FORTINET CERTIFIED SOLUTION SPECIALIST
Zero Trust Access

FORTINET
Authorized
Premier Training Center

Zero Trust Access

In this course, you will learn how to define, design, deploy, and manage Zero Trust Access (ZTA) using different Fortinet solutions. You will also learn how to configure FortiGate, FortiClient EMS, FortiAuthenticator, FortiNAC, and FortiAnalyzer to secure network and application access, monitor ZTA enforcement, and automate incident response.

Product Version

- FortiOS 7.2
- FortiSwitch 7.2
- FortiClient EMS 7.0
- FortiNAC 9.4
- FortiAuthenticator 6.4
- FortiAnalyzer 7.2

Course Duration

- Lecture time (estimated): 4 hours
- Lab time (estimated): 9 hours
- Total course duration (estimated): 13 hours
  - 2 full days or 3 half days

Who Should Attend

Networking and security professionals involved in the design, implementation, and operation of ZTA solutions using Fortinet products should attend this course.

Certification

This course is intended to help you prepare for the *Fortinet NSE 7 - Zero Trust Access 7.2* certification exam. This exam is in the Fortinet Certified Solution Specialist - Zero Trust Access certification track.

Prerequisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- *FCP - FortiGate Infrastructure*
- *FCP - FortiGate Security*
- *FCP - FortiClient EMS*
- *FCP - FortiAnalyzer*
- *FCP - FortiAuthenticator*
- *FCP - FortiNAC*

Agenda

1. ZTA Overview
2. ZTA Components
3. Securing Network Access With FortiNAC
4. Configure ZTNA for Secure Application Access
5. Expanding Secure Access With Endpoint Posture and Compliance Checks
6. Monitoring ZTA Enforcement and Responding to Incidents

Objectives

After completing this course, you will be able to:

- Understand ZTA architecture and the problems it solves
- Identify and review technology components required for ZTA enforcement
- Identify zero trust network access (ZTNA) as a component of ZTA
- Configure captive portal and agents for securely onboarding devices to the corporate, guest, and BYOD networks
- Configure security policies for onboarding and compliance, and provide dynamic access based on configured criteria
- Configure FortiGate ZTNA with tagging rules for dynamic groups and securing application access
- Configure endpoint posture and compliance checks, and monitor the status of connected endpoints
- Explain the role of a centralized logging platform (FortiAnalyzer)
- Explore remediation options to automate incident response for both on-net and off-net devices

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-ZTA

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using a purchase order (PO) through Fortinet Resellers or Authorized Training Partners.

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-ZTA-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 4
- CPE lab hours: 9
- CISSP domains: Identity and Access Management (IAM)

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.