Exam Questions PCNSE

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

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

NEW QUESTION 1
Which three split tunnel methods are supported by a globalProtect gateway? (Choose three.)

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

Answer: ABC

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

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

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

Answer: C

NEW QUESTION 4
Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

A. CRL
B. CRT
C. OCSP
D. Cert-Validation-Profile
E. SSL/TLS Service Profile

Answer: AC

NEW QUESTION 5
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 6
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 7
Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

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

Answer: C

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

NEW QUESTION 8
A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

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

Answer: AB

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-a1dd- 8064499f5b9d

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
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

Answer: D

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

NEW QUESTION 10
To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

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

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 11
Which two virtualization platforms officially support the deployment of Palo Alto Networks VM- Series firewalls? (Choose two.)

A. Red Hat Enterprise Virtualization (RHEV)

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

Answer: BD

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

NEW QUESTION 13
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."
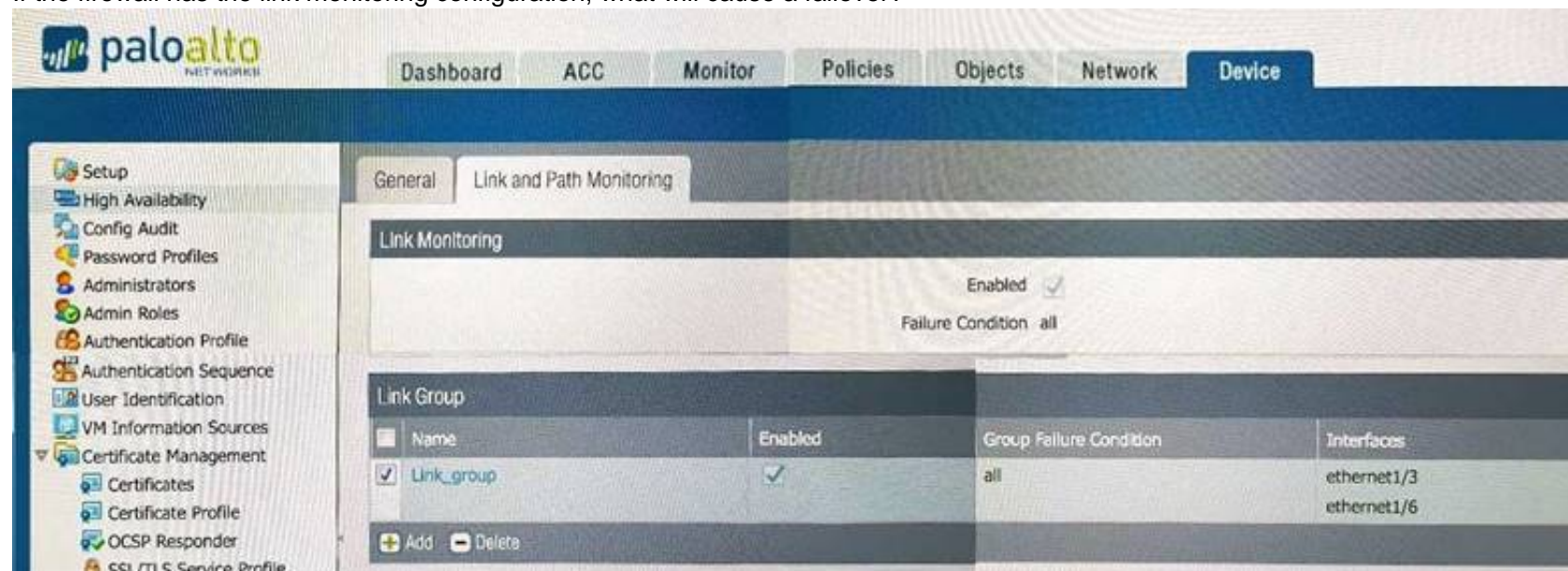
Answer: B

NEW QUESTION 18
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 20
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

Answer: A

NEW QUESTION 21
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

Answer: B

NEW QUESTION 25

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 30
How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

