Palo Alto Networks.PSE-Strata.by.Rian.91q

Number: PSE-Strata
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: PSE-Strata
Exam Name: Palo Alto Networks System Engineer - Strata

Exam A

QUESTION 1
Decryption port mirroring is now supported on which platform?

A. all hardware-based and VM-Series firewalls with the exception of VMware NSX. Citrix SDX, or public cloud hypervisors
B. in hardware only
C. only one the PA-5000 Series and higher
D. all hardware-based and VM-Series firewalls regardless of where installed

Correct Answer: D
Section:

QUESTION 2
Select the BOM for the Prisma Access, to provide access for 5500 mobile users and 10 remote locations (100Mbps each) for one year, including Base Support and minimal logging. The customer already has 4x PA5220r 8x PA3220,1x Panorama VM for 25 devices.

A. 5500x PAN-GPCS-USER-C-BAS-1YR, 1000x PAN-GPCS-NET-B-BAS-1YR, 1x PAN-LGS-1TB-1YR
B. 5500x PAN-GPCS-USER-C-BAS-1YR, 1000x PAN-GPCS-NET-B-BAS-1YR, 1x PAN-SVC-BAS-PRA-25. 1x PAN-PRA-25
C. 5500x PAN-GPCS-USER-C-BAS-1YR, 1000x PAN-GPCS-NET-B-BAS-1YRr 1x PAN-LGS-1TB-1YR, 1x PAN-PRA-25, 1x PAN-SVC-BAS-PRA-25
D. 1x PAN-GPCS-USER-C-BAS-1YR, 1x PAN-GPCS-NET-B-BAS-1YR, 1x PAN-LGS-1TB-1YR

Correct Answer: C
Section:

QUESTION 3
As you prepare to scan your Amazon S3 account, what enables Prisma service permission to access Amazon S3?

A. access key ID
B. secret access key
C. administrative Password
D. AWS account ID

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/prisma/prisma-saas/prisma-saas-admin/secure-cloud-apps/add-cloud-apps-to-prisma-saas/begin-scanning-an-amazon-s3-app.html

QUESTION 4
Which option is required to Activate/Retrieve a Device Management License on the M-100 Appliance after the Auth Codes have been activated on the Palo Alto Networks Support Site?

A. Generate a Stats Dump File and upload it to the Palo Alto Networks support portal
B. Select Panorama > Licenses and click Activate feature using authorization code
C. Generate a Tech Support File and call PANTAC

D. Select Device > Licenses and click Activate feature using authorization code

Correct Answer: B
Section:

QUESTION 5
What is the basis for purchasing Cortex XDR licensing?

A. volume of logs being processed based on Datalake purchased
B. number of nodes and endpoints providing logs
C. unlimited licenses
D. number of NGFWs

Correct Answer: B
Section:
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/migrate-your-cortex-xdr-license

QUESTION 6
Which two components must be configured within User-ID on a new firewall that has been implemented? (Choose two.)

A. User Mapping
B. Proxy Authentication
C. Group Mapping
D. 802.1X Authentication

Correct Answer: A, C
Section:
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/enable-user-id

QUESTION 7
Which four steps of the cyberattack lifecycle does the Palo Alto Networks Security Operating Platform prevent? (Choose four.)

A. breach the perimeter
B. weaponize vulnerabilities
C. lateral movement
D. exfiltrate data
E. recon the target
F. deliver the malware

Correct Answer: A, C, D, F
Section:

QUESTION 8
Which three settings must be configured to enable Credential Phishing Prevention? (Choose three.)

A. define an SSL decryption rulebase
B. enable User-ID
C. validate credential submission detection
D. enable App-ID
E. define URL Filtering Profile

Correct Answer: B, C, E
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/preventcredential-phishing.html

QUESTION 9
An SE is preparing an SLR report for a school and wants to emphasize URL filtering capabilities because the school is concerned that its students are accessing inappropriate websites. The URL categories being chosen by default in the report are not highlighting these types of websites. How should the SE show the customer the firewall can detect that these websites are being accessed?

A. Create a footnote within the SLR generation tool
B. Edit the Key-Findings text to list the other types of categories that may be of interest
C. Remove unwanted categories listed under 'High Risk' and use relevant information
D. Produce the report and edit the PDF manually

Correct Answer: C
Section:

QUESTION 10
Which three methods used to map users to IP addresses are supported in Palo Alto Networks firewalls? (Choose three.)

A. eDirectory monitoring
B. Client Probing
C. SNMP server
D. TACACS
E. Active Directory monitoring
F. Lotus Domino
G. RADIUS

Correct Answer: B, D, G
Section:
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/user-idconcepts/user-mapping

QUESTION 11
When the Cortex Data Lake is sized for Traps Management Service, which two factors should be considered? (Choose two.)

A. retention requirements
B. Traps agent forensic data
C. the number of Traps agents
D. agent size and OS

Correct Answer: B, D
Section:

QUESTION 12
What are two benefits of using Panorama for a customer who is deploying virtual firewalls to secure data center traffic? (Choose two.)

A. It can provide the Automated Correlation Engine functionality, which the virtual firewalls do not support.
B. It can monitor the virtual firewalls' physical hosts and Vmotion them as necessary
C. It can automatically create address groups for use with KVM.
D. It can bootstrap the virtual firewalls for dynamic deployment scenarios.

Correct Answer: A, D
Section:

QUESTION 13
Which two tabs in Panorama can be used to identify templates to define a common base configuration? (Choose two.)

A. Network Tab
B. Policies Tab
C. Device Tab
D. Objects Tab

Correct Answer: A, C
Section:
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-webinterface/panorama-templates/template-stacks

QUESTION 14
An endpoint, inside an organization, is infected with known malware that attempts to make a command-and-control connection to a C2 server via the destination IP address Which mechanism prevents this connection from succeeding?

