IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **NetSec-Generalist**

Title : Palo Alto Networks Network Security Generalist

Version : DEMO

1.When a firewall acts as an application-level gateway (ALG), what does it require in order to establish a connection?
A. Pinhole
B. Dynamic IP and Port (DIPP)
C. Session Initiation Protocol (SIP)
D. Payload
Answer: A
Explanation:
When a firewall functions as an Application-Level Gateway (ALG), it intercepts, inspects, and dynamically manages traffic at the application layer of the OSI model. The primary role of an ALG is to provide deep packet inspection (DPI), address translation, and protocol compliance enforcement.
To establish a connection successfully, an ALG requires a pinhole—a temporary, dynamically created rule that allows the firewall to permit the return traffic necessary for specific applications (e.g., VoIP, FTP, and SIP-based traffic). These pinholes are essential because many applications dynamically negotiate port numbers, making static firewall rules ineffective.
For example, when a Session Initiation Protocol (SIP) application initiates a connection, the firewall dynamically opens a pinhole to allow the SIP media stream (RTP) to pass through while maintaining security controls. Once the session ends, the pinhole is closed to prevent unauthorized access.
Reference to Firewall Deployment and Security Features:
Firewall Deployment – ALGs are commonly deployed in enterprise network firewalls to manage application-specific connections securely.
Security Policies – Firewalls use ALG security policies to allow or block dynamically negotiated connections.
VPN Configurations – Some VPNs rely on ALGs for handling complex applications requiring NAT traversal.
Threat Prevention – ALGs help detect and prevent application-layer threats by inspecting traffic content.
WildFire – Not directly related, but deep inspection features like WildFire can work alongside ALG to inspect payloads for malware.
Panorama – Used for centralized policy management, including ALG-based policies.
Zero Trust Architectures – ALG enhances Zero Trust by ensuring only explicitly allowed application traffic is permitted through temporary pinholes.
Thus, the correct answer is A. Pinhole because it enables a firewall to establish application-layer connections securely while enforcing dynamic traffic filtering.

2.Which action is only taken during slow path in the NGFW policy?
A. Session lookup
B. SSUTLS decryption
C. Layer 2-Layer 4 firewall processing
D. Security policy lookup
Answer: B
Explanation:
In Palo Alto Networks Next-Generation Firewall (NGFW), packet processing is categorized into the fast path (also known as the accelerated path) and the slow path (also known as deep inspection processing). The slow path is responsible for handling operations that require deep content inspection

and policy enforcement beyond standard Layer 2-4 packet forwarding.
Slow Path Processing and SSL/TLS Decryption
SSL/TLS decryption is performed only during the slow path because it involves computationally intensive tasks such as:
Intercepting encrypted traffic and performing man-in-the-middle (MITM) decryption.
Extracting the SSL handshake and certificate details for security inspection.
Inspecting decrypted payloads for threats, malicious content, and compliance with security policies.
Re-encrypting the traffic before forwarding it to the intended destination.
This process is critical in environments where encrypted threats can bypass traditional security inspection mechanisms. However, it significantly impacts firewall performance, making it a slow path action.
Other Answer Choices Analysis
(A) Session Lookup – This occurs in the fast path as part of session establishment before any deeper inspection. It checks whether an incoming packet belongs to an existing session.
(C) Layer 2–Layer 4 Firewall Processing – These are stateless or stateful filtering actions (e.g., access control, NAT, and basic connection tracking), handled in the fast path.
(D) Security Policy Lookup – This is also in the fast path, where the firewall determines whether to allow, deny, or perform further inspection based on the defined security policy rules.
Reference and Justification:
Firewall Deployment – SSL/TLS decryption is part of the firewall's deep packet inspection and Zero Trust enforcement strategies.
Security Policies – NGFWs use SSL decryption to enforce security policies, ensuring compliance and blocking encrypted threats.
VPN Configurations – SSL VPNs and IPsec VPNs also undergo decryption processing in specific security enforcement zones.
Threat Prevention – Palo Alto's Threat Prevention engine analyzes decrypted traffic for malware, C2 (Command-and-Control) connections, and exploit attempts.
WildFire – Inspects decrypted traffic for zero-day malware and sandboxing analysis.
Panorama – Provides centralized logging and policy enforcement for SSL decryption events.
Zero Trust Architectures – Decryption is a crucial Zero Trust principle, ensuring encrypted traffic is not blindly trusted.
Thus, SSL/TLS decryption is the correct answer as it is performed exclusively in the slow path of Palo Alto Networks NGFWs.

