Certification Guide

McAfee Certified Product Specialist

McAfee Network Security Platform (NSP)

Why Get Intel Security Certified?

As technology and security threats continue to evolve, organizations are looking for employees with the most up-to-date certifications on the most current techniques and technologies. In a well cited IDC White Paper, over 70% of IT Managers surveyed felt certifications are valuable for their team and were worth the time and money to maintain.

Becoming Intel Security certified distinguishes you from other security professionals and helps validate that you have mastery of the critical skills covered by the certification exams. Earning a certification also your commitment to continued learning and professional growth.

About Intel Security Certification Program

Currently, Intel offers two industry-recognized certifications as part of our Intel Security Certification Program: Intel Security Certified Product Specialist and Intel Security Certified Security Professional.

The Intel Security Certified Product Specialist certifications are designed for candidates who administer a specific McAfee product or suite of products, and have one to three years of experience with that product or product suite. This certification level allows candidates to demonstrate knowledge in the following key product areas:

- Installation
- Configuration
- Management
- Basic architecture and troubleshooting

The Intel Security Certified Security Professional certifications are designed for security practitioners, penetration testers, auditors, consultants, administrators — with one to three years of experience. This certification level allows candidates to demonstrate knowledge in the following high-level assessment areas:

- Profiling and inventorying
- Vulnerability identification
- Vulnerability exploitation
- Expanding influence

About This Guide

This guide is intended to help prepare you for the **Intel Security Certified Security Professional — Network Security Platform (NSP)** exam. For more information about other certification exams or about the Intel Security Certification program go to **www.mcafee.com** and select **For Business**, **Enterprise**, **Services**, and then **Education Services**.

Highlights

This guide has been developed as a resource for your preparation to take the Intel Security Certified Product Specialist — NSP Exam (MA0-101). The following information is provided:

- About the Intel Security Certification Program
- Exam details
- Suggested resources for exam preparation
- Knowledge domain topics
- Sample exam items

Intel Security Certified Product Specialist — Network Security Platform (NSP)

This exam validates that the successful candidate has the knowledge and skills necessary to successfully install, configure, and manage a McAfee Network Security Platform solution. It is intended for security professionals with one to three years of experience using the McAfee NSP product and associated technologies.

intel Security

Certification Guide

Exam Details

- Associated exam: MA0-101
- Associated Training: McAfee Network Security Platform Administration (4 days)
- Number of Questions: 100
- Exam Duration: 140 Minutes
- Passing Score: 70%
- Exam Price: $150 USD (Exam prices are subject to change. Please visit the following link for exact pricing: **http://www.pearsonvue.com/intel/index.asp**

Exam Preparation

Suggested preparation for this exam is:

- 4 Days Network Security Platform Administration training (**https://mcafee.netexam.com/catalog.html**)
- Minimum of one year using McAfee NSP
- Knowledge domains (see later in the guide)
- Sample questions (see later in the guide)

Certificate Registration

Intel Security has partnered with Pearson VUE, the global leader in computer-based testing, to administer our certification program. Pearson VUE makes the certification process easy from start to finish. With over 5,000 global locations, you can conveniently test your knowledge and become Intel Security Certified.

To register for an exam, go to: **http://www.pearsonvue.com/intel/index.asp**

Exam Duration

The Intel Security Certification Program has built in time to include the following actions during an exam challenge at each testing facility:

- Time to answer exam questions
- Time to review instructions and provide comments after completion

Intel Security reserves the right to change the exam content and time requirements at any time. The most accurate means of obtaining this information is to contact the exam delivery provider on the day of your exam challenge. A notification appears on your screen before the exam begins that shows the maximum time allowed for answering the questions in that exam.

Certification Transcripts

Individuals who have passed an Intel Security certification exam are granted access to the Intel Security Certification Program Candidate site. On the site, you will find:

- Your official Intel Security Certification Program transcript and access to the transcript sharing tool
- The ability to download custom certification logos
- Additional information and offers for Intel-certified individuals
- Your contact preferences and profile
- News and promotions

McAfee Network Security Platform Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee Network Security Platform Administration** (4 days) course is recommended.

This course provides in-depth training on how to use McAfee Network Security Platform (NSP). At the end of this course, you will be able to plan the NSP deployment, install and configure the Manager, manager users and resources, configure and manage policies, analyze and respond to threats, and tune your security policies for maximum effectiveness.