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

Answer: D

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

NEW QUESTION 33
An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

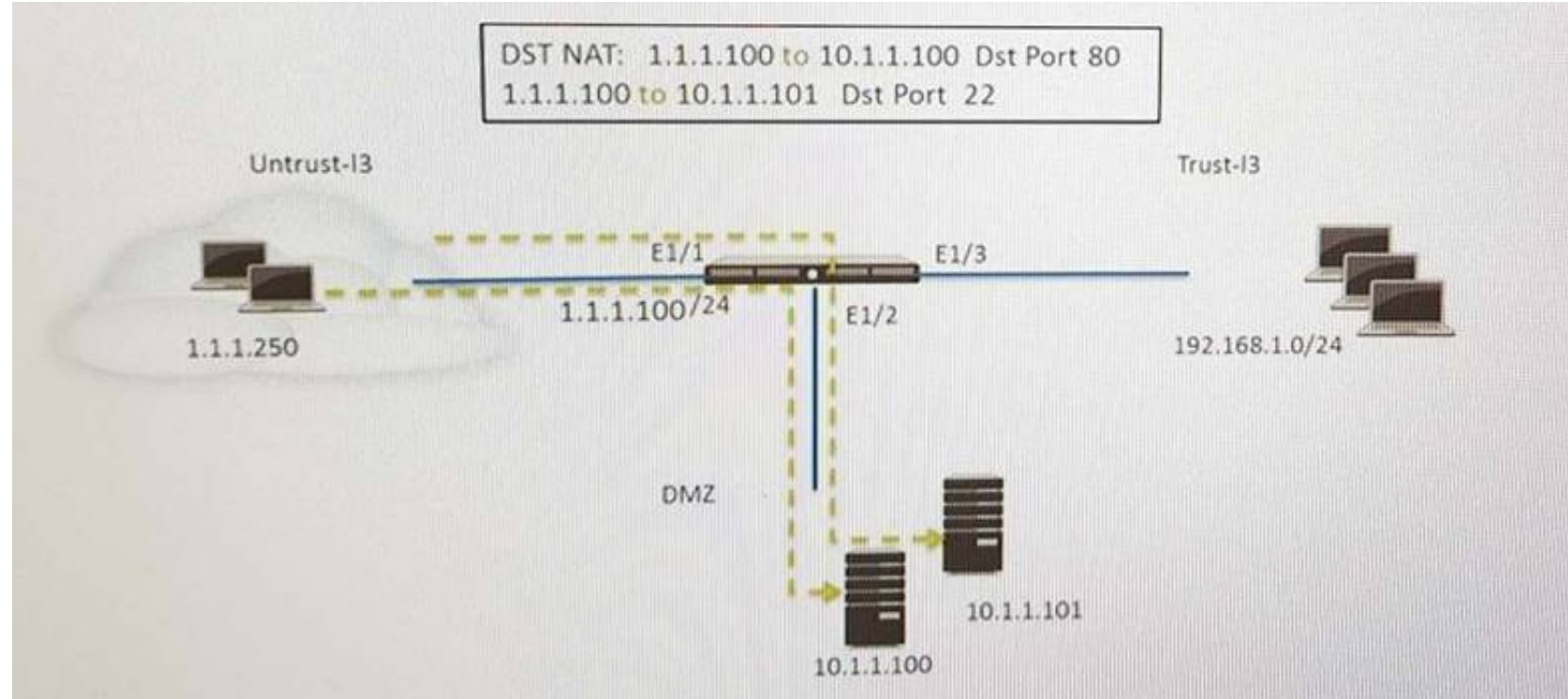A. Port Inspection
B. Certificate revocation
C. Content-ID
D. App-ID

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/quality-of-service/qos-for-applications-and-users

NEW QUESTION 34
Refer to the exhibit.

An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and HOST B (10.1.1.101) receives SSH traffic.)
Which two security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to Untrust (10.1.1.1), web-browsing -Allow
B. Untrust (Any) to Untrust (10.1.1.1), ssh -Allow
C. Untrust (Any) to DMZ (10.1.1.1), web-browsing -Allow
D. Untrust (Any) to DMZ (10.1.1.1), ssh –Allow
E. Untrust (Any) to DMZ (10.1.1.100.10.1.1.101), ssh, web-browsing -Allow

Answer: CD

NEW QUESTION 38
Which three settings are defined within the Templates object of Panorama? (Choose three.)

A. Setup
B. Virtual Routers
C. Interfaces
D. Security

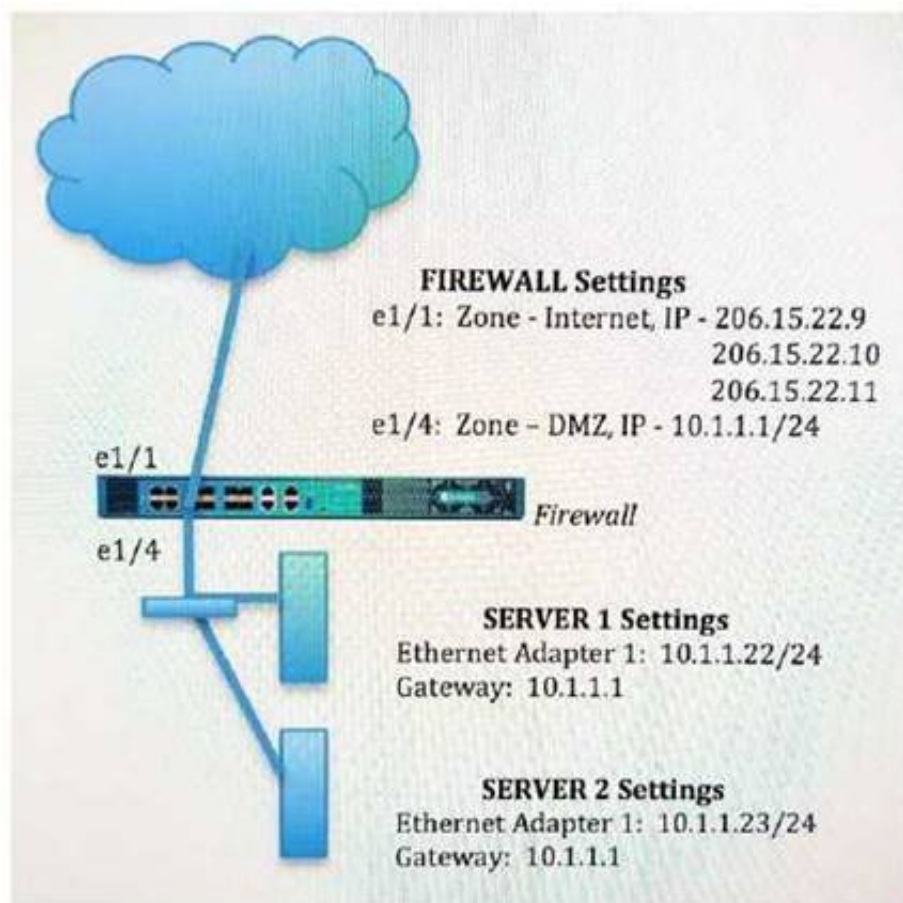E. Application Override

Answer: ADE

NEW QUESTION 41
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

Answer: ABC

NEW QUESTION 42
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 45
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 49
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

Answer: DEF

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

NEW QUESTION 52
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

Answer: D

NEW QUESTION 57
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

Answer: DEF

NEW QUESTION 58
Which event will happen if an administrator uses an Application Override Policy?

