Exam Questions PCNSE

Palo Alto Networks Certified Security Engineer (PCNSE)PAN-OS 9.0

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

NEW QUESTION 1
- (Exam Topic 2)
Which option is part of the content inspection process?

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

Answer: B

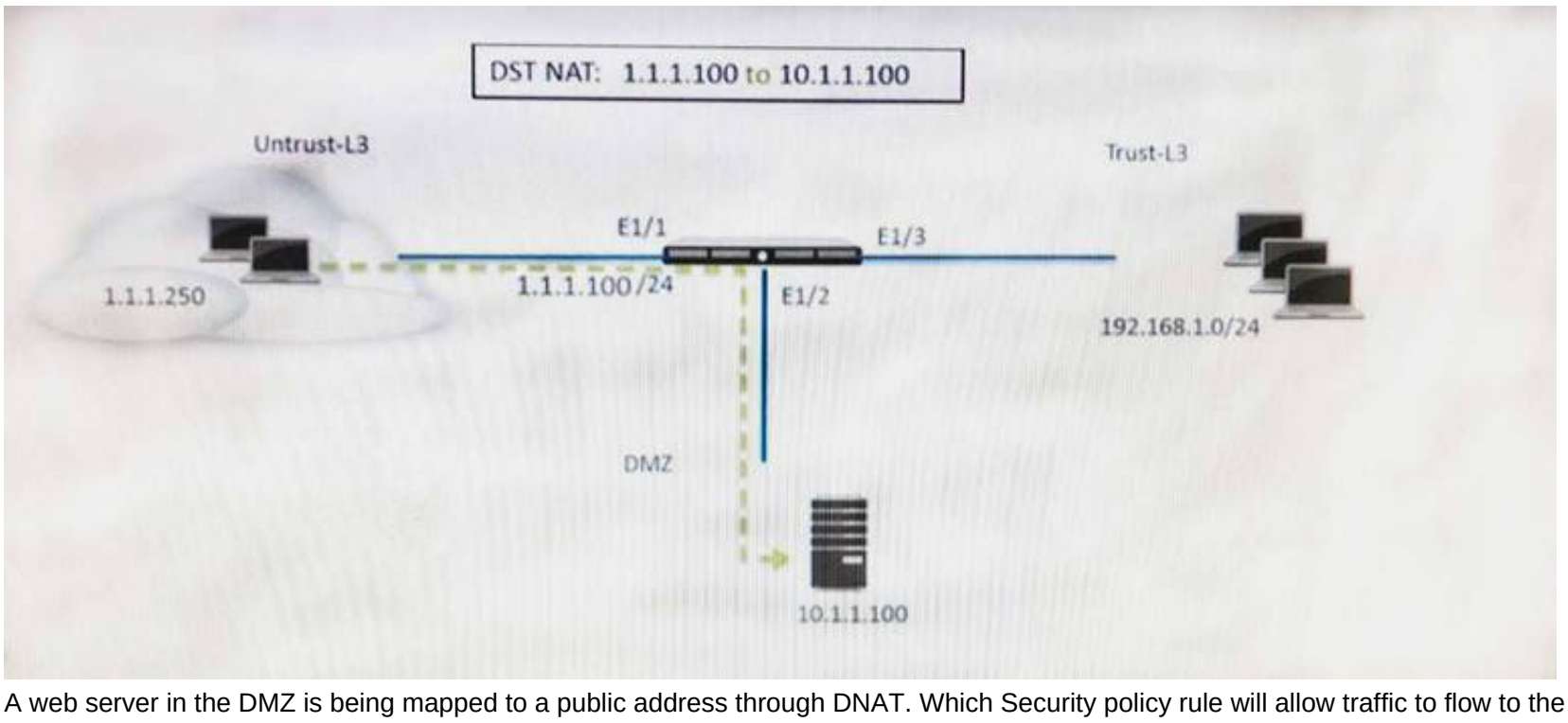
Explanation:
http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

NEW QUESTION 2
- (Exam Topic 2)
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 3
- (Exam Topic 2)
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: C

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

NEW QUESTION 4
- (Exam Topic 2)
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: BDE

NEW QUESTION 5
- (Exam Topic 2)

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 6
- (Exam Topic 2)
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://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environmen

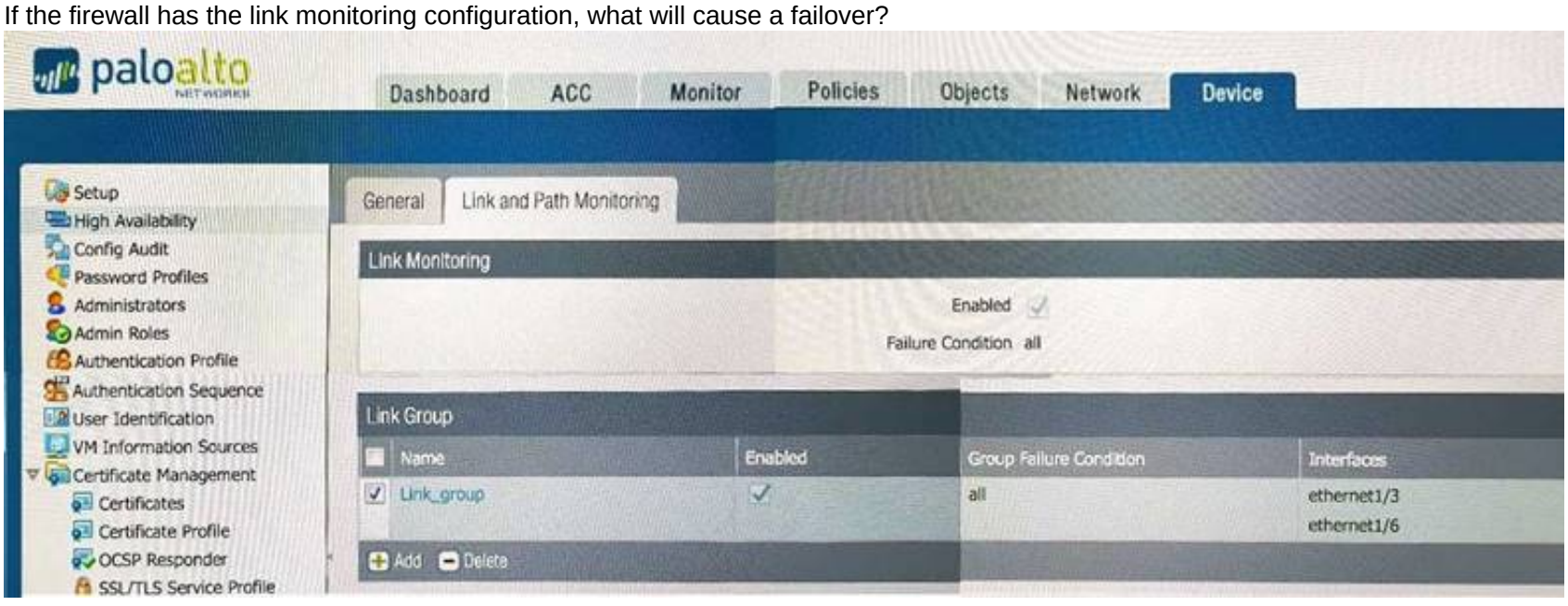
NEW QUESTION 7
- (Exam Topic 2)
Which DoS protection mechanism detects and prevents session exhaustion attacks?

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 8
- (Exam Topic 2)
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 9
- (Exam Topic 2)
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 10
- (Exam Topic 2)
A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server.
Which solution in PAN-OS® software would help in this case?

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

Answer: D

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-net

NEW QUESTION 10
- (Exam Topic 2)
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/administer-panorama/ba panorama-and-firewall-configurations

NEW QUESTION 13
- (Exam Topic 2)
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.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-inte

NEW QUESTION 18
- (Exam Topic 2)
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 19
- (Exam Topic 2)
VPN traffic intended for an administrator's Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. Replay
C. Web Application
D. DoS Protection

Answer: B

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel#

NEW QUESTION 21
- (Exam Topic 2)
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 26
- (Exam Topic 2)
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 28
- (Exam Topic 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 33
- (Exam Topic 2)
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: AD

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#

NEW QUESTION 37
- (Exam Topic 2)
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

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

NEW QUESTION 38
- (Exam Topic 2)
A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a Palo Alto Networks firewall that was previously being used in a lab. The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg txt. The firewall is currently running PAN-OS 10.0 and using a lab config The contents of init-cfg txi in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command:> request resort system Upon restart, the firewall fails to begin the bootstrapping process The failure is caused because

A. Firewall must be m factory default state or have all private data deleted for bootstrapping

B. The hostname is a required parameter, but it is missing in imt-cfg txt
C. The USB must be formatted using the ext3 file system, FAT32 is not supported
D. PANOS version must be 91.x at a minimum but the firewall is running 10.0.x
E. The bootstrap.xml file is a required file but it is missing

Answer: C

NEW QUESTION 40
- (Exam Topic 2)
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-mana ssltls-service-profile

NEW QUESTION 45
- (Exam Topic 2)
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
docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deploy

NEW QUESTION 47
- (Exam Topic 2)
Which is the maximum number of samples that can be submitted to WildFire per day, based on wildfire subscription?

A. 15,000
B. 10,000
C. 75,00
D. 5,000

Answer: B

NEW QUESTION 52
- (Exam Topic 2)
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: DE

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

NEW QUESTION 57
- (Exam Topic 2)
Which three authentication factors does PAN-OS® software support for MFA (Choose three.)

A. Push
B. Pull
C. Okta Adaptive
D. Voice
E. SMS

Answer: ADE

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

NEW QUESTION 60
- (Exam Topic 2)
Which Palo Alto Networks VM-Series firewall is valid?

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

Answer: C

Explanation:
Reference:
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series

NEW QUESTION 65
- (Exam Topic 2)
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: C

NEW QUESTION 66
- (Exam Topic 2)
An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

A. Enable and configure the Packet Buffer protection thresholds.Enable Packet Buffer Protection per ingress zone.
B. Enable and then configure Packet Buffer thresholdsEnable Interface Buffer protection.
C. Create and Apply Zone Protection Profiles in all ingress zones.Enable Packet Buffer Protection per ingress zone.
D. Configure and apply Zone Protection Profiles for all egress zones.Enable Packet Buffer Protection pre egress zone.
E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits.Enable Zone Buffer Protection per zone.

