PaloaltoNetworks.PSE-Strata.v2025-04-23.q126

Exam Code:	PSE-Strata
Exam Name:	Palo Alto Networks System Engineer Professional - Strata Exam
Certification Provider:	Paloalto Networks
Free Question Number:	126
Version:	v2025-04-23
# of views:	4138
# of Questions views:	1260
https://www.freepdfdumps.com/PaloaltoNetworks.PSE-Strata.v2025-04-23.q126.html	

NEW QUESTION: 1
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 (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-concepts/wildfire-sign

NEW QUESTION: 2
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: (SHOW ANSWER)
In a Palo Alto Networks Next-Generation Firewall (NGFW), supporting asymmetric routing with redundancy requires specific features to handle traffic that may not follow the same path in both directions.
* Active / active high availability (HA): This feature allows two firewalls to operate in tandem, sharing the traffic load. Active/active HA mode is designed to handle asymmetric routing scenarios where traffic might ingress through one firewall and egress through another, ensuring continuity and redundancy.

* non-SYN first packet: This feature is crucial for dealing with non-standard traffic patterns where the initial packet may not always be a SYN packet (typical in TCP connections). It allows the firewall to handle and correctly process such packets, which is essential in asymmetric routing scenarios.

NEW QUESTION: 3
Which task would be identified in Best Practice Assessment tool?
A. identify sanctioned and unsanctioned SaaS applications
B. identify the visibility and presence of command-and-control sessions
C. identify and provide recommendations for device management access
D. identify the threats associated with each application
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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-1YRr 1x PAN-LGS-1TB-1YR, 1x PAN-PRA-25, 1x PAN-SVC-BAS-PRA-25
C. 5500x PAN-GPCS-USER-C-BAS-1YR, 1000x PAN-GPCS-NET-B-BAS-1YR, 1x PAN-SVC-BAS-PRA-25. 1x PAN-PRA-25
D. 1x PAN-GPCS-USER-C-BAS-1YR, 1x PAN-GPCS-NET-B-BAS-1YR, 1x PAN-LGS-1TB-1YR
Answer: B (LEAVE A REPLY)

NEW QUESTION: 5
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 (LEAVE A REPLY)
Palo Alto Networks uses proprietary technologies to identify and control traffic sources regardless of IP address or network segment. These technologies include:
* User-ID (A): This technology maps IP addresses to user identities, allowing policies to be enforced based on user or group identity rather than just IP addresses. This is especially useful in dynamic environments where IP addresses can change frequently.

* Device-ID (A): This technology helps to identify and control devices accessing the network. It provides visibility into which devices are on the network and ensures that policies can be applied based on device type and identity.
References:
* Palo Alto Networks, User-ID and Device-ID Documentation.
* Palo Alto Networks, Technology Whitepapers.

NEW QUESTION: 6
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 (LEAVE A REPLY)
The Vulnerability Protection Profile on a Next-Generation Firewall (NGFW) includes signatures specifically designed to protect against a variety of threats, including brute force attacks. This profile utilizes a database of known vulnerabilities and exploits to detect and block malicious attempts to compromise network security. By applying this profile, administrators can prevent attackers from successfully using brute force methods to gain unauthorized access to systems.

NEW QUESTION: 7
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: (SHOW ANSWER)
Explanation
https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus

NEW QUESTION: 8
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 (LEAVE A REPLY)

When a Palo Alto Networks next-generation firewall (NGFW) is unable to retrieve a DNS verdict from the DNS cloud service within the configured lookup time, it will allow the request and all subsequent responses.
This is to ensure that legitimate traffic is not disrupted due to the inability to obtain a verdict in a timely manner.
* Default Behavior:
* The firewall is designed to maintain network availability and reliability. If it cannot retrieve a DNS verdict, it defaults to allowing the traffic to prevent unnecessary disruption.

NEW QUESTION: 9
A client chooses to not block uncategorized websites.
Which two additions should be made to help provide some protection? (Choose two.)
A. A file blocking profile attached to security policy rules that allow uncategorized websites to help reduce the risk of drive by downloads
B. A URL filtering profile with the action set to continue for unknown URL categories to security policy rules that allow web access
C. A security policy rule using only known URL categories with the action set to allow
D. A data filtering profile with a custom data pattern to security policy rules that deny uncategorized websites
Answer: (SHOW ANSWER)

NEW QUESTION: 10
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,C (LEAVE A REPLY)
When a client chooses not to block uncategorized websites, additional measures are necessary to maintain a level of protection.
* A URL filtering profile with the action set to continue for unknown URL categories: By setting the action to continue, users will be prompted before accessing uncategorized websites, which provides an extra layer of caution and awareness, helping to mitigate risks associated with unknown sites.
* A file blocking profile attached to security policy rules: This helps to reduce the risk of drive-by downloads by blocking potentially harmful file types from being downloaded when users visit

uncategorized websites. This additional layer of security ensures that even if users access risky sites, the likelihood of malicious file downloads is minimized.

NEW QUESTION: 11
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: (SHOW ANSWER)
In PAN-OS, when a portable executable (PE) file larger than 10 MB (default threshold) is encountered, it is not forwarded to the WildFire cloud service. This is due to size limitations on file submissions to the service.
* Default Behavior:
* Files exceeding the size limit are not forwarded to WildFire for analysis.

NEW QUESTION: 12
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: (SHOW ANSWER)
When generating an SLR (Security Lifecycle Review) report for a school concerned about students accessing inappropriate websites, the SE should:
* Remove unwanted categories listed under 'High Risk' and focus on categories that are relevant to the school's concerns. This approach allows the SE to tailor the report to highlight specific URL categories that the school is worried about, such as adult content, violence, or other inappropriate material.
By customizing the report to emphasize these categories, the SE can effectively demonstrate the firewall's capability to detect and block access to inappropriate websites, addressing the school's specific concerns directly.
This customization ensures that the SLR report is relevant and useful for the customer's needs, showcasing the firewall's strengths in URL filtering and content control.

