Question #:1

Which prevention technique will prevent attacks based on packet count?

A. zone protection profile

B. URL filtering profile

C. antivirus profile

D. vulnerability profile

Answer: A

Question #:2

What are three differences between security policies and security profiles? (Choose three.)

A. Security policies are attached to security profiles

B. Security profiles are attached to security policies

C. Security profiles should only be used on allowed traffic

D. Security profiles are used to block traffic by themselves

E. Security policies can block or allow traffic

Answer: B C E

Question #:3

A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified

B. Rule Usage Filter >Hit Count > Unused in 30 days

C. Rule Usage Filter > Unused Apps

D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer: B

Question #:4

A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

A. Windows-based agent on a domain controller

B. Captive Portal

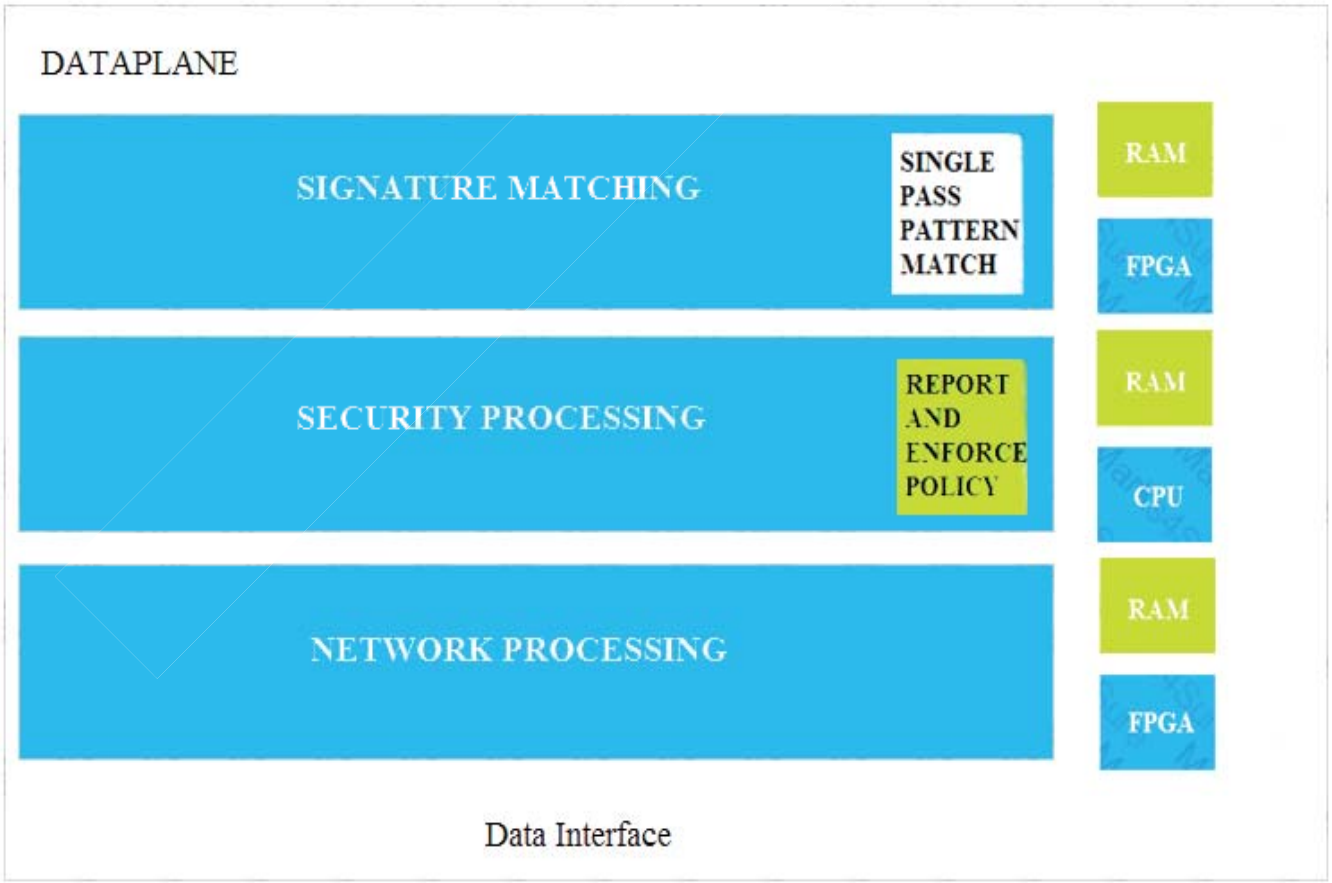
C. Citrix terminal server with adequate data-plane resources

D. PAN-OS integrated agent

Answer: A

Question #:5

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?