Answer: A

NEW QUESTION 69
- (Exam Topic 2)
How does Panorama prompt VMWare NSX to quarantine an infected VM?

A. HTTP Server Profile
B. Syslog Server Profile
C. Email Server Profile
D. SNMP Server Profile

Answer: A

NEW QUESTION 73
- (Exam Topic 2)
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 77
- (Exam Topic 2)
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 80
- (Exam Topic 2)
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 84
- (Exam Topic 2)
On the NGFW. how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

A. * 1.Select Device > Certificate Management > Certificates >Devace > Certificates* 2. Import the certificate.* 3 Select Import Private Key* 4 Click Generate to generate the new certificate
B. * 1 Select Device > Certificates * 2 Select Certificate Profile* 3 Generate the certificate* 4 Select Block Private Key Export.
C. * 1 Select Device > Certificates * 2 Select Certificate Profile.* 3 Generate the certificate* 4 Select Block Private Key Export
D. * 1 Select Device > Certificate Management > Certificates > Device > Certificates * 2 Generate the certificate* 3 Select Block Private Key Export* 4 Click Genet ale to generate the new certificate.

Answer: D

NEW QUESTION 85
- (Exam Topic 2)
When is the content inspection performed in the packet flow process?

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

Answer: A

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

NEW QUESTION 88
- (Exam Topic 2)
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

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

NEW QUESTION 90
- (Exam Topic 2)
Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

A. respond to changes in user behavior or potential threats using manual policy changes
B. respond to changes in user behavior or potential threats without automatic policy changes
C. respond to changes in user behavior and confirmed threats with manual policy changes
D. respond to changes in user behavior or potential threats without manual policy changes

Answer: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:tex

NEW QUESTION 93
- (Exam Topic 2)
Which CLI command can be used to export the tcpdump capture?

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

Answer: C

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

NEW QUESTION 96
- (Exam Topic 2)
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 99
- (Exam Topic 2)
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: ACF

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administra
The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:
Configure SAML AuthenticationConfigure TACACS+ AuthenticationConfigure RADIUS Authentication

NEW QUESTION 101
- (Exam Topic 2)
Which operation will impact the performance of the management plane?

A. WildFire Submissions
B. DoS Protection
C. decrypting SSL Sessions
D. Generating a SaaS Application Report.

Answer: D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSvCAK
Decrypting SSL Sessions is a dataplane task.DoS Protection is a Dataplane task.Wildfire submissions is a Dataplane task.Generating a SaaS Application report is a Management Plane function.

NEW QUESTION 105
- (Exam Topic 2)
Which event will happen if an administrator uses an Application Override Policy?

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

Answer: B

Explanation:

Reference:
https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Overrid
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown- applications#

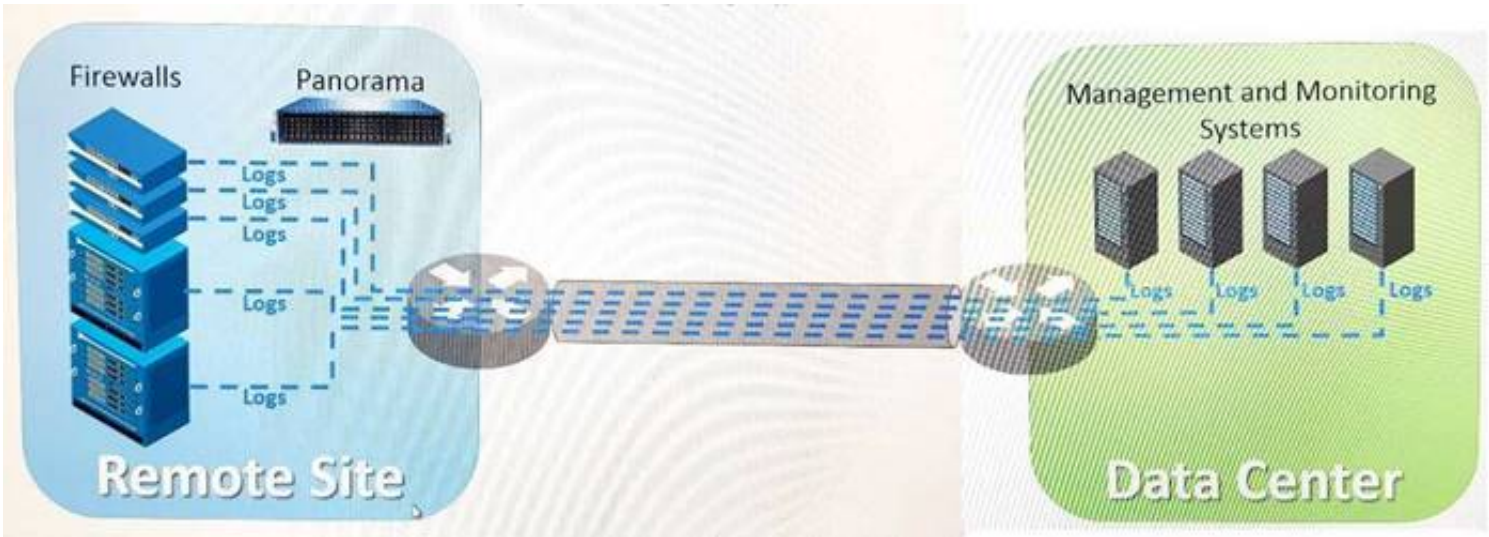
NEW QUESTION 108
- (Exam Topic 2)
A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers. Which option will protect the individual servers?

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: D

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/d To protect critical web or DNS servers on your network, protect the individual servers. To do this, set
appropriate flooding and resource protection thresholds in a DoS protection profile, and create a DoS protection policy rule that applies the profile to each server's IP address by adding the IP addresses as the rule's destination criteria.

NEW QUESTION 112
- (Exam Topic 2)
Refer to exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.
How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all existing monitoring/ security platforms?

A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
C. Configure log compression and optimization features on all remote firewalls.
D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Answer: A

Explanation:
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKFCA0
"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link"
"With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

NEW QUESTION 117
- (Exam Topic 2)
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: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFiCAK

NEW QUESTION 120
- (Exam Topic 2)
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
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClQSCA0

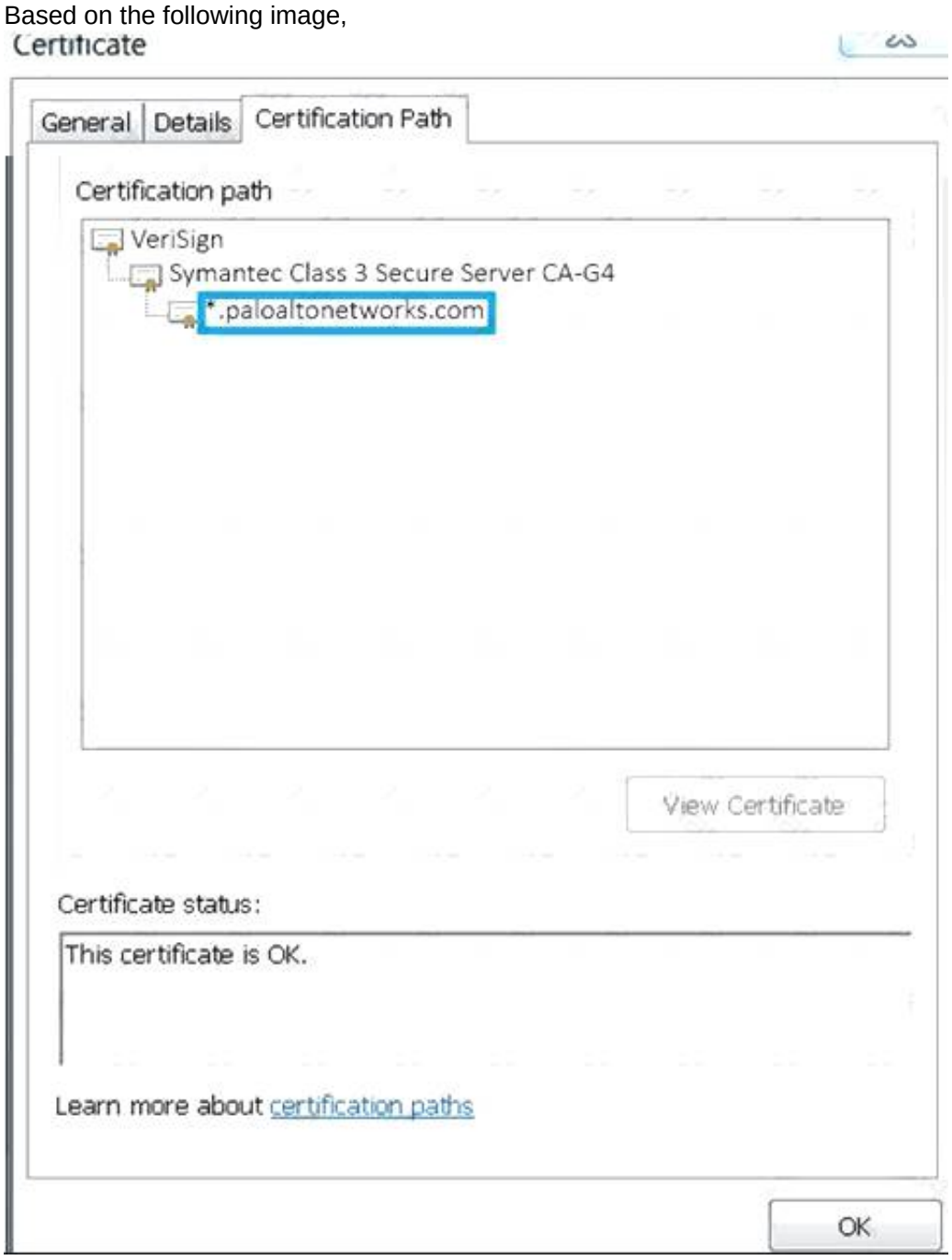
NEW QUESTION 125
- (Exam Topic 2)
Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

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

Answer: DEF

Explanation:
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

NEW QUESTION 127
- (Exam Topic 2)
Based on the following image,



what is the correct path of root, intermediate, and end-user certificate?