NEW QUESTION: 13

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

A. Cost savings due to reduction in IT management effort and device

B. minimized threat landscape due to reducing internet footprint to a single point of failure

C. operational efficiencies due to reduction in manual incident review and decrease in mean time to resolution (MTTR)

D. improved revenue due to more efficient network traffic throughput

E. Increased security due to scalable cloud delivered security Services (CDSS)

Answer: A,D,E (LEAVE A REPLY)

NEW QUESTION: 14

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: B,C,E (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 15

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

A. SSL decryption rules

B. URL Filtering Profiles

C. WildFire Profiles

D. Prisma Access

E. multi-factor authentication

Answer: (SHOW ANSWER)

NEW QUESTION: 16

What filtering criteria is used to determine what users to include as members of a dynamic user group?

A. Tags

B. Login IDs

C. Security Policy Rules

D. IP Addresses

Answer: (SHOW ANSWER)

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

NEW QUESTION: 17
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: (SHOW ANSWER)
Using Panorama for managing virtual firewalls in a data center deployment provides several advantages:
* Automated Correlation Engine Functionality: Panorama offers an Automated Correlation Engine that can aggregate and analyze logs from multiple firewalls, including virtual ones, to identify patterns and threats that individual firewalls might not detect. This centralized analysis capability is crucial for comprehensive threat detection and response (Palo Alto Networks) (Palo Alto Networks).
* Bootstrapping Virtual Firewalls: Panorama can automate the deployment of virtual firewalls by using bootstrapping configurations. This allows for dynamic and rapid deployment of firewalls in cloud environments, ensuring that security policies are consistently applied from the moment the virtual firewalls are launched (Palo Alto Networks) (Palo Alto Networks).

NEW QUESTION: 18
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: A,C,D (LEAVE A REPLY)
The Palo Alto Networks platform approach to security offers several key benefits:
* Operational Efficiencies: By automating incident review and response, the platform reduces the need for manual intervention, thereby decreasing the mean time to resolution (MTTR). This streamlines security operations and allows teams to focus on more strategic tasks.
* Increased Security: The scalable cloud-delivered security services (CDSS) provided by Palo Alto Networks ensure that security measures can be dynamically scaled to meet the needs of the organization, offering robust protection against evolving threats.
* Cost Savings: The platform reduces the overall IT management effort and device requirements, leading to significant cost savings. This is achieved through integrated solutions that minimize the need for multiple disparate security products and simplify management.

NEW QUESTION: 19
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. identify sanctioned and unsanctioned SaaS applications
D. expose the visibility and presence of command-and-control sessions
E. use of device management access and settings
Answer: (SHOW ANSWER)

NEW QUESTION: 20
How many recursion levels are supported for compressed files in PAN-OS 8.0?
A. 3
B. 5
C. 2
D. 4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
As you prepare to scan your Amazon S3 account, what enables Prisma service permission to access Amazon S3?
A. administrative Password
B. AWS account ID
C. secret access key
D. access key ID
Answer: D (LEAVE A REPLY)

NEW QUESTION: 22

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

NEW QUESTION: 23
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: (SHOW ANSWER)
For the User-ID Agent to perform WMI (Windows Management Instrumentation) Authentication on a Windows Server, the following domain permissions are required:
* Domain Administrators: This group has the highest level of privileges in the domain and can perform any action within the Active Directory domain.
* Distributed COM Users: This group allows members to launch, activate, and use Distributed COM objects on the server.
* Event Log Readers: This group provides read access to the event logs, which is crucial for the User-ID Agent to collect security events necessary for user identification (Palo Alto Networks) (Palo Alto Networks).

NEW QUESTION: 24

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

NEW QUESTION: 25
Which two components must to be configured within User-ID on a new firewall that has been implemented? (Choose two.)
A. Group Mapping
B. 802.1X Authentication
C. Proxy Authentication
D. User mapping
Answer: A,D (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/enable-user-id

NEW QUESTION: 26
Which decryption requirement ensures that inspection can be provided to all inbound traffic routed to internal application and database servers?
A. Configuration of an SSL Inbound Decryption policy without installing certificates
B. Installation of certificates from the application server and database server on the NGFW and configuration of an SSL Inbound Decryption policy
C. Installation of a trusted root CA certificate on the NGFW and configuration of an SSL Inbound Decryption policy
D. Configuration of an SSL Inbound Decryption policy using one of the built-in certificates included in the certificate store
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
What are five benefits of Palo Alto Networks NGFWs (Next Generation Firewalls)? (Select the five correct answers.)
A. Convenient configuration Wizard
B. Seemless integration with the Threat Intelligence Cloud
C. Easy-to-use GUI which is the same on all models
D. Predictable throughput

E. Identical security subscriptions on all models
F. Comprehensive security platform designed to scale functionality over time
Answer: B,C,D,E,F (LEAVE A REPLY)

NEW QUESTION: 28
Which two features are found in a Palo Alto Networks NGFW but are absent in a legacy firewall product? (Choose two.)
A. Policy match is based on application
B. Identification of application is possible on any port
C. Traffic control is based on IP port, and protocol
D. Traffic is separated by zones
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 29
Which three actions should be taken before deploying a firewall evaluation unit in the customer's environment? (Choose three.)
A. Upgrade the evaluation unit to the most current recommended firmware, unless a demo of the upgrade process is planned.
B. Reset the evaluation unit to factory default to ensure that data from any previous customer evaluation is removed.
C. Inform the customer that they will need to provide a SPAN port for the evaluation unit assuming a TAP mode deployment.
D. Request that the customs make port 3978 available to allow the evaluation unit to communicate with Panorama.
E. Set expectations around which information will be presented in the Security Lifecycle Review because sensitive information may be made visible.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 30
Which two products can send logs to the Cortex Data Lake? (Choose two.)
A. Prisma Access
B. AutoFocus
C. PA-3260 firewall
D. Prisma Public Cloud
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 31
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 (LEAVE A REPLY)
When calculating log sizing for the Cortex Data Lake on the NGFW, the average log size used is 1500 bytes.
This size helps in estimating storage requirements and planning for log retention policies efficiently, ensuring that there is adequate storage capacity to handle the volume of logs generated by the network firewalls (Palo Alto Networks) (Palo Alto Networks).

