

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 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 CLI-ref.pdf

NEW QUESTION 2

- (Exam Topic 2)

An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

- A. default-browser-challenge
- B. default-authentication-bypass
- C. default-web-format
- D. default-no-captive-portal

Answer: D

NEW QUESTION 3

- (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 4

- (Exam Topic 2)

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: AB

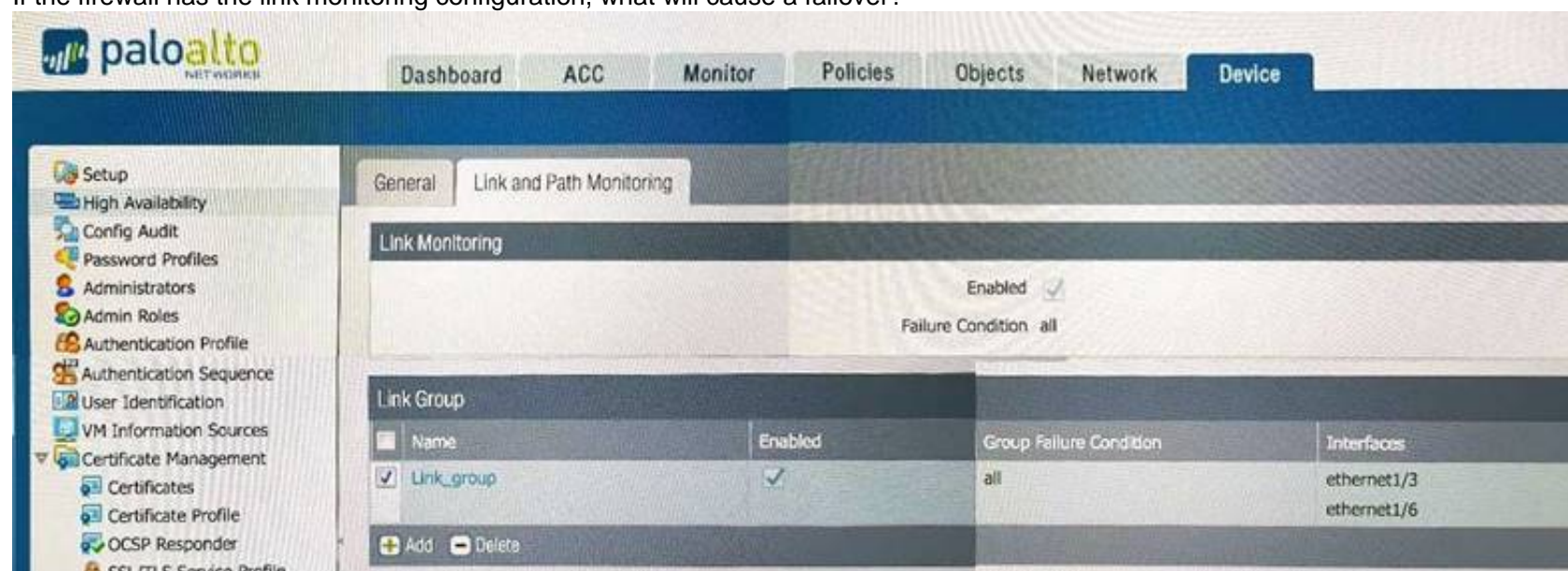
Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0> <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

NEW QUESTION 5

- (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 6

- (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 7

- (Exam Topic 2)

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (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 9

- (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-intel>

NEW QUESTION 10

- (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 10

- (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 14

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 18

- (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 21

- (Exam Topic 2)

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

- A. Configuration Logs
- B. System Logs
- C. Task Manager
- D. Traffic Logs

Answer: BC

NEW QUESTION 25

- (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?

