Vendor: Palo Alto Networks

Exam Code:PCNSE

Exam Name: Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x

Version: Demo

QUESTION 1

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

A. Microsoft Active Directory

B. Microsoft Terminal Services

C. Aerohive Wireless Access Point

D. Palo Alto Networks Captive Portal

Correct Answer: B

QUESTION 2

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration Once deployed each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

A. IPsec tunnels using IKEv2

B. PPTP tunnels

C. GlobalProtect satellite

D. GlobalProtect client

Correct Answer: C

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface- help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite- configuration-tab.html

---

QUESTION 3

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

A. ACC

B. System Logs

C. App Scope

D. Session Browser

Correct Answer: D

QUESTION 4

A network administrator is trying to prevent domain username and password submissions to phishing sites on some allowed URL categories Which set of steps does the administrator need to take in the URL Filtering profile to prevent credential phishing on the firewall?

A. Choose the URL categories on Site Access column and set action to block Click the User credential Detection tab and select IP User Mapping Commit

B. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select use IP User Mapping Commit

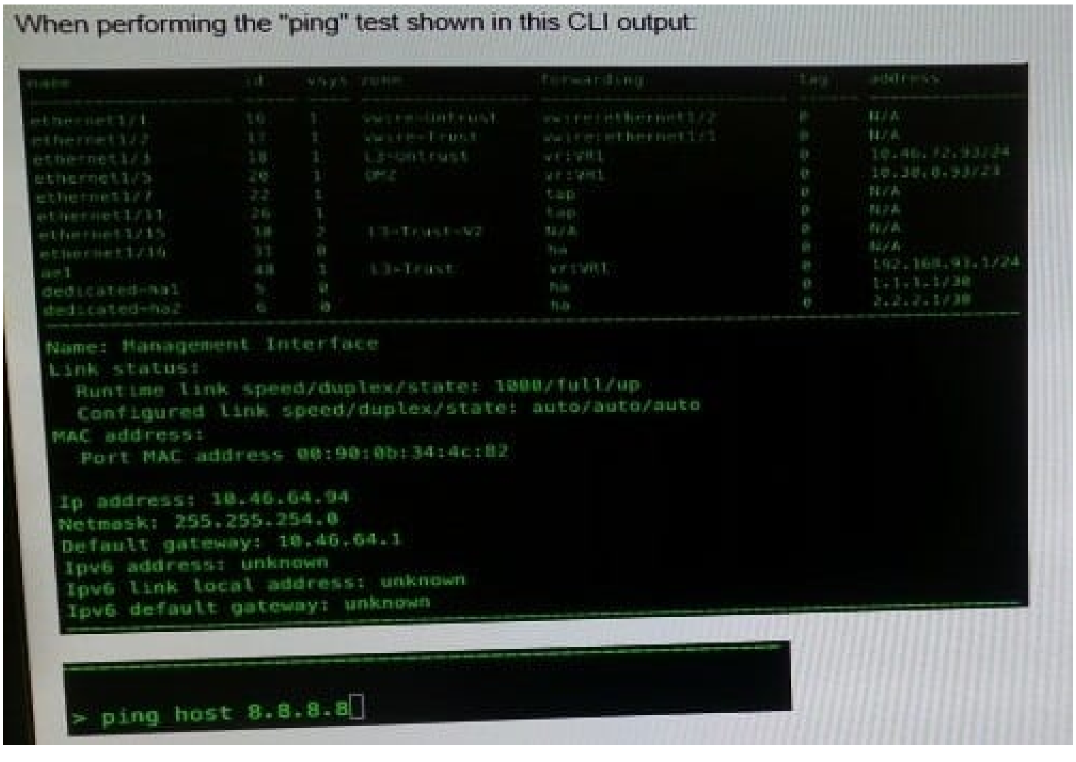
C. Choose the URL categories in the User Credential Submission column and set action to block Select the URL filtering settings and enable Domain Credential Filter Commit