NEW QUESTION: 32
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. Monthly
B. Weekly
C. Daily
D. Bi-weekly
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 33
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: B,C (LEAVE A REPLY)
When configuring the NGFW to act as a decryption broker for multiple transparent bridge security chains, the following items are required:
* A unique Transparent Bridge Decryption Forwarding Profile to a single Decryption policy rule (B):

Each decryption policy rule must be associated with a unique Transparent Bridge Decryption Forwarding Profile. This ensures that decrypted traffic is forwarded appropriately to the specific security chain.
* A unique Decryption policy rule is required per security chain (C): You need to create a separate decryption policy rule for each security chain. This allows you to distribute the decrypted traffic among multiple security chains based on policy criteria.
These configurations enable the firewall to effectively manage and distribute the load across multiple security chains, ensuring optimal performance and security (Palo Alto Networks) (Palo Alto Networks)

NEW QUESTION: 34
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 does not consider port information, instead relying on App-ID signatures that do not reference ports.
B. Palo Alto Networks NGFW protects all applications on all ports while leaving all ports opened by default.
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 keep ports closed by default, only opening ports after understanding the application request, and then opening only the application-specified ports.
Answer: (SHOW ANSWER)

NEW QUESTION: 35
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: B,D,G (LEAVE A REPLY)
Explanation
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/user-id-concepts/user-mapping

NEW QUESTION: 36

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

A. Multi-factor authentication (MFA)

B. Dynamic user groups (DUGs)

C. URL Filtering Profiles

D. WildFire analysis

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 37

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. a unique Decryption policy rule is required per security chain

B. a unique Transparent Bridge Decryption Forwarding Profile to a single Decryption policy rule

C. dedicated pair of decryption forwarding interfaces required per security chain

D. a single pair of decryption forwarding interfaces

Answer: (SHOW ANSWER)

NEW QUESTION: 38

What aspect of PAN-OS allows for the NGFW admin to create a policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility?

A. Remote Device UserID Agent

B. user-to-tag mapping

C. Dynamic User Groups

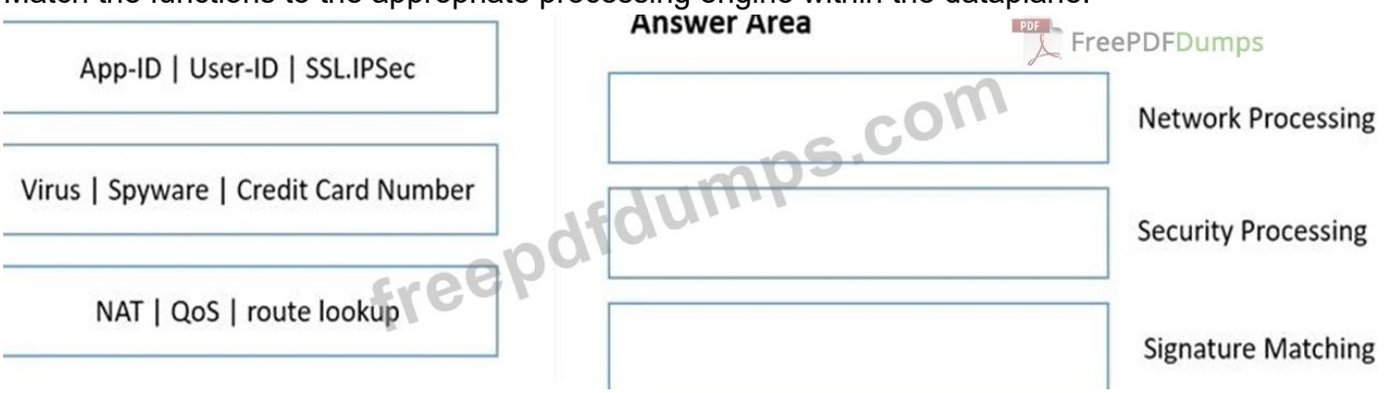
D. Dynamic Address Groups

Answer: (SHOW ANSWER)

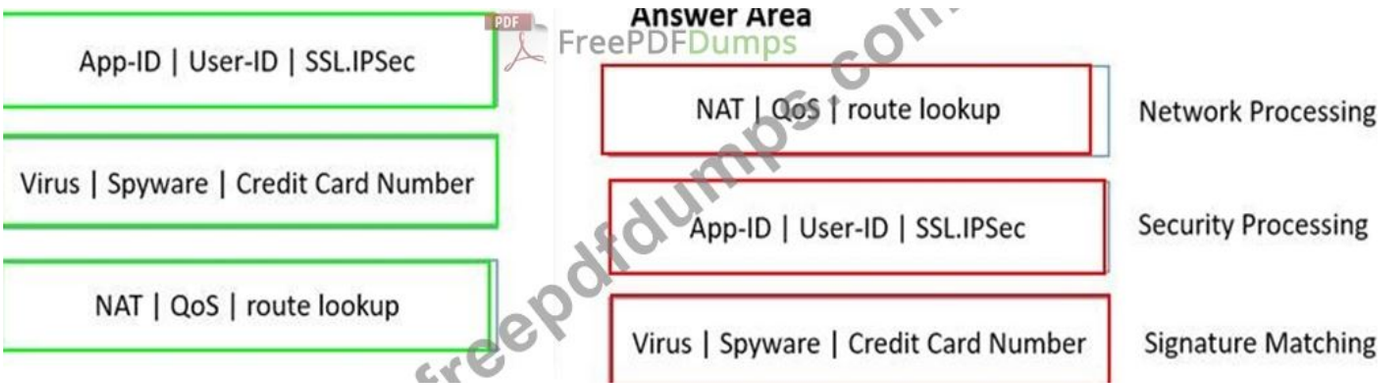
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups

NEW QUESTION: 39

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



Answer:



NEW QUESTION: 40
What component is needed if there is a large scale deployment of Next Generation Firewalls with multiple Panorama Management Servers?
A. M-600 Appliance
B. Panorama Large Scale VPN Plugin
C. Panorama Interconnect Plugin
D. Palo Alto Networks Cluster License
Answer: C (LEAVE A REPLY)
https://savantsolutions.net/wp-content/uploads/woocommerce_uploads/2019/05/pcnse-study-guide-v9.pdf (27)