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 61
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 64
An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN- OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web-browsing traffic from any to any zone. What must the administrator configure so that the PAN-OS® software can be upgraded?

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

Answer: A

NEW QUESTION 67
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
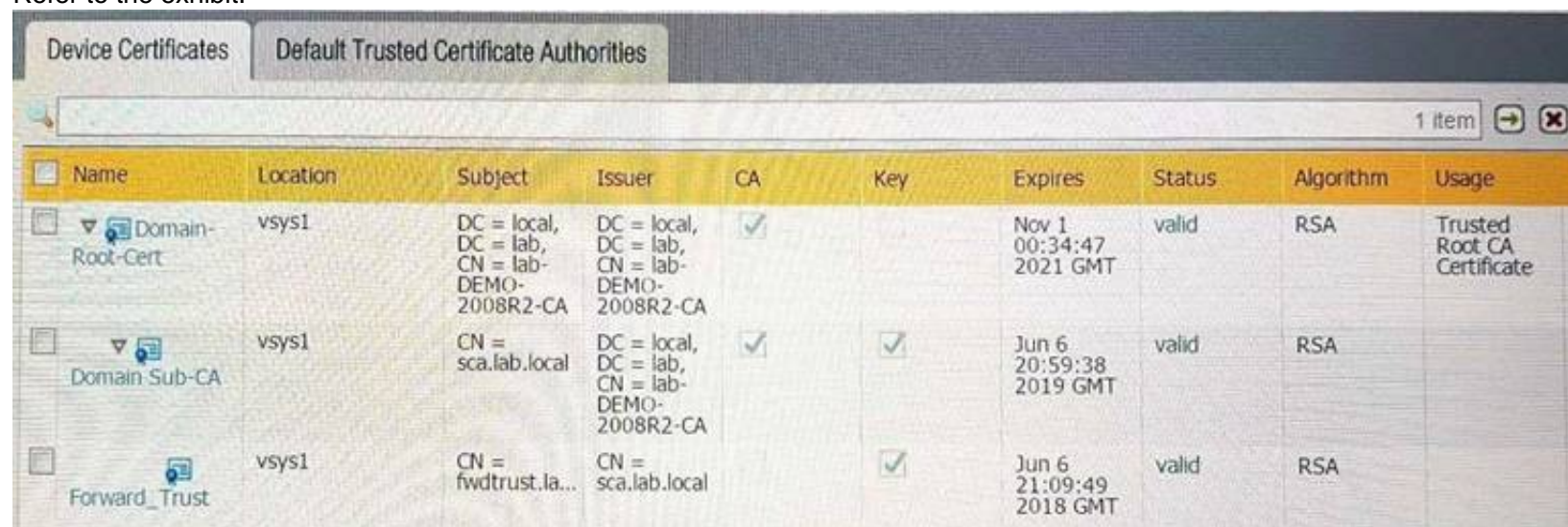
Explanation:
Reference: https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance

NEW QUESTION 68
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 70
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.

Answer: D

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-ssltls-service-profile

NEW QUESTION 72
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 74
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