D. Choose the URL categories in the User Credential Submission column and set action to block Select the User credential Detection tab and select Use Domain Credential Filter Commit

Correct Answer: D

credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions to known corporate credentials. You can configure solutions that detect and prevent credential phishing using URL filtering profiles and User-ID agents. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-credential-phishing-prevention

QUESTION 5



When performing the "ping" test shown in this CLI output:

```
name              id    vsys  zone            forwarding            tag   address
----------------- ----- ----- --------------- --------------------- ----- ----------------
ethernet1/1       16    1     vwire-Untrust   vwire:ethernet1/2     0     N/A
ethernet1/2       17    1     vwire-Trust     vwire:ethernet1/1     0     N/A
ethernet1/3       18    1     L3-Untrust      vr:VR1                0     10.46.72.93/24
ethernet1/5       20    1     DMZ             vr:VR1                0     10.30.0.93/24
ethernet1/7       22    1                     tap                   0     N/A
ethernet1/11      26    1                     tap                   0     N/A
ethernet1/15      30    2     L3-Trust-V2     N/A                   0     N/A
ethernet1/16      31    0                     ha                    0     N/A
ae1               48    1     L3-Trust        vr:VR1                0     192.168.93.1/24
dedicated-ha1     5     0                     ha                    0     1.1.1.1/30
dedicated-ha2     6     0                     ha                    0     2.2.2.1/30
-------------------------------------------------------------------------------------
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 1000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:90:0b:34:4c:82

Ip address: 10.46.64.94
Netmask: 255.255.254.0
Default gateway: 10.46.64.1
Ipv6 address: unknown
Ipv6 link local address: unknown
Ipv6 default gateway: unknown
-------------------------------------------------------------------------------------

-------------------------------------------------------------
> ping host 8.8.8.8
```

What will be the source address in the ICMP packet?