NEW QUESTION: 41
How does SSL Forward Proxy decryption work?
A. The firewall resides between the internal client and internal server to intercept traffic between the two.
B. The SSL Forward Proxy Firewall creates a certificate intended for the client that is intercepted and altered by the firewall.
C. SSL Forward Proxy decryption policy decrypts and inspects SSL/TLS traffic from internal users to the web.
D. If the server's certificate is signed by a CA that the firewall does not trust, the firewall will use the certificate only on Forward Trust.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
What are three valid sources that are supported for user IP address mapping in Palo Alto Networks NGFW? (Choose three.)
A. Client Probing
B. RADIUS
C. Active Directory monitoring
D. Lotus Domino
E. eDirectory monitoring
F. TACACS

Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 43
Which three items contain information about Command-and-Control (C2) hosts? (Choose three.)
A. SaaS reports
B. Data filtering logs
C. WildFire analysis reports
D. Threat logs
E. Botnet reports
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 44
Which two actions can be configured in an Anti-Spyware profile to address command-and-control (C2) traffic from compromised hosts? (Choose two.)
A. Alert
B. Quarantine
C. Redirect
D. Reset
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 45
Which two tabs in Panorama can be used to identify templates to define a common base configuration? (Choose two)
A. Monitor Tab
B. Network Tab
C. Device Tab
D. Objects Tab
E. Policies Tab
Answer: B,C (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-web-interface/ panorama-templates/template-stacks

NEW QUESTION: 46
What is used to choose the best path on a virtual router that has two or more different routes to the same destination?
A. Path monitoring
B. Administrative distance
C. Metric
D. Source zone
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
Which Palo Alto Networks security platform component should an administrator use to extend policies to remote users are not connecting to the internet from behind a firewall?
A. Threat Intelligence Cloud
B. GlobalProtect
C. Traps
D. Aperture
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Palo Alto Networks publishes updated Command and Control signatures.
How frequently should the related signatures schedule be set?
A. Once an hour
B. Once a day
C. Once a week
D. Once every minute
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
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: (SHOW ANSWER)
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/prevent-credential-phishing.html

NEW QUESTION: 50

The Palo Ao Networks Cloud Identity Engino (CIE) includes which service that supports identity Providers (ldP)?
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 (LEAVE A REPLY)
The Palo Alto Networks Cloud Identity Engine (CIE) includes services such as Directory Sync and Cloud Authentication Service. These services support identity providers (IdP) using standards like SAML 2.0 and OAuth2. Directory Sync ensures that user and group information from on-premises directories are available in the cloud, while Cloud Authentication Service facilitates secure authentication and single sign-on (SSO) for users.

NEW QUESTION: 51
Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)
A. Verify AutoFocus is enabled below Device Management tab.
B. Check for WildFire forwarding logs.
C. Check the license
D. Verify AutoFocus status using CLI.
E. Check the WebUI Dashboard AutoFocus widget.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 52
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: (SHOW ANSWER)
Dynamic User Groups (DUGs) is a built-in feature of PAN-OS that allows NGFW administrators to create policies that provide auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. DUGs dynamically update group membership based on user attributes and behavior, enabling real-time policy enforcement and automatic response to security incidents.

NEW QUESTION: 53
What is the basis for purchasing Cortex XDR licensing?
A. volume of logs being processed based on Datalake purchased
B. unlimited licenses

C. number of NGFWs
D. number of nodes and endpoints providing logs
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
What two advantages of the DNS Sinkholing feature? (Choose two)
A. It can be deployed independently of an Anti-Spyware Profile.
B. It is monitoring DNS requests passively for malware domains.
C. It can work upstream from the internal DNS server.
D. It is forging DNS replies to known malicious domains.
Answer: C,D (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/threat-prevention/dns-sinkholing

NEW QUESTION: 55
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. Gain visibility of and control over applications and functionality in the traffic flow using a port and protocol firewall
B. Validate user identities through authentication
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: B,C (LEAVE A REPLY)

NEW QUESTION: 56
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: C,D (LEAVE A REPLY)
Deploying Panorama in a High Availability (HA) configuration provides significant advantages, especially for maintaining the management layer and ensuring robust log collection. Here are the key reasons:
* Ensure Management Continuity: By deploying a second Panorama appliance in an HA setup, you can ensure continuous management of your firewall environment. In the event that the

primary Panorama appliance fails, the secondary appliance can take over, ensuring that there is no interruption in management capabilities. This is crucial for maintaining operational stability and uninterrupted administrative functions (Palo Alto Networks) (Palo Alto Networks).
* Improve Log Collection Redundancy: An HA setup improves the redundancy and reliability of log collection. If the primary Panorama appliance that is collecting logs from various firewalls becomes unavailable, the secondary appliance can continue the log collection process. This ensures that all security events and network activities are recorded without gaps, which is essential for effective monitoring and incident response (Palo Alto Networks) (Palo Alto Networks Knowledge Base).

NEW QUESTION: 57
A potential customer requires an NGFW solution that enables high-throughput, low-latency network security and also inspects the application.
Which aspect of the Palo Alto Networks NGFW capabilities should be highlighted to help address these requirements?
A. GlobalProtect
B. threat prevention
C. Elastic Load Balancing (ELB)
D. single-pass architecture (SPA)
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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 ml cloud-status
B. show mlav cloud-status
C. show wfml cloud-status
D. show av cloud-status
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which two new file types are supported on the WF-500 in PAN-OS 9? (Choose two)
A. RAR
B. Zip
C. ELF
D. 7-Zip
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 60

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

NEW QUESTION: 61
What are two core values of the Palo Alto Network Security Operating Platform? (Choose two.}
A. safe enablement of all applications
B. prevention of cyber attacks
C. threat remediation
D. defense against threats with static security solution
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 62
Which proprietary technology solutions will allow a customer to identify and control traffic sources regardless of internet protocol (IP) address or network segment?
A. Source-D and Network.ID
B. User-ID and Source-ID
C. Source ID and Device-ID
D. User ID and Device-ID
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which Security profile on the Next-Generation Firewall (NGFW) includes Signatures to protect against brute force attacks?
A. Antivirus profile
B. Vulnerability Protection profile

