IPRULERS

PALO ALTO NETWORKS TRAINING AND CERTIFICATION

www.iprulers.com training@iprulers.com

Palo Alto Networks offers a broad range of role-based certifications that are compatible with their Network security technologies.

We **IPRULERS** develops and delivers world-class Network Security training and curriculum for the Palo Alto Networks. These training programs are available for both open enrollment by the public and for private onsite training in classroom and virtual delivery formats. Palo Alto Networks training from IPRULERS provides the next-generation firewall knowledge to secure your network and safely enable applications. Your level of expertise in your field is elevated through certification. The reputation, job effectiveness, and marketability of a professional who holds a Palo Alto Networks certification all improve. By the time you complete our comprehensive training program, you will be eligible to do the PCNSA and PCNSE Certifications.

CERTIFICATION

PCNSA

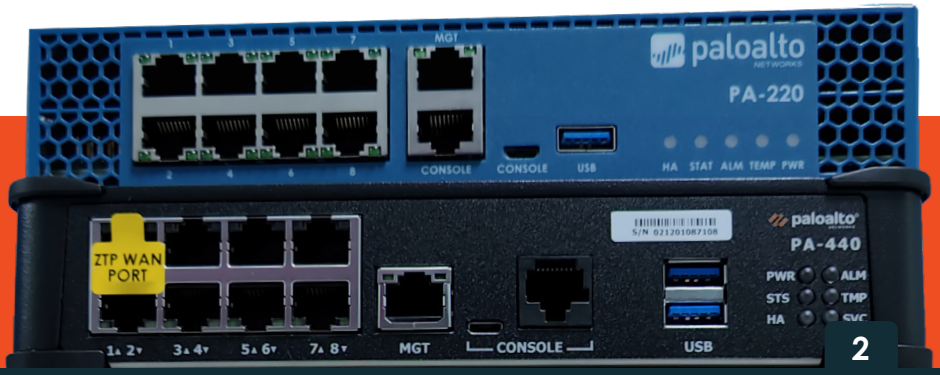
PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA)

PCNSE

PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ENGINEER (PCNSE)

COURSE MODULES

(EDU-210) FIREWALL 11.0 ESSENTIALS : *CONFIGURATION AND MANAGEMENT.*
(EDU-220) PANORAMA 11.0 : *MANAGING FIREWALLS AT SCALE.*
(EDU-330) FIREWALL11.0 : *TROUBLESHOOTING*



CERTIFICATION DETAILS

paloalto NETWORKS

PCNSA

PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ADMINISTRATOR (PCNSA)

The **PCNSA certification** validates the knowledge and skills required for network security administrators responsible for deploying and operating Palo Alto Networks Next-Generation Firewalls (NGFWs). PCNSA certified individuals have demonstrated knowledge of the Palo Alto Networks NGFW feature set and in the Palo Alto Networks product portfolio core components.

PREREQUISITES

There are no prerequisites required.

Recommended Training Courses

Firewall 11.0 Essentials: Configuration and Management (EDU-210)

PCNSA COURSE OUTLINE

Domain	*Weight (%)*
Device Management and Services	***22%***
Managing Objects	***20%***
Policy Evaluation and Management	***28%***
Securing Traffic	***30%***

Domain 1 Device Management and Services (22%)

1.1 Demonstrate knowledge of firewall management interfaces.

- 1.1.1 Management interfaces
- 1.1.2 Methods of access
- 1.1.3 Access restrictions
- 1.1.4 Identity-management traffic flow
- 1.1.5 Management services
- 1.1.6 Service routes

1.2 Provision local administrators

- 1.2.1 Authentication profile
- 1.2.2 Authentication sequence

1.3 Assign role-based authentication

1.4 Maintain firewall configurations.

1.4.1 Running configuration.
1.4.2 Candidate configuration.
1.4.3 Discern when to use load, save, import, and export.
1.4.4 Differentiate between configurations states.
1.4.5 Back up Panorama configurations & firewalls from Panorama.

1.5 Push policy updates to Panorama-managed firewalls

1.5.1 Device groups and hierarchy
1.5.2 Where to place policies.
1.5.3 Implications of Panorama management.
1.5.4 Impact of templates, template stacks, and hierarchy.