A. Palo Alto Networks > Symantec > VeriSign
B. Symantec > VeriSign > Palo Alto Networks
C. VeriSign > Palo Alto Networks > Symantec
D. VeriSign > Symantec > Palo Alto Networks

Answer: B

NEW QUESTION 132
- (Exam Topic 2)

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

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

Answer: A

Explanation:
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishi
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/cred phishing-prevention

NEW QUESTION 136
- (Exam Topic 2)
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

Explanation:
System Resources (widget)Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or
Panorama).https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/dashboard/dashboard-widg

NEW QUESTION 137
- (Exam Topic 2)
VPN traffic intended for an administrator’s Palo Alto Networks NGFW is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

A. Zone Protection
B. DoS Protection
C. Web Application
D. Replay

Answer: D

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec

NEW QUESTION 140
- (Exam Topic 2)
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 145
- (Exam Topic 2)
Which administrative authentication method supports authorization by an external service?

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

Answer: C

NEW QUESTION 150
- (Exam Topic 2)
Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

A. User-logon (Always on)
B. At-boot
C. On-demand
D. Pre-logon

Answer:

D

NEW QUESTION 151
- (Exam Topic 2)
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: ABC

NEW QUESTION 155
- (Exam Topic 2)
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

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

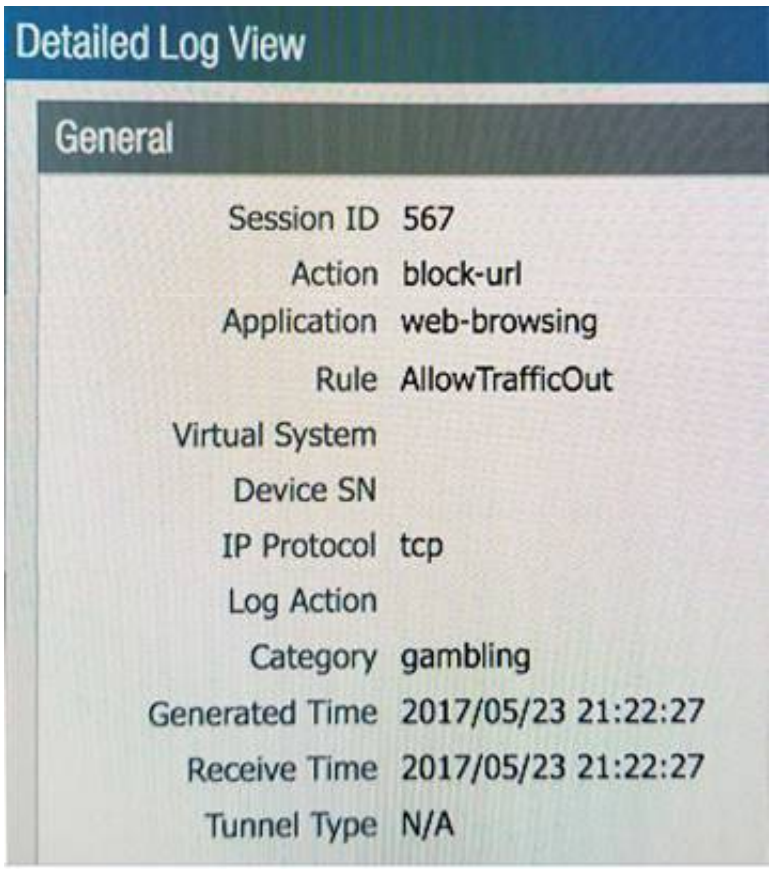
NEW QUESTION 158
- (Exam Topic 2)
A customer has an application that is being identified as unknown-top for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

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

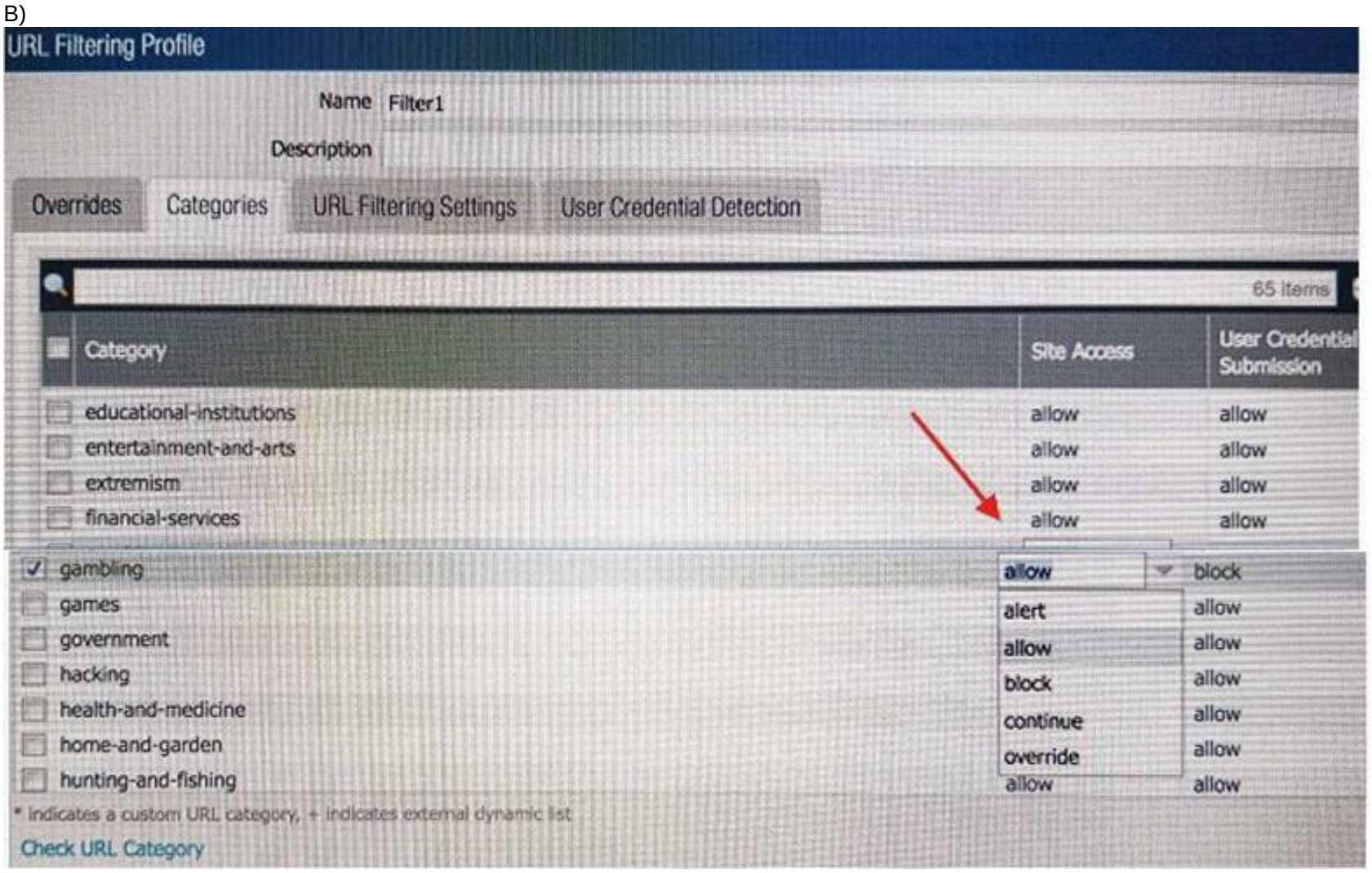
Answer: AC

Explanation:
Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box.Choices are limited to applications currently in the App-ID database.Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS.Use CasesThree primary uses cases for Application Override Policy are:
To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature
To bypass the Signature Match Engine (within the SP3 architecture) to improve processing timesA discussion of typical uses of application override and specific implementation examples is here:https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application

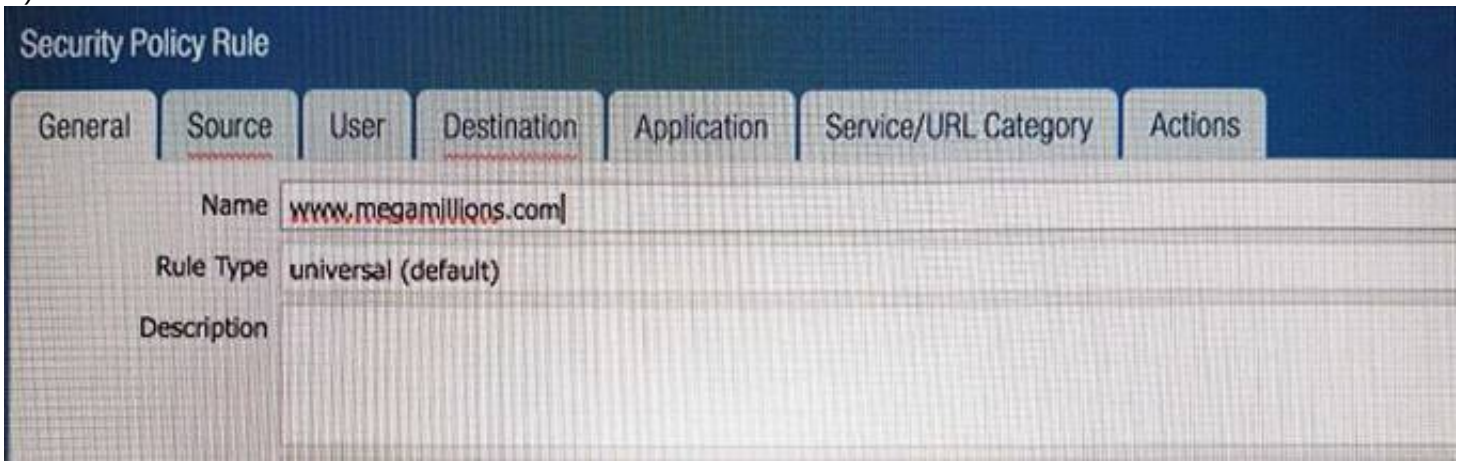
NEW QUESTION 159
- (Exam Topic 2)
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.
Which configuration change should the administrator make?
A)


