Question 1

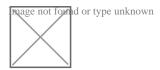A user at an external system with the IP address 65.124 57 5 quenes the DNS server at 4 2 2 2 for the IP address of the web server www xyz com The DNS server returns an address of 172 16 151
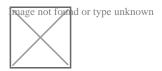
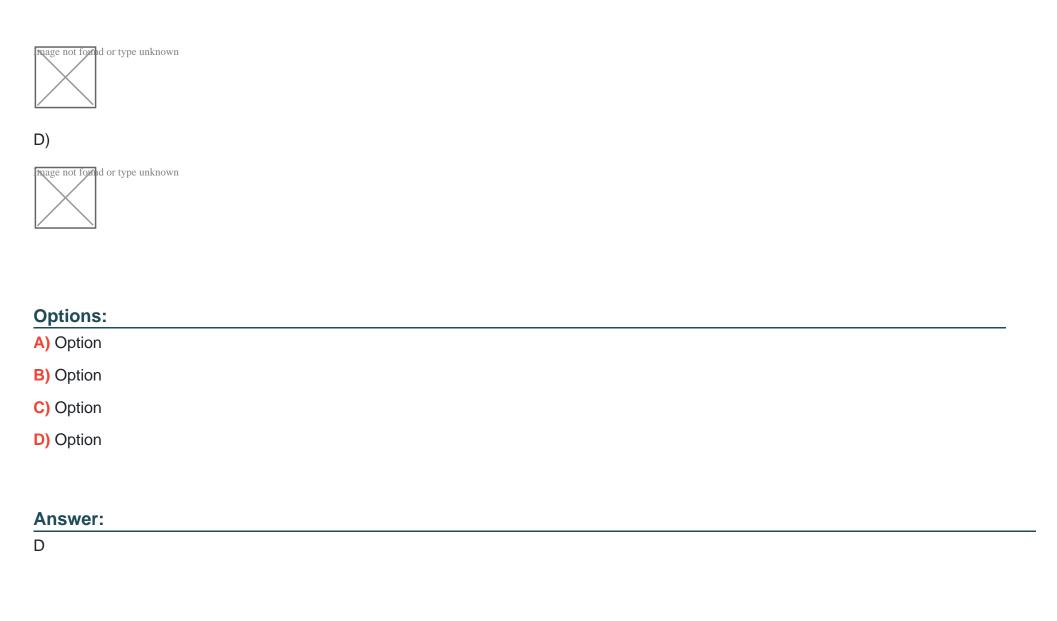In order to reach the web server, which Security rule and NAT rule must be configured on the firewall?

A)

B)

C)

Image not found or type unknown

D)

Image not found or type unknown

Options:

A) Option

B) Option

C) Option

D) Option

Answer:

D

Question 2

Your company has to Active Directory domain controllers spread across multiple WAN links All users authenticate to Active Directory Each link has substantial network bandwidth to support all mission-critical applications. The firewalls management plane is highly utilized

Given this scenario which type of User-ID agent is considered a best practice by Palo Alto Networks?

Options:

A) PAN-OS integrated agent

B) Captive Portal

C) Citrix terminal server agent with adequate data-plane resources

D) Windows-based User-ID agent on a standalone server

Answer:

A

Question 3

Question Type: **MultipleChoice**

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (Cas)

i. 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)

ii. Enterpnse-Untrusted-CA, which is verified as Forward Untrust Certificate

iii. Enterprise-Intermediate-CA

iv. Enterprise-Root-CA which is verified only as Trusted Root CA

An 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 firewall

Options:

A) Enterprise-Untrusted-CA which is a self-signed CA

B) Enterprise-Trusted-CA which is a self-signed CA

C) Enterprise-Intermediate-CA which was. in turn, issued by Enterprise-Root-CA

D) Enterprise-Root-CA which is a self-signed CA

Answer:

A

Question 4

Which GlobalProtect component must be configured to enable Chentless VPN?

Options:

A) GlobalProtect satellite

B) GlobalProtect app

C) GlobalProtect portal

D) GlobalProtect gateway

Answer:

C

Explanation:

Creating the GlobalProtect portal is as simple as letting it know if you have accessed it already. A new gateway for accessing the GlobalProtect portal will appear. Client authentication can be used with an existing one.

Question 5

Question Type: **MultipleChoice**

Panorama provides which two SD_WAN functions? (Choose two.)

Options:

A) data plane

B) physical network links

C) network monitoring

D) control plane

Answer:

C, D

Question 6

What are three reasons why an installed session can be identified with the application

Options:

A) The TCP connection was terminated without identifying any application data

B) The client sent a TCP segment with the PUSH flag set

C) There is not enough application data after the TCP connection was established

D) The TCP connection did not fully establish

E) There was no application data after the TCP connection was established

Answer:

A, C, E

Question 7

What happens when en A P firewall cluster synchronies IPsec tunnel secunty associations (SAs)?

Options:

A) Phase 2 SAs are synchronized over HA2 finks

B) Phase 1 and Phase 2 SAs are synchronized over HA2 links

C) Phase 1 SAs are synchronized over HA1 links

D) Phase 1 and Phase 2 SAs are synchronized over HA3 links

Answer:

A