Networking & Infrastructure

Program Brochure · 2026

FORTINET NSE 4–7 TRACK

The Fortinet security fabric.

Advanced ↗ 96 Hours ↗ NSE4-7 ↗

Networking & Infrastructure

Connect. Secure. Scale.

10 programs in this track



8

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03
Who it's for 04
Learning outcomes 05
Program runway 06
Detailed curriculum 07
Tools & frameworks 10
Projects & capstone 11
Certification & method 12
Learning path 13
FAQs 14



AT A GLANCE

Level	**Advanced**
Duration	**96 Hours**
Modules	**8**
Certificate	**NSE4-7**

Program overview

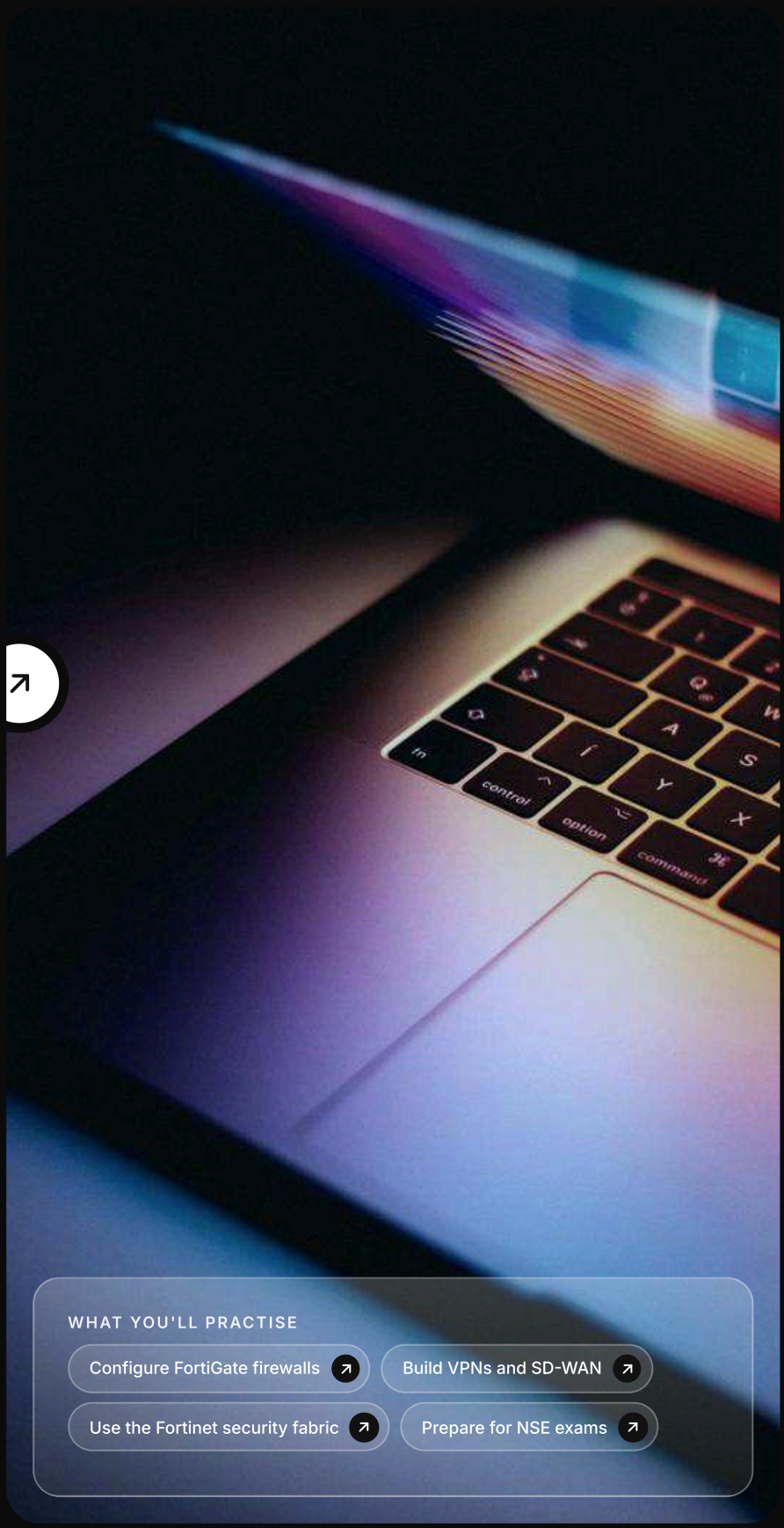
The Fortinet security fabric.

