Network Security Expert (NSE) 8

NSE 8 Certification

Welcome to the Fortinet NSE 8 Certification exam preparation handbook. The purpose of this document is to provide all the information required by the test taker to prepare for the NSE 8 certification exams.

Fortinet NSE 8 certification recognizes the successful candidate’s comprehensive and in-depth ability to design, configure, and troubleshoot network security using Fortinet products in complex networks.

NSE 8 is the top-level certification in the Fortinet NSE program and is designed to reflect best practices using Fortinet solutions in the network security and cybersecurity industry.

Audience

The intended audience for this document is as follows:

- Network security and cybersecurity professionals interested in attempting the NSE 8 certification written and practical examinations.
- Partners, distributors, authorized training centers (ATCs), and members of the public looking for more information related to the NSE 8 program.

Certification Requirements

Assessment for Fortinet NSE 8 certification is composed of two parts: a written exam and a practical exam. There are no prerequisites to take the Fortinet NSE 8 written exam. However, the candidate must pass the NSE 8 written exam before they can take the Fortinet NSE 8 practical exam. The written exam on its own is not a certification. You must pass both the written exam and practical exam to obtain NSE 8 certification.

Written Exam

The Fortinet NSE 8 written exam is a 120-minute multiple-choice exam that is offered at Pearson VUE test centers worldwide and through the OnVUE online proctored service. Questions include design and configuration scenarios using exhibits, configuration extracts, and troubleshooting captures. The exam assesses the networking, security, and Fortinet solution knowledge and experience of the test taker.

A set of practice questions is available at the Fortinet Training Institute. The practice questions are intended to provide a reference about the type of question included in the written exam.
NSE 8 written exam details:

- Name: NSE 8 - Fortinet Network Security Expert
- Exam series: NSE8_812
- Language: English only
- Available at: Pearson VUE Test Centers and OnVUE worldwide
- Cost: USD 400.00
- Number of questions: 60
- Time allowed to complete: 120 minutes
- Scoring method: Each question must be 100% correct for credit. No partial credit is given. No deductions are made for incorrect answers.
- Types of questions: Multiple choice and multiple select with exhibits
- Time required between unsuccessful attempts: 15 days
- Retesting: A test taker cannot retest on an exam version that was already passed.
- Time for acknowledgment and score to be reflected in Training Institute transcripts: 21 days
- Scoring: Pass or fail
- Score report: At the end of the exam, a score report is displayed to the test taker showing the overall result, pass or fail, and an indication of performance for each exam section. No further details or assistance are provided. The score report is not a certificate. It is a summary of the candidate’s written exam results only. The score report can be viewed and downloaded from the candidate’s Pearson VUE account.
- Expiration: 2 years

**Practical Exam**

After the candidate has passed the prerequisite NSE 8 written exam, they can register to take the practical exam online.

The Fortinet NSE 8 practical exam is a nine (9) hour practical assessment delivered over two (2) sessions: the first one is 5 hours long, and the second one is 4 hours long. During the practical exam, the candidate must build, configure and troubleshoot a complete network topology that includes multiple Fortinet products and solutions.

Details of the NSE 8 practical exam:

- Name: NSE 8 Practical Exam
- Exam series: NSE8_870
- Language: English only
• Available at: Online proctored
• Cost: USD 1600.00
• Number of tasks: 30
  o Part 1: 15 tasks
  o Part 2: 15 tasks

  **Note:** Part 1 and Part 2 of the exam are completely separate sessions. Tasks from part 1 will not be accessible during part 2 of the exam.
• Time allowed to complete: 9 hours
  o Session 1: 5 hours
  o Session 2: 4 hours
• A session consists of the following time blocks:
  o 15 minutes (average): Validation by the proctor
  o 5 minutes (max): Reading/Accepting the Terms & Conditions
  o 5 minutes (max): Lab Instruction
  o 4 or 5 hours (max): Completing the exam tasks
  o 5 minutes(max): Exam feedback
• Task scoring method: Some tasks must be 100% correct for credit, while others allow for partial credit. No deductions are made for incorrect answers.
• Type of tasks: Hands-on configuration and troubleshooting
• Time required between unsuccessful attempts: 30 days
• Time for acknowledgment and score to be reflected in the Training Institute transcripts: 30 days
• Exam scoring: pass or fail
• The test taker will receive an Exam Summary report document showing their overall result, pass or fail, and an indication of performance for each exam section. No further detail or assistance is provided.
• Expiration: 3 years

**Instruction Training**

To prepare yourself for the NSE 8 practical exam you will be enrolled into the NSE 8 Practical Instruction Training one week before your exam date. This training consists of the following elements:

1) Instruction Video (explaining what to expect and how to work with the exam environment).
2) Quiz (to validate your understanding of the key components of the instruction video).
Exam Scheduling

Eligible students can purchase a voucher for the NSE 8 practical exam from Fortinet and request that the exam scheduling be initiated.