A. DNS Sinkholing
B. DNS Proxy
C. Anti-Spyware Signatures
D. Wildfire Analysis

Correct Answer: A
Section:

QUESTION 15
How frequently do WildFire signatures move into the antivirus database?

A. every 24 hours
B. every 12 hours
C. once a week
D. every 1 hour

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfireconcepts/wildfire-signatures

QUESTION 16
What are two presales selling advantages of using Expedition? (Choose two.)

A. map migration gaps to professional services statement of Works (SOWs)
B. streamline & migrate to Layer7 policies using Policy Optimizer
C. reduce effort to implement policies based on App-ID and User-ID
D. easy migration process to move to Palo Alto Networks NGFWs

Correct Answer: A, D
Section:

QUESTION 17
Which two features are found in a Palo Alto Networks NGFW but are absent in a legacy firewall product? (Choose two.)

A. Traffic is separated by zones
B. Policy match is based on application
C. Identification of application is possible on any port
D. Traffic control is based on IP port, and protocol

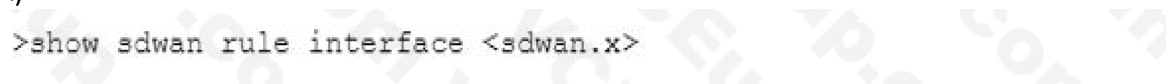
Correct Answer: B, C
Section:

QUESTION 18
An administrator wants to justify the expense of a second Panorama appliance for HA of the management layer.
The customer already has multiple M-100s set up as a log collector group. What are two valid reasons for deploying Panorama in High Availability? (Choose two.)

A. Control of post rules
B. Control local firewall rules
C. Ensure management continuity
D. Improve log collection redundancy

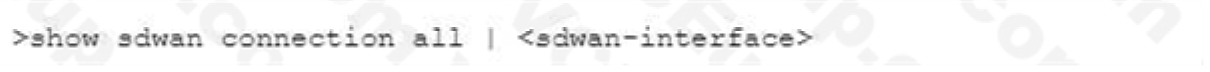
Correct Answer: C, D
Section:

QUESTION 19
Which CLI allows you to view the names of SD-WAN policy rules that send traffic to the specified virtual SD-WAN interface, along with the performance metrics?
A)



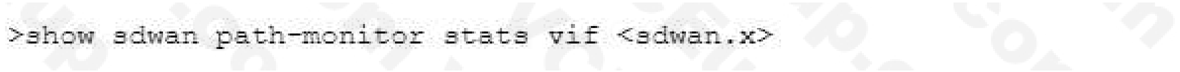
```
>show sdwan rule interface <sdwan.x>
```

B)



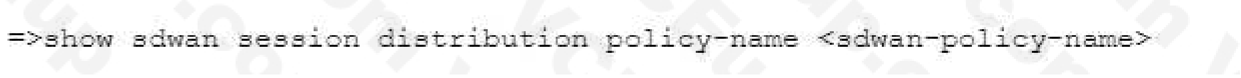
```
>show sdwan connection all | <sdwan-interface>
```

C)



```
>show sdwan path-monitor stats vif <sdwan.x>
```

D)



```
=>show sdwan session distribution policy-name <sdwan-policy-name>
```

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

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html

QUESTION 20
Which two network events are highlighted through correlation objects as potential security risks?
(Choose two.)

A. Identified vulnerability exploits
B. Launch of an identified malware executable file
C. Endpoints access files from a removable drive
D. Suspicious host behavior

Correct Answer: A, D
Section:

QUESTION 21
Which three categories are identified as best practices in the Best Practice Assessment tool? (Choose three.)

A. use of decryption policies
B. measure the adoption of URL filters. App-ID. User-ID
C. use of device management access and settings
D. expose the visibility and presence of command-and-control sessions
E. identify sanctioned and unsanctioned SaaS applications

Correct Answer: A, B, E
Section:

QUESTION 22
Which three platform components can identify and protect against malicious email links? (Choose three.)

A. WildFire hybrid cloud solution
B. WildFire public cloud
C. WF-500
D. M-200

E. M-600

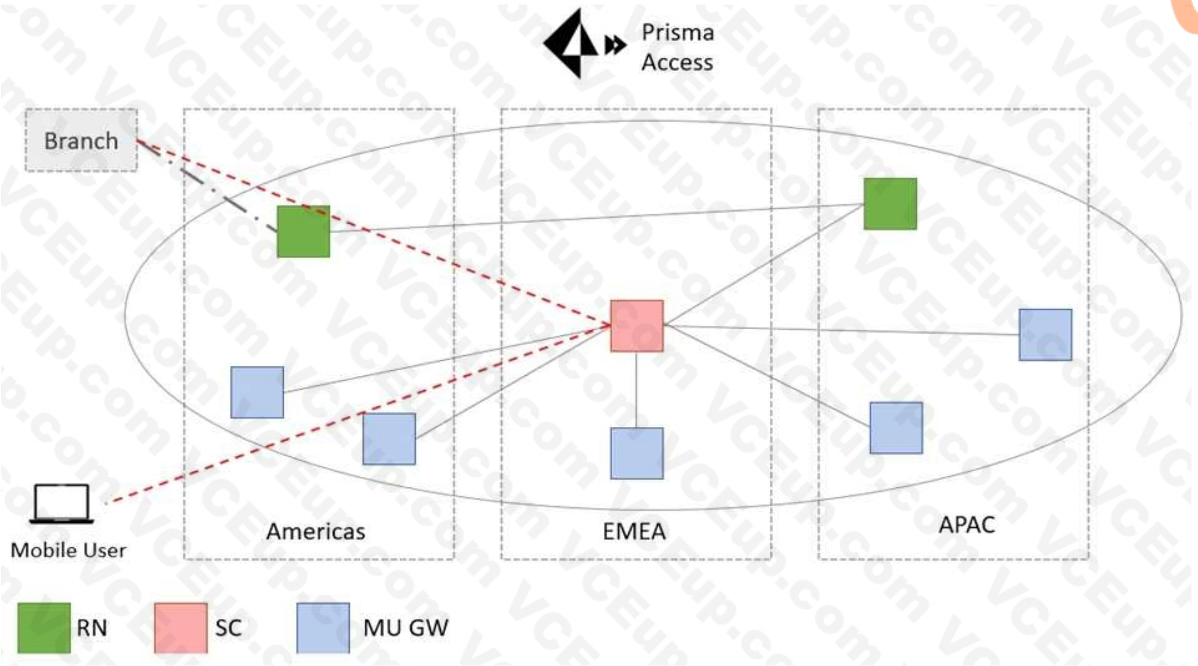
Correct Answer: B, C, D
Section:

