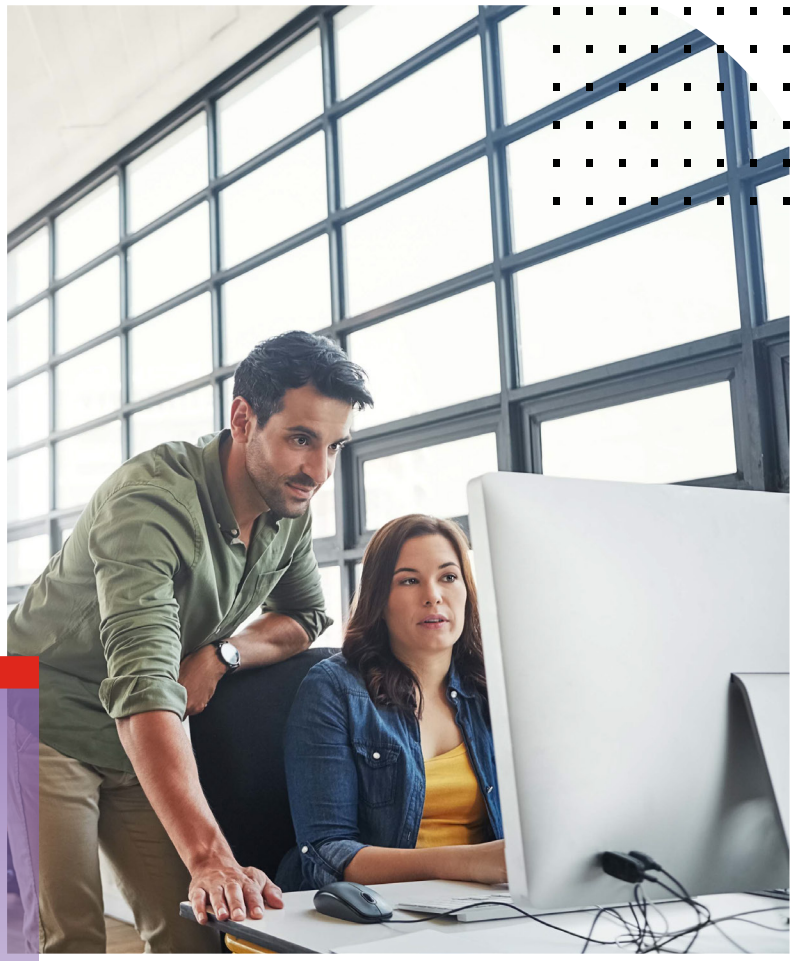
FORTINET
NSE Training Institute

EDUCATION PATHWAY

Security-Driven Networking



NSE Training Institute

The purpose of NSE Training Institute Education Pathways is to create a career map through Fortinet's NSE Training Institute learning, allowing individuals to navigate their educational journey from curriculum to careers. This education pathway focuses on Security-Driven Networking (SDN) and the potential job opportunities that exist around the technology.

Security-Driven Networking

Network security refers to the technologies and policies used to defend any network, network traffic, and network-accessible assets from cyberattacks, unauthorized access, and data loss. It must protect at both the edge and inside the network, with a layered approach.

Networks are continually growing and evolving, and new technologies increase the attack surface and open the door to new threats. At the same time, cyber criminals are launching increasingly sophisticated attacks. The following are common challenges to securing networks:

- Network performance slowdowns
- Sophisticated, targeted attacks
- Lack of visibility into entire network
- Complexity: too many disparate products
- Shortage of IT professionals

NIST/NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed.

NICE Cybersecurity Workforce Framework—Work Roles

Work Roles act as the most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks. Work Roles are not specific job titles.

Fortinet's NSE Training Institute's Security-Driven Networking education pathway aligns to the following NICE Cybersecurity Workforce Work Roles.