Refer to the ‘NSE 8 Handbook – Practical Exam Scheduling’ section for the detailed steps on how to schedule your session.

Practical Examination Components

Exam Delivery

The NSE 8 practical exam includes a rich mix of Fortinet products and solutions and is fully virtualized. Each student will work in their own unique and independent environment or pod.

All material necessary to complete the exam is provided on each pod through a remote connection:

- Digital version of the exam tasks and diagrams
- Digital access to configuration guides: handbooks, administration guides, and CLI documents for all the products and solutions are included in the exam

No external documentation or materials are allowed during the exam.

Being online proctored, each NSE 8 test taker will use their computer to connect to the exam environment from their home or office space to complete all the tasks included in the practical exam.

There are strict rules regarding your local computer setup and the location where you want to take the exam. You must fulfill all requirements to be allowed to start your exam.

Location requirements

Your testing environment must meet the following requirements to take the exam:

- A private room - No other individuals are allowed in the same room during the exam
  - The test taker must be seated at a hard surface like a desk or table, and preferably with your back to the main room entrance. Standing desks will not be permitted.
- Clean desk - No materials/tools of any kind are allowed on the desk during the exam

Computer requirements

Your computer setup must meet the following requirements for successfully connecting to the live proctor and the exam delivery environment:

- Stable internet connection (At least 4Mbps Up/Down)
- Open outbound access to the following TCP/UDP ports: 80, 443, 843, 1935, 61613
- Webcam and microphone for live interaction with the live proctor
- Mozilla Firefox Web browser
- ProctorU extension installed (https://www.proctoru.com/firefox)
- A maximum of two (2) displays are allowed
- A dual-screen setup with a resolution of at least 1920x1080 per screen is highly recommended

**Tip:** During the exam, it is not allowed to have any other application running in the background. As a best practice, you should consider creating a temporary new account on your computer with a clean profile.

Before the exam can start, the proctor will make sure your environment meets the requirements set. **Note:** If your environment does not meet the requirements, you will not be allowed to start the exam.

**Other requirements**

The following requirements must also be fulfilled to take the NSE 8 practical exam:

- The test taker must present a government-issued photo ID to the live proctor.

**Test Environment**

Each test taker’s pod will have a dedicated virtual environment with a dedicated bastion host that has all the required tools and software needed to complete the exam.

**Main software:**

- Operating System: Windows Server 2019
- Mozilla Firefox (default browser) – Accessing devices GUI
- mRemoteNG - Accessing devices CLI, Console and GUI (RDP)
- Putty – Accessing devices CLI

**Additional software:**

- Lubuntu Linux Clients (desktop)
- Debian Linux servers
- Wireshark
- Notepad++
- Foxit PDF Reader
Exam Preparation

Certification Topics

Candidates preparing for the Fortinet NSE 8 certification should be familiar with the topics covered in the certification exams.

Note: This list is a guideline only. The topics covered on the exam may change at any time without notice.

Written Exam Certification Topics

1. Security Architecture
   a. Demonstrate knowledge of FortiGate Network Security products
      i. Chassis solutions 6000/7000 modules and architecture
      ii. Correct hardware production selection based on design
   b. Demonstrate knowledge of Fortinet Security Fabric Solution deployments
      i. FortiMail
      ii. FortiSandbox
      iii. Traditional networks and hybrid/cloud/multi-cloud networks
      iv. Logging and management protocols used by Fortinet, and required network architecture for resiliency
   c. Demonstrate knowledge of Fortinet high-availability solutions
      i. Core products
      ii. Types of the HA solutions
      iii. HA and Cloud deployments
      iv. Optimization

2. Infrastructure
   a. Demonstrate knowledge of FortiGate operation modes
      i. Transparent Mode and Layer-2 Traffic
      ii. VDOM and VDOM links
   b. Demonstrate knowledge of FortiGate hardware technology
      i. NP6/NP7/nTurbo/CP9/SoC4 acceleration and acceleration concepts
      ii. Hyperscale requirements, operation, limitations
      iii. Traffic Flows during acceleration and offloading
      iv. Describe and design hardware accelerated networks with FortiGate devices
      v. FortiGate chassis/module architecture
      vi. Life of packet
      vii. Hardware offloading
   c. Demonstrate knowledge of non-FortiGate hardware technology
      i. Hardware v virtual
      ii. FAZ, SIEM
   d. Demonstrate knowledge of Fortinet solutions for cloud security
      i. Private cloud
      ii. Public cloud
      iii. SAAS
      iv. SASE