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

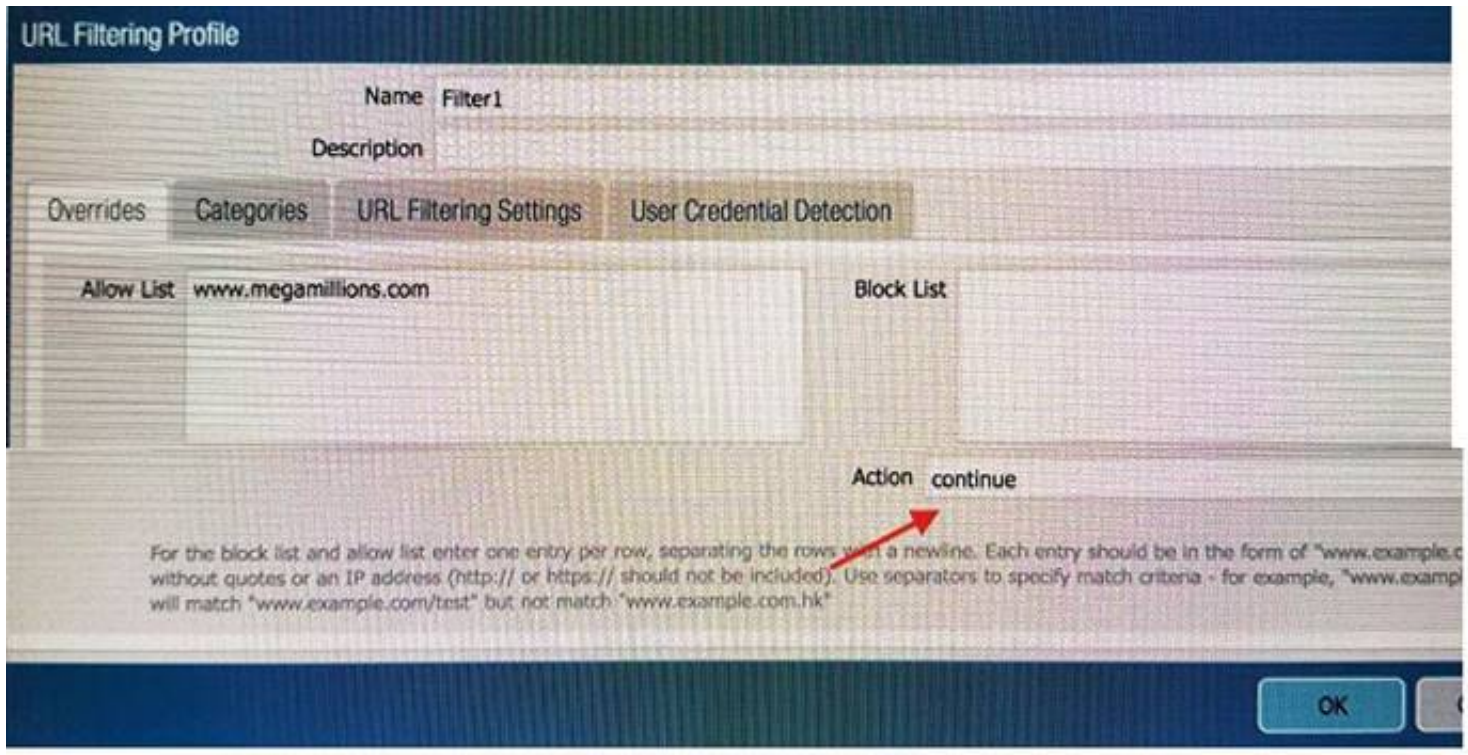
B)


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category

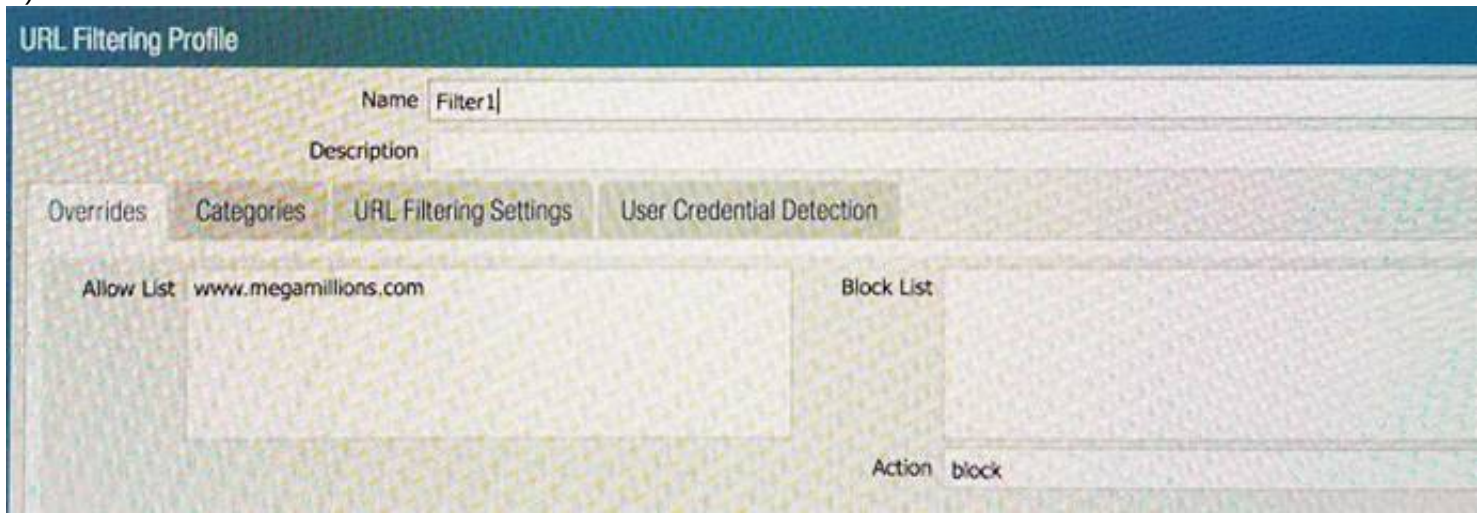
C)


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description

D)



E)



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

Answer: B

NEW QUESTION 160
- (Exam Topic 2)
Decrypted packets from the website https://www.microsoft.com will appear as which application and service within the Traffic log?

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

Answer: A

Explanation:
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted. Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS

NEW QUESTION 161
- (Exam Topic 2)
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

Explanation:
To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Monitor Syslog Senders for User Mapping.While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

NEW QUESTION 163
- (Exam Topic 2)
In High Availability, which information is transferred via the HA data link?

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

Answer: A

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

NEW QUESTION 167
- (Exam Topic 2)
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: A

NEW QUESTION 172
- (Exam Topic 2)
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 https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capt

NEW QUESTION 173
- (Exam Topic 2)
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 177
- (Exam Topic 2)
An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.
How would the administrator establish the chain of trust?

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

Answer: A

Explanation:
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/pla panorama-deployment

NEW QUESTION 178
- (Exam Topic 2)
Which feature can be configured on VM-Series firewalls?

A. aggregate interfaces
B. machine learning
C. multiple virtual systems
D. GlobalProtect

Answer: D

NEW QUESTION 182
- (Exam Topic 2)

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 185
- (Exam Topic 2)
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. Wildfire update package
B. User-ID agent
C. Anti virus update package
D. Application and Threats update package

Answer: D

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.
: https://live.paloaltonetworks.com/t5/Featured-Articles/Best-Practices-for-PAN-OS-Upgrade/ta-p/111045

NEW QUESTION 188
- (Exam Topic 2)
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 192
- (Exam Topic 2)
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 197
- (Exam Topic 1)
An administrator needs to gather information about the CPU utilization on both the management plane and the data plane
Where does the administrator view the desired data?

A. Monitor > Utilization
B. Resources Widget on the Dashboard
C. Support > Resources
D. Application Command and Control Center

Answer: A

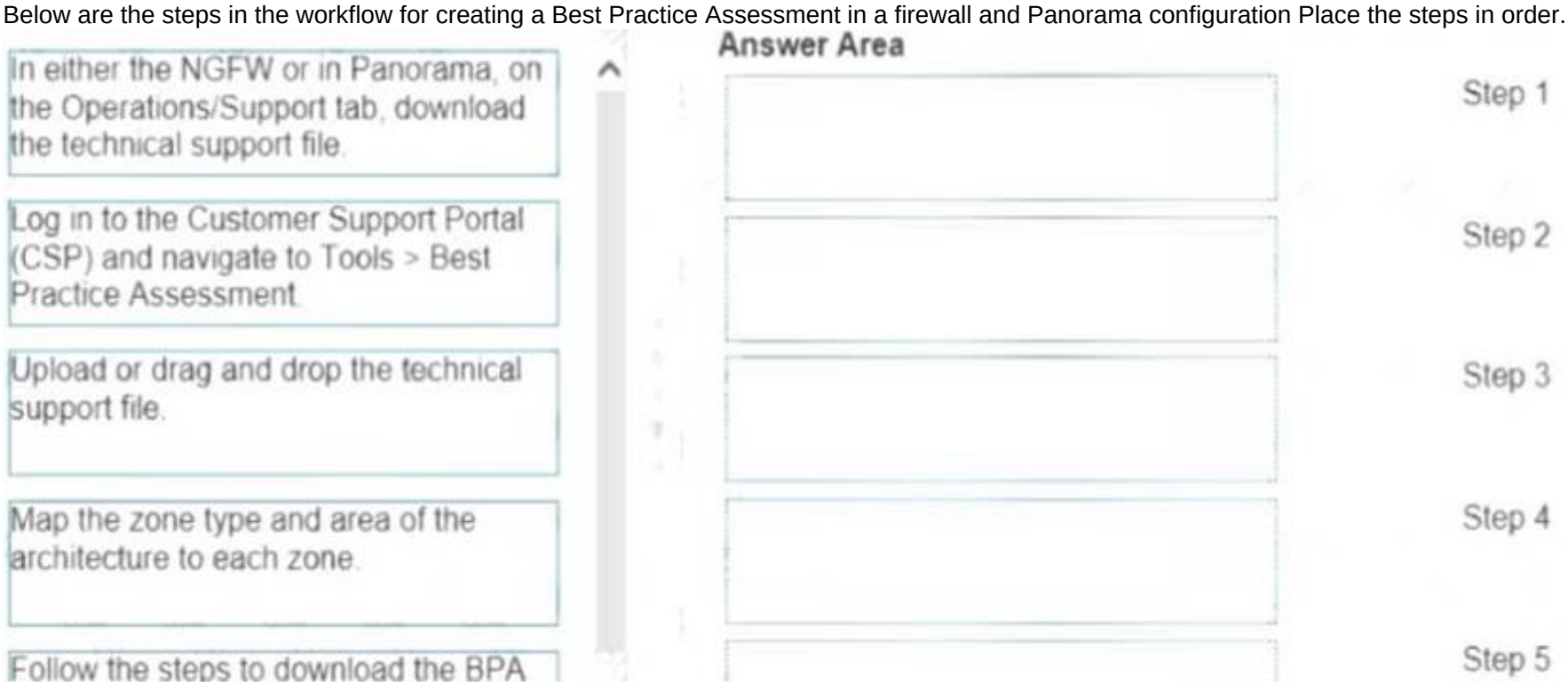
NEW QUESTION 199
- (Exam Topic 2)
An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.
Which priority is correct for the passive firewall?

