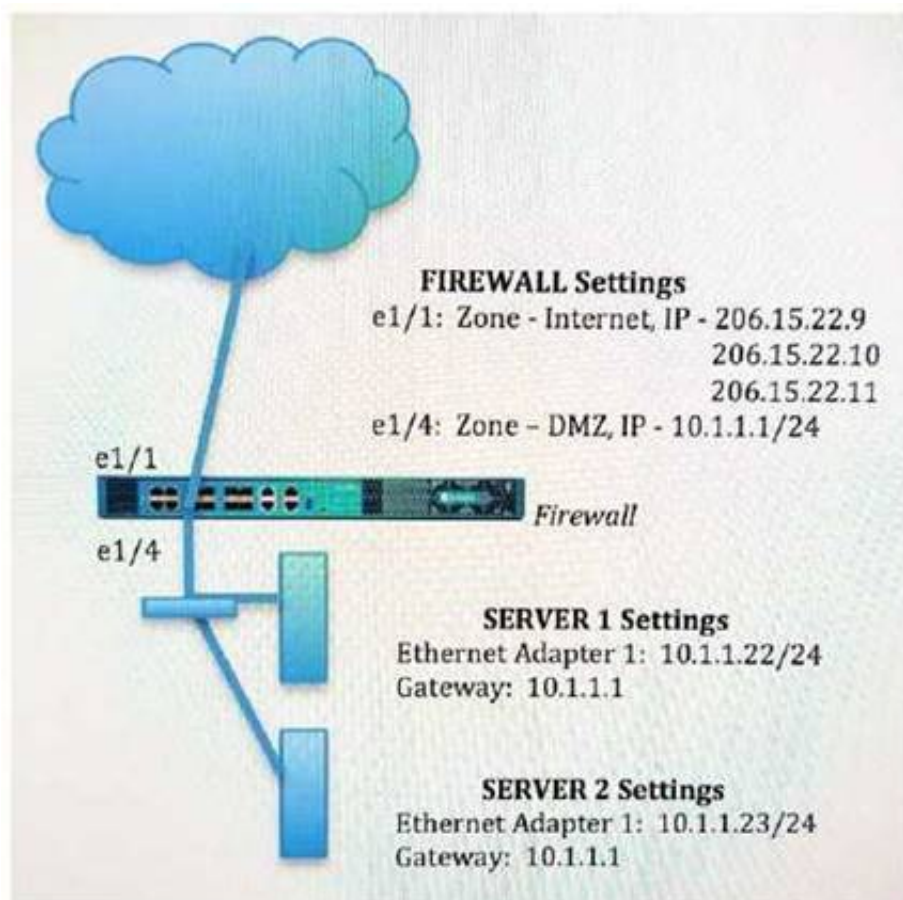How quickly will the firewall receive back a verdict?

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

Answer: D

NEW QUESTION 57
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

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

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

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

Answer: D

NEW QUESTION 59
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

Answer: A

NEW QUESTION 60
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.

Answer: A

NEW QUESTION 61
If the firewall is configured for credential phishing prevention using the "Domain Credential Filter" method, which login will be detected as credential theft?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 66
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

Answer: B

NEW QUESTION 68
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

Answer: D

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

NEW QUESTION 72
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.

Answer: D

NEW QUESTION 75
Refer to the exhibit.

Which certificates can be used as a Forwarded Trust certificate?

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

Answer: A

NEW QUESTION 80
Which 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

Answer: D

NEW QUESTION 82
Which CLI command can be used to export the tcpdump capture?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 86
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.

Answer: D

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

NEW QUESTION 87
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

Answer: BCD

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite
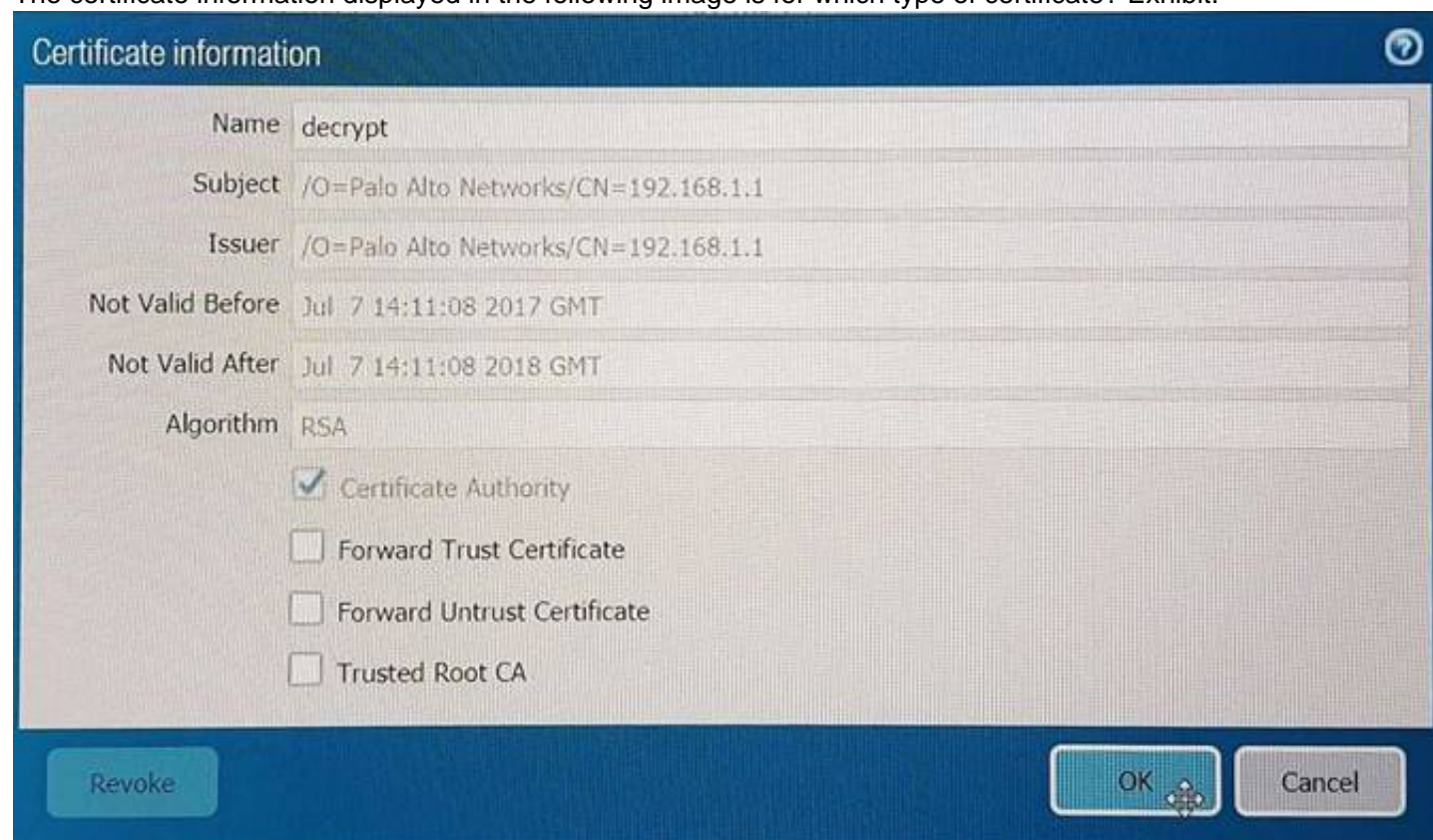
NEW QUESTION 91