QUESTION 23
When having a customer pre-sales call, which aspects of the NGFW should be covered?

A. The NGFW simplifies your operations through analytics and automation while giving you consistent protection through exceptional visibility and control across the data center, perimeter, branch, mobile and cloud networks
B. The Palo Alto Networks-developed URL filtering database, PAN-DB provides high-performance local caching for maximum inline performance on URL lookups, and offers coverage against malicious URLs and IP addresses. As WildFire identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs), the PAN-DB database is updated with information on malicious URLs so that you can block malware downloads and disable Command and Control (C2) communications to protect your network from cyberthreats. URL categories that identify confirmed malicious content — malware, phishing, and C2 are updated every five minutes — to ensure that you can manage access to these sites within minutes of categorization
C. The NGFW creates tunnels that allow users/systems to connect securely over a public network, as if they were connecting over a local area network (LAN). To set up a VPN tunnel you need a pair of devices that can authenticate each other and encrypt the flow of information between them The devices can be a pair of Palo Alto Networks firewalls, or a Palo Alto Networks firewall along with a VPN-capable device from another vendor
D. Palo Alto Networks URL Filtering allows you to monitor and control the sites users can access, to prevent phishing attacks by controlling the sites to which users can submit valid corporate credentials, and to enforce safe search for search engines like Google and Bing

Correct Answer: D
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering

QUESTION 24



What action would address the sub-optimal traffic path shown in the figure?
Key:
RN - Remote Network
SC - Service Connection
MU GW - Mobile User Gateway

A. Onboard a Service Connection in the Americas region

B. Remove the Service Connection in the EMEA region

C. Onboard a Service Connection in the APAC region

D. Onboard a Remote Network location in the EMEA region

Correct Answer: C
Section:

QUESTION 25
What are the three possible verdicts in WildFire Submissions log entries for a submitted sample?
(Choose four.)

A. Benign

B. Spyware

C. Malicious

D. Phishing

E. Grayware

Correct Answer: A, C, D, E
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/monitor-wildfire-activity/use-the-firewall-to-monitor-malware/monitor-wildfire-submissions-and-analysisreports.html

QUESTION 26
In which two cases should the Hardware offering of Panorama be chosen over the Virtual Offering?
(Choose two.)

A. Dedicated Logger Mode is required

B. Logs per second exceed 10,000

C. Appliance needs to be moved into data center

D. Device count is under 100

Correct Answer: A, B
Section:

QUESTION 27
How do you configure the rate of file submissions to WildFire in the NGFW?

A. based on the purchased license uploaded

B. QoS tagging

C. maximum number of files per minute

D. maximum number of files per day

Correct Answer: C
Section:
Explanation:
https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/submit-files-for-wildfire-analysis/firewall-file-forwarding-capacity-by-model

QUESTION 28
Palo Alto Networks publishes updated Command-and-Control signatures. How frequently should the related signatures schedule be set?

A. Once a day
B. Once a week
C. Once every minute
D. Once an hour

Correct Answer: B
Section:

QUESTION 29
Which are the three mandatory components needed to run Cortex XDR? (Choose three.)

A. Panorama
B. NGFW with PANOS 8 0.5 or later
C. Cortex Data Lake
D. Traps
E. Pathfinder
F. Directory Syn Service

Correct Answer: B, C, F
Section:
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture

QUESTION 30
Which selection must be configured on PAN-OS External Dynamic Lists to support MineMeld indicators?

A. Prototype
B. Inputs
C. Class
D. Feed Base URL

Correct Answer: D
Section:
Explanation:
https://live.paloaltonetworks.com/t5/minemeld-articles/connecting-pan-os-to-minemeld-using-external-dynamic-lists/ta-p/190414

QUESTION 31
Which two new file types are supported on the WF-500 in PAN-OS 9? (Choose two)

A. ELF
B. 7-Zip
C. Zip
D. RAR

Correct Answer: B, D
Section:
Explanation:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-file-type-support

QUESTION 32
A customer is concerned about zero-day targeted attacks against its intellectual property.
Which solution informs a customer whether an attack is specifically targeted at them?

A. Traps TMS
B. AutoFocus
C. Panorama Correlation Report
D. Firewall Botnet Report

Correct Answer: D
Section:

QUESTION 33
Prisma SaaS provides which two SaaS threat prevention capabilities? (Choose two)

A. shellcode protection
B. file quarantine
C. SaaS AppID signatures
D. WildFire analysis
E. remote procedural call (RPC) interrogation

Correct Answer: C, D
Section:

QUESTION 34
A client chooses to not block uncategorized websites.
Which two additions should be made to help provide some protection? (Choose two.)

