FORTINET
NSE Training Institute

EDUCATION PATHWAY

Adaptive Cloud Security

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 Adaptive Cloud Security and the potential job opportunities that exist around the technology.

Adaptive Cloud Security

As cloud adoption accelerates, organizations are increasingly reliant on cloud-based services and infrastructures. Yet, organizations often end up with a heterogeneous set of technologies in use, with disparate security controls in various cloud environments. Fortinet Adaptive Cloud Security solutions provide the necessary visibility and control across cloud infrastructures, enabling secure applications and connectivity from data center to cloud.

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

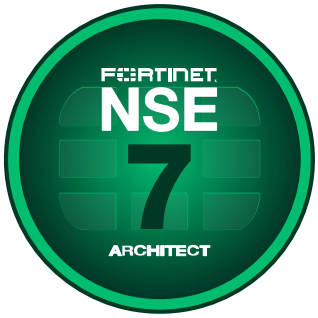
Work Roles act as the most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks. Work Roles are not specific job titles.

Fortinet's NSE Training Institute's Adaptive Cloud Security education pathway aligns to the following NICE Cybersecurity Workforce Work Roles.

Certifications

Work Role	NSE 4	NSE 6	NSE 7
All-Source Analyst (AN-ASA-001)		X	
Cyber Operator (CO-OPS-001)		X	X
Information Systems Security Developer (SP-SYS-001)	X		X
Information Systems Security Manager (OV-MGT-001)	X		
Product Support Manager (OV-PMA-003)	X	X	
Secure Software Assessor (SP-DEV-002)		X	
Systems Developer (SP-SYS-002)	X		X
Systems Requirements Planner (SP-SRP-001)	X		X
Technical Support Specialist (OM-STS-001)	X	X	
Threat/Warning Analyst (AN-TWA-001)		X	X

Adaptive Cloud Security Certifications



NSE 4 FortiGate Security *24 content 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), 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.
FortiGate Infrastructure *16 content hours* *NSE 4*	**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 6 FortiMail *26 content hours* *NSE 6*	**In this class, participants will learn how to use FortiMail to protect your networks from existing email-borne threats. Additionally, participants will learn how to integrate with FortiSandbox to detect and block emerging threats.** Participants will explore the role of FortiMail as a specialized device, and how its features extend beyond FortiGate email filtering to provide both high-performance and in-depth security for business-critical communications. Participants will analyze email security challenges that administrators of small businesses and carriers face, and learn where and how to deploy, manage, and troubleshoot FortiMail.
FortiWeb *24 content hours* *NSE 6*	**In this class, participants will learn how to deploy, configure, and troubleshoot Fortinet's web application firewall: FortiWeb.** This course will explain key concepts of web application security, and lead lab exercises in which you will explore protection and performance features. In the lab, you will experience traffic and attack simulations that use real web applications. Participants will work with simulations to learn how to distribute load from virtual servers to real servers, while enforcing logical parameters, inspecting flow, and securing hypertext transfer protocol (HTTP) session cookies.

FortiADC *8 content hours* *NSE 6*	**In this class, participants will learn how to configure and administrate the most commonly used features of a FortiADC.** Participants will explore Layer 4 and Layer 7 server load balancing, link load balancing, global load balancing, high availability, firewall policies, advanced routing, and more. These administrative fundamentals will provide participants with a solid understanding of how to implement an application delivery controller.
FortiDDoS *8 content hours* *NSE 6*	**In this class, participants will learn how to form network baseline data, and how to recognize and mitigate individual and distributed denial-of-service (DDoS) attacks while preserving service and network performance.** Participants will deploy FortiDDoS to learn about normal network traffic patterns. Participants will simulate attacks, observe the defense, and adjust the automatically estimated behavior. With a focus on core feature skills, topics also include network behavior analysis and application-specific integrated circuit (ASIC) chips.
NSE 7 Private Cloud *16 content hours* *NSE 7*	**In this advanced course, participants will learn about the different components that make up the infrastructures of private clouds and the security challenges these environments present.** Participants will learn how to address these security challenges with the Fortinet cloud security offering, using the software-defined network (SDN) connectors, and how to deploy a FortiGate VMX and configure the Fortinet integration with OpenStack.

Adaptive Cloud Security Workshops

FortiADC Application Delivery Without Limits

With bandwidth demand growing faster than budgets, and with cyberattacks constantly on the rise, it can be challenging to securely, and efficiently, deliver applications at the speed users expect.

Advanced Email Security Solution With FortiMail

In this workshop, participants learn how FortiMail replaces incumbent secure email gateways with a product tailored for advanced threat defense, including Microsoft 365 integration and Client to Authenticator Protocol (CTAP) program.

Achieve PCI DSS Compliance With FortiWeb

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using artificial intelligence (AI)-enhanced multilayer and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day attacks.

Security, Visibility, and Control of Public Cloud Infrastructure and Workloads

In this workshop, participants learn how to provision and secure public cloud resources using the Fortinet Security Fabric. Participants will create public and private cloud fabric connectors and apply intent-based segmentation to effectively manage risk in multi-cloud environments.

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 16, 2021 11:07 PM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\927904 - Adaptive Cloud Security\ep-FA-adaptive-cloud-security-4162021\ep-FA-adaptive-cloud-security-4162021

834265-A-0-EN