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. (page 9)
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pd page 315

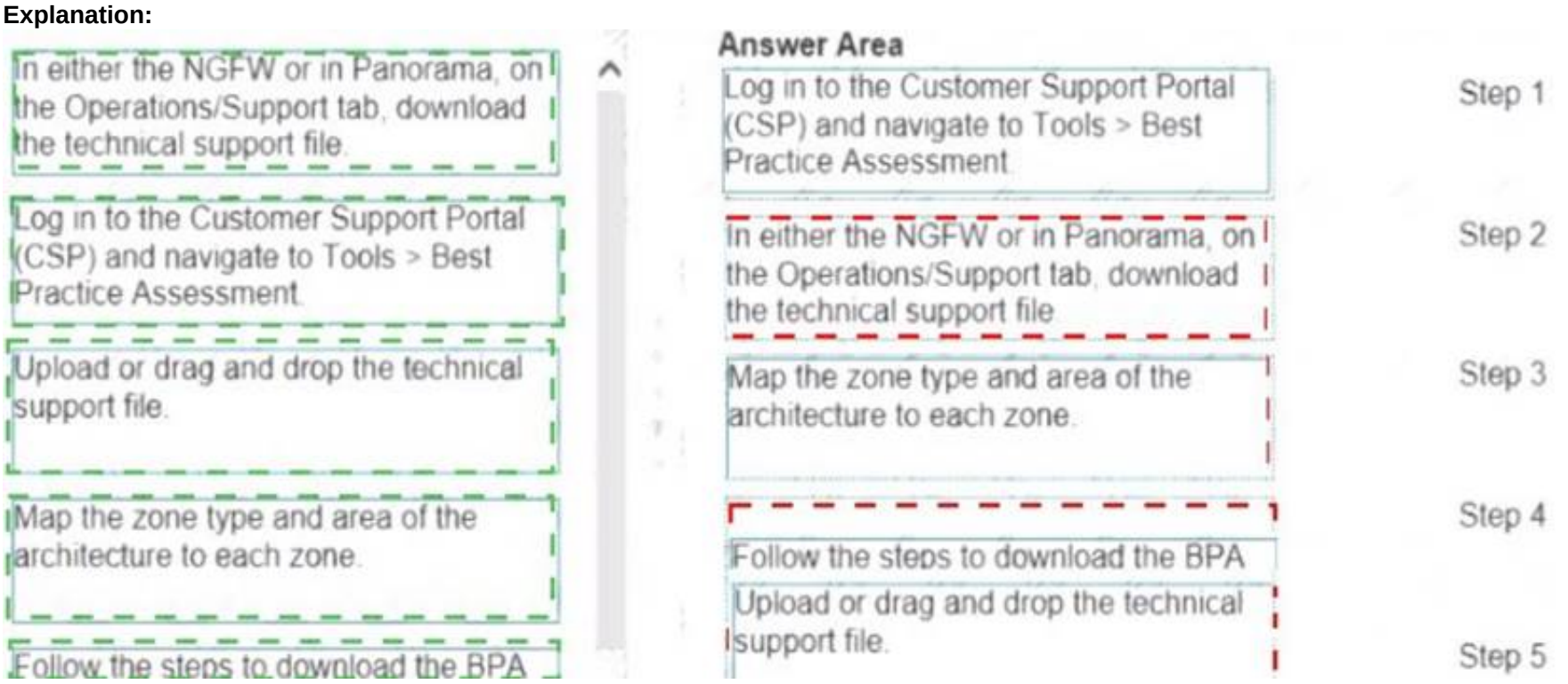
NEW QUESTION 203
- (Exam Topic 1)
Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration Place the steps in order.



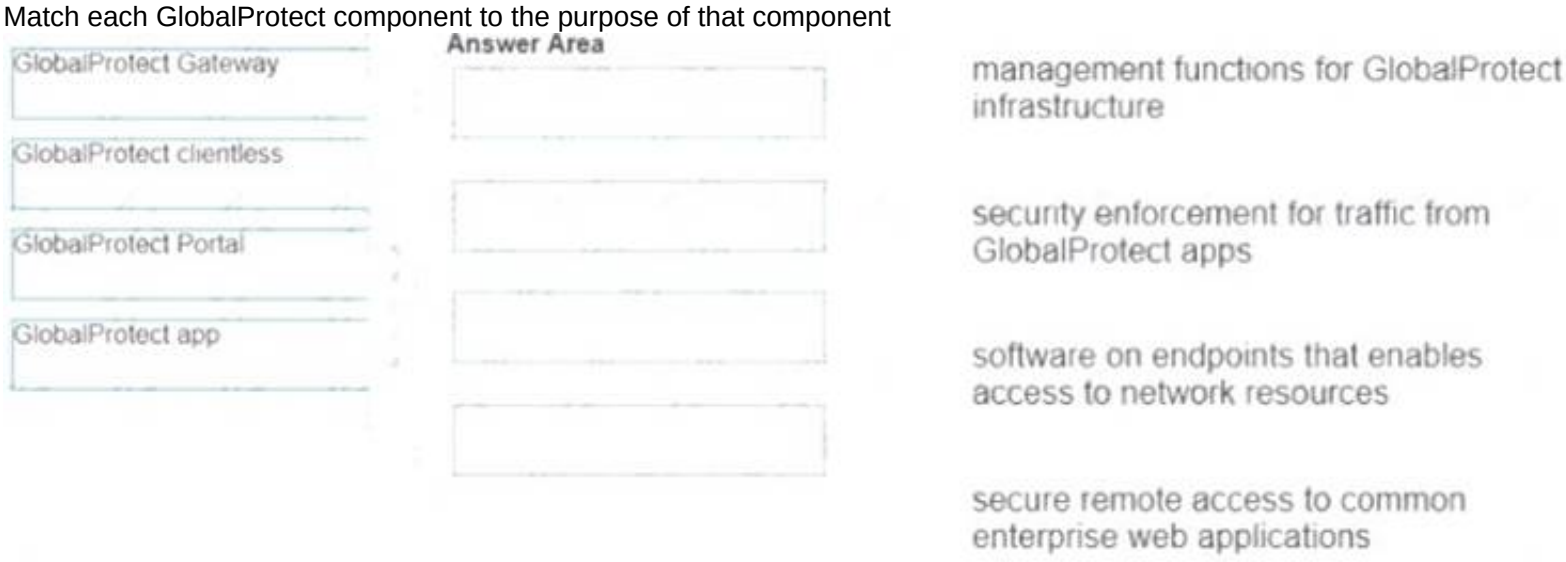
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 207
- (Exam Topic 1)
Match each GlobalProtect component to the purpose of that component



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps
The GlobalProtect app software runs on endpoints and enables access to your network resources

NEW QUESTION 211
- (Exam Topic 1)
In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

A. wildcard server certificate
B. enterprise CA certificate
C. client certificate
D. server certificate
E. self-signed CA certificate

Answer: BE

NEW QUESTION 214
- (Exam Topic 1)
When setting up a security profile which three items can you use? (Choose three)

A. Wildfire analysis
B. anti-ransom ware
C. antivirus
D. URL filtering
E. decryption profile

Answer: ACD

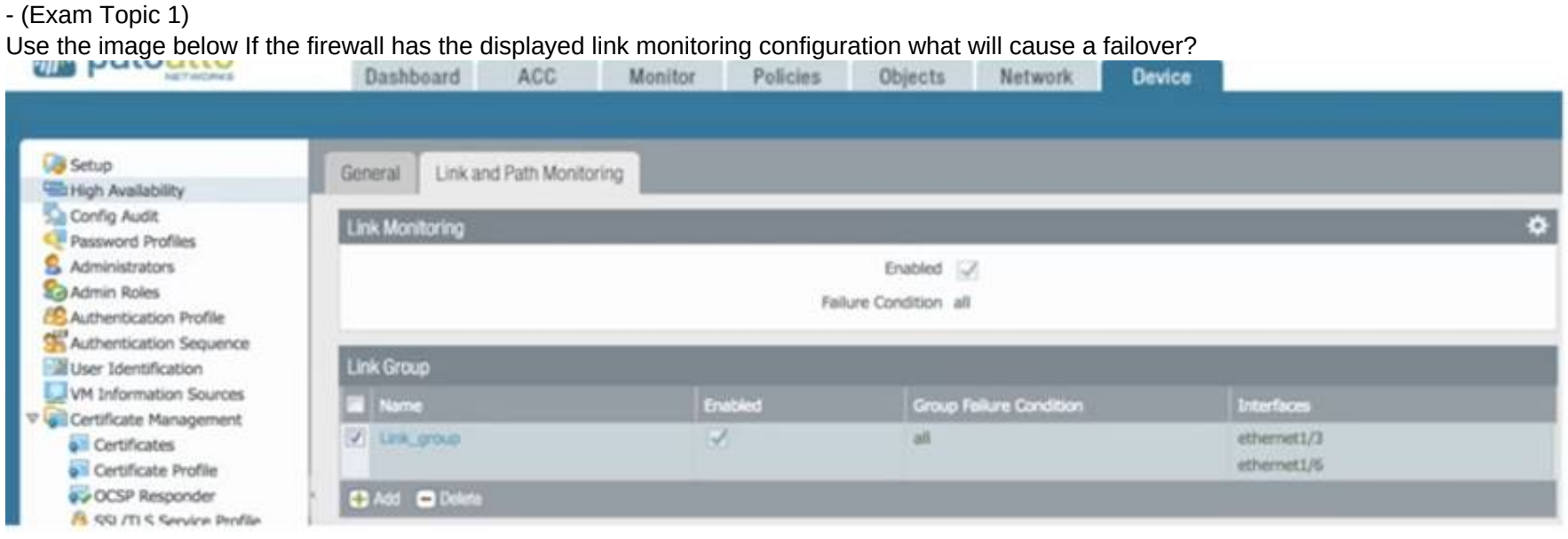
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION 219
- (Exam Topic 1)
In a firewall, which three decryption methods are valid? (Choose three)

A. SSL Inbound Inspection
B. SSL Outbound Proxyless Inspection
C. SSL Inbound Proxy
D. Decryption Mirror
E. SSH Proxy

Answer: ADE

NEW QUESTION 222
- (Exam Topic 1)
Use the image below If the firewall has the displayed link monitoring configuration what will cause a failover?