Fortinet security across FortiGate, the security fabric and advanced NSE levels.

The Fortinet Security Fabric connects firewalls, SD-WAN, switching, wireless and endpoint security into one managed platform. This advanced track builds skills from FortiGate administration through to expert-level enterprise firewall, SD-WAN and fabric design, aligned to the NSE 4 to 7 objectives, now offered by Fortinet as FCP and FCSS certifications.

DELIVERY

Instructor-led · Live virtual · Blended



WHAT YOU'LL PRACTISE

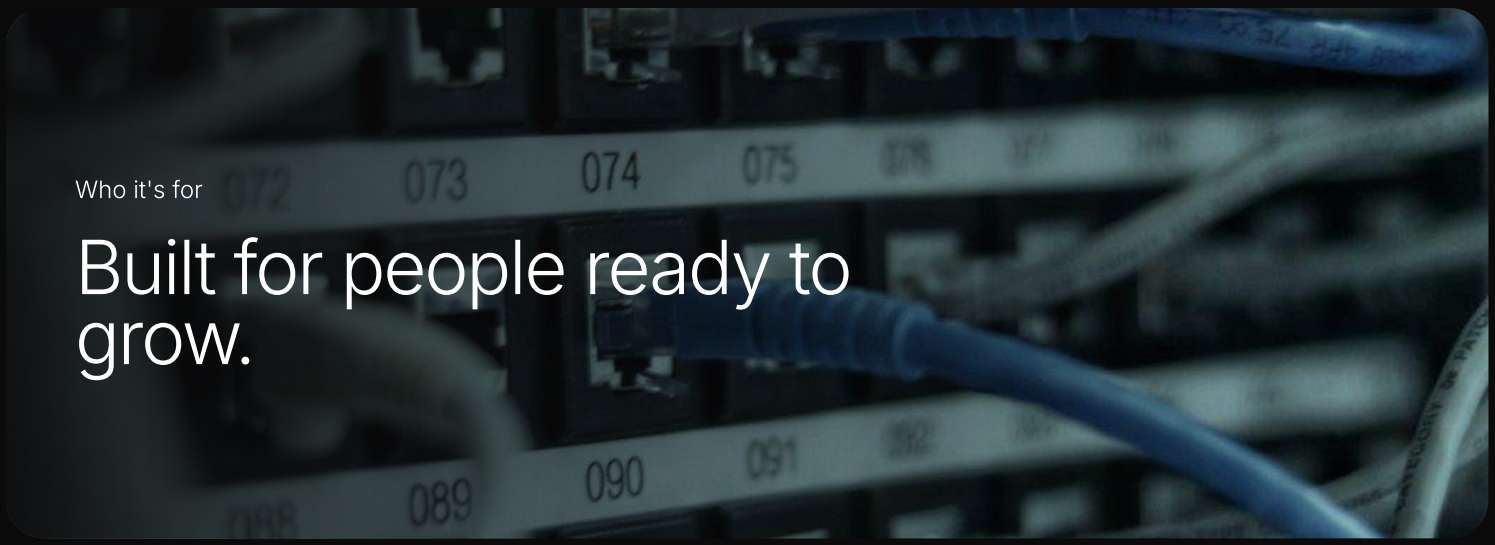
- Configure FortiGate firewalls
- Build VPNs and SD-WAN
- Use the Fortinet security fabric
- Prepare for NSE exams

LEVEL
Advanced

DURATION
96 Hours

CERTIFICATION
NSE4-7

TRACK
Networking & Infrastructure



Who it's for

Built for people ready to grow.

01

Beginners

Network+ and CCNA foundations

02

Network engineers

CCNP Enterprise, SD-WAN, automation

03

Security engineers

Palo Alto, Fortinet, network security

04

Architects

CCIE prep, Zero Trust, SASE / SSE

PREREQUISITES

- Strong TCP/IP, routing and NAT knowledge 01
- Experience with firewall or VPN concepts 02
- Familiarity with enterprise network design 03

ROLES THIS PREPARES YOU FOR

- Fortinet Security Engineer ↗
- Firewall Administrator ↗
- Network Security Engineer ↗
- SD-WAN Engineer ↗
- Security Solutions Architect ↗

Learning outcomes

What you'll be able to do.



