Palo Alto Networks PCNSE

Module 1: Core Concepts (12%)

Section 1.1: Understand Palo Alto Networks Core Components

- Security components
- Firewall components
- Panorama components
- PAN-OS subscriptions and the features they enable
- Plug-in components
- Heatmap and BPA reports
- Artificial intelligence operations (AIOps)/Telemetry
- IPv6
- Internet of Things (IoT)

Section 1.2: Interface and Zone Types

- Layer 2 interfaces
- Layer 3 interfaces
- Virtual Wire (vWire) interfaces
- Tap interfaces
- Subinterfaces
- Tunnel interfaces
- Aggregate interfaces
- Loopback interfaces
- Decrypt mirror interfaces
- VLAN interfaces

Section 1.3: Decryption Strategies

- Risks and implications of enabling decryption
- Use cases
- Decryption types
- Decryption profiles and certificates
- Create decryption policy in the firewall
- Configure SSH proxy

Section 1.4: User-ID Enforcement

- Methods of building user-to-IP mappings
- User-ID agent vs agentless comparison
- Methods of User-ID redistribution
- Methods of group mapping
- Server profile and authentication profile

Section 1.5: Authentication Policy

- Purpose and use case
- Dependencies
- Captive portal vs GlobalProtect (GP) client

Section 1.6: Management vs Data Plane

- Differentiate between management plane and data plane functions

Section 1.7: Multi-VSYS Environments

- User-ID hub
- Inter-vsys routing
- Service routes
- Administration

Module 2: Deploy and Configure Core Components (20%)

Section 2.1: Management Profiles

- Interface management profile
- SSL/TLS service profile

Section 2.2: Security Profiles

- Custom configuration of Security profiles and Security profile groups
- URL filtering vs credential theft prevention
- DNS Security
- Tuning and exceptions
- Threat prevention vs advanced threat prevention
- URL Filtering vs Advanced URL Filtering

Section 2.3: Protection Profiles

- Zone protection
- Packet buffer protection
- DoS protection

Section 2.4: Deployment Design

- High availability (HA)
- HA pair setup
- Zero Touch Provisioning (ZTP)
- Bootstrapping

Section 2.5: Certificates and Access

- Role-based access control (RBAC)
- Authentication methods and sequences
- Certificate management and profiles

Section 2.6: Routing and NAT

- Dynamic routing, redistribution profiles, static routes
- Policy-based forwarding
- NAT configurations and rules

Section 2.7: Site-to-Site Tunnels

- IPSec components
- GRE tunnels
- Tunnel monitoring and troubleshooting

Section 2.8: Application QoS

- QoS profiles, rules, and policies
- Monitoring and bandwidth control per application

Module 3: Deploy and Configure Features and Subscriptions (17%)

Section 3.1: App-ID

- Security rules with App-ID
- Converting port-based to App-ID rules
- Custom apps and threats

Section 3.2: GlobalProtect

- Licensing and setup
- Gateway, portal, and client configurations
- HIP and split tunneling

Section 3.3: Decryption

- Inbound decryption
- SSL forward proxy
- SSH proxy

Section 3.4: User-ID

- Agents, group mapping, dynamic user groups

Section 3.5: WildFire

- Submission profiles
- File types and schedules
- Forwarding decrypted traffic

Section 3.6: Web Proxy

- Transparent and explicit proxies

Module 4: Deploy and Configure Firewalls Using Panorama (17%)

Section 4.1: Templates

- Template stacks and value overrides
- Variables in templates

Section 4.2: Device Groups

- Device group hierarchies and use cases
- Pre-rules, post-rules, and local rules

Section 4.3: Configuration Management

- Licensing
- Commit recovery and schedules
- Importing configurations

Section 4.4: Role-Based Access

- RBAC in Panorama

Module 5: Manage and Operate (16%)

Section 5.1: Log Forwarding

- Log types and criticalities
- External services integration

Section 5.2: System Upgrades

- Single firewall and HA upgrades
- Panorama updates

Section 5.3: High Availability (HA)

- HA functions, interfaces, clustering, and failover

Module 6: Troubleshooting (18%)

Section 6.1: Site-to-Site Tunnels

- IPSec and GRE tunnel issues
- Route-based vs policy-based

Section 6.2: Interfaces

- Transceivers, settings, LACP, tagging

Section 6.3: Decryption

- SSL forward proxy, exclusions, certificates

Section 6.4: Routing

- Dynamic routing and policy-based forwarding

Section 6.5: Resource Protections

- Zone, DoS, and packet buffer protections

Section 6.6: GlobalProtect

- Portal and gateway issues

Section 6.7: Policies

- NAT, security, and authentication troubleshooting

Section 6.8: HA Functions

- Failover triggers and monitoring