C. URL Filtering profile
D. Anti-Spyware profile
Answer: (SHOW ANSWER)

NEW QUESTION: 64
Which three considerations should be made prior to installing a decryption policy on the NGFW? (Choose three.)
A. Inability to access websites
B. Exclude certain types of traffic in decryption policy
C. Include all traffic types in decryption policy
D. Deploy decryption setting all at one time
E. Ensure throughput is not an issue
Answer: (SHOW ANSWER)

NEW QUESTION: 65
A customer requires protections and verdicts for PE (portable executable) and ELF (executable and linkable format) as well as integration with products and services can also access the immediate verdicts to coordinate enforcement to prevent successful attacks.
What competitive feature does Palo Alto Networks provide that will address this requirement?
A. File Blocking Profile
B. Dynamic Unpacking
C. WildFire
D. DNS Security
Answer: C (LEAVE A REPLY)
https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/real-time-wildfire-verdicts-and-signatures-for-pe-and-elf-files.html

NEW QUESTION: 66
In an HA pair running Active/Passive mode, over which interface do the dataplanes communicate?
A. HA3
B. HA1
C. HA2
D. HA4
Answer: A (LEAVE A REPLY)
In an HA (High Availability) pair running in Active/Passive mode, the dataplanes communicate over the HA3 interface. This interface is used for the synchronization of session information and other runtime data between the active and passive firewalls, ensuring stateful failover and seamless transition in case of a failure.

NEW QUESTION: 67

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

A. Virtual wire

B. active / active high availability (HA)

C. virtual systems

D. Layer 2 interfaces

Answer: A (LEAVE A REPLY)

NEW QUESTION: 68

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

A. NGFW discard a response from the DNS server.

B. NGFW temporarily disable DNS Security function.

C. NGFW permit a response from the DNS server.

D. NGFW resend a verdict challenge to DNS service cloud.

Answer: (SHOW ANSWER)

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security

NEW QUESTION: 69

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

A. maximum number of files per day

B. maximum number of files per minute

C. based on the purchased license uploaded

D. QoS tagging

Answer: (SHOW ANSWER)

NEW QUESTION: 70

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 (LEAVE A REPLY)

WildFire, a cloud-based threat analysis service from Palo Alto Networks, is capable of detecting zero-day malware across several types of traffic, including SMTP, HTTPS, and FTP. By analyzing files transmitted over these protocols, WildFire can identify malicious activities that traditional security measures might miss.

SMTP (Simple Mail Transfer Protocol) is used for email transmission, HTTPS (HyperText Transfer Protocol Secure) secures web traffic, and FTP (File Transfer Protocol) is used for file

transfers. These protocols are commonly exploited by attackers to distribute malware, making WildFire's ability to monitor and analyze them critical for comprehensive network security.

NEW QUESTION: 71
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,D (LEAVE A REPLY)
WildFire, a cloud-based malware analysis service provided by Palo Alto Networks, supports the analysis of various file types to detect malicious content. Specifically, it supports:
B: 7-Zip: WildFire can analyze compressed files in the 7-Zip format, which is commonly used to distribute malware in compressed archives.
C: Flash: Analysis of Flash files helps in detecting malware that can be embedded in Flash content, which has historically been a common vector for exploits.
D: RPM: WildFire supports the analysis of RPM packages, which are used in various Linux distributions and can be used to distribute malicious software.

NEW QUESTION: 72
Which two statements correctly describe what a Network Packet Broker does for a Palo Alto Networks NGFW? (Choose two.)
A. It provides a third-party SSL decryption option, which can increase the total number of third-party devices performing analysis and enforcement.
B. It allows SSL decryption to be offloaded to the NGFW and traffic to be decrypted multiple times.
C. It allows SSL decryption to be offloaded to the NGFW and traffic to be decrypted only once.
D. It eliminates the need for a third-party SSL decryption option, which reduces the total number of third-party devices performing decryption.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 73
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. An App-ID security policy rule to block traffic sourcing from the untrust zone
C. Security profiles to security policy rules for traffic sourcing from the untrust zone
D. Zone protection profile on the zone of the ingress interface
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which two methods are used to check for Corporate Credential Submissions? (Choose two.)
A. doman credentialiter
B. IP user mapping
C. User-ID credential check
D. LDAP query
Answer: (SHOW ANSWER)

NEW QUESTION: 75
Which three script types can be analyzed in WildFire? (Choose three)
A. JScript
B. PythonScript
C. PowerShell Script
D. MonoSenpt
E. VBScript
Answer: A,B,E (LEAVE A REPLY)

NEW QUESTION: 76
Palo Alto Networks publishes updated Command-and-Control signatures. How frequently should the related signatures schedule be set?
A. Once a week
B. Once a day
C. Once an hour
D. Once every minute
Answer: (SHOW ANSWER)

NEW QUESTION: 77
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. Enable WMI probing in high security networks

E. User-ID can support a maximum of 15 hops

Answer: (SHOW ANSWER)

