Palo Alto Networks

PSE-Strata
Palo Alto Networks System Engineer Professional - Strata

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Total Questions: 139
Latest Version: 8.0

Question: 1

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

A. VBScript
B. JScript
C. MonoScript
D. PythonScript
E. PowerShell Script

Answer: ABE

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: 2

Which two configuration items are required when the NGFW needs to act as a decryption broker for multiple transparent bridge security chains? (Choose two.)

A. dedicated pair of decryption forwarding interfaces required per security chain
B. a unique Transparent Bridge Decryption Forwarding Profile to a single Decryption policy rule
C. a unique Decryption policy rule is required per security chain
D. a single pair of decryption forwarding interfaces

Answer: BC

Question: 3

Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)

A. Quarantine
B. Allow

C. Reset
D. Redirect
E. Drop
F. Alert

Answer: BCEF

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles.html

Question: 4

A price-sensitive customer wants to prevent attacks on a Windows Virtual Server. The server will max out at 100Mbps but needs to have 45.000 sessions to connect to multiple hosts within a data center Which VM instance should be used to secure the network by this customer?

A. VM-200
B. VM-100
C. VM-50
D. VM-300

Answer: C

Question: 5

Which license is required to receive weekly dynamic updates to the correlation objects on the firewall and Panorama?

A. WildFire on the firewall, and AutoFocus on Panorama
B. Threat Prevention on the firewall, and Support on Panorama
C. GlobalProtect on the firewall, and Threat Prevention on Panorama
D. URL Filtering on the firewall, and MineMeld on Panorama

Answer: B

Question: 6

Which three items contain information about Command-and-Control (C2) hosts? (Choose three.)

A. Threat logs
B. WildFire analysis reports
C. Botnet reports
D. Data filtering logs

E. SaaS reports

Answer: BCD

Question: 7

When the Cortex Data Lake is sized for Prisma Access mobile users, what is a valid log size range you would use per day. per user?

A. 1500 to 2500 bytes
B. 10MB to 30 MB
C. 1MB to 5 MB
D. 100MB to 200 MB

Answer: D

Question: 8

A customer with a legacy firewall architecture is focused on port and protocol level security, and has heard that next generation firewalls open all ports by default. What is the appropriate rebuttal that positions the value of a NGFW over a legacy firewall?

A. Palo Alto Networks keep ports closed by default, only opening ports after understanding the application request, and then opening only the application-specified ports.
B. Palo Alto Networks does not consider port information, instead relying on App-ID signatures that do not reference ports.
C. Default policies block all interzone traffic. Palo Alto Networks empowers you to control applications by default ports or a configurable list of approved ports on a per-policy basis.
D. Palo Alto Networks NGFW protects all applications on all ports while leaving all ports opened by default.

Answer: B

Question: 9

Which two steps are required to configure the Decryption Broker? (Choose two.)

A. reboot the firewall to activate the license
B. activate the Decryption Broker license
C. enable SSL Forward Proxy decryption
D. enable a pair of virtual wire interfaces to forward decrypted traffic

Answer: BD

Question: 10

What are three purposes for the Eval Systems, Security Lifecycle Reviews and Prevention Posture Assessment tools? (Choose three.)

A. when you're delivering a security strategy
B. when client's want to see the power of the platform
C. provide users visibility into the applications currently allowed on the network
D. help streamline the deployment and migration of NGFWs
E. assess the state of NGFW feature adoption

Answer: BCE

Question: 11

An Administrator needs a PDF summary report that contains information compiled from existing reports based on data for the Top five(5) in each category Which two timeframe options are available to send this report? (Choose two.)

A. Daily
B. Monthly
C. Weekly
D. Bi-weekly

Answer: AC

Question: 12

Which three signature-based Threat Prevention features of the firewall are informed by intelligence from the Threat Intelligence Cloud? (Choose three.)

A. Vulnerability protection
B. Anti-Spyware
C. Anti-Virus
D. Botnet detection
E. App-ID protection

Answer: ABE

Question: 13

The firewall includes predefined reports, custom reports can be built for specific data and actionable tasks, or predefined and custom reports can be combined to compile information needed to monitor network security.
The firewall provides which three types of reports? (Choose three.)