01	Administer FortiGate firewalls, policies and security profiles confidently
02	Configure IPsec and SSL VPNs on FortiGate
03	Deploy and tune Fortinet secure SD-WAN
04	Centrally manage devices with FortiManager and FortiAnalyzer
05	Integrate fabric components for coordinated threat response
06	Troubleshoot complex FortiGate deployments using diagnostic tools

Program runway

Module by module.

8
modules · 96 hours

01	**FortiGate Administration Foundations** FortiOS architecture and initial setup, Interfaces, VLANs and zones, Firewall policies and NAT	12 hrs
02	**Security Profiles and Inspection** SSL/SSH inspection modes, Antivirus and IPS profiles, Web and DNS filtering	12 hrs
03	**VPNs and Authentication** IPsec site-to-site VPN, Dial-up IPsec and ZTNA concepts, SSL VPN and FortiClient	12 hrs
04	**High Availability and Routing** FGCP active-passive and active-active, Session synchronisation, Static and dynamic routing on FortiOS	12 hrs
05	**Fortinet Secure SD-WAN** SD-WAN zones and members, Performance SLAs, SD-WAN rules and steering	14 hrs
06	**FortiManager and FortiAnalyzer** FortiManager ADOMs and policy packages, Device provisioning and templates, FortiAnalyzer logging and reports	12 hrs
07	**Security Fabric and Advanced Defence** Security Fabric connectors, FortiSwitch and FortiAP integration, Automation stitches	12 hrs
08	**Expert Troubleshooting and Exam Prep** Diagnose debug flow, Packet sniffer and session table, VPN and SD-WAN debugging	10 hrs
★	**Capstone · Multi-Site Fortinet Fabric Build** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

FortiGate Administration Foundations

12 hours

Hands-on lab
Deploy a FortiGate VM with interfaces, policies and NAT.

TOPICS COVERED

- FortiOS architecture and initial setup
- Interfaces, VLANs and zones
- Firewall policies and NAT
- Administrative access and profiles
- Logging and monitoring

Module 02

Security Profiles and Inspection

12 hours

Hands-on lab
Apply full security profiles and verify blocking with test traffic.

TOPICS COVERED

- SSL/SSH inspection modes
- Antivirus and IPS profiles
- Web and DNS filtering
- Application control
- Proxy vs flow-based inspection

Module 03

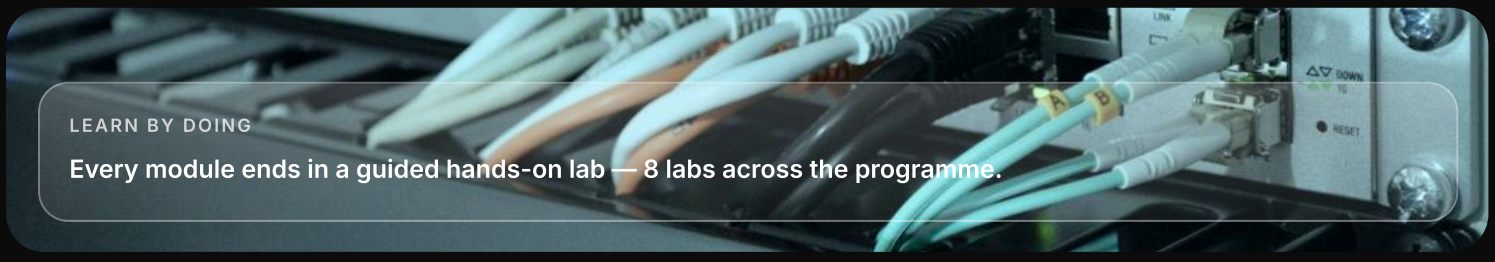
VPNs and Authentication

12 hours

Hands-on lab
Build a site-to-site IPsec VPN and remote-access VPN with LDAP users.