NEW QUESTION: 78

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>
```

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 79

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. 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

C. It represents the remediation server that the client should visit for patching

D. It will take over as the new DNS resolver for that client and prevent further DNS requests from occurring in the meantime

Answer: (SHOW ANSWER)

NEW QUESTION: 80

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

A. VBScript

B. JScript

C. MonoScript

D. PythonScript

E. PowerShell Script

Answer: A,B,E (LEAVE A REPLY)

WildFire, Palo Alto Networks' advanced threat analysis service, has expanded its capabilities to analyze the following new script types:

* VBScript: A scripting language commonly used in Windows environments for automation and administrative tasks, which can be exploited for malicious purposes.

* JScript: A Microsoft implementation of JavaScript, used in various applications and often targeted by attackers for script-based exploits.
* PowerShell Script: A powerful scripting language used for task automation and configuration management in Windows, which has become a common target for advanced attacks due to its capabilities.
By analyzing these script types, WildFire enhances its ability to detect and prevent sophisticated attacks that leverage scripting languages.
References:
* Palo Alto Networks WildFire Datasheet
* Palo Alto Networks WildFire Administration Guide

NEW QUESTION: 81
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 (LEAVE A REPLY)
https://docs.paloaltonetworks.com/vm-series/8-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series-firewall-on-aws/configure-activepassive-ha-on-aws.html

NEW QUESTION: 82
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: A,C (LEAVE A REPLY)
In a Palo Alto Networks firewall, when configuring User-ID, there are two essential components that must be configured: User Mapping and Group Mapping.
* User Mapping involves identifying users by their usernames, which helps in associating network traffic with user activity. This is critical for applying user-specific policies and monitoring user activities.
* Group Mapping involves associating users with their respective groups, typically pulled from a directory
* service like LDAP. This allows the firewall to apply policies based on group membership, making it easier to manage policies for large numbers of users.

These components enable the firewall to enforce security policies based on user identity and group membership, enhancing overall network security by ensuring that policies are applied accurately.

NEW QUESTION: 83
How often are the databases for Anti-virus. Application, Threats, and WildFire subscription updated?
A. Anti-virus (daily), Application (weekly), Threats (daily), WildFire (5 minutes)
B. Anti-virus (weekly), Application (daily), Threats (daily), WildFire (5 minutes)
C. Anti-virus (weekly): Application (daily). Threats (weekly), WildFire (5 minutes)
D. Anti-virus (daily), Application (weekly), Threats (weekly), WildFire (5 minutes)
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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 slow path for further inspection. If subject to content inspection, it will pass through a single stream-based content inspection engines before egress
B. 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.
C. 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
D. 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
Answer: (SHOW ANSWER)

NEW QUESTION: 85
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 (LEAVE A REPLY)
When beginning to understand the Zero Trust protect surface using the Palo Alto Networks Zero Trust reference architecture, the following two steps are crucial:

* Validate User Identities through Authentication (A): This step involves ensuring that all users are authenticated properly. By verifying the identities of users attempting to access the network, organizations can ensure that only authorized users can access sensitive resources. This is a fundamental principle of Zero Trust, which operates on the premise of "never trust, always verify."
* Categorize Data and Applications by Levels of Sensitivity (C): This involves identifying and classifying data and applications based on their sensitivity and importance to the organization. By understanding what needs to be protected and the level of sensitivity, security policies can be tailored to provide appropriate levels of protection. This helps in prioritizing security measures based on the criticality of the data and applications.
References:
* Palo Alto Networks, Zero Trust Architecture Documentation.
* NIST Zero Trust Architecture (NIST SP 800-207).

NEW QUESTION: 86
A large number of next-generation firewalls (NGFWs), along with Panorama and WildFire have been positioned for a prospective customer. The customer is concerned about storing retrieving and archiving firewall logs and has indicated that logs must be retained for a minimum of 60 days. An additional requirement is ingestion of a maximum of 10,000 logs per second.
What will best meet the customer's logging requirements?
A. Appropriate Data Lake storage determined by using the Data Lake Calculator
B. NGFWs that have at least 10TB of internal storage
C. Appropriately sized NGFW based on use of the POPSICLE tool
D. A pair of fully populated M-300 storage appliances
Answer: A (LEAVE A REPLY)

NEW QUESTION: 87
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. Custom App-ID rules
B. Content Filtering
C. App-ID
D. WildFire
Answer: D (LEAVE A REPLY)

NEW QUESTION: 88
Which license is required to receive weekly dynamic updates to the correlation objects on the firewall and Panorama?
A. Threat Prevention on the firewall, and Support on Panorama
B. GlobalProtect on the firewall, and Threat Prevention on Panorama

C. WildFire on the firewall, and AutoFocus on Panorama
D. URL Filtering on the firewall, and MindMeld on Panorama
Answer: (SHOW ANSWER)

NEW QUESTION: 89
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: (SHOW ANSWER)
Palo Alto Networks Single Pass Parallel Processing (SP3) architecture is designed to handle traffic efficiently and securely. The key aspect of SP3 is:
Single Pass Processing (C): This means that all traffic is processed in a single pass through the firewall, regardless of the number of security features enabled. There is no additional performance impact for each feature because the firewall processes all security functions (such as threat prevention, URL filtering, and application control) simultaneously in a single pass. This architecture ensures high performance and low latency while maintaining robust security.
References:
* Palo Alto Networks, Single Pass Parallel Processing (SP3) Whitepaper.
* Palo Alto Networks, Firewall Performance and Architecture Documentation.

NEW QUESTION: 90
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 in released
B. Utilize dynamic updates with an aggressive update schedule
C. Store updates on an intermediary server and point all the firewalls to it
D. Monitor update announcements and manually push updates to firewalls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 91
Which two designs require virtual systems? (Choose two.)
A. A virtual router as a replacement for an internet-facing router
B. A VMware NSX deployment that needs micros segmentation
C. A single physical firewall shared by different organizations, each with unique traffic control needs
D. A shared gateway interface that does not need a full administrative boundary

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 92
How do Highly Suspicious artifacts in-AutoFocus help identify when an unknown, potential zero-day, targeted attack occur to allow one to adjust the security posture?
A. Highly Suspicious artifacts have been seen infecting a broad, significant range of companies.
B. Highly Suspicious artifacts are High Risk artifacts that have been seen in very few samples.
C. Highly Suspicious artifacts are associated with High-Risk payloads that are inflicting massive amounts of damage to end customers.
D. All High Risk artifacts are automatically classified as Highly Suspicious.
Answer: (SHOW ANSWER)

NEW QUESTION: 93
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. Device count is under 100
C. Appliance needs to be moved into data center
D. Logs per second exceed 10,000
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 94
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: (SHOW ANSWER)
To avoid split-brain scenarios in an active/passive high availability (HA) pair deployment, it is essential to ensure reliable communication between the HA peers. Using the management interface as the HA1 backup link provides an additional communication path between the

firewalls, ensuring they can synchronize state information and avoid scenarios where both units assume the active role due to a communication failure.

NEW QUESTION: 95
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,B (LEAVE A REPLY)
Decryption Broker on a Next-Generation Firewall (NGFW) provides two primary benefits:
* Offloading SSL decryption: The NGFW decrypts traffic once and then forwards it to multiple security devices for inspection, avoiding the need to decrypt and re-encrypt traffic multiple times, thus
* improving efficiency.
* Reducing third-party devices: By handling SSL decryption within the NGFW, the need for separate, dedicated SSL decryption devices is eliminated, reducing the complexity and number of devices required for network security.
These features streamline traffic analysis and enforcement while maintaining robust security.
References: Palo Alto Networks Decryption Broker documentation.

NEW QUESTION: 96
Palo Alto Networks maintains a dynamic database of malicious domains. Which two Security Platform components use this database to prevent threats? (Choose two)
A. DNS-based command-and-control signatures
B. BrightCloud Url Filtering
C. PAN-DB URL Filtering
D. Brute-force signatures
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 97
Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?
A. 5 minute WildFire updates to threat signatures
B. WildFire hybrid deployment
C. Access to the WildFire API
D. PE file upload to WildFire

Answer: D (LEAVE A REPLY)

NEW QUESTION: 98
The WildFire Inline Machine Learning is configured using which Content-ID profiles?
A. Antivirus Profile
B. WildFire Analysis Profile
C. Threat Prevention Profile
D. File Blocking Profile
Answer: A (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/wildfire-features/configure-wildfire-inline-ml.html

NEW QUESTION: 99
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,B,E (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security

NEW QUESTION: 100
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. DoS Protection Profile
B. Vulnerability Protection Profile
C. File Blocking Profile
D. URL Filtering Profile
Answer: (SHOW ANSWER)

NEW QUESTION: 101
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. Firewall Botnet Report
B. AutoFocus
C. Panorama Correlation Report
D. Traps TMS

Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
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 (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports

NEW QUESTION: 103
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 (LEAVE A REPLY)
Palo Alto Networks NGFW provides several mechanisms for user mapping, which helps in identifying and applying policies based on user identity rather than just IP addresses.
* Captive Portal: This method redirects users to a portal where they must authenticate before accessing the network. It captures user credentials and maps them to their IP addresses.
* Domain server monitoring: This involves monitoring Active Directory (AD) domain controllers to map users to their respective IP addresses based on login events.
* Client probing: This mechanism involves directly querying devices on the network to determine the logged-in user. It's useful for mapping IP addresses to usernames dynamically.

NEW QUESTION: 104
Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)
A. Reset
B. Quarantine
C. Drop
D. Allow
E. Redirect
F. Alert

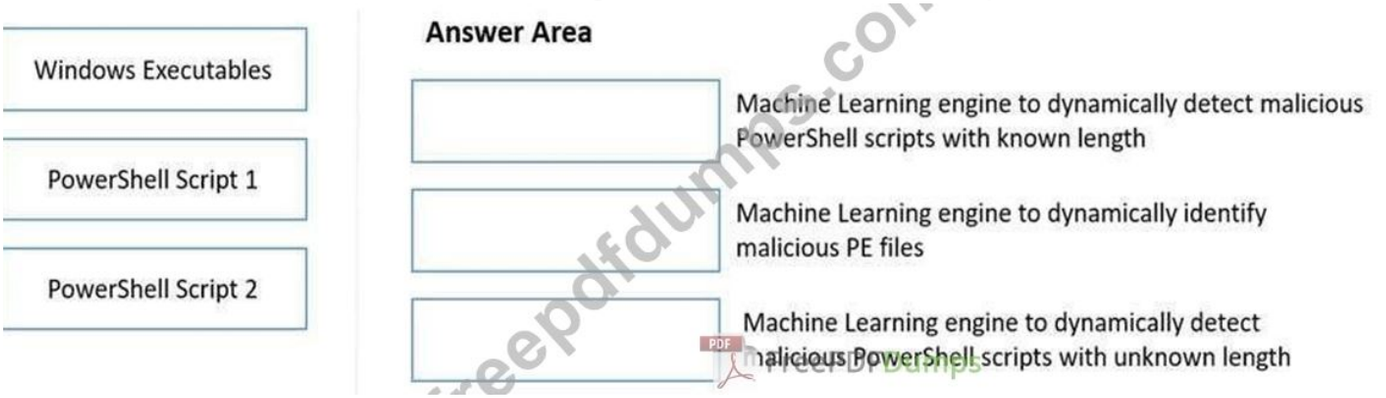
Answer: A,C,D,F (LEAVE A REPLY)
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

NEW QUESTION: 105
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 (LEAVE A REPLY)
The key benefit of Palo Alto Networks' Single Pass Parallel Processing (SP3) design is that it allows the addition of new functions to existing hardware without significant performance degradation. The SP3 architecture processes traffic in a single pass, applying all security functions (such as threat prevention, URL filtering, and application identification) simultaneously, which enhances performance and efficiency. This design ensures that the firewall can scale to meet increasing demands and integrate new security features as they are developed.
References: Palo Alto Networks SP3 architecture whitepaper.

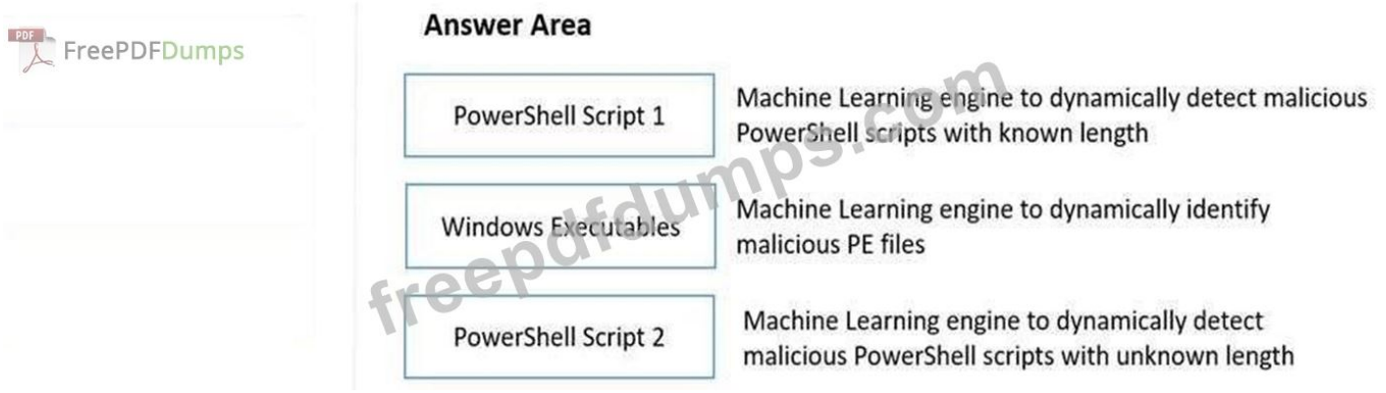
NEW QUESTION: 106
What two types of certificates are used to configure SSL Forward Proxy? (hoose two.)
A. Enterprise CA-signed certificates
B. Self-Signed certificates
C. Intermediate certificates
D. Private key certificates
Answer: (SHOW ANSWER)
To configure SSL Forward Proxy, two types of certificates can be used:
* Enterprise CA-signed certificates: These certificates are issued by a Certificate Authority (CA) within the organization, ensuring trust within the enterprise environment.
* Self-Signed certificates: These are generated and signed by the firewall itself. While easier to deploy, they may not be trusted by external clients unless explicitly added to their trust stores.