1.6 Schedule and install dynamic updates

1.6.1 From Panorama
1.6.2 From the firewall
1.6.3 Scheduling and staggering updates on an HA pair.

1.7 Create and apply security zones to policies

1.7.1 Identify zone types.
1.7.2 External types
1.7.3 Layer 2
1.7.4 Layer 3
1.7.5 TAP
1.7.6 VWire
1.7.7 Tunnel

1.8 Identify and configure firewall interfaces

1.8.1 Different types of interfaces
1.8.2 How interface types affect Security policies

1.9 Maintain and enhance the configuration of a virtual or logical router

1.9.1 Steps to create a static route.
1.9.2 How to use the routing table.
1.9.3 What interface types can be added to a virtual or logical router.
1.9.4 How to configure route monitoring

Domain 2 Managing Objects (20%)

2.1 Create and maintain address & address group objects

2.1.1 How to tag objects.
2.1.2 Differentiate between address objects.
2.1.3 Static groups versus dynamic groups.

2.2 Create and maintain services and services groups

2.3 Create and maintain external dynamic lists

2.4 Configure and maintain application filters and application groups

2.4.1 When to use filters versus groups.
2.4.2 The purpose of application characteristics as defined in the App-ID database.

Domain 3 Policy Evaluation and Management (28%)

3.1 Develop the appropriate application-based Security policy

3.1.1 Create an appropriate App-ID rule.
3.1.2 Rule shadowing
3.1.3 Group rules by tag
3.1.4 The potential impact of App-ID updates to existing Security policy rules.
3.1.5 Policy usage statistics

3.2 Differentiate specific security rule types

3.2.1 Interzone
3.2.2 Intrazone
3.2.3 Universal

3.3 Configure Security policy match conditions, actions, and logging options

3.3.1 Application filters and groups
3.3.2 Logging options
3.3.3 App-ID
3.3.4 User-ID
3.3.5 Device-ID
3.3.6 Application filter in policy
3.3.7 Application group in policy
3.3.8 EDLs

3.4 Identify and implement proper NAT policies

3.4.1 Destination
3.4.2 Source

3.5 Optimize Security policies using appropriate tools.

3.5.1 Policy test match tool
3.5.2 Policy Optimizer

Domain 4 Securing Traffic (30%)

4.1 Compare and contrast different types of Security profiles

4.1.1 Antivirus
4.1.2 Anti-Spyware
4.1.3 Vulnerability Protection
4.1.4 URL Filtering
4.1.5 WildFire Analysis

4.2 Create, modify, add & apply the appropriate Security profiles & groups

4.2.1 Antivirus
4.2.2 Anti-Spyware
4.2.3 Vulnerability Protection
4.2.4 URL Filtering
4.2.5 WildFire Analysis
4.2.6 Configure threat prevention policy

4.3 Differentiate between Security profile actions

4.4 Use information available in logs

- 4.4.1 Traffic
- 4.4.2 Threat
- 4.4.3 Data
- 4.4.4 System logs

4.5 Enable DNS Security to control traffic based on domains

- 4.5.1 Configure DNS Security
- 4.5.2 Apply DNS Security in policy

4.6 Create and deploy URL -filtering-based controls

- 4.6.1 Apply a URL profile in a Security policy.
- 4.6.2 Create a URL Filtering profile.
- 4.6.3 Create a custom URL category.
- 4.6.4 Control traffic based on a URL category.
- 4.6.5 Why a URL was blocked.
- 4.6.6 How to allow a blocked URL.
- 4.6.7 How to request a URL recategorization

4.7 Differentiate between group mapping & IP-to-user mapping within policies and logs

- 4.7.1 How to control access to specific locations.
- 4.7.2 How to apply to specific policies.
- 4.7.3 Identify users within the ACC and the monitor tab

paloalto NETWORKS

PCNSE

PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ENGINEER (PCNSE)

The **PCNSE certification** validates the knowledge and skills required for network security engineers that design, deploy, operate, manage, and troubleshoot Palo Alto Networks Next-Generation Firewalls. PCNSE-certified individuals have demonstrated in-depth knowledge of the Palo Alto Networks product portfolio and can make full use of it in most implementations.

PREREQUISITES

Students must have completed the Firewall Essentials: Configuration and Management EDU-210) class.

