# Palo Alto Network Certified Network Security Engineer

Zetlan Technologies

# Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

# Course Modules

### 1. Core Concepts

- Identify how Palo Alto Networks products work together
  - 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)
- Determine and assess appropriate interface or zone types
  - Layer 2 interfaces
  - Layer 3 interfaces
  - Virtual wire (vwire) interfaces
  - Tap interfaces
  - Sub-interfaces
  - Tunnel interfaces
  - Aggregate interfaces
  - Loopback interfaces
  - Decrypt mirror interfaces
  - VLAN interfaces

# Palo Alto Network Certified Network Security Engineer

- Identify decryption deployment strategies
  - Risks and implications of enabling decryption
  - Use cases
  - Decryption types
  - Decryption profiles and certificates
  - Create decryption policy in the firewall
  - Configure SSH Proxy
- Enforce User-ID
  - Methods of building user-to-IP mappings
  - Determine if User-ID agent or agentless should be used
  - Compare and contrast User-ID agents
  - Methods of User-ID redistribution
  - Methods of group mapping
  - Server profile & authentication profile
- Determine how and when to use the Authentication policy
  - Purpose of, and use case for, the Authentication policy
  - Dependencies
  - Captive portal versus GlobalProtect (GP) client
- Dift betwn the fundmntl that reside on the mngmnt & data plane
- Define multiple virtual systems (multi-vsys) environment
  - User-ID hub
  - Inter-vsys routing
  - Service routes
  - Administration

# Palo Alto Network Certified Network Security Engineer

## 2. Deploy and Configure Core Components

- Configure management profiles
  - Interface management profile
  - SSL/TLS service profile
- Deploy and configure Security profiles
  - Custom config of difft Security profiles and Securty profile groups
  - Relationship between URL filtering and credential theft preventn
  - Usernme & domain name in HTTP header insertn DNS Security
  - How to tune or add exceptions to a Security profile
  - Compare & contrast threat preventn & advanced threat preventn
  - Compare and contrast URL Filtering and Advanced URL Filtering
- Config zone protection, packet buffer protection, & DoS protection
  - Customized values versus default settings
  - Classified versus aggregate profile types
  - Layer 3 and Layer 4 header inspection
- Design the deployment config of a Palo Alto Networks firewall
  - Advanced high availability (HA) deployments
  - HA pair
  - Zero Touch Provisioning (ZTP)
  - Bootstrapping

# Palo Alto Network Certified Network Security Engineer

- Configure authorization, authentication, and device access
  - Role-based access control for authorization
  - Different methods used to authenticate
  - The authentication sequence
  - The device access method
- Configure and manage certificates
  - Usage
  - Profiles
  - Chains
- Configure routing
  - Dynamic routing
  - Redistribution profiles
  - Static routes
  - Path monitoring
  - Policy-based forwarding
  - Virtual router versus logical router
- Configure NAT
  - NAT policy rules
  - Security rules
  - Source NAT
  - No NAT
  - Use session browser to find NAT rule name
  - U-Turn NAT
  - Check HIT counts

# Palo Alto Network Certified Network Security Engineer

- Configure site-to-site tunnels
  - IPSec components
  - Static peers and dynamic peers for IPSec
  - IPSec tunnel monitor profiles
  - IPSec tunnel testing
  - Generic Routing Encapsulation (GRE)
  - One-to-one and one-to-many tunnels
  - Determine when to use proxy IDs
- Configure service routes
  - Default
  - Custom
  - Destination
  - Custom routes for different vsys versus destination routes
  - How to verify service routes
- Configure application-based QoS
  - Enablement requirements
  - QoS policy rule
  - Add DSCP/TOS component
  - QoS profile
  - Determine how to control bandwidth use on a per-app basis
  - Use QoS to monitor bandwidth utilization

### 3. Deploy and Configure Features and Subscriptions

- Configure App-ID
  - Create security rules with App-ID
  - Convert port and protocol rules to App-ID rules
  - Identify the impact of app override to the overall functionality
  - Create custom apps and threats
  - Review App-ID dependencies
- Configure Global Protect
  - Global Protect licensing
  - Configure gateway and portal
  - GlobalProtect agent
  - Differentiate between login methods
  - Configure Clientless VPN
  - Host information profile (HIP)
  - Configure multiple gateway agent profiles
  - Split tunnelling
- Configure decryption
  - Inbound decryption
  - SSL forward proxy
  - SSL decryption exclusions
  - SSH proxy

# Palo Alto Network Certified Network Security Engineer

- Configure User-ID
  - User-ID agent and agentless
  - User-ID group mapping
  - Shared User-ID mapping across virtual systems
  - Data redistribution
  - User-ID methods
  - Benefits of using dynamic user groups in policy rules
  - Requirements to support dynamic user groups
  - How Global Protect internal and external gateways can be used
- Configure Wild Fire
  - Submission profile
  - Action profile
  - Submissions and verdicts
  - Signature actions
  - File types and file sizes
  - Update schedule
  - Forwarding of decrypted traffic
- Configure Web Proxy
  - Transparent proxy
  - Explicit proxy

## 4. Deploy and Configure Firewalls Using Panorama

- Configure templates and template stacks
  - Components configured in a template
  - How the order of templates in a stack affects the config push
  - Overriding a template value in a stack
  - Configure variables in templates
  - Relationship between Panorama and devices as pertaining
- Configure device groups
  - Device group hierarchies
  - Identify what device groups contain
  - Diffrnte betwn different use cases for pre-rules, local rules, etc.,
  - Identify the impact of configuring a primary device
  - Assign firewalls to device groups
- Manage firewall configurations within Panorama
  - Licensing
  - Commit recovery feature
  - Automatic commit recovery
  - Commit types and schedules
  - Config backups
  - Commit type options
  - Dynamic updates for Panorama & Panorama-managed devices
  - Software and dynamic updates
  - Import firewall configuration into Panorama
  - Configure log collectors

# Palo Alto Network Certified Network Security Engineer

## 5. Manage and Operate

- Manage and configure Log Forwarding
  - Identify log types and criticalities
  - Manage external services
  - Create and manage tags
  - Identfy system and traffic issues usg the web interface & CLI tools
  - Configure Log Forwarding profile and device log settings
  - Log monitoring
  - Customize logging and reporting settings
- Plan & execute the process to upgrade a Palo Alto Networks systm
  - Single firewall
  - HA pairs
  - Panorama push
  - Dynamic updates
- Manage HA functions
  - Link monitoring
  - Path monitoring
  - HA links
  - Failover
  - Active/active and active/passive
  - HA interfaces
  - Clustering
  - Election setting

## 6. Troubleshooting

- Troubleshoot site-to-site tunnels
  - IPSec
  - GRE
  - One-to-one and one-to-many tunnels
  - Route-based versus policy-based remote hosts
  - Tunnel monitoring
- Troubleshoot interfaces
  - Transceivers
  - Settings
  - Aggregate interfaces, LACP
  - Counters
  - Tagging
- Troubleshoot decryption
  - Inbound decryption
  - SSL forward proxy
  - SSH proxy
  - Identify what can't be decrypted & config exclusions & bypasses
  - Certificates

# Palo Alto Network Certified Network Security Engineer

- Troubleshoot routing
  - Dynamic routing
  - Redistribution profiles
  - Static routes
  - Route monitoring
  - Policy-based forwarding
  - Multicast routing
  - Service routes
- General Troubleshooting
  - Logs
  - Packet capture (pcap)
  - Reports
- Troubleshoot resource protections
  - Zone protection profiles
  - DoS protections
  - Packet buffer protections
- Troubleshoot Global Protect
  - Portal and Gateway
  - Access to resources
  - Global Protect client

# Palo Alto Network Certified Network Security Engineer



- Troubleshoot policies
  - NAT
  - Security
  - Decryption
  - Authentication
- Troubleshoot HA functions
  - Monitor
  - Failover triggers

Zetlan Technologies

# LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

## ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474