A. Signature Matching

B. Network Processing

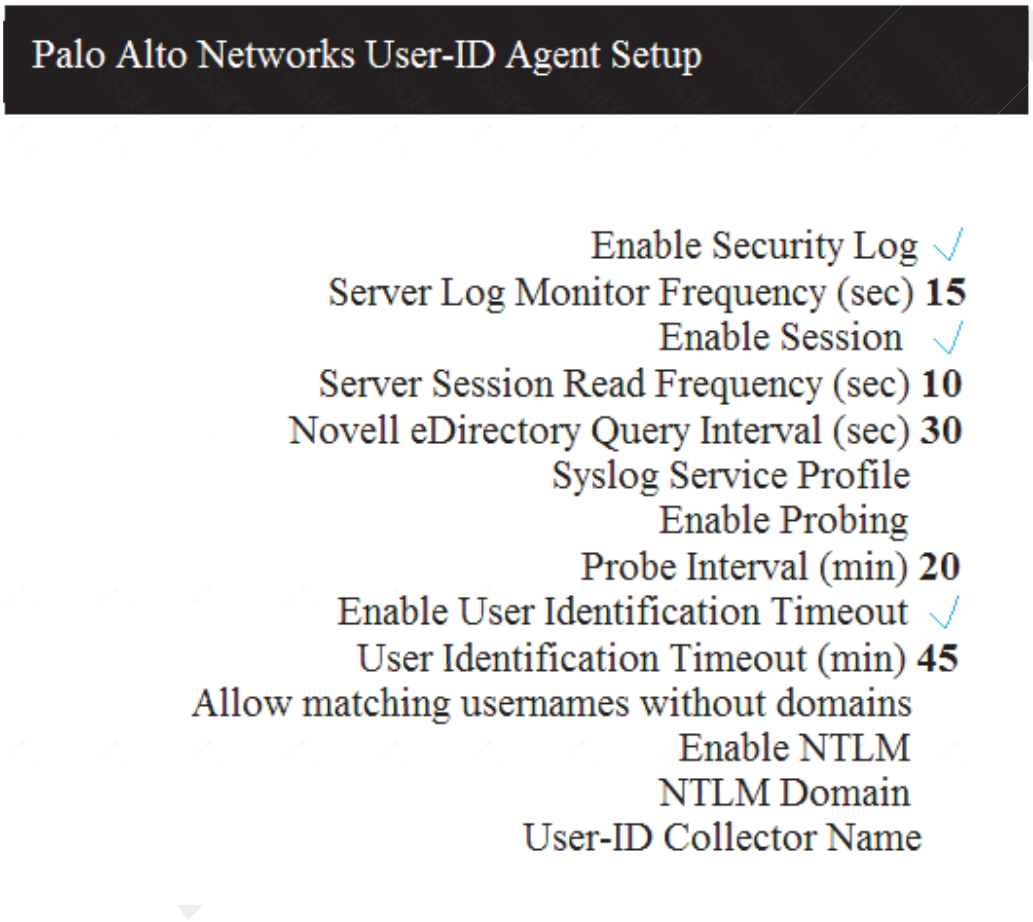
C. Security Processing

D. Security Matching

Answer: A

Question #:6

Which two configuration settings shown are not the default? (Choose two.)