Recommended Training Courses

Mandatory Training: Panorama 11.0 Managing Firewalls at Scale (EDU-220)

Optional training: Firewall11.0: Troubleshooting (EDU-330)

PCNSE COURSE OUTLINE

Panorama 11.0 Managing Firewalls at Scale (EDU-220)

Domain	Weight (%)
Core Concepts	12%
Deploy and Configure Core Components	20%
Deploy and Configure Features and Subscriptions	17%
Deploy and Configure Firewalls Using Panorama	17%
Manage and Operate	16%
Troubleshooting	18%

Domain 1 Core Concepts (12%)

1.1 Identify how Palo Alto Networks products work together to improve PAN-OS services

1.1.1 Security components
1.1.2 Firewall components
1.1.3 Panorama components
1.1.4 PAN-OS subscriptions and the features they enable.
1.1.5 Plug-in components
1.1.6 Heatmap and BPA reports
1.1.7 Artificial intelligence operations (AIOps)/Telemetry
1.1.8 IPv6
1.1.9 Internet of things (IoT)

1.2 Determine and assess appropriate interface or zone types for various environments

1.2.1 Layer 2 interfaces
1.2.2 Layer 3 interfaces
1.2.3 Virtual wire (vwire) interfaces
1.2.4 Tap interfaces
1.2.5 Sub interfaces
1.2.6 Tunnel interfaces
1.2.7 Aggregate interfaces
1.2.8 Loopback interfaces
1.2.9 Decrypt mirror interfaces
1.2.10 VLAN interfaces

1.3 Identify decryption deployment strategies

1.3.1 Risks and implications of enabling decryption.
1.3.2 Use cases
1.3.3 Decryption types
1.3.4 Decryption profiles and certificates
1.3.5 Create decryption policy in the firewall.
1.3.6 Configure SSH Proxy

1.4 Enforce User-ID

1.4.1 Methods of building user-to-IP mappings
1.4.2 Determine if User-ID agent or agentless should be used.
1.4.3 Compare and contrast User-ID agents.
1.4.4 Methods of User-ID redistribution
1.4.5 Methods of group mapping
1.4.6 Server profile & authentication profile

1.5 Determine how and when to use the Authentication policy

1.5.1 Purpose of, and use case for, the Authentication policy
1.5.2 Dependencies
1.5.3 Captive portal versus Global Protect (GP) client

1.6 Differentiate between the fundamental functions that reside on the management plane and data plane

1.7 Define multiple virtual systems (multi-vsys) environment

1.7.1 User-ID hub
1.7.2 Inter-vsys routing
1.7.3 Service routes
1.7.4 Administration

Domain 2 Deploy and Configure Core Components (20%)

2.1 Configure management profiles

2.1.1 Interface management profile
2.1.2 SSL/TLS service profile

Task 2.2 Deploy and configure Security profiles

2.2.1 Custom configuration of different Security profiles and Security profiles groups
2.2.2 Relationship between URL filtering and credential theft prevention
2.2.3 Use of username and domain name in HTTP header insertion
2.2.4 DNS Security
2.2.5 How to tune or add exceptions to a Security profile.
2.2.6 Compare and contrast threat prevention and advanced threat prevention.
2.2.7 Compare and contrast URL Filtering and Advanced URL Filtering

2.3 Configure zone protection, packet buffer protection & DoS protection

2.3.1 Customized values versus default settings
2.3.2 Classified versus aggregate profile types.
2.3.3 Layer 3 and Layer 4 header inspection

2.4 Design the deployment configuration of a Palo Alto Networks firewall

2.4.1 Advanced high availability (HA) deployments
2.4.2 HA pair
2.4.3 Zero Touch Provisioning (ZTP)
2.4.4 Bootstrapping

2.5 Configure authorization, authentication and device access

2.5.1 Role-based access control for authorization
2.5.2 Different methods used to authenticate.
2.5.3 The authentication sequence
2.5.4 The device access method

2.6 Configure and manage certificates

2.6.1 Usage
2.6.2 Profiles
2.6.3 Chains

2.7 Configure routing

2..7.1 Dynamic routing
2.7.2 Redistribution profiles
2.7.3 Static routes
2.7.4 Path monitoring
2.7.5 Policy-based forwarding
2.7.6 Virtual router versus logical router

2.8 Configure NAT

2..8.1 NAT policy rules
2.8.2 Security rules
2.8.3 Source NAT
2.8.4 No NAT
2.8.5 Use session browser to find NAT rule name.
2.8.6 U-Turn NAT
2.8.7 Check HIT counts

2.9 Configure site-to-site tunnels

2.9.1 IPSec components
2.9.2 Static peers and dynamic peers for IPSec
2.9.3 IPSec tunnel monitor profiles
2.9.4 IPSec tunnel testing
2.9.5 Generic Routing Encapsulation (GRE)
2.9.6 One-to-one and one-to-many tunnels
2.9.7 Determine when to use proxy IDs

2.10 Configure service routes

2.10.1 Default
2.10.2 Custom
2.10.3 Destination
2.10.4 Custom routes for different vsys versus destination routes
2.10.5 How to verify service routes.

2.11 Configure application based QoS

2.11.1 Enablement requirements
2.11.2 QoS policy rule
2.11.3 Add DSCP/TOS component.
2.11.4 QoS profile
2.11.5 Determine how to control bandwidth use on a per-application basis.
2.11.6 Use QoS to monitor bandwidth utilization

Domain 3 Deploy and Configure Features and Subscriptions (17%)

3.1 Configure App-ID

3.1.1 Create security rules with App-ID
3.1.2 Convert port and protocol rules to App-ID rules
3.1.3 Identify the impact of application override to the overall functionality of the firewall.
3.1.4 Create custom apps and threats.
3.1.5 Review App-ID dependencies

3.2 Configure Global Protect

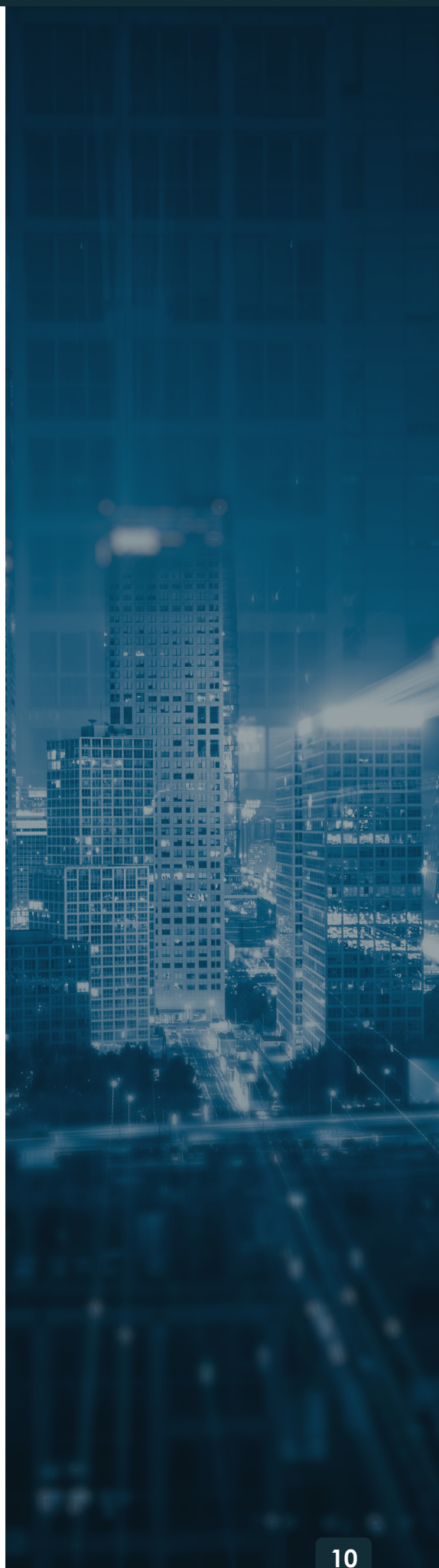
3.2.1 Global Protect licensing.
3.2.2 Configure gateway and portal.
3.2.3 Global Protect agent.
3.2.4 Differentiate between logins methods.
3.2.5 Configure Clientless VPN
3.2.6 Host information profile (HIP)
3.2.7 Configure multiple gateway agent profiles.
3.2.8 Split tunneling

3.3 Configure decryption

3.3.1 Inbound decryption
3.3.2 SSL forward proxy
3.3.3 SSL decryption exclusions
3.3.4 SSH proxy

3.4 Configure User-ID

3.4.1 User-ID agent and agentless
3.4.2 User-ID group mapping
3.4.3 Shared User-ID mapping across virtual systems
3.4.4 Data redistribution
3.4.5 User-ID methods
3.4.6 Benefits of using dynamic user groups in policy rules
3.4.7 Requirements to support dynamic user groups.
3.4.8 How Global Protect internal and external gateways can be used.



3.5 Configure WildFire

3.5.1 Submission profile
3.5.2 Action profile
3.5.3 Submissions and verdicts
3.5.4 Signature actions
3.5.5 File types and file sizes
3.5.6 Update schedule
3.5.7 Forwarding of decrypted traffic

3.6 Configure Web Proxy

3.6.1 Transparent proxy
3.6.2 Explicit proxy

Domain 4 Deploy and Configure Firewalls Using Panorama (17%)

4.1 Configure templates and template stacks

4.1.1 Components configured in a template.
4.1.2 How the order of templates in a stack affects the configuration push to a firewall
4.1.3 Overriding a template value in a stack.
4.1.4 Configure variables in templates.
4.1.5 Relationship between Panorama and devices as pertaining to dynamic. updates versions, policy implementation, and/or HA peers

4.2 Configure device groups.

4.2.1 Device group hierarchies
4.2.2 Identify what device groups contain.
4.2.3 Differentiate between different use cases for pre-rules, local rules, the default rules, and post-rules
4.2.4 Identify the impact of configuring a primary device.
4.2.5 Assign firewalls to device groups

4.3 Manage firewall configurations within Panorama.

4.3.1 Licensing
4.3.2 Commit recovery feature
4.3.3 Automatic commit recovery
4.3.4 Commit types and schedules
4.3.5 Config backups
4.3.6 Commit type options
4.3.7 Manage dynamic updates for Panorama and Panorama-managed devices.
4.3.8 Software and dynamic updates
4.3.9 Import firewall configuration into Panorama
4.3.10 Configure log collectors.
4.3.11 Check firewall health and status from Panorama
4.3.12 Configure role-based access on Panorama.

Domain 5 Manage and Operate (16%)

5.1 Manage and configure Log Forwarding

5.1.1 Identify log types and criticalities.
5.1.2 Manage external services.
5.1.3 Create and manage tags.
5.1.4 Identify system and traffic issues using the web interface and CLI tools.
5.1.5 Configure Log Forwarding profile and device log settings.
5.1.6 Log monitoring
5.1.7 Customize logging and reporting settings.

5.2 Plan and execute the process to upgrade a Palo Alto Networks system

5.2.1 Single firewall
5.2.2 HA pairs
5.2.3 Panorama push
5.2.4 Dynamic updates

5.3 Manage HA functions.

5.3.1 Link monitoring
5.3.2 Path monitoring
5.3.3 HA links
5.3.4 Failover
5.3.5 Active/active and active/passive
5.3.6 HA interfaces
5.3.7 Clustering
5.3.8 Election setting

6.1 Troubleshoot site-to-site tunnels.

6.1.1 IPSec
6.1.2 GRE
6.1.3 One-to-one and one-to-many tunnels
6.1.4 Route-based versus policy-based remote hosts
6.1.5 Tunnel monitoring

6.2 Troubleshoot interfaces.

6.2.1 Transceivers
6.2.2 Settings
6.2.3 Aggregate interfaces, LACP
6.2.4 Counters
6.2.5 Tagging

6.3 Troubleshoot decryption.

6.3.1 Inbound decryption
6.3.2 SSL forward proxy
6.3.3 SSH proxy
6.3.4 Identify what cannot be decrypted &configure exclusions and bypasses.
6.3.5 Certificates

6.4 Troubleshoot routing.

6.4.1 Dynamic routing
6.4.2 Redistribution profiles
6.4.3 Static routes
6.4.4 Route monitoring
6.4.5 Policy-based forwarding
6.4.6 Multicast routing
6.4.7 Service routes

6.5 General Troubleshooting

6.4.1 Logs
6.4.2 Packet capture (pcap)
6.4.3 Reports

6.6 Troubleshoot resource protections.

6.6.1 Zone protection profiles
6.6.2 DoS protections
6.6.3 Packet buffer protections

6.7 Troubleshoot Global Protect

6.7.1 Portal and Gateway
6.7.2 Access to resources
6.7.3 Global Protect client.

6.8 Troubleshoot policies.

6.8.1 NAT
6.8.2 Security
6.8.3 Decryption
6.8.4 Authentication

6.9 Troubleshoot HA functions.

6.9.1 Monitor
6.9.2 Failover triggers

- Use Firewall tools, including the WebUI and CLI, to investigate networking issues.
- Follow proven troubleshooting methodologies that are specific to individual features.
- Understand the Flow-Logic used by the Next-Generation Firewall
- Learn how to configure and enable Packet Capture and advanced Packet-Level Diagnostic Features
- Identify necessary System Daemons and their logs to resolve various real-life scenarios.
- Solve numerous advanced, scenario-based challenges.
- Troubleshoot common issues related to firewall deployment.
- Troubleshoot connectivity problems.
- Troubleshoot policy and NAT-related Issues.
- Troubleshoot User-D
- Troubleshoot Site-to-Site VPN problems.
- Troubleshoot Global Protect™ related issues.
- Identify performance problems.
- How to use the Customer Support Portal

TRAINER'S PROFILE

- IP Rulers is managed by an expert team of trainers with over 20 years' experience in the industry and in hands-on training.
- All the trainers have multiple CCIEs in their respective areas of interest.
- Individual trainers' profiles can be provided upon request by email, along with demos and LinkedIn profiles.
- Online and classroom demos are also available upon request

LAB INFRASTRUCTURE

IP Rulers has a fully equipped Palo Alto network lab, specially designed for the PCNSA, PCNSE training, with an enhanced lab topology that represent real world network. Students will have the following equipment and software configured for their training; they may also get the chance to see newer hardware and software during this period.

PALO ALTO NETWORKS EQUIPMENT AND SOFTWARE LIST

PHYSICAL EQUIPMENT

- ***PALO ALTO NETWORKS PA-220***
- ***PALO ALTO NETWORKS PA-440***

VIRTUAL MACHINES

- ***PALO ALTO NETWORKS VM-50***
- ***PALO ALTO NETWORKS PAN-OS 11.0***
- ***PALO ALTO NETWORKS PANORAMA VIRTUAL APPLIANCE 11.0***

SUPPORTING MACHINES

- ***TEST PC: WINDOWS 10 ENTERPRISE***
- ***AD/DNS: WINDOW SERVER 2016***
- ***LINUX KALI***

MODE OF TRAINING

Classroom-based Training	Online Training	Corporate Training
Go old-school. Make friends and have fun, just like elementary grades. Follow lectures, turn in assignments and appear for exams in campus-style!	Sit in the comfort of your home as you move through the course. Instructors will guide you in predetermined sessions. Hundreds of supporting videos available, in case you want to outshine yourself.	Lectures and hands-on training for office employees, in the comfort of their own office. Sponsored by employers to push up their employees above the market competence.

One-on-One Training	Fast Track Training	Private Group Training
An instructor will train you in private – without any external intrusion. Ideal if you want to progress on your own. Schedule your classes according to your own timeline as you advance, without disruption to your daily routine.	No time to follow regular class timeline? Go fast track – speed through the course, whether it be alone, or online, in groups, on an accelerated timescale, to give the icing on the cake.	You and your friends like to be together in a class, but without any outsiders? You've got it! Feel as if you have hired your own instructor. A way to combat shyness, with the comfort your friend-circle.

Lab workshop training
This would be helpful for those who are already familiar with the technologies in depth with hands-on to clear their ccie lab exam.

TARGET AUDIENCE

Security Administrators, Security Operations Specialists, Security Analysts, Security Engineers, and Security Architects

BENEFITS

The Palo Alto Network certification covers how to design, deploy, operate, manage, and troubleshoot Palo Alto Networks Next-Generation Firewalls.

PCNSE is an expert-level certification that validates your knowledge of the security operating platform, ensuring you can use its full functionality to benefit your company and demonstrate your expertise.

The PCNSE certification can advance your organization's career or even provide opportunities to work for a larger, more prominent company. It can also help you transition to new roles and responsibilities within the technology industry, such as network security architecture or cybersecurity consulting.

IP Rulers, 201, Wasl Business Central. 29B street, Sheikh Rashid Road.Port Saeed, Dubai.

www.iprulers.com

training@iprulers.com

+971559454771 | +97143346660