Answer: A

NEW QUESTION 78
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

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN-OS-6.0-CLI-ref.pdf

NEW QUESTION 79
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 83
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
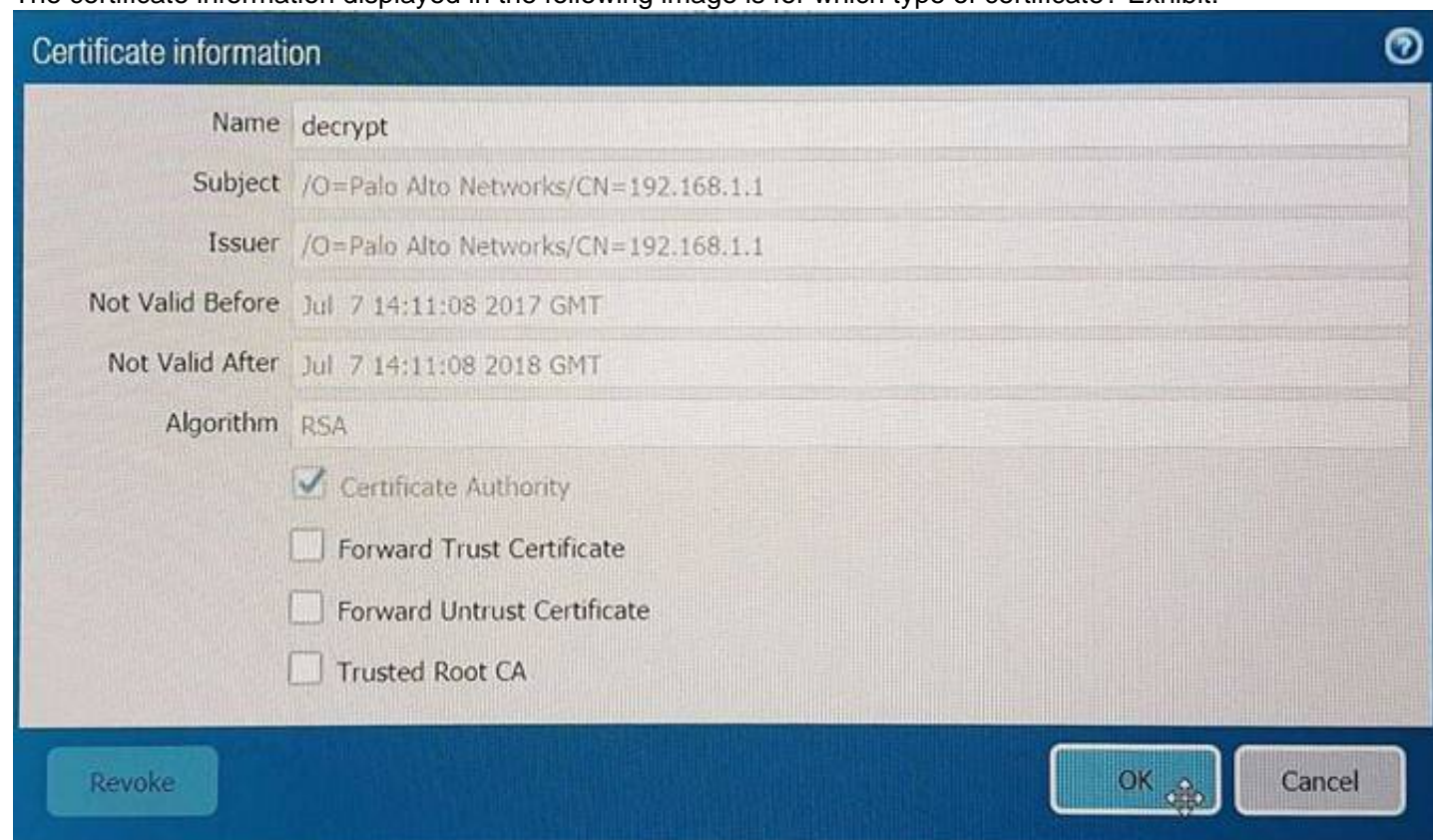B. Application Command Center
C. TCP Dump
D. Packet Capture

Answer: B

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

NEW QUESTION 86
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 91
Which feature must you configure to prevent users form accidentally submitting their corporate
credentials to a phishing website?

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing

NEW QUESTION 92
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 96
Which three firewall states are valid? (Choose three.)

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

Answer: ADE

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

NEW QUESTION 97
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 100
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 102
An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating
system on an internal system. Which Security Profile type will prevent this attack?

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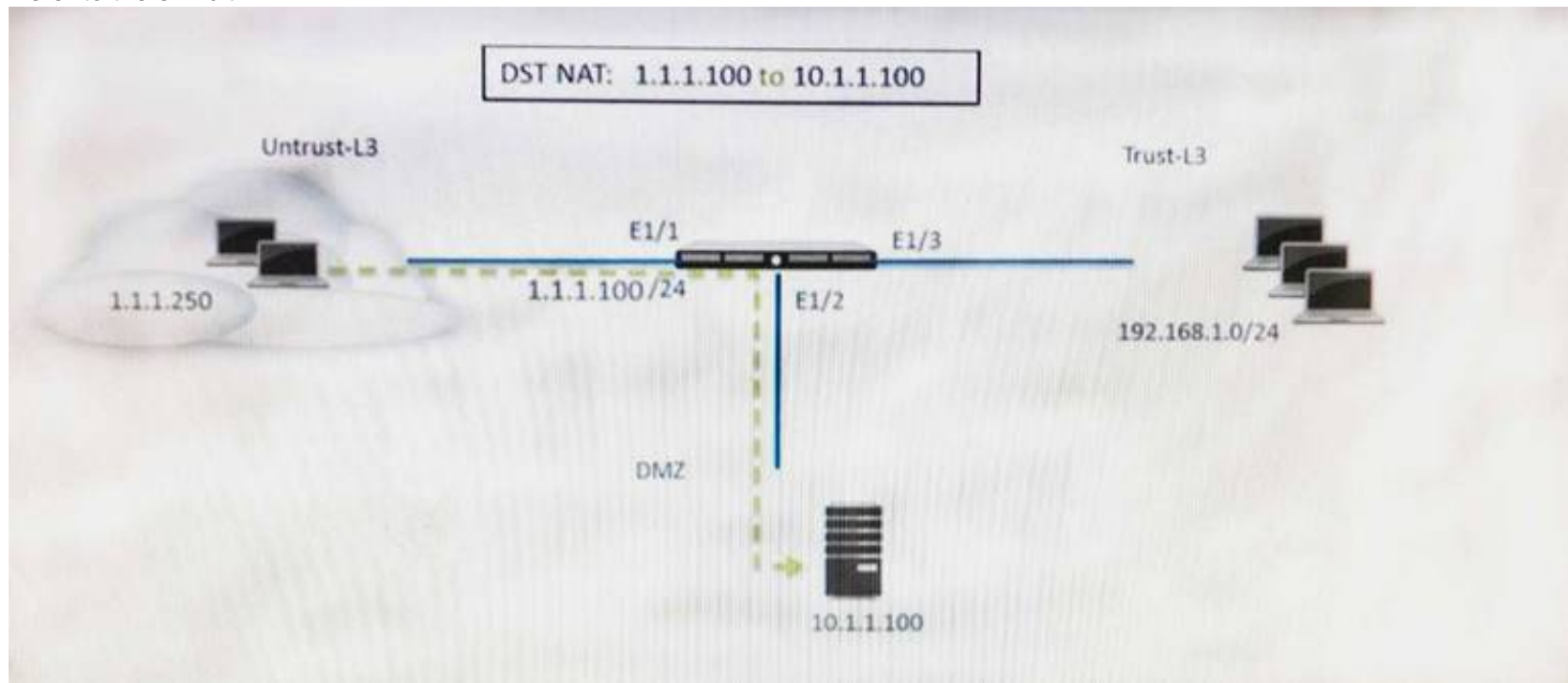B. Anti-Spyware
C. URL Filtering
D. Antivirus

