NSE8: Fortinet Network Security Expert 8 Practical Exam (802)

Opis

Praktyczny egzamin NSE8: Fortinet Network Security Expert 8 Practical Exam (802) jest dostępny dla kandydatów po spełnieniu warunku dopuszczenia do niego, jakim jest zaliczenie w pierwszej kolejności egzaminu pisemnego NSE8: Fortinet Network Security Expert 8 Written Exam (801) w jednym z centrów testowych Pearson VUE. Do egzaminu praktycznego może podejść bezpośrednio w jednym z ośrodków testowych NSE 8 zlokalizowanych w siedzibach firmy Fortinet na całym świecie lub w formie zdalnej. Podczas 2 dniowego egzaminu praktycznego NSE 8 kandydacie muszą przeprowadzić konfigurację szeregu produktów Fortinet i zbudować oraz zweryfikować pełną topologię sieci – wszystkie zadania praktyczne odpowiadają zagadnieniom z egzaminu pisemnego

Podczas obu egzaminów nie są dozwolone jakiekolwiek dodatkowe/pomocnicze materiały – wszelkie tego typu pomoce kandydaci muszą zostawić poza salami egzaminacyjnymi.

UWAGA.

Egzaminy NSE 8 (pisemny i praktyczny) są egzaminami przygotowanymi dla ekspertów w dziedzinie bezpieczeństwa sieci i całego portfolio produktów bezpieczeństwa Fortinet. Proces przygotowania do egzaminu może być kosztowny i czasochłonny. Oprócz formalnego wykształcenia, trzeba posiadać doświadczenie praktyczne z różnorodnych, złożonych środowisk sieciowych oraz doświadczenie wynikające z rozwiązywania skomplikowanych problemów związanych z bezpieczeństwem.

Aktualna wersja egzaminu bazuje na następujących wersjach oprogramowania:

FortiGate 5.2.x

FortiManager / FortiAnalyzer 5.2.x

FortiADC (VM and D series) 4.3.x

FortiWeb 5.3.x

FortiSandbox 2.0.x

FortiAuthenticator 3.0.x

FortiMail 5.2.x

FortiVoice Enterprise 4.0.x

Wymagania

Pozytywny wynik egzaminu. Nie ma punktacji cząstkowej pytań, każda z udzielonych odpowiedzi musi być w 100% prawidłowa.

Przebieg egzaminu:

Maksymalny czas trwania egzaminu: 2 dni pod nadzorem prowadzącego.

Egzamin w języku angielskim.

Pytania typu test wyboru :

- jedna prawidłowa odpowiedź
- wiele prawidłowych odpowiedzi
- odpowiedzi do ręcznego uzupełnienia

Przybliżona liczba zadań: 48

W przypadku niepowodzenia kolejne podejście do egzaminu jest możliwe po 15 dniach karencji. W przypadku pozytywnego wyniku informacja o posiadaniu certyfikacji NSE 7 pojawi się w transkrypcie kandydata w Fortinet Learning Center (FLC) w przeciągu maksymalnie 21 dni.

Kandydat otrzymuje dokument z informacją zdał lub nie zdał oraz wyszczególnieniem, które sekcje zostały zaliczone a które nie. Ponad tą informację nie są udzielane jakiekolwiek bardziej szczegółowe informacje.

Cena egzaminu (podana przez producenta):

1600 USD

Gdzie

Egzamin praktyczny zdawany jest w wyznaczonych ośrodkach testowych NSE 8 zlokalizowanych w wyznaczonych lokalizacjach firmy Fortinet na całym świecie lub zdalnie. Egzamin wymaga wcześniejszego potwierdzenia terminu i dostępności laboratorium egzaminacyjnego.