A. A URL filtering profile with the action set to continue for unknown URL categories to security policy rules that allow web access
B. A data filtering profile with a custom data pattern to security policy rules that deny uncategorized websites
C. A file blocking profile attached to security policy rules that allow uncategorized websites to help reduce the risk of drive by downloads
D. A security policy rule using only known URL categories with the action set to allow

Correct Answer: A, B
Section:

QUESTION 35
A customer is seeing an increase in the number of malicious files coming in from undetectable sources in their network. These files include doc and .pdf file types.
The customer uses a firewall with User-ID enabled
Which feature must also be enabled to prevent these attacks?

A. Content Filtering

B. WildFire

C. Custom App-ID rules

D. App-ID

Correct Answer: B
Section:

QUESTION 36
XYZ Corporation has a legacy environment with asymmetric routing. The customer understands that Palo Alto Networks firewalls can support asymmetric routing with redundancy. Which two features must be enabled to meet the customer's requirements? (Choose two.)

A. Policy-based forwarding

B. HA active/active

C. Virtual systems

D. HA active/passive

Correct Answer: A, B
Section:
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/route-based-redundancy

QUESTION 37
How often are the databases for Anti-virus. Application, Threats, and WildFire subscription updated?

A. Anti-virus (weekly): Application (daily). Threats (weekly), WildFire (5 minutes)

B. Anti-virus (weekly), Application (daily), Threats (daily), WildFire (5 minutes)

C. Anti-virus (daily), Application (weekly), Threats (weekly), WildFire (5 minutes)

D. Anti-virus (daily), Application (weekly), Threats (daily), WildFire (5 minutes)

Correct Answer: C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html

QUESTION 38
A company has deployed the following
• VM-300 firewalls in AWS
• endpoint protection with the Traps Management Service
• a Panorama M-200 for managing its VM-Series firewalls
• PA-5220s for its internet perimeter,
• Prisma SaaS for SaaS security.
Which two products can send logs to the Cortex Data Lake? (Choose two).

A. Prisma SaaS

B. Traps Management Service

C. VM-300 firewalls

D. Panorama M-200 appliance

Correct Answer: C, D
Section:

QUESTION 39
Which profile or policy should be applied to protect against port scans from the internet?

A. Interface management profile on the zone of the ingress interface
B. Zone protection profile on the zone of the ingress interface
C. An App-ID security policy rule to block traffic sourcing from the untrust zone
D. Security profiles to security policy rules for traffic sourcing from the untrust zone

Correct Answer: B
Section:

QUESTION 40
When log sizing is factored for the Cortex Data Lake on the NGFW, what is the average log size used in calculation?

A. 8MB
B. depends on the Cortex Data Lake tier purchased
C. 18 bytes
D. 1500 bytes

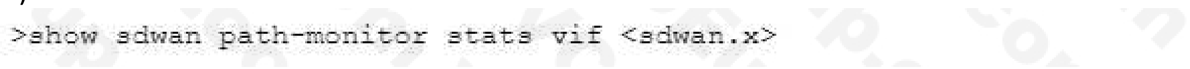
Correct Answer: D
Section:
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVMCA0

QUESTION 41
What can be applied to prevent users from unknowingly downloading malicious file types from the internet?

A. A vulnerability profile to security policy rules that deny general web access
B. An antivirus profile to security policy rules that deny general web access
C. A zone protection profile to the untrust zone
D. A file blocking profile to security policy rules that allow general web access

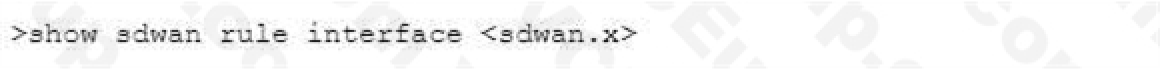
Correct Answer: D
Section:
Explanation:
https://docs.paloaltonetworks.com/best-practices/8-1/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles.html

QUESTION 42
Which CLI command will allow you to view latency, jitter and packet loss on a virtual SD-WAN interface?
A)



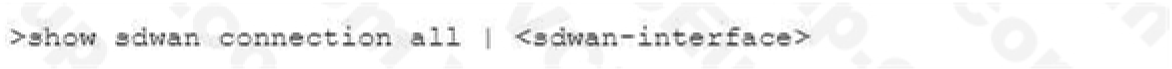
```
>show sdwan path-monitor stats vif <sdwan.x>
```

B)



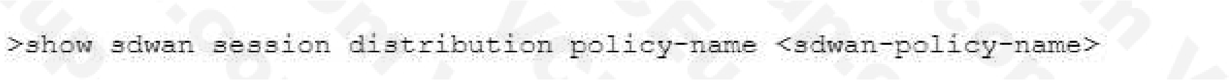
```
>show sdwan rule interface <sdwan.x>
```

C)



```
>show sdwan connection all | <sdwan-interface>
```

D)



```
>show sdwan session distribution policy-name <sdwan-policy-name>
```

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

Correct Answer: A
Section:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html

QUESTION 43
A service provider has acquired a pair of PA-7080s for its data center to secure its customer base's traffic. The server provider's traffic is largely generated by smart phones and averages 6.000,000 concurrent sessions.
Which Network Processing Card should be recommended in the Bill of Materials?

A. PA-7000-20GQ-NPC
B. PA-7000-40G-NPC
C. PA-7000-20GQXM-NPC
D. PA-7000-20G-NPC

Correct Answer: C
Section:

QUESTION 44
A customer is concerned about malicious activity occurring directly on their endpoints and will not be visible to their firewalls.
Which three actions does the Traps agent execute during a security event, beyond ensuring the prevention of this activity? (Choose three.)

A. Informs WildFire and sends up a signature to the Cloud
B. Collects forensic information about the event
C. Communicates the status of the endpoint to the ESM
D. Notifies the user about the event
E. Remediates the event by deleting the malicious file

Correct Answer: B, C, D
Section:
Explanation:
https://investors.paloaltonetworks.com/node/11156/html

QUESTION 45
Which two types of security chains are supported by the Decryption Broker? (Choose two.)