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.

Answer: BD

NEW QUESTION 93
The certificate information displayed in the following image is for which type of certificate? Exhibit:

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

Answer: D

NEW QUESTION 98
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.

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administ er-panorama/back-up-panorama-and-firewall-configurations

NEW QUESTION 99
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.

Answer: A

NEW QUESTION 101
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.

Answer: CD

NEW QUESTION 105
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.

Answer: AB

NEW QUESTION 106
Which virtual router feature determines if a specific destination IP address is reachable?

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

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf

NEW QUESTION 109
An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.
Which interface type and license feature are necessary to meet the requirement?

A. Decryption Mirror interface with the Threat Analysis license
B. Virtual Wire interface with the Decryption Port Export license
C. Tap interface with the Decryption Port Mirror license
D. Decryption Mirror interface with the associated Decryption Port Mirror license

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring

NEW QUESTION 111
An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port. Which log entry can the administrator use to verify that
sessions are being decrypted?

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

Answer: A

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

NEW QUESTION 116
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.

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management

NEW QUESTION 121
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


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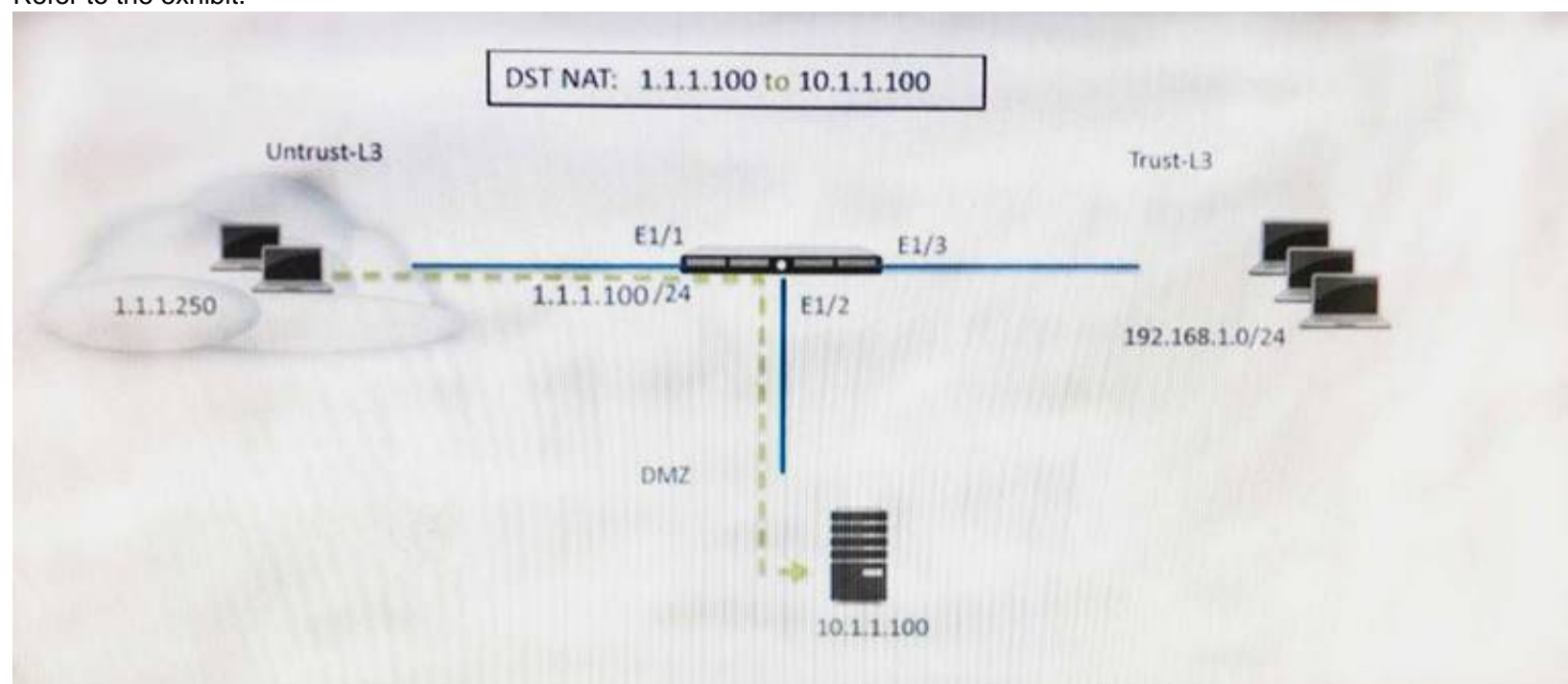
What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

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

Answer: D

NEW QUESTION 125
Refer to the exhibit.

A web server in the DMZ is being mapped to a public address through DNAT. Which Security policy rule will allow traffic to flow to the web server?

