



**Keith Cantillon**

Senior Academy Training  
Engineer at Palo Alto Networks

**Palo Alto Networks®  
Cybersecurity Academy**

**Formando a los  
profesionales de la  
ciberseguridad del futuro**



**Amador Gabaldón**

Tech Manager en PUE Academy



# Palo Alto Networks® Cybersecurity Academy

Formando a los profesionales de la ciberseguridad del futuro

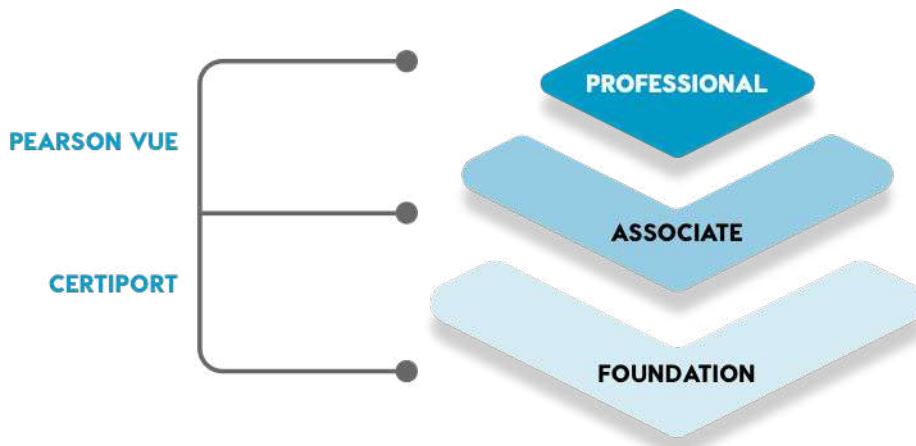
# ¿Qué es PUE Academy?

**Acercamos la formación y certificación tecnológica al ámbito educativo** con acciones formativas al profesorado, a las instituciones académicas y a sus alumnos a través de la gestión e implementación de las iniciativas académicas de las principales organizaciones y multinacionales del sector TIC.

La **capacitación de la docencia**, así como la **empleabilidad** y **reconocimiento profesional** de los alumnos formados, son nuestros máximos objetivos.



# Full-service solutions for the skilling journey



LEARN ▶ PRACTICE ▶ CERTIFY



# Nuestros servicios a la comunidad educativa TIC

- **Distribución, gestión e implementación** de las iniciativas académicas de las multinacionales de referencia en el sector tecnológico.
- **Soporte, apoyo y asesoramiento** en su despliegue.
- **Formación** oficial para docentes, staff técnico y estudiantes.
- **Acceso a recursos** docentes y material de estudio oficial.
- Servicios para facilitar la **certificación** de docentes y estudiantes: plataforma online PUE Certification Service y Certification Credits.
- Participación de los centros en las **comunidades educativas** de los diversos programas educativos y de certificación.
- **Recursos de marketing** para posicionar al centro en sus figuras oficiales.



# CYBERSECURITY ACADEMY

Educating the  
**Workforce of Tomorrow**





# CYBERSECURITY ACADEMY

## Our Mission

Educate the workforce of tomorrow.

To prepare students for successful careers in cybersecurity and address the needs of our customers around the globe.

# The Cybersecurity Academy Network

100+  
Countries



200+  
High Schools



2600+  
Academies



500k+  
Students  
engaged

# Our Commitment to Diversity

---

- We believe that innovation can't succeed without **appropriate representation** and an **empowered workforce**.
- Our pledge is to create **more and broader pathways** into cybersecurity.



**Innovation Needs Diversity to Succeed**

# CYBERSECURITY ACADEMY

"NOTHING WORTHWHILE WAS

EVER ACHIEVED WITHOUT EFFORT."

## Academy Curriculum and Programs



# Academic Curriculum

## INTRODUCTORY

**Cybersecurity**  
Foundation

**Network Security**  
Fundamentals

**Cloud Security**  
Fundamentals

**Security Operations**  
Fundamentals

**Secure Access Service**  
Edge Fundamentals

## ADVANCED

**Firewall Essentials**

**Cloud Security Automation**

**Security Operations**  
Configuration

**Secure Access Service**  
Edge Architecture

**Note:** All academic courses align to the U.S. National Initiative for Cybersecurity Education ([NICE](#)) framework and Cybersecurity Work Roles.

# Introductory Course Modules

## Cybersecurity Foundation

1. Cybersecurity Landscape
2. Cybersecurity Threats
3. Cybersecurity Attack Types
4. Cybersecurity Design Models
5. Security Operating Platform

## Cloud Security Fundamentals (Prisma)

1. Cloud, Virtualization, Storage
2. Cloud Native Security
3. Cloud and Data Center Security
4. Mobile and Cloud Security
5. Secure the Cloud (Prisma)

## Secure Access Service Edge (SASE) Fundamentals

1. SASE Review
2. Cloud Access Security Broker (CASB)
3. Cloud Secure Web Gateway (CSWG)
4. Autonomous Digital Experience Management (ADEM)

## Network Security Fundamentals (Strata)

1. The Connected Globe
2. IP Addressing
3. Packet Encapsulation
4. Network and Endpoint Security
5. Network Security Principles

## Security Operations Fundamentals (Cortex)

1. Elements and Process of SOC
2. CSOC Infrastructure and Automation
3. Advanced Endpoint Protection
4. Threat Prevention and Intelligence
5. Secure the Future (Cortex)

# Lab Overview for Fundamentals Courses

Cybersecurity Foundation	Network Security Fundamentals	Cloud Security Fundamentals	Security Operations Fundamentals
<p><b>Lab 01:</b> Configuring TCP/IP and a Virtual Router</p> <p><b>Lab 02:</b> Malware Analysis</p> <p>* <b>Lab 03:</b> Creating a Zero Trust Environment</p> <p><b>Lab 04:</b> Configuring Authentication</p> <p><b>Lab 05:</b> Using Two-Factor Authentication to Secure the Firewall</p> <p><b>Lab 06:</b> Allowing Only Trusted Applications</p> <p>* Also included in the <b>SASE Fundamentals</b> course.</p>	<p><b>Lab 01:</b> Configuring DHCP</p> <p><b>Lab 02:</b> Configuring Virtual IP Addresses</p> <p><b>Lab 03:</b> Creating Packet Captures</p> <p><b>Lab 04:</b> Analyzing Packet Captures</p> <p><b>Lab 05:</b> Managing Certificates</p> <p><b>Lab 06:</b> Decrypting SSH Traffic</p> <p><b>Lab 07:</b> Decrypting SSL Inbound Traffic</p> <p><b>Lab 08:</b> Backing up Firewall Logs</p>	<p><b>Lab 01:</b> Protecting Sensitive Data</p> <p><b>Lab 02:</b> Preventing Internet Threats with File Blocking</p> <p><b>Lab 03:</b> Container Network Security</p> <p><b>Lab 04:</b> Denying International Attackers</p> <p>* <b>Lab 05:</b> Configuring HIP for Global Protect</p> <p><b>Lab 06:</b> Container Vulnerability Scanning</p> <p>* Also included in the <b>SASE Fundamentals</b> course.</p>	<p><b>Lab 01:</b> Network Traffic Analysis</p> <p><b>Lab 02:</b> Using the Application Command Center to Find Threats</p> <p><b>Lab 03:</b> Analyzing Firewall Logs</p> <p><b>Lab 04:</b> Log Forwarding to Linux</p> <p><b>Lab 05:</b> Stopping Reconnaissance Attacks</p> <p><b>Lab 06:</b> Securing Endpoints using Vulnerability Profiles</p> <p><b>Lab 07:</b> Threat Intelligence</p> <p><b>Lab 08:</b> Using Dynamic Block Lists</p>

# Entry-Level Certification



**PC CET**

Palo Alto Networks Certified  
Cybersecurity Entry-Level Technician

## INTRODUCTORY

**Cybersecurity**  
Foundation

**Network Security**  
Fundamentals

**Cloud Security**  
Fundamentals

**Security Operations**  
Fundamentals

**Secure Access Service**  
Edge Fundamentals

# Advanced-Level Certification



**PCNSA**

Palo Alto Networks Certified  
Network Security Administrator

**ADVANCED**

Firewall Essentials

Cloud Security Automation

Security Operations  
Configuration

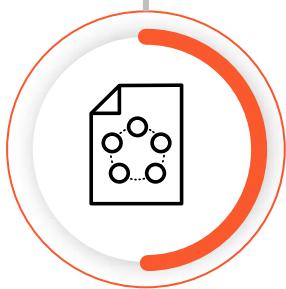
Secure Access Service  
Edge Architecture



**Plus...** access to all Palo Alto Networks Certifications

# Academy Partner Benefits

Academy Partners receive **free access** to:



## Curriculum

Student course materials

Aligns to the NICE framework



## Faculty Training

Complete trainings for selected courses

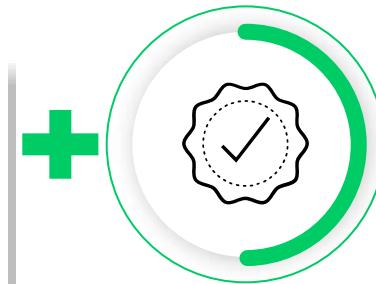
- Self-paced, asynchronous

Begin teaching!



## Virtual Firewalls

VM-50s (fully licensed) for your course labs or competition preparation



## Discount Certifications

Free and discounted Palo Alto Networks Certifications

No cost study guides and practice exams

# Getting Started

Complete the PAN Cybersecurity Academy Application

1

2

3

4

Welcome email is sent with next steps including the course enrollment and program onboarding.

Faculty completes the curriculum training for the courses they plan to teach.

**Begin teaching!**

# Programs and Competitions



## Secure the Future

Company sponsored competition for college students to demonstrate their skills!

Finalists are eligible to interview for Palo Alto Networks opportunities and a \$10,000 cash prize.



## CCDC

Top 1000 cyber students in the US compete in the Collegiate Cyber Defense Competition (CCDC).

As **Technical Sponsor**, we provide custom courseware, Next Generation Firewalls and financial support.

# Programs and Competitions



## Virginia Department for Blind and Visually Impaired (VDBVI)

We support this important and overlooked workforce.

We customized our labs to make cybersecurity learning and career opportunities possible.



## Cyber Madness

**Statewide high school competition in North Dakota,** where students configure (next generation) firewalls for scholarships and prizes!

## ....and MORE:

- NICE K-12 Conference
- Cyber 9/12 Strategy Challenge
- Cyber Education Discovery Forum
- CyberCon at Bismarck State
- Turtle Mountain Community College Cybersecurity Camp

# Cybersecurity Survival Guide



## Fundamental Principles and Best Practices



Seventh Edition | June 2023

paloalto  
CYBERSECURITY  
ACADEMY

CYBERSECURITY SURVIVAL GUIDE

SEVENTH EDITION

**Module 1 – Fundamentals of Cybersecurity**

**Knowledge Objectives**

- Discuss modern computing trends, application threat vectors, cloud computing and software-as-a-service (SaaS) application challenges, data protection and privacy regulations and standards, and recent cyberattack.
- Explain attacker motivations and the Cyberattack Lifecycle.
- Describe cyberattack techniques and types, including malware, vulnerabilities, exploits, spearphishing, phishing, botnets and botnets, advanced persistent threats, and DDoS attacks.
- Explain various cybersecurity models, concepts, and principles, including perimeter-based security and the Zero Trust model.
- Discuss the key capabilities of the Security Operating Pattern and its key components.

**1.0 Cybersecurity Landscape**

The modern cybersecurity landscape is rapidly changing and facing an environment fraught with advanced threats and increasingly sophisticated threat actors. This section describes computing trends that are shaping the cybersecurity landscape, application frameworks and objects (or threat vectors), cloud computing and SaaS application security challenges, various information security and data protection regulations and standards, and some recent cyberattack analysis.

**Note**

The terms "enterprise" and "organization" are used throughout this guide to describe organizations, networks, and applications in general. The use of these terms is not intended to exclude other types of organizations, networks, or applications, and should be understood to include not only large businesses and enterprises but also small and medium size businesses (SMBs), government, state-owned enterprises (SOEs), public services, military, healthcare, and research, among others.

**Key Terms**

An actor (or threat vector) is a person or tool that can attack users or target a network.

CYBERSECURITY SURVIVAL GUIDE, SEV EDITION | 1

Unique split framework, enabling continuous update to ensure that the latest local policies to always reflect.

**Advanced Threat Protection**

Sophisticated attacks that use multiple legitimate applications and processes for malicious operations have become more common, are hard to detect, and require deeper visibility to correlate malicious behavior. For behavior-based protection to be effective, including behavioral threat protection, it must correlate activity within the network processes, so that the understand everything happening on the network. The Cortex XDR agent spans across behavioral-based protection in a few different ways:

- Indirect attacks often comprise multiple events that occur in the system. By itself, each event may not be suspicious enough to trigger an alert, but when combined with other events, they work together to achieve their goal. Stringing together, however, they may represent a malicious event flow.
- With behavioral threat protection, the Cortex XDR agent can detect and act on malicious chains of events that span multiple hosts and endpoints. It correlates multiple events from the same user registry activity (see Figure 4-6). When the Cortex XDR agent detects a breach, it executes a policy-based action, such as "Block" or "Silent." In addition, it respects the behavior of the entire environment by blocking the entire chain of events that occurred in the malicious activity chain. The Cortex XDR agent can stop suspicious files that were involved in malicious flows. Behavioral threat protection is ideal for preventing against script-based and fileless attacks.

**Figure 4-6**

Advanced threat protection with Cortex XDR

Cortex XDR Prevents Block threats on all hosts in the environment and correlates them to identify a long-term attack on endpoint 1. Identify long-term attack on endpoint 1. Determine user's behavior. Detect malicious activity chain. Block threats on all hosts in the environment and correlate them to identify a long-term attack on endpoint 1. Determine user's behavior. Detect malicious activity chain. Action: Block or silent. Stop defining attacks with user's behavior over time.

CYBERSECURITY SURVIVAL GUIDE, SEV EDITION | 287

Our annual **Cybersecurity Survival Guide** free publication covers fundamental principles and best practices, including **Cybersecurity Foundations, Network Security Fundamentals, Security Operations Fundamentals, Cloud Security Fundamentals and SASE Fundamentals**.

# CYBERSECURITY ACADEMY

# Thank You

---

[paloaltonetworks.com](https://paloaltonetworks.com)





# Palo Alto Networks® Cybersecurity Academy

Formando a los profesionales de la ciberseguridad del futuro

Sign In

Create Account

EN



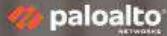
Get Started

Contact Us

Resources

Get Support

Under Attack?



Products

Solutions

Services

Partners

Company

More

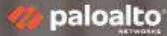
Unit 42 Threat Research

# Education Services

Your learning your way

[Sign In](#)[Create Account](#)

EN

[Get Started](#)[Contact Us](#)[Resources](#)[Get Support](#)[Under Attack?](#)[Products](#)[Solutions](#)[Services](#)[Partners](#)[Company](#)[More](#)[Unit 42 Threat Research](#)

# Educate

Your learning your way.



## Cybersecurity Academy

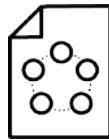
**Educating the Workforce of Tomorrow**

Our students are the next generation of cybersecurity professionals. The Cybersecurity Academy builds careers and closes the cybersecurity skills gap.

Academic institutions, become a member of our academy network and access our free, comprehensive cybersecurity education program.

# Beneficios del programa

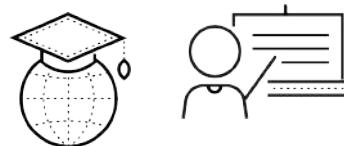
## Acceso a contenidos & soporte



Plataforma Moodle

Dos tracks disponibles

## Formación de instructores



Convocatorias de formación del profesorado

## Labs para docencia



Distintas opciones para acceso a labs para estudiantes

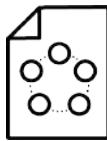
## Descuento en certificaciones oficiales



40% de descuento en exámenes de certificación Palo Alto Networks (PCCET & PCNSA)

# Recorrido Académico

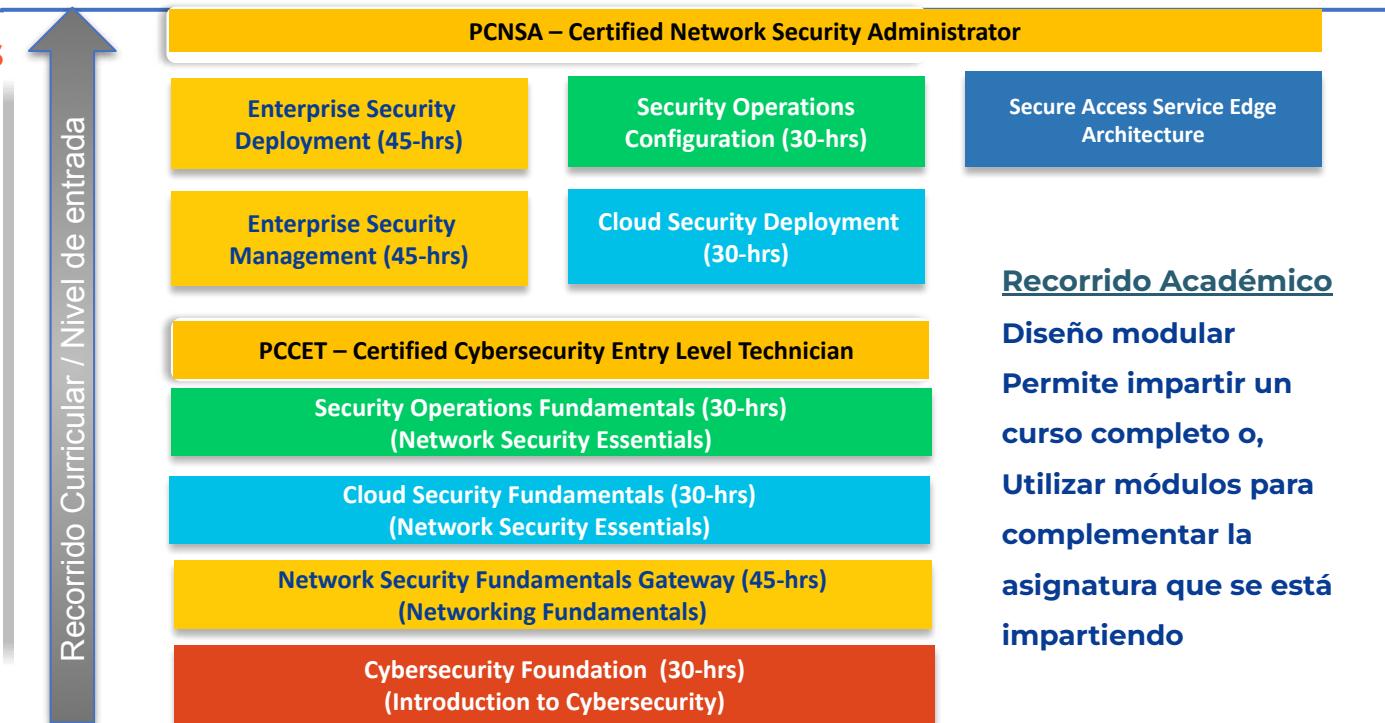
## Acceso a contenidos & soporte



## Recorrido Académico

Plataforma Moodle

Recorrido Curricular / Nivel de entrada

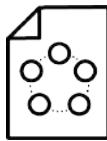


## Recorrido Académico

**Diseño modular**  
**Permite impartir un curso completo o, Utilizar módulos para complementar la asignatura que se está impartiendo**

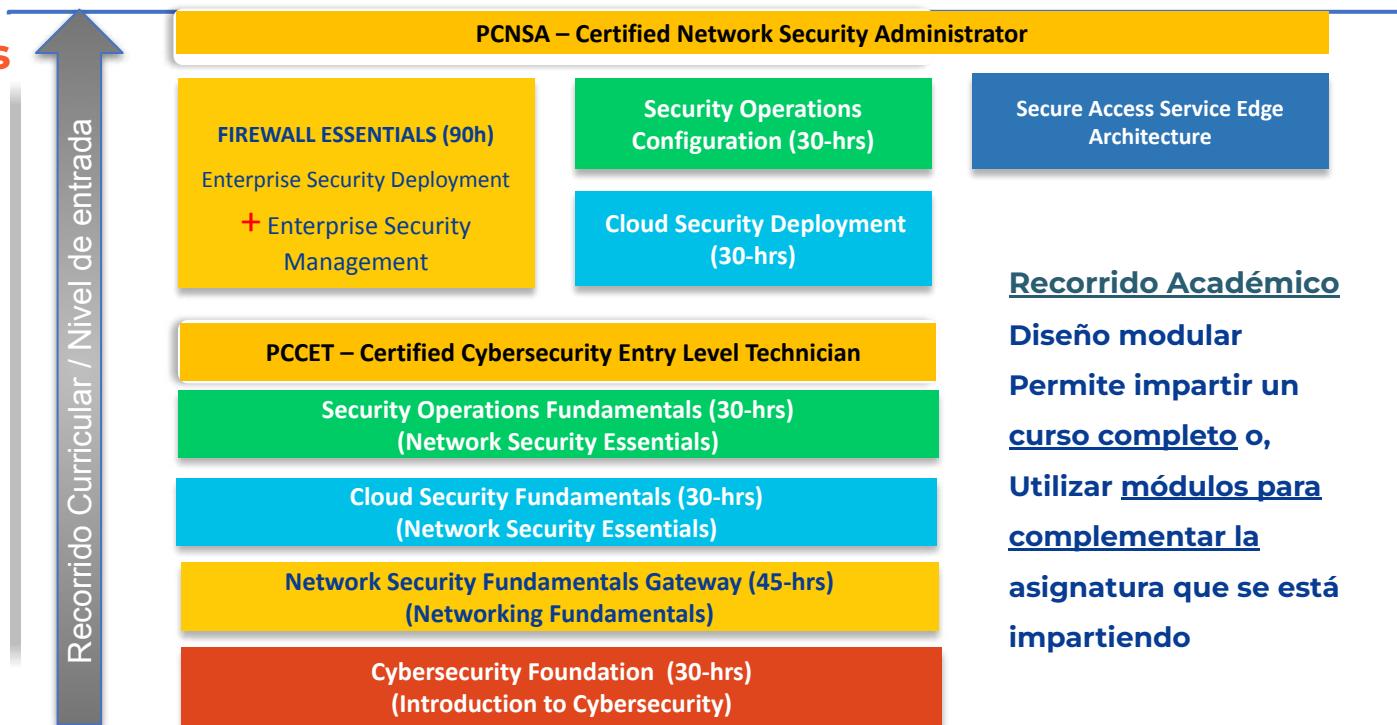
# Recorrido Académico

## Acceso a contenidos & soporte



## Recorrido Académico

Plataforma Moodle



# Plataforma LMS del programa



Español - Internacional (es) ▾

Acceder

Crear nueva cuenta



# Plataforma LMS - Dashboard



Recent ▾ English (en) ▾

Amador Gabaldon 

## Palo Alto Networks Academy: Dashboard

Customise this page

Message

### Course overview

All (except removed from view) ▾

Last accessed ▾

List ▾

★ CF-PUE Academy-03/23/24

...

★ FE-PUE Academy-12/22/23

...

★ SO-PUE Academy-03/23/24

...

★ CS-PUE Academy-03/23/24

...

★ NS-PUE Academy-03/23/24

...

Cybersecurity Academy Onboarding - Self Paced V6

36% Complete

...

★ Firewall Essentials-PUE Academy-02/02/23

...

# Curso Firewall Essentials - PCNSA- Cabecera

Palo Alto Networks Academy

Recent English (en)

Firewall Essentials-PUE Acad...

Participants

Grades

Course Information

Module 1 - Platform and Arc...

Module 2 - Firewall Initial Co...

Module 3 - Firewall Configur...

Module 4 - Firewall Administr...

Module 5 - Connecting Secu...

Module 6 - Security Policies

Module 7 - NAT Policies

Module 8 - Application Ident...

Module 9 - Security Profiles

Module 10 - URL Filtering

Module 11 - Wildfire

15 ENROLLED STUDENTS

0 STUDENTS COMPLETED

10 IN PROGRESS

5 YET TO START

Course Information



PA-7000-PANTRAY

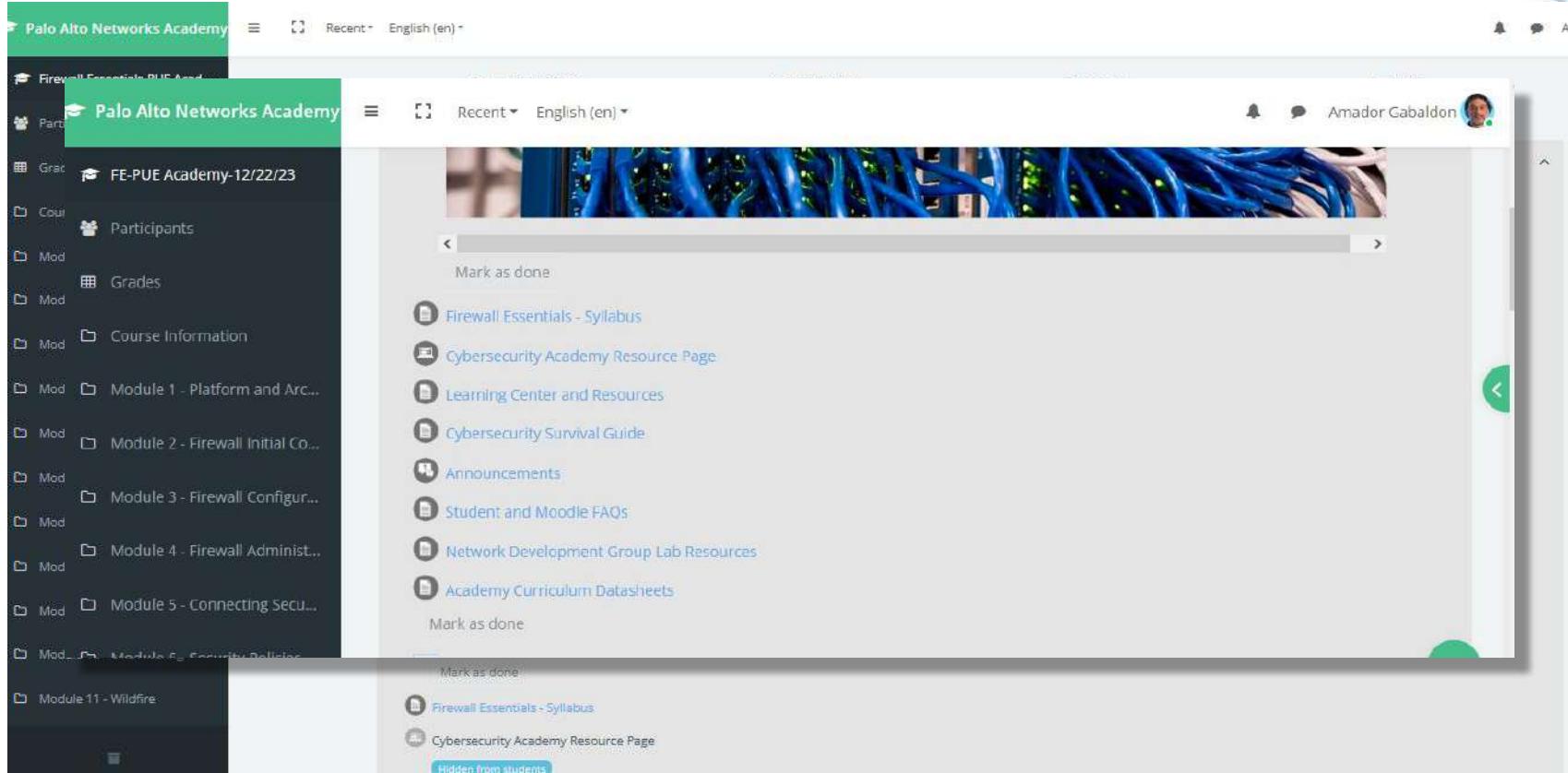
Mark as done:

Firewall Essentials - Syllabus

Cybersecurity Academy Resource Page

Hidden from students

# Curso Firewall Essentials - PCNSA- Cabecera



The screenshot shows the Moodle course interface for "Firewall Essentials - PCNSA- Cabecera". The course navigation bar at the top includes links for "Recent" and "English (en)". On the right, there are notifications, a user profile for "Amador Gabaldon", and a search bar.

The course structure on the left side of the screen is as follows:

- Participate
- Graduate FE-PUE Academy-12/22/23
- Participants
- Mod Grades
- Mod Course Information
- Mod Module 1 - Platform and Arc...
- Mod Module 2 - Firewall Initial Co...
- Mod Module 3 - Firewall Configur...
- Mod Module 4 - Firewall Administ...
- Mod Module 5 - Connecting Secu...
- Mod Module 6 - Security Policies
- Module 11 - Wildfire

The main content area displays a banner image of server racks with blue cables. Below the banner, there are two sections of course resources:

**Mark as done**

- Firewall Essentials - Syllabus
- Cybersecurity Academy Resource Page
- Learning Center and Resources
- Cybersecurity Survival Guide
- Announcements
- Student and Moodle FAQs
- Network Development Group Lab Resources
- Academy Curriculum Datasheets

**Mark as done**

- Firewall Essentials - Syllabus
- Cybersecurity Academy Resource Page

A small button at the bottom of the resource list says "Hidden from students".

# Curso Firewall Essentials - PCNSA- Objetivos

**Palo Alto Networks Cybersecurity Academy**

## **Firewall 10.1 Essentials: Configuration and Management (EDU-210)** **Course Syllabus**

### **Course Description:**

Successful completion course should enhance the student's understanding of how to configure and manage Palo Alto Networks Next- Generation Firewalls. The course focuses on configuring, managing, and monitoring a firewall in a lab environment, including the following:

- Configure and manage the essential features of Palo Alto Networks next-generation firewalls
- Configure and manage Security and NAT policies to enable approved traffic to and from zones
- Configure and manage Threat Prevention strategies to block traffic from known and unknown IP addresses, domains, and URLs
- Monitor network traffic using the interactive web interface and firewall reports



# Curso Firewall Essentials - PCNSA- Recursos adicionales

Palo Alto Networks Academy Recent English (en) Amador Gabaldon

## Learning Center and Resources

Here's a link to the publicly available techdocs publications from Palo Alto Networks.  
<https://docs.paloaltonetworks.com>

For information about Palo Alto Networks Certifications please visit this page:  
<https://www.paloaltonetworks.com/services/education/certification>

The UNIT 42 global threat intelligence team at Palo Alto Networks regularly publishes cybersecurity research whitepapers and threat analytics. This link is a public site.  
<https://unit42.paloaltonetworks.com/>

Click the link below to navigate to the Palo Alto Academy site. At the Academy site you can view an outline of the Academy Curriculum, and access Academy Support information. This link is a public site.  
<https://www.paloaltonetworks.com/services/education/academy>

Digital Learning: The Palo Alto Networks Learning Center offers digital learning classes on Cybersecurity Fundamentals, Networking Security, Cloud Security and Security Operations Center security. The courses require a free registration.

Click the link below to visit the Digital Learning page and preview datasheets for all four courses.  
<https://www.paloaltonetworks.com/services/education/digital-learning>

Click the link below for step-by-step instructions for enrolling in the digital learning program



# Curso Firewall Essentials - PCNSA- Survival Guide

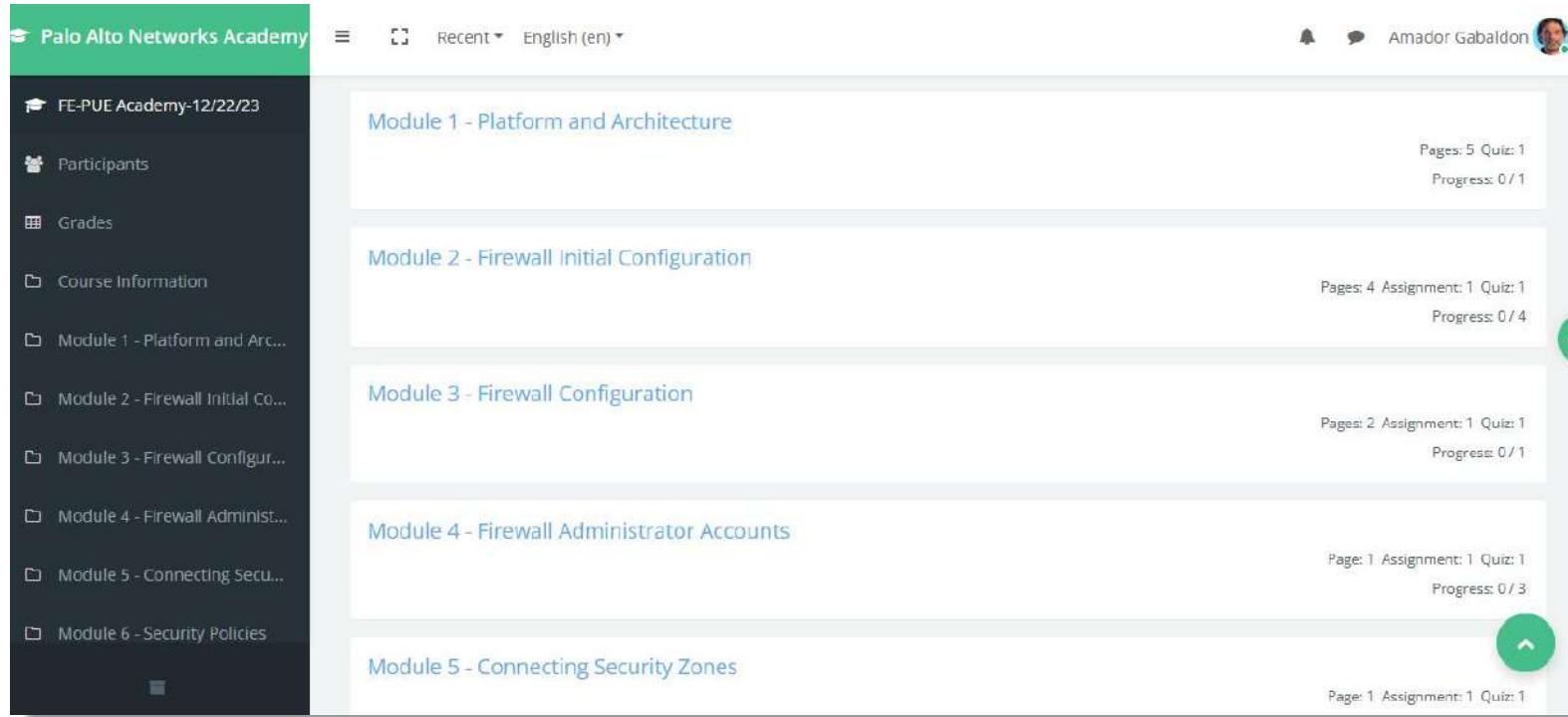


## CYBERSECURITY SURVIVAL GUIDE



Fundamental Principles & Best Practices

# Firewall Essentials – PCNSA - Módulos



The screenshot shows the course navigation menu on the left and a list of modules on the right. The modules are:

- Module 1 - Platform and Architecture
- Module 2 - Firewall Initial Configuration
- Module 3 - Firewall Configuration
- Module 4 - Firewall Administrator Accounts
- Module 5 - Connecting Security Zones

Each module card includes the following details:

- Module 1: Pages: 5 Quiz: 1 Progress: 0 / 1
- Module 2: Pages: 4 Assignment: 1 Quiz: 1 Progress: 0 / 4
- Module 3: Pages: 2 Assignment: 1 Quiz: 1 Progress: 0 / 1
- Module 4: Page: 1 Assignment: 1 Quiz: 1 Progress: 0 / 3
- Module 5: Page: 1 Assignment: 1 Quiz: 1 Progress: 0 / 1

# Estructura de los Módulos - Contenidos



Recent ▾ English (en) ▾



Amador Gabaldon



## Resources



Reading - Initial Configuration



Interactive: Initial Configuration

## Labs



Lab 1 - Firewall Connect to the Management Network

Mark as done



Lab Knowledge Check - DHCP

Mark as done



Lab Knowledge Check - Virtual IP

Mark as done

## Assessments



Quiz #2 - Configuring and Managing Firewall Interfaces

Receive a grade

Receive a pass grade



# Recursos: Objetivos y artículos de Lectura

Recent ▾ English (en) ▾

Amador Gabaldon 

## Resources

-  [Reading - Initial Configuration](#)
-  [Interactive: Initial Configuration](#)

## Labs

-  [Lab 1 - Firewall Connect to the Management Network](#)  
Mark as done
-  [Lab Knowledge Check - DHCP](#)  
Mark as done
-  [Lab Knowledge Check - Virtual IP](#)  
Mark as done

## Assessments

-  [Quiz #2 - Configuring and Managing Firewall Interfaces](#)  
Receive a grade Receive a pass grade

# Recursos: Prácticas de Laboratorio

Recent ▾ English (en) ▾

Amador Gabaldon 

## Resources

- Reading - Initial Configuration
- Interactive: Initial Configuration

## Labs

- Lab 1 - Firewall Connect to the Management Network
  - Mark as done
- Lab Knowledge Check - DHCP
  - Mark as done
- Lab Knowledge Check - Virtual IP
  - Mark as done

## Assessments

- Quiz #2 - Configuring and Managing Firewall Interfaces
  - Receive a grade
  - Receive a pass grade

# Recursos: Cuestionario de Módulo



Recent ▾ English (en) ▾



Amador Gabaldon



- 

## Resources

- [Reading - Initial Configuration](#)
- [Interactive: Initial Configuration](#)

## Labs

- [Lab 1 - Firewall Connect to the Management Network](#)  
[Mark as done](#)
- [Lab Knowledge Check - DHCP](#)  
[Mark as done](#)
- [Lab Knowledge Check - Virtual IP](#)  
[Mark as done](#)

## Assessments

- [Quiz #2 - Configuring and Managing Firewall Interfaces](#)  
[Receive a grade](#) [Receive a pass grade](#)

# Recursos Adicionales para instructores

## Module 8 - Faculty Resources

Pages: 8 File: 1 Folder: 1 URLs: 2

Progress: 0 / 11

### Interactive Activities - Additional Links

[Mark as done](#)

### PCNSA Data Sheet

[Mark as done](#)

### Module Presentations

[Mark as done](#)

### Module Reading Review Questions Answers

[Mark as done](#)

### Additional Resources

[Mark as done](#)

### OS 10 VMware Workstation LAB OVA Files and Resources

### OS 9 VMware Workstation LAB OVA Files and Resources

### Student Self-Enrollment Setup

[Mark as done](#)

### Instructor FAQs

[Mark as done](#)

### Course Error Reporting Form

[Mark as done](#)

### Threat Techniques and Vulnerabilities Presentation

[Mark as done](#)

### Additional Firewall Presentations

# Cuestionarios y Certificado de Compleción - I

## Firewall 10.1 Essentials Certificate - Certificado de Superación del Curso - PA

**Restricted** Not available unless:

All of:

The activity [Quiz #1 - Security Architecture Planning](#) is complete and passed

The activity [Quiz #2 - Configuring and Managing Firewall Interfaces](#) is complete and passed

The activity [Quiz #3 - Firewall Configuration](#) is complete and passed

The activity [Quiz #4 - Managing Firewall Administrator Accounts](#) is complete and passed

The activity [Quiz #5 - Configure and Manage Firewall Security Zones](#) is complete and passed

The activity [Quiz #6 - Creating and Managing Security Policies](#) is complete and passed

The activity [Quiz #7 - Creating and Managing NAT Policy Rules](#) is complete and passed

The activity [Quiz #8 - Application Identification](#) is complete and passed

The activity [Quiz #9 - Security Profiles](#) is complete and passed

The activity [Quiz 10 - URL Filtering](#) is complete and passed

The activity [Quiz 11 - WildFire](#) is complete and passed

The activity [Quiz 12 - User-ID](#) is complete and passed

The activity [Quiz 13 - Encrypted Traffic](#) is complete and passed

The activity [Quiz 14 - Logs and Reports](#) is complete and passed

You achieve a required score in [210 Final Exam](#)

You belong to [PUE Academy](#)

# Cuestionarios y Certificado de Compleción - II



## Palo Alto Networks Authorized Cybersecurity Academy Instructor

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

**PUE Academy Student**

By successfully passing the course:

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

has successfully completed all requirements to become a  
Palo Alto Networks® Cybersecurity Academy Instructor.

A handwritten signature in black ink, appearing to read "Nikesh Arora".

Nikesh Arora  
Chairman and CEO  
Palo Alto Networks

Authorization Date

May 12th, 2023

Authorization Number



Cybersecurity  
Academy

[https://paloaltonetworksacademy.net/mod/customcert/verify\\_certificate.php](https://paloaltonetworksacademy.net/mod/customcert/verify_certificate.php)

# Opciones de Laboratorio

## Labs para Docencia



Distintas opciones  
para acceso a labs  
para docencia

- **Laboratorios virtuales integrados en los cursos**
  - basados en la plataforma NDG LaaS (Lab as a Service)
  - basados en Cloud
- **Laboratorios basados en Firewall VM-50 Palo Alto Networks (OVAs)**
  - Firewall + Virtual Router + DMZ Server + Client
  - Guías / Vídeos de integración e implementación en plataformas de virtualización
- **Descuentos en modelos seleccionados de dispositivos Firewalls**

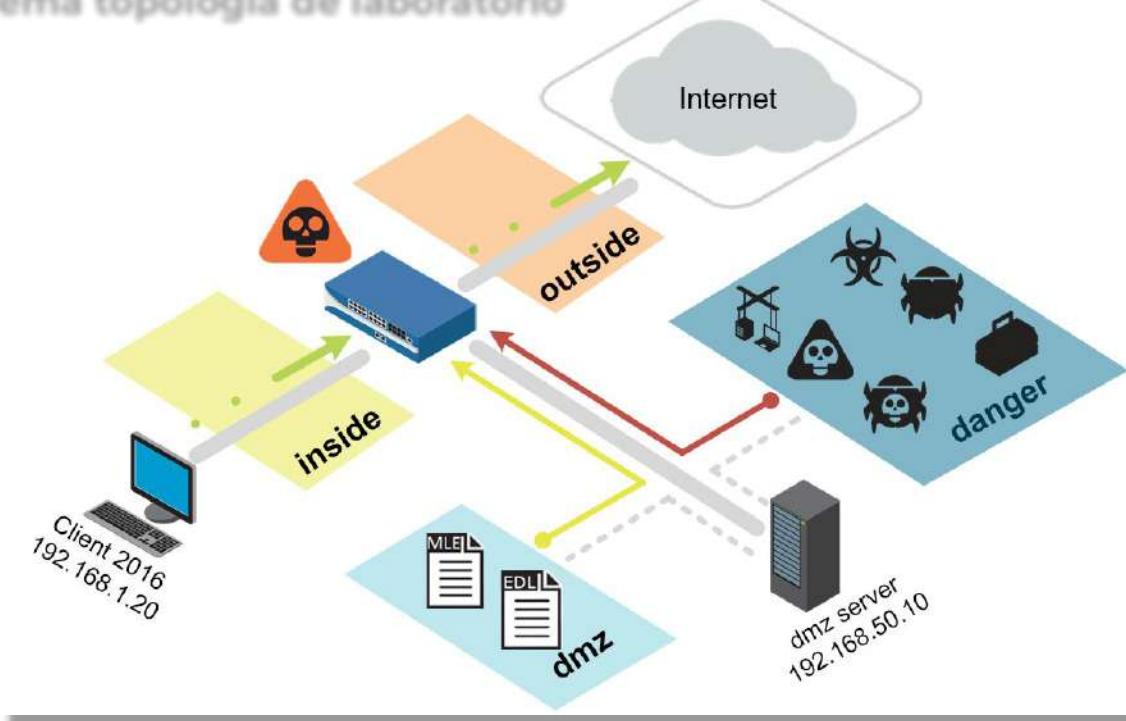
# Opciones de Laboratorio

## Esquema topología de laboratorio

### Labs para docencia



Distintas opciones para acceso a labs para docencia



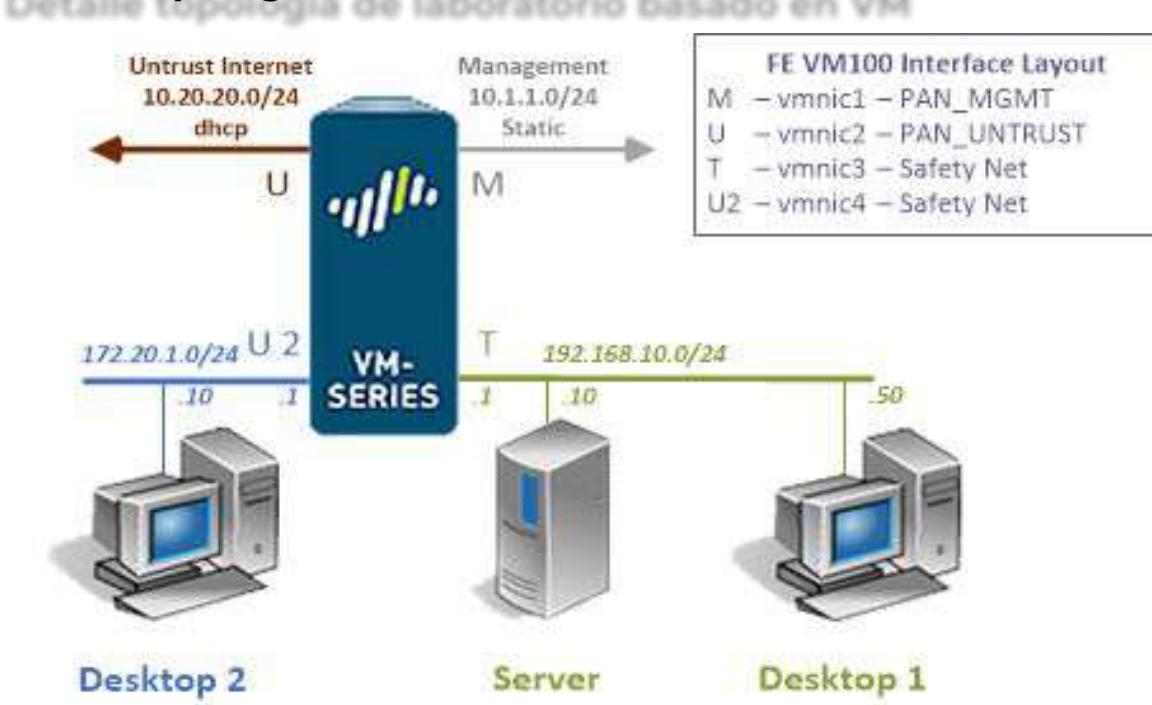
# Opciones de Laboratorio

## Labs para docencia



Distintas opciones para acceso a labs para docencia

### Detalle topología de laboratorio basado en VM



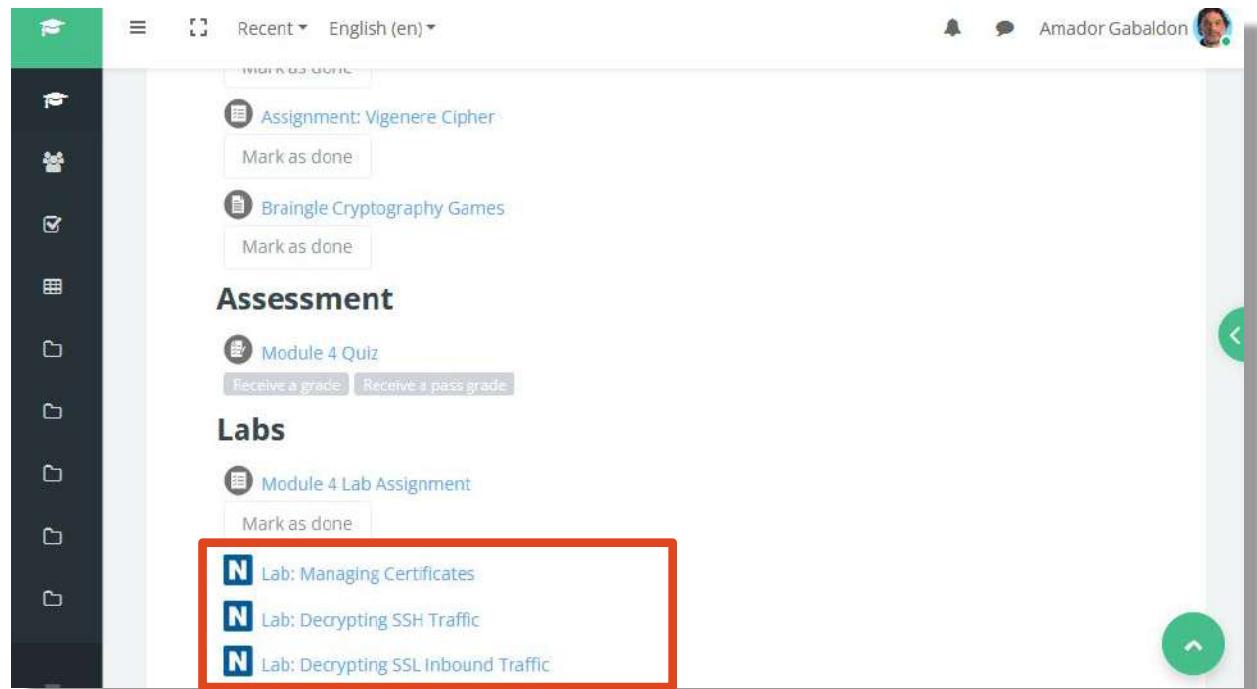
# Laboratorios LaaS

## Labs para docencia



Distintas opciones  
para acceso a labs  
para docencia

### Accesos directos desde la plataforma Palo Alto Networks



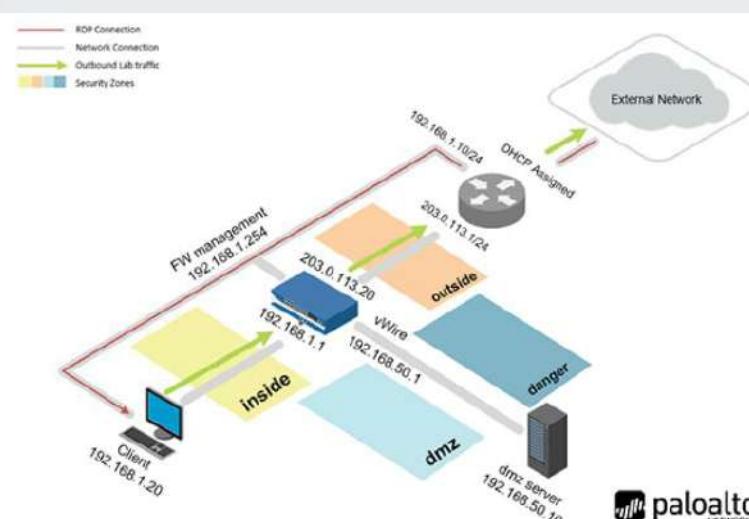
The screenshot shows the user interface of the Palo Alto Networks Cybersecurity Academy. On the left, there is a sidebar with icons for VM-Series, Recent, English (en), a bell, a message bubble, and a user profile for Amador Gabaldon. The main content area has sections for "Recent", "Assignment: Vigenere Cipher" (with a "Mark as done" button), "Braingle Cryptography Games" (with a "Mark as done" button), "Assessment" (Module 4 Quiz with "Receive a grade" and "Receive a pass grade" buttons), and "Labs". The "Labs" section contains three items: "Module 4 Lab Assignment" (with a "Mark as done" button) and three labs starting with 'N': "Lab: Managing Certificates", "Lab: Decrypting SSH Traffic", and "Lab: Decrypting SSL Inbound Traffic". The last two items are highlighted with a red rectangle.

# Laboratorios Laas

Firewall Essentials-PUE Academy-02/02/23 Acceso a laboratorios prácticos Curso EDU210 - PCNSA

**Labs**

- [Lab 01: Connect to the Management Network](#)
- [Lab 02: Working with Firewall Configurations and Log Files](#)
- [Lab 03: Working with Firewall Administrator Accounts](#)
- [Lab 04: Connecting the Firewall to Production Networks](#)
- [Lab 05: Configuring Security Policy Rules and NAT Policy Rules](#)
- [Lab 06: Blocking Packet- and Protocol-Based Attacks](#)
- [Lab 07: Blocking Threats from Known-Bad Sources](#)
- [Lab 08: Blocking Threats Using App-ID](#)
- [Lab 09: Maintaining Application-Based Policies](#)
- [Lab 10: Blocking Threats Using Custom Applications](#)
- [Lab 11: Blocking Threats with User-ID](#)
- [Lab 12: Blocking Unknown Malware with WildFire](#)
- [Lab 13: Blocking Threats in Encrypted Traffic](#)
- [Lab 14: Preventing Use of Stolen Credentials](#)



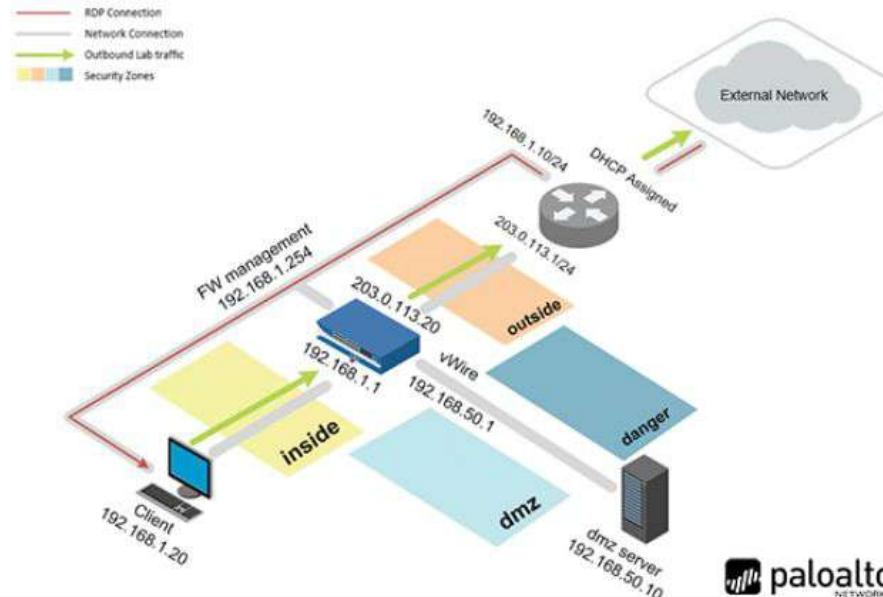
The diagram illustrates a Palo Alto Networks Firewall configuration. It features three security zones: Inside (yellow), dmz (light blue), and outside (orange). A client computer (IP: 192.168.1.20) is connected to the Inside zone. A dmz server (IP: 192.168.50.10) is located in the dmz zone. An external network (IP: 203.0.113.1/24) is connected to the outside zone via a connection labeled "DHCP Assigned". A legend at the top right identifies the line colors: red for RDP Connection, grey for Network Connection, green for Outbound Lab traffic, and yellow for Security Zones.

# Laboratorios LaaS - Topología

MyNETLAB > RGMCNCVE2.H87.P27051.PAN10\_210 > Reservation 39370 > Lab 02: Working with Firewall Configurations and Log Files

Time Remaining  
1 10  
hrs. min.

 Topology    Content ▾    Status    Client ▾    Firewall ▾    DMZ ▾    VRouter ▾



 paloalto  
NETWORKS

# Laboratorios LaaS – Doc Prácticas

Screenshot of a web-based interface, likely a cloud lab management tool. The top navigation bar includes tabs for Topology, Content (selected), Status, Client, Firewall, DMZ, and VRouter. Below the navigation is a search bar, page number (1 de 33), and zoom controls (80%). The main content area displays logos for NDG, NETLAB+, and Palo Alto Networks, followed by the text "PALO ALTO NETWORKS EDU 210" and the subtitle "Lab 2: Working with Firewall Configurations and Log Files".



# Laboratorios LaaS -Status

MyNETLAB > RGMNCNVE2.H87.P27051.PAN10\_210 > Reservation 39370 > Lab 02: Working with Firewall Configurations and Log Files

Time Remaining 0 49 hrs. min.

Learn Modules Teach Account Help

> Topology Content Status Client Firewall DMZ VRouter

### Lab Devices

Device	Type	Power	Status	Connections	Action
Client	Linux	 Powered On			
Firewall	Linux	 Powered On			
DMZ	Linux	 Powered On			
VRouter	Linux	 Powered On			

# Laboratorios LaaS - Cliente

MyNETLAB > RGMNCV2.H87.P27051.PAN10\_210 > Reservation 39370 > Lab 02: Working with Firewall Configurations and Log Files

Time Remaining  
0 46 hrs. min.

Topology Content Status Client Firewall DMZ VRouter

Applications 00:03

# Laboratorios LaaS – Consola FW

MyNETLAB > RGMCNCVE2.H87.P27051.PAN10\_210 > Reservation 39370 > Lab 02: Working with Firewall Configurations and Log Files

> Topology    Content    Status    Client    Firewall    DMZ    VRouter

Time Remaining

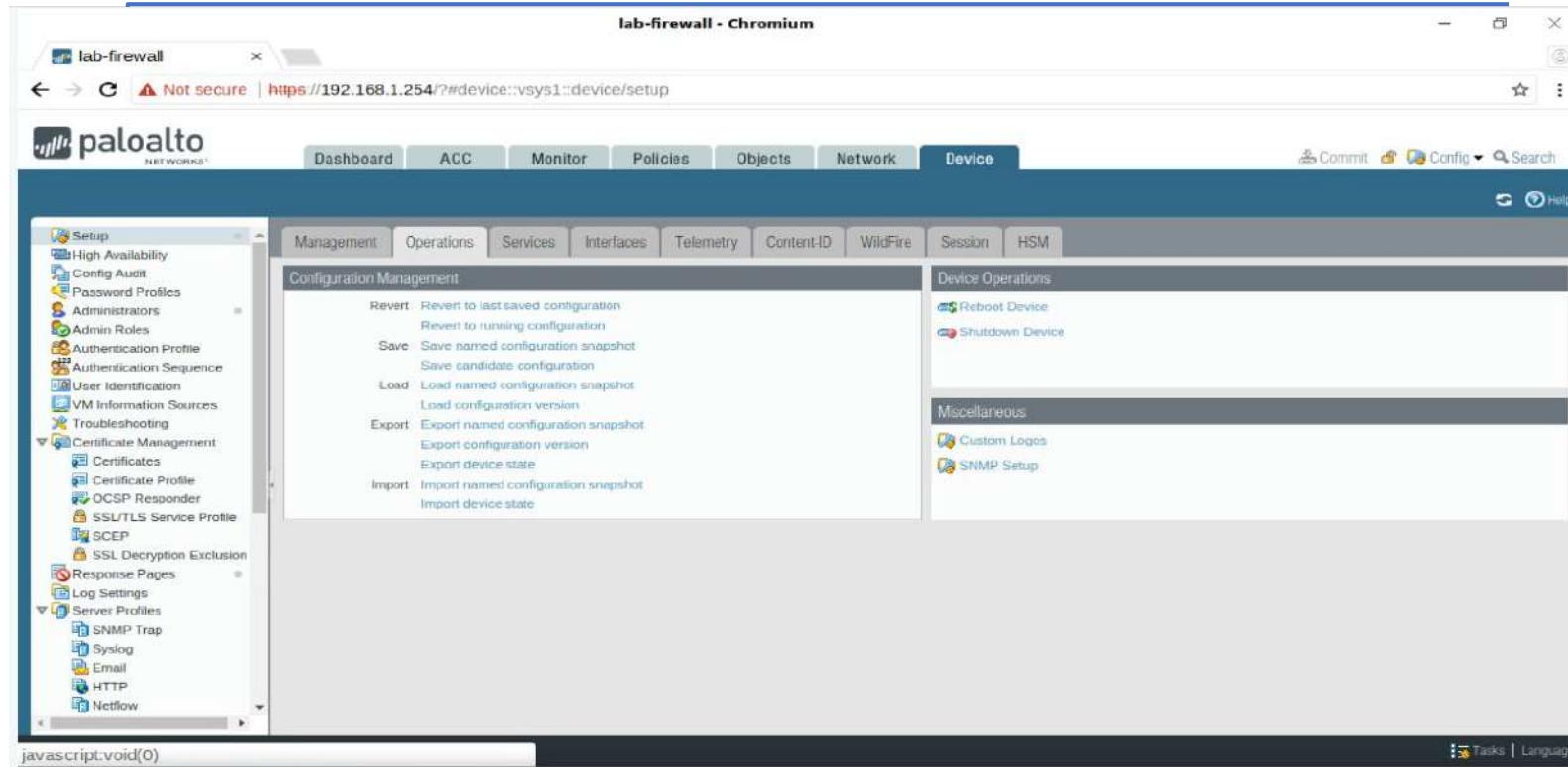
0 45

hrs. min.

```
Firewall]# login: [ 71.465190] Bits 55-60 of /proc/PID/pagemap entries are about to stop being page-shift some time soon. See the linux/Documentation/vm/pagemap.txt for details.  
[ 1066.990327] perf: interrupt took too long (2596 > 2560), lowering kernel.perf_event_max_sample_rate to 79000  
[ 1393.399926] perf: interrupt took too long (3171 > 3131), lowering kernel.perf_event_max_sample_rate to 63000
```

```
Firewall]# login: _
```

# Laboratorios LabaaS – Acceso Cliente a FW



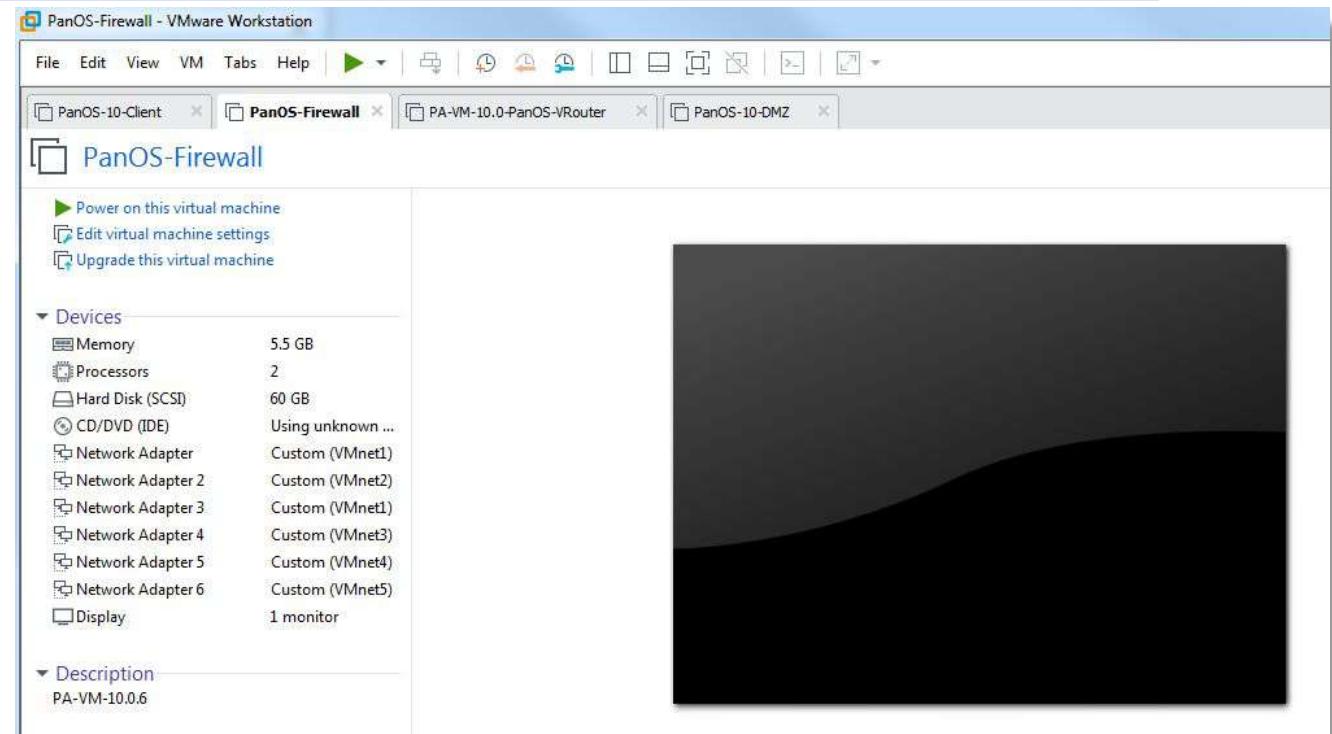
The screenshot shows the Palo Alto Networks Firewall configuration interface within a Chromium browser window. The URL is <https://192.168.1.254/#device::vsys1::device/setup>. The interface includes a navigation bar with tabs: Dashboard, ACC, Monitor, Policies, Objects, Network, Device (selected), Session, and HSM. On the left is a sidebar with sections like Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Troubleshooting, Certificate Management, Response Pages, Log Settings, Server Profiles, and Netflow. The main content area has tabs for Management, Operations, Services, Interfaces, Telemetry, Content-ID, WildFire, Session, and HSM. Under Management, there's a 'Configuration Management' section with options for Revert, Save, Load, Export, and Import configurations. There are also sections for Device Operations (Reboot Device, Shutdown Device) and Miscellaneous (Custom Logos, SNMP Setup). The bottom of the browser window shows a JavaScript error: "Uncaught ReferenceError: chrome is not defined".