A. virtual wire
B. transparent bridge

C. Layer 3

D. Layer 2

Correct Answer: B, C
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-security-chains-multiple.html

QUESTION 46
Which three new script types can be analyzed in WildFire? (Choose three.)

A. VBScript

B. JScript

C. MonoScript

D. PythonScript

E. PowerShell Script

Correct Answer: A, B, E
Section:
Explanation:
The WildFire cloud is capable of analyzing the following script types:
JScript (.js)
VBScript (.vbs)
PowerShell Script (.ps1)
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/script-sample-support

QUESTION 47
A customer requests that a known spyware threat signature be triggered based on a rate of occurrence, for example, 10 hits in 5 seconds.
How is this goal accomplished?

A. Create a custom spyware signature matching the known signature with the time attribute

B. Add a correlation object that tracks the occurrences and triggers above the desired threshold

C. Submit a request to Palo Alto Networks to change the behavior at the next update

D. Configure the Anti-Spyware profile with the number of rule counts to match the occurrence frequency

Correct Answer: A
Section:

QUESTION 48
For customers with high bandwidth requirements for Service Connections, what two limitations exist when onboarding multiple Service Connections to the same Prisma Access location servicing a single Datacenter? (Choose two.)

A. Network segments in the Datacenter need to be advertised to only one Service Connection

B. The customer edge device needs to support policy-based routing with symmetric return functionality

C. The resources in the Datacenter will only be able to reach remote network resources that share the same region

D. A maximum of four service connections per Datacenter are supported with this topology

Correct Answer: A, D
Section:

QUESTION 49
WildFire subscription supports analysis of which three types? (Choose three.)

A. GIF
B. 7-Zip
C. Flash
D. RPM
E. ISO
F. DMG

Correct Answer: B, C, E
Section:
Explanation:
Reference: https://www.niap-ccevs.org/MMO/Product/st_vid11032-agd1.pdf

QUESTION 50
In an HA pair running Active/Passive mode, over which interface do the dataplanes communicate?

A. HA3
B. HA1
C. HA2
D. HA4

Correct Answer: C
Section:

QUESTION 51
A potential customer requires an NGFW solution which enables high-throughput, low-latency network security, all while incorporating unprecedented features and technology. They need a solution that solves the performance problems that plague today's security infrastructure.
Which aspect of the Palo Alto Networks NGFW capabilities can you highlight to help them address the requirements?

A. SP3 (Single Pass Parallel Processing)
B. GlobalProtect
C. Threat Prevention
D. Elastic Load Balancers

Correct Answer: A
Section:
Explanation:
Reference: https://www.paloguard.com/SP3-Architecture.asp

QUESTION 52
Which three features are used to prevent abuse of stolen credentials? (Choose three.)

A. multi-factor authentication
B. URL Filtering Profiles
C. WildFire Profiles
D. Prisma Access
E. SSL decryption rules

Correct Answer: A, C, E
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse

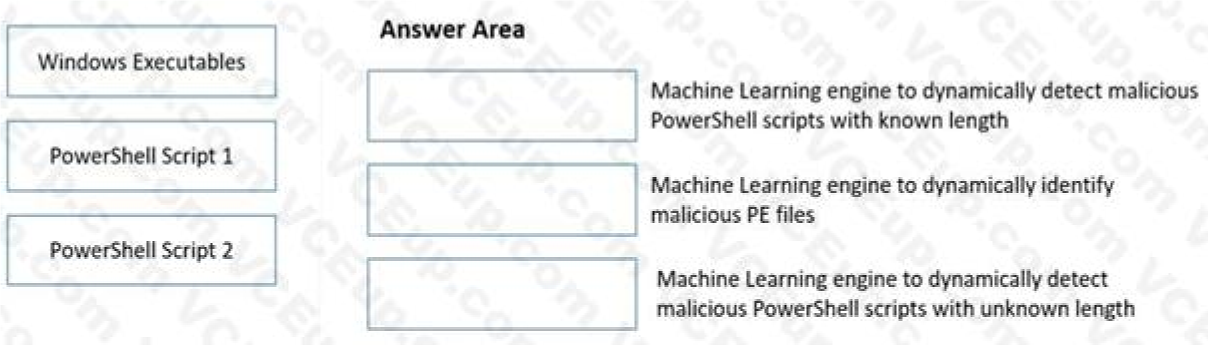
QUESTION 53
A customer has business-critical applications that rely on the general web-browsing application.
Which security profile can help prevent drive-by-downloads while still allowing web-browsing traffic?

A. File Blocking Profile
B. DoS Protection Profile
C. URL Filtering Profile
D. Vulnerability Protection Profile

Correct Answer: A
Section:
Explanation:
Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjaw53CvdHyAhUPy4UKHXT5D-
MQFnoECAMQAQ&url=https%3A%2F%2Fknowledgebase.paloaltonetworks.com%2Fservlet%2FfileField%3FentityId%3Dka10g000000U0roAAC%26field%3DAttachment_1__Body__s&usg=AOvVaw3DCBM7-
FwWInkWYANLrzUt (32)

QUESTION 54
DRAG DROP
Match the WildFire Inline Machine Learning Model to the correct description for that model.

Select and Place:



Windows Executables
PowerShell Script 1
PowerShell Script 2

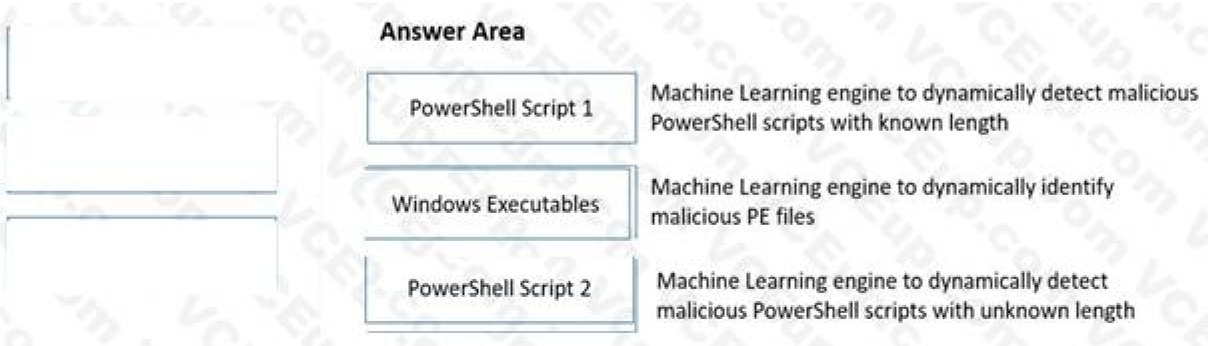
Answer Area

Machine Learning engine to dynamically detect malicious PowerShell scripts with known length

Machine Learning engine to dynamically identify malicious PE files

Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

Correct Answer:



Answer Area

PowerShell Script 1 — Machine Learning engine to dynamically detect malicious PowerShell scripts with known length

Windows Executables — Machine Learning engine to dynamically identify malicious PE files

PowerShell Script 2 — Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-inpanos-100/configure-wildfire-inline-ml.html

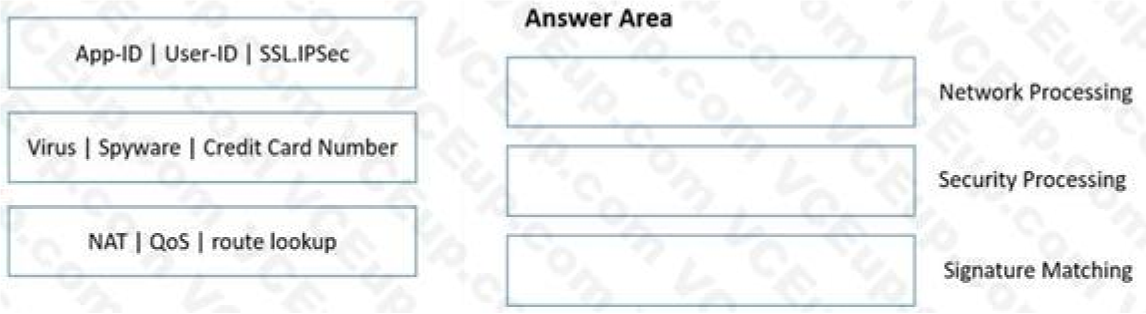
QUESTION 55
Which statement is true about Deviating Devices and metrics?

A. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation
B. Deviating Device Tab is only available with a SD-WAN Subscription
C. An Administrator can set the metric health baseline along with a valid standard deviation
D. Deviating Device Tab is only available for hardware-based firewalls

Correct Answer: A
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health.html

QUESTION 56
DRAG DROP
Match the functions to the appropriate processing engine within the dataplane.

Select and Place:



App-ID | User-ID | SSL.IPSec

Virus | Spyware | Credit Card Number

NAT | QoS | route lookup

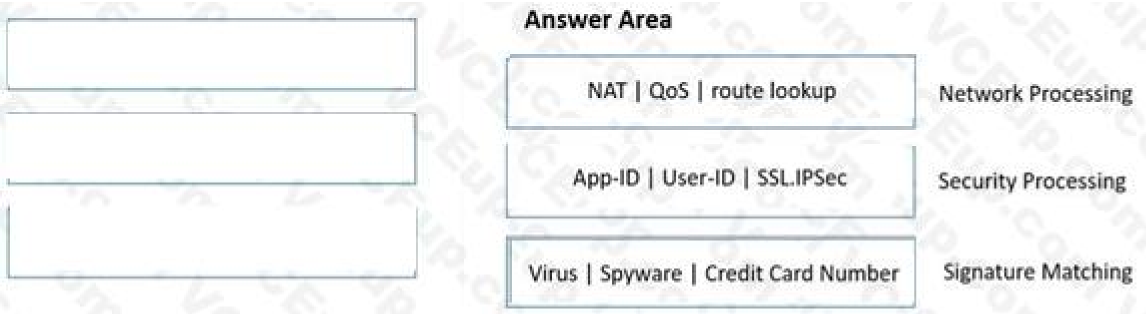
Answer Area

Network Processing

Security Processing

Signature Matching

Correct Answer:



Answer Area

NAT | QoS | route lookup — Network Processing

App-ID | User-ID | SSL.IPSec — Security Processing

Virus | Spyware | Credit Card Number — Signature Matching

Section:
Explanation:

QUESTION 57
What are three considerations when deploying User-ID? (Choose three.)

A. Specify included and excluded networks when configuring User-ID
B. Only enable User-ID on trusted zones
C. Use a dedicated service account for User-ID services with the minimal permissions necessary
D. User-ID can support a maximum of 15 hops
E. Enable WMI probing in high security networks

Correct Answer: A, B, C
Section:

QUESTION 58
Which three considerations should be made prior to installing a decryption policy on the NGFW? (Choose three.)

A. Include all traffic types in decryption policy
B. Inability to access websites
C. Exclude certain types of traffic in decryption policy
D. Deploy decryption setting all at one time
E. Ensure throughput is not an issue

Correct Answer: A, B, C
Section:

QUESTION 59
Which three components are specific to the Query Builder found in the Custom Report creation dialog of the firewall? (Choose three.)

A. Connector
B. Database
C. Recipient
D. Operator
E. Attribute
F. Schedule

Correct Answer: A, D, E
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/view-andmanage-reports/generate-custom-reports

QUESTION 60
What three Tabs are available in the Detailed Device Health on Panorama for hardware-based firewalls? (Choose three.)

A. Errors

B. Environments
C. Interfaces
D. Mounts
E. Throughput
F. Sessions
G. Status

Correct Answer: B, C, F
Section:
Explanation:
Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/detailed-device-health-in-panorama.html

QUESTION 61
Which is the smallest Panorama solution that can be used to manage up to 2500 Palo Alto Networks Next Generation firewalls?

A. M-200
B. M-600
C. M-100
D. Panorama VM-Series

Correct Answer: D
Section:
Explanation:
Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boF1CAI

QUESTION 62
XYZ Corporation has a legacy environment with asymmetric routing. The customer understands that Palo Alto Networks firewalls can support asymmetric routing with redundancy.
Which two features must be enabled to meet the customer's requirements? (Choose two.)

A. Virtual systems
B. HA active/active
C. HA active/passive
D. Policy-based forwarding

Correct Answer: B, D
Section:

QUESTION 63
Access to a business site is blocked by URL Filtering inline machine learning (ML) and considered as a false-positive.
How should the site be made available?

A. Disable URL Filtering inline ML
B. Create a custom URL category and add it to the Security policy
C. Create a custom URL category and add it on exception of the inline ML profile
D. Change the action of real-time detection category on URL filtering profile

Correct Answer: C
Section:

QUESTION 64
Which two features can be enabled to support asymmetric routing with redundancy on a Palo Alto networks next-generation firewall (NGFW)? (Choose two.)

A. Active / active high availability (HA)
B. Multiple virtual systems
C. non-SYN first packet
D. Asymmetric routing profile

Correct Answer: A, C
Section:

QUESTION 65
Which three mechanisms are valid for enabling user mapping? (Choose three.)

A. Captive Portal
B. Domain server monitoring
C. Reverse DNS lookup
D. User behaviour recognition
E. Client probing

Correct Answer: A, B, E
Section:

QUESTION 66
Which three of the following actions must be taken to enable Credential Phishing Prevention?
(Choose three.)

A. Enable User Credential Detection
B. Enable User-ID
C. Define a Secure Sockets Layer (SSL) decryption rule base
D. Enable App-ID
E. Define a uniform resource locator (URL) Filtering profile

Correct Answer: A, B, E
Section:

QUESTION 67
Which two configuration elements can be used to prevent abuse of stolen credentials? (Choose two.)

A. WildFire analysis
B. Dynamic user groups (DUGs)
C. Multi-factor authentication (MFA)
D. URL Filtering Profiles

Correct Answer: C, D
Section:

QUESTION 68
What are two benefits of the sinkhole Internet Protocol (IP) address that DNS Security sends to the client in place of malicious IP addresses? (Choose two.)

A. The client communicates with it instead of the malicious IP address
B. It represents the remediation server that the client should visit for patching
C. It will take over as the new DNS resolver for that client and prevent further DNS requests from occurring in the meantime
D. In situations where the internal DNS server is between the client and the firewall, it gives the firewall the ability to identify the clients who originated the query to the malicious domain

Correct Answer: A, D
Section:

QUESTION 69
A customer worried about unknown attacks is hesitant to enable SSL decryption due to privacy and regulatory issues. How does the platform address the customer's concern?

A. It overcomes reservations about SSL decrypt by offloading to a higher-capacity firewall to help with the decrypt throughput
B. It shows how AutoFocus can provide visibility into targeted attacks at the industry sector
C. It allows a list of websites or URL categories to be defined for exclusion from decryption
D. It bypasses the need to decrypt SSL traffic by analyzing the file while still encrypted

Correct Answer: C
Section:

QUESTION 70
WildFire machine learning (ML) for portable executable (PE) files is enabled in the antivirus profile and added to the appropriate firewall rules in the profile. In the Palo Alto Networks WildFire test av file, an attempt to download the test file is allowed through.
Which command returns a valid result to verify the ML is working from the command line.

A. show wfml cloud-status
B. show mlav cloud-status
C. show ml cloud-status
D. show av cloud-status

Correct Answer: B
Section:

QUESTION 71
A Fortune 500 customer has expressed interest in purchasing WildFire; however, they do not want to send discovered malware outside of their network.
Which version of WildFire will meet this customer's requirements?

A. WildFire Private Cloud
B. WildFire Government Cloud
C. WildFire Secure Cloud
D. WildFire Public Cloud

Correct Answer: A
Section:

QUESTION 72
Which filtering criterion is used to determine users to be included as members of a dynamic user group (DUG)?

A. Security policy rule
B. Tag
C. Login ID
D. IP address

Correct Answer: B
Section:

QUESTION 73
A customer is starting to understand their Zero Trust protect surface using the Palo Alto Networks Zero Trust reference architecture.
What are two steps in this process? (Choose two.)

A. Validate user identities through authentication
B. Gain visibility of and control over applications and functionality in the traffic flow using a port and protocol firewall
C. Categorize data and applications by levels of sensitivity
D. Prioritize securing the endpoints of privileged users because if non-privileged user endpoints are exploited, the impact will be minimal due to perimeter controls

Correct Answer: A, C
Section:

QUESTION 74
Which proprietary technology solutions will allow a customer to identify and control traffic sources regardless of internet protocol (IP) address or network segment?

A. User ID and Device-ID
B. Source-D and Network.ID
C. Source ID and Device-ID
D. User-ID and Source-ID

Correct Answer: A
Section:

QUESTION 75
When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can belogged?

A. X-Forwarded-For
B. HTTP method
C. HTTP response status code
D. Content type

Correct Answer: A
Section:

QUESTION 76

Which statement applies to Palo Alto Networks Single Pass Parallel Processing (SP3)?

A. It processes each feature in a separate single pass with additional performance impact for each enabled feature.
B. Its processing applies only to security features and does not include any networking features.
C. It processes all traffic in a single pass with no additional performance impact for each enabled feature.
D. It splits the traffic and processes all security features in a single pass and all network features in a separate pass

Correct Answer: C
Section:

QUESTION 77

WildFire can discover zero-day malware in which three types of traffic? (Choose three)

A. SMTP
B. HTTPS
C. FTP
D. DNS
E. TFTP

Correct Answer: A, B, C
Section:

QUESTION 78

In Panorama, which three reports or logs will help identify the inclusion of a host source in a command-and-control (C2) incident? (Choose three.)

A. SaaS reports
B. data filtering logs
C. WildFire analysis reports
D. threat logs
E. botnet reports

Correct Answer: C, D, E
Section:

QUESTION 79

What is the recommended way to ensure that firewalls have the most current set of signatures for up-to-date protection?

A. Run a Perl script to regularly check for updates and alert when one is released
B. Monitor update announcements and manually push updates to Crewall
C. Store updates on an intermediary server and point all the firewalls to it
D. Use dynamic updates with the most aggressive schedule required by business needs

Correct Answer: D
Section:

QUESTION 80

Which of the following statements is valid with regard to Domain Name System (DNS) sinkholing?

A. it requires the Vulnerability Protection profile to be enabled
B. DNS sinkholing signatures are packaged and delivered through Vulnerability Protection updates
C. infected hosts connecting to the Sinkhole Internet Protocol (IP) address can be identified in the traffic logs
D. It requires a Sinkhole license in order to activate

Correct Answer: C
Section:

QUESTION 81
A customer with a fully licensed Palo Alto Networks firewall is concerned about threats based on domain generation algorithms (DGAS).
Which Security profile is used to configure Domain Name Security (DNS) to Identity and block previously unknown DGA-based threats in real time?

A. URL Filtering profile
B. WildFire Analysis profile
C. Vulnerability Protection profile
D. Anti-Spyware profile

Correct Answer: D
Section:

QUESTION 82
Which three actions should be taken before deploying a firewall evaluation unt in a customer environment? (Choose three.)

A. Request that the customer make part 3978 available to allow the evaluation unit to communicate with Panorama
B. Inform the customer that a SPAN port must be provided for the evaluation unit, assuming a TAP mode deployment.
C. Upgrade the evaluation unit to the most current recommended firmware, unless a demo of the upgrade process is planned.
D. Set expectations for information being presented in the Security Lifecycle Review (SLR) because personal user information will be made visible
E. Reset the evaluation unit to factory default to ensure that data from any previous customer evaluation is removed

Correct Answer: B, C, E
Section:

QUESTION 83
Which statement best describes the business value of Palo Alto Networks Zero Touch Provisioning
(ZTP)?

A. It is designed to simplify and automate the onboarding of new firewalls to the Panorama management server.
B. When it is in place, it removes the need for an onsite firewall
C. When the service is purchased, Palo Alto Networks sends an engineer to physically deploy the firewall to the customer environment
D. It allows a firewall to be automatically connected to the local network wirelessly

Correct Answer: A
Section:

QUESTION 84

In PAN-OS 10.0 and later, DNS Security allows policy actions to be applied based on which three domains? (Choose three.)

A. grayware
B. command and control (C2)
C. benign
D. government
E. malware

Correct Answer: A, C, E
Section:

QUESTION 85
What will best enhance security of a production online system while minimizing the impact for the existing network?

A. Layer 2 interfaces
B. active / active high availability (HA)
C. Virtual wire
D. virtual systems

Correct Answer: C
Section:

QUESTION 86
Which Security profile on the Next-Generation Firewall (NGFW) includes Signatures to protect against brute force attacks?

A. Vulnerability Protection profile
B. Antivirus profile
C. URL Filtering profile
D. Anti-Spyware profile

Correct Answer: A
Section:

QUESTION 87
A prospective customer currently uses a firewall that provides only Layer 4 inspection and protections. The customer sees traffic going to an external destination, port 53, but cannot determine what Layer 7 application traffic is going over that port Which capability of PAN-OS would address the customer's lack of visibility?

A. Device ID, because it will give visibility into which devices are communicating with external destinations over port 53
B. single pass architecture (SPA), because it will improve the performance of the Palo Alto Networks Layer 7 inspection
C. User-ID, because it will allow the customer to see which users are sending traffic to external destinations over port 53
D. App-ID, because it will give visibility into what exact applications are being run over that port and allow the customer to block unsanctioned applications using port 53

Correct Answer: D
Section:

QUESTION 88
Which solution informs a customer concerned about zero-day targeted attacks whether an attack is specifically targeted at its property?

A. AutoFocus
B. Panorama Correlation Report
C. Cortex XSOAR Community edition
D. Cortex XDR Prevent

Correct Answer: A
Section:

QUESTION 89
In which two ways can PAN-OS software consume MineMeld outputs? (Choose two.)

A. TXT
B. API
C. CSV
D. EDL

Correct Answer: A, D
Section:

QUESTION 90
Which domain permissions are required by the User-ID Agent for WMI Authentication on a Windows Server? (Choose three.)

A. Domain Administrators
B. Enterprise Administrators
C. Distributed COM Users
D. Event Log Readers
E. Server Operator

Correct Answer: A, D, E
Section:
Explanation:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/user-id-agent-setup/user-id-agent-setupwmi-authentication

QUESTION 91
Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?

A. WildFire hybrid deployment
B. 5 minute WildFire updates to threat signatures
C. Access to the WildFire API
D. PE file upload to WildFire

Correct Answer: D
Section: