

Palo Alto Networks Certified Network Security Administrator (PCNSA)

This Palo Alto Networks Certified Network Security Administrator (PCNSA) training covers how to manage Palo Alto's security platform and architecture to understand security best practices. The PCNSA focuses on installing, maintaining, and managing Palo Alto Networks' next-generation firewalls to protect networks. To learn how to navigate firewalls on Palo Alto's security OS, an extensive background in digital security isn't a prerequisite for our PCNSA training.

[CBT Nuggets course material](#) →

WEEK 1

Building a Palo Alto Firewall Lab in ESXi

154 min.

Intro to Building a Lab using ESXi	1
ESXi Based Lab Overview	12
Deploy the Firewall VM	4
ESXi Networking	3
Lab Routing with Vynos	4
Setting up Basic FW Management	10
Configure L3 Zones, Virtual Routers, and Interfaces	13
LAB Clients and Servers	10

Configuring Palo Alto Firewall Management Access

Overview	1
Intro to Configuring Palo Alto Firewall Management Access	1
Management Access Overview	8
Using the CLI for Management	16
Using the GUI for Management	4
Using APIs for Management	4
Access Restrictions	12
Service Routes	5

Configuring Palo Alto IPv4 FW Routing

Overview	1
Intro to Palo Alto IPv4 FW Routing	1
Palo Alto FW IPv4 Routing Overview	7
Adding Directly Connected Routes	9
Adding a Static Default Route	9
Adding a Second Default Route Using ISP-B	7

Using Path Monitoring 10

WEEK 2

157 min.

Dynamic Routing Protocols Overview 10

Configure and Verify RIP 4

Configure and Verify OSPF 4

Configure and Verify BGP 5

Using Source NAT on the Palo Alto FW

Overview 1

Intro to Address Translation on the Palo Alto FW 1

Address Translation Overview 17

Source NAT Game Plan 6

Source NAT with Static IP (SIP) 15

Source NAT with Dynamic IP (DIP) 12

Source NAT with Dynamic IP and Port (DIPP) 11

Configuring Multiple Palo Alto FW Admins

Overview 1

Into to Multiple Palo Alto FW Admins 1

Multiple Firewall Admins Overview 8

Configure an LDAP Server Profile 6

Configure an Authentication Profile 3

Creating a New Admin Account 7

Using an Authentication Sequence 7

Working with Locks 7

Managing Configurations 13

Understanding Palo Alto FW Security Policy Fundamentals

Overview 1

Intro to Security Policy Fundamentals 1

Security Policy Fundamentals Overview 13

WEEK 3

152 min.

Confirm the Lab Topology 5

Create a Basic Security Policy 9

Include IPv4 as Part of the Security Policy Rule 4

Using Address Objects in Security Policy 7

Adding Color Coding to Zones 4

Adding Logging to the Interzone-default Rule 7

Using Applications in Security Policies 13

Stateful Firewalls 4

Using Destination NAT on the Palo Alto FW

Overview 1

Intro to Destination NAT 1

Destination NAT Overview 13

Destination NAT Game Plan 6

Destination NAT with Static IP 15

Port-based Destination NAT 9

DNAT for DNS Services Example 10

DNAT Using FQDN (Dynamic IP) 14

Using Palo Alto FW SSL/TLS Decryption

Overview 1

Intro to SSL Forward Proxy 2

SSL-TLS Decryption Overview	9
SSL Decryption Game Plan	4
Configure FW to Trust Corporate CA	3
Create Signing Cert for FW	9

WEEK 4

151 min.

Create Decryption Profile	3
Create Decryption Policy Rules	8
Testing SSL Decryption	8
Adding a Cert for FW Management	10

Using Palo Alto FW URL Filtering

Overview	1
Intro to URL Filtering	1
URL Filtering Overview	9
URL Category Directly in Security Policy Rule	8
Custom URL Categories	6
External Dynamic Lists	14
URL Filtering Security Profiles	14
Modifying the URL Filtering Profile	5

Using a Palo Alto FW Virtual Wire

Overview	1
Intro to Palo Alto FW Virtual Wire	1
Virtual Wire Overview	14
Virtual Wire Between Clients and a Server	8
Permitting Traffic Through the Virtual Wire	6
Adding NAT to the Virtual Wire	8

Virtual Wire Between Clients Their Gateway	10
Creating a Security Policy Rule	5
Troubleshooting Virtual Wire and DHCP	7

Using Palo Alto FW App IDs

Overview	1
----------	---

WEEK 5

156 min.

Intro to Palo Alto FW App-IDs	1
App-ID Overview	10
Application Object Fundamentals	8
App-IDs in Security Policy Rules	3
Application Groups in Security Policy Rules	9
Application Filters	8
Grouping Rules by Tag	6
Rule Shadowing	6

Using Palo Alto FW Antivirus and WildFire

Overview	1
Intro to Palo Alto FW Antivirus and WildFire	1
Antivirus and Wildfire Overview	6
Game Plan for AV and WildFire	6
Creating an Antivirus Profile	6
Using the Antivirus Profile in a Security Policy	11
Creating a WildFire Analysis Profile	3
Using the WildFire Analysis Profile in Policy	2
Configure WildFire Settings	3
Antivirus and WildFire Updates	6

Verifying WildFire Analysis 9

Using PA FW Anti-Spyware and Protection Profiles

Overview 1

Intro to Anti-Spyware & Vuln. Protection 1

Anti-Spyware and Vuln. Protection Overview 9

Add Access to DMZ from Outside 3

Injection Attack Demonstration 7

Create a Vulnerability Protection Profile 6

Testing a Vulnerability Protection Profile 12

Anti-Spyware Profiles 10

WEEK 6

Managing Palo Alto FW Updates

152 min.

Overview 1

Intro to Managing Palo Alto FW Updates 1

Firewall Updates Overview 6

Bringing Up a New FW 7

Installing Dynamic Updates 13

Using Application Filters for New App-IDs 4

Update PAN-OS on the FW 15

Using Palo Alto FW L2, TAP, & VLAN Interfaces

Overview 1

Intro to L2, VLAN, & Sub-Interfaces 1

L2, VLAN, & Sub-Interfaces Overview 19

Create VLANs and Zones 5

Create L2 and Sub-Interfaces 6

Create Security Policy Rules 13

Create VLAN L3 Interfaces 7

Testing VLAN Interfaces 6

TAP Interfaces 10

Using Panorama to Manage Palo Alto FWs

Overview 1

Intro to Panorama 1

Panorama Overview 11

Deploying the Panorama VM 6

Using a Cert for Management 8

Adding Firewalls to Panorama 7

WEEK 7

153 min.

Creating Templates 13

Creating Template Stacks 10

Using Objects in Devices Groups 12

Policies in Device Groups 5

Importing FW Configurations 9

Configuring Palo Alto FW User-ID

Overview 1

Intro to Palo Alto FW User-ID 1

User-ID Overview 9

User-ID Game Plan 5

Setting up User-ID 9

Adding User-ID in Security Policy Rules 6

Add LDAP and Group Mapping 6

Using Groups in Security Policy 9

Optimizing Palo Alto FW Security Policies

Overview	1
Intro to Optimizing PA FW Security Policies	1
Policy Optimization Overview	7
Adding Deny Rules Matching Dynamic Lists	5
Testing Policy Matches	6
The Policy Optimizer	6
Using Temporary Rules	11
Using Logs and Reports	10
Using the Application Command Center (ACC)	9

WEEK 8

1 min.