FIREWALL PALO ALTO & CHECKPOINT

CloudLamb
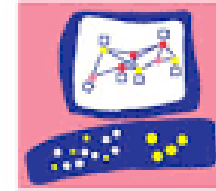E-Learning

Preparación para la certificación **CERTIFIED SECURITY ADMINISTRATOR (CCSA)**

Con este curso el participante tendrá los conocimientos necesarios para instalar y configurar el sistema Firewall CheckPoint Gaia R80.10 el cual cumple la función de proteger la red de las vulnerabilidades de los sistemas informáticos ya que el firewall proporciona una arquitectura de seguridad integral con puntos de aplicación flexibles para la protección avanzada contra los últimos ataques generados en la red.

Instructor curso CheckPoint
Luis Hidalgo Perfil en
LinkedIn: **https://www.linkedin.com/in/lhidalgo0204/**

Requisitos técnicos

Es recomendable que su laptop y/o computadora, cuente con los siguientes recursos para tener un ambiente de laboratorio acorde a las prácticas del curso:
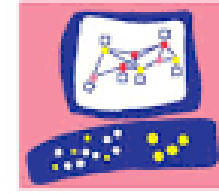
- **Memoria RAM de 12 Gb o superior**
- **Interfaz de red inalámbrica (wifi)**
- **Espacio en disco duro de al menos 100 Gb**

Curso 100% práctico en español con laboratorios guiados desde el primer día de clases.

Contenido del curso

OBJECTIVES

• Know how to perform periodic administrator tasks

• Describe the basic functions of the Gaia operating system

• Recognize Smart Console features, functions, and tools

• Describe the Check Point Firewall infrastructure

• Understand how Smart Console is used by administrators to grant permissions
and user access

• Learn how Check Point security solutions and products work and how they protect networks

• Understand licensing and contract requirements for Check Point security products

• Describe the essential elements of a Security Policy
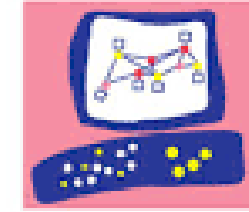
Instructor curso CheckPoint
Luis Hidalgo Perfil en
LinkedIn: **https://www.linkedin.com/in/lhidalgo0204/**

Contentido del curso

- Understand the Check Point policy layer concept
- Understand how to enable the Application Control and URL F software blades to block access to various applications
- Describe how to configure manual and automatic NAT
- Identify tools designed to monitor data, determine threats ar recognize opportunities for performance improvements
- Identify Smart Event components used to store network activity logs and identify events
- Know how Site-to-Site and Remote Access VPN deployments and communities work
- Explain the basic concepts of Cluster XL technology and its advantages

Curso 100% práctico en español con laboratorios guiados desde el primer día de clases.

Firewall Palo Alto

Cap I .-Next -Generation Firewall Setup and Management
Connection
- Palo Alto Networks Product Portfolio and Architecture
- Connect to the Management Network
- Manage Firewall Configurations
- Manage Firewall Administrator Accounts

CapII.-ZoneSecurity, Security and NAT Policies
- TheCyberattackLifecycle
- ConnecttoProductionNetworks
- BlockingThreatsUsingSecurity and NAT Policies

Cap III .-Protection Profiles for Zones and DoS Attacks
- Block Packet and Protocol Based Attacks
- Block Threats From Known Bad Sources

Cap IV.-APP-ID to Block Threats

- Block Threats by Identifying Applications
- Maintain Application-based Policies
- Block Threats Using Custom Applications

Cap V.-WildFireVersus Malware
- Block Unknown Threats
- Block Threats in Encrypted Traffic

CapVI.-Security Profilesand Security Policies
- **Block ThreatsUsingSecurity Profiles**

CapVII.-Device-ID toBlock Threats
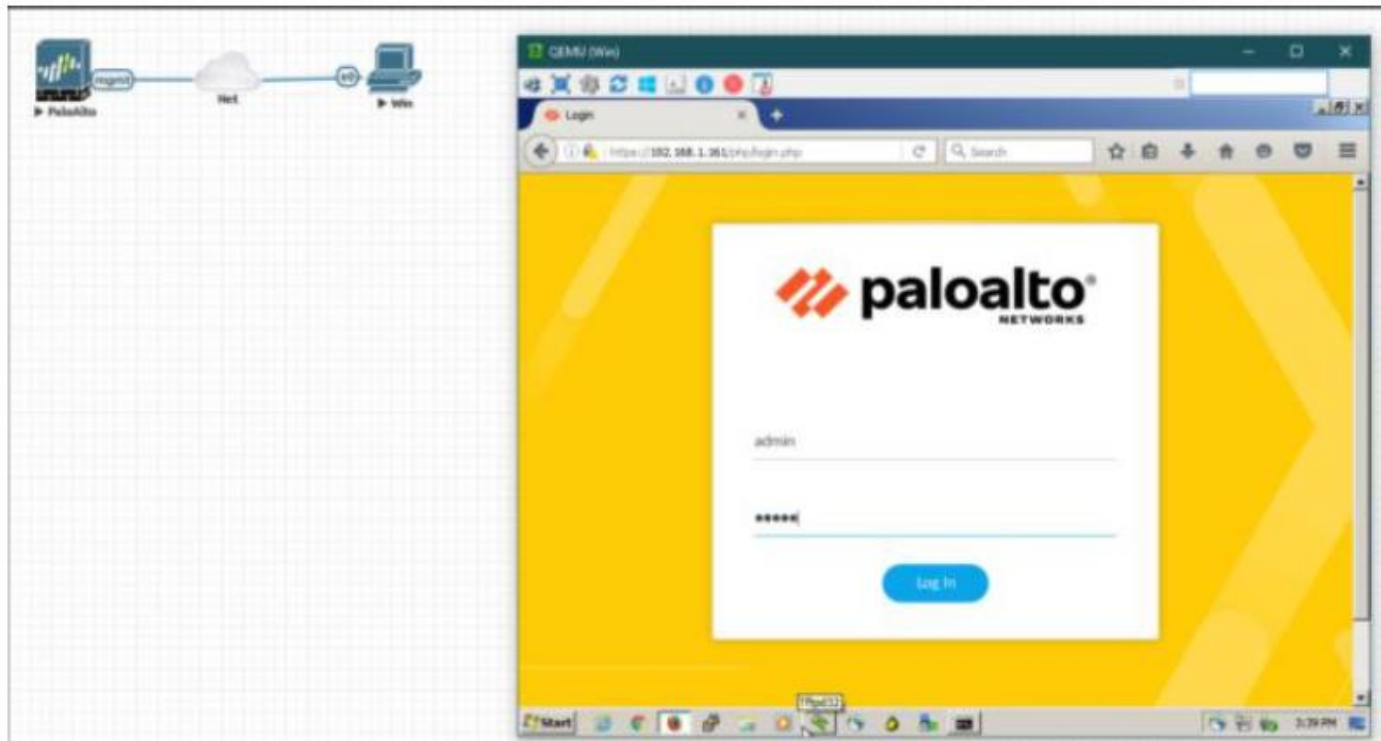- **Block ThreatsbyIdentifyingDevices**

Cap VIII.-Security Policies and User-ID for Increased Security
- Block Threats By Identifying Users
- Prevent Use of Stolen Credentials

Cap IX.-Threat and Traffic Information
- Viewing Threat and Traffic Information

El curso Palo Alto incluye el laboratorio Virtual emulador EVE lo cual no consumirá Recursos de su ordenador

El Futuro sólo lo formarás con tu esfuerzo

CloudLamb
E-Learning