A. Enable Security Log

B. Server Log Monitor Frequency (sec)

C. Enable Session

D. Enable Probing

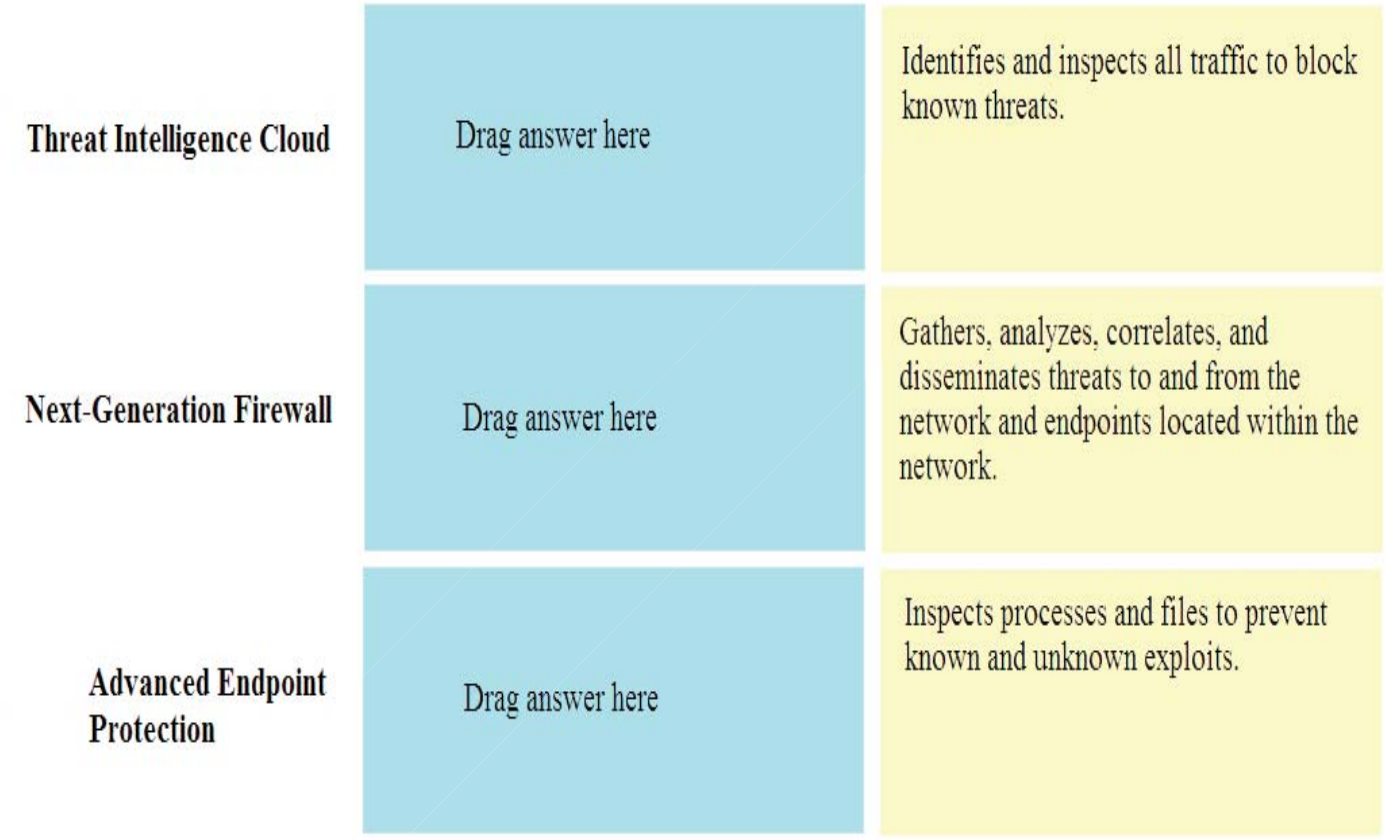
Answer: B C

Explanation

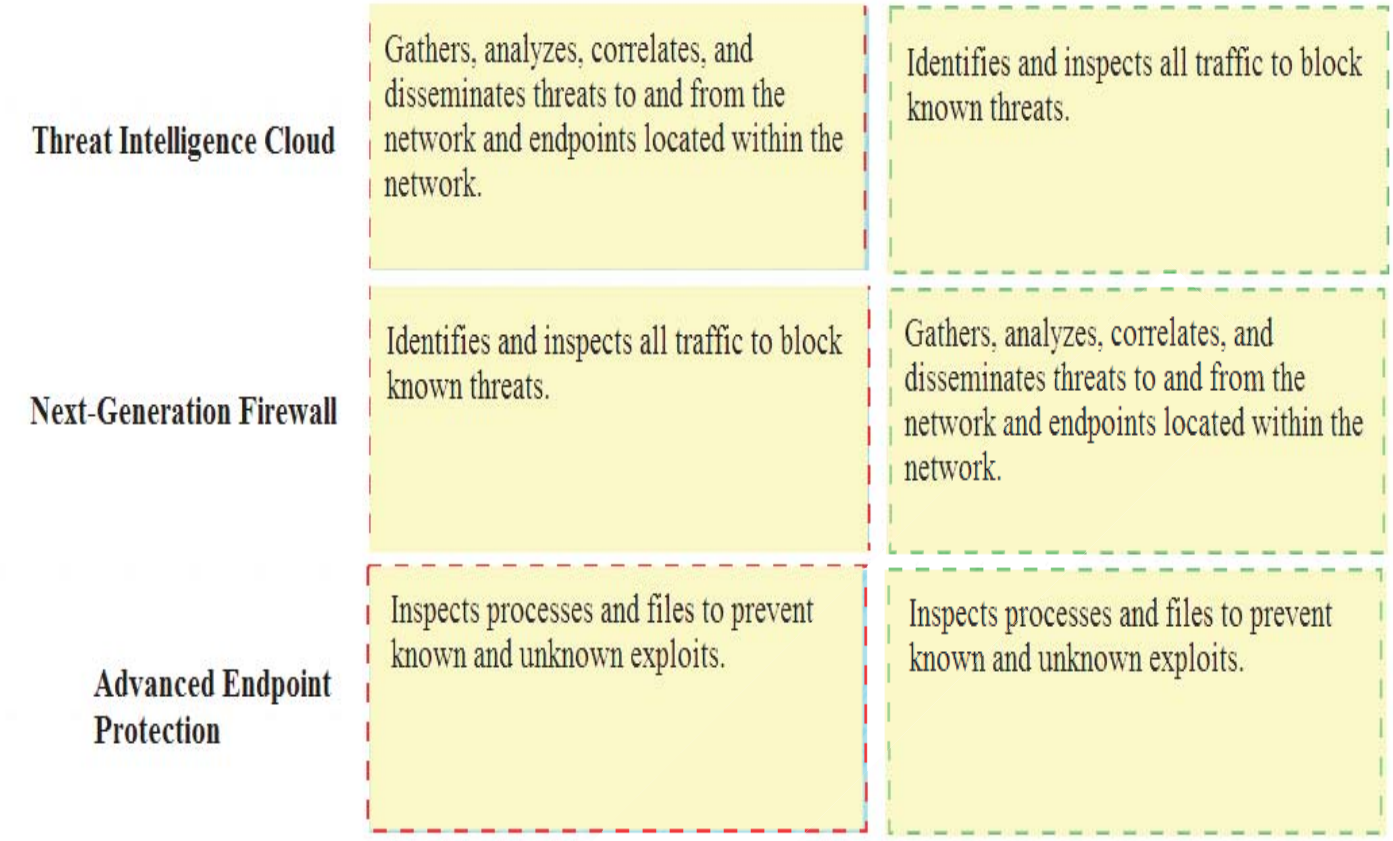
References:

Question #:7

Match the Palo Alto Networks Security Operating Platform architecture to its description.



Answer:



Explanation

Threat Intelligence Cloud – Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.

Next-Generation Firewall – Identifies and inspects all traffic to block known threats

Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

Question #:8

Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP –to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.

Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

A. syslog

B. RADIUS

C. UID redistribution

D. XFF headers

Answer: A

Question #:9

Which URL profiling action does not generate a log entry when a user attempts to access that URL?

A. Override

B. Allow

C. Block

D. Continue

Answer: B

Explanation

References:

Question #:10

Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

A. Layer 2

B. Tap

C. Layer 3

D. Virtual Wire

Answer: B

Question #:11

Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser

B. Role-based

C. Dynamic