Answer: A

Explanation:

Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection

NEW QUESTION 107
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 109
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 114
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 119
Which two subscriptions are available when configuring panorama to push dynamic updates to connected devices? (Choose two.)

A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus

Answer: CD

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

NEW QUESTION 120
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

Answer: ADF

NEW QUESTION 125
What is exchanged through the HA2 link?

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

Answer: C

Explanation:
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

NEW QUESTION 128
A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

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

Answer: AC

NEW QUESTION 133
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 138
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 to assign untagged (native) traffic to its own zone which options differentiates multiple VLAN into separate zones?

A. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN I
B. Repeat forevery additional VLANand use a VLAN ID of 0 for untagged traffi
C. Assign each interface/subinterface to a unique zone.
D. Create V-Wire objects with two V-Wire sub interface and assign only a single VLAN ID to the "Tag Allowed field one of the V-Wire object Repeat for every additional VLAN and use a VIAN ID of 0 for untagged traffi
E. Assign each interface/subinterfaceto a unique zone.
F. Create V-Wire objects with two V-Wire interfaces and define a range "0- 4096" in the 'Tag Allowed filed of the V-Wire object.
G. Create Layer 3 sub interfaces that are each assigned to a single VLAN ID and a common virtual route
H. The physical Layer 3interface would handle untagged traffi
I. Assign each interface /subinterface to a unique zon
J. Do not assign any interface anIP address

Answer: C

NEW QUESTION 139
Which logs enable a firewall administrator to determine whether a session was decrypted?

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

Answer: B

NEW QUESTION 141
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 146
Which log file can be used to identify SSL decryption failures?

A. Configuration
B. Threats
C. ACC
D. Traffic

Answer: C

NEW QUESTION 149
An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:
•Firewall has Internet connectivity through e1/1.
•Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
•Service route is configured, sourcing update traffic from e1/1.
•A communication error appears in the System logs when updates are performed.
•Download does not complete.
What must be configured to enable the firewall to download the current version of PAN-OS software?

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

Answer: D

NEW QUESTION 152
Which three firewall states are valid? (Choose three)

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

Answer: ABC

NEW QUESTION 153
An administrator wants to upgrade an NGFW from PAN-OS® 7 .1. 2 to PAN-OS® 8 .0.2 The firewall is not a part of an HA pair. What needs to be updated first?

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

Answer: B

NEW QUESTION 158
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 160
When configuring the firewall for packet capture, what are the valid stage types?

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

Answer: D

NEW QUESTION 163

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

A. Client Probing
B. Port mapping
C. Server monitoring
D. Syslog listening

Answer: D

NEW QUESTION 164
When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

A. Load named configuration snapshot
B. Load configuration version
C. Save candidate config
D. Export device state

Answer: A

NEW QUESTION 169
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 174
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 176
Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

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

Answer: C

NEW QUESTION 179
Which Panorama administrator types require the configuration of at least one access domain? (Choose two)

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

Answer: DE

NEW QUESTION 180
Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two)

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

Answer: AB

NEW QUESTION 181
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 183
A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured. What can be the cause of this problem?

A. No Zone has been configured on Ethernet 1/4.
B. Interface Ethernet 1/1 is in Virtual Wire Mode.
C. DNS has not been properly configured on the firewall.
D. DNS has not been properly configured on the host.

Answer: A

NEW QUESTION 185
A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk. What action will bring the VPN up and allow traffic to start passing between the sites?

A. Change the Site-B IKE Gateway profile version to match Site-A,
B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.
C. Enable NAT Traversal on the Site-A IKE Gateway profile.
D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A

Answer: D

NEW QUESTION 188
A logging infrastructure may need to handle more than 10,000 logs per second. Which two options support a dedicated log collector function? (Choose two)

A. Panorama virtual appliance on ESX(i) only
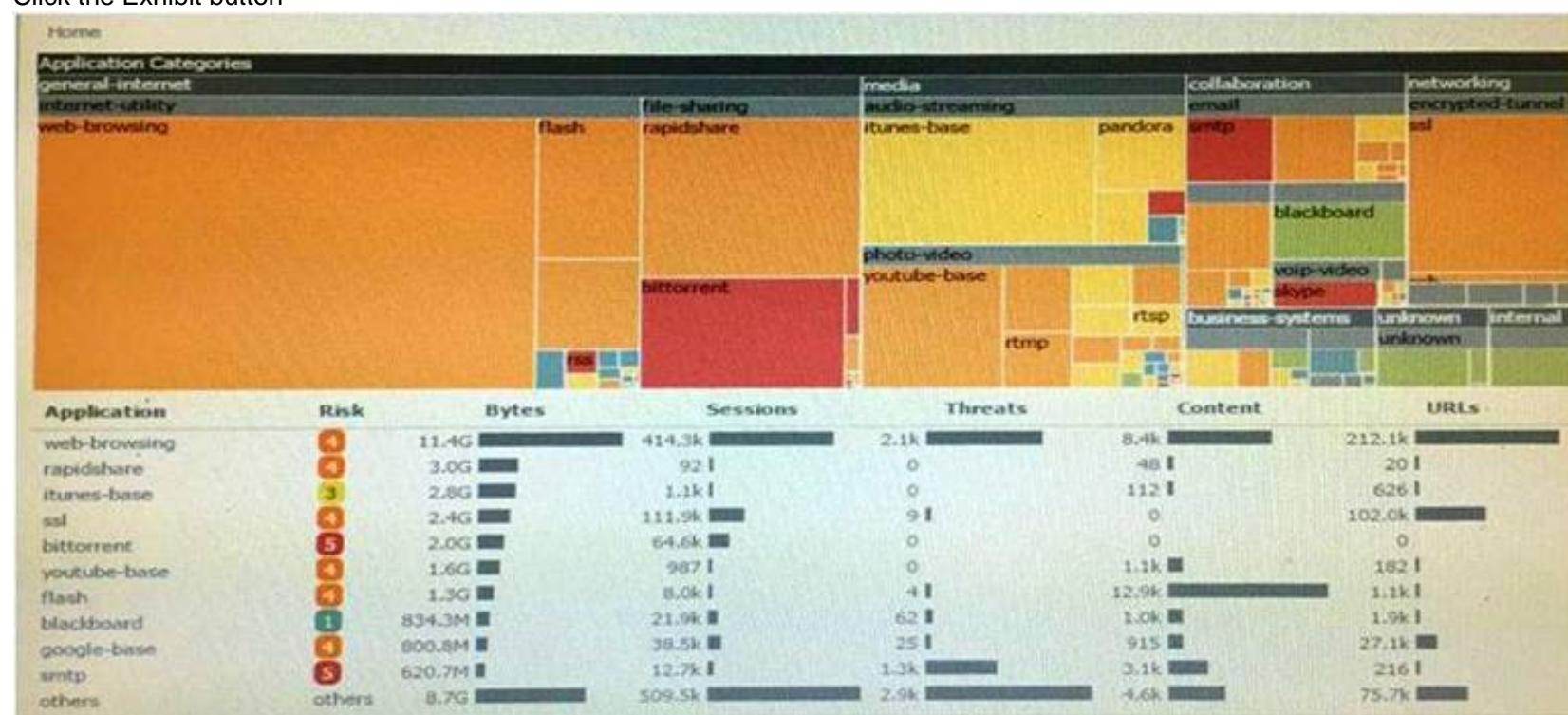B. M-500
C. M-100 with Panorama installed
D. M-100

Answer: BC

Explanation:
(httpHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and- Design-Guide/ta-p/72181"s://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing- and-Design-Guide/ta-p/72181)

NEW QUESTION 193
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 194

How is the Forward Untrust Certificate used?

A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
B. It is used when web servers request a client certificate.
C. It is presented to clients when the server they are connecting to is signed by a certificate authority that is not trusted by firewall.
D. It is used for Captive Portal to identify unknown users.

Answer: C

NEW QUESTION 196
What are three valid actions in a File Blocking Profile? (Choose three)

A. Forward
B. Block
C. Alret
D. Upload
E. Reset-both
F. Continue

Answer: ABC

Explanation:
https://live.paloaltonetworksHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623".com/t5/Configuration- ArticHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"les/File-Blocking-RulebHYPERLINK "https://live.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p/53623"ase-and-Action-Precedence/ta-p/53623

NEW QUESTION 199
Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address?

A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.
B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.
C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.
D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000.

Answer: C

NEW QUESTION 203
A company has a pair of Palo Alto Networks firewalls configured as an Acitve/Passive High Availability (HA) pair.
What allows the firewall administrator to determine the last date a failover event occurred?

A. From the CLI issue use the show System log
B. Apply the filter subtype eq ha to the System log
C. Apply the filter subtype eq ha to the configuration log
D. Check the status of the High Availability widget on the Dashboard of the GUI

Answer: B

NEW QUESTION 207
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 212
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 216
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 221
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 222
A firewall administrator has completed most of the steps required to provision a standalone Palo Alto Networks Next-Generation Firewall. As a final step, the administrator wants to test one of the security policies.
Which CLI command syntax will display the rule that matches the test?

A. test security -policy- match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number
B. show security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
C. test security rule source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>
D. show security-policy-match source <ip_address> destination <IP_address> destination port <port number> protocol <protocol number>test security-policy-match source

Answer: A

Explanation:
test security-policy-match source <source IP> destination <destination IP> protocol <protocol number>
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Test-Which-Security-Policy- Applies-to-a-Traffic-Flow/ta-p/53693

NEW QUESTION 223
A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.
Given the following zone information:
• DMZ zone: DMZ-L3
• Public zone: Untrust-L3
• Guest zone: Guest-L3
• Web server zone: Trust-L3
• Public IP address (Untrust-L3): 1.1.1.1
• Private IP address (Trust-L3): 192.168.1.50
What should be configured as the destination zone on the Original Packet tab of NAT Policy rule?