Zagadnienia egzaminacyjne:

Egzamin NSE8: Fortinet Network Security Expert 8 Exam został zaprojektowany do sprawdzania wiedzy i umiejętności kandydatów z następujących obszarów (w przypadku egzaminu praktycznego jest to weryfikacja realnych umiejętności praktycznych) :

- FortiGate device operation
    - Controlling management access
    - CLI operation and configuration
        - Commands
        - Advanced CLI configuration
    - Advanced troubleshooting
        - Diagnostics
        - Packet and flow captures
        - Analysis
    - GUI operation and configuration
        - Dashboards
        - Menus
    - Hardware operation and configuration
        - Hardware-related features and configuration
    - Firmware management
        - Upgrades
- FortiGate operation modes and VDOMS
    - Operation mode definition and configuration
        - NAT / route mode
        - Transparent mode
    - Cluster operation
        - Advanced cluster management
        - Different cluster operation options
    - Advanced VDOM operation and configuration
        - Resource settings
        - Operation modes
        - Inter-VDOM configurations
    - Virtual clustering
        - Operation and configuration

- FortiGate network connectivity and reachability
    - High availability (HA) operation and configuration
        - Operation modes
        - Configuring and connecting
    - Advanced clustering operation
        - Cluster management
        - VDOMs and HA
        - Virtual Cluster HA
    - HA and load balancing
    - Advanced FortiOS network connectivity
        - WAN load balancing
        - Link load balancing
    - Advanced interface operation and configuration
        - VLANs
        - Wireless
        - DHCP
        - LACP
    - OSI Layer 2 protocols
        - VLANs
        - ARP
        - Layer 2 features and configurations
    - IPv4 addressing and routing
        - Static routing
        - IPv4 to IPv6
    - IPv6 addressing and routing
        - Static routing
        - IPv6 to IPv4
    - Advanced static and dynamic routing
        - IPv4 and IPv6: static, BGP, OSPF
- FortiGate policies and NGFW
    - Advanced firewall operation and configuration
        - Firewall policies
            - IPv4
            - IPv6
        - Web and explicit proxy
    - Advanced security policies
        - Security profile configuration
    - NAT operation and configuration
        - Basic NAT
        - Advanced NAT: NAT64, NAT46

    - Firewall policies
        - Advanced configuration and features
    - Endpoint control operation and configuration
        - Device identification
    - Third-party integration
        - Protocols
        - Features
- FortiGate VPNs
    - Advanced IPSec VPN operation and configuration
        - Dynamic IPsec
        - VPN tunnels
        - Authentication
    - Advanced SSL VPNs operation and configuration
        - Modes of operation and configuration
        - SSL VPN web portals
        - Secure browsing
    - VPNs and advanced routing
        - VPNs and static routing
        - VPNs and dynamic routing
- FortiGate authentication
    - Users and user groups
    - Authentication methods ‘operation and configuration
    - Firewall policies and authentication
    - Fortinet Single Sign-On
    - Third-party integration and authentication
    - Two-factor authentication
- Fortinet wireless solutions
    - Deploying wireless solutions
    - FortiGate as wireless controller
    - Configuring secure wireless
    - Protecting wireless networks
- Fortinet centralized reports and management
    - Remote log and reporting operation and configuration
    - FortiAnalyzer operation and configuration
        - Advanced FortiAnalyzer features
    - FortiManager operation and configuration
        - Advanced FortiManager features
    - FortiOS logging and reporting
- Fortinet advanced technologies
    - FortiGate security features and advanced technologies integration

        - Architecture integration
        - Design integration
        - Interoperability between FortiGate and advanced technologies solutions
    - FortiADC (D series) operation and configuration
        - Basic networking
        - Deployment options
        - System management
        - Server load balancing and its components
    - FortiWeb operation and configuration
        - Basic networking
        - Deployment options
        - Policy configuration
        - User authentication
        - Load balancing configuration
        - Attack blocking behavior and configuration
    - FortiSandbox integration and configuration
        - Basic networking
        - Deployment options
        - FortiGate and advanced technologies integration
        - Types of detection
    - FortiAuthenticator advanced operation and configuration
        - Basic setup and configuration
        - Authentication and user management
        - Fortinet Single Sign-On options
    - FortiMail advanced operation and configuration
        - Basic networking
        - Deployment options and operation modes
        - System settings configuration
        - Policy and profiles configuration
        - Antispam settings
    - FortiVoice enterprise
        - Basic settings and operation
        - Phone system settings and extensions