A. Untrust (any) to Untrust (10. 1.1. 100), web browsing – Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing – Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing – Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing – Allow

Answer: B

NEW QUESTION 129
A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from

the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.
Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web- browsing traffic to this server on tcp/443.

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

Answer: A

NEW QUESTION 130
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%.

Answer: BC

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

NEW QUESTION 134
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

Answer: A

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

NEW QUESTION 136
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. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

NEW QUESTION 137
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

A. Verify AutoFocus status using CLI.
B. Check the WebUI Dashboard AutoFocus widget.
C. Check for WildFire forwarding logs.
D. Check the license
E. Verify AutoFocus is enabled below Device Management tab.

Answer: BD

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

NEW QUESTION 140
Which CLI command enables an administrator to check the CPU utilization of the dataplane?

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

Answer: A

NEW QUESTION 142
Which DoS protection mechanism detects and prevents session exhaustion attacks?

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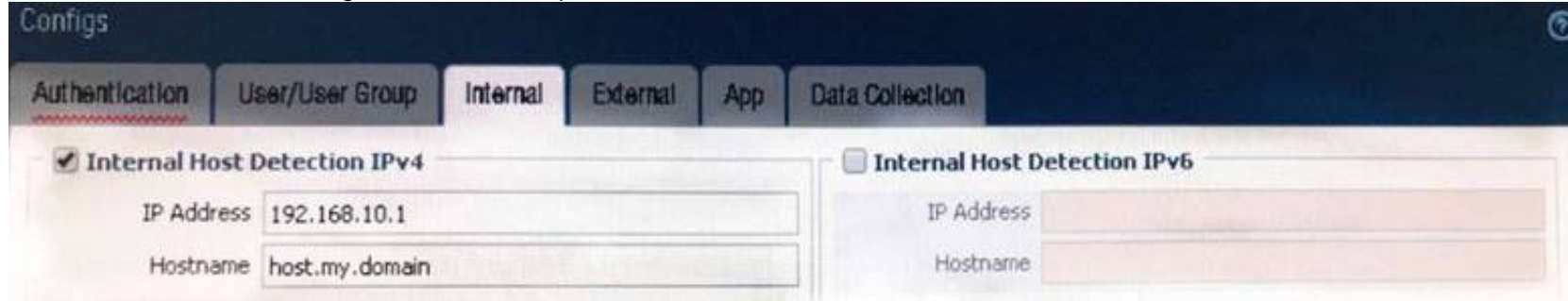C. Resource Protection
D. TCP Port Scan Protection

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

NEW QUESTION 147
View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

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

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

NEW QUESTION 150
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. Mastered
B. Not Mastered

Answer: A

Explanation:

Dependencies : Before upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS Upgrade. Reference: https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS- Upgrade/ta-p/111045

NEW QUESTION 152
An administrator sees several inbound sessions identified as unknown-tcp in the traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this as their accounting application and to scan this traffic for threats. Which option would achieve this result?

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

Answer: A

NEW QUESTION 155
Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

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

Answer: C

NEW QUESTION 159
Which data flow describes redistribution of user mappings?

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

Answer: B

NEW QUESTION 163
Which two features does PAN-OS® software use to identify applications? (Choose two)

A. port number
B. session number
C. transaction characteristics
D. application layer payload

Answer: CD

NEW QUESTION 165
Which four NGFW multi-factor authentication factors are supported by PAN-OSS? (Choose four.)

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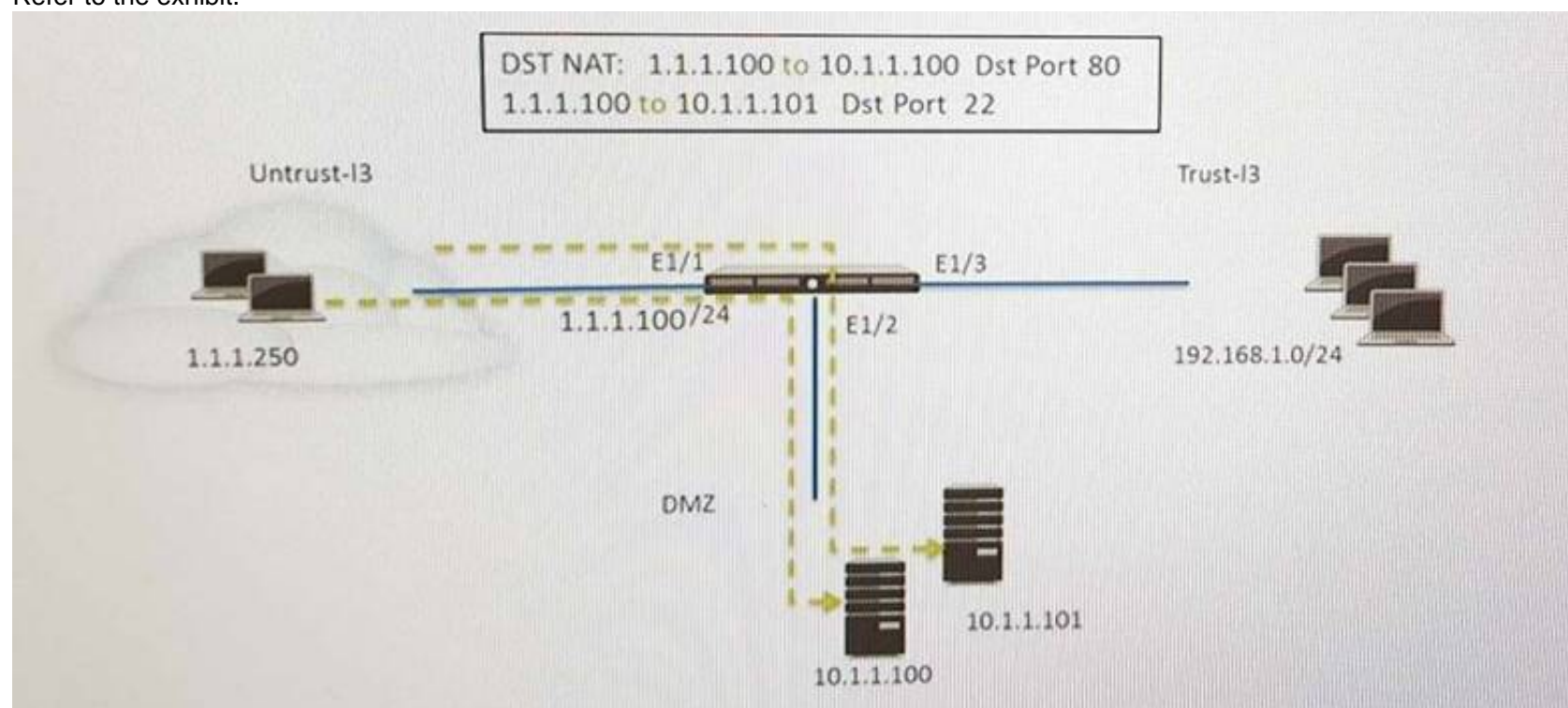D. SSH keyE.One-Time Password F.Voice