A. Untrust-L3
B. DMZ-L3
C. Guest-L3
D. Trust-L3

Answer: A

NEW QUESTION 227
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 231
A network administrator uses Panorama to push security polices to managed firewalls at branch offices. Which policy type should be configured on Panorama if the administrators at the branch office sites to override these products?

A. Pre Rules
B. Post Rules
C. Explicit Rules
D. Implicit Rules

Answer: A

NEW QUESTION 234

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 235
What are three valid method of user mapping? (Choose three)

A. Syslog
B. XML API
C. 802.1X
D. WildFire
E. Server Monitoring

Answer: ABE

NEW QUESTION 237
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 238
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 240
A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's
firewall.

Which interface configuration will accept specific VLAN IDs?
Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two)

A. A report can be created that identifies unclassified traffic on the network.
B. Different security profiles can be applied to traffic matching rules 2 and 3.
C. Rule 2 and 3 apply to traffic on different ports.
D. Separate Log Forwarding profiles can be applied to rules 2 and 3.

Answer: BD

NEW QUESTION 245
A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment?

A. The two devices must share a routable floating IP address
B. The two devices may be different models within the PA-5000 series
C. The HA1 IP address from each peer must be on a different subnet
D. The management port may be used for a backup control connection

Answer: D

NEW QUESTION 246
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 250
After pushing a security policy from Panorama to a PA-3020 firwall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem?

A. A Server Profile has not been configured for logging to this Panorama device.
B. Panorama is not licensed to receive logs from this particular firewall.
C. The firewall is not licensed for logging to this Panorama device.
D. None of the firwwall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 253
A company.com wants to enable Application Override. Given the following screenshot:

Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.
B. Traffic will be forced to operate over UDP Port 16384.
C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".
D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines.

Answer: AC

NEW QUESTION 256
A Network Administrator wants to deploy a Large Scale VPN solution. The Network Administrator has chosen a GlobalProtect Satellite solution. This configuration needs to be deployed to multiple remote offices and the Network Administrator decides to use Panorama to deploy the configurations.
How should this be accomplished?

A. Create a Template with the appropriate IKE Gateway settings
B. Create a Template with the appropriate IPSec tunnel settings
C. Create a Device Group with the appropriate IKE Gateway settings
D. Create a Device Group with the appropriate IPSec tunnel settings

Answer: B

NEW QUESTION 258
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 accomplish 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 261
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 266
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 271
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 276
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 279
Which Panorama feature allows for logs generated by Panorama to be forwarded to an external Security Information and Event Management(SIEM) system?

A. Panorama Log Settings
B. Panorama Log Templates
C. Panorama Device Group Log Forwarding
D. Collector Log Forwarding for Collector Groups

Answer: A

Explanation:
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_admiHYPERLINK
"https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-

destinations"nguidHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"e/manage-log- collection/enable-log-forwarding-from-panorama-to-external-destinaHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"tions

NEW QUESTION 282
What will be the source address in the ICMP packet?
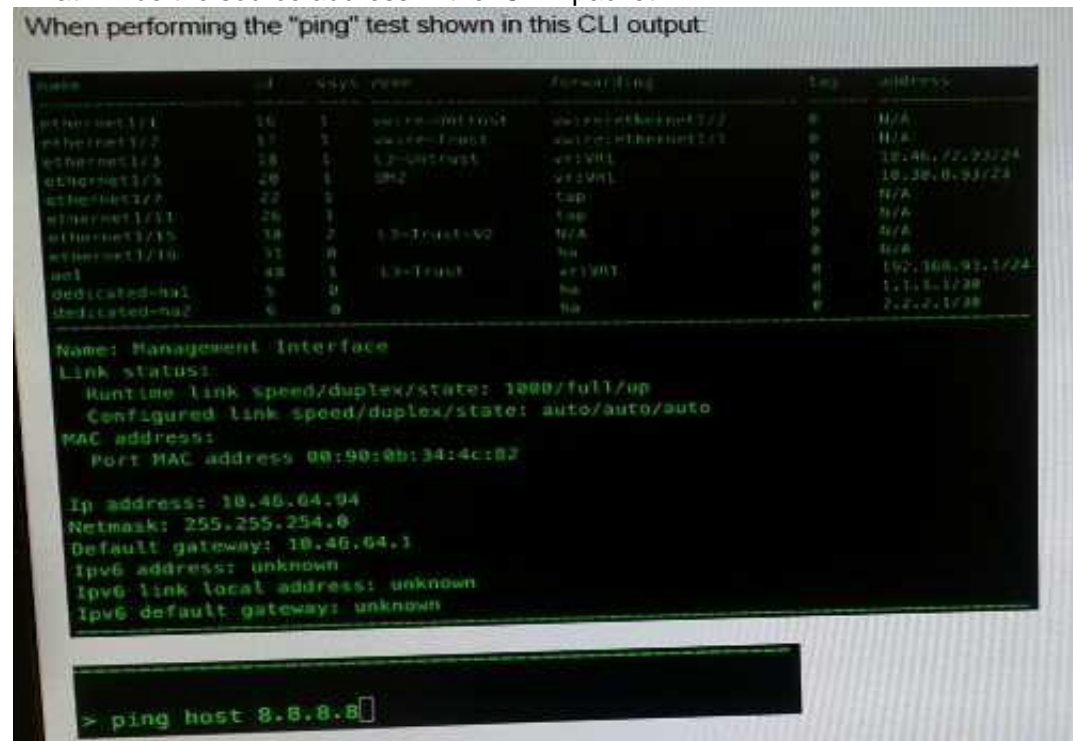
A. 10.30.0.93
B. 10.46.72.93
C. 10.46.64.94
D. 192.168.93.1

Answer: C

NEW QUESTION 283
A file sharing application is being permitted and no one knows what this application is used for. How should this application be blocked?

