Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

NSE4 FortiGate Security & Infrastructure bundle

CÓDIGO:	DURACIÓN:	Precio:
FNT_FT-FGT-SEC_INF	40 Hours (5 días)	A consultar

Description

In this course, you will learn how to use the most common FortiGate features, including security profiles, networking and infrastructure features.
In interactive labs, you will explore firewall policies, the Fortinet Security Fabric, user authentication, and how to protect your network using security profiles, such as IPS, antivirus, web filtering, application control, and more.
These administration fundamentals will provide you with a solid understanding of how to implement basic network security.
Topics include features commonly applied in complex or larger enterprise or MSSP networks, such as advanced routing, redundant infrastructure, virtual domains (VDOMs), zero trust network access (ZTNA), SSL VPN, site-to-site IPsec VPN, single sign-on (SSO), and diagnostics.

Objetivos

After completing this course, you will be able to:

- Deploy the appropriate operation mode for your network
- Use the GUI and CLI for administration
- Control network access to configured networks using firewall policies
- Apply port forwarding, source NAT, and destination NAT
- Authenticate users using firewall policies
- Understand encryption functions and certificates
- Inspect SSL/TLS-secured traffic to prevent encryption used to bypass security policies
- Configure security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites
- Apply application control techniques to monitor and control network applications that might use standard or non-standard protocols and ports
- Fight hacking and denial of service (DoS)
- Collect and interpret log entries
- Identify the characteristics of the Fortinet Security Fabric
- Analyze a FortiGate route table
- Route packets using policy-based and static routes for multipath and load-balanced deployments
- Divide FortiGate into two or more virtual devices, each operating as an independent FortiGate, by configuring virtual domains (VDOMs)
- Understand the fundamentals and benefits of using ZTNA
- Offer an SSL VPN for secure access to your private network
- Establish an IPsec VPN tunnel between two FortiGate devices
- Implement a meshed or partially redundant VPN
- Diagnose failed IKE exchanges
- Offer Fortinet Single Sign-On (FSSO) access to network services, integrated with Microsoft Active Directory (AD)
- Deploy FortiGate devices as an HA cluster for fault tolerance and high performance
- Diagnose and correct common problems

Público

Networking and security professionals involved in the management, configuration, administration, and monitoring of FortiGate devices used to secure their organizations' networks should attend this course.
You should have a thorough understanding of all the topics covered in the FortiGate Security course before attending the FortiGate Infrastructure course.
Networking and security professionals involved in the design, implementation, and administration of a network infrastructure using FortiGate devices should attend this course.

This course assumes knowledge of basic FortiGate fundamentals. You should have a thorough understanding of all the topics covered in the FortiGate Security course before attending the FortiGate Infrastructure course.

Requisitos Previos

- Knowledge of network protocols
- Basic understanding of firewall concepts
- Knowledge of OSI layers
- Knowledge of firewall concepts in an IPv4 network
- Knowledge of the fundamentals of FortiGate, as presented in the FortiGate Security course

Programa

1. Introduction and Initial Configuration
2. Firewall Policies
3. Network Address Translation
4. Firewall Authentication
5. Logging and Monitoring
6. Certificate Operations
7. Web Filtering
8. Application Control
9. Antivirus
10. Intrusion Prevention and Denial of Service
11. Security Fabric
12. Routing
13. Virtual Domains
14. Fortinet Single Sign-On
15. ZTNA
16. SSL VPN
17. IPsec VPN
18. High Availability
19. Diagnostics

Fechas Programadas

A petición. Gracias por contactarnos.

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.