Network Security Engineering with Palo Alto

Prepare for the Palo Alto Certified Network Security Professional (PCNSP) exam, and learn to deploy and support Palo Alto's full network security ecosystem. This course teaches you how Strata firewalls, Prisma Access, and Prisma SD-WAN fit together in real-world on-prem, cloud, and hybrid environments. You'll learn about deployment, policy management, decryption, and remote user security. This Palo Alto network security professional training helps you learn practical skills with hardware and cloud tools including local Firewall management, as well as cloud management via tools like Strata Cloud Manager (SCM), helping you stand out as a certified network security professional.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Palo Alto FW Factory Reset & Setup

Overview of Initial Build

Reset and Configure the Management Plane

Cleanup, and Create L3 Zones

Configure Data Plane Interfaces

Configure DHCP Services

Configure Default Route

Configure Address Translation

Configure Basic Security Policy Rule

Troubleshooting

Palo Alto FW Setup Using Trunking

Intro to Palo Alto FW Setup Using Trunking

Trunking and Sub-Interface Overview

Configure the Management Plane

Cleanup, and Create L3 Zones on FW-B

Configure Data Plane Interfaces on FW-B

Configure DHCP Services on FW-B

Configure Default Route on FW-B

Configure NAT-PAT on FW-B

Configure Basic Security Policy Rule on FW-B

Verify and Packet Capture

Troubleshooting

Traffic Flow & Forwarding Logic

Intro to Traffic Flow & Forwarding Logic on the Palo Alto Firewall

Traffic Flow & Forwarding Logic Overview

The Forwarding Decision Chain

Why “A Route Exists” Isn’t the Same as “It Will Work.”

Demonstration of the Longest Match Rule

No Session, No Log- When Forwarding Fails Before Policy

Intra-Zone Traffic

Troubleshooting Scenario

Security Policy Evaluation

Intro to Palo Alto Firewall Security Policy Evaluation

Security Policy Evaluation Overview

Adding Tags to Colorize Zones

Policy Evaluation and Hit Counts

Security Policy Rule DMZ to Outside

Rule Order and Shadowed Rules

Verifying Rule Hits and Response from Firewall

Troubleshooting Scenario

PA FW Log and Session Correlation

Introduction to Log and Session Correlation on the Palo Alto Firewall

Log and Session Correlation Overview

Historical Evidence on the Firewall – Traffic Logs

Current Flows - Sessions

Changing Policy With Existing Sessions

Troubleshooting Scenario

PA FW Source Address Translation

Intro to Source NAT-PAT

Source NAT-PAT Overview

Order of Operations

Proving NAT with Evidence

Multiple SPs and Default Routes

NAT Policies for Multiple SPs

Troubleshooting Scenario

Palo Alto Destination NAT

Intro to PA FW Destination NAT

Destination NAT/PAT Overview

DNAT and Security Policies

Verifying DNAT

Source NAT with Bi-Directional Support

Port-Forwarding (PAT) is Still Destination NAT

Troubleshooting Scenario

Palo Alto Networks App-ID

Intro to PA FW App-ID

App-ID Fundamentals

When App-ID is Known vs Incomplete or Unknown

App-ID Granularity and Shifts Mid-Session

Using Policy Optimizer to Identify Apps Seen

Troubleshooting Scenario

Palo Alto User-ID

Intro to Palo Alto User-ID

User-ID Overview

Game Plan for User-ID

Configuring User-ID

Verify User-ID

Group Mappings

Testing Group Mapping in Policy

User-ID Troubleshooting Scenario

SSL Forward Proxy Essentials

Introduction to Palo Alto SSL Forward Proxy

TLS and Decryption Overview

Demonstration Without SSL Forward Proxy

Configure Certs for Trusted and Untrusted

Configure Decryption Profiles and Rules

Testing SSL Forward Proxy

Troubleshooting Scenario

Protecting Public-Facing Apps

Intro to Inbound SSL Inspection

SSL Inbound Inspection Overview

Game Plan for SSL Inbound Inspection

Cert Management for SSL Inbound Inspection

Create Decryption Profile and Policy

Test and Verify Inbound SSL Inspection

Validation of SSL Inbound Inspection

Security Profiles and Updates

Intro to Security Profiles, Updates, and CDSS

Security Profiles, Updates, and CDSS Overview

Creating and Applying Security Profiles

Building and Applying a Profile Stack

Verifying the Results of Applied Security Profiles

Content and Software Updates

Validation for Security Profiles

Keeping the Lights On

Intro to HA, Certificates and Operations

HA, Certificates, and Operations Overview

HA Configuration and Operations

Testing and Validating HA Operations

Digital Certificates Recap

Backups and Configuration Management

System Health and Monitoring

Validation for HA-Certs-Logs

Meet Strata Cloud Manager (SCM)

Intro to Strata Cloud Manager

Management Options

WEEK 2

Folders, Inheritance, and Variables

Onboarding a FW to SCM

Using Central Policies Pushed from SCM

Testing the Data Plane

Troubleshooting Inheritance

Authoring Policies in the Cloud

Intro to Building NGFW Policies in SCM

Policy Building Overview

Region-01 Configuration Review and Testing

Snippet Configuration Review and Testing

Creation and configuration of Region-03

Testing and verification of Region-03

Troubleshooting

SSL Decryption at Scale with SCM

Intro to SSL Decryption at Scale with SCM

SSL Decryption at Scale with SCM Overview and Game Plan

Managing Decryption Certificates in SCM

Creating Decryption Policies and Profiles in SCM

Verifying SSL Decryption in Multiple Regions

Verification of FW-C

Summarizing What Can Go Wrong

Palo Alto Zero Trust

Intro to Palo Alto Zero Trust

Zero Trust Overview

Zero Trust Game Plan

Creating an AD Security Policy Rule

Configure Security Policy Rules for HR and IT Apps

Testing and Verifying Policies

Adding Decryption for Visibility

Troubleshooting Exercise