Jak się przygotować:

Droga do sukcesu – NSE 8
Fortinet udostępnia wiele zasobów, które pomagają w przygotowaniu się do certyfikowanych egzaminów, począwszy od ogólnodostępnej dokumentacji, bazy wiedzy, przykładowe konfiguracji po autoryzowane szkolenia. Poniższe kroki stanowią proponowaną „drogę do sukcesu” jakim jest uzyskanie tytułu NSE 8 :

Sugerowane

Znajomość następujące dokumentów:

- Administration Guides and Handbooks:
  - FortiGate
  - FortiManager
  - FortiAnalyzer
  - FortiADC (VM and D Series)
  - FortiWeb
  - FortiSandbox
  - FortiAuthenticator
  - FortiMail
  - FortiVoice (Enterprise)
- CLI References
- Cookbooks
- Fortinet Knowledge Base articles

Zapoznać się z FAQ dotyczącym certyfikacji i egzaminów NSE 8
https://www.fortinet.com/content/dam/fortinet/assets/training/NSE8_Certification_ExamFAQ.pdf

Wysoce rekomendowane

Udział w następujących szkoleniach:

NSE2 - Network Security Solutions

https://www.fortinet.com/support-and-training/training/courses/fortigate-network-security-solutions.html

NSE3 - Advanced Network Security Solutions

https://www.fortinet.com/support-and-training/training/courses/network-security-advanced-solutions.html

NSE4 - FortiGate I

http://www.compendium.pl/szkolenie/6502/szkolenie-autoryzowane-fortinet-nse4-fortigate-i

NSE4 - FortiGate II

http://www.compendium.pl/szkolenie/6503/szkolenie-autoryzowane-fortinet-nse4-fortigate-ii

NSE5 - FortiAnalyzer Network Security Reporting

http://www.compendium.pl/szkolenie/6231/szkolenie-autoryzowane-fortinet-nse5-fortianalyzer-network-security-reporting

NSE5 - FortiManager Centralized Device Management

http://www.compendium.pl/szkolenie/6232/szkolenie-autoryzowane-fortinet-nse5-fortimanager-centralized-device-management

NSE6 - FortiAP Wireless LAN

http://www.compendium.pl/szkolenie/6233/szkolenie-autoryzowane-fortinet-nse6-fortiap-wireless-lan

NSE6 – FortiDDoS

http://www.compendium.pl/szkolenie/6525/szkolenie-autoryzowane-fortinet-nse6-fortiddos

NSE6 - FortiMail Email Security

http://www.compendium.pl/szkolenie/6234/szkolenie-autoryzowane-fortinet-nse6-fortimail-email-security

NSE6 – FortiSandbox

http://www.compendium.pl/szkolenie/6523/szkolenie-autoryzowane-fortinet-nse6-fortisandbox

NSE6 - FortiWeb Web Application Firewall

http://www.compendium.pl/szkolenie/6235/szkolenie-autoryzowane-fortinet-nse6-fortiweb-web-application-firewall

NSE7 - FortiGate III

http://www.compendium.pl/szkolenie/6506/szkolenie-autoryzowane-fortinet-nse7-fortigate-iii

Wiedza z zakresu innych technologii i zagadnień:

- Advanced virtual Infrastructure knowledge and experience.
- Advanced switching and routing knowledge and experience.
- Advanced OS knowledge: Windows and Linux
- Security vulnerabilities and penetration testing tools

Doświadczenie zawodowe:

Bardzo mocno rekomendowane jest posiadanie wiedzy i wieloletniego doświadczenia związanego zarówno z rozwiązaniami Fortinet jak i innych dostawców z grupy rozwiązań sieciowych i bezpieczeństwa w obszarach:

- Projektowania
- Wdrażania
- Zarządzania/Administracji
- Rozwiązywania problemów