



SonicWALL Network Security Basic Administration Training (NS-101)

Cursusduur: 2 Dagen Cursuscode: SW400

Beschrijving:

Learn to design, implement, and troubleshoot SonicWALL security devices running SonicOS firmware. This course, formerly titled Network Security Essentials Administrator, provides you with the background, knowledge, and hands-on experience to begin designing, implementing, and troubleshooting SonicWALL security appliances running SonicOS firmware. This technical training covers configuration and deployment of the SonicOS firmware. You will become familiar with a wide spectrum of SonicWALL's innovative feature set, such as Unified Threat Management (UTM), Single Sign On, VPN, SSL VPN, and Content Filtering Service. As you examine the wide array of security features SonicOS has to offer, you will learn validation of settings and troubleshooting techniques using the SonicWALL diagnostic tools. Formative evaluations (knowledge checks and hands-on exercises) are incorporated throughout this course to test new skill sets.

SPECIAL PROMOTION: a SonicWALL TZ210, 5th generation firewall/VPN/UTM appliance, is until 31 March 2012 included for FREE in the price of the course.

Doelgroep:

System engineers, channel partners, service partners, and system administrators

Doelstelling:

- Design, implement, and troubleshoot SonicWALL security appliances running SonicOS Enhanced firmware
 - Components of SonicWALL's feature set
 - Configure and deploy SonicOS Enhanced firmware
 - Use SonicWALL diagnostic tools to validate and troubleshoot
-

Vereiste kennis en vaardigheden:

To attend this course, prerequisite skills and knowledge are required, including completing three e-Learning courses prior to beginning this class. Information from these e-Learning modules is included on the certification exam. The prerequisite training is available from SonicWALL at <http://www.sonicwall.com/us/support/eLearning.html> and includes:

Network Security Technology Overview e-Learning (~2 hours)

For those new to network security, this optional online course provides an introduction to the key concepts and fundamentals of network security. While this course is not mandatory, it is strongly suggested.

Network Security Essentials e-Learning (~6 hours)

This online course will provide you with critical foundational information concerning firewall technology, security risks and remediation, and network security design and implementation considerations. Additionally, you will learn how to configure and implement SonicWALL firewall appliances and extend the firewall's capability using rules, security applications, and other network specific functions and troubleshooting techniques. You will practice key activities through online simulations.

Virtual Private Networking with SonicOS e-Learning (~6 hours)

A critical follow-on to the Network Security Essentials e-Learning course, this online course will give you a comprehensive education

Examens en certificering

Certified SonicWALL System Administrator (CSSA) for Network Security

The certification exam is available online via your personal work MySonicWALL account. During training, you will be given an activation key that will allow you to access the exam up to three times. If you successfully complete this course and pass the certification exam, you will be deemed a Certified SonicWALL System Administrator (CSSA).

The exam is administered outside the class. You will be allotted 180 minutes to complete 60 questions. A passing score is 80% or higher.

At the end of the exam, you will be notified immediately of your exam score and pass or fail status. Upon passing the exam, you will receive an e-mail containing your CSSA certificate. You can view your certification details, print your certificate, access CSSA certification logos, and much more on MySonicWALL.

in core VPN technology, design, and implementation considerations. You will also learn about SonicWALL-specific VPN configuration and deployment as well as troubleshooting techniques. As in Securing Networks with SonicOS, you will be able to practice key activities through online simulations.

Other skills required include:

- Basic knowledge of networking concepts, network topologies, and the OSI model of networking protocol stacks
- Understanding of TCP/IP, network addressing, subnets, and Network Address Translation (NAT)
- Knowledge of basic router concepts
- Familiarity with IPSec functionality and implementation

Cursusinhoud:

1. Course Introduction	• SSL VPN with Local User Database	Lab 4: NAT: Inbound Server Access
2. Operating System Fundamentals	• SSL VPN and Global VPN Client with LDAP Authentication	Lab 5: WAN ISP Failover and Outbound Load
• Registration	• Content Filtering Service	Lab 6: Policy-Based Routing
• OS Fundamentals	• Content Filtering Service Using Single Sign-On	Lab 7: Site-to-Site VPN Settings
• System Backup and Restore	5. Unified Threat Management	Lab 8: Hub and Spoke VPN Settings (Optional)
3. Scalability and Reliability	6. Secure Wireless Overview	Lab 9: Route-Based VPN
• WAN ISP Failover and Ethernet Load Balancing	• Wireless Products	Lab 10: Global VPN Client with Local Database (Optional)
• Policy-Based Routing	• Wireless Threats	Lab 11: SSL VPN with Local Database
• High Availability	• Wireless Solutions	Lab 12: SSL VPN with LDAP Authentication
4. Secure Access and Content Control	Labs	Lab 13: Content Filtering Service with LDAP
• VPN: Gateway-to-Gateway, Hub and Spoke, Mesh	Lab 1: Updating the SonicOS Enhanced Firmware	Lab 14: CFS with LDAP Authentication Using Single Sign-On
• Route-Based VPN	Lab 2: Initial Setup and Configuration	Lab 15: Unified Threat Management
• GVC with Local User DB	Lab 3: SonicWALL Administration	

Extra informatie:

Please arrange your coursebooking via the SonicWALL partner. See the following URL.
http://www.sonicwall.com/benelux/2756.html#heading_7923

Nadere informatie:

Neem voor nadere informatie of boekingen contact op met onze Customer Service Desk 030 - 60 89 444

info@globalknowledge.nl

www.globalknowledge.nl

Iepenhoeve 5, 3438 MR Nieuwegein