A. SNMP Reports
B. PDF Summary Reports
C. Netflow Reports
D. Botnet Reports
E. User or Group Activity Reports

Answer: CDE

Question: 14

Which Palo Alto Networks pre-sales tool involves approximately 4 hour interview to discuss a customer's current security posture?

A. BPA
B. PPA
C. Expedition
D. SLR

Answer: A

Question: 15

What is the key benefit of Palo Alto Networks Single Pass Parallel Processing design?

A. There are no benefits other than slight performance upgrades
B. It allows Palo Alto Networks to add new functions to existing hardware
C. Only one processor is needed to complete all the functions within the box
D. It allows Palo Alto Networks to add new devices to existing hardware

Answer: B

Question: 16

Which security profile on the NGFW includes signatures to protect you from brute force attacks?

A. Zone Protection Profile
B. URL Filtering Profile
C. Vulnerability Protection Profile
D. Anti-Spyware Profile

Answer: C

Question: 17

The need for a file proxy solution, virus and spyware scanner, a vulnerability scanner, and HTTP decoder for URL filtering is handled by which component in the NGFW?

A. First Packet Processor
B. Stream-based Signature Engine
C. SIA (Scan It All) Processing Engine
D. Security Processing Engine

Answer: B

Reference:
https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdfn (page 6)

Question: 18

A customer is looking for an analytics tool that uses the logs on the firewall to detect actionable events on the network. They require something to automatically process a series of related threat events that, when combined, indicate a likely compromised host on their network or some other higher level conclusion. They need to pinpoint the area of risk, such as compromised hosts on the network, allows you to assess the risk and take action to prevent exploitation of network resources.
Which feature of PAN-OS can you talk about to address their requirement to optimize their business outcomes?

A. The Automated Correlation Engine
B. Cortex XDR and Cortex Data Lake
C. WildFire with API calls for automation
D. 3rd Party SIEM which can ingest NGFW logs and perform event correlation

Answer: A

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/use-the-automated-correlation-engine.html

Question: 19

Which two email links, contained in SMTP and POP3, can be submitted from WildFire analysis with a WildFire subscription? (Choose two.)

A. FTP
B. HTTPS
C. RTP
D. HTTP

Answer: B, D

Question: 20

What two types of certificates are used to configure SSL Forward Proxy? (Choose two.)

A. Enterprise CA-signed certificates
B. Self-Signed certificates
C. Intermediate certificates
D. Private key certificates

Answer: A, B

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward-proxy#:~:text=You%20can%20use%20an%20enterprise,as%20the%20forward%20trust

%20certificate.&text=Certificate%20Name-,.,unique%20name%20for%20each%20firewall

Question: 21

Which two of the following does decryption broker provide on a NGFW? (Choose two.)

A. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic only once
B. Eliminates the need for a third party SSL decryption option which allows you to reduce the total number of third party devices performing analysis and enforcement
C. Provides a third party SSL decryption option which allows you to increase the total number of third party devices performing analysis and enforcement
D. Decryption broker allows you to offload SSL decryption to the Palo Alto Networks next-generation firewall and decrypt traffic multiple times

Answer: A, D

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker.html

Question: 22

There are different Master Keys on Panorama and managed firewalls.
What is the result if a Panorama Administrator pushes configuration to managed firewalls?

A. The push operation will fail regardless of an error or not within the configuration itself
B. Provided there's no error within the configuration to be pushed, the push will succeed
C. The Master Key from the managed firewalls will be overwritten with the Master Key from Panorama
D. There will be a popup to ask if the Master Key from the Panorama should replace the Master Key from the managed firewalls

Answer: A

Reference:
https://www.reddit.com/r/paloaltonetworks/comments/onz15y/what_is_the_result_if_a_panorama_administrator/

Question: 23

Which task would be identified in Best Practice Assessment tool?

A. identify the visibility and presence of command-and-control sessions
B. identify sanctioned and unsanctioned SaaS applications
C. identify the threats associated with each application
D. identify and provide recommendations for device management access

Answer: B

Question: 24

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

Answer: A

Question: 25

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

Answer: A, D

Question: 26

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

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

Answer: B, C, E

Reference: https://www.niap-ccevs.org/MMO/Product/st_vid11032-agd1.pdf

Question: 27

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

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

Answer: C

Question: 28

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

Answer: A

Reference: https://www.paloguard.com/SP3-Architecture.asp

Question: 29

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

Answer: A, C, E

Reference: https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-delivers-industry-first-capabilities-to-prevent-credential-theft-and-abuse

Question: 30

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

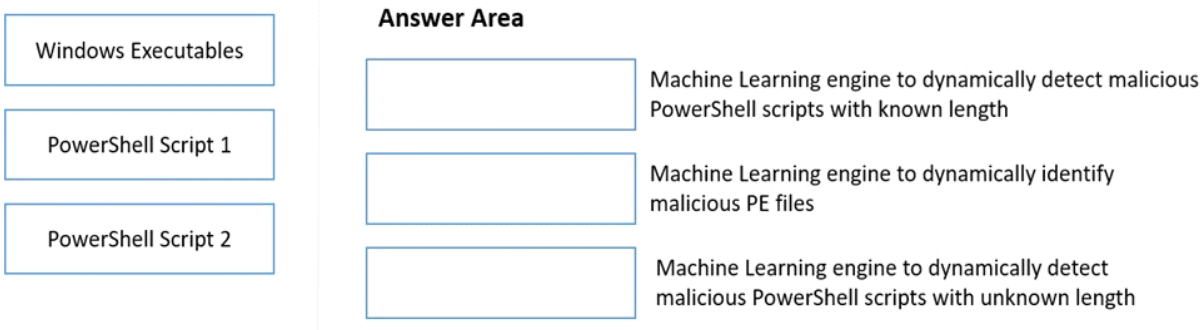
Answer: A

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: 31

Match the WildFire Inline Machine Learning Model to the correct description for that model.



Answer:

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

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

Question: 32

Which statement is true about Deviating Devices and metrics?

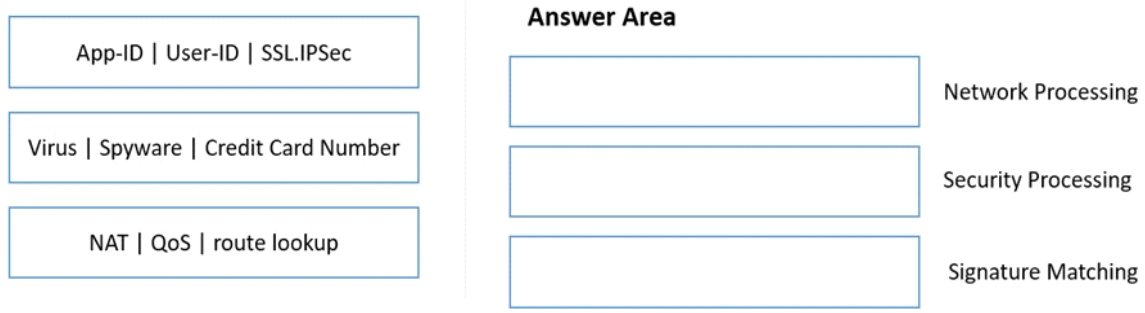
A. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation
B. Deviating Device Tab is only available with a SD-WAN Subscription
C. An Administrator can set the metric health baseline along with a valid standard deviation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

Answer: A

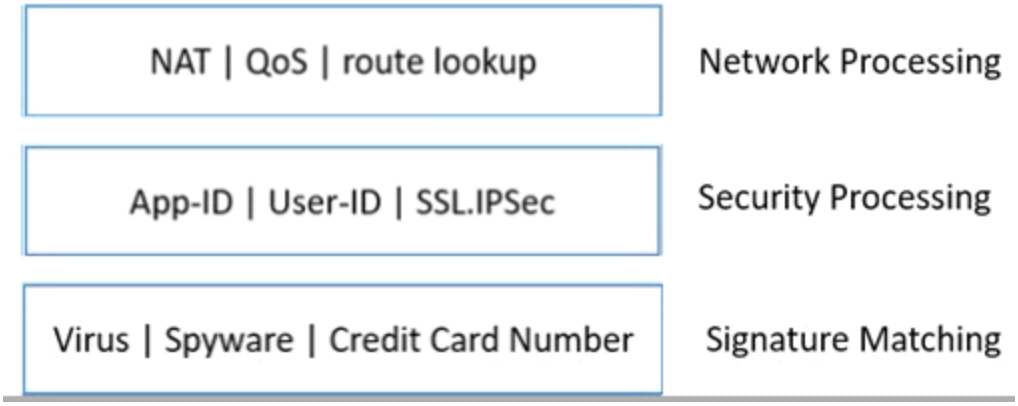
Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health.html

Question: 33

Match the functions to the appropriate processing engine within the dataplane.



Answer:



Question: 34

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

Answer: A, B, C

Question: 35

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

Answer: A, B, C

Question: 36

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

Answer: A, D, E

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports

Question: 37

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

Answer: B, C, D

Question: 38

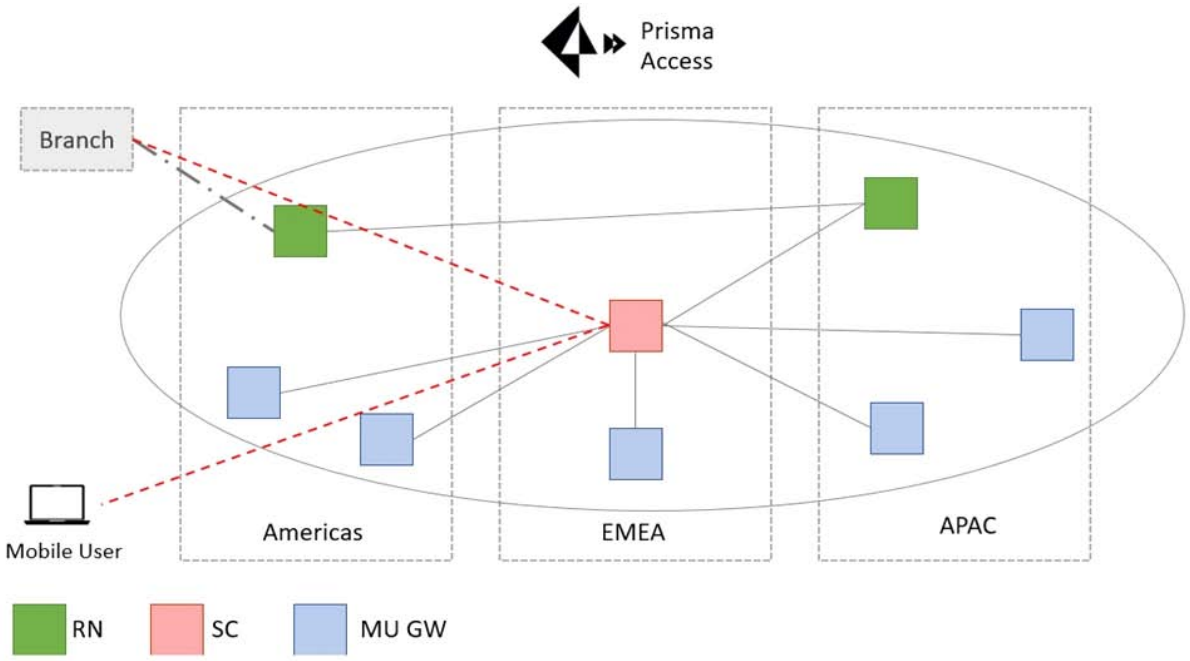
When having a customer pre-sales call, which aspects of the NGFW should be covered?

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

Answer: D

Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering

Question: 39



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

Answer: C

Question: 40

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

Answer: A, C, D, E

Reference: https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/monitor-wildfire-activity/use-the-firewall-to-monitor-malware/monitor-wildfire-submissions-and-analysis-reports.html

Question: 41

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

Answer: B, C, F

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: 42

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

Answer: D

Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boF1CAI

Question: 43

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

Answer: B, D

Question: 44

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

Answer: C

Question: 45

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

Answer: A, C

Question: 46

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

Answer: A, B, E

Question: 47

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

Answer: A, B, E

Question: 48

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

Answer: C, D

Question: 49

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

Answer: A, D

Question: 50

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

Answer: C

Question: 51

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

Answer: B

Question: 52

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

Answer: A

Question: 53

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

Answer: B

Question: 54

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

Answer: A, C

Question: 55

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

Answer: A

Question: 56

When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?

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

Answer: A

Question: 57

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

Answer: C

Question: 58

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

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

Answer: A, B, C

Question: 59

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

Answer: C, D, E

Question: 60

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

Answer: D

Question: 61

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

Answer: C

Question: 62

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

Answer: D

Question: 63

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

Answer: B, C, E

Question: 64

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

Answer: A

Question: 65

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

Answer: A, C, E

Question: 66

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

Answer: C

Question: 67

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

Answer: A

Question: 68

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

Answer: D

Question: 69

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

Answer: A

Question: 70

A customer requires protections and verdicts for portable executable (PE) and executable and linkable format (ELF), as well as the ability to integrate with existing security tools.
Which Cloud-Delivered Security Service (CDSS) does Palo Alto Networks provide that will address this requirement?

A. Dynamic Unpacking
B. WildFire
C. DNS Security
D. File Blocking profile

Answer: B

Question: 71

A WildFire subscription is required for which two of the following activities? (Choose two)

A. Filter uniform resource locator (URL) sites by category.
B. Forward advanced file types from the firewall for analysis.
C. Use the WildFire Application Programming Interface (API) to submit website links for analysis
D. Enforce policy based on Host Information Profile (HIP)
E. Decrypt Secure Sockets Layer (SSL)

Answer: B, C

Question: 72

Within the Five-Step Methodology of Zero Trust, in which step would application access and user access be defined?

A. Step 3: Architect a Zero Trust Network
B. Step 5. Monitor and Maintain the Network
C. Step 4: Create the Zero Trust Policy
D. Step 1: Define the Protect Surface
E. Step 2 Map the Protect Surface Transaction Flows

Answer: D

Question: 73

Which two features are key in preventing unknown targeted attacks? (Choose two)

A. nighty botnet report
B. App-ID with the Zero Trust model
C. WildFire Cloud threat analysis
D. Single Pass Parallel Processing (SP3)

Answer: B, C

Question: 74

A customer is designing a private data center to host their new web application along with a separate headquarters for users.
Which cloud-delivered security service (CDSS) would be recommended for the headquarters only?

A. Threat Prevention
B. DNS Security
C. WildFire
D. Advanced URL Filtering (AURLF)

Answer: A

Question: 75

Which two methods are used to check for Corporate Credential Submissions? (Choose two.)

A. doman credentialiter
B. User-ID credential check
C. LDAP query
D. IP user mapping

Answer: A, B

Question: 76

Which CLI command allows visibility into SD-WAN events such as path Selection and path quality measurements?

A. >show sdwan path-monitor stats vif
B. >show sdwan session distribution policy-name
C. >show sdwan connection all
D. >show sdwan event

Answer: D

Question: 77

A customer requires an analytics tool with the following attributes:
- Uses the logs on the firewall to detect actionable events on the network
- Automatically processes a series of related threat events that, when combines, indicate a likely comprised host on the network
- Pinpoints the area of risk and allows for assessment of the risk to action can be taken to prevent exploitation of network resources
Which feature of PAN-OS will address these requirements?

A. WildFire with application program interface (API) calls for automation
B. Third-party security information and event management (SIEM) which can ingest next-generation firewall (NGFW) logs
C. Automated correlation engine (ACE)
D. Cortex XDR and Cortex Data Lake

Answer: C

Question: 78

What are three key benefits of the Palo Alto Networks platform approach to security? (Choose three)

A. operational efficiencies due to reduction in manual incident review and decrease in mean time to resolution (MTTR)
B. improved revenue due to more efficient network traffic throughput
C. Increased security due to scalable cloud delivered security Services (CDSS)
D. Cost savings due to reduction in IT management effort and device

Answer: B, C, D

Question: 79

Which Palo Alto Networks security component should an administrator use to and NGFW policies to remote users?

