

# **Paloalto Networks NetSec-Pro**

## **Palo Alto Networks Certified Network Security Professional**

**Thank You for Downloading NetSec-Pro Updated Exam  
Questions**

<https://certs4sale.com/paloalto-networks/netsec-pro-pdf-exam-dumps>

PALO ALTO NETWORKS NETWORK SECURITY PROFESSIONAL

## NetSec-Pro

### Palo Alto Networks Certified Network Security Professional

Practice Questions & Detailed Solutions Guide

#### About This Preparation Guide

This guide contains authentic technical practice questions, answer keys, and in-depth explanations designed to prepare candidates for the Palo Alto Networks Certified Network Security Professional (NetSec-Pro) exam.

#### Exam Domains Covered

The NetSec-Pro certification evaluates expertise across critical Palo Alto Networks infrastructure & cloud security areas:

- SSL/TLS Inspection Strategies & Certificate Pinning Exceptions
- Zero Trust Network Architecture & Zone-Based Security Hardening
- Panorama Centralized Management, Logging Profiles & Monitoring
- Prisma Access Integration for Remote Users & Enterprise DLP
- CN-Series Microsegmentation, Fast Path vs. Slow Path Inspection Optimization

### Question 1

SINGLE CHOICE

Your organization is evaluating SSL/TLS inspection strategies for their Strata NGFW deployment. They need to inspect encrypted traffic to websites accessed by employees while maintaining compliance with certificate pinning applications used by third-party financial software. Which decryption approach best balances security inspection with application compatibility?

- A. SSL Forward Proxy with a granular decryption policy that excludes traffic to domains matching the financial vendor's certificate pinning requirements
- B. SSL Inbound Inspection for all encrypted traffic to ensure complete visibility of all external communications
- C. No decryption for the entire traffic flow to avoid interference with certificate pinning
- D. SSH Proxy to handle all encrypted protocol inspection uniformly

**Answer: A**

#### Explanation:

SSL Forward Proxy decryption allows selective inspection of outbound HTTPS traffic and can be configured with granular policies to exclude specific domains or traffic patterns—critical for avoiding certificate pinning conflicts. SSL Inbound Inspection is designed for inspecting inbound encrypted connections to servers, not outbound employee web traffic. No decryption sacrifices security visibility entirely. SSH Proxy is for SSH protocol specifically, not HTTPS. The correct answer demonstrates understanding that decryption policies must be tailored to business requirements and application compatibility.

### Question 2

MULTIPLE CHOICE

A mid-sized enterprise is implementing network segmentation using Palo Alto Networks zone-based security. They have separate zones for guest WiFi, corporate endpoints, and critical infrastructure. When designing security policies between these zones, which of the following best reflects network hardening principles and Zero Trust architecture? (Select two.)

- A. Apply User-ID and Device-ID based policies to restrict guest WiFi traffic from accessing corporate zone resources, even if network connectivity exists
- B. Create explicit deny-all default rules between zones and only permit traffic that is whitelisted for business purposes
- C. Allow guest WiFi to critical infrastructure zone traffic since both zones are behind the corporate firewall
- D. Use Content-ID signatures to automatically permit safe traffic categories without explicit policy rules

**Answer: A, B**

#### Explanation:

Zero Trust architecture requires verification at every level and default denial with explicit allowlisting. User-ID and Device-ID provide identity and device posture context for more granular control than network-based rules alone, making option A correct. Option B directly reflects the Zero Trust principle of explicit whitelisting and deny-by-default.

Option C violates segmentation by allowing any internal-to-critical traffic without inspection. Option D mischaracterizes Content-ID as an access control mechanism—it inspects application content but doesn't replace policy controls, and relying on automatic permitting contradicts Zero Trust.

### Question 3

SINGLE CHOICE

An organization has deployed Panorama to manage 150+ firewalls across multiple regions. During a recent security incident, the SOC team discovered that logging was inconsistent across firewalls—some were missing traffic logs for policy denials. When reviewing Panorama's monitoring and logging capabilities, which configuration should the security team verify to ensure consistent log collection from all managed devices?

- A. Verify that Panorama's log forwarding profiles are configured to collect traffic logs from all managed firewalls and that the Panorama-to-syslog destination is properly sized
- B. Check that User-ID probes are deployed on every firewall to enable traffic logging
- C. Confirm that Advanced Threat Prevention is enabled on all firewalls, as it automatically generates traffic logs
- D. Ensure that Mobile Security is active, which centralizes all logging through Panorama

**Answer: A**

#### Explanation:

Panorama acts as a centralized management and logging hub. To ensure consistent log collection, administrators must configure log forwarding profiles that specify which log types (traffic, threat, etc.) are collected from managed devices and where they are sent. This is a fundamental Panorama logging configuration task.

User-ID does not control logging behavior. Advanced Threat Prevention and Mobile Security are security features but not the mechanism for centralized logging configuration—they generate logs that are forwarded via the logging profiles already configured. Verifying log forwarding profiles and destination capacity directly addresses the inconsistent logging issue.

### Question 4

SINGLE CHOICE

Your organization is deploying Prisma Access to provide secure remote access for 500 distributed employees. The remote users need access to both public-facing company web applications and private internal databases. Additionally, the company must apply Data Loss Prevention (DLP) policies to inspect traffic from remote users. Which combination of Prisma Access configurations enables this use case while maintaining security?

- A. Configure both public application access and private application access; enable CDSS to include Enterprise DLP inspection for remote user traffic
- B. Use only private application access mode and route all public internet traffic through a legacy perimeter firewall
- C. Deploy Prisma Access with public application access only and manually configure VPN tunnels for private application access
- D. Enable remote user configuration with built-in DLP rules that automatically block all sensitive data transfers

**Answer: A**

#### Explanation:

Prisma Access supports both public and private application access modes. Public application access allows secure internet browsing, while private application access provides secure connectivity to internal resources. When Enterprise DLP is added as a Cloud-Delivered Security Service (CDSS), it applies consistent DLP policies to all remote user traffic regardless of destination.

Option B defeats the purpose of Prisma Access by requiring a legacy firewall. Option C suggests manual VPN tunneling, which is not how Prisma Access architecture works. Option D oversimplifies DLP—policies must be tuned to business requirements, not universally block sensitive data, which would break legitimate business workflows.

**Question 5****SINGLE CHOICE**

An organization has implemented CN-Series firewalls in their Kubernetes cluster for microsegmentation and is experiencing high latency on some pod-to-pod communication. The security team must decide whether to adjust the inspection path to improve performance without compromising threat detection. Which approach correctly balances inspection efficacy with performance for CN-Series?

- A. Implement fast path inspection for whitelisted pod-to-pod traffic after it has been validated through slow path; continue slow path inspection for new or suspicious connections
- B. Disable all packet inspection on the fast path and rely entirely on policy rules at the network layer
- C. Move all traffic through the slow path to maximize threat detection regardless of performance impact
- D. Use fast path exclusively for all east-west traffic to eliminate latency

**Answer: A****Explanation:**

Fast path and slow path are complementary inspection mechanisms. Slow path performs deep packet inspection (DPI) and threat analysis but is computationally expensive. Fast path handles connection lookups and policy enforcement more efficiently. The optimal approach for containerized environments is to establish trust through initial slow path analysis, then accelerate known-good traffic via fast path while maintaining inspection for new or anomalous connections. This preserves security while improving performance.

Option B removes threat inspection entirely. Option C ignores performance requirements. Option D skips inspection for all traffic, defeating the security purpose of microsegmentation.

## End of Practice Guide

You have completed reviewing the Palo Alto Networks NetSec-Pro practice scenario set.



# THANK YOU FOR DOWNLOADING NETSEC- PRO UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our NetSec-Pro Exam Product

Visit Our Site to Purchase the Full Set of Actual NetSec-Pro Exam Questions With Answers.

## Money Back Guarantee



Click The Link Below

<https://certs4sale.com/paloalto-networks/netsec-pro-pdf-exam-dumps>