A. ethernet1/3 and ethernet1/6 going down
B. etheme!1/3 going down
C. ethernet1/6 going down
D. ethernet1/3 or ethernet1/6 going down

Answer: A

NEW QUESTION 227

- (Exam Topic 1)
An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant Which two statements are correct regarding the bootstrap package contents? (Choose two)

A. The /config /content and /software folders are mandatory while the /license and /plugin folders are optional
B. The bootstrap package is stored on an AFS share or a discrete container file bucket
C. The directory structure must include a /config /content, /software and /license folders
D. The init-cfg txt and bootstrap.xml files are both optional configuration items for the /config folder
E. The bootstrap xml file allows for automated deployment of VM-Senes firewalls with full network and policy configurations.

Answer: DE

NEW QUESTION 231
- (Exam Topic 1)
When you configure a Layer 3 interface what is one mandatory step?

A. Configure Security profiles, which need to be attached to each Layer 3 interface
B. Configure Interface Management profiles which need to be attached to each Layer 3 interface
C. Configure virtual routers to route the traffic for each Layer 3 interface
D. Configure service routes to route the traffic for each Layer 3 interface

Answer: A

NEW QUESTION 234
- (Exam Topic 1)
Before you upgrade a Palo Alto Networks NGFW what must you do?

A. Make sure that the PAN-OS support contract is valid for at least another year
B. Export a device state of the firewall
C. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.
D. Make sure that the firewall is running a supported version of the app + threat update

Answer: B

NEW QUESTION 235
- (Exam Topic 1)
When overriding a template configuration locally on a firewall, what should you consider?

A. Only Panorama can revert the override
B. Panorama will lose visibility into the overridden configuration
C. Panorama will update the template with the overridden value
D. The firewall template will show that it is out of sync within Panorama

Answer: B

NEW QUESTION 238
- (Exam Topic 1)
A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

A. Enterprise-Trusted-CA; which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system)i
B. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificateii
C. Enterprise-Intermediate-CAi
D. Enterprise-Root-CA which is verified only as Trusted Root CAAn end-user visits https //www example-website com/ with a server certificate Common Name (CN) www example-website com The firewall does the SSL Forward Proxy decryption for the website and the server certificate is not trusted by the firewallThe end-user's browser will show that the certificate for www example-website com was issued by which of the following?
E. Enterprise-Untrusted-CA which is a self-signed CA
F. Enterprise-Trusted-CA which is a self-signed CA
G. Enterprise-Intermediate-CA which wa
H. in turn, issued by Enterprise-Root-CA
I. Enterprise-Root-CA which is a self-signed CA

Answer: B

NEW QUESTION 239
- (Exam Topic 1)
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. Layer 3 interfaces but configuring EIGRP on the attached virtual router
B. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
C. Layer 3 or Aggregate Ethernet interfaces but configuring EIGRP on subinterfaces only
D. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel {with the GlobalProtect License to support LSVPN and EIGRP protocols)

Answer: D

NEW QUESTION 241
- (Exam Topic 1)

A firewall should be advertising the static route 10 2 0 0/24 into OSPF The configuration on the neighbor is correct but the route is not in the neighbor's routing table
Which two configurations should you check on the firewall'? (Choose two)

A. Within the redistribution profile ensure that Redist is selected
B. In the redistribution profile check that the source type is set to "ospf"
C. In the OSFP configuration ensure that the correct redistribution profile is selected in the OSPF Export Rules section
D. Ensure that the OSPF neighbor state is "2-Way"

Answer: AC

NEW QUESTION 246
- (Exam Topic 1)
A traffic log might list an application as "not-applicable" for which two reasons'? (Choose two)

A. 0The firewall did not install the session
B. The TCP connection terminated without identifying any application data
C. The firewall dropped a TCP SYN packet
D. There was not enough application data after the TCP connection was established

Answer: AD

NEW QUESTION 250
- (Exam Topic 1)
An engineer must configure the Decryption Broker feature
Which Decryption Broker security chain supports bi-directional traffic flow?

A. Layer 2 security chain
B. Layer 3 security chain
C. Transparent Bridge security chain
D. Transparent Proxy security chain

Answer: B

Explanation:
Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

NEW QUESTION 252
- (Exam Topic 1)
Which two statements correctly identify the number of Decryption Broker security chains that are supported on a pair of decryption-forwarding interfaces'? (Choose two)

A. A single transparent bridge security chain is supported per pair of interfaces
B. L3 security chains support up to 32 security chains
C. L3 security chains support up to 64 security chains
D. A single transparent bridge security chain is supported per firewall

Answer: AD

NEW QUESTION 254
- (Exam Topic 1)
What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

A. the website matches a category that is not allowed for most users
B. the website matches a high-risk category
C. the web server requires mutual authentication
D. the website matches a sensitive category

Answer: AD

NEW QUESTION 255
- (Exam Topic 1)
An engineer is planning an SSL decryption implementation
Which of the following statements is a best practice for SSL decryption?

A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate
B. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate
C. Use an enterprise CA-signed certificate for the Forward Untrust certificate
D. Use the same Forward Trust certificate on all firewalls in the network

Answer: D

NEW QUESTION 259
- (Exam Topic 1)
As a best practice, which URL category should you target first for SSL decryption*?

A. Online Storage and Backup
B. High Risk
C. Health and Medicine
D. Financial Services

Answer: A

NEW QUESTION 261
- (Exam Topic 1)
Which rule type controls end user SSL traffic to external websites?

A. SSL Outbound Proxyless Inspection
B. SSL Forward Proxy
C. SSL Inbound Inspection
D. SSH Proxy

Answer: C

NEW QUESTION 262
- (Exam Topic 1)
An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version
What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously
B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version
C. Upgrade Panorama to a version at or above the target firewall version
D. Export the device state perform the update, and then import the device state

Answer: A

NEW QUESTION 267
- (Exam Topic 1)
An administrator has a PA-820 firewall with an active Threat Prevention subscription The administrator is considering adding a WildFire subscription
How does adding the WildFire subscription improve the security posture of the organization1?

A. Protection against unknown malware can be provided in near real-time
B. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall
C. After 24 hours WildFire signatures are included in the antivirus update
D. WildFire and Threat Prevention combine to minimize the attack surface

Answer: D

NEW QUESTION 268
- (Exam Topic 1)
Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

A. not-applicable
B. incomplete
C. unknown-ip
D. unknown-udp

Answer: D

Explanation:
To safely enable applications you must classify all traffic, across all ports, all the time. With App-ID, the only applications that are typically classified as unknown traffic—tcp, udp or non-syn-tcp—in the ACC and the Traffic logs are commercially available applications that have not yet been added to App-ID, internal or custom applications on your network, or potential threats.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-cu

NEW QUESTION 272
- (Exam Topic 1)
In a Panorama template which three types of objects are configurable? (Choose three)

A. HIP objects
B. QoS profiles
C. interface management profiles
D. certificate profiles
E. security profiles

Answer: ACE

NEW QUESTION 275
- (Exam Topic 1)
Given the following configuration, which route is used for destination 10.10.0.4?

```
set network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 1" metric 30
set network virtual-router 2 routing-table ip static-route "Route 1" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 1" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 2" metric 20
set network virtual-router 2 routing-table ip static-route "Route 2" destination
10.10.0.0/24
set network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address
10.10.20.1
set network virtual-router 2 routing-table ip static-route "Route 3" metric 5
set network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0
set network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast
set network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address
192.168.1.2
set network virtual-router 2 routing-table ip static-route "Route 4" metric 10
set network virtual-router 2 routing-table ip static-route "Route 4" destination
10.10.1.0/25
set network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast
```

A. Route 4
B. Route 3
C. Route 1
D. Route 3

Answer: A

NEW QUESTION 278
- (Exam Topic 1)
When you configure an active/active high availability pair which two links can you use? (Choose two)

A. HA2 backup
B. HA3
C. Console Backup
D. HSCI-C

Answer: AC

NEW QUESTION 279
- (Exam Topic 1)
An administrator has 750 firewalls The administrator's central-management Panorama instance deploys dynamic updates to the firewalls
The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the
configuration does not appear what is the root cause?

A. Panorama has no connection to Palo Alto Networks update servers
B. Panorama does not have valid licenses to push the dynamic updates
C. No service route is configured on the firewalls to Palo Alto Networks update servers
D. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed

Answer: D

NEW QUESTION 281
- (Exam Topic 2)
What file type upload is supported as part of the basic WildFire service?

A. PE
B. BAT
C. VBS
D. ELF

Answer: A

NEW QUESTION 285
- (Exam Topic 2)
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: AC

Explanation:
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-e

NEW QUESTION 286
- (Exam Topic 2)
For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two)

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

Answer: BD

NEW QUESTION 291
- (Exam Topic 2)
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-po the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations
"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways.When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the
enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

NEW QUESTION 294
- (Exam Topic 2)
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: DE

NEW QUESTION 295
- (Exam Topic 2)
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

NEW QUESTION 296
- (Exam Topic 2)

To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure.