A. Block all unauthorized applications using a security policy
B. Block all known internal custom applications
C. Create a WildFire Analysis Profile that blocks Layer 4 and Layer 7 attacks
D. Create a File blocking profile that blocks Layer 4 and Layer 7 attacks

Answer: D

NEW QUESTION 286
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 289
When a malware-infected host attempts to resolve a known command-and-control server, the traffic matches a security policy with DNS sinhole enabled, generating a traffic log.
What will be the destination IP Address in that log entry?

A. The IP Address of sinkhole.paloaltonetworks.com
B. The IP Address of the command-and-control server
C. The IP Address specified in the sinkhole configuration
D. The IP Address of one of the external DNS servers identified in the anti-spyware database

Answer: C

Explanation:
https://live.paloaltonetworks.com/t5/MaHYPERLINK "https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function- is-Working/ta-p/65864"naHYPERLINK "https://live.paloaltonetworks.com/t5/Management- Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864"gement-Articles/How-to- Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

NEW QUESTION 291
Which two logs on the firewall will contain authentication-related information useful for troubleshooting purpose (Choose two)

A. ms.log
B. traffic.log
C. system.log
D. dp-monitor.log
E. authd.log

Answer: CE

NEW QUESTION 294
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 297
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

A. Enable support for non-standard syslog messages under device management
B. Check the custom-format check box in the syslog server profile
C. Select a non-standard syslog server profile
D. Create a custom log format under the syslog server profile

Answer: D

NEW QUESTION 298
Which Device Group option is assigned by default in Panorama whenever a new device group is created to manage a Firewall?

A. Master
B. Universal
C. Shared
D. Global

Answer: C

NEW QUESTION 302
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 307
YouTube videos are consuming too much bandwidth on the network, causing delays in mission- critical traffic. The administrator wants to throttle YouTube traffic. The following interfaces and zones are in use on the firewall:
* ethernet1/1, Zone: Untrust (Internet-facing)
* ethernet1/2, Zone: Trust (client-facing)
A QoS profile has been created, and QoS has been enabled on both interfaces. A QoS rule exists to put the YouTube application into QoS class 6. Interface Ethernet1/1 has a QoS profile called Outbound, and interface Ethernet1/2 has a QoS profile called Inbound.
Which setting for class 6 with throttle YouTube traffic?

A. Outbound profile with Guaranteed Ingress
B. Outbound profile with Maximum Ingress
C. Inbound profile with Guaranteed Egress
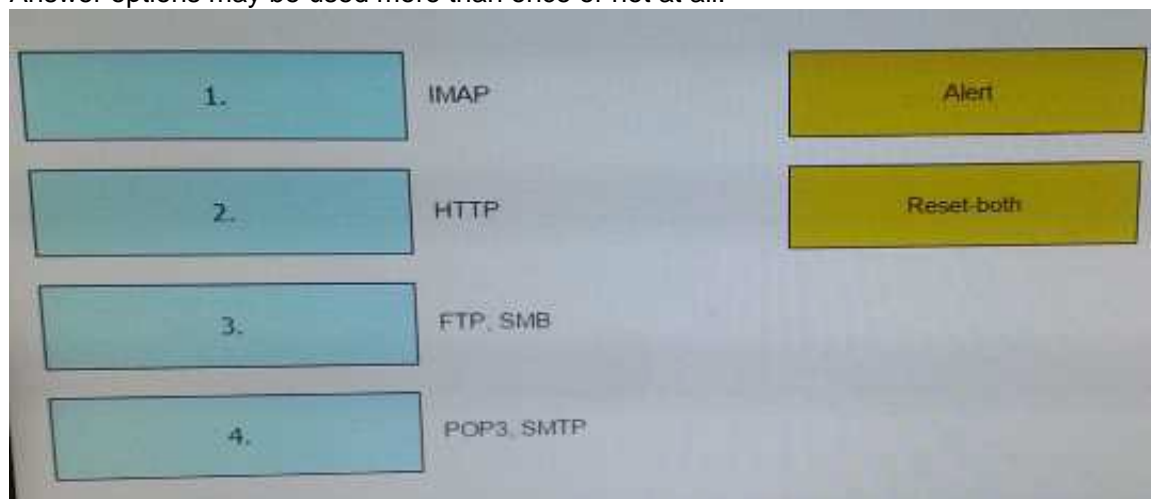D. Inbound profile with Maximum Egress

Answer: D

NEW QUESTION 310

DRAG DROP

When using the predefined default profile, the policy will inspect for viruses on the decoders. Match each decoder with its default action.

Answer options may be used more than once or not at all.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

IMAP , POP3 , SMTP - > Alert
HTTP,FTP,SMB -> Reset-both

NEW QUESTION 311
......

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