# Laboratorios basado en OVAs – VM-50 FW

## Labs para Docencia



Distintas opciones  
para acceso a labs  
para docencia



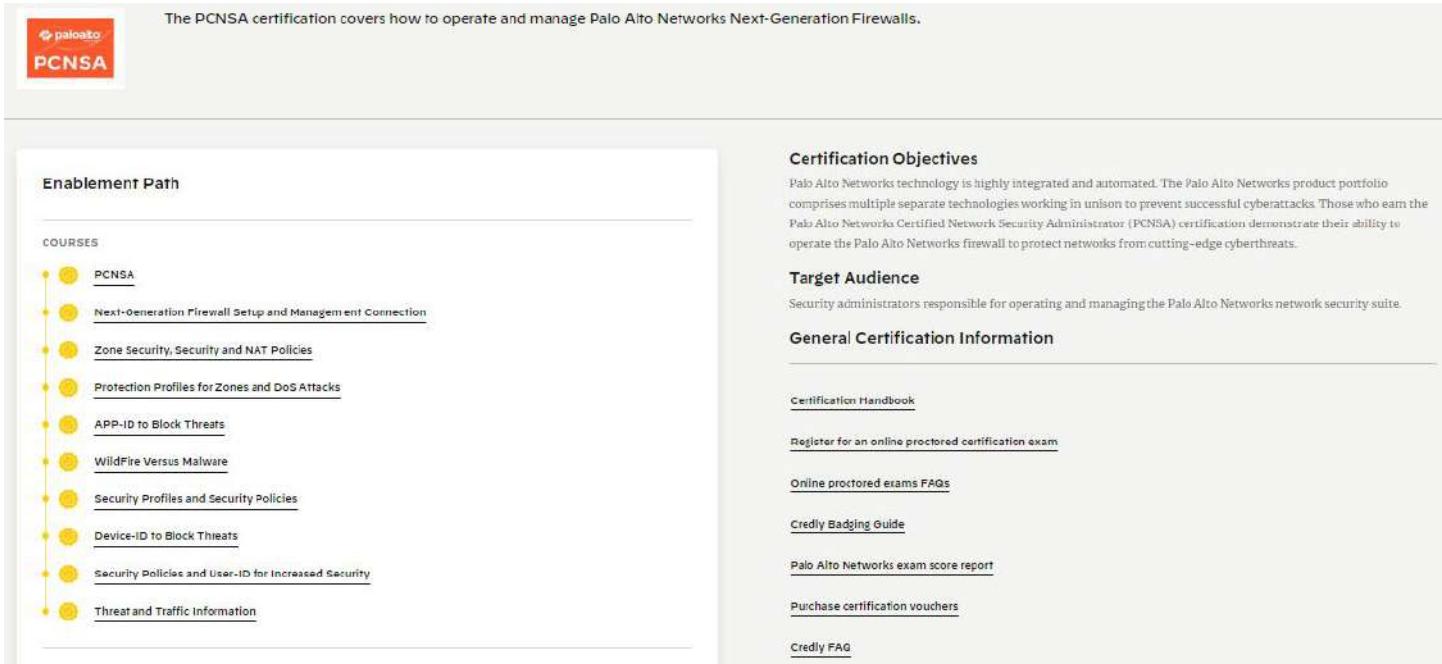
# Descuentos académicos Exámenes Certificación Oficial - PCNSA

Descuento en certificaciones oficiales



40% de descuento en exámenes de certificación Palo Alto Networks (PCCET & PCNSA)

The PCNSA certification covers how to operate and manage Palo Alto Networks Next-Generation Firewalls.



**Enablement Path**

**COURSES**

- [PCNSA](#)
- [Next-Generation Firewall Setup and Management Configuration](#)
- [Zone Security, Security and NAT Policies](#)
- [Protection Profiles for Zones and DoS Attacks](#)
- [APP-ID to Block Threats](#)
- [WildFire Versus Malware](#)
- [Security Profiles and Security Policies](#)
- [Device-ID to Block Threats](#)
- [Security Policies and User-ID for Increased Security](#)
- [Threat and Traffic Information](#)

**Certification Objectives**

Palo Alto Networks technology is highly integrated and automated. The Palo Alto Networks product portfolio comprises multiple separate technologies working in unison to prevent successful cyberattacks. Those who earn the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification demonstrate their ability to operate the Palo Alto Networks firewall to protect networks from cutting-edge cyberthreats.

**Target Audience**

Security administrators responsible for operating and managing the Palo Alto Networks network security suite.

**General Certification Information**

[Certification Handbook](#)

[Register for an online proctored certification exam](#)

[Online proctored exams FAQs](#)

[Credly Badging Guide](#)

[Palo Alto Networks exam score report](#)

[Purchase certification vouchers](#)

[Credly FAQ](#)

# Descuentos académicos Exámenes Certificación Oficial - PCNSA

Descuento en certificaciones oficiales



40% de descuento en exámenes de certificación Palo Alto Networks (PCCET & PCNSA)

## What is the format of the PCNSA exam?

- Certification Name: Palo Alto Networks Certified Network Security Administrator
- Delivered through Pearson VUE: <https://home.pearsonvue.com/paloaltonetworks>
- Exam Series: PCNSA
- Total Seat Time: 90 minutes
- Time for Exam Items: 80 minutes
- Time for reviewing [Palo Alto Networks Exam Security Policy](#): 5 minutes, and 5 minutes for Survey
- Number of items: 50–60
- Format: Multiple choice, Scenarios with Graphics, and Matching
- Language: English and Japanese

# PUE Academy

## Training & Certification Center (TCC) - Academy Support Center (ASC)



### Servicios de Formación

Dirigidos a la comunidad educativa global (staff técnico, docentes, alumnos y exalumnos)

[+ Info](#)



### Servicios de certificación

Dirigidos a la comunidad educativa global (staff técnico, docentes, alumnos y exalumnos)

[+ Info](#)



### Centros oficiales

PUE Academy ayuda a las instituciones educativas a convertirse en centros oficiales de formación y certificación de las organizaciones tecnológicas con más reconocimiento mundial.

[+ Info](#)



### Soporte

Para la correcta implementación de las iniciativas Academy a las que se les dará acceso.

[+ Info](#)

# Oferta de formación oficial dirigida a la comunidad educativa

DÓNDE ESTAMOS | CONTACTO | TRABAJA CON NOSOTROS | NEWSLETTER | ESP

SERVICIOS FORMACIÓN CERTIFICACIÓN PUE ACADEMY CONOCE PUE BLOG

PROGRAMAS EDUCATIVOS CURSOS PRÓXIMOS CURSOS CONOCE PUE ACADEMY EVENTOS EU DIGITAL SKILLS CASOS DE ÉXITO PUE ACADEMY MEMBERS BLOG SOLICITUD INFO

ORACLE®

Unity®

Python INSTITUTE PI  
Open Education & Development Group

Project Management Institute.

vmware IT ACADEMY

COMMUNICATION SKILLS BUSINESS

ITIL®  
ACCREDITED TRAINING ORGANIZATION  
PeopleCert ON BEHALF OF AXELOS

ATC AUTHORIZED Training Center

paloalto®  
NETWORKS

# Oferta de formación oficial dirigida a la comunidad educativa

PRÓXIMOS CURSOS. CONSULTA TODAS LAS CONVOCATORIAS DE ESTE CURSO [AQUÍ](#)

**Nota:** Los precios indicados a continuación no incluyen el 21% de IVA

05 nov 2024

**CONFIRMADO** | Palo Alto Networks Certified Network Security Administrator - PCNSA - Online

17 dic 2024

90 horas | Online | Español | Martes (18:30h - 20:00h)

 [INSCRIBIRME](#)

+ INFO



**30%**

**EN TODOS  
NUESTROS CURSOS  
OFICIALES**



Certificación oficial  
incluida para nuestro  
colectivo PUE Alumni

NO acumulable con otras promociones

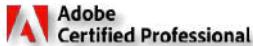
**+ Plazas de formación  
incluidas en la suscripción**

# Modalidad de suscripción

## Programas disponibles de PUE Academy Center



Microsoft Learn For Educators



Office



Microsoft Fundamentals



## Ventajas para el centro:

- Membresía AAC - Centro Palo Alto Networks Cybersecurity Academy
- Gestión de los cursos y recursos oficiales del programa
- Licenciamiento de Firewall para uso docente.
- Formación de instructores
- Certificados de finalización
- 40% de descuento en la certificación oficial PCCET/PCNSA para docentes y alumnos
- Soporte de PUE Academy Authorized Regional Academy (ARA) para la correcta implementación del programa

# Entérate en primicia de nuestros eventos y novedades

Apúntate a nuestra newsletter para enterarte en primicia de nuestros eventos, novedades, lo más innovador en Data y Cloud, y lo último en formación y certificación en tecnología.



**iSuscríbete  
aquí!**



# Palo Alto Networks® Cybersecurity Academy

**Formando a los profesionales de la ciberseguridad del futuro**

**PUE Academy Awards**

# PUE Academy Awards 2023



reconoce a  
Universidad Europea

como  
Mejor centro Palo Alto Networks®  
Cybersecurity Academy

Año 2023





# ¡Gracias!

**Contáctanos. Estamos para ayudarte**

 [pueacademy@pue.es](mailto:pueacademy@pue.es)

 [www.pue.es/pue-academy](http://www.pue.es/pue-academy)

## SEDE BARCELONA

Avda. Diagonal, 98-100  
08019 Barcelona  
93 206 02 49



## SEDE MADRID

C/ Arregui y Aruej, 25-27  
28007 Madrid  
91 162 06 69

Blog

in

tw

yt

