PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks System Engineer Professional - Strata

Palo Alto Networks PSE-Strata

Version Demo

Total Demo Questions: 18

Total Premium Questions: 181

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Discovery	52
Topic 2, Design	40
Topic 3, Demonstration	35
Topic 4, Proof of Concept	4
Topic 5, Deployment	50
Total	181

QUESTION NO: 1

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: B

Explanation:

PPA is the correct pre-sales engagement because it is a structured, interview-led assessment of a customer's current cybersecurity posture. The approximately four-hour conversation is used to understand the customer's environment, security architecture, operational processes, existing controls, business priorities, and areas where risk or coverage gaps may exist. This discovery-led approach gives the account team a holistic view of the customer's security maturity and helps shape a relevant Palo Alto Networks platform recommendation and roadmap.

The output of a PPA is therefore based primarily on the information gathered from stakeholders during the assessment workshop. It is intended to connect the customer's current state and desired outcomes to a practical security strategy, rather than simply collecting a technical device configuration or a set of logs. Palo Alto Networks positions assessments and advisory engagements as a way to evaluate security needs, identify improvement opportunities, and plan appropriate services and technology adoption. See Palo Alto Networks' Services overview and Network Security overview for the company's assessment and security-platform context.

QUESTION NO: 2

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

Explanation:

X-Forwarded-For is an HTTP request-header value that can be captured when HTTP Header Logging is enabled in a URL Filtering profile. This header is commonly inserted by a proxy, reverse proxy, or load balancer to convey the original client IP address when the web server or firewall-facing connection originates from an intermediary. Capturing it in URL-related logging gives security teams additional context for investigating web activity, particularly in environments where clients traverse explicit proxies or application delivery infrastructure.

Palo Alto Networks URL Filtering profiles include the option to log HTTP headers associated with web requests. The resulting URL log information can include selected request-header values, including X-Forwarded-For, alongside other URL-filtering context such as the requested URL, category, action, source, and destination. This visibility is useful when correlating a web request observed by the firewall with the originating address reported by upstream HTTP infrastructure. For configuration and operational details, see the Palo Alto Networks URL Filtering documentation and the log field descriptions.

QUESTION NO: 3

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

Explanation:

The **Anti-Spyware profile** is used to apply Palo Alto Networks DNS Security protections to DNS traffic. DNS Security is configured through the profile's DNS Policies settings, where administrators define the action taken for domains assigned to DNS Security categories, such as malware, phishing, command-and-control, and newly registered domains. The service uses Palo Alto Networks cloud-based analysis and threat intelligence to identify malicious domains, including domains generated through domain generation algorithms (DGAs), even when those domains have not previously been observed in the local firewall environment. This cloud-delivered approach allows the firewall to receive timely DNS threat verdicts and enforce blocking or other configured actions during DNS resolution, helping prevent endpoints from connecting to attacker-controlled infrastructure. The profile can be attached to a Security policy rule so that DNS queries matching the rule are inspected and handled according to the configured DNS policy actions. Palo Alto Networks specifically documents DNS Security configuration under Anti-Spyware profiles and describes DGA detection as a DNS Security capability. See the Palo Alto Networks DNS Security configuration documentation and the Anti-Spyware profile documentation.

QUESTION NO: 4

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: C

Explanation:

1MB to 5 MB is a valid daily log-volume estimate per Prisma Access mobile user when sizing Cortex Data Lake capacity. Sizing must account for the amount of log data generated by user traffic and the security processing applied to that traffic, including traffic, threat, URL Filtering, and other enabled logging functions. Mobile-user log generation varies considerably with browsing habits, applications in use, traffic volume, policy configuration, and the logging level selected. Therefore, a range rather than one fixed number is appropriate during initial capacity planning.

Using 1 MB to 5 MB per user per day provides a practical baseline for estimating the total daily ingestion requirement: multiply the expected mobile-user population by an expected value in that range, then account for the required retention period and any additional Prisma Access locations, services, or log sources. The final entitlement and storage design should be validated against the organization's actual telemetry after deployment, because logging profiles and user behavior can materially change consumption. Palo Alto Networks describes Cortex Data Lake as the centralized logging platform for collecting and managing firewall and Prisma Access logs; see the Cortex Data Lake documentation and the Prisma Access documentation.

QUESTION NO: 5

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

Explanation:

A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation. Panorama establishes this baseline automatically from the device's recent health data rather than relying on a manually entered threshold. It uses the prior seven days of observed metric health to calculate an average and incorporates the standard deviation to account for normal variation in that metric's behavior. This statistical baseline gives Panorama a context-sensitive expectation for each monitored metric, so a device is identified as deviating when its current behavior differs materially from its own established normal pattern.

This approach is valuable because health values can vary naturally between devices, deployments, and time periods. Comparing a firewall against a baseline derived from its own historical data helps administrators focus on unusual operational conditions instead of treating every environmental difference as a problem. The Deviating Devices view therefore supports proactive investigation by surfacing devices whose metric values depart from the calculated health baseline. Palo Alto Networks documents the baseline calculation and the Deviating Devices health workflow in the Panorama Managed Devices Health documentation. Additional context on monitoring managed firewalls is available in the Panorama Device Health documentation.

QUESTION NO: 6

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: B C

Explanation:

For Traps Management Service, Cortex Data Lake sizing must account for **the number of Traps agents** and **Traps agent forensic data**. Each managed endpoint generates telemetry and event information, so the agent count is a primary indicator of the total service scale and expected ingestion volume. The endpoint population also determines the potential volume of endpoint data that the management service must process and retain.

Forensic data is a separate sizing consideration because endpoint investigations can collect substantially more detailed evidence than routine alert metadata. This evidence can include files and associated endpoint artifacts gathered to support analysis of a security event. Organizations that enable or expect frequent forensic-data collection need sufficient Cortex Data Lake capacity for this workload in addition to the baseline endpoint-management activity. Palo Alto Networks describes Cortex Data Lake as the cloud logging and data-storage platform used by its security services, while Cortex endpoint documentation describes the collection and use of endpoint data for investigation and response. See the Cortex Data Lake documentation and the Cortex XDR documentation.

QUESTION NO: 7

Which statement is true about Post Rules configured in a Panorama device group?

A. Post Rules are evaluated after locally defined firewall policy rules

B. Post Rules are evaluated before Pre Rules

C. Post Rules can be edited locally on each managed firewall

D. Post Rules are evaluated only when no Security policy rule matches traffic

ANSWER: A

Explanation:

Post Rules are evaluated after locally defined Security policy rules on the managed firewall. Panorama uses Pre Rules to enforce centrally managed policy before firewall-local rules, while Post Rules provide centrally managed policy that is evaluated after local rules. This allows an organization to apply a baseline block or cleanup policy without preventing authorized local exceptions that are evaluated earlier.

Both Pre Rules and Post Rules are centrally managed from Panorama and are pushed to the managed firewalls. The firewall administrator can view these rules but cannot edit them locally. See the Panorama device groups documentation.

QUESTION NO: 8

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

Explanation:

WildFire is the Palo Alto Networks threat-analysis service that addresses this requirement. WildFire analyzes potentially malicious files, including Windows PE and Linux ELF executables, and returns malware verdicts that can be used to drive prevention controls. Its cloud-delivered analysis and intelligence pipeline enables protections to be generated and distributed quickly when a file is identified as malicious.

A key capability for this use case is Real-Time WildFire, which provides immediate verdicts and signatures for PE and ELF files. These verdicts can be consumed by integrated Palo Alto Networks products and services so they can coordinate enforcement actions, such as blocking known malicious files and preventing subsequent attack stages. This reduces the opportunity for adversaries to successfully deliver or execute malware across endpoints, networks, and cloud-connected environments.

Palo Alto Networks documents the availability of real-time verdicts and signatures for PE and ELF files in its WildFire cloud features documentation: Real-Time WildFire Verdicts and Signatures for PE and ELF Files. Additional WildFire capabilities and workflow information are available in the WildFire documentation.

QUESTION NO: 9

Which three activities can the botnet report track? (Choose three.)

A. Accessing domains registered in the last 30 days

B. Visiting a malicious URL

C. Launching a P2P application

D. Detecting malware within a one-hour period

E. Initiating API calls to other applications

F. Using dynamic DNS domain providers

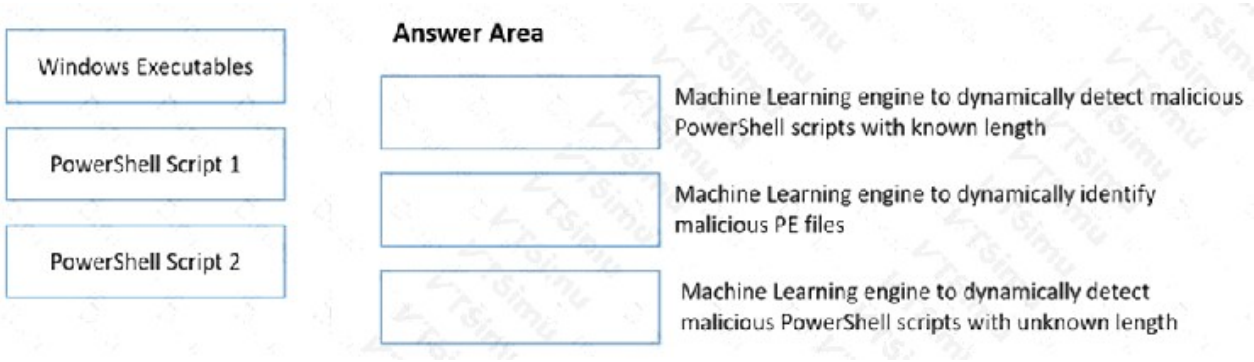
ANSWER: A C F

Explanation:

The Botnet report can track **Accessing domains registered in the last 30 days**, **Launching a P2P application**, and **Using dynamic DNS domain providers**. These behaviors are useful botnet indicators because attackers commonly use recently registered domains as short-lived infrastructure, dynamic DNS services to maintain changing command-and-control destinations, and peer-to-peer applications or protocols to distribute malware or support decentralized communications. The report correlates relevant firewall traffic and threat-intelligence-related activity so that an administrator can identify internal hosts exhibiting these potentially suspicious patterns and investigate them further. Recently registered domain access is especially valuable because newly created domains have little established reputation and can be rapidly rotated by attackers. Dynamic DNS activity can similarly reveal connections that evade reliance on fixed IP addresses. Peer-to-peer activity provides another behavioral signal that can help locate hosts requiring validation, particularly where that traffic is unexpected for the user, endpoint, or network segment. Palo Alto Networks describes Botnet reporting and its use of these indicators in its Controlling Botnets guide. Related reporting and monitoring capabilities are documented in the PAN-OS Reports documentation.

QUESTION NO: 10 - (SIMULATION)

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



ANSWER: See the explanation for the answer

Explanation:

Match the models as follows:

QUESTION NO: 11

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: A C

Explanation:

Templates in Panorama provide a reusable mechanism for defining common device and network configuration settings and then pushing those settings to multiple managed firewalls. The **Network Tab** is correct because a template includes the shared networking configuration required by firewalls, such as interfaces, zones, virtual routers, routing configuration, and related network settings. This allows firewalls with comparable connectivity designs to inherit a consistent network baseline.

The **Device Tab** is also correct because templates centrally define shared device-level settings, including system configuration, administrator-related settings, server profiles, setup and operational settings, and logging-related configuration. Panorama documentation describes templates as the method for configuring the settings available in the Device and Network tabs for one or more firewalls. Administrators can use template stacks where necessary, allowing a common base template to be combined with templates containing location- or role-specific settings. This layered approach supports consistent configuration while retaining the flexibility required for groups of firewalls with different operational needs. See the Palo Alto Networks Templates and Template Stacks documentation and the template configuration guidance.

QUESTION NO: 12

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

Explanation:

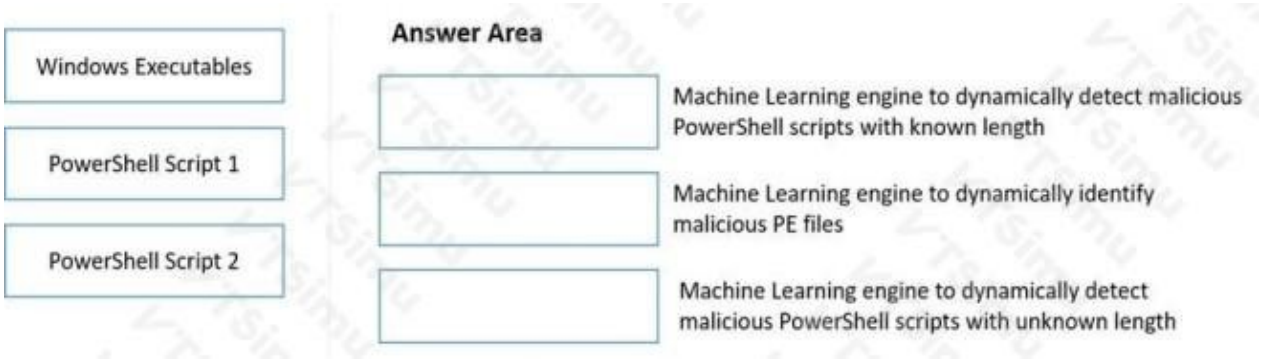
The Palo Alto Networks platform approach is designed to consolidate security capabilities around a common platform, with integrated prevention, centralized visibility, and automation rather than disconnected point products. Therefore, *operational efficiencies due to reduction in manual incident review and decrease in mean time to resolution (MTTR)* is a key benefit: correlated telemetry and automated workflows help security teams investigate and respond with less manual effort. *Increased security due to scalable cloud delivered security Services (CDSS)* is also a core benefit because cloud-delivered services continuously provide protections such as threat prevention, DNS Security, URL Filtering, and WildFire analysis across supported enforcement points. Finally, *Cost savings due to reduction in IT management effort and device* reflects the platform value of simplifying operations and reducing the management burden associated with maintaining numerous separate security tools and appliances. Palo Alto Networks describes its platform strategy as using tightly integrated products and services to improve prevention and operational outcomes, while its cloud-delivered security services extend consistent, scalable protections. See the Cloud-Delivered Security Services overview and the Palo Alto Networks cybersecurity platform overview.

QUESTION NO: 13 - (DRAG DROP)

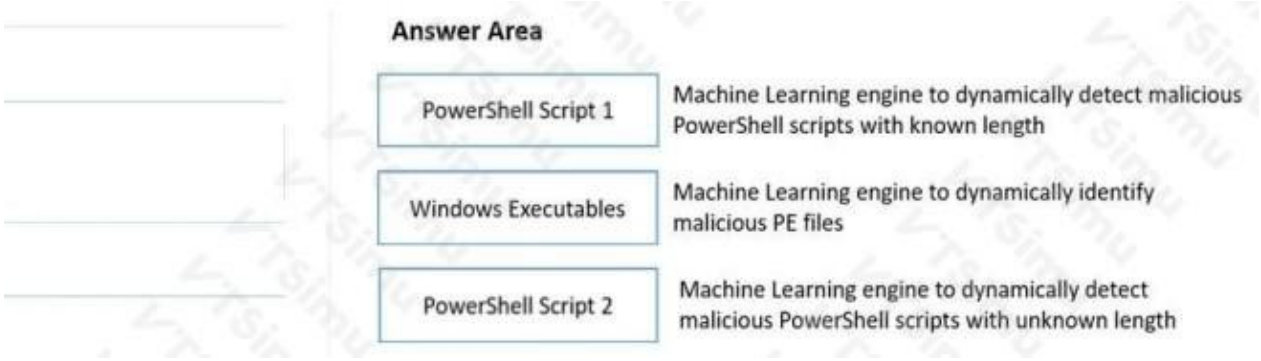
DRAG DROP

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

Select and Place:



ANSWER:



Explanation:

WildFire Inline Machine Learning uses distinct model types because executable files and PowerShell scripts have different structures and require different real-time inspection approaches. The Windows Executables model is designed for Portable Executable content, allowing the firewall to dynamically identify malicious PE files as they are evaluated inline. This gives the platform a way to recognize suspicious executable characteristics before relying only on a traditional signature-based verdict.

PowerShell script inspection is divided into two models based on whether the script has a known, fixed length or an unknown length. PowerShell Script 1 applies to malicious PowerShell scripts with known length, while PowerShell Script 2 applies to malicious PowerShell scripts with unknown length. Separating these scenarios lets the inline ML capability process scripts appropriately while preserving the performance requirements of traffic flowing through the firewall.

These mappings reflect the documented WildFire Inline ML model categories and their stated detection coverage. Palo Alto Networks documents the configuration and behavior of these models in its Configure WildFire Inline ML documentation. The corresponding supported file-type and model information is also available in the WildFire Inline Machine Learning administration documentation.

QUESTION NO: 14

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: A B C

Explanation:

Threat logs, **WildFire analysis reports**, and **Botnet reports** provide complementary visibility into command-and-control activity and potentially compromised endpoints. Threat logs record security events detected by the firewall, including connections that match signatures or intelligence associated with C2 and malware activity. The log details, such as source and destination addresses, application, rule, threat identity, and severity, help an analyst identify the internal host involved and investigate the communication.

WildFire analysis reports add malware-behavior context. When WildFire detonates a submitted sample, its report can document network activity observed during analysis, including attempted communications with external hosts that may function as C2 infrastructure. This gives security teams actionable indicators and behavioral evidence for incident investigation.

Botnet reports aggregate and present botnet-related activity observed for hosts on the network, helping analysts identify endpoints that exhibit suspicious communication patterns or interact with known malicious infrastructure. Together, these sources support both event-level investigation and broader identification of infected hosts. Palo Alto Networks documents the relevant telemetry in its Threat Logs documentation, WildFire Analysis Reports documentation, and Botnet Activity monitoring documentation.

QUESTION NO: 15

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: C D E

Explanation:

Upgrading the evaluation unit to the most current recommended firmware, unless a demo of the upgrade process is planned, establishes a known and supported software baseline before the customer evaluation begins. This helps ensure that the testing reflects current platform capabilities, fixes, and security improvements rather than behavior caused by an outdated PAN-OS release. Palo Alto Networks documents the importance of following supported software upgrade paths and release guidance in its PAN-OS Upgrade Guide.

Setting expectations for information being presented in the Security Lifecycle Review (SLR) because personal user information will be made visible is essential to obtain customer awareness and agreement before collecting and analyzing traffic metadata. An SLR is intended to provide visibility into observed applications, threats, users, and traffic patterns, so privacy and data-handling expectations must be addressed before the evaluation starts. Palo Alto Networks describes the assessment and reporting workflow in its Security Lifecycle Review overview.

Resetting the evaluation unit to factory default to ensure that data from any previous customer evaluation is removed protects customer confidentiality and prevents previous policies, logs, objects, certificates, and configuration artifacts from affecting the new evaluation. Beginning from a clean state also makes the resulting configuration and findings attributable to the current customer environment.

QUESTION NO: 16

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: A C

Explanation:

Ensure management continuity is a primary purpose of Panorama high availability. The HA peer maintains synchronized Panorama configuration and can assume the active management role if the active Panorama appliance becomes unavailable. This preserves centralized administration of managed firewalls, device groups, templates, shared objects, and policy workflows, reducing the operational impact of a management-appliance failure.

Control of post rules is also a valid management-layer reason for Panorama HA. Post-rules are centrally managed Panorama policy rules that are applied after locally defined firewall rules. Maintaining an available Panorama management service ensures that administrators can continue to administer, update, commit, and push that centralized policy structure during an appliance failure. In practical terms, the HA investment protects the availability of the centralized policy-control function, including post-rule administration.

The existing multiple M-100 appliances in a Log Collector group address the separate log-collection architecture. Panorama HA is intended to provide redundancy for Panorama management functionality; Palo Alto Networks documents log-collection redundancy separately through the use of multiple Log Collectors in a Collector Group. See Set Up Panorama in a High Availability Configuration and Configure a Log Collector Group.

QUESTION NO: 17

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: D

Explanation:

The Best Practice Assessment (BPA) tool evaluates a Palo Alto Networks NGFW or Panorama configuration against Palo Alto Networks deployment and security best-practice checks. Its report includes configuration findings and actionable recommendations across operational and security areas, including how administrative and management-plane access to devices is configured. Therefore, *identify and provide recommendations for device management access* is a BPA-aligned task: the assessment can highlight management-access exposure and configuration gaps, then recommend hardening measures that improve the security and operational resilience of the firewall or Panorama deployment. BPA is intended to turn configuration analysis into prioritized guidance that helps administrators align their environments with validated best practices, rather than merely inventorying application usage or producing standalone threat intelligence. Palo Alto Networks describes BPA as an assessment of firewall configuration and security posture that provides recommendations for improvement. See the Best Practice Assessment documentation and Palo Alto Networks' Best Practice Assessment service overview.

QUESTION NO: 18

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

A. validate credential submission detection

B. enable User-ID

C. define an SSL decryption rulebase

D. define URL Filtering Profile

E. Enable App-ID

ANSWER: B C D

Explanation:

Credential Phishing Prevention requires User-ID, a URL Filtering profile, and an SSL decryption rulebase. User-ID provides the firewall with the identity and directory context needed to recognize and protect an organization's users and credentials. The URL Filtering profile is where credential-phishing protections are configured and applied to Security policy rules that govern users' web access. The profile enables the firewall to use URL categorization and credential-submission controls as part of its inspection of web traffic.

An SSL Forward Proxy decryption policy is also required for encrypted web sessions. Most credential-submission activity occurs over HTTPS, so the firewall must decrypt applicable outbound traffic to inspect the HTTP content and identify form submissions that contain protected credentials. These components work together: identity context from User-ID, policy enforcement through URL Filtering, and visibility into encrypted sessions through decryption. Palo Alto Networks describes Credential Phishing Prevention configuration and its dependency on decryption and URL Filtering in its Prevent Credential Phishing documentation. Additional decryption policy configuration guidance is available in the Configure Decryption documentation.