To register for this course, go to: **https://mcafee.netexam.com/catalog.html**

Practical (Hands-on) Experience

A minimum of one year of experience using McAfee NSP and associated technologies. Recommended hands-on activities include but are not limited to:

- Architecture design
- Installation/upgrade
- Configuration
- Management
- Troubleshooting

Technical ServicePortal

The Technical ServicePortal provides a single point of access to valuable tools and resources, such as:

- Documentation
- Security bulletins
- Technical articles
- Product downloads
- Tools

To access the ServicePortal, go to: **https://support.mcafee.com**

Expert Center Community

The Expert Center is a community for McAfee product users. Here you will find valuable information for your McAfee products, such as

- Instructional videos and whitepapers
- Discussion feeds for experts and other users
- Guidelines to establish baselines, and to harden your IT environment
- Ways to expedite monitoring, response, and remediation processes

To access the Expert Center, go to: **https://community.mcafee.com/community/business/expertcenter**

Exam Knowledge Domains

Setup

- NSP Installation (e.g. server requirements, planning)
- NSP Configuration (e.g. domains, user account, authentication, response management and notification)
- NSP Navigation
- Sensor Installation (e.g. sensor sizing, planning, placement, ports, operational modes)
- Sensor Configuration (e.g. CLI commands)
- Maintenance and troubleshooting (e.g. backup, database tuning, file pruning)
- Integration (e.g. EPO, NTBA, GTI)

Policy Management

- Policy Manager (e.g. creation, assignment)
- IPS Policies (e.g. custom attach editor, attack definitions, import/export, system tuning)
- Advanced Malware Policies
- Inspection Options Policies
- Connection Limiting Policies
- Firewall Policies
- Quality of Service (QoS) Policies
- Exceptions (e.g. ignore rules, fliehash exceptions, domain name exceptions)
- Objects (e.g. policy groups, rule objects, attack set profiles)

Event Management

- Dashboard Monitoring
- Threat Analysis (e.g. threat explorer, malware detections, attack log, pcap analysis, recognizing patterns
- Response Actions (e.g. white list, black list, update policies, create ignore rules)
- Reporting

Sample Exam Items

The following exam items are provided for review. These items are similar in style and content to those referenced in the Intel Security Certified Product Specialist — NSP exam. The answers are provided after the questions.

1. **Upon initial configuration, which of the following allows management connection to the Sensor?**
   - **A** RJ45
   - **B** RJ11
   - **C** Monitoring port
   - **D** Console port
2. **To archive alerts and packets logs, you must navigate through which of the following paths?**
   - **A** Manage | Maintenance | Archiving
   - **B** Manage | Alerts | Archiving
   - **C** Maintenance | Alerts | Archiving
   - **D** Manage | Maintenance | Alerts | Archiving
3. **Why is the DBAdmin tool considered a preferred method of performing system maintenance tasks that could be performed within the NSM?**
   - **A** Saves additional workload on the Manager
   - **B** Reliability
   - **C** Speed
   - **D** Ease of use
4. **Which step needs to be completed before a sensor can be configured?**
   - **A** Sensor IP addressing must be set
   - **B** Sensor must be added to the Manager
   - **C** Sensor username and password must be set
   - **D** Sensor Gateway addressing must be set
5. **Which command can be issued on a Sensor to check the health of the Sensor?**
   - **A** show health sensor
   - **B** show health status
   - **C** show config
   - **D** check health
6. **In the Policy Manager, a policy can be modified at the interface level unless that policy was initially created in a:**
   - **A** Parent Domain.
   - **B** Child Domain.
   - **C** Top Domain.
   - **D** non-adjacent domain.
7. **A rule set cannot be applied to a policy with:**
   - **A** the same rule set applied to both traffic flows.
   - **B** one rule set applied to all traffic.
   - **C** different rule sets applied to each traffic flow.
   - **D** two rule sets applied to each traffic flow.
8. **At the device level, the IPS policy cannot be modified to include/exclude:**
   - **A** Default McAfee Attacks.
   - **B** Modified McAfee Attacks.
   - **C** Custom McAfee Format Attacks.
   - **D** Custom Snort Attacks.

9. **On the NSP CLI, what is the command that enables the L2 mode feature?**
   - **A** layer2 mode off
   - **B** layer2 mode on
   - **C** layer2 mode assert
   - **D** layer2 mode deassert
10. **If domain-level exception object settings are assigned at the Sensor level:**
   - **A** other resources using that object on that Sensor are not affected
   - **B** other resources using that object on that Sensor are also affected
   - **C** a Fault level of warning will be sent to the NSM to warn the administrators
   - **D** the Sensor level settings will be ignored; domain-level settings always take precedence

Answer Key

1. D
2. D
3. A
4. B
5. A
6. A
7. D
8. B
9. B
10. B

Intel Security
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com