AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 26/02/2024

Sign up

Fortinet Training: Fortigate Infrastructure Security (**EDU-NSE4**)

EXAMINATION NOT INCLUDED IN PRICE

5 days (35 hours)

PRESENTATION

In recent years, Fortinet has become a leader in network security, with its Fortigate tool for unified threat management consolidating several security functions such as firewall, intrusion prevention, web filtering, anti-malware and anti-spam protection.

In this 5-day training course, Fortigate Security will focus on the first 3 days, so that you can grasp the fundamentals of this technology. You'll get hands-on experience with equipment located in our training environment. Through exercises you will configure firewall rules, IPSEC VPN tunnels, SSL VPN access, malware protection, URL filtering profiles, user authentication through a captive portal.

At the end of these 5 days, we'll move on to Fortigate infrastructure and you'll get to grips with FortiGate's advanced architecture functions. You'll configure SD-Wan, advanced routing, FortiGate high availability, transparent mode, redundant IPsec tunnels, VDOMS, Single Sign On and more.

At the end of this 5-day training course, you will be able to master Forgate Security and its infrastructure, and pass the NSE4 certification.

As with all our training courses, we'll be using the latest stable version of Fortigate 7.4.

Fortigate Security objectives

- Describing FortiGate's UTM functionalities
- Neutralize malware threats, harmful applications and limit access to inappropriate sites
- Control network access according to device type
- Authenticate users through a customizable captive portal
- Implement an SSL VPN for mobile users' access to the corporate network
- Implement an IPsec VPN for mobile users' access to the corporate network
- Apply PAT, NAT source and NAT destination
- Interpret logs and generate reports
- Using the GUI and CLI
- Implementing anti-intrusion protection
- Control the use of applications on your network

Fortigate Infrastructure objectives

- Configuring SD-Wan
- Monitor the status of each SDWan link
- Configuring load balancing within SD-Wan
- Deploying a cluster on FortiGate
- Inspect and secure network traffic without impacting routing
- Analyze a FortiGate routing table
- Divide a physical FortiGate into several independent virtual FortiGates using Virtual Domains.
- Designing and selecting an IPsec VPN architecture
- Compare IPsec VPNs in Interface (route-based) or Tunnel (policy-based) mode
- Implement a new IPSec VPN architecture
- Troubleshoot and diagnose simple problems on FortiGate
- Implement user identification or transparent authentication in active Directory environments

TARGET AUDIENCE

- FortiGate network and security architect
- FortiGate firewall administrator

PREREQUISITES

- Knowledge of OSI model layers
- Knowledge of firewall concepts

FortiGate Security Program - 3 days

Introduction to FortiGate and UTMs

- High-level features

- Implementation decisions
- Basic administration
- Integrated servers
- Fundamental Maintenance
- FortiGate in the Security Fabric

Firewall

- Firewall rules
  - Firewall policies
  - Configuring firewall strategies
  - Firewall policy management
- Firewall rules with user authentication
  - Authentication firewall authentication methods
  - Remote authentication servers
  - User groups
  - Using firewall policies for authentication
  - Authentication via a captive portal
  - Monitoring and troubleshooting

The NAT

- Introduction to NAT
- NAT firewall policy
- NAT central
- Sessions

Log management and supervision

- Log Basics
- Local Logging
- Remote Logging
- Log Settings
- View, Search, and Monitor Logs
- Protecting Log Data

Certificates Application control & URL filtering

- Certificates
  - Authentication and data security using certificates
  - Inspect figures
  - Managing digital certificates in FortiGate

- Application control
  - Inspection modes
  - Web filtering basics
  - Additional proxy-based Web filtering functions
  - DNS filtering
- URL filtering
  - Inspection modes
  - Web filtering basics
  - Additional proxy-based Web filtering functions

VPNS

- VPN SSL
  - Describe SSL-VPN
  - SSL-VPN deployment modes
  - SSL-VPN configuration
  - Kingdoms and personal bookmarks
  - SSL-VPN access
- IPSEC VPN in dial-up mode
- IPsec Introduction
- IKE Phase 1 and IKE Phase 2
- Dialup IPsec VPN

FortiGate Infrastructure Program - 2 days

Routing

- FortiGate routing
- Routing monitor and route attributes
- Multipath routing

SD-Wan

- Introduction to the software-defined WAN
- SD-WAN performance SLA
- SD-WAN rules

Virtualization & L2 analysis

- Virtualization
  - VDOM concepts
  - VDOM administrators
  - VDOM configuration
  - Inter-VDOM links
- L2 analysis
  - IPSec VPN in site-to-site mode
  - The FSSO
  - High availability
  - The explicit proxy
  - Diagnostics

IPSec VPN in site-to-site & FSSO mode

- VPN
  - VPN topologies
  - Site-to-site VPN configuration
- FSSO
  - FSSO function and deployment
  - FSSO With Active Directory
  - NTLM authentication
  - FSSO parameters

Proxy Explicite

- Web proxy concepts
- Web proxy server configuration
- Authentication and authorization of Web proxy servers

High availability & Diagnostics

- HA Operating modes
- HA cluster synchronization
- Workload and AP tilting
- Diagnostics
  - General diagnosis
  - Debug flow
  - CPU and memory
  - Firmware and Hardware

Certification

This course and FortiGate Infrastructure prepare you for NSE4 certification.

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.