Both types of certificates allow the firewall to decrypt and inspect SSL/TLS traffic, ensuring that malicious traffic can be detected and blocked even when encrypted.
References: Palo Alto Networks SSL Decryption documentation.

NEW QUESTION: 107
What are three sources of malware sample data for the Threat Intelligence Cloud? (Choose three)
A. Correlation Objects generated by AutoFocus
B. Third-party data feeds such as partnership with ProofPomt and the Cyber Threat Alliance
C. Next-generation firewalls deployed with WildFire Analysis Security Profiles
D. Palo Alto Networks non-firewall products such as Traps and Prisma SaaS
E. WF-500 configured as private clouds for privacy concerns
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 108
Drag and Drop Question
Match the WildFire Inline Machine Learning Model to the correct description for that model.



Answer:



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

NEW QUESTION: 109

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. Monthly
B. Daily
C. Weekly
D. Bi-weekly
Answer: (SHOW ANSWER)

NEW QUESTION: 110
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: (SHOW ANSWER)
The Eval Systems, Security Lifecycle Reviews, and Prevention Posture Assessment tools serve several purposes:
* When you're delivering a security strategy: These tools help in presenting a comprehensive security strategy to clients by highlighting the effectiveness and benefits of using Palo Alto Networks' solutions.
* When clients want to see the power of the platform: They provide an opportunity for clients to witness the capabilities and impact of the Palo Alto Networks platform in real-world scenarios.
* Assess the state of NGFW feature adoption: These tools help in evaluating how well the Next-Generation Firewall features have been adopted and utilized within the client's network, identifying areas for improvement and optimization.
References:
* Palo Alto Networks Security Lifecycle Review Guide
* Palo Alto Networks Prevention Posture Assessment Documentation

NEW QUESTION: 111
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: (SHOW ANSWER)

When sizing the Cortex Data Lake for Traps Management Service, two key factors must be considered:
* Retention Requirements: It is essential to determine how long the logs and data need to be retained in the Cortex Data Lake. This affects the overall storage capacity required, as longer retention periods will necessitate more storage space (Palo Alto Networks) (Palo Alto Networks).
* The Number of Traps Agents: The total number of Traps agents deployed will directly impact the volume of data being generated and sent to the Cortex Data Lake. More agents mean more data, which in turn requires a larger data lake capacity to handle the increased load (Palo Alto Networks) (Palo Alto Networks).

NEW QUESTION: 112
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: (SHOW ANSWER)
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html

NEW QUESTION: 113
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. SIA (Scan It All) Processing Engine
B. Stream-based Signature Engine
C. First Packet Processor
D. Security Processing Engine
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114

Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)
A. Alert
B. Redirect
C. Drop
D. Allow
E. Reset
F. Quarantine
Answer: (SHOW ANSWER)

NEW QUESTION: 115
When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?
A. HTTP method
B. HTTP response status code
C. X-Forwarded-For
D. Content type
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which two features are found in a Palo Alto Networks NGFW but are absent in a legacy firewall product?
(Choose two.)
A. Identification of application is possible on any port
B. Policy match is based on application
C. Traffic is separated by zones
D. Traffic control is based on IP port, and protocol
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?
A. PE file upload to WildFire
B. 5 minute WildFire updates to threat signatures
C. WildFire hybrid deployment
D. Access to the WildFire API
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
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 (LEAVE A REPLY)
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/migrate-your-cortex-xdr-license

NEW QUESTION: 119
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. There will be a popup to ask if the Master Key from the Panorama should replace the Master Key from the managed firewalls
C. The Master Key from the managed firewalls will be overwritten with the Master Key from Panorama
D. Provided there's no error within the configuration to be pushed, the push will succeed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
When having a customer pre-sales call, which aspects of the NGFW should be covered?
A. 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
B. 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
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. 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
Answer: B (LEAVE A REPLY)

NEW QUESTION: 121
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: (SHOW ANSWER)
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-web-interface/panorama-templates/template-stacks

NEW QUESTION: 122
Which variable is used to regulate the rate of file submission to WildFire?
A. Based on the purchase license
B. Maximum number of files per minute
C. Available bandwidth
D. Maximum number of files per day
Answer: B (LEAVE A REPLY)
https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/submit-files-for-wildfire-analysis/ firewall-file-forwarding-capacity-by-model

NEW QUESTION: 123
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: A,B,C (LEAVE A REPLY)
The following platform components can identify and protect against malicious email links:

* WildFire hybrid cloud solution (A): This solution integrates on-premises and cloud-based threat intelligence to detect and prevent malware, including malicious email links.
* WildFire public cloud (B): This component leverages the power of the cloud to provide real-time updates and protection against the latest threats, including those found in email links.
* WF-500 (C): This appliance is designed to analyze files and links to detect malware and prevent it from spreading within the network.
These components work together to provide comprehensive protection against email-based threats, ensuring that organizations can identify and block malicious links before they cause harm.

NEW QUESTION: 124
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 (LEAVE A REPLY)
Explanation
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-task

NEW QUESTION: 125
What two types of certificates are used to configure SSL Forward Proxy? (hoose two.)
A. Intermediate certificates
B. Self-Signed certificates
C. Private key certificates
D. Enterprise CA-signed certificates
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 126

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: (SHOW ANSWER)

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