Answer: BCEF

NEW QUESTION 170
Which three firewall states are valid? (Choose three)

A. Suspended
B. Passive
C. Active
D. Pending E.Functional

Answer: ABC

NEW QUESTION 173
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) received 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) Ssh-Allow
B. Untrust (Any) to DMZ (1.1.1.100) Ssh-Allow
C. Untrust (Any) to DMZ (1.1.1.100) Web-browsing -Allow
D. Untrust (Any) to Untrust (10.1.1.1) Web-browsing -Allow

Answer: CD

NEW QUESTION 175
An administrator has configured a QoS policy rule and a QoS profile that limits the maximum allowable bandwidth for the YouTube application. However , YouTube is consuming more than the maximum bandwidth allotment configured.
Which configuration step needs to be configured to enable QoS?

A. Enable QoS Data Filtering Profile

B. Enable QoS monitor
C. Enable Qos interface
D. Enable Qos in the interface Management Profile.

Answer: C

NEW QUESTION 179
Which feature can provide NGFWs with User-ID mapping information?

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

Answer: A

NEW QUESTION 181
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 action after enough packets allow for App-IDidentification
B. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port numbers Use ofan "application" allows the firewall to take action after enough packets allow for App-ID identification regardless of the portsbeing used.
C. There are no differences between "service" or "application" Use of an "application" simplifies configuration by allowing use ofa friendly application name instead of port numbers.
D. Use of a "service" enables the firewall to take immediate action with the first observed packet based on port number
E. Use ofan "application" allows the firewall to take immediate action it the port being used is a member of the application standardport list

Answer: B

NEW QUESTION 184
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. Gray ware
B. Malware
C. Spyware
D. Phishing

Answer: A

NEW QUESTION 186
In which two types of deployment is active/active HA configuration supported? (Choose two.)

A. TAP mode
B. Layer 2 mode
C. Virtual Wire mode
D. Layer 3 mode

Answer: CD

NEW QUESTION 191
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. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
B. Add QoS Profiles to throttle incoming requests
C. Add a tuned DoS Protection Profile
D. Add an Anti-Spyware Profile to block attacking IP address

Answer: C

NEW QUESTION 196
Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

A. Select download-and-install.
B. Select download-and-install, with "Disable new apps in content update" selected.
C. Select download-only.
D. Select disable application updates and select "Install only Threat updates"

Answer: C

NEW QUESTION 201
Which Zone Pair and Rule Type will allow a successful connection for a user on the internet zone to a web server hosted in the DMZ zone? The web server is reachable using a destination Nat policy in the Palo Alto Networks firewall.
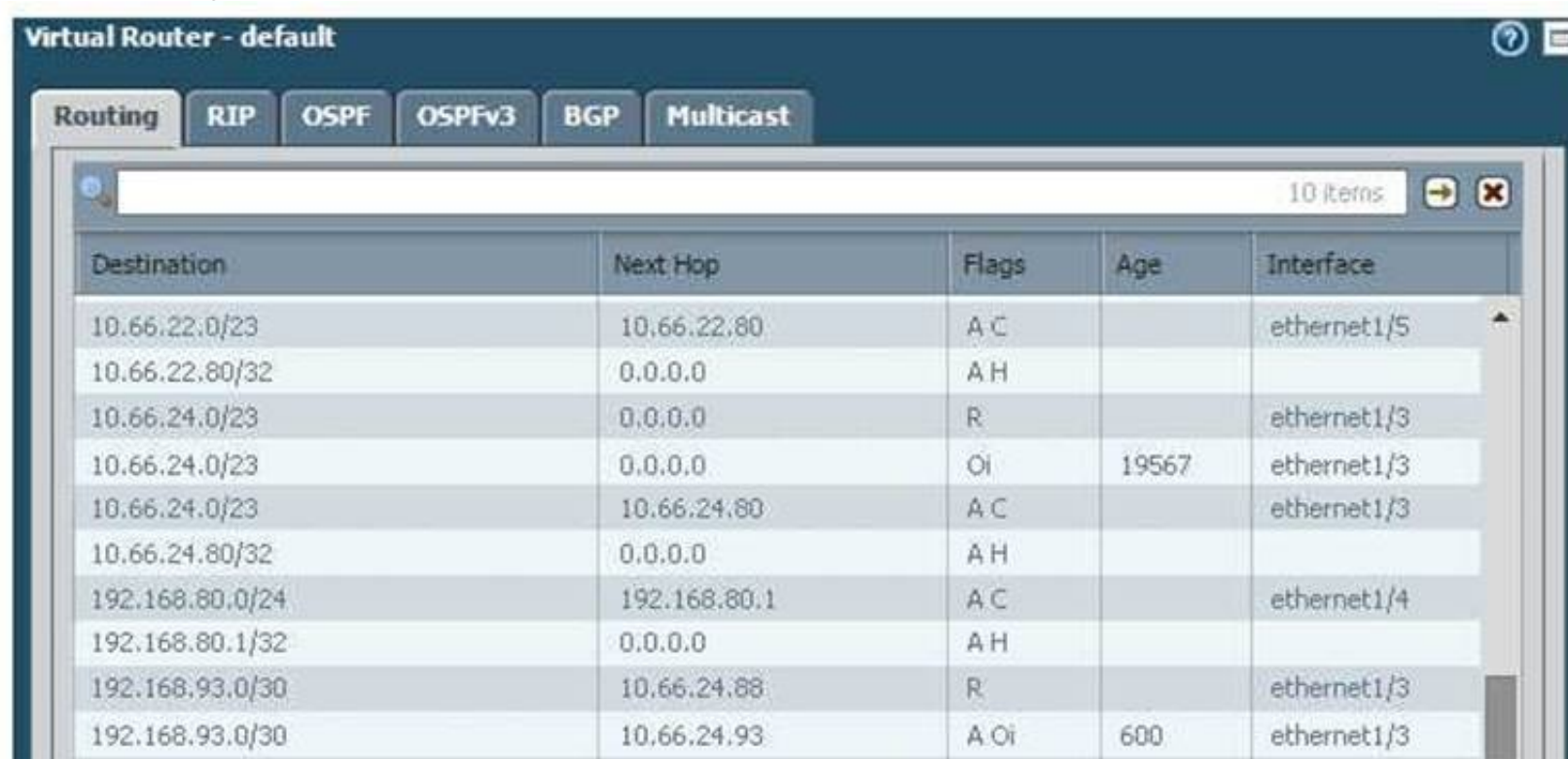
A. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:"intrazone"
B. Zone Pair:Source Zone: Internet Destination Zone: DMZ Rule Type:"intrazone" or "universal"
C. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:"intrazone" or "universal"
D. Zone Pair:Source Zone: Internet Destination Zone: Internet Rule Type:"intrazone"

Answer: B

NEW QUESTION 205
Given the following table.

Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network?

A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.
B. Configuring the metric for RIP to be higher than that of OSPF Int.
C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.
D. Configuring the metric for RIP to be lower than that OSPF Ext.

Answer: A

NEW QUESTION 207
A company is upgrading its existing Palo Alto Networks firewall from version 7.0.1 to 7.0.4.
Which three methods can the firewall administrator use to install PAN-OS 8.0.4 across the enterprise?(Choose three)

A. Download PAN-OS 8.0.4 files from the support site and install them on each firewall after manually uploading.
B. Download PAN-OS 8.0.4 to a USB drive and the firewall will automatically update after the USB drive is inserted in the firewall.
C. Push the PAN-OS 8.0.4 updates from the support site to install on each firewall.
D. Push the PAN-OS 8.0.4 update from one firewall to all of the other remaining after updating one firewall.
E. Download and install PAN-OS 8.0.4 directly on each firewall.
F. Download and push PAN-OS 8.0.4 from Panorama to each firewall.

Answer: ACF

NEW QUESTION 212
Which three fields can be included in a pcap filter? (Choose three)

A. Egress interface
B. Source IP
C. Rule number
D. Destination IP
E. Ingress interface

Answer: BCD

Explanation:
(https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta- p/72069)

NEW QUESTION 213
A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.
Which CLI command will help identify the issue?

A. test routing fib virtual-router vr1
B. show routing route type static destination 98.139.183.24
C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
D. show routing interface

Answer: C

NEW QUESTION 214
Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two)

A. Configure the management interface as HA3 Backup
B. Configure Ethernet 1/1 as HA1 Backup
C. Configure Ethernet 1/1 as HA2 Backup
D. Configure the management interface as HA2 Backup
E. Configure the management interface as HA1 Backup
F. Configure ethernet1/1 as HA3 Backup

Answer: BE

NEW QUESTION 219
Click the Exhibit button
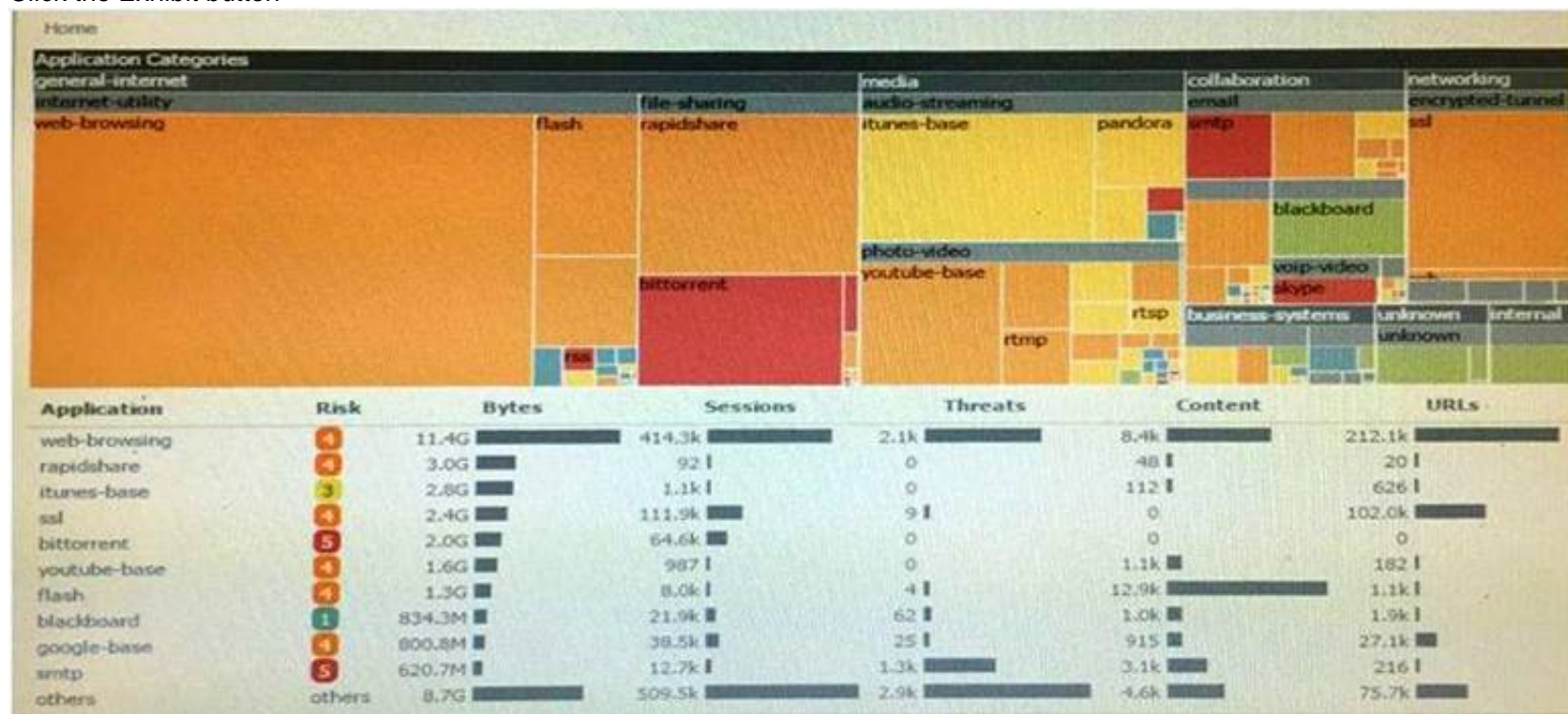
An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.
What would be the administrator's next step?

A. Right-Click on the bittorrent link and select Value from the context menu
B. Create a global filter for bittorrent traffic and then view Traffic logs.
C. Create local filter for bittorrent traffic and then view Traffic logs.
D. Click on the bittorrent application link to view network activity

Answer: D

NEW QUESTION 220
Which command can be used to validate a Captive Portal policy?

A. eval captive-portal policy <criteria>
B. request cp-policy-eval <criteria>
C. test cp-policy-match <criteria>
D. debug cp-policy <criteria>

Answer: C

NEW QUESTION 225
The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.
Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

A. test panoramas-connect 10.10.10.5
B. show panoramas-status
C. show arp all I match 10.10.10.5
D. topdump filter "host 10.10.10.5
E. debug dataplane packet-diag set capture on

Answer: BD

NEW QUESTION 226
Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon?

A. Certificate revocation list
B. Trusted root certificate
C. Machine certificate
D. Online Certificate Status Protocol

Answer: C

NEW QUESTION 228
Which three log-forwarding destinations require a server profile to be configured? (Choose three)

A. SNMP Trap
B. Email
C. RADIUS
D. Kerberos
E. Panorama
F. Syslog

Answer: ABF

NEW QUESTION 232
A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled. Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment?

A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkhole
B. File Blocking profiles applied to outbound security policies with action set to alert
C. Vulnerability Protection profiles applied to outbound security policies with action set to block
D. Antivirus profiles applied to outbound security policies with action set to alert

Answer: A

NEW QUESTION 236
How does Panorama handle incoming logs when it reaches the maximum storage capacity?

A. Panorama discards incoming logs when storage capacity full.
B. Panorama stops accepting logs until licenses for additional storage space are applied
C. Panorama stops accepting logs until a reboot to clean storage space.
D. Panorama automatically deletes older logs to create space for new ones.

Answer: D

Explanation:
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up- panorama/determine-panorama-log-storage-requirements)

NEW QUESTION 241
Only two Trust to Untrust allow rules have been created in the Security policy Rule1 allows google-base
Rule2 allows youtube-base
The youtube-base App-ID depends on google-base to function. The google-base App-ID implicitly uses SSL and web-browsing. When user try to accesss https://www.youtube.com in a web browser, they get an error indecating that the server cannot be found.
Which action will allow youtube.com display in the browser correctly?

A. Add SSL App-ID to Rule1
B. Create an additional Trust to Untrust Rule, add the web-browsing, and SSL App-ID's to it
C. Add the DNS App-ID to Rule2
D. Add the Web-browsing App-ID to Rule2

Answer: C

NEW QUESTION 246
Which three options are available when creating a security profile? (Choose three)

A. Anti-Malware
B. File Blocking
C. Url Filtering
D. IDS/ISP
E. Threat Prevention
F. Antivirus

Answer: ABF

NEW QUESTION 250
Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two)

A. Vulnerability Object
B. DoS Protection Profile
C. Data Filtering Profile
D. Zone Protection Profile

Answer: BD

NEW QUESTION 253
The IT department has received complaints abou VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter.
Which feature can be used to identify, in real time, the applications taking up the most bandwidth?

A. QoS Statistics
B. Applications Report
C. Application Command Center (ACC)
D. QoS Log

Answer: A

NEW QUESTION 257
A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.
Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network?

A. Zone Protection Policy with UDP Flood Protection
B. QoS Policy to throttle traffic below maximum limit
C. Security Policy rule to deny trafic to the IP address and port that is under attack
D. Classified DoS Protection Policy using destination IP only with a Protect action

Answer: D

NEW QUESTION 258
Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two)

A. From the Panorama tab of the Panorama GUI select Log Collector mode and then commit changes
B. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.
C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.
D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.
E. Log in the Panorama CLI of the dedicated Log Collector

Answer: BE

Explanation:
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

NEW QUESTION 263
The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.
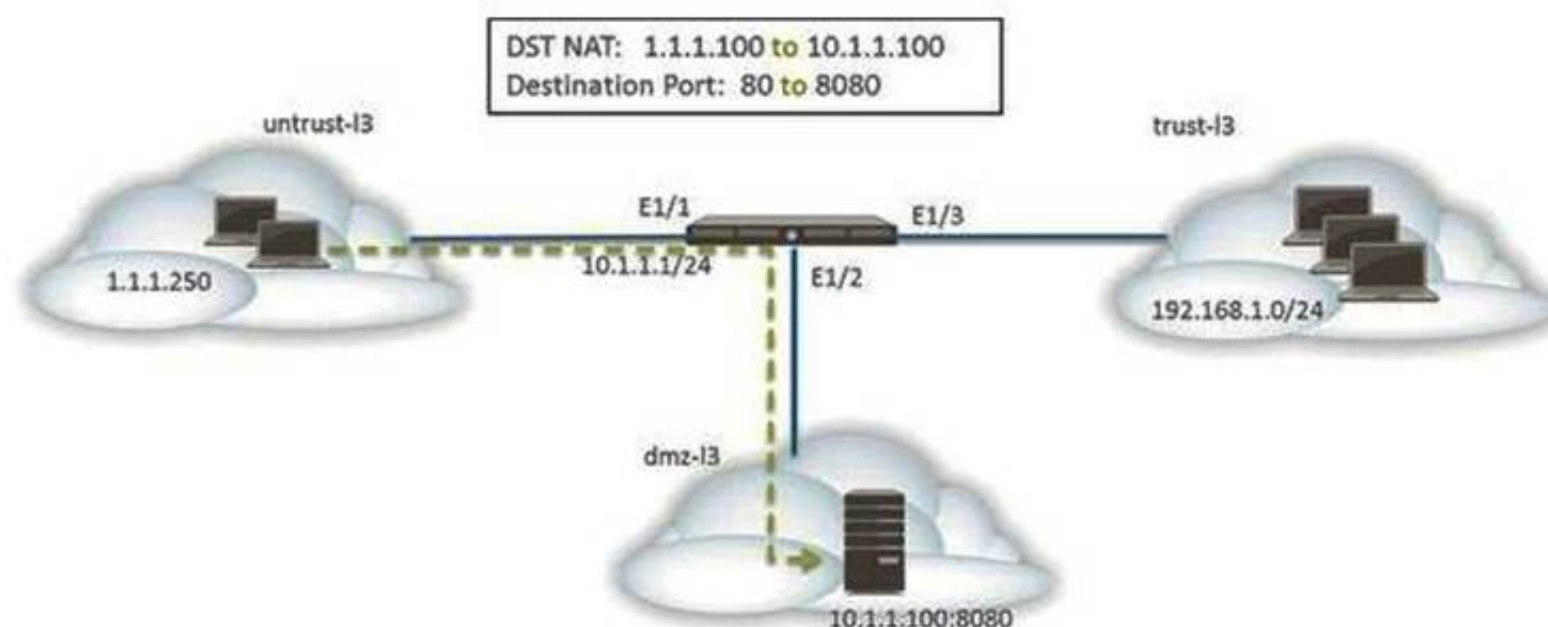
Which NAT and security rules must be configured on the firewall? (Choose two)

A. A security policy with a source of any from untrust-I3 Zone to a destination of 10.1.1.100 in dmz-I3 zone using web-browsing application
B. A NAT rule with a source of any from untrust-I3 zone to a destination of 10.1.1.100 in dmz-zone using service-http service.
C. A NAT rule with a source of any from untrust-I3 zone to a destination of 1.1.1.100 in untrust-I3 zone using service-http service.
D. A security policy with a source of any from untrust-I3 zone to a destination of 1.1.100 in dmz-I3 zone using web-browsing application.

Answer: BD

NEW QUESTION 265
A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewall
Which part of files needs to be imported back into the replacement firewall that is using Panorama?

A. Device state and license files
B. Configuration and serial number files
C. Configuration and statistics files
D. Configuration and Large Scale VPN (LSVPN) setups file

Answer: A

NEW QUESTION 266
A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.
What could cause this condition?

A. The firewall does not have an active WildFire subscription.
B. The engineer's account does not have permission to view WildFire Submissions.
C. A policy is blocking WildFire Submission traffic.
D. Though WildFire is working, there are currently no WildFire Submissions log entries.

Answer: B

NEW QUESTION 268
Click the Exhibit button below,

A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20.
Which is the next hop IP address for the HTTPS traffic from Will's PC?

A. 172.20.30.1
B. 172.20.40.1
C. 172.20.20.1
D. 172.20.10.1

Answer: C

NEW QUESTION 272
Which three function are found on the dataplane of a PA-5050? (Choose three)

A. Protocol Decoder
B. Dynamic routing
C. Management
D. Network Processing
E. Signature Match

Answer: BDE

NEW QUESTION 274
What can missing SSL packets when performing a packet capture on dataplane interfaces?

A. The packets are hardware offloaded to the offloaded processor on the dataplane
B. The missing packets are offloaded to the management plane CPU
C. The packets are not captured because they are encrypted
D. There is a hardware problem with offloading FPGA on the management plane

Answer: A

NEW QUESTION 279
Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only?

A. Disable Server Response Inspection
B. Apply an Application Override
C. Disable HIP Profile
D. Add server IP Security Policy exception

Answer: A

NEW QUESTION 281
How are IPV6 DNS queries configured to user interface ethernet1/3?

A. Network > Virtual Router > DNS Interface
B. Objects > CustomerObjects > DNS
C. Network > Interface Mgrnt
D. Device > Setup > Services > Service Route Configuration

Answer: D

NEW QUESTION 283
A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters?

A. From the CLI, issue the show counter global filter pcap yes command.
B. From the CLI, issue the show counter global filter packet-filter yes command.
C. From the GUI, select show global counters under the monitor tab.
D. From the CLI, issue the show counter interface command for the ingress interface.

Answer: B

NEW QUESTION 287
A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem?

A. DHCP has been set to Auto.
B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.
C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.
D. DNS has not been properly configured on the firewall

Answer: B

NEW QUESTION 292
The GlobalProtect Portal interface and IP address have been configured. Which other value needs to be defined to complete the network settings configuration of GlobalPortect Portal?

A. Server Certificate
B. Client Certificate
C. Authentication Profile
D. Certificate Profile

Answer: A

Explanation:
(https://live.paloaltonetworks.HYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351"com/t5/Configuration-Articles/How-to- Configure-GlobalProtect/ta-p/58351)

NEW QUESTION 297
Which Palo Alto Networks VM-Series firewall is supported for VMware NSX?

A. VM-100
B. VM-200
C. VM-1000-HV
D. VM-300

Answer: C

NEW QUESTION 302
Support for which authentication method was added in PAN-OS 8.0?

A. RADIUS
B. LDAP
C. Diameter
D. TACACS+

Answer: D

Explanation:
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

NEW QUESTION 305
Which option is an IPv6 routing protocol?

A. RIPv3
B. OSPFv3
C. OSPv3
D. BGP NG

Answer: B

NEW QUESTION 308
Firewall administrators cannot authenticate to a firewall GUI.
Which two logs on that firewall will contain authentication-related information useful in troubleshooting this issue? (Choose two.)