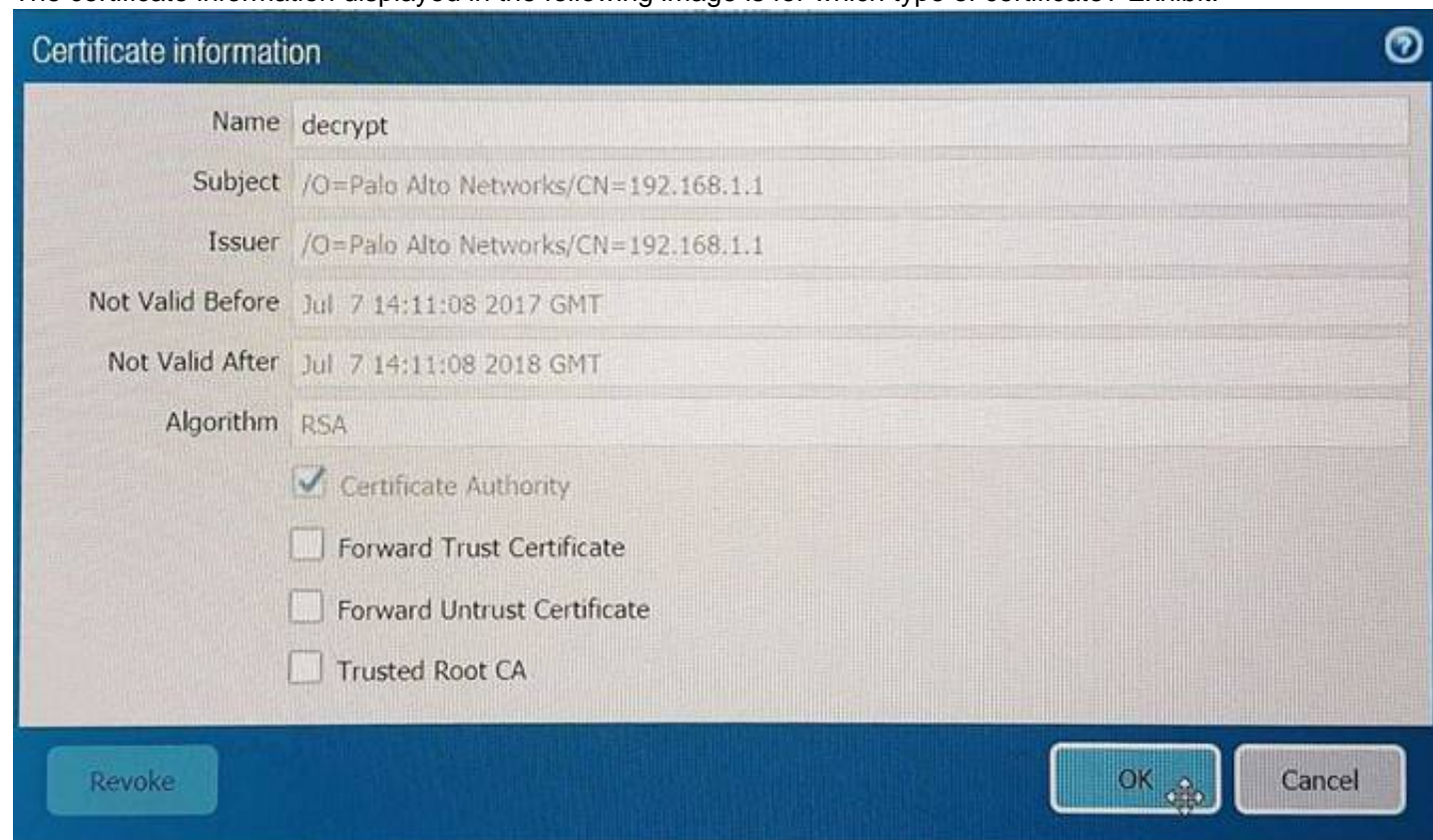
- A. Custom application
- B. System logs show an application error and neither signature is used.
- C. Downloaded application
- D. Custom and downloaded application signature files are merged and both are used

Answer: C

NEW QUESTION 28

- (Exam Topic 2)

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: B

NEW QUESTION 31

- (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 32

- (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 33

- (Exam Topic 2)

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

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

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

Answer: AB

Explanation:

Reference:

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

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRqCAK>

VLAN interface is not necessary but in this scenario we assume it is. Create VLAN object, VLAN interface and VLAN Zone. Attach VLAN interface to VLAN object together with two L2 interfaces then attach VLAN interface to virtual router. Without VLAN interface you can pass traffic between interfaces on the same network and with VLAN interface you can route traffic to other networks.

NEW QUESTION 35

- (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 38

- (Exam Topic 2)

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

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides which settings to send.

Answer: A

Explanation:

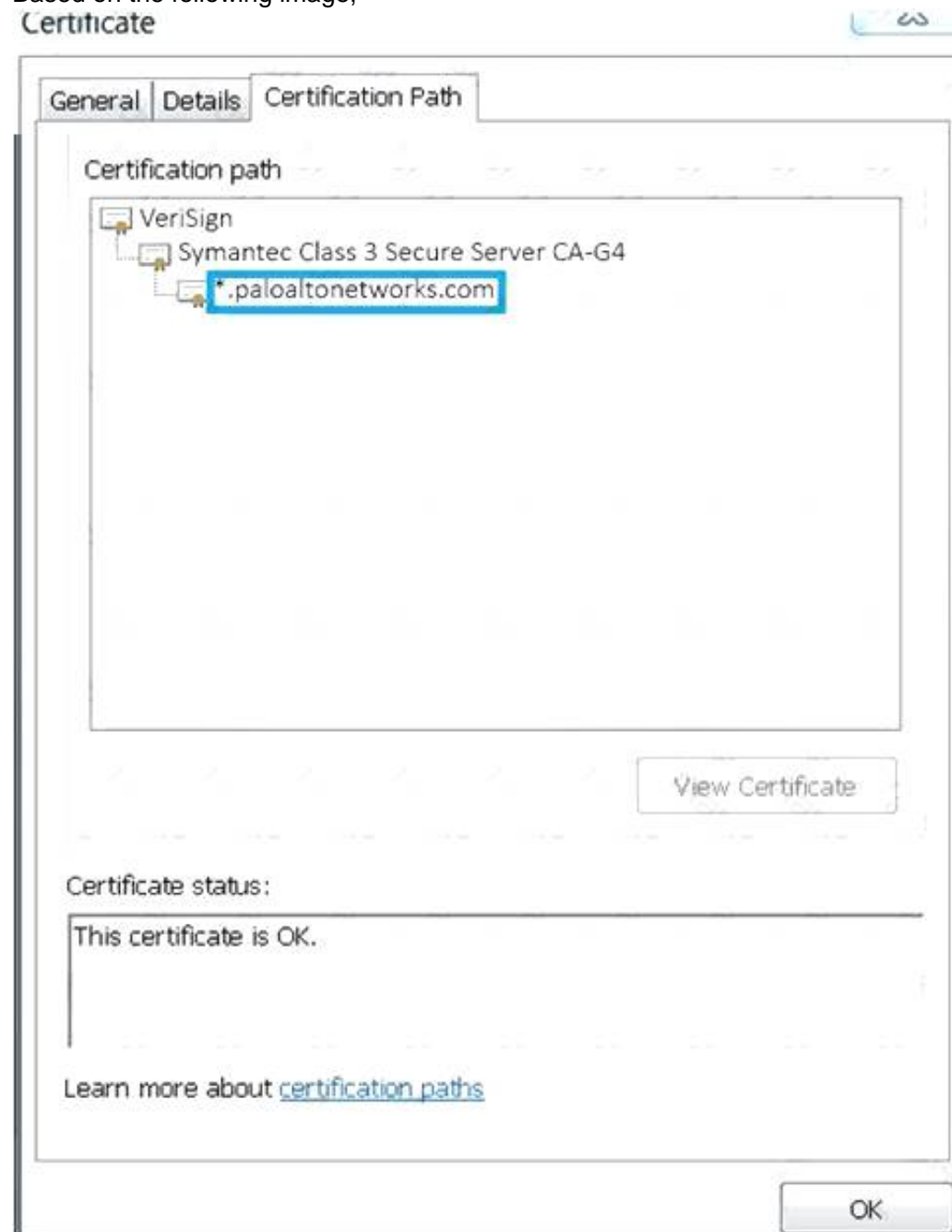
Reference:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

