FORTINET
NSE Training Institute

Zero-Trust Access Education Pathway

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 Zero-Trust Access and the potential job opportunities that exist around the technology.

Zero-Trust Access

The growth of unsecure or unknown devices attaching to the network, along with a host of breaches due to stolen credentials, has stretched trust beyond the breaking point. Network administrators must adopt a zero-trust approach to network access. Fortinet Network Access solutions offer the necessary device security to see and control all devices and users across the entire network. With proactive protection, organizations can ensure their networks are secure from the latest threats.

Fortinet's unique Zero-Trust Access framework leverages a tightly integrated collection of security solutions that enables enterprises to:

- Identify and classify all users and devices seeking network access
- Assess their state of compliance with internal security policies
- Automatically assign them to zones of control
- Continuously monitor them both on and off the network

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 Zero-Trust Access 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 Defense Infrastructure Support Specialist (PR-INF-001)	X		
Cyber Operator (CO-OPS-001)		X	
Information Systems Security Developer (SP-SYS-001)			X
Information Systems Security Manager (OV-MGT-001)			X
Product Support Manager (OV-PMA-003)		X	X
Security Architect (SP-ARC-002)			X
Systems Developer (SP-SYS-002)			X
Systems Requirements Planner (SP-SRP-001)			X
Technical Support Specialist (OM-STS-001)		X	X
Vulnerability Assessment Analyst (PR-VAM-001)			X

Zero-Trust Access Curriculum

Zero-Trust Access Courses Sequence

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

FortiNAC
24 content hours
NSE 6

In this course, participants will learn how to leverage the powerful and diverse capabilities of FortiNAC, using best practices for achieving visibility, control, and response.

Participants will explore the administrative tasks necessary to achieve network visibility, control, and automated threat response. These fundamentals will provide participants with a solid understanding of how to implement network visibility and security automation.

Integrated and Cloud Wireless
8 content hours
NSE 6

In this course, participants will learn how to deploy, configure, and troubleshoot secure wireless LAN using an integrated wireless solution. This includes FortiGate, FortiAP, FortiWiFi, FortiAP Cloud, FortiPlanner and FortiPresence. The course explores RF concepts and key standards for wireless LAN, devices configuration, security settings, and troubleshooting.

Participants will enforce their knowledge deploying a secure wireless LAN centrally managed from the FortiGate wireless controller.

FortiVoice
16 content hours
NSE 6

FortiAuthenticator
16 content hours
NSE 6

In this course, participants will learn how to configure FortiVoice systems, including using the phones.

Participants will explore FortiVoice profiles, extension setups, trunk configurations, and call features.

In this class, participants will learn how to use FortiAuthenticator for secure authentication and identity management. Participants will learn how to configure and deploy FortiAutheticator, use FortiAuthenticator for certificate management and two-factor authentication, authenticate users using LDAP and RADIUS servers, and explore SAML SSO and how FortiAuthenticator can act as both a SAML identity provider and service provider. Finally, participants will examine some helpful troubleshooting techniques.

In interactive labs, participants will explore how to authenticate users, with FortiAuthenticator acting as a RADIUS and LDAP server, a certificate authority (CA), and logon event collector that uses—and extends—the Fortinet Single Sign-On (FSSO) framework to transparently authenticate users. Participants will explore portal services, FortiTokens, and digital certificates.

NSE 7

Secure Access
16 content hours
NSE 7

In this course, participants will learn how FortiGate, FortiAP, FortiSwitch, and FortiAuthenticator enable secure connectivity over wired and wireless networks. Participants will also learn how to provision, administer, and monitor FortiAP and FortiSwitch devices using FortiManager. This course covers the deployment, integration, and troubleshooting of advanced authentication scenarios, as well as best practices forsecurely connecting wireless and wired users. Participants will learn how to keep the network secure by leveraging Fortinet Security Fabric integration between FortiGate, FortiSwitch, FortiAP, and FortiAnalyzer to automatically quarantine risky and compromised devices using IOC triggers.

Zero-Trust Access Workshops

Securely Embrace the IoT Revolution with FortiNAC

The proliferation of Internet-of-Things (IoT) devices has made it necessary for organizations to improve their visibility into what is attached to their networks. They need to know every device and every user accessing their networks.

Fortinet Teleworker Solution Engineered for Remote and Secure Productivity

In this workshop, participants learn about how Fortinet solutions offer an integrated solution to support telework. FortiGate next-generation firewalls (NGFWs) have built-in support for IPsec VPNs, enabling remote workers to connect securely to the company network.

Proactive Advanced Endpoint Protection, Visibility, and Control for Critical Assets

Fortinet strengthens endpoint security through integrated visibility, control, and proactive defense. With the ability to discover, monitor, and assess endpoint risks, organizations can ensure endpoint compliance, mitigate risks, and reduce exposure.

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

February 17, 2021 2:59 AM

834901-0-0-EN

D:\Fortinet\2020 Old templates\Image Graphics\Academy Pathways\898648 - Education Pathways Segments\FA-zero-trust-access-education-pathway-2172021\FA-zero-trust-access-education-pathway-2172021