Number: NetSec-Generalist
Passing Score: 800
Time Limit: 120
File Version: 3.0

# Exam Code: NetSec-Generalist

# Exam Name: Palo Alto Networks Network Security Generalist

**Exam A**

**QUESTION 1**
Which Cloud-Delivered Security Services (CDSS) solution is required to configure and enable Advanced DNS Security?

A. Advanced WildFire
B. Enterprise SaaS Security
C. Advanced Threat Prevention
D. Advanced URL Filtering

**Correct Answer: D**
**Section:**

**QUESTION 2**
What is the main security benefit of adding a CN-Series firewall to an existing VM-Series firewall deployment when the customer is using containers?

A. It provides perimeter threat detection and inspection outside the container itself.
B. It prevents lateral threat movement within the container itself.
C. It monitors and logs traffic outside the container itself.
D. It enables core zone segmentation within the container itself.

**Correct Answer: B**
**Section:**

**QUESTION 3**
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.

**Correct Answer: A**
**Section:**

**QUESTION 4**
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

**Correct Answer: A**

**Section:**

**QUESTION 5**
An IT security administrator is maintaining connectivity and security between on-premises infrastructure, private cloud, and public cloud environments in Strata Cloud Manager (SCM).
Which set of practices must be implemented to effectively manage certificates and ensure secure communication across these segmented environments?

A. Use a centralized certificate management solution. Regularly renew and update certificates. Employ strong encryption protocols.
B. Use self-signed certificates for all environments. Renew certificates manually once a year. Avoid automating certificate management to maintain control.
C. Rely on the cloud provider's default certificates. Avoid renewing certificates to reduce overhead and complexity. Manage certificate deployment manually.
D. Implement different certificate authorities (CAs) for each environment. Use default certificate settings. Renew certificates only when they expire to reduce overhead and complexity.

**Correct Answer: A**
**Section:**

**QUESTION 6**
At a minimum, which action must be taken to ensure traffic coming from outside an organization to the DMZ can access the DMZ zone for a company using private IP address space?

A. Configure static NAT for all incoming traffic.
B. Create NAT policies on post-NAT addresses for all traffic destined for DMZ.
C. Configure NAT policies on the pre-NAT addresses and post-NAT zone.
D. Create policies only for pre-NAT addresses and any destination zone.

**Correct Answer: B**
**Section:**

**QUESTION 7**
A company uses Prisma Access to provide secure connectivity for mobile users to access its corporate-sanctioned Google Workspace and wants to block access to all unsanctioned Google Workspace environments.
What would an administrator configure in the snippet to achieve this goal?

A. Dynamic Address Groups
B. Tenant restrictions
C. Dynamic User Groups
D. URL category

**Correct Answer: B**
**Section:**

**QUESTION 8**
Which two cloud deployment high availability (HA) options would cause a firewall administrator to use Cloud NGFW? (Choose two.)

A. Automated autoscaling
B. Terraform to automate HA
C. Dedicated vNIC for HA
D. Deployed with load balancers

**Correct Answer: A**
**Section:**

**QUESTION 9**
A company currently uses Prisma Access for its mobile users. A use case is discovered in which mobile users will need to access an internal site, but there is no existing network communication between the mobile users and the internal site.
Which Prisma Access functionality needs to be deployed to enable routing between the mobile users and the internal site?

A. Interconnect license
B. Service connection
C. Autonomous Digital Experience Manager (ADEM)
D. Security processing node

**Correct Answer: B**
**Section:**

**QUESTION 10**
How are content updates downloaded and installed for Cloud NGFWs?

A. Through the management console
B. Through Panorama
C. Automatically
D. From the Customer Support Portal

**Correct Answer: C**
**Section:**

**QUESTION 11**
Which statement best demonstrates a fundamental difference between Content-ID and traditional network security methods?

A. Content-ID inspects traffic at the application layer to provide real-time threat protection.
B. Content-ID focuses on blocking malicious IP addresses and ports.
C. Traditional methods provide comprehensive application layer inspection.
D. Traditional methods block specific applications using signatures.

**Correct Answer: A**
**Section:**

**QUESTION 12**
Which two SSH Proxy decryption profile configurations will reduce network attack surface? (Choose two.)

A. Allow sessions if resources not available.
B. Allow sessions with unsupported versions.
C. Block sessions on certificate errors.
D. Block sessions with unsupported versions.

**Correct Answer: C**
**Section:**

**QUESTION 13**

Which feature is available in both Panorama and Strata Cloud Manager (SCM)?

A. Template stacks
B. Configuration snippets
C. Policy Optimizer
D. Plug-ins

**Correct Answer: B**
**Section:**

**QUESTION 14**
Which action in the Customer Support Portal is required to generate authorization codes for Software NGFWs?

A. Download authorization codes from the public cloud marketplace.
B. Create a deployment profile.
C. Use the Enterprise Support Agreement (ESA) authorization code.
D. Register the device with the cloud service provider.

**Correct Answer: B**
**Section:**

**QUESTION 15**
Which two pieces of information are needed prior to deploying server certificates from a trusted third-party certificate authority (CA) to GlobalProtect components? (Choose two.)