NEW QUESTION 39

- (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 41

- (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. Matching any valid corporate username.

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishing-prevention>

Reference:

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

NEW QUESTION 46

- (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 49

- (Exam Topic 2)

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

Answer: AB

NEW QUESTION 52

- (Exam Topic 2)

A customer wants to set up a site-to-site VPN using tunnel interfaces? Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. Vpn-tunnel.1024
- B. vpn-tunne.1
- C. tunnel 1025
- D. tunne
- E. 1

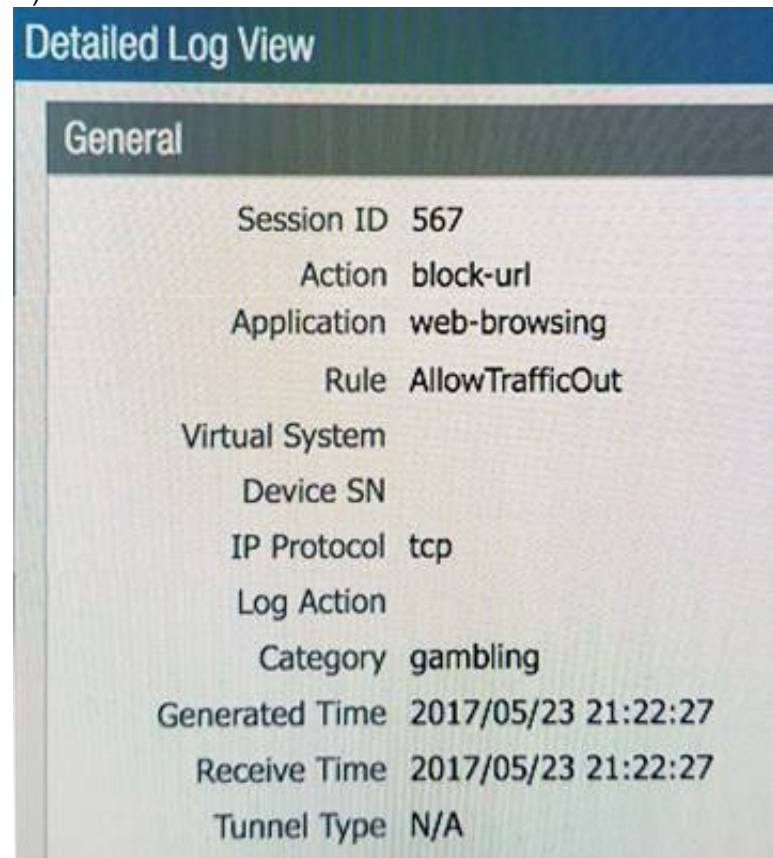
Answer: CD

NEW QUESTION 55

- (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)



B)

URL Filtering Profile

Name: Filter1
 Description:

Overrides Categories **URL Filtering Settings** User Credential Detection

65 items

Category	Site Access	User Credential Submission
<input type="checkbox"/> educational-institutions	allow	allow
<input type="checkbox"/> entertainment-and-arts	allow	allow
<input type="checkbox"/> extremism	allow	allow
<input type="checkbox"/> financial-services	allow	allow
<input checked="" type="checkbox"/> gambling	allow	block
<input type="checkbox"/> games	alert	allow
<input type="checkbox"/> government	allow	allow
<input type="checkbox"/> hacking	block	allow
<input type="checkbox"/> health-and-medicine	continue	allow
<input type="checkbox"/> home-and-garden	override	allow
<input type="checkbox"/> hunting-and-fishing	allow	allow

* Indicates a custom URL category, + indicates external dynamic list
[Check URL Category](#)

C)

Security Policy Rule

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

Name: www.megamillions.com

Rule Type: universal (default)

Description:

D)

URL Filtering Profile

Name: Filter1
 Description:

Overrides Categories URL Filtering Settings **User Credential Detection**

Allow List: www.megamillions.com

Block List:

Action: continue

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

OK

E)

URL Filtering Profile

Name: Filter1
 Description:

Overrides Categories URL Filtering Settings **User Credential Detection**

Allow List: www.megamillions.com

Block List:

Action: block

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

Answer: B

NEW QUESTION 59

- (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 62

- (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 65

- (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 69

- (Exam Topic 2)

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

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

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.ht>

NEW QUESTION 73

- (Exam Topic 2)

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

- A. Correlated Event

- Answer: B**

- (Exam Topic 2)

Which three firewall states are valid? (Choose three)

- Answer: ADE**

Reference:

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

- (Exam Topic 2)

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

- Answer: AC**

- (Exam Topic 1)

An administrator wants to enable zone protection. Before doing so, what must the administrator consider?

- Answer: A**

- (Exam Topic 1)

Refer to the exhibit.

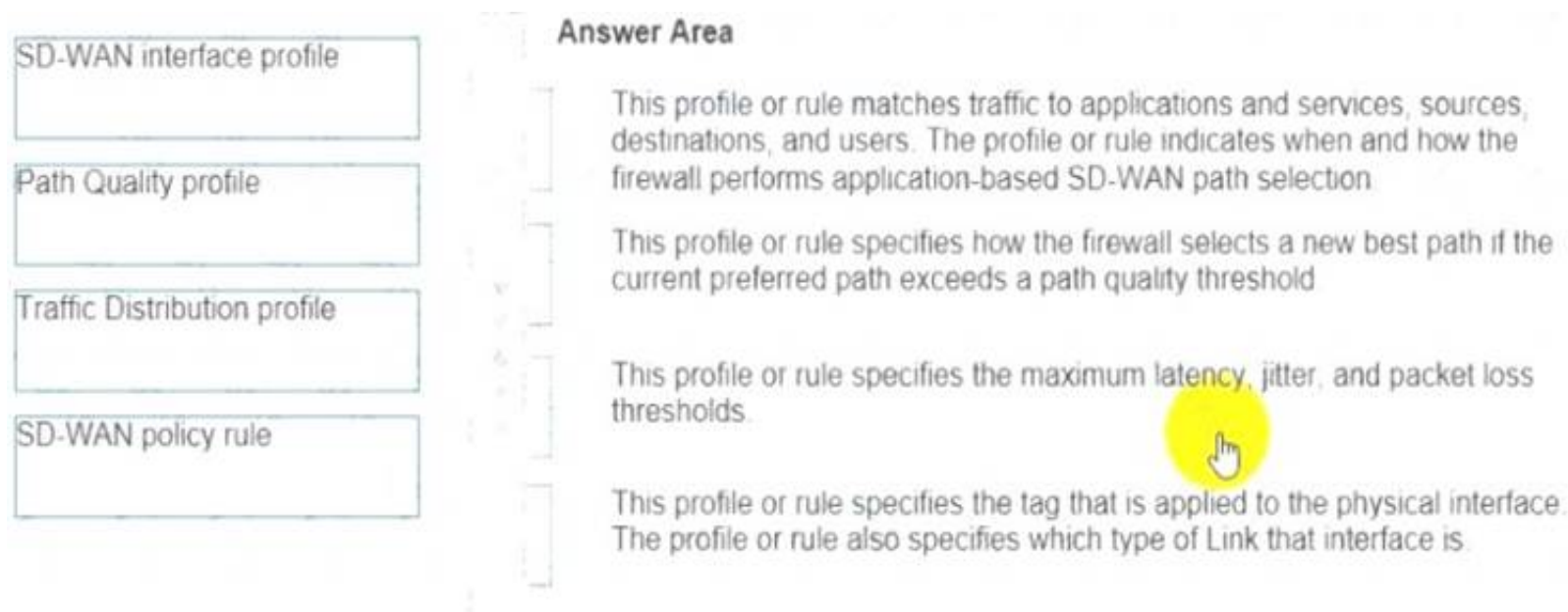
NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
Domain-Root-Cert	CN = demo.local	CN = demo.local			Jul 23 16:50:22 2021 GMT	valid	RSA	Trusted Root CA
Domain-Sub-CA	CN = sub.demo.local	CN = demo.local			Jul 23 16:52:26 2021 GMT	valid	RSA	
Forward-Trust	CN = fwdtrust.demo.local	CN = sub.demo.local			Jul 23 16:53:38 2021 GMT	valid	RSA	

Which certificate can be used as the Forward Trust certificate?

- Answer: D**

- (Exam Topic 1)

Match each SD-WAN configuration element to the description of that element.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- > An SD-WAN Interface Profile specifies the Tag that you apply to the physical interface, and also specifies the type of Link that interface is (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, or other). The Interface Profile is also where you specify the maximum upload and download speeds (in Mbps) of the ISP's connection. You can also change whether the firewall monitors the path frequently or not; the firewall monitors link types appropriately by default.
- > A Layer3 Ethernet Interface with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this interface (red arrow) to indicate the characteristics of the interface. The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.
- > A virtual SD-WAN Interface is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)
- > A Path Quality Profile specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.
- > A Traffic Distribution Profile specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.
- > The preceding elements come together in SD-WAN Policy Rules. The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.
<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements.h>

NEW QUESTION 94

- (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 95

- (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 97

- (Exam Topic 1)

Given the following snippet of a WildFire submission log, did the end-user get access to the requested information and why or why not?

TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
wildfire	smtp-base	allow	Watch Public DNS and SMTP	d96eb449-2...		high			malicious
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		
file	smtp-base	alert	Watch Public DNS and SMTP	d96eb449-2...		low	any		

- A. Ye
- B. because the action is set to "allow "
- C. No because WildFire categorized a file with the verdict "malicious"
- D. Yes because the action is set to "alert"
- E. No because WildFire classified the seventy as "high."

Answer: B

NEW QUESTION 100

- (Exam Topic 1)

Match each type of DoS attack to an example of that type of attack

application-based attack

protocol-based attack

volumetric attack

Answer Area

Slowloris attack

SYN flood attack

UDP flood attack

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Plan to defend your network against different types of DoS attacks:

➤ Application-Based Attacks

—Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example of this is the Slowloris attack.

➤ Protocol-Based Attacks

—Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.

➤ Volumetric Attacks

—High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources. An example of this is a UDP flood attack.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht>

NEW QUESTION 102

- (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 104

- (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 105

- (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 107

- (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 108

- (Exam Topic 1)

What are two characteristic types that can be defined for a variable? (Choose two)

- A. zone
- B. FQDN
- C. path group
- D. IP netmask

Answer: BD

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-tem>

NEW QUESTION 109

- (Exam Topic 1)

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall. An end-user visits the untrusted website [https //www firewall-do-not-trust-website com](https://www.firewall-do-not-trust-website.com)

<input type="checkbox"/>	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...
<input type="checkbox"/>	Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:48:4...	valid	RSA
<input type="checkbox"/>	Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:49:0...	valid	RSA
<input type="checkbox"/>	Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:55:2...	valid	RSA
<input type="checkbox"/>	Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:56:4...	valid	RSA

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

- A. Forward-Untrust-Certificate
- B. Forward-Trust-Certificate
- C. Firewall-CA
- D. Firewall-Trusted-Root-CA

Answer: B

NEW QUESTION 110

- (Exam Topic 1)

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three)

- A. Destination Zone
- B. App-ID
- C. Custom URL Category
- D. User-ID
- E. Source Interface

Answer: ADE

NEW QUESTION 111

- (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 113

- (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 116

- (Exam Topic 1)

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world Panorama will manage the firewalls

The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration

Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. variables
- B. template stacks
- C. collector groups
- D. virtual systems

Answer: C

NEW QUESTION 121

- (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 125

- (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
```

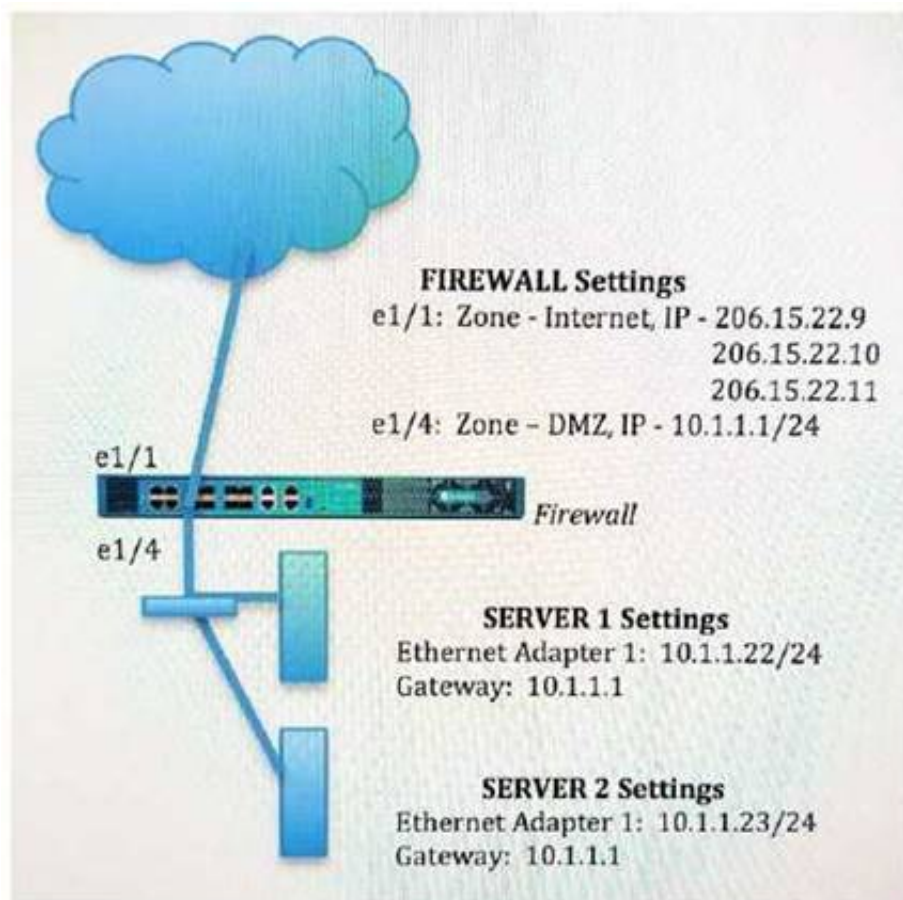
- A. Route 4
- B. Route 3
- C. Route 1
- D. Route 3

Answer: A

NEW QUESTION 126

- (Exam Topic 2)

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



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

NEW QUESTION 128

- (Exam Topic 2)

An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

- A. Security policy rule allowing SSL to the target server
- B. Firewall connectivity to a CRL
- C. Root certificate imported into the firewall with "Trust" enabled
- D. Importation of a certificate from an HSM

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

NEW QUESTION 129

- (Exam Topic 2)

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: D

NEW QUESTION 133

- (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: allow Rule #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=kA10g000000CIEyCAK>

NEW QUESTION 135

- (Exam Topic 2)

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:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-m>

NEW QUESTION 136

- (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 from connecting to the GlobalProtect gateway from a quarantined device
- B. by using security 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 appropriate XSOAR playbook
- D. There is no native auto-quarantine feature so a custom script would need to be leveraged.

Answer: A

NEW QUESTION 139

- (Exam Topic 2)

What are two benefits of nested device groups in Panorama? (Choose two.)

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

Answer: AC

Explanation:

Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.

NEW QUESTION 143

- (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 144

- (Exam Topic 3)

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

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

Answer: BCD

Explanation:

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

NEW QUESTION 149

- (Exam Topic 3)

The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.

Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two)

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

Answer: BD

NEW QUESTION 151

- (Exam Topic 3)

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

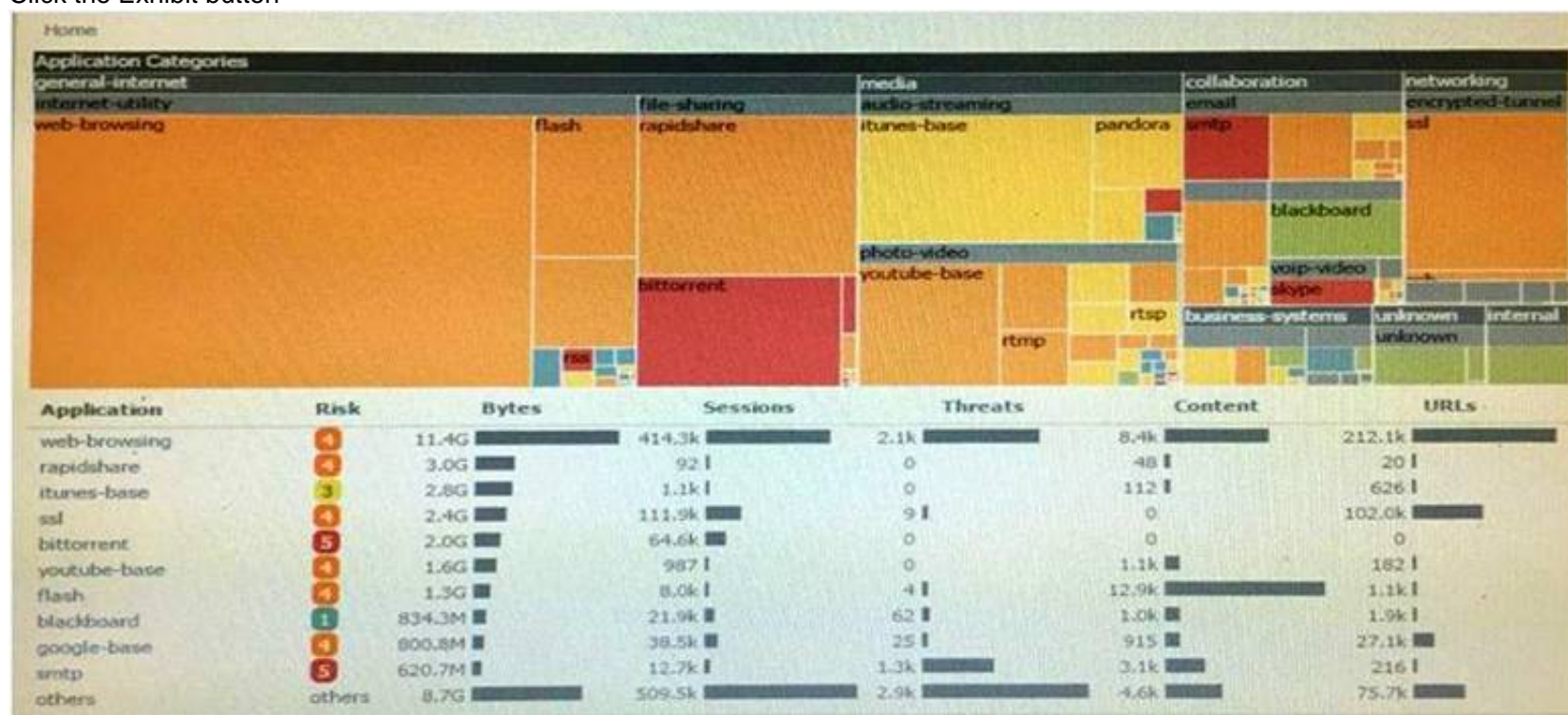
- A. Protocol Decoder
- B. Dynamic routing
- C. Management
- D. Network Processing
- E. Signature Match

Answer: BDE

NEW QUESTION 154

- (Exam Topic 3)

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 159

- (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?

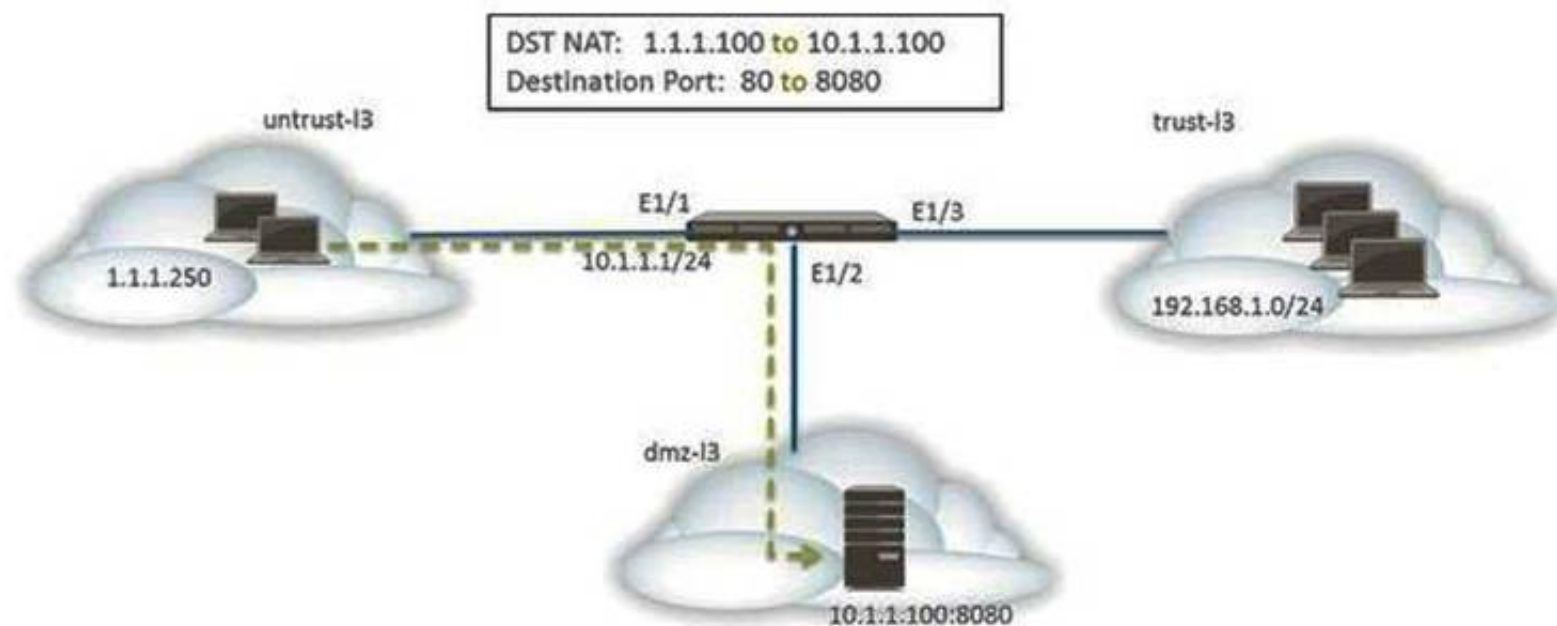
- A. Enable on Site-A only
- B. Enable on Site-B only
- C. Enable on Site-B only with passive mode
- D. Enable on Site-A and Site-B

Answer: D

NEW QUESTION 162

- (Exam Topic 3)

The web server is configured to listen for HTTP traffic on port 8080. The clients access the web server using the IP address 1.1.1.100 on TCP Port 80. The destination NAT rule is configured to translate both IP address and report to 10.1.1.100 on TCP Port 8080.



Which NAT and security rules must be configured on the firewall? (Choose two)

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

Answer: BD

NEW QUESTION 165

- (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 166

- (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 170

- (Exam Topic 3)

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 173

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 174

- (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 176

- (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

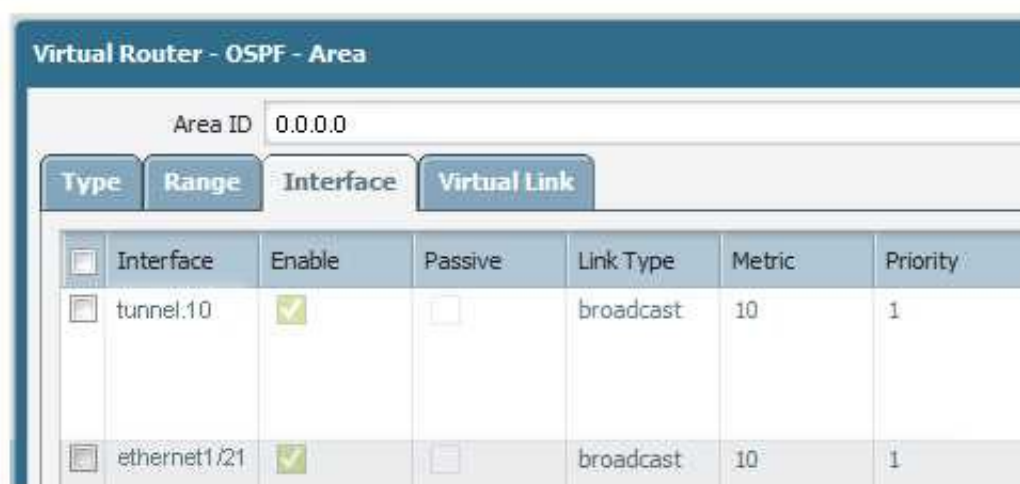
Explanation:

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 181

- (Exam Topic 3)

Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunnel is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.



Type	Range	Interface	Virtual Link
<input type="checkbox"/>	Interface	Enable	Passive
<input type="checkbox"/>	tunnel.1/0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ethernet1/21	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Which Link Type setting will correct the error?

- A. Set tunne
- B. 1 to p2p
- C. Set tunne
- D. 1 to p2mp
- E. Set Ethernet 1/1 to p2mp
- F. Set Ethernet 1/1 to p2p

Answer: A

NEW QUESTION 183

- (Exam Topic 3)

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://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.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/ta-p/59>

NEW QUESTION 187

- (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:

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 addresses 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 secrets do not match between the Palo Alto firewall and the ASA
- D. The dead peer detection settings do not match between the Palo Alto Networks Firewall and the ASA

Answer: B

NEW QUESTION 190

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 193

- (Exam Topic 3)

Which URL Filtering Security Profile action tags the URL Filtering category to the URL Filtering log?

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

Answer: B

NEW QUESTION 194

- (Exam Topic 3)

Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

- A. link requirements
- B. the name of the ISP
- C. IP Addresses
- D. branch and hub locations

Answer: ACD

NEW QUESTION 198

- (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 199

- (Exam Topic 3)

After pushing a security policy from Panorama to a PA-3020 firewall, 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 firewall's policies have been assigned a Log Forwarding profile

Answer: D

NEW QUESTION 200

- (Exam Topic 3)

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.

		Source			Destination						
	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default	allow	none	
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any	deny	none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any	deny	none	

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 203

- (Exam Topic 3)

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 208

- (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 210

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 213

- (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 215

- (Exam Topic 3)

How is the Forward Untrust Certificate used?

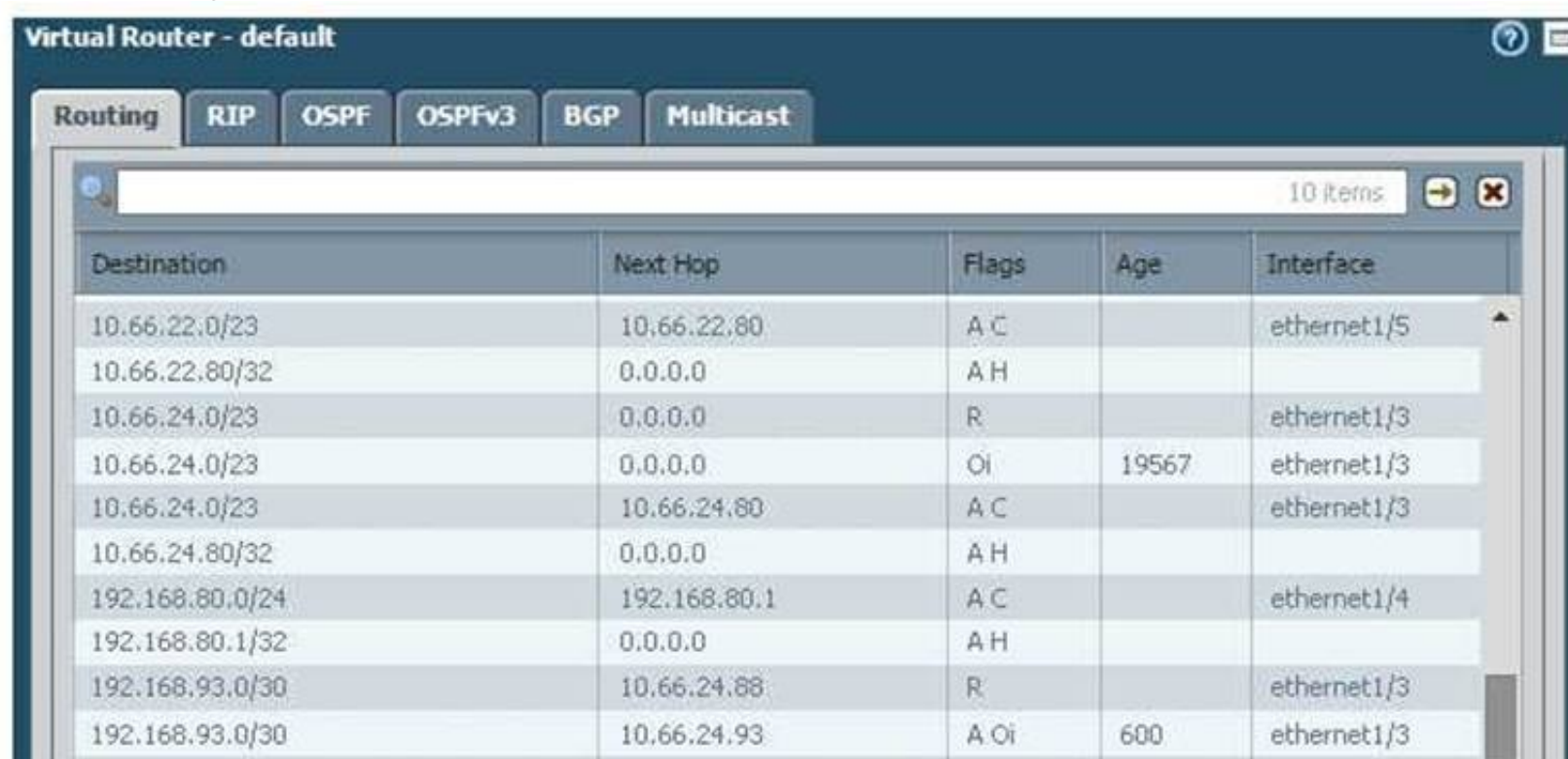
- A. It issues certificates encountered on the Untrust security zone when clients attempt to connect to a site that has be decrypted/
- B. It is used when web servers request a client certificate.
- C. It is presented to clients when the server they are connecting to is signed by a certificate authority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

Answer: C

NEW QUESTION 218

- (Exam Topic 3)

Given the following table.



Destination	Next Hop	Flags	Age	Interface
10.66.22.0/23	10.66.22.80	A C		ethernet1/5
10.66.22.80/32	0.0.0.0	A H		
10.66.24.0/23	0.0.0.0	R		ethernet1/3
10.66.24.0/23	0.0.0.0	Oi	19567	ethernet1/3
10.66.24.0/23	10.66.24.80	A C		ethernet1/3
10.66.24.80/32	0.0.0.0	A H		
192.168.80.0/24	192.168.80.1	A C		ethernet1/4
192.168.80.1/32	0.0.0.0	A H		
192.168.93.0/30	10.66.24.88	R		ethernet1/3
192.168.93.0/30	10.66.24.93	A Oi	600	ethernet1/3

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

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

Answer: A

NEW QUESTION 221

- (Exam Topic 3)

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:

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

NEW QUESTION 224

- (Exam Topic 3)

Which option is an IPv6 routing protocol?

- A. RIPv3
- B. OSPFv3
- C. OSPv3

D. BGP NG

Answer: B

NEW QUESTION 225

- (Exam Topic 3)

A network administrator uses Panorama to push security policies 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 230

- (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 235

.....

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