Work Role	NSE 4	NSE 5	NSE 7
All-Source Analyst (AN-ASA-001)		X	
Cyber Defense Infrastructure Support Specialist (PR-INF-001)	X	X	
Database Administrator (OM-DTA-001)		X	
Enterprise Architect (SP-ARC-001)			X
Information Systems Security Developer (SP-SYS-001)			X
Information Systems Security Manager (OV-MGT-001)			X
Mission Assessment Specialist (AN-ASA-002)		X	
Security Architect (SP-ARC-002)			X
Security Control Assessor (SP-RSK-002)			X
Systems Developer (SP-SYS-002)			X
Systems Requirements Planner (SP-SRP-001)			X
Technical Support Specialist (OM-STS-001)			X
Vulnerability Assessment Analyst (PR-VAM-001)	X	X	

Security-Driven Networking Curriculum

NSE 4 FortiGate Security *24 content hours* *NSE 4* FortiGate Infrastructure *16 hours* *NSE 4*	**In this course, participants will learn how to use basic FortiGate features, including security profiles.** Participants will explore firewall policies, security fabric, user authentication, secure sockets layer virtual private network (SSL VPN), dial-up internet protocol security (IPsec) VPN, and how to protect a network using security profiles such as intrusion prevention system (IPS), antivirus, web filtering, application control, and more. These administration fundamentals will provide participants with a solid understanding of how to implement basic network security. **In this course, participants will learn how to use advanced FortiGate networking and security.** Topics include features commonly applied in complex or larger enterprise or managed security service provider (MSSP) networks, such as advanced routing, transparent mode, redundant infrastructure, site-to-site IPsec VPN, single sign-on (SSO), web proxy, and diagnostics.
NSE 5 FortiManager *16 content hours* *NSE 5*	**In this class, participants will learn the fundamentals of using FortiManager for centralized network administration of many FortiGate devices.** Participants will explore deployment strategies, which include single or multiple ADOMs, device registration, policy packages, shared objects, installing configuration changes, provisioning FortiManager as a local FortiGuard distribution server, and troubleshooting the features that are critical to day-to-day use after you deploy FortiManager.
NSE 7 Enterprise Firewall *24 content hours* *NSE 7*	**In this course, participants will learn how to implement, troubleshoot, and centrally manage an enterprise security infrastructure composed of multiple FortiGate devices.**

Security-Driven Networking Workshops

What's New in FortiOS

In this workshop, participants will learn about the new FortiOS features and capabilities that were designed to provide the broad visibility, integrated threat intelligence, and automated response required for digital business.

Getting Started with the FortiGate Firewall

In this workshop, participants learn the basics of how to install a FortiGate and use it to protect a network.

Constructing a Secure SD-WAN Architecture

As organizations transition to a digital business model, their network topologies are significantly impacted. The adoption of cloud services, the virtualization of the traditional network, and an increasingly mobile workforce accessing applications in the cloud are accelerating advancements.

SD-Branch: Securing Your Network Access Infrastructure with FortiSwitch, FortiAP, and FortiLink

Fortinet secure access architecture powered by FortiLink is uniquely suited to SD-Branch deployments, with Ethernet switch and wireless access point management built into the same platform that drives our Secure software-defined wide-area network (SD-WAN) solution, the FortiGate, and FortiOS.

Fortifying the Enterprise Network (NGFW Solution)

In this workshop, participants learn how Fortinet network security leverages a single operating system that works across different network security use cases.

Cybersecurity for Safe, Reliable, Secure Industrial Control Systems (ICS)

Connections between IT and operational technology (OT) systems are no longer air gapped, introducing the potential for hackers to penetrate industrial control systems, risking the safety and availability of critical infrastructure. Security for OT requires visibility, control, and analytics to meet safety and availability requirements.

Fortinet Company Overview

Fortinet (NASDAQ: FTNT) secures top Fortune 100 enterprises, leading service providers, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface, enabling them to meet the ever-increasing performance requirements of the borderless network both today and into the future.

Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments.

Fortinet ranks #1 in the most security appliances shipped worldwide, and provides the broadest protection on the market from IoT to the cloud. As the leading security innovator, Fortinet holds more patents than any other vendor. More than 385,000 customers trust Fortinet to protect their businesses with the Fortinet Security Fabric.

Learn more at Fortinet.com, FortiGuard Labs, NSE Certification Program, Security Academy Program, or the Veterans Program.

FORTINET
NSE Training Institute

www.fortinet.com

April 21, 2021 12:36 AM
D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\927903 - Security Driven Networking\ep-security-driven-networking-4152021\ep-security-driven-networking-4152021
834549-A-0-EN