A. Encrypted private key and certificate (PKCS12)
B. Subject Alternative Name (SAN)
C. Certificate and key files
D. Passphrase for private key

**Correct Answer: A**
**Section:**

**QUESTION 16**
In conjunction with Advanced URL Filtering, which feature can be enabled after usemame-to-IP mapping is set up?

A. Host information profile (HIP)
B. Credential phishing prevention
C. Client probing
D. Indexed data matching

**Correct Answer: B**
**Section:**

**QUESTION 17**
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

**Correct Answer: A**
**Section:**

**QUESTION 18**
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

**Correct Answer: B**
**Section:**

**QUESTION 19**
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

**Correct Answer: B**
**Section:**

**QUESTION 20**
In Prisma SD-WAN. what is the recommended initial action when VoIP traffic experiences high latency and packet loss during business hours?

A. Configure a new VPN gateway connection.
B. Monitor real-time path performance metrics.
C. Add new link tags to existing interfaces.
D. Disable the most recently created path quality.

**Correct Answer: B**
**Section:**

**QUESTION 21**
A hospital system allows mobile medical imaging trailers to connect directly to the internal network of its various campuses. The network security team is concerned about this direct connection and wants to begin implementing a Zero Trust approach in the flat network.
Which solution provides cost-effective network segmentation and security enforcement in this scenario?

A. Deploy edge firewalls at each campus entry point to monitor and control various traffic types through direct connection with the trailers.
B. Manually inspect large images like holograms and MRIs, but permit smaller images to pass freely through the campus core firewalls.

C. Configure separate zones to isolate the imaging trailer's traffic and apply enforcement using the existing campus core firewalls.
D. Configure access control lists on the campus core switches to control and inspect traffic based on image size, type, and frequency.

**Correct Answer: C**
**Section:**

**QUESTION 22**
How does Panorama improve reporting capabilities of an organization's next-generation firewall deployment?

A. By aggregating and analyzing logs from multiple firewalls
B. By automating all Security policy creations for multiple firewalls
C. By pushing out all firewall policies from a single physical appliance
D. By replacing the need for individual firewall deployment

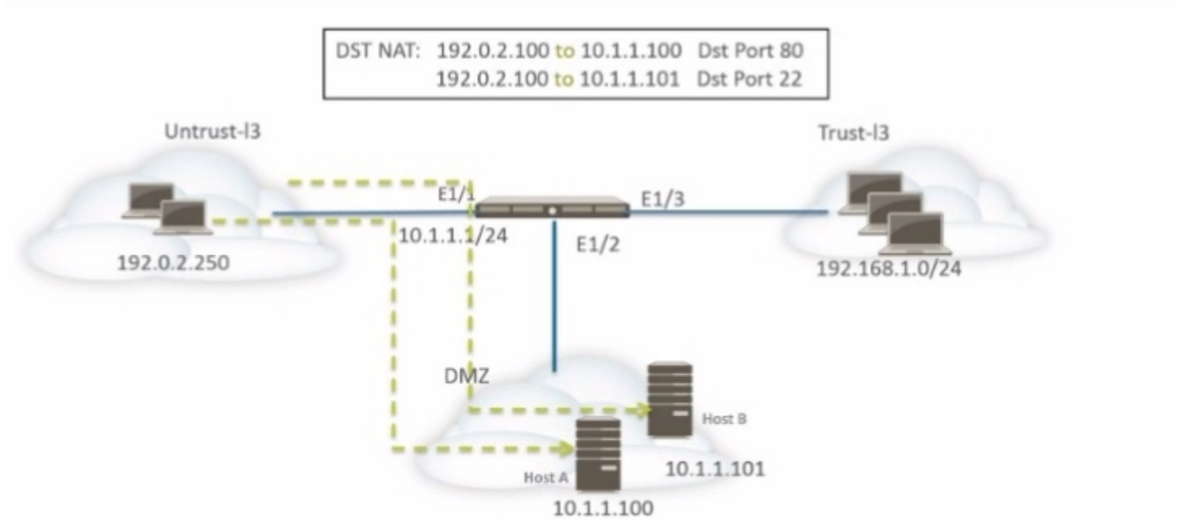
**Correct Answer: A**
**Section:**

**QUESTION 23**
Which two content updates can be pushed to next-generation firewalls from Panorama? (Choose two.)

A. GlobalProtect data file
B. WildFire
C. Advanced URL Filtering
D. Applications and threats

**Correct Answer: B**
**Section:**

**QUESTION 24**
Refer to the exhibit.




A network administrator is using DNAT to map two servers to one public IP address. Traffic will be directed to a specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

Which two sets of Security policy rules will accomplish this configuration? (Choose two.)

A. Source: Untrust (Any) Destination: Untrust Application(s): web-browsing Action: allow
B. Source: Untrust (Any) Destination: Trust Application(s): web-browsing, ssh Action: allow
C. Source: Untrust (Any) Destination: DMZ Application(s): web-browsing Action: allow
D. Source: Untrust (Any) Destination: DMZ Application(s): ssh Action: allow

**Correct Answer: A**
**Section:**