TOPICS COVERED

- IPsec site-to-site VPN
- Dial-up IPsec and ZTNA concepts
- SSL VPN and FortiClient
- User authentication and FSSO
- LDAP and RADIUS integration



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

High Availability and Routing

12 hours

Hands-on lab
Configure an HA cluster and verify failover with live sessions.

TOPICS COVERED

- FGCP active-passive and active-active
- Session synchronisation
- Static and dynamic routing on FortiOS
- BGP and OSPF on FortiGate
- VDOMs and multi-tenancy

Module 05

Fortinet Secure SD-WAN

14 hours

Hands-on lab
Build SD-WAN rules steering applications by SLA across two links.

TOPICS COVERED

- SD-WAN zones and members
- Performance SLAs
- SD-WAN rules and steering
- ADVPN overlays
- SD-WAN monitoring

Fortinet

Module 06

FortiManager and FortiAnalyzer

12 hours

Hands-on lab
Push a policy package from FortiManager and review FortiAnalyzer reports.

TOPICS COVERED

- FortiManager ADOMs and policy packages
- Device provisioning and templates
- FortiAnalyzer logging and reports
- Event handlers and playbooks
- Centralised change workflows



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 07–08

Module 07

Security Fabric and Advanced Defence

12 hours

Hands-on lab
Create an automation stitch that quarantines a compromised host.

TOPICS COVERED

- Security Fabric connectors
- FortiSwitch and FortiAP integration
- Automation stitches
- FortiSandbox and threat intelligence
- Enterprise firewall design

