Vendor: Palo Alto Networks

Exam Code: NetSec-Generalist

Exam Name: Palo Alto Networks Network Security Generalist

Version: 25.051

QUESTION 1
An administrator has imported a pair of firewalls to Panorama under the same template stack. As a part of the template stack, the administrator wants to create a high availability (HA) template to be shared by the firewalls.

Which dynamic component should the administrator use when setting the Peer HA1 IP address?

A. Template stack
B. Template variable
C. Address object
D. Dynamic Address Group

Answer: B
Explanation:
When configuring High Availability (HA) settings in Panorama, administrators need to ensure that each firewall in the HA pair has a unique Peer HA1 IP address while using a shared template stack. This is achieved using Template Variables, which allow dynamic configurations per firewall.

Why Template Variable is the Correct Answer?
Ensures Unique HA1 IP Addresses
HA pairs require two separate HA1 IP addresses (one per firewall).
Using template variables, the administrator can assign different values to each firewall without creating separate templates.

Template Variables Provide Flexibility
Instead of hardcoding HA1 IP addresses in the template, variables allow different firewalls to dynamically inherit unique values.
This avoids duplication and ensures configuration scalability when managing multiple firewalls.

QUESTION 2
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.

Answer: C**Explanation:**
When setting up NAT for inbound traffic to a DMZ using private IP addressing, the correct approach is to configure NAT policies on:

Pre-NAT addresses - Refers to the public IP address that external users access.
Post-NAT zone - Refers to the internal (DMZ) zone where the private IP resides.

This ensures that inbound requests are translated correctly from public to private addresses and that firewall policies can enforce access control.

Why is Pre-NAT Address & Post-NAT Zone the Correct Choice?
NAT Rules Must Use Pre-NAT Addresses
The firewall processes NAT rules first, meaning firewall security policies reference pre-NAT IPs.
This ensures incoming traffic is properly matched before translation.

Post-NAT Zone Ensures Correct Forwarding
The destination zone must match the actual (post-NAT) zone to allow correct security policy enforcement.

QUESTION 3
In which mode should an ION device be configured at a newly acquired site to allow site traffic to be audited without steering traffic?

A. Access
B. Control
C. Disabled
D. Analytics

Answer: D
Explanation:
An ION device (used in Prisma SD-WAN) must be configured in Analytics mode at a newly acquired site to audit traffic without steering it. This mode allows administrators to monitor network behavior without actively modifying traffic paths.

Why Analytics Mode is the Correct Choice?
Passively Observes Traffic
The ION device monitors and logs site traffic for analysis.
No active control over routing or traffic flow is applied.
Useful for Network Auditing Before Full Deployment
Analytics mode provides visibility into site traffic before committing to SD-WAN policy changes.
Helps identify optimization opportunities and troubleshoot connectivity before enabling traffic steering.

QUESTION 4
Which functionality does an NGFW use to determine whether new session setups are legitimate or illegitimate?

A. SYN flood protection
B. SYN bit
C. Random Early Detection (RED)
D. SYN cookies

Answer: A
Explanation:
An NGFW (Next-Generation Firewall) determines whether new session setups are legitimate or illegitimate by using SYN flood protection, which is a key component of DoS/DDoS mitigation.

How SYN Flood Protection Works in an NGFW:
Detects High SYN Traffic Rates - SYN flood attacks occur when a large number of half-open TCP connections are created, overwhelming a server or firewall.
Implements SYN Cookies or Rate-Limiting - To mitigate attacks, the NGFW applies SYN cookies or connection rate limits to filter out illegitimate connection attempts.
Maintains a Secure State Table - The firewall tracks legitimate and suspicious SYN requests, ensuring only genuine connections are allowed through.
Protects Against TCP-Based Attacks - Prevents resource exhaustion caused by attackers flooding SYN packets without completing the TCP handshake.

QUESTION 5
A network engineer needs to configure a Prisma SD-WAN environment to optimize and secure traffic flow between branch offices and the data center.

Which action should the engineer prioritize to achieve the most operationally efficient communication?

A. Ensure all branch office traffic is routed through a central hub for inspection.
B. Create NAT policies to translate internal branch IP addresses to public IP addresses.
C. Define security zones for branch offices and the data center.
D. Configure dynamic path selection based on network performance metrics.

Answer: D
Explanation:
In a Prisma SD-WAN environment, the most operationally efficient way to optimize and secure traffic between branch offices and the data center is to configure dynamic path selection.

How Dynamic Path Selection Optimizes Traffic:
Monitors Real-Time Network Performance - Prisma SD-WAN continuously measures latency, jitter, and packet loss across multiple WAN links.
Automatically Chooses the Best Path - It dynamically routes traffic through the best-performing link to maintain high application performance.
Improves Reliability and Redundancy - If a link degrades, failover occurs seamlessly to another available path.
Enhances Security - Works in conjunction with security policies to route sensitive traffic through trusted paths.

QUESTION 6
Why would an enterprise architect use a Zero Trust Network Access (ZTNA) connector instead of a service connection for private application access?

A. It controls traffic from the mobile endpoint to any of the organization's internal resources.
B. It functions as the attachment point for IPSec-based connections to remote site or branch networks.
C. It supports traffic sourced from on-premises or public cloud-based resources to mobile users and remote networks.
D. It automatically discovers private applications and suggests Security policy rules for them.

Answer: D
Explanation:
A Zero Trust Network Access (ZTNA) connector is used instead of a service connection for private application access because it provides automatic application discovery and policy enforcement.

Why is ZTNA Connector the Right Choice?
Discovers Private Applications
The ZTNA connector automatically identifies previously unknown or unmanaged private applications running in a data center or cloud environment.

Suggests Security Policy Rules
After discovering applications, it suggests appropriate security policies to control user access, ensuring Zero Trust principles are followed.

Granular Access Control
It enforces least-privilege access and applies identity-based security policies for private applications.

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

Answer: B
Explanation:
A company using Prisma Access to secure Google Workspace access while blocking unsanctioned Google tenants must implement Tenant Restrictions.

Why are Tenant Restrictions the Right Choice?
Restricts Google Workspace Access to Approved Tenants
Tenant restrictions allow only authorized Google Workspace tenants (e.g., the company's official domain) and block access to personal or unauthorized instances.

Prevents Data Exfiltration & Shadow IT Risks
Without tenant restrictions, users could log into personal Google accounts and transfer corporate data to external environments.

Works with Prisma Access Security Policies
Prisma Access enforces tenant restrictions at the cloud level, ensuring compliance without requiring local device policies.

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

Answer: AD
Explanation:
Cloud high availability (HA) strategies differ from traditional HA deployments in physical firewalls. Cloud NGFW provides cloud-native high availability options that align with cloud architectures, particularly in AWS and Azure environments.

Automated Autoscaling
Cloud NGFW automatically scales up or down based on traffic demand and load conditions.

This ensures consistent security enforcement without manual intervention.
Auto-scaling is managed by cloud-native services (AWS Auto Scaling, Azure Virtual Machine Scale Sets, etc.).

Deployed with Load Balancers
Cloud NGFW can be integrated with cloud-native load balancers (AWS Elastic Load Balancing, Azure Load Balancer) to distribute traffic.
This helps ensure high availability and failover in case of firewall instance failures.

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

Answer: B
Explanation:
Prisma Access provides secure remote access for mobile users, but by default, mobile users cannot access internal sites unless explicitly configured.

How Service Connection Enables Routing Between Mobile Users and Internal Sites:
Service Connection establishes a secure tunnel between Prisma Access and the internal network.
Allows direct routing between mobile users and internal applications.
Enables access without requiring additional VPN connections.
Ensures that Prisma Access can securely route traffic between mobile users and the internal site.

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

Answer: C
Explanation:
Cloud NGFWs receive content updates automatically as part of cloud-native security services.
These updates include:
Threat prevention updates (IPS, malware signatures).
App-ID updates to maintain accurate application identification.
WildFire updates for new malware detection.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**