A. ms log
B. authd log
C. System log
D. Traffic log
E. dp-monitor .log

Answer: BC

NEW QUESTION 312
When is it necessary to activate a license when provisioning a new Palo Alto Networks firewall?

A. When configuring Certificate Profiles
B. When configuring GlobalProtect portal
C. When configuring User Activity Reports
D. When configuring Antivirus Dynamic Updates

Answer: D

NEW QUESTION 316
What are two prerequisites for configuring a pair of Palo Alto Networks firewalls in an active/passive High Availability (HA) pair? (Choose two.)

A. The firewalls must have the same set of licenses.
B. The management interfaces must to be on the same network.
C. The peer HA1 IP address must be the same on both firewalls.
D. HA1 should be connected to HA1. Either directly or with an intermediate Layer 2 device.

Answer: AD

NEW QUESTION 319
Which authentication source requires the installation of Palo Alto Networks software, other than PAN-OS 7x, to obtain a username-to-IP-address mapping?

A. Microsoft Active Directory
B. Microsoft Terminal Services
C. Aerohive Wireless Access Point
D. Palo Alto Networks Captive Portal

Answer: B

NEW QUESTION 322
A network design change requires an existing firewall to start accessing Palo Alto Updates from a data plane interface address instead of the management interface.
Which configuration setting needs to be modified?

A. Service route
B. Default route
C. Management profile
D. Authentication profile

Answer: A

NEW QUESTION 327
Which URL Filtering Security Profile action togs the URL Filtering category to the URL Filtering log?

A. Log
B. Alert
C. Allow
D. Default

Answer: B

NEW QUESTION 329
People are having intermittent quality issues during a live meeting via web application.

A. Use QoS profile to define QoS Classes
B. Use QoS Classes to define QoS Profile
C. Use QoS Profile to define QoS Classes and a QoS Policy
D. Use QoS Classes to define QoS Profile and a QoS Policy

Answer: C

NEW QUESTION 333
Which URL Filtering Security Profile action logs the URL Filtering category to the URL Filtering log?

A. Log
B. Alert
C. Allow
D. Default

Answer: B

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering- profile-actions

NEW QUESTION 336
Several offices are connected with VPNs using static IPV4 routes. An administrator has been tasked with implementing OSPF to replace static routing.
Which step is required to accoumplish this goal?

A. Assign an IP address on each tunnel interface at each site
B. Enable OSPFv3 on each tunnel interface and use Area ID 0.0.0.0
C. Assign OSPF Area ID 0.0.0.0 to all Ethernet and tunnel interfaces
D. Create new VPN zones at each site to terminate each VPN connection

Answer: C

NEW QUESTION 339
A network security engineer has a requirement to allow an external server to access an internal web server. The internal web server must also initiate connections with the external server.
What can be done to simplify the NAT policy?

A. Configure ECMP to handle matching NAT traffic
B. Configure a NAT Policy rule with Dynamic IP and Port
C. Create a new Source NAT Policy rule that matches the existing traffic and enable the Bi-directional option
D. Create a new Destination NAT Policy rule that matches the existing traffic and enable the Bi- directional option

Answer: C

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples

NEW QUESTION 344
Which CLI command displays the current management plane memory utilization?

A. > debug management-server show
B. > show running resource-monitor
C. > show system info
D. > show system resources

Answer: D

Explanation:
https://HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-
p/59364"live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-p/59364
"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top'
command in Linux." https://live.HYPERLINK "https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret- show-system-resources/ta-
p/59364"paloHYPERLINK
"https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system- resources/ta-p/59364"altonetworHYPERLINK
"https://live.paloaltonetworks.com/t5/Learning- Articles/How-to-Interpret-show-system-resources/ta-p/59364"ks.com/t5/Learning-Articles/How-to- Interpret-show-
system-resources/ta-p/59364

NEW QUESTION 348
In an enterprise deployment, a network security engineer wants to assign to a group of administrators without creating local administrator accounts on the firewall.
Which authentication method must be used?

A. LDAP
B. Kerberos
C. Certification based authentication
D. RADIUS with Vendor-Specific Attributes

Answer: D

NEW QUESTION 350
A company hosts a publicly accessible web server behind a Palo Alto Networks next-generation firewall with the following configuration information:
* Users outside the company are in the "Untrust-L3" zone.
* The web server physically resides in the "Trust-L3" zone.
* Web server public IP address: 23.54.6.10
* Web server private IP address: 192.168.1.10
Which two items must the NAT policy contain to allow users in the Untrust-L3 zone to access the web server? (Choose two.)

A. Destination IPof 23.54.6.10
B. UntrustL3 for both Source and Destination Zone
C. Destination IP of 192.168.1.10
D. UntrustL3 for Source Zone and Trust-L3 for Destination Zone

Answer: AB

NEW QUESTION 354
A distributed log collection deployment has dedicated log Collectors. A developer needs a device to send logs to Panorama instead of sending logs to the Collector Group.
What should be done first?

A. Remove the cable from the management interface, reload the log Collector and then re-connect that cable
B. Contact Palo Alto Networks Support team to enter kernel mode commands to allow adjustments
C. remove the device from the Collector Group
D. Revert to a previous configuration

Answer: C

NEW QUESTION 357
Which two actions are required to make Microsoft Active Directory users appear in a firewall traffic log? (Choose two.)

A. Run the User-ID Agent using an Active Directory account that has "event log viewer" permissions
B. Enable User-ID on the zone object for the destination zone
C. Run the User-ID Agent using an Active Directory account that has "domain administrator" permissions
D. Enable User-ID on the zone object for the source zone
E. Configure a RADIUS server profile to point to a domain controller

Answer: AD

NEW QUESTION 359
Which two virtualized environments support Active/Active High Availability (HA) in PAN-OS 8.0? (Choose two.)

A. KVM
B. VMware ESX
C. VMware NSX
D. AWS

Answer: AB

NEW QUESTION 360
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSE Product From:

https://www.2passeasy.com/dumps/PCNSE/

Money Back Guarantee

PCNSE Practice Exam Features:

* PCNSE Questions and Answers Updated Frequently

* PCNSE Practice Questions Verified by Expert Senior Certified Staff

* PCNSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year