SonicWall Network Security Professional Course (SNSP)

Description:

A key issue affecting an organization's business productivity and employee efficiency today is its ability to respond to dynamic changes in the **cyber threat landscape**.

Coming up on the heels of the highly successful SNSA program launched earlier this year, SonicWall now presents the **SonicWall Network Security Professional** (**SNSP**) course, an expert-level training and certification program that builds on the **enterprise security skills** learned in the SNSA course.

Previously known as the **Network Security Advance Administration** (**NSAA**) course, the revamped **SNSP** curriculum expands on the topics covered in **SNSA** and features advanced SonicWall firewall configuration and administration tasks aimed at helping enterprises adapt to dynamic security environments.

Relevant changes to the curriculum include an enhanced and deeper scope of **SonicOS 6.5**.x features and functionality, as well as changes in the learning and delivery methodologies to better balance the professional needs of the students and the business requirements for network and cyber security.

Course Objectives:

The students will learn how to monitor, investigate, analyze, and configure SonicWall Next-Gen firewalls running SonicOS to enable **advanced functionality** related to Secure and Remote Connectivity, Network Optimization, and Threat Prevention.

Upon successful completion of the SNSP program, the students will be able to demonstrate SonicWall product expertise and the application skill sets required to mount a proactive, effective defense against current and evolving network and cyber security threats.

Training Delivery Modality:

A Learner-centric **Instructor-Led** Classroom Training approach that will enhance your learning experience:

- The instructor-facilitated sessions include fully immersive hands-on lab activities that will guide you through advanced firewall configuration and administration tasks in a simulated SonicOS environment.
- The scenario-based sessions will also enable you to assess, evaluate, and take the required actions over various types of cyber threats in a risk-free lab environment.
- The lecture components of the curriculum include best practices and SonicWall recommendations for various configuration tasks.

Certification:

Successful completion of the SNSA curriculum qualifies you to take the SNSP Certification Exam. While this exam is not a part of the class, you will have access to it on-line via your individual SonicWall University account.
For more information about certifications, visit the About SonicWall Certifications page.

Duration:

Two (2) Business Days

Intended Audience:

Security professionals, System engineers, channel partners, service partners, and end users with 1+ years of experience in implementing IT security technologies (Network, Applications, and Systems) and are **also SNSA-certified**.

Prerequisites:

- In-depth understanding of networking fundamentals and architecture, including OSI data model, IP addressing, dynamic routing, switching, VoIP, cloud and virtualization, network topologies and connectivity, wired and wireless networks, system backup and recovery, network applications and peripherals, network management protocols, etc.
- Knowledge of enterprise security concepts and technologies, such as firewalls, gateways, VPN architecture, threat protection, content filtering, NAT, IPSec, SSL, DPI, zones, encryption and cryptography, access control, Identity management, security compliance policies, latest cyber threats and vulnerabilities, etc.
- **SonicWall Network Security Administration** (**SNSA**) certification.

Course Syllabus:

Instructor-Led Training Sessions

0 Course Introduction and Overview
1. Configuring VPN Auto Provisioning
2. Configuring Advanced Routing
3. Configuring Advanced Interface Settings
4. Using SonicOS CLI
5. Configuring Capture Client
6. Capturing and Replaying Packets
7. Configuring DPI-SSL/TLS Server
8. Configuring DPI-SSH
9. Configuring App Rules
10. Configuring App Control
11. Configuring Advanced High Availability
12. Excluding Trusted Content
13. Resolving and Reporting False Positives
14. Configuring Content Filtering
15. Implementing Best Practices

Student Assessment:

- Formative evaluations (knowledge checks and hands-on classroom exercises) are incorporated throughout the course. The proctored Certification exam is available on-line via your SonicWall University Account. When you complete the instructor-led training course, you will be given an exam activation key that will allow you to access the exam. Any participant who successfully completes this course and passes the certification exam will be deemed a **SonicWall Network Security Professional** (**SNSP**).
- The exam is administered outside the class. You are given 180 minutes for 60 questions. A passing score is 75% or higher. The exam covers all course material.
- The exam is proctored online. At the end of the exam you are immediately notified of your exam score and if you tentatively passed or failed the exam. Once the proctoring review is complete, you will receive your final exam results. Upon successfully passing the exam, and completion of the proctoring review, you will be sent an email containing your SNSP certificate.
- In addition, you can view your certification details, such as the certification expiration date, at SonicWall University. You can also print your certificate and access the **SNSP** certification logo for use on your business cards, email signatures, and resume.

Duration of Certification:

All SonicWall Certifications are good for two years from the date that you pass the exam.

For more information, email training@SonicWall.com