3.Which Security profile should be queried when investigating logs for upload attempts that were recently blocked due to sensitive information leaks?
A. Anti-spyware
B. Data Filtering
C. Antivirus
D. URL Filtering
Answer: B
Explanation:
When investigating logs for upload attempts that were recently blocked due to sensitive information leaks, the appropriate Security Profile to query is Data Filtering.

Why Data Filtering?
Data Filtering is a content inspection security profile within Palo Alto Networks Next-Generation Firewalls (NGFWs) that detects and prevents the unauthorized transmission of sensitive or confidential data. This security profile is designed to inspect files, text, and patterns in network traffic and block uploads that match predefined data patterns such as:
Personally Identifiable Information (PII) – e.g., Social Security Numbers, Credit Card Numbers, Passport Numbers
Financial Data – e.g., Bank Account Numbers, SWIFT Codes
Health Information (HIPAA Compliance) – e.g., Patient Medical Records
Custom Data Patterns – Organizations can define proprietary data patterns for detection
How Data Filtering Works in Firewall Logs?
Firewall Policy Application – The Data Filtering profile is attached to Security Policies that inspect file transfers (HTTP, FTP, SMB, SMTP, etc.).
Traffic Inspection – The firewall scans the payload for sensitive data patterns before allowing or blocking the transfer.
Alert and Block Actions – If sensitive data is detected in an upload, the firewall can alert, block, or quarantine the file transfer.
Log Investigation – Security Administrators can analyze Threat Logs (Monitor > Logs > Data Filtering Logs) to review:
File Name
Destination IP
Source User
Matched Data Pattern
Action Taken (Allowed/Blocked)
Reference to Firewall Deployment and Security Features:
Firewall Deployment – Data Filtering is enforced at the firewall level to prevent sensitive data exfiltration.
Security Policies – Configured to enforce Data Filtering rules based on business-critical data classifications.
VPN Configurations – Ensures encrypted VPN traffic is also subject to data inspection to prevent insider data leaks.
Threat Prevention – Helps mitigate the risk of data theft, insider threats, and accidental exposure of sensitive information.
WildFire Integration – Data Filtering can work alongside WildFire to inspect files for advanced threats and malware.
Panorama – Provides centralized visibility and management of Data Filtering logs across multiple firewalls.
Zero Trust Architectures – Aligns with Zero Trust principles by enforcing strict content inspection and access control policies to prevent unauthorized data transfers.
Thus, the correct answer is B. Data Filtering, as it directly pertains to preventing and investigating data leaks in upload attempts blocked by the firewall.

4.When using the perfect forward secrecy (PFS) key exchange, how does a firewall behave when SSL Inbound Inspection is enabled?
A. It acts as meddler-in-the-middle between the client and the internal server.

B. It acts transparently between the client and the internal server.
C. It decrypts inbound and outbound SSH connections.
D. It decrypts traffic between the client and the external server.
Answer: A
Explanation:
Perfect Forward Secrecy (PFS) is a cryptographic feature in SSL/TLS key exchange that ensures each session uses a unique key that is not derived from previous sessions. This prevents attackers from decrypting historical encrypted traffic even if they obtain the server's private key.
When SSL Inbound Inspection is enabled on a Palo Alto Networks Next-Generation Firewall (NGFW), the firewall decrypts inbound encrypted traffic destined for an internal server to inspect it for threats, malware, or policy violations.
Firewall Behavior with PFS and SSL Inbound Inspection
Meddler-in-the-Middle (MITM) Role – Since PFS prevents session key reuse, the firewall cannot use static keys for decryption. Instead, it must act as a man-in-the-middle (MITM) between the client and the internal server.
Decryption Process –
The firewall terminates the SSL session from the external client.
It then establishes a new encrypted session between itself and the internal server.
This allows the firewall to decrypt, inspect, and then re-encrypt traffic before forwarding it to the server.
Security Implications –
This approach ensures threat detection and policy enforcement before encrypted traffic reaches critical internal servers.
However, it breaks end-to-end encryption since the firewall acts as an intermediary.
Why Other Options Are Incorrect?
B. It acts transparently between the client and the internal server. ❌
Incorrect, because SSL Inbound Inspection requires the firewall to actively terminate and re-establish SSL connections, making it a non-transparent MITM.
C. It decrypts inbound and outbound SSH connections. ❌
Incorrect, because SSL Inbound Inspection applies only to SSL/TLS traffic, not SSH connections. SSH decryption requires a different feature (e.g., SSH Proxy).
D. It decrypts traffic between the client and the external server. ❌
Incorrect, because SSL Inbound Inspection is designed to inspect traffic destined for an internal server, not external connections. SSL Forward Proxy would be used for outbound traffic decryption.
Reference to Firewall Deployment and Security Features:
Firewall Deployment – SSL Inbound Inspection is used in enterprise environments to monitor encrypted traffic heading to internal servers.
Security Policies – Decryption policies control which inbound SSL sessions are decrypted.
VPN Configurations – PFS is commonly used in IPsec VPNs, ensuring that keys change per session.
Threat Prevention – Enables deep inspection of SSL/TLS traffic to detect malware, exploits, and data leaks.
WildFire Integration – Extracts potentially malicious files from encrypted traffic for advanced sandboxing and malware detection.
Panorama – Provides centralized management of SSL decryption logs and security policies.
Zero Trust Architectures – Ensures encrypted traffic is continuously inspected, aligning with Zero Trust

security principles.
Thus, the correct answer is:
✅ A. It acts as meddler-in-the-middle between the client and the internal server.

5.What should be reviewed when log forwarding from an NGFW to Strata Logging Service becomes disconnected?
A. Device certificates
B. Decryption profile
C. Auth codes
D. Software warranty
Answer: A
Explanation:
When log forwarding from a Palo Alto Networks NGFW to the Strata Logging Service (formerly Cortex Data Lake) becomes disconnected, the primary aspect to review is device certificates. This is because the firewall uses certificates for mutual authentication with the logging service. If these certificates are missing, expired, or invalid, the firewall will fail to establish a secure connection, preventing log forwarding.
Key Reasons Why Device Certificates Are Critical
Authentication Requirement – The NGFW uses a Palo Alto Networks-issued device certificate for authentication before it can send logs to the Strata Logging Service.
Expiration Issues – If the certificate has expired, the NGFW will be unable to authenticate, causing a disconnection.
Misconfiguration or Revocation – If the certificate is not properly installed, revoked, or incorrectly assigned, the logging service will reject log forwarding attempts.
Cloud Trust Relationship – The firewall relies on secure cloud-based authentication, where certificates validate the NGFW's identity before log ingestion.
How to Verify and Fix Certificate Issues
Check Certificate Status
Navigate to Device > Certificates in the NGFW web interface.
Verify the presence of a valid Palo Alto Networks device certificate.
Look for expiration dates and renew if necessary.
Reinstall Certificates
If the certificate is missing or invalid, reinstall it by retrieving the correct device certificate from the Palo Alto Networks Customer Support Portal (CSP).
Ensure Correct Certificate Chain
Verify that the correct root CA certificate is installed and trusted by the firewall.
Confirm Connectivity to Strata Logging Service
Ensure that outbound connections to the logging service are not blocked due to misconfigured security policies, firewalls, or proxies.
Other Answer Choices Analysis
(B) Decryption Profile – SSL/TLS decryption settings affect traffic inspection but have no impact on log forwarding.
(C) Auth Codes – Authentication codes are used during the initial device registration with Strata Logging Service but do not impact ongoing log forwarding.

(D) Software Warranty – The firewall's warranty does not influence log forwarding; however, an active support license is required for continuous access to Strata Logging Service.
Reference and Justification:
Firewall Deployment – Certificates are fundamental to secure NGFW cloud communication.
Security Policies – Proper authentication ensures logs are securely transmitted.
Threat Prevention & WildFire – Logging failures could impact threat visibility and WildFire analysis.
Panorama – Uses the same authentication mechanisms for centralized logging.
Zero Trust Architectures – Requires strict identity verification, including valid certificates.
Thus, Device Certificates (A) is the correct answer, as log forwarding depends on a valid, authenticated certificate to establish connectivity with Strata Logging Service.