3. Networking
   a. Demonstrate knowledge of advanced routing and networking technologies
i. Static Routing
ii. Dynamic Routing (OSPF/BGP)
iii. Routing and high availability concepts
iv. Asymmetric Routing
v. Secure SD-WAN Routing
vi. Policy Routing
vii. Multi-cast routing
viii. Routing control
ix. NAT
   1. Dual-bidirectional NAT between two address domains
   2. Interpret NAT information presented in Session table output
x. IPv6
   1. NAT46 & NAT 64, SLAAC, DHCPv6, DNSv6
xi. Traffic shaping
   1. Interface-based shaping configuration
   2. Effects on hardware acceleration
xii. Virtual wire pairs
   1. VWP with VLAN tags
b. Demonstrate knowledge of advanced VPN design methodologies
   i. SSL VPN / IPSEC
   ii. Aggregate VPN
   iii. ADVVPN
   iv. VXLAN over IPSEC
   v. GRE
   vi. IKEv1 vs IKEv2 differences
c. Demonstrate knowledge of Fortinet access solutions advanced configurations and features
   i. FortiSwitch advanced configurations
      1. MCLAG
   ii. FortiAP advanced configurations
      1. Remote tunneling
   iii. Advanced use cases of FortiExtender (IPSEC VPN, VLAN mode)
      1. IPSEC VPN
      2. VLAN mode
   iv. FortiOS access control features
      1. Control Policy
      2. Device Profiling
      3. DHCP Option 82
      4. FortiNAC configuration
      5. Remediation Policy
d. Demonstrate knowledge of how to integrate Fortinet access solutions
   i. Advanced authentication for access layer
      1. FortiAP radius based dynamic vlan
      2. RADIUS based dynamic VLAN
   ii. FortiLink advanced configurations
      1. Quarantine NAC vlans
      2. FortiLink over L3
   iii. Centralized management of access products from FortiManager
   iv. Design Fortinet access layer solutions
      1. Wireless planning
      2. Switch stack design
      3. ZTNA solutions
   v. Fortinet Security Fabric and integrated management of Firewall, access, and ATP products
e. Demonstrate knowledge of application delivery
4. Secure SD-WAN
   a. Demonstrate knowledge of SD-WAN advanced architecture and design
      i. Design and implement a full featured SD-WAN solution with dynamic routing
      ii. Local traffic routing with SD-WAN
      iii. Understanding SD-WAN rules and failover
   b. Demonstrate knowledge of SD-WAN advanced features
      i. Azure vWAN
      ii. ADVPN design and requirements
      iii. Packet duplication and aggregate tunnels
      iv. Network overlays
   c. Demonstrate knowledge of SD-WAN troubleshooting
      i. Session failover with NAT
      ii. Session route change with max bandwidth method
      iii. Shortcut tunnels and BGP

5. Security Solutions
   a. Demonstrate knowledge of Fortinet application security solutions
      i. Operation and deployment modes
      ii. Designing resilient solutions
      iii. Advanced security inspection
      iv. FortiGuard services for enhanced Fortinet solutions
      v. Troubleshooting application security issues
   b. Demonstrate knowledge of Fortinet network security solutions
      i. Inspection modes
      ii. Security profiles
      iii. Troubleshooting FortiOS security features
      iv. FortiGuard services for FortiOS security services
      v. VoIP
         1. VoIP ALG / proxy
         2. SIP kernel-helper
         3. Flow SIP
      vi. HTTP/2
         1. SSL inspection with HTTP/2
   c. Demonstrate knowledge of authentication mechanisms
      i. Implement SAML authentication
      ii. Integrate external authentication using Radius / LDAP
      iii. Configuring Fortinet product authentication using FortiAuthenticator
      iv. Authentication using VSAs with Radius for automated roles / profiles
      v. Two factor authentication using certificates and tokens
      vi. Fortinet FSSO using collectors and FortiAuthenticator
      vii. Integrate with AD certificate services
      viii. RBAC, authentication and certificate management solutions with Fortinet Management products

   a. Demonstrate knowledge of Fortinet SOC solution
      i. Integrate Fortinet solutions for advanced threat protection
      ii. Security incident handling
      iii. Security incident enrichment
      iv. Threat analysis and incident response
      v. Automated remediation
      vi. Fortinet management and logging tools
   b. Demonstrate knowledge of Fortinet endpoint solutions
      i. Network admission control solution
ii. Device On-boarding using various methods  
iii. FCT Client Profile  
iv. VPN Profile Management  
v. FortiClient EMS installation package managing  
vi. EMS on net / off net  
vii. ZTNA Policy / configuration (EMS/FCT/FG/FAC)  
viii. Endpoint protection (Client/Guest)  
ix. Quarantine functions on both LAN/WLAN  
x. EDR - Playbooks / Exceptions

7. Automation  
a. Demonstrate knowledge of Fortinet Automation tools, solutions, and integrations  
   i. Automation Stitches  
   ii. Understand Fabric connectors  
   iii. Zero Touch Configuration/Zero Touch Provisioning  
   iv. Automated Response Systems (SOAR/Handlers)  
   v. FortiSIEM log automation triggers  
b. Demonstrate knowledge of Fortinet build-in scripting capabilities  
   i. FortiManager CLI/TCL Scripting  
   ii. FMG CLI Template + Variables  
   iii. FortiGate AutoScript  
c. Demonstrate knowledge of Fortinet API configuration and usage  
   i. FortiGate webhook triggers  
   ii. API Integration within the Security Fabric  
   iii. Understand principles of API usage (including required config)  
   iv. Solutions for rollout and management of large scale FortiGate networks (Fortinet or 3rd party management tools)

Practical Exam Certification Topics

1. Networking  
a) SD-WAN Deployments  
b) Dynamic Routing  
c) Traffic Engineering  
d) Secure Access  
e) VPN Connections  
f) High Availability and clustering  
g) Troubleshooting network deployments

2. Central Management  
a) Central Management Deployments  
b) Automation  
c) Security Operations  
d) Troubleshooting Central Management Deployments

3. Authentication  
a) Authentication Integration  
b) Troubleshooting Authentication Scenarios

4. Threat Protection  
a) Securing EndPoints  
b) Securing Applications  
c) Securing the Network  
d) Troubleshooting Threat Protection
Products and Firmware Versions

This section details all the products and firmware versions used for the NSE 8 exams.

The new version of the NSE 8 exams will be based on the most current firmware available on the Fortinet support site. The NSE 8 candidate should have the knowledge required to configure a network environment with the latest firmware versions available, and up to two major releases, following the date that the exam becomes available to the public.

<table>
<thead>
<tr>
<th>Product</th>
<th>Base Firmware</th>
<th>Written Exam</th>
<th>Practical Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiAnalyzer</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiAuthenticator</td>
<td>6.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiManager</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiSandbox</td>
<td>4.x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiADC</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiWeb</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiMail</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiClient</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiClientEMS</td>
<td>7.x +</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FortiSwitch (VM)</td>
<td>7.x +</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiSwitch</td>
<td>7.x +</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>FortiAP</td>
<td>7.x+</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiDDoS</td>
<td>5.x +</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiNAC</td>
<td>9.x +</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiExtender</td>
<td>7.x +</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiSIEM</td>
<td>6.x +</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiEDR</td>
<td>5.x+</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>FortiSOAR</td>
<td>7.x +</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Note: Firmware versions may change at any time without notice. Please review the latest version of this document, the FAQ document, and the NSE 8 exam description, when preparing for your exam.

About the base firmware versions:

- The NSE 8 certification program will have base firmware versions for all the solutions. The program will be adaptable to support up to two additional major releases during the life of the exam.
- The expert candidate’s knowledge of Fortinet features, technologies, and solutions should extend beyond a single OS version.

Additional exam components include, but are not limited to:
- Windows 2019
- Lubuntu desktop
- Debian Linux server

**Recommended Study Materials**

This section lists the recommended study materials to help certification candidates prepare for the NSE 8 certification exams.

Administration guides and handbooks:
- FortiGate, FortiManager, FortiAnalyzer
- FortiADC, FortiWeb, FortiMail
- FortiSandbox, FortiAuthenticator, FortiClient
- FortiSwitch
- CLI references
- Cookbooks
- Fortinet Knowledge Base articles

**Recommended Preparatory Courses**

The NSE 8 certification exams have no prerequisites, but it is highly recommended that test candidates complete the following courses before attempting the certification exams.

<table>
<thead>
<tr>
<th>NSE 4</th>
<th>NSE 5</th>
<th>NSE 6</th>
<th>NSE 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGate Security</td>
<td>FortiAnalyzer</td>
<td>FortiWeb</td>
<td>LAN Edge</td>
</tr>
<tr>
<td>FortiGate Infrastructure</td>
<td>FortiManager</td>
<td>FortiMail</td>
<td>SD-WAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FortiADC</td>
<td>Enterprise Firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FortiSandbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FortiAuthenticator</td>
<td></td>
</tr>
</tbody>
</table>
NSE 8 Immersion Workshop

The NSE 8 Immersion workshop is available for candidates that have passed the NSE 8 written exam. This workshop will give you a hands-on experience at the level of the NSE 8 exam as a preparation and learning tool for your NSE 8 practical exam. It is highly recommended to use this experience as a self-assessment and to get familiar with the delivery tools used on the actual exam as part of your preparation.

Recommended Knowledge and Experience

It is strongly recommended that the test candidates have extensive knowledge and experience in the following areas:

- Third-party systems and practices:
  - Advanced virtual Infrastructures
  - Advanced switching and routing
  - Advanced operating systems: Windows and Linux
  - Security vulnerabilities and penetration testing tools and techniques

- Fortinet solutions, networking, and security practices:
  - Design
  - Deployment
  - Management and administration
  - Troubleshooting

For more information, please visit:
https://www.fortinet.com/support/training/network-security-expert-program.html
Successful Candidates

Sequential Identification Numbers

The Fortinet NSE 8 certification uses a numbering scheme to uniquely identify candidate certification. The numbering scheme starts at 3072.

This numbering scheme is based on cryptography. In cryptography, key size or key length is the number of bits in a key used by a cryptographic algorithm (such as a cipher). Key length defines the upper bound on an algorithm's security. RSA key 3072 is the next step for keys intended to extend beyond 2030. This is the same approach that we have for our NSE 8 certified engineers.

Reference: https://en.wikipedia.org/wiki/Key_size

This unique ID is perpetual and tied to the test taker's name and information.

Awards

If the test taker passes both exams (written and practical) he/she will receive, at their registered home/office address, the following awards in a customized award box (the content of the box may differ in some cases):

- Electronic NSE 8 certificate:
  - Available for download from the test taker’s Fortinet Training Institute account

- Physical NSE 8 certificate:
  - Signed by Ken Xie (CEO) and Michael Xie (CTO)

- NSE 8 plaque:
  - With the test taker’s name and NSE 8 ID printed

- NSE 8 Pin:
  - With the logo of the program
NSE 8 Validity and Recertification

Certification Validity

The NSE 8 certification is valid for three (3) years.

**Important!** On January 31, 2022, the Fortinet Training Institute changed the validity period of the NSE 8 Certification for all valid (active) certifications, and for all new certifications granted after this date, from two (2) to three (3) years.

First-time test takers:

- For the written exam: unlimited attempts.
- For the practical exam: unlimited attempts are also allowed. Passing the written exam is mandatory to schedule and attempt the practical exam.

Recertification

To recertify the following requirements apply:

- While the certification is still valid (within the three-year period), the candidate must take and pass the written exam only (three attempts maximum).

- An additional 30-day period after the expiration date is available to candidates who must recertify. The 30-day period starts on the certification expiration date. If the exam is scheduled and passed within the valid three-year period of the certification plus the 30 days, there will be no penalties, and the certification will remain valid for an additional three years.

- If the candidate fails the written exam after three (3) attempts, they must continue to attempt the written exam until they pass it; however, the candidate must schedule and pass the most updated version of the practical exam also.

- When scheduling the written exam for recertification at Pearson VUE, the candidate must ensure that the scheduled appointment is no more than six (6) months before the expiration date of their current certification.

**Important!** The earliest recertification testing appointment allowed is six (6) months before certification expiration.

The Fortinet Training Institute sends expiration notifications to the users as follows:

- 90, 45, and 5 days before the expiration date
The NSE 8 certification date is fixed to the date the test taker passed the practical exam. This is the date shown on the NSE 8 plaque and the physical certificate shipped in the NSE 8 award box. If the candidate keeps the certification valid after the recertification is completed, the only change will be the expiration year of the certification, the day and the month will remain unchanged.

When the candidate passes the written recertification exam, it also recertifies any other NSE certifications the candidate has achieved previously, including those that have expired, for the same period of three years.

About This Document

The purpose of this document is to provide all the information required by the test taker to prepare for the NSE 8 certification.

Document Version

This document contains all the current information related to the NSE 8 program and its components. It is subject to change without notice. Review the latest version of this document, the FAQ document, and the NSE 8 exam description on the Fortinet public website: