

Capacitación E-Learning



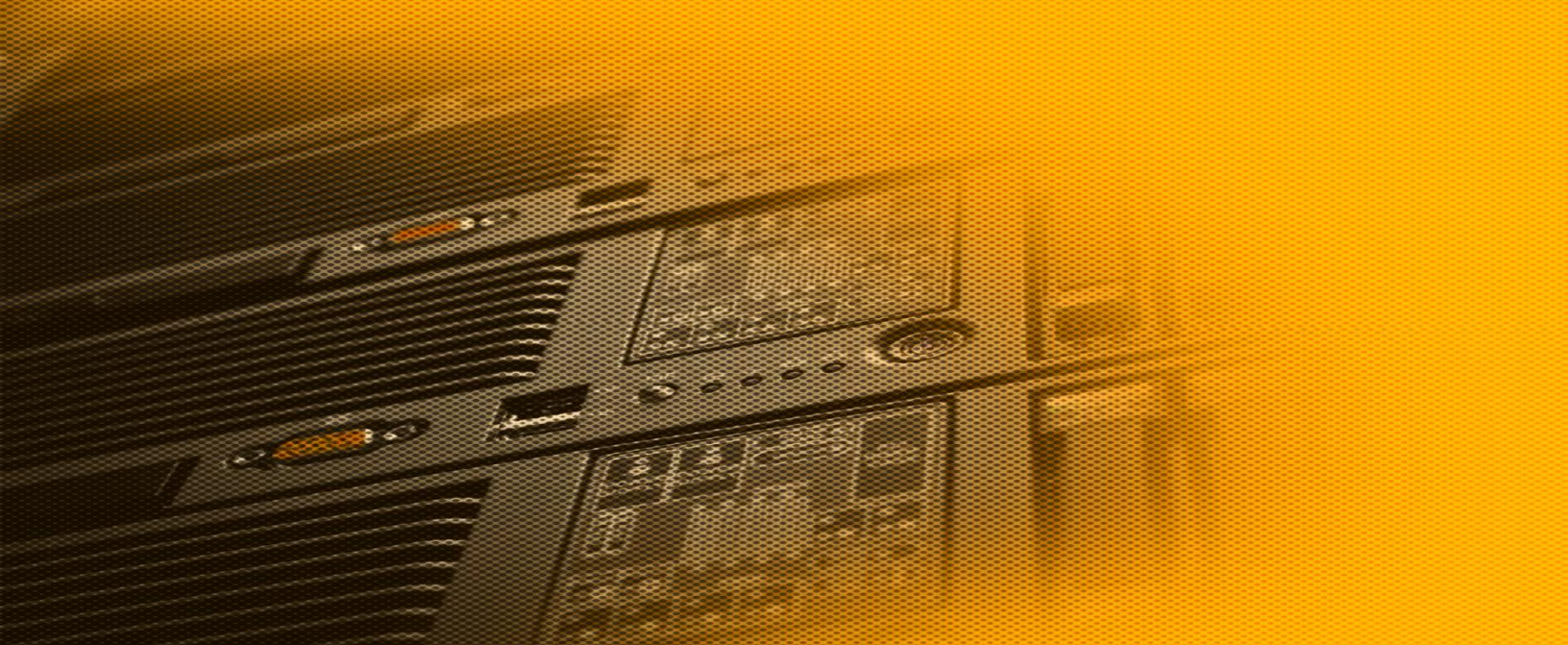
CISCO FIREPOWER

300-710 SNCF

Rendimiento, visibilidad y control: vitales para sacar provecho de la virtualización



Las organizaciones hoy en día intercambian más datos confidenciales con los clientes por ello necesitan más herramientas que les permitan salvar toda la información relevante y para ello necesitan contar con una solución que mejore sustancialmente la seguridad de las comunicaciones las cuales apuestan ya por **Cisco FirePower**, la nueva generación de Firewall del gigante de las telecomunicaciones.



¿Por qué Cisco FirePower?

FirePower, es la última generación de Firewall de Cisco, también conocido como *Next Generation Firewall* (NGFW). Ofrece protección antes, durante y posterior a una amenaza utilizando técnicas de seguridad de última generación con tecnologías tales como:

- ✓ IPS
- ✓ URL Filtering
- ✓ AVC (Application Visibility and Control)
- ✓ Security Intelligence (blacklist de IP, URL y DNS)

Este curso tiene dos finalidades fundamentales:

La primera es, ofrecer el conocimiento de apoyo para la obtención de la certificación **300-710 SNCF** (*Security Networks with Cisco FirePower*), la cual forma parte de la curricula de la **certificación CCNP Security**. Obteniendo la certificación **SNCF**, el candidato se convierte en ***FirePower Specialist***.

Y la segunda es, obtener conocimientos sólidos en los fundamentos, implementación, configuración y troubleshooting de la tecnología FirePower en ambientes reales, permitiendo así el desarrollo profesional del candidato en esta tecnología.



El curso se impartirá en español con una duración en 36 hrs de clases en tiempo real.

Contenido programático...



1. Introducción certificación SNCF

2. Introducción FirePower

2.1 SourceFire

2.2 FirePower

2.2 FirePower Threat Defense (FTD)

3. Introducción Hardware/Virtual

3.1 FMC / FMCv

3.2 SourceFire Series 7000 & 8000

3.2 ASA 5500-X

3.3 FirePower Series 1000, 1100, 2100, 4100, 9300

3.5 FTDv

4. Introducción Firewall/IPS

4.1 NGIPS

4.2 NGFW

5. Firewall Modes

5.1 Routed

5.2 Transparent

5.3 IPS

6. Interface Modes

6.1 Layer 3

6.2 Layer 2 (BVI)

6.3 IRB (Layer 3 + Layer 2)

6.4 Passive

6.5 ERSPAN

6.6 Inline

6.7 Inline-Set

7. High Availability

- 7.1 Failover Active / Standby
- 7.2 Cluster
- 7.3 Container Instance (Failover & Cluster)

8. Object Management

- 8.1 Objects
- 8.2 Intrusion Rules

9. Device Management

- 9.1 Agregar FTD en FMC
- 9.2 Network Address Translation (NAT)
- 9.3 Platform Settings
- 9.4 QoS
- 9.5 Certificados para VPN

10. Políticas

- 10.1 Intrusion
- 10.2 Prefilter
- 10.3 SSL
- 10.4 Malware
- 10.5 Identity
- 10.6 DNS
- 10.7 File & Malware
- 10.8 Network Discovery
- 10.9 Correlation Policies
- 10.10 Security Intelligence
- 10.11 Access Control Policies
- 10.12 Access Control Rules

11. Integraciones

- 11.1 pxGrid ISE
- 11.2 Threat Intelligence Director
- 11.3 AMP for Networks

12. Troubleshooting

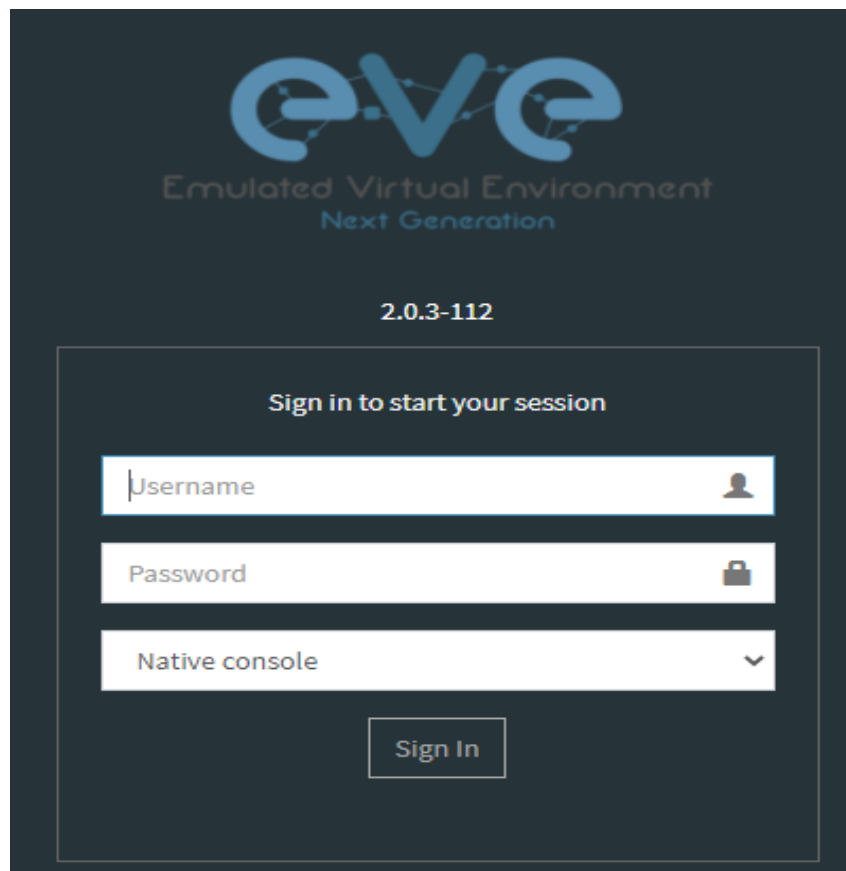
- 12.1 Troubleshooting FMC (CLI / GUI)
- 12.2 Troubleshooting FTD (CLI)

13. Miscellaneous

- 13.1 Reportes
- 13.2 Import/Export
- 13.3 Backup/Restore
- 13.4 Scheduling
- 13.5 Application Detectors
- 13.6 Actions/Alerts
- 13.8 Cisco Threat Response

¿Laboratorio virtual?

- ❖ **Contará con laboratorio virtual bajo el emulador EVE para el desarrollo de las prácticas.**
- ❖ **CloudLamb les dará los accesos al laboratorio EVE el primer día de clases.**
- ❖ **El curso está dirigido a Profesionales del área de Telecomunicaciones/Sistemas y carreras afines orientados al mundo de la tecnología con interés en adquirir o reforzar los conocimientos en FirePower.**



The image shows a login interface for the EVE Emulated Virtual Environment. At the top, the logo 'eve' is displayed in a stylized blue font, with the text 'Emulated Virtual Environment' and 'Next Generation' below it. The version number '2.0.3-112' is centered below the logo. The main content area is a dark gray box with a white border, containing the text 'Sign in to start your session'. Below this text are three input fields: 'Username' with a user icon, 'Password' with a lock icon, and 'Native console' with a dropdown arrow. A 'Sign In' button is located at the bottom of the form.