A. Prisma SaaS API
B. Threat intelligence Cloud
C. GlobalProtect
D. Cortex XDR

Answer: C

Question: 80

The ability to prevent users from resolving internet protocol (IP) addresses to malicious, grayware, or newly registered domains is provided by which Security service?

A. WildFire
B. DNS Security
C. Threat Prevention
D. loT Security

Answer: B

Question: 81

in which step of the Palo Alto Networks Five-Step Zero Trust Methodology would an organization's critical data, applications, assets, and services (DAAS) be identified?

A. Step 4. Create the Zero Trust policy.
B. Step 2: Map the transaction flows.
C. Step 3. Architect a Zero Trust network.
D. Step 1: Define the protect surface

Answer: D

Question: 82

Which built-in feature of PAN-OS allows the NGFW administrator to create a policy that provides autoremediation for anomalous user behavior and malicious activity while maintaining user visibility?

A. Dynamic user groups (DUGS)
B. tagging groups
C. remote device User-ID groups
D. dynamic address groups (DAGs)

Answer: A

Question: 83

What will a Palo Alto Networks next-generation firewall (NGFW) do when it is unable to retrieve a DNS verdict from the DNS cloud service in the configured lookup time?

A. allow the request and all subsequent responses
B. temporarily disable the DNS Security function
C. block the query
D. discard the request and all subsequent responses

Answer: A

Question: 84

What is the default behavior in PAN-OS when a 12 MB portable executable (PE) fe is forwarded to the WildFire cloud service?

A. PE File is not forwarded.
B. Flash file is not forwarded.
C. PE File is forwarded
D. Flash file is forwarded

Answer: C

Question: 85

What is an advantage of having WildFire machine learning (ML) capability Inline on the firewall?

A. It eliminates of the necessity for dynamic analysis in the cloud
B. It enables the firewall to block unknown malicious files in real time and prevent patient zero without disrupting business productivity
C. It is always able to give more accurate verdicts than the cloud ML analysis reducing false positives and false negatives
D. It improves the CPU performance of content inspection

Answer: B

Question: 86

Which three script types can be analyzed in WildFire? (Choose three)

A. PythonScript
B. MonoSenpt
C. JScript

D. PowerShell Script
E. VBScript

Answer: A, C, E

Question: 87

What are two ways to manually add and remove members of dynamic user groups (DUGs)? (Choose two)

A. Add the user to an external dynamic list (EDL).
B. Tag the user using Panorama or the Web Ul of the firewall.
C. Tag the user through the firewalls XML API.
D. Tag the user through Active Directory

Answer: B, C

Question: 88

A packet that is already associated with a current session arrives at the firewall.
What is the flow of the packet after the firewall determines that it is matched with an existing session?

A. it is sent through the fast path because session establishment is not required. If subject to content inspection, it will pass through a single stream-based content inspection engine before egress.
B. It is sent through the slow path for further inspection. If subject to content inspection, it will pass through a single stream-based content inspection engines before egress
C. It is sent through the fast path because session establishment is not required. If subject to content inspection, it will pass through multiple content inspection engines before egress
D. It is sent through the slow path for further inspection. If subject to content inspection, it will pass through multiple content inspection engines before egress

Answer: A

Question: 89

What helps avoid split brain in active / passive high availability (HA) pair deployment?

A. Enable preemption on both firewalls in the HA pair.
B. Use a standard traffic interface as the HA3 link.
C. Use the management interface as the HA1 backup link
D. Use a standard traffic interface as the HA2 backup

Answer: C

Question: 90

The Palo Ao Networks Cloud Identity Engino (CIE) includes which service that supports identity Providers (IdP)?

A. Directory Sync and Cloud Authentication Service that support IdP ung SAML 2.0 and OAuth2
B. Cloud Authentication Service that supports IdP using SAML 2.0 and OAuth2
C. Directory Sync and Cloud Authentication Service that support IdP ng SAML 2.0
D. Directory Sync that supports IdP using SAML 2.0

Answer: A

Question: 91

Which component is needed for a large-scale deployment of NGFWs with multiple Panorama Management Servers?

A. M-600 appliance
B. Panorama Interconnect plugin
C. Panorama Large Scale VPN (LSVPN) plugin
D. Palo Alto Networks Cluster license

Answer: B

Question: 92

What are three sources of malware sample data for the Threat Intelligence Cloud? (Choose three)

A. Next-generation firewalls deployed with WildFire Analysis Security Profiles
B. WF-500 configured as private clouds for privacy concerns
C. Correlation Objects generated by AutoFocus
D. Third-party data feeds such as partnership with ProofPomt and the Cyber Threat Alliance
E. Palo Alto Networks non-firewall products such as Traps and Prisma SaaS

Answer: CDE

https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus

Question: 93

What are two core values of the Palo Alto Network Security Operating Platform? (Choose two.}

A. prevention of cyber attacks
B. safe enablement of all applications
C. threat remediation
D. defense against threats with static security solution

Answer: AC

Question: 94

What are two advantages of the DNS Sinkholing feature? (Choose two.)

A. It forges DNS replies to known malicious domains.
B. It monitors DNS requests passively for malware domains.
C. It can be deployed independently of an Anti-Spyware Profile.
D. It can work upstream from the internal DNS server.

Answer: AD

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/threat-prevention/dns-sinkholing

Question: 95

Which two products can send logs to the Cortex Data Lake? (Choose two.)

A. AutoFocus
B. PA-3260 firewall
C. Prisma Access
D. Prisma Public Cloud

Answer: BC

https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-cortex-data-lake/forward-logs-to-cortex-data-lake

Question: 96

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

Answer: AC

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/enable-user-id

Question: 97

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

Answer: ACDF

Question: 98

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

Answer: BCE

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/prevent-credential-phishing.html

Question: 99

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

Answer: C

Question: 100

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

Answer: BDG

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/user-id-concepts/user-mapping

Question: 101

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

Answer: BD

Question: 102

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.

Answer: AD

Question: 103

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

Answer: AC

https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-web-interface/panorama-templates/template-stacks

Question: 104

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

Answer: A

Question: 105

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

Answer: A

https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-concepts/wildfire-signatures

Question: 106

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

Answer: AD

Question: 107

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

Answer: BC

Question: 108

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

Answer: CD

Question: 109

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

Answer: A

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

Question: 110

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

Answer: AD

Question: 111

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

Answer: A, B, E

Question: 112

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

Answer: AB

Question: 113

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

Answer: C

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

Question: 114

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

Answer: B

Question: 115

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

Answer: BCF

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture

Question: 116

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

Answer: D

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

Question: 117

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

Answer: BD

https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-file-type-support

Question: 118

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

Answer: D

Question: 119

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

Answer: CD

Question: 120

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

Answer: A, B

Question: 121

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

Answer: B

Question: 122

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

Answer: D

Question: 123

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

Answer: C

Question: 124

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

Answer: A

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: 125

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

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

Answer: AD

Question: 126

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

Answer: ADE

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-setup-wmi-authentication

Question: 127

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

Answer: D

Question: 128

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

Answer: B

Question: 129

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

Answer: B

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/migrate-your-cortex-xdr-license

Question: 130

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

Answer: AB

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/route-based-redundancy

Question: 131

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)

Answer: C

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html

Question: 132

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

Answer: CD

Question: 133

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

Answer: B

Question: 134

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

Answer: D

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVMCA0

Question: 135

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

Answer: D

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: 136

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

Answer: A

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

Question: 137

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

Answer: C

Question: 138

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

Answer: BCD

https://investors.paloaltonetworks.com/node/11156/html

Question: 139

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

Answer: BC

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-security-chains-multiple.html

For More Information – Visit link below:

http://www.certsgrade.com/

PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

Discount Coupon Code: CERTSGRADE10