A. 10.30.0.93

B. 10.46.72.93

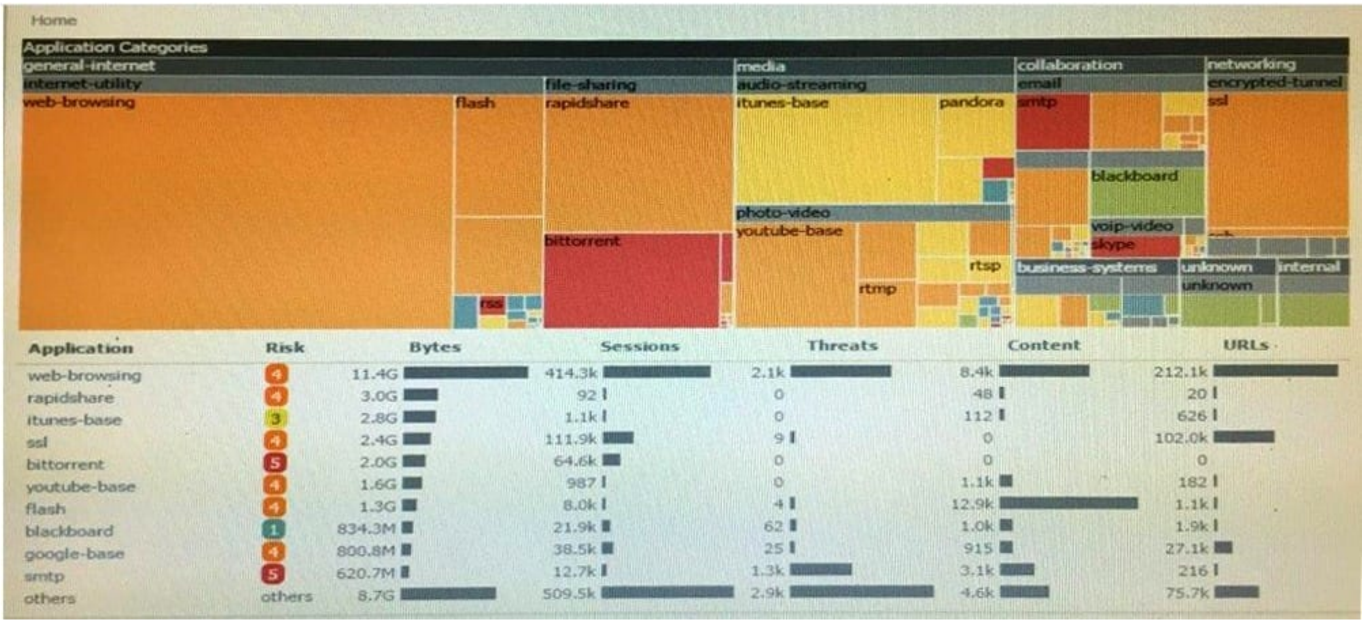
C. 10.46.64.94

D. 192.168.93.1

Correct Answer: C

QUESTION 6

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?



Application	Risk	Bytes	Sessions	Threats	Content	URLs
web-browsing	4	11.4G	414.3k	2.1k	8.4k	212.1k
rapidshare	4	3.0G	92	0	48	20
itunes-base	3	2.8G	1.1k	0	112	626
ssl	4	2.4G	111.9k	9	0	102.0k
bittorrent	5	2.0G	64.6k	0	0	0
youtube-base	4	1.6G	987	0	1.1k	182
flash	4	1.3G	8.0k	4	12.9k	1.1k
blackboard	1	834.3M	21.9k	62	1.0k	1.9k
google-base	4	800.8M	38.5k	25	915	27.1k
smtp	5	620.7M	12.7k	1.3k	3.1k	216
others	others	8.7G	509.5k	2.9k	4.6k	75.7k

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

Correct Answer: D

QUESTION 7

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

Correct Answer: D

QUESTION 8

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. 0

B. 99

C. 1

D. 255

Correct Answer: D

Reference:

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

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

QUESTION 9

What is considered the best practice with regards to zone protection?

A. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse

B. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs

C. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection

D. Set the Alarm Rate threshold for event-log messages to high severity or critical severity

Correct Answer: B

https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices

---

QUESTION 10

An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently. HTTP and SSL requests contain the c IP address of the web server and the client browser is redirected to the proxy

Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. DNS proxy

B. Explicit proxy

C. SSL forward proxy

D. Transparent proxy

Correct Answer: D

A transparent proxy is a type of web proxy that intercepts and redirects HTTP and HTTPS requests without requiring any configuration on the client browser1. The firewall acts as a gateway between the client and the web server, and performs security checks on the traffic. A transparent proxy can be configured on PAN-OS 11.0 firewalls by performing the following steps1: Enable Web Proxy under Device > Setup > Services Select Transparent Proxy as the Proxy Type Configure a Service Route for Web Proxy Configure SSL/TLS Service Profile for Web Proxy Configure Security Policy Rules for Web Proxy Traffic By configuring a transparent proxy on PAN-OS 11.0 firewalls, an organization can migrate from their existing web proxy architecture without changing their network topology or client settings2. The firewall will maintain the same type of traffic flow as before, where HTTP and HTTPS requests contain the IP address of the web server and the client browser is redirected to the proxy1. Answer A is not correct because DNS proxy is a type of web proxy that intercepts DNS queries from clients and resolves them using an external DNS server3. This type of proxy does not redirect HTTP or HTTPS requests to the firewall.

QUESTION 11

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

A. Log

B. Alert

C. Allow

D. Default

Correct Answer: B

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

---

QUESTION 12

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain?

A. a Security policy with \\'known-user" selected in the Source User field

B. an Authentication policy with \\'unknown\\' selected in the Source User field

C. a Security policy with \\'unknown\\' selected in the Source User field

D. an Authentication policy with \\'known-user\\' selected in the Source User field

Correct Answer: B