A. BGP (Border Gateway Protocol)
B. PBP (Packet Buffer Protection)
C. PGP (Packet Gateway Protocol)
D. PBP (Protocol Based Protection)

Answer: D

NEW QUESTION 300
- (Exam Topic 2)
Which option describes the operation of the automatic commit recovery feature?

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

Answer: A

NEW QUESTION 301
- (Exam Topic 2)
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: B

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEyCAK

NEW QUESTION 305
- (Exam Topic 2)
How can an administrator configure the NGFW to automatically quarantine a device using GlobalProtect?

A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users fromconnecting to the GlobalProtect gateway from a quarantined device
B. by using secunty policies, log forwarding profiles, and log settings.
C. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the approbate XSOAR playbook
D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 306
- (Exam Topic 2)
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: BC

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEWCA0

NEW QUESTION 307
- (Exam Topic 2)
An administrator wants to upgrade an NGFW from PAN-OS® 9.0 to PAN-OS® 10.0. 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

Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-t

NEW QUESTION 309
- (Exam Topic 2)
Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

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

Answer: A

Explanation:
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/1

NEW QUESTION 313
- (Exam Topic 3)
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

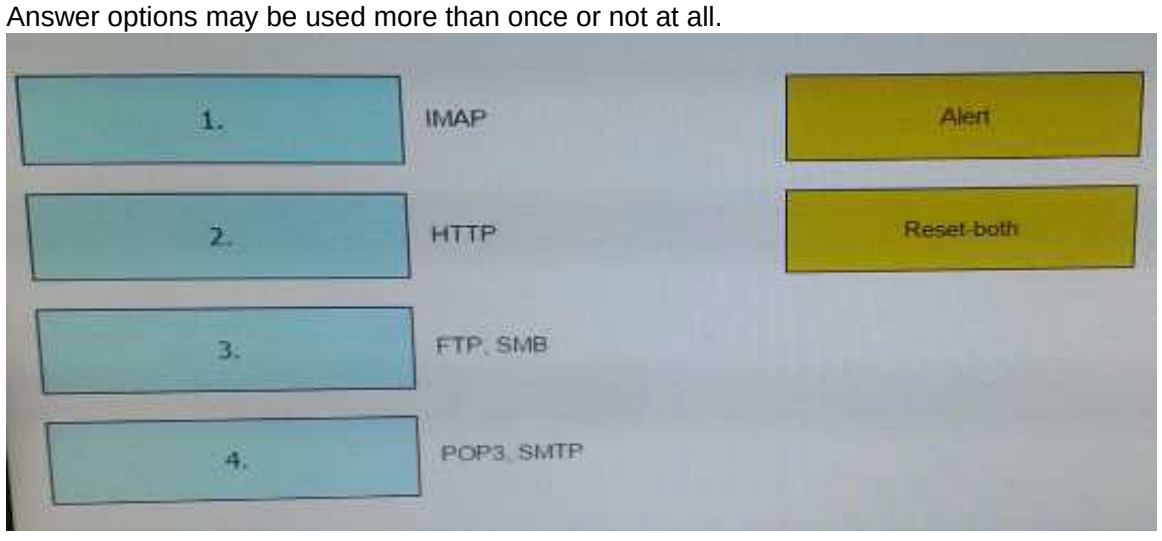
Answer: AD

NEW QUESTION 314
- (Exam Topic 3)
A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report?

A. Blocked Activity
B. Bandwidth Activity
C. Threat Activity
D. Network Activity

Answer: D

NEW QUESTION 315
- (Exam Topic 3)
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 317
- (Exam Topic 3)
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 322
- (Exam Topic 3)
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 324
- (Exam Topic 3)
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 329
- (Exam Topic 3)
During the packet flow process, which two processes are performed in application identification? (Choose two.)

A. pattern based application identification
B. application changed from content inspection
C. session application identified
D. application override policy match

Answer: AD

NEW QUESTION 332
- (Exam Topic 3)
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.paloaltonetworks.com/t5/Configuration-Articles/File-Blocking-Rulebase-and-Action-Precedence/ta-p

NEW QUESTION 335
- (Exam Topic 3)
Site-A and Site-B need to use IKEv2 to establish a VPN connection. Site A connects directly to the internet using a public IP address. Site-B uses a private IP address behind an ISP router to connect to the internet.
How should NAT Traversal be implemented for the VPN connection to be established between Site-A and Site-B?

A. Enable on Site-A only
B. Enable on Site-B only
C. Enable on Site-B only with passive mode
D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 339
- (Exam Topic 3)
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 344
- (Exam Topic 3)
Which three options does the WF-500 appliance support for local analysis? (Choose three)

A. E-mail links
B. APK files
C. jar files
D. PNG files
E. Portable Executable (PE) files

Answer: ACE

NEW QUESTION 349
- (Exam Topic 3)
A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles> Anti-Spyware and select default profile.
What should be done next?

A. Click the simple-critical rule and then click the Action drop-down list.
B. Click the Exceptions tab and then click show all signatures.
C. View the default actions displayed in the Action column.
D. Click the Rules tab and then look for rules with "default" in the Action column.

Answer: B

NEW QUESTION 352
- (Exam Topic 3)
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 357
- (Exam Topic 3)
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 360
- (Exam Topic 3)
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 364
- (Exam Topic 3)
A network security engineer needs to configure a virtual router using IPv6 addresses. Which two routing options support these addresses? (Choose two)

A. BGP not sure
B. OSPFv3
C. RIP
D. Static Route

Answer: BD

Explanation:
https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols

NEW QUESTION 367
- (Exam Topic 3)
Which client software can be used to connect remote Linux client into a Palo Alto Networks Infrastructure without sacrificing the ability to scan traffic and protect against threats?

A. X-Auth IPsec VPN
B. GlobalProtect Apple IOS
C. GlobalProtect SSL
D. GlobalProtect Linux

Answer: A

Explanation:
(http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/)

NEW QUESTION 372
- (Exam Topic 3)
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-Tr

NEW QUESTION 375
- (Exam Topic 3)
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 380
- (Exam Topic 3)
Which three rule types are available when defining policies in Panorama? (Choose three.)

A. Pre Rules
B. Post Rules
C. Default Rules
D. Stealth Rules
E. Clean Up Rules

Answer: ABC

Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defini

NEW QUESTION 381
- (Exam Topic 3)
Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two)

A. The devices are pre-configured with a virtual wire pair out the first two interfaces.
B. The devices are licensed and ready for deployment.
C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.
D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.
E. The interface are pingable.

Answer: BC

NEW QUESTION 383
- (Exam Topic 3)

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 387
- (Exam Topic 3)
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.com/t5/Configuration-Articles/How-to-Configure-GlobalProtect/ta-p/58351)

NEW QUESTION 391
- (Exam Topic 3)
An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:
less mp-log ikemgr.log:

```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:52:33 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <==== Due to
timeout.
2014-08-05 03:52:33 [INFO]: ====> PHASE-1 SA DELETED <====
====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <====
2014-08-05 03:53:54 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed.SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <==== Due to
timeout.
2014-08-05 03:53:54 [INFO]: ====> PHASE-1 SA DELETED <====
```

What could be the cause of this problem?

A. The public IP addresse do not match for both the Palo Alto Networks Firewall and the ASA.
B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.
C. The shared secerts do not match between the Palo Alto firewall and the ASA
D. The deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 393
- (Exam Topic 3)
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

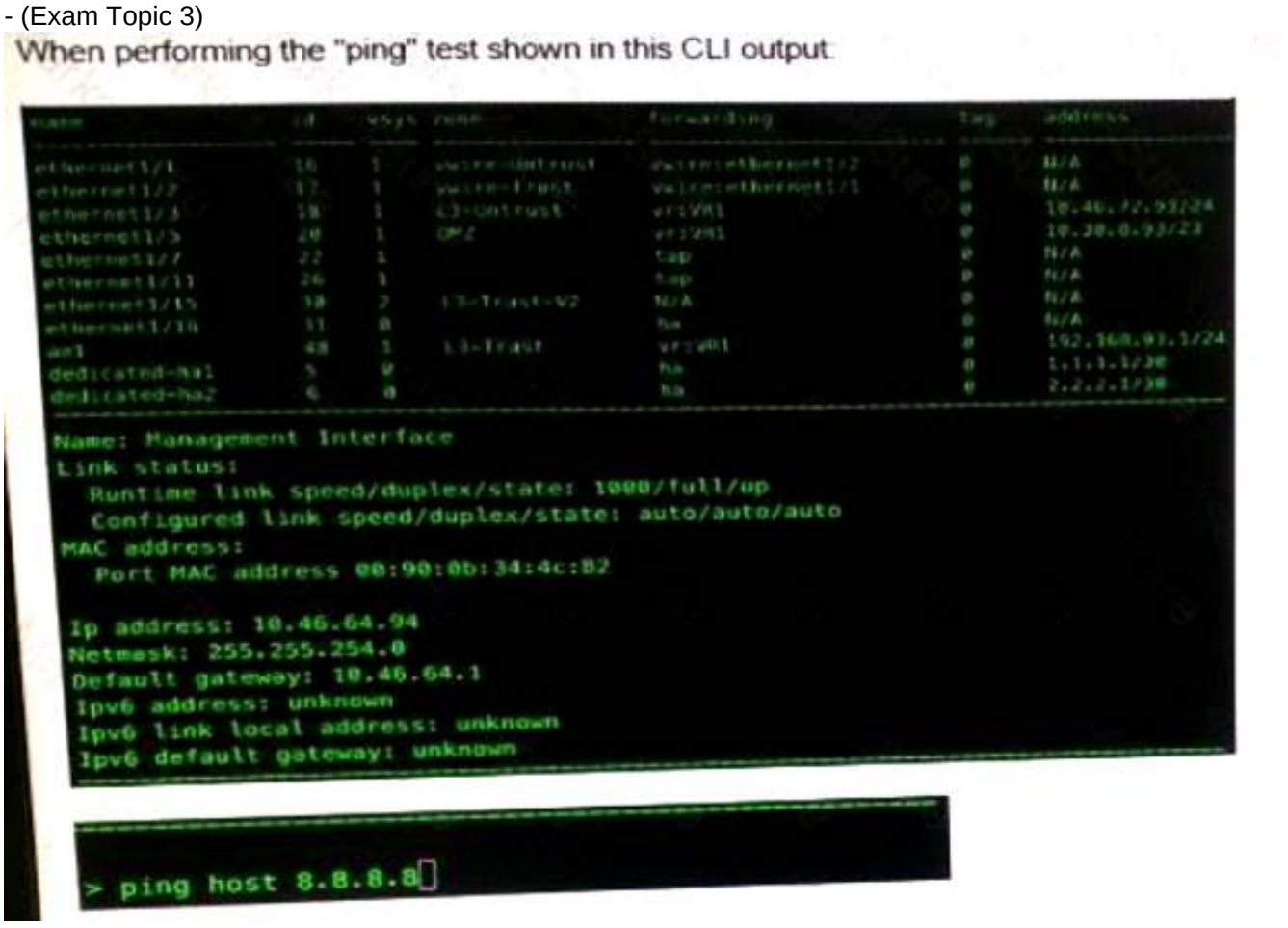
Explanation:
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/deter

NEW QUESTION 397
- (Exam Topic 3)
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 401
- (Exam Topic 3)
When performing the "ping" test shown in this CLI output



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 402
- (Exam Topic 3)
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 404
- (Exam Topic 3)
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 406
- (Exam Topic 3)
What must be used in Security Policy Rule that contain addresses where NAT policy applies?

A. Pre-NAT addresse and Pre-NAT zones
B. Post-NAT addresse and Post-Nat zones
C. Pre-NAT addresse and Post-Nat zones

D. Post-Nat addresses and Pre-NAT zones

Answer: C

NEW QUESTION 407
- (Exam Topic 3) A
users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com goes to http://www company com How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

A. Create and add a monitor profile with an action of fail over in the PBF rule in question
B. Create and add a monitor profile with an action of wait recover in the PBF rule in question
C. Configure path monitoring for the next hop gateway on the default route in the virtual router
D. Enable and configure a link monitoring profile for the external interface of the firewall

Answer: C

NEW QUESTION 409
- (Exam Topic 3)
An administrator has left a firewall to use the data of port for all management service which there functions are performed by the data face? (Choose three.)

A. NTP
B. Antivirus
C. Wildfire updates
D. NAT
E. File tracking

Answer: ACD

NEW QUESTION 411
- (Exam Topic 3)
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 416
- (Exam Topic 3)
Panorama provides which two SD_WAN functions? (Choose two.)

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

Answer: CD

NEW QUESTION 418
- (Exam Topic 3)
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

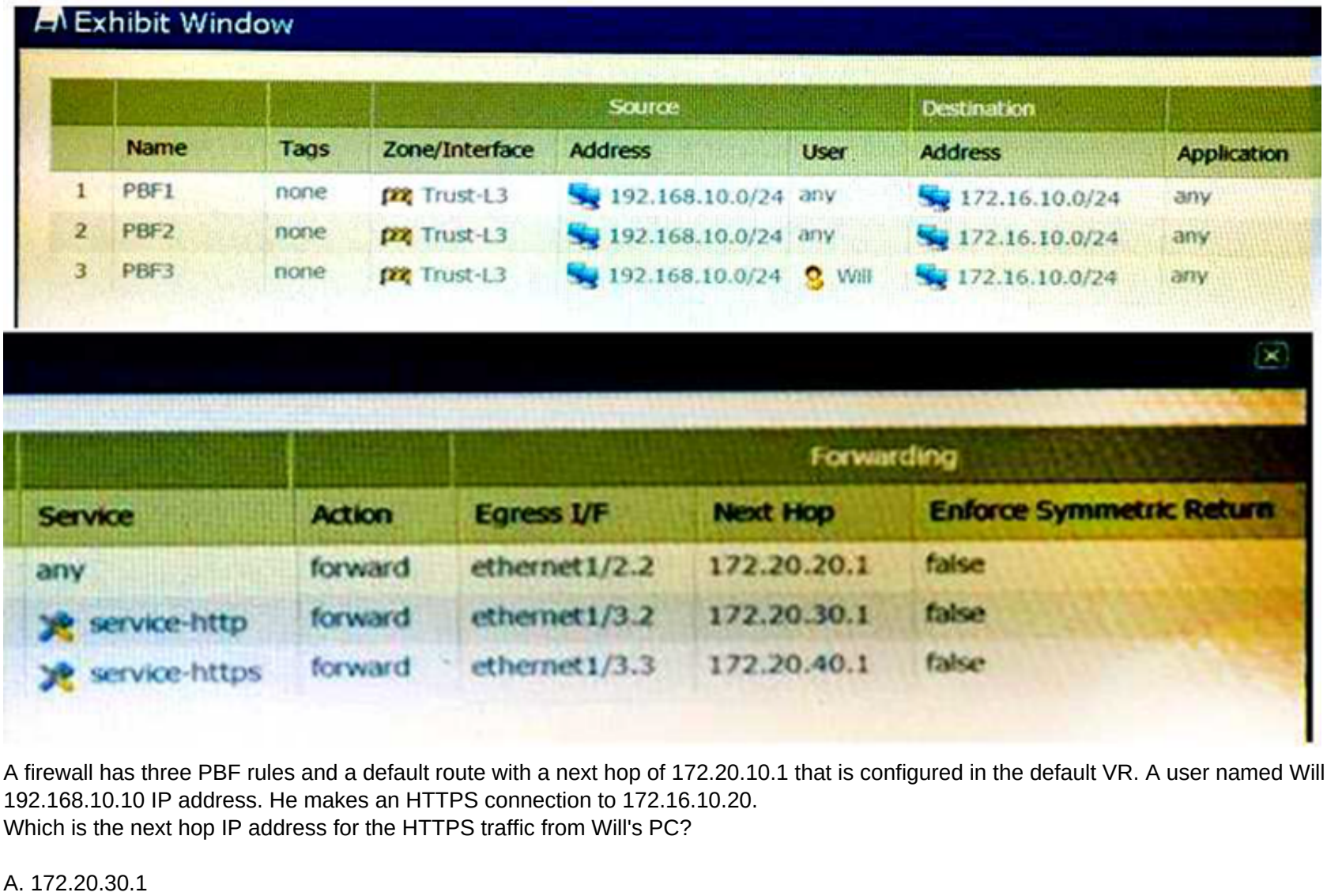
NEW QUESTION 419
- (Exam Topic 3)
How can a Palo Alto Networks firewall be configured to send syslog messages in a format compatible with non-standard syslog servers?

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 424

- (Exam Topic 3)
Click the Exhibit button below,

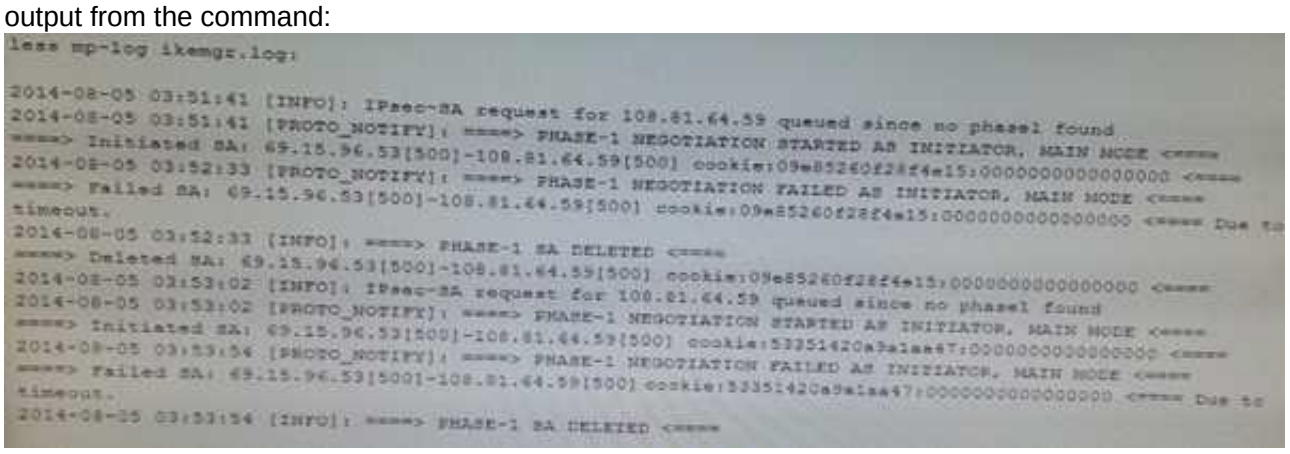


A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address. He makes an HTTPS connection to 172.16.10.20.
Which is the next hop IP address for the HTTPS traffic from Will's PC?

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

Answer: C

NEW QUESTION 428
- (Exam Topic 3)
An administrator is configuring an IPSec VPN to a Cisco ASA at the administrator's home and experiencing issues completing the connection. the following is the output from the command:



What could be the cause of this problem?

A. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA.
B. The Proxy IDs on the Palo Alto Networks Firewall do not match the setting on the ASA.
C. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.
D. The shared secrets do not match between the Palo Alto Networks Firewall and the ASA.

Answer: C

NEW QUESTION 432
- (Exam Topic 3)
Which operation will impact performance of the management plane?

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

Answer: C

NEW QUESTION 437
- (Exam Topic 3)
Which interface configuration will accept specific VLAN IDs?

A. Tab Mode
B. Subinterface
C. Access Interface
D. Trunk Interface

Answer: B

NEW QUESTION 442
- (Exam Topic 3)
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-u

NEW QUESTION 445
- (Exam Topic 3)
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 450
- (Exam Topic 3)
What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three)

A. Clean
B. Bengin
C. Adware
D. Suspicious
E. Grayware
F. Malware

Answer: BEF

Explanation:
https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw

NEW QUESTION 454
- (Exam Topic 3)
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 457
- (Exam Topic 3)
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 458
- (Exam Topic 3)
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 460
- (Exam Topic 3)
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 465
- (Exam Topic 3)
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 469
- (Exam Topic 3)
Palo Alto Networks maintains a dynamic database of malicious domains.
Which two Security Platform components use this database to prevent threats? (Choose two)

A. Brute-force signatures
B. BrightCloud Url Filtering
C. PAN-DB URL Filtering
D. DNS-based command-and-control signatures

Answer: CD

NEW QUESTION 472
.....

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