Module 08

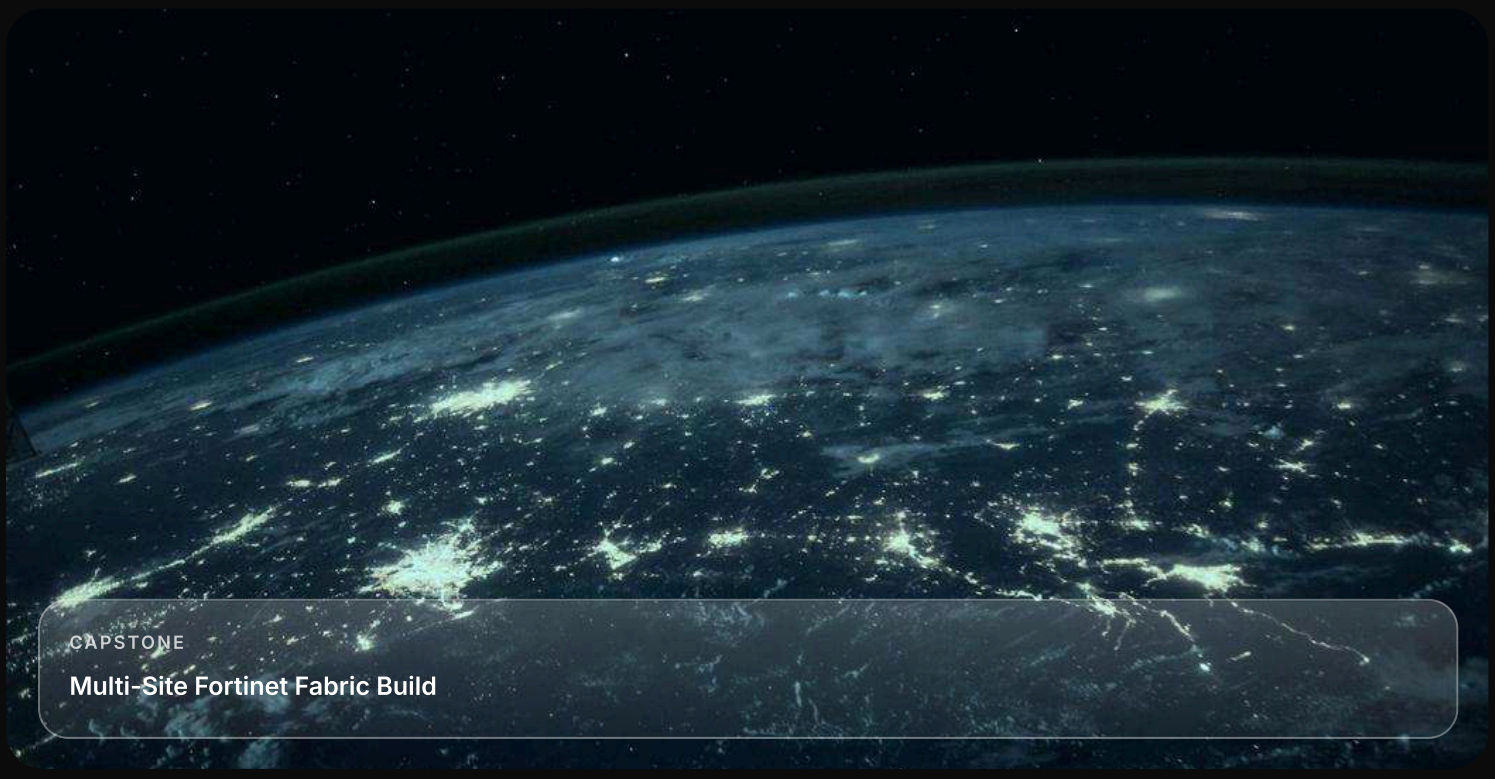
Expert Troubleshooting and Exam Prep

10 hours

Hands-on lab
Resolve injected VPN, routing and policy faults using debug flow.

TOPICS COVERED

- Diagnose debug flow
- Packet sniffer and session table
- VPN and SD-WAN debugging
- FCP and FCSS exam domains
- Timed practice scenarios



CAPSTONE

Multi-Site Fortinet Fabric Build



Fortinet
Security fabric & NGFW

What you will build

Configure FortiGate firewalls	01
Build VPNs and SD-WAN	02
Use the Fortinet security fabric	03
Prepare for NSE exams	04



01

Branch FortiGate Deployment

Deploy a FortiGate branch with security profiles, SSL inspection, VPN to headquarters and documented policies.

02

Secure SD-WAN Design

Design and implement secure SD-WAN across two branches with performance SLAs, application steering and an ADVPN overlay between sites.

03

Fabric Automation Response

Integrate Security Fabric components and build automation stitches that detect, alert on and isolate compromised endpoints without manual intervention.



Capstone project

Multi-Site Fortinet Fabric Build

Design and deploy a centrally managed multi-site Fortinet environment with HA, VPNs, secure SD-WAN, security profiles and fabric automation, then troubleshoot injected faults and present the architecture.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

NSE4-7

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

Real-world attack and use-case scenarios open every module.

Phase 02

Apply

Hands-on lab work, CTF challenges and live projects.

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive

Learning path · Networking & Infrastructure

Where this program fits.

Beginner	Intermediate	Advanced	Expert
2 programs	3 programs	You are here	2 programs

Before this

Cisco CCNP Enterprise	120 Hours
Network Security Fundamentals	48 Hours
SD-WAN & Network Automation	56 Hours

Up next

Zero Trust Network Architecture	48 Hours
SASE & SSE Architecture	40 Hours



CAREER ROLES

- Fortinet Security Engineer
- Firewall Administrator
- Network Security Engineer
- SD-WAN Engineer
- Security Solutions Architect

Questions, answered.

Q01

Do I need prior experience to join?

Yes. You should understand TCP/IP, routing, NAT and VPN concepts and ideally have firewall administration experience. Prior Fortinet exposure helps, but FortiGate fundamentals are covered at the start before advancing to expert topics.

Q02

How is the program delivered and scheduled?

The 96 hours program is instructor-led and delivered live virtual or blended, combining concept sessions, demonstrations and guided hands-on work. Batch timings and session frequency are confirmed with the academy team at enrollment.

Q03

Will I get a certificate, and is the official exam included?

You receive a Samcommunity Academy certificate of completion after passing the program assessments. The Fortinet FCP and FCSS (formerly NSE 4–7) exam is booked and taken separately through Fortinet's official testing process; exam fees are included only if stated in your enrollment details.

Q04

What labs and tools will I have access to?

Labs use FortiGate, FortiManager and FortiAnalyzer virtual machines where licensing permits, alongside Linux and Windows test hosts. Lab access arrangements and setup guidance are shared during onboarding.

Q05

Is career support provided?

Yes. You receive guidance on building a portfolio from your projects, presenting skills on your resume and preparing for interviews. Career support helps you present yourself well, but job placement, interviews and salaries are not guaranteed.

Let's talk